PUBLICAÇÕES DO CENTRO DE ESTUDOS MATEMATICOS
DA
FACULDADE DE CIÊNCIAS DO PORTO

N.º 19

PUBLICAÇÃO RECEBEU UM SUBSÍDIO DA JUNTA DE INVESTIGAÇÃO MATEMÁTICA

GRUPOS ABELIANOS
ANEIS E IDEAIS NÃO COMUTATIVOS
SISTEMAS HIPER-COMPLEXOS
E
REPRESENTAÇÕES

Tomo 2º

por

A. ALMEIDA COSTA

prof.ext.da Universidade do Pôrto

1948

ÍNDICE

PREFÁCIO

Conforme se anunciou no nº 3 desta Colecção, intitulado "Grupos abelianos e Anéis e Ideais não comutativos", deveríamos publicar agora um outro número que completasse aquele, por forma a expor o conteúdo da importante memória de E. Noether, "Hyperkomplexe Grössen und Darstellungstheorie", publicada em 1929 no tomo 30 da Mathematische Zeitschrift. O projecto formulado não deixou de executar-se (Cap. VIII e IX). Foi-se, todavia, bastante mais longe. Por um lado, seguindo ainda a grande algebrista, tratam-se (Cap. IX e XI) aplicações da teoria das representações aos anéis de matrizes e à teoria não comutativa de Galois, tais como a eminente autora as faz no seu trabalho "Nichtkommutative Algebra", publicado em 1933 no tomo 37 daquela citada revista; por outro, retoma-se toda a doutrina constante da 2ª parte do nosso livro referido, de modo a desenvolvê-la no sentido de pôr o leitor ao corrente de resultados bastante recentes sobre a teoria geral dos anéis não comutativos, resultados devidos a von Neumann, Hopkins, Asano, Dieudonné, Levitzki e Almeida Costa, muitos dos quais recebem pela primeira vez uma exposição ordenada. É nos 4 primeiros Capítulos que, sobre um fundo devido essencialmente a Wedderburn, Dickson, Artin, Noether e Köthe, se faz esse desenvolvimento.

Os Capítulos V e VI começam a preparação para as álgebras. Os enunciados que neles se dão expõem-se, essencialmente, como faz Albert nas suas importantes obras, muito conhecidas: "Modern Higher Algebra" e "Structure of algebras". Este último livro é largamente utilizado em quase todo o texto. No Capítulo VII, a sua utilização foi dupla. Certos resultados que aí estabelecemos sobre os corpos comutativos provêm da sua influência, associada à do trabalho fundamental de Steinitz, "Algebraische Theorie der Körper", dado à estampa no "Journal für die reine und angewandte Mathematik", tomo 137, 1910.

Embora este tomo seja extenso, muito deixamos de versar, que se encontra já em livros notáveis vindos a lume no curto espaço de 9 anos (1935, 1939, 1943 e 1944). Queremos referir-nos aos livros de Deuring, Albert, Jacobson e Artin-Nesbitt-Thrall, frequentemente citados na exposição. Por isso aqui

manifestamos o desejo de fazer seguir este número de dois outros tomos, não previstos a princípio.

A parte final do volume (Cap.XII) é consagrada à Teoria dos produtos cruzados, incluindo uma generalização de Teichmüller. No tomo seguinte, voltaremos à teoria geral dos anéis não comutativos e prosseguiremos nas álgebras, por forma a salientarmos mais algumas aplicações da teoria das representações (Brauer) e a estudar as álgebras com radical (Brauer).

Relembrando uma ordem de ideias a que aludimos já no nº 1 (Elementos da Teoria dos Grupos), digamos também que tratamos o fundamental para as aplicações da "Teoria das representações dos anéis e dos grupos abstractos" à Física dos Quanta [Wigner,(1) Weyl, van der Waerden]. Pelo que toca às representações dos grupos, a exposição dos métodos de G.Frobenius e I.Schur envolve ideias mais simples, como oportunamente se afirmou. Esse facto levou-nos a dedicar-lhe o décimo Capítulo deste livro, que pode ser lido independentemente dos anteriores, e em seguimento imediato àquela nossa publicação de nº 1. E, dando-se a circunstância de tratarmos, ainda nesse Capítulo X, algumas questões fáceis relacionadas com as teorias das representações do grupo das rotações do espaço ordinário e das representações do grupo de Lorentz, julgamo-nos dispensados de escrever o anunciado tomo 2º dos "Elementos da Teoria dos Grupos". É evidente que a índole do livro, não obstante o papel essencial que cabe em Quântica à teoria das representações dos grupos contínuos [Lie, Cartan, Weyl], não poderia permitir-nos outras referências a essa importante questão, mal se justificando até os elementos que expomos.

A fim de serem ilucidados os interessados nos assuntos da Álgebra abstracta e das suas aplicações, indicamos aqui a ordem que convém seguir na leitura das nossas exposições so-

(1) Fazemos aqui uma referência especial ao livro de E.Wigner, por não ser citado no texto: "Gruppentheorie und ihre Anwendungen auf die Quantenmechanik der Atomspektren". Berlin, 1931.

bre este domínio:

nº 1 - Elementos da Teoria dos Grupos;

nº 7 - Elementos da Teoria dos Anéis;

nº 3 - Grupos abelianos e Anéis e Ideais não comutativos;

nº 19- Sistemas hiper-complexos e representações.

Salientaremos, porém, que a compreensão duma grande parte do exposto neste número (em especial os 4 primeiros Capítulos) pouco mais exige do que o conhecimento dos quatro primeiros cadernos de "Álgebra Moderna", saídos no Porto por iniciativa da Junta de Investigação Matemática.

Depois da publicação, em 1930 e 1931, dum livro célebre de B.L.van der Waerden, "Moderne Algebra", em dois tomos, ficou ao alcance dos estudiosos de todo o mundo um instrumento de trabalho que os habilita a tomar contacto rápido com a Álgebra abstracta, incluindo os resultados mais recentes.(1) A influência exercida por esse livro reconhece-se no estilo e nas citações de grande número de trabalhos feitos em toda a parte. Nos nossos volumes, atrás citados, todos publicados nesta Colecção, transparece claramente que tem sido ele o nosso grande orientador.

A actividade, em Portugal, no domínio da Álgebra moderna, é extremamente reduzida. Estamos absolutamente convencidos de que poderiam realizar-se, no nosso país, progressos rápidos nesta matéria, se alguns jovens diplomados portugueses a ela quizessem dedicar a sua atenção. Os métodos da Álgebra moderna revestem-se duma elegância e dum sentido de generalidade que parecem não ter rival. Recebe-se uma sensação de alegria e segurança, sempre que, nos outros ramos da matemática, métodos análogos podem ser usados. O regime de adaptação à sua disciplina pode, de começo, revelar-se penoso. Vencidas as primeiras dificuldades, que provêm apenas de educação, abrem-se, em seguida, horizontes que interessam. Os trabalhos de grande número de algebristas célebres aparecem ao estudioso como exemplos de reflexão acabada, que tomará por modelo e se esforçará por imitar.

(1) A 2ª edição desta obra tem as datas de 1937 (tomo 1º) e de 1940 (tomo 2º).

Se os nossos esforços puderem contribuir, por pouco que seja, para criar alguns entusiastas que se abalancem aos estudos de que falamos, largamente nos sentiremos recompensados de os ter efectuado, certos como estamos de que as nossas indicações poderão evitar perdas de tempo em busca de planos de trabalho sempre difíceis de conceber.

Queremos fazer uma observação importante. Há, em todo o texto, erros de várias ordens: há erros de doutrina, há lapsos de revisão, há índices ilegíveis, etc. [logo na pg.1, linha 21, se deve pôr $\lambda a = \lambda(u.a)$, em vez de $\lambda a = \lambda.u.a$!]. O leitor atento não deixará de o observar e de fazer as necessárias correcções. Agradecer-lhe-emos toda a crítica que nos dirija.

Para terminar, deixamos aqui exarados à Junta de Investigação Matemática os nossos agradecimentos pelo importante subsídio que nos foi concedido, a fim de podermos custear uma parte desta publicação.

Porto, Setembro de 1946.

A. Almeida Costa

ANEIS E IDEAIS NÃO COMUTATIVOS

Capítulo I

Aneis e seus ideais como sub-módulos

1) Generalidades - Dado um anel $\mathcal{Y}$, êste é sempre um grupo abeliano com os seguintes operadores: os elementos de $\mathcal{Y}$.

Um ideal direito $\mathcal{K}$ é um sub-módulo admissível de $\mathcal{Y}$, se os elementos do anel operam à direita; um ideal esquerdo $\mathcal{H}$ é um sub-módulo admissível, se os elementos do anel operam à esquerda; e um ideal bilateral $\mathcal{A}$ corresponde ao caso de os elementos de $\mathcal{Y}$ operarem à direita e à esquerda.

Pode existir, para $\mathcal{Y}$, um outro domínio operatório estranho, cujos elementos representaremos por $\lambda, \mu, \nu, \ldots$.

Nêsse caso, suporemos que, dados dois elementos $a, b \in \mathcal{Y}$, os novos operadores, além das propriedades de operadores modulares, segundo as quais,

$$\lambda a \in \mathcal{Y}, \quad \lambda(a+b) = \lambda a + \lambda b,$$

gozarão ainda da propriedade seguinte: $\lambda(ab) = \lambda a.b = a.\lambda b$.

Os sub-grupos admissíveis serão, então, os ideais admissíveis: tais ideais conterão, com a, os elementos $\lambda a, \mu a, \ldots$.

Se $\mathcal{Y}$ tem elemento um = u, a limitação da noção de ideal que acaba de fazer-se é desnecessária, visto ser $\lambda a = \lambda.u.a = \lambda u.a$, $\lambda a = \lambda.a\ u = a.\lambda u$.

Tomemos agora dois ideais direitos $\mathcal{K}$ e $\mathcal{K}'$. Uma homomorfia ou uma isomorfia entre êstes ideais é sempre considerada no sentido operatório: se $a, b \in \mathcal{K}$, e $a', b' \in \mathcal{K}'$, $s \in \mathcal{Y}$, a correspondência entre a e a' ($a \longrightarrow a'$) está condicionada como segue:

$$a \longrightarrow a', \qquad a + b \longrightarrow a' + b',$$
$$\lambda a \longrightarrow \lambda a', \qquad a\,s \longrightarrow a's .$$

Um ideal direito diz-se simples, se não possui qualquer sub-ideal direito autêntico, salvo o ideal nulo. Trata-se de divisor normal simples, no sentido da terminologia usada nos grupos com operadores.

Um ideal direito, soma directa de ideais direitos não nulos,

$$\mathfrak{k} = \mathfrak{k}_1 + \cdots + \mathfrak{k}_s ,$$

diz-se unilateral e directamente decomponível (à direita).

No caso dum ideal bilateral $\mathfrak{a}$, suponhamo-lo soma directa de ideais bilaterais não nulos:

$$\mathfrak{a} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n .$$

Diz-se, então, que $\mathfrak{a}$ é bilateral e directamente decomponível.

É claro que esta definição sòmente se aplica aos ideais bilaterais, pois que a soma directa de tais ideais é um ideal bilateral.

Se um anel se pode escrever como soma directa de dois ideais bilaterais, diz-se redutível. No caso contrário é irredutível. Um anel $\mathfrak{J}$ diz-se totalmente redutível, se, dado um ideal bilateral arbitrário $\mathfrak{a}$, existir um ideal bilateral $\mathfrak{a}'$ tal que $\mathfrak{J} = \mathfrak{a} + \mathfrak{a}'$.

A designação de anel completamente redutível é costume empregar-se com o significado de anel que é soma directa de ideais direitos (ou esquerdos) simples.

Chama-se simples[1], todo o anel que não tem ideal bilateral, salvo os ideais nulo e unidade.

TEOREMA:- Se $a \in \mathfrak{J}$ é um elemento fixo, a correspondência $r \longrightarrow a\,r$, na qual $r \in \mathfrak{k}$, é um homomorfismo operatório.

Os elementos ar definem um ideal direito, havendo, assim, dois sub-grupos admissíveis a comparar. Ora

$$r \longrightarrow a\,r , \qquad r + r' \longrightarrow a(r + r') = ar + ar' ,$$
$$rs \longrightarrow a.rs = ar.s , \qquad \lambda r \longrightarrow a.\,\lambda r = \lambda .ar ,$$

o que demonstra o teorema.

(1) Os vocábulos que utilizamos podem encontrar-se com significado diferente noutros autores.

Teorema: - Um ideal direito simples só pode ter como correspondente homomorfo em $\mathfrak{J}$ o ideal nulo ou um ideal isomorfo. Se Δ é um conjunto homomorfo de $\mathfrak{k}$, Δ é um ideal $\mathfrak{k}'$.

Os elementos de $\mathfrak{k}$ que têm o elemento nulo de $\mathfrak{k}'$ como correspondente constituem um ideal $\mathfrak{k}'' \subseteq \mathfrak{k}$. Se $\mathfrak{k}'' = (0)$, tem-se um isomorfismo; se $\mathfrak{k}'' = \mathfrak{k}$, todos os elementos de $\mathfrak{k}$ têm por imagem o elemento nulo, q. e. d. .

As demonstrações que faremos em tôda a exposição referem-se geralmente a ideais direitos. É evidente, porém, que há demonstrações análogas para os ideais esquerdos. Também, em geral, não suporemos a existência de domínio operatório estranho ao anel. É fácil de vêr, todavia, quais as demonstrações que se estendem a tal caso, sempre, bem entendido, com a hipótese de serem ùnicamente postos em jôgo os ideais admissíveis.

2) Nilideais - Um elemento $a \in \mathfrak{J}$, que não seja o elemento nulo, diz-se nilpotente, se existir um inteiro σ tal que $a^\sigma = 0$. Os elementos nilpotentes são divisores de zero (à esquerda e à direita). Um sub-anel $\mathfrak{J}_1$, de $\mathfrak{J}$, que pode ser o próprio anel, diz-se nilpotente, se existir um inteiro σ tal que $\mathfrak{J}_1^\sigma = (0)$. σ chama-se, então, o expoente do sub-anel. Em particular, o ideal direito $\mathfrak{k}$ é nilpotente e de expoente σ, se se tiver $\mathfrak{k}^\sigma = (0)$. Diz-se ideal direito (ou esquerdo) semi-nilpotente o que goza da seguinte propriedade: um conjunto finito qualquer de elementos do ideal gera um sub-anel nilpotente. Todo o ideal nilpotente é semi-nilpotente, mas a inversa não é verdadeira. Um nilideal direito é um ideal cujos elementos são nilpotentes. Todo o ideal semi-nilpotente é nil ideal, mas a inversa não é verdadeira. Também se usam as designações análogas de nilanel e de sub-nilanel.

Tomemos o anel seguinte:[1] $0, r_1, r_2, \ldots$ são elementos constituindo uma infinidade numerável, para os quais

$$r_i + r_j = r_j + r_i , \quad r_i + r_i = 0 ; \quad r_i^2 = r_{i-1} , \quad r_1^2 = 0 .$$

Os produtos supõem-se comutativos e as leis associativa e

(1) Tirado de G.Köthe, "Die Struktur der Ringe, deren Restklassenring nach dem Radikal vollständig reduzibel ist", "Mathematische Zeitschrift", Band 32, 1930, pags. 161 a 186.

distributiva escrevem-se por hipótese. Todos os elementos dêste anel são nilpotentes. Trata-se dum nilanel (nilideal) que é semi-nilpotente mas não é nilpotente.

Teorema:- Se $a \in \mathfrak{J}$ é tal que $a^\rho = 0$, o elemento $(a+b)^\rho$ pertence ao ideal bilateral $\mathfrak{k}$, gerado por b. De facto, tem-se

$$(a+b)^\rho \equiv a^\rho(\mathfrak{k}) \equiv 0(\mathfrak{k}) \ .$$

Corolário 1º:- Se $\mathfrak{k}$ é nilideal, o elemento $a+b$ é nilpotente.

Corolário 2º:- A soma dum nilideal direito e dum nilideal bilateral é um nilideal direito.

No caso de ideais nilpotentes ou semi-nilpotentes, podemos precisar êstes resultados.

Teorema:- A soma de dois ideais nilpotentes direitos é um ideal nilpotente direito. Designemos com $\mathfrak{K}_1$ e $\mathfrak{K}_2$ os ideais. Por hipótese, tem-se $\mathfrak{K}_1^{\sigma_1} = (0)$, $\mathfrak{K}_2^{\sigma_2} = (0)$. O ideal direito $(\mathfrak{K}_1, \mathfrak{K}_2) = \mathfrak{K}$ verifica a relação $\mathfrak{K}^{\sigma_1+\sigma_2-1} = (0)$, como vamos vêr. Conforme as definições de produto e de soma de ideais, o ideal $\mathfrak{K}^{\sigma_1+\sigma_2-1}$ é uma soma de ideais direitos, cada um dos quais produto de $\sigma_1 + \sigma_2 - 1$ factores. Se, por ex., $\mathfrak{K}_1$ figura no produto menos de σ_1 vezes, necessàriamente figura $\mathfrak{K}_2$, pelo menos, σ_2 vezes. Os produtos em questão são pois, e por ex., da forma

$$\Delta = \cdots (\mathfrak{K}_2 \cdots)\ (\mathfrak{K}_2 \cdots) \cdots = \mathfrak{M}(\mathfrak{K}_2 \cdots)\ (\mathfrak{K}_2 \cdots) \cdots \ ,$$

com repetição do parêntesis σ_2 vezes, pelo menos. Ora tem-se

$$\Delta \subseteq \mathfrak{M}\mathfrak{K}_2 \cdot \mathfrak{K}_2 \cdots = \mathfrak{M}\mathfrak{K}_2^{\sigma_2} = (0) \ , \qquad \text{q. e. d.}$$

Tem também lugar êste outro

Teorema:- Existe sempre um ideal bilateral nilpotente que contém um ideal nilpotente direito dado. Conhecido $\mathfrak{K}$, consideremos o ideal esquerdo gerado pelos seus elementos.

Obtem-se $\mathfrak{N} = (\mathfrak{K}, \mathfrak{J}\mathfrak{K})$, que é um ideal bilateral. Estudemos $\mathfrak{J}\mathfrak{K}$. Tem-se, se $\mathfrak{K}^\sigma = (0)$,

$$(\mathfrak{J}\mathfrak{K})^\sigma = \mathfrak{J}(\mathfrak{K}\mathfrak{J})^{\sigma-1}\mathfrak{K} \subseteq \mathfrak{J}\mathfrak{K}^{\sigma-1}\mathfrak{K} = (0) \ .$$

$\mathfrak{N}$ aparece como soma de dois ideais nilpotentes direitos.

Corolário:- Um anel sem ideal nilpotente esquerdo também não tem ideal nilpotente direito.

Teorema:- A soma de dois ideais semi-nilpotentes direitos, $\mathfrak{K}_1$ e $\mathfrak{K}_2$, é um ideal direito semi-nilpotente $\mathfrak{K} = (\mathfrak{K}_1, \mathfrak{K}_2)$.[1]

Suponhamos, com efeito, que o teorema não tem lugar. Existirá, em $\mathfrak{K}$, um conjunto finito de elementos, $r_1, r_2, \ldots, r_m$, os quais gerarão um anel $\mathfrak{J}_1$ gozando da propriedade seguinte: dado um inteiro N, arbitràriamente grande, haverá um produto $\prod_{j=1}^{N} r_{i_j} \neq 0$, escolhendo convenientemente os i_j entre os números $1, 2, \ldots, m$. Pondo $r_k = r_k^{(1)} + r_k^{(2)}$, onde o índice superior (1) significa $\in \mathfrak{K}_1$, (2) significa $\in \mathfrak{K}_2$ e $k = 1, 2, \ldots, m$, vê-se que o anel $\mathfrak{J}_2$, gerado pelos elementos $r_k^{(1)}$, $r_k^{(2)}$ não é nilpotente, por ser $\mathfrak{J}_1 \subseteq \mathfrak{J}_2$. Chamemos $t_1, \ldots, t_q$ um conjunto tomado nos $r_k^{(i)}$, $i = 1, 2$, satisfazendo à condição de ser um conjunto mínimo gerando um anel potente (não nilpotente) $\mathfrak{Z}_1$. Nos t_j não podem figurar apenas elementos $r_k^{(1)}$ ou $r_k^{(2)}$, pois que êstes ou aqueles geram, por hipótese, aneis nilpotentes. Será $q \geq 2$. Visto que $t_2, \ldots, t_q$ geram um anel nilpotente $\mathfrak{Z}_2$, ponhamos $\mathfrak{Z}_2^\beta = (0)$, e, visto que t_1 é nilpotente, ponhamos $t_1^\alpha = 0$. Os elementos

$$t_1^\gamma \cdot \Pi\ t_{i_\sigma} \ , \quad \begin{cases} 0 < \gamma < \alpha \ , \\ i_\sigma = 2, 3, \ldots, q \ , \\ \text{número de factores do produto } \Pi \leq \beta - 1 \ , \end{cases}$$

(1) J. Levitzki, "On the radical of a general ring", Bulletin of the American Mathematical Society, vol. 49, 1943, pgs. 462 a 466.

são em número finito e serão designados com $v_1, v_2, \ldots, v_s$. Como t_1, por definição, pertence a um dos ideais $\mathfrak{N}_1$ ou $\mathfrak{N}_2$, todos os elementos v_j pertencem igualmente a um dêsses ideais. O anel gerado pelos v_j será nilpotente. Vamos vêr, porém, que os raciocínios que vínhamos fazendo, baseados na consideração de $\mathfrak{N}$ não ser semi-nilpotente, levam ao absurdo de ser potente o anel gerado pelos v_j. Para isso mostraremos que, dado um inteiro arbitràriamente grande, N', é possível encontrar um produto de mais do que N' factores v_j diferente de zero. Tomemos o inteiro $N > \beta(N'+2)$, e seja $P = t_{i_1} \cdot t_{i_2} \ldots t_{i_N}$ um produto de N factores t_j $(j = 1,2,\ldots,q)$ tal que $P \neq 0$. Não pode haver em P mais do que $\beta - 1$ factores consecutivos diferentes de t_1, e, por isso, pode escrever-se

$$P = \ldots (t_1^{\gamma_1} \ldots)(t_1^{\gamma_2} \ldots) \ldots,$$

onde os elementos entre parêntesis são necessàriamente elementos v_j. O número X dêstes v_j satisfaz à relação

$$X\beta + 2\beta - 2 \geqq N > \beta(N'+2),$$

o que dá $X\beta - 2 > N'\beta$, ou $X > N'$, q. e. d.

Teorema:- Existe sempre um ideal bilateral semi-nilpotente que contém um ideal direito semi-nilpotente dado. Conhecido $\mathfrak{N}$, o teorema resulta provando que $\mathfrak{a} = (\mathfrak{N}, \mathfrak{J}\mathfrak{N})$ é semi-nilpotente. E isto será conseqüência de se mostrar que $\mathfrak{J}\mathfrak{N}$ é semi-nilpotente. Se, com efeito, $\mathfrak{J}\mathfrak{N}$ não estivesse nessas condições, seria potente o anel gerado pelos elementos $t_1, t_2, \ldots, t_n$, onde $t_l = \sum s^{(l)} r^{(l)}$, $(s^{(l)} \in \mathfrak{J}$, $r^{(l)} \in \mathfrak{N})$. Seria igualmente potente um anel gerado por certos elementos $s_1 r_1, \ldots, s_q r_q$, que entram como parcelas nos t_l. Para cada N, existiria um produto $P = s_{i_1} r_{i_1} \ldots s_{i_N} r_{i_N} \neq 0$, onde $i_1, \ldots, i_N$ tomariam alguns dos valores $1,2,\ldots,q$. Escrevendo P sob a forma

$$P = s_{i_1} \cdot r_{i_1} \; s_{i_2} \ldots r_{i_{N-1}} \; s_{i_N} \cdot r_{i_N},$$

verificar-se-ia que $r_1 s_2, \ldots, r_{N-1} s_N$ gerariam um anel potente, o que é absurdo.

Corolário - Um anel sem ideal direito semi-nilpotente também não tem ideal esquerdo semi-nilpotente.

Terminaremos êste § com a demonstração de algumas proposições de que faremos uso posterior.

Teorema:- Se $\mathfrak{N} \neq (0)$ é um ideal direito simples e $\mathfrak{x}$ é um nilideal direito, tem-se $\mathfrak{N}\mathfrak{x} = (0)$. O ideal direito $\mathfrak{N}\mathfrak{x}$ está contido em $\mathfrak{N}$. Se pudesse ser $\mathfrak{N}\mathfrak{x} = \mathfrak{N}$, existiria um elemento $a \in \mathfrak{N}$, diferente de zero, tal que $a\mathfrak{x} = \mathfrak{N}$. Se $s \in \mathfrak{x}$ satisfizesse à igualdade $as = a$, ter-se-ia $a = as = as^2 = \ldots = as^m = 0$, se $s^m = 0$. Recaía-se no absurdo $a = 0$.

Teorema:- Se $\mathfrak{J}$ é um anel com elemento u e $\mathfrak{N}$ um ideal direito no qual existe um elemento r tal que $u - r$ é nilpotente, tem-se $\mathfrak{N} = \mathfrak{J}$.

Pondo, com efeito, $u - r = r_1$, é $r = u - r_1$, e o elemento $u + r_1 + r_1^2 + \ldots = v$ é bem determinado. A igualdade $(u - r_1)v = u$, ou $rv = u$, mostra que é $u \in \mathfrak{N}$, o que demonstra o teorema.

Corolário - Se $\mathfrak{J}$ é um anel com elemento u e se o ideal direito $\mathfrak{N}$ verifica a igualdade $(\mathfrak{N}, \mathfrak{N}_1) = \mathfrak{J}$, onde $\mathfrak{N}_1$ é nilideal, tem-se $\mathfrak{N} = \mathfrak{J}$.

3) O radical - Seja $\mathfrak{J}$ um anel qualquer. Um elemento $r \in \mathfrak{J}$ diz-se uma raiz, se o ideal bilateral que êle gera é nilpotente. Então, o ideal direito (ou esquerdo) gerado pelo elemento r é também nilpotente. E a inversa é verdadeira. Se r gera o ideal direito nilpotente $\mathfrak{N}$, êste está contido num ideal bilateral nilpotente. Ora êste último contém o ideal bilateral gerado pelo elemento r. Vê-se, assim, que todo o elemento pertencente a um ideal direito (ou esquerdo) nilpotente é uma raiz. O conjunto das raizes diz-se radical de $\mathfrak{J}$ e representa-se com $\mathfrak{R}$.(1)

(1) Veja-se, por ex., B. van der Waerden, "Moderne Algebra", II Teil, 1931, Cap. XVI. Confronte-se igualmente E. Noether, "Hyperkomplexe Grössen und Darstellungstheorie", Mathematische Zeitschrift, Band 30, 1929, pgs. 640 a 692.

Teorema:- O radical $\mathcal{R}$ é um ideal bilateral. Sejam r_1 e r_2 duas raizes e $\mathfrak{a}_1$, $\mathfrak{a}_2$ os ideais bilaterais por elas gerados. O elemento $r_1 - r_2$ é uma raiz, porque pertence ao ideal nilpotente $(\mathfrak{a}_1, \mathfrak{a}_2)$; os elementos sr_1 e $r_1 s$ são raizes, porque pertencem a $\mathfrak{a}_1$, q. e. d. .

Podemos dizer ainda que o radical $\mathcal{R}$ é o conjunto unido de todos os ideais nilpotentes. $\mathcal{R}$ é nilideal, mas não é geralmente nilpotente.

Consideremos um anel $\mathcal{r}$ com elemento u. $\mathcal{r}$ não pode ser nilpotente. Se é simples, não tem radical. Vamos vêr, por ex., que o anel $\mathfrak{M}$ das matrizes quadradas dos elementos dum corpo $\mathcal{F}$ não tem radical, exactamente por ser simples. Seja $0 \neq a \in \mathfrak{a}$. Basta provar que o ideal bilateral $\mathfrak{a}$ é idêntico a $\mathfrak{M}$. Ora, ponhamos $a = \sum \lambda_{ik}\, e_{ik}$, com $\lambda_{ik} \in \mathcal{F}$, $e_{ik}\, e_{jm} = \delta_{kj} \cdot e_{jm}$, δ_{kj} = símbolo de Kronecker, e e_{ik} = matriz quadrada com elementos todos nulos, salvo o elemento da linha de ordem i e da coluna de ordem k, que é igual ao elemento um do corpo.(1) Tem-se, supondo $\lambda_{ji} \neq 0$, $\lambda_{ji}^{-1}\, e_{mj}\, a\, e_{jn} = \lambda_{ji}^{-1}\, e_{mj} \lambda_{ji}\, e_{ji} \cdot e_{jn} = e_{mn} \in \mathfrak{a}$. O ideal $\mathfrak{a}$ contém tôdas as matrizes e_{mn}, pelo que é idêntico a $\mathfrak{M}$.

Teorema:- Se $\mathcal{P}$ é um ideal bilateral de $\mathcal{r}$ satisfazendo às condições $\mathcal{P} \subseteq \mathcal{R}$, $\mathcal{P}^{\sigma}\mathcal{R}^{\sigma} = (0)$, o radical de $\mathcal{r}/\mathcal{P} = \mathcal{r}'$ é $\mathcal{R}/\mathcal{P} = \mathcal{R}'$.

No homomorfismo $\mathcal{r} \sim \mathcal{r}'$, os ideais direitos $\mathcal{R}$ e $\mathcal{R}'$ são correspondentes. Seja $a' \in \mathcal{R}'$. O ideal direito $\mathfrak{k}'$, gerado por a', é um conjunto de elementos da forma $a's' + ma'$. Se um elemento $a \in \mathcal{R}$ é tal que $a \longrightarrow a'$, o ideal direito $\mathfrak{k}$, gerado por a, é o conjunto de elementos $as + ma$. Vê-se que $\mathfrak{k} \longrightarrow \mathfrak{k}'$. E, como $\mathfrak{k}^{\sigma} = (0)$, será também $\mathfrak{k}'^{\sigma} = (0)$. O ideal direito gerado por a' é nilpotente, de modo que $\mathcal{R}'$ está contido no radical de $\mathcal{r}'$. Inversamente, seja a' uma raiz de $\mathcal{r}'$. Vamos provar que $a' \in \mathcal{R}'$. De facto, a' gera um ideal direito nilpotente $\mathfrak{k}'$. Pondo $\mathfrak{k}'^{\sigma} = (0)$, consideremos $\mathfrak{k} \subseteq \mathcal{P}$, tal que $\mathfrak{k} \longrightarrow \mathfrak{k}'$. Como $\mathfrak{k}^{\sigma} \longrightarrow \mathfrak{k}'^{\sigma} = (0)$, vê-se que $\mathfrak{k}^{\sigma} \subseteq \mathcal{P}$. Portanto, sendo $\mathcal{P}^{\zeta}\mathcal{R}^{\zeta} = (0)$, é também $(\mathfrak{k}^{\sigma})^{\zeta}(\mathfrak{k}^{\sigma})^{\zeta} = (0)$. Daqui se conclui $\mathfrak{k} \subseteq \mathcal{R}$, $\mathfrak{k}' \subseteq \mathcal{R}'$, q. e. d. .

(1) Para mais detalhes, consulte-se o tomo 1º, "Grupos abelianos e Aneis e ideais não comutativos", pgs. 132.

Corolário:- Se $\mathcal{P}$ é nilpotente, $\mathcal{r}/\mathcal{P}$ tem o radical $\mathcal{R}/\mathcal{P}$. Em particular, verifica-se que $\mathcal{r}/\mathcal{R}$ não tem radical, se $\mathcal{R}$ é nilpotente. Admitindo ser $\mathcal{R}^{\sigma} = (0)$, o radical de $\mathcal{r}/\mathcal{R}^{k}$ é $\mathcal{R}/\mathcal{R}^{k}$, se $k \geq \sigma - 1$. Para $k = \sigma$, o resultado subsiste.

O anel cociente $\mathcal{r}' = \mathcal{r}/\mathcal{R}$ pode conter ainda ideais nilpotentes. A êsse respeito é válido o seguinte

Teorema:- É condição necessária e suficiente, para que $\mathcal{r}'$ não tenha radical, que $\mathcal{R}$ contenha o ideal bilateral $\mathfrak{a}$, sempre que contenha uma potência do mesmo ideal. Se não existe radical de $\mathcal{r}'$, suponhamos $\mathfrak{a}^{\sigma} \subseteq \mathcal{R}$. Estudando $\mathcal{r} \sim \mathcal{r}'$, vê-se que $\mathfrak{a}'$ (correspondente de $\mathfrak{a}$) verifica $\mathfrak{a}'^{\sigma} = (0)$, ou seja $\mathfrak{a}' = (0)$. Logo é $\mathfrak{a} \subseteq \mathcal{R}$. Inversamente, se $\mathcal{R}$ goza da propriedade indicada, suponhamos $\mathfrak{a}'^{\sigma} = (0)$. Como é $\mathfrak{a}^{\sigma} \subseteq \mathcal{R}$, é $\mathfrak{a} \subseteq \mathcal{R}$, e, portanto, $\mathfrak{a}' = (0)$, q. e. d. .

Corolário:- Se fôr $\mathcal{R}^{\sigma} = (0)$, $\mathcal{r}'$ não tem radical. Tomemos $\mathfrak{a}$ e suponhamos $\mathfrak{a}^{\sigma} \subseteq \mathcal{R}$. Será $\mathfrak{a}^{\sigma} = (0)$, $\mathfrak{a} \subseteq \mathcal{R}$, q. e. d. .

Teorema:- É condição necessária e suficiente, para que $\mathcal{R}$ seja nilpotente, que seja finita tôda a cadeia de ideais bilaterais $\mathcal{L}_i$, de $\mathcal{r}$, contidos em $\mathcal{R}$, da forma $\mathcal{L}_0 \supseteq \mathcal{L}_0\mathcal{L}_0 \supseteq \mathcal{L}_0\mathcal{L}_0\mathcal{L}_0 \supseteq \ldots$(1)

É imediato que a condição é necessária. Inversamente, supondo realizada a condição, tem-se

$$\mathcal{R} \supseteq \mathcal{R}^2 \supseteq \mathcal{R}^3 \supseteq \cdots , \qquad \mathcal{R}^n = \mathcal{R}^{n+k} ,$$

onde n é um inteiro determinado e k um inteiro qualquer. Vamos vêr que vale a igualdade $\mathcal{R}^n = \mathcal{O} = (0)$. Se fôsse $\mathcal{O} \neq (0)$, como seria $\mathcal{O} = \mathcal{O}^2 = \mathcal{O}^3 = \ldots$, existiria uma sucessão de elementos $b_1, b_2, \ldots, b_{ms} \ldots \in \mathcal{O}$ tais que o produto de qualquer número dêles consecutivos seria $\neq 0$.(2) Então, ter-se-ia (pondo $\mathcal{O} b_{2+3k} \cdot \mathcal{O} = \mathcal{L}_k$), para cada r, $\mathcal{L}_0\mathcal{L}_1 \ldots \mathcal{L}_r \supset (0)$. Por outro lado existiria um inteiro q tal que

(1) Cfr. J. Levitzki, "A characteristic condition for semi-primary rings", "Duke Mathematical Journal", vol. XI, 1944, pgs. 367 a 368.

(2) Veja-se a nota do fim do teorema.

$$\mathcal{L}_0 \supseteq \mathcal{L}_0\mathcal{L}_1 \supseteq \cdots \supseteq \mathcal{L}_0\mathcal{L}_1 \cdots \mathcal{L}_q = \mathcal{L} = \mathcal{L}\,\mathcal{L}_{q+1}$$

Como $\mathcal{L}_{q+1}$ estaria contido num ideal bilateral gerado por um elemento de $\mathcal{R}$, seria nilpotente, e ter-se-ia o absurdo

$$(0) \subset \mathcal{L} = \mathcal{L}\,\mathcal{L}_{q+1}^{\sigma} = (0).$$

Nota:- Pode proceder-se à construção de $b_1, b_2, \ldots, b_m, \ldots$ do modo a seguir. Toma-se $0 \neq b_0 \in \mathcal{U}$. Em seguida, por ser $\mathcal{U} = \mathcal{U}_1^2$, escreve-se b_0 sob a forma $b_0 = \sum \alpha_i \alpha_i'$. Destas parcelas, há uma, pelo menos, que não é nula. Suponhamos $\alpha_1 \alpha_1' \neq 0$. Faz-se $b_1 = \alpha_1$. Depois, como α_1' não é nulo, põe-se $\alpha_1' = \sum \beta_j \beta_j'$. O produto $b_1 \alpha_1' = b_1 \sum \beta_j \beta_j'$ tem uma parcela, pelo menos, não nula. Se $b_1 \beta_1 \beta_1' \neq 0$, toma-se $b_2 = \beta_1$, e procede-se sucessivamente.

Consideremos um nilanel $\mathcal{T}$, para o qual cada elemento gere um ideal bilateral nilpotente. Tem-se $\mathcal{T} = \mathcal{R}$ e é válido o

Corolário:- É condição necessária e suficiente, para que $\mathcal{T}$ seja nilpotente, que seja finita tôda a cadeia de ideais bilaterais do anel como a do teorema.

Uma segunda noção de radical (radical $\mathcal{R}^*$ de Köthe, loc. cit.) é a que resulta das considerações a seguir. Tomemos todos os nilideais bilaterais. Tem lugar o seguinte

Teorema:- O conjunto unido dos nilideais bilaterais é um nilideal bilateral. Os ideais $(\mathfrak{a}, \mathfrak{a}')$, $(\mathfrak{a}, \mathfrak{a}'')$, ..., em que $\mathfrak{a}, \mathfrak{a}', \ldots$ representam nilideais bilaterais, são nilideais bilaterais. Tomemos a e a', elementos do conjunto unido. Se $a \in \mathfrak{a}$, $a' \in \mathfrak{a}'$, o elemento $a - a'$ pertence a $(\mathfrak{a}, \mathfrak{a}')$, e, portanto, pertence ao conjunto unido. Depois, se a pertence ao conjunto unido, supondo $a \in \mathfrak{a}$, é também $sa \in \mathfrak{a}$, $as \in \mathfrak{a}$, de sorte que as e sa pertencem ao conjunto unido. O ideal bilateral constituído pelo conjunto unido é nilideal, e, como tal, é o nilideal bilateral máximo do anel. Designá-lo-emos com $\mathcal{U}$. Quando $\mathcal{U}$ contiver todos os nilideais unilaterais (direitos esquerdos) diz-se radical $\mathcal{R}^*$. Resulta imediatamente que,

quando $\mathcal{R}^*$ existe, é $\mathcal{R} \subseteq \mathcal{R}^*$. Em todos os casos é $\mathcal{R} \subseteq \mathcal{U}$. Quando $\mathcal{R}^*$ existe, pode definir-se, à semelhança de $\mathcal{R}$, como o conjunto dos elementos de $\mathcal{T}$ que geram nilideais bilaterais ou dos elementos que geram nilideais direitos.

Teorema:- É necessário e suficiente, para que $\mathcal{R}^*$ exista, que a soma dum número finito de nilideais direitos seja um nilideal direito.

A condição é necessária. Se $\mathcal{R}^*$ existe, um nilideal direito está sempre contido num nilideal bilateral. Portanto, a soma de dois nilideais direitos é um nilideal direito.

A condição é suficiente. Dado o nilideal esquerdo $\mathcal{N}$, consideremos o ideal bilateral $(\mathcal{N}, \mathcal{N}\mathcal{T})$. Vamos vêr que o ideal bilateral $\mathcal{N}\mathcal{T}$ é nilideal. Um elemento que lhe pertença é da forma $\Sigma a_i s_i$, com $a_i \in \mathcal{N}$, $s_i \in \mathcal{T}$. Um elemento $a_i s_i$ é nilpotente, pelo facto de ser nilpotente o elemento $s_i a_i$. Dêste modo, $\Sigma a_i s_i$ pertence a uma soma $(a_1\mathcal{T}, \ldots, a_r\mathcal{T})$ dum número finito de nilideais direitos. Por isso, $\Sigma a_i s_i$ é nilpotente e $\mathcal{N}\mathcal{T}$ é nilideal. Então, o ideal bilateral $(\mathcal{N}, \mathcal{N}\mathcal{T})$ é nilideal. Como contém $\mathcal{N}$, será $\mathcal{N} \subseteq \mathcal{U}$. Pelo facto de todos os ideais esquerdos pertencerem a $\mathcal{U}$, segue-se agora que a soma dum número finito de nilideais esquerdos é um nilideal esquerdo. Como anteriormente, prova-se que $\mathcal{U}$ contém todos os nilideais direitos, e o teorema fica demonstrado.

Corolário 1º:- $\mathcal{R}^*$ existe, se $\mathcal{U}$ contiver todos os nilideais direitos.

Corolário 2º:- Seja $\mathcal{T}$ um anel com radical $\mathcal{R}^*$. Se $\mathcal{T}_1$ é um sub-anel de $\mathcal{T}$, se $\mathcal{R}_1$ está contido em $\mathcal{R}^*$ e se $\mathcal{T} = (\mathcal{T}_1, \mathcal{R}_1)$, o anel $\mathcal{T}_1$ tem radical. Partindo do nilideal $\mathfrak{n}_1$, de $\mathcal{T}_1$, construamos $\mathfrak{n} = (\mathfrak{n}_1, \mathfrak{n}_1\mathcal{T}) = (\mathfrak{n}_1, \mathfrak{n}_1\mathcal{R}_1)$. Como $\mathfrak{n}_1\mathcal{R}_1 \subseteq \mathcal{R}^*$, $\mathfrak{n}$ é nilideal. $\mathfrak{n}_1$ está contido em $\mathcal{R}^*$, de modo que a soma dum número finito de nilideais direitos de $\mathcal{T}_1$ é um nilideal direito. Fica demonstrado ainda que o radical de $\mathcal{T}_1$ é $[\mathcal{T}_1, \mathcal{R}^*]$, pois que êste último é nilideal bilateral de $\mathcal{T}_1$.

Teorema:- Se $\mathcal{T}$ é comutativo, $\mathcal{R}^*$ existe e é $\mathcal{R}^* = \mathcal{R}$. A existência resulta do corolário 1º que acaba de ser enunciado. Tendo em conta que um elemento nilpotente gera um ideal nilpotente, todos os elementos de $\mathcal{R}^*$ estão contidos em $\mathcal{R}$. Será $\mathcal{R}^* = \mathcal{R}$.

Um elemento a dum anel diz-se <u>pròpriamente nilpotente</u>, se o ideal direito $a\mathfrak{T}$ (e, portanto, o ideal esquerdo $\mathfrak{T}a$)[1] fôr nilideal. É válido o

<u>Teorema</u>:- <u>É condição necessária e suficiente, para que $\mathfrak{K}^*$ exista, que o conjunto dos elementos pròpriamente nilpotentes constitua um ideal bilateral</u>[2]. Sejam a_1 e a_2 elementos pròpriamente nilpotentes. Os ideais $a_1\mathfrak{T}$ e $a_2\mathfrak{T}$ são nilideais direitos, o mesmo se dizendo da soma $(a_1\mathfrak{T}, a_2\mathfrak{T})$. Por conseqüência, $(a_1 - a_2)\mathfrak{T}$ pertence a $\mathfrak{K}^*$ e $a_1 - a_2$ é pròpriamente nilpotente. Por outro lado, se a é pròpriamente nilpotente, também o são as e sa, $(s \in \mathfrak{T})$. Inversamente, se o conjunto dos elementos pròpriamente nilpotentes fôr um ideal bilateral $\mathfrak{N}_1$, tomemos um elemento r dum nilideal direito $\mathfrak{r}$. O ideal direito $r\mathfrak{T} \subseteq \mathfrak{r}$ é nilideal, portanto r é pròpriamente nilpotente. Conclui-se $\mathfrak{r} \subseteq \mathfrak{N}_1$, e pode enunciar-se o seguinte

<u>Teorema</u>:- <u>O radical $\mathfrak{K}^*$ é o ideal bilateral $\mathfrak{N}_1$, conjunto dos elementos pròpriamente nilpotentes</u>.

Contràriamente ao que sucede com o radical $\mathfrak{K}$, vale para $\mathfrak{K}^*$ o

<u>Teorema</u>:- <u>Se $\mathfrak{K}^*$ existe, $\mathfrak{T}/\mathfrak{K}^*$ não tem nilideal</u>. Reconhece-se esta afirmação estudando o homomorfismo $\mathfrak{T} \sim \mathfrak{T}/\mathfrak{K}^*$.

Acêrca das relações entre $\mathfrak{K}$ e $\mathfrak{K}^*$, podemos enunciar os dois teoremas a seguir.

<u>Teorema 1º</u>:- <u>É necessário e suficiente, para que $\mathfrak{K}^*$ exista e seja $\mathfrak{K} = \mathfrak{K}^*$, que $\mathfrak{T}/\mathfrak{K}$ não tenha nilideal</u>. A demonstração é imediata.

<u>Teorema 2º</u>:- <u>É necessário e suficiente, para que $\mathfrak{K}^*$ exista e seja $\mathfrak{K}^* = \mathfrak{K}$, que cada elemento pròpriamente nilpotente gere um ideal nilpotente</u>. A demonstração é imediata.

(1) Se as é nilpotente, supondo $(as)^\sigma = 0$, tem-se $(sa)^{\sigma+1} = s(as)^\sigma a = 0$.

(2) Poderia também dizer-se: É necessário e basta, para que $\mathfrak{K}^*$ exista, que a diferença de dois elementos pròpriamente nilpotentes seja pròpriamente nilpotente.

Finalmente, seja $\mathfrak{P}$ um nilideal bilateral de $\mathfrak{T}$. Se $\mathfrak{K}^*$ existe, o anel $\mathfrak{T}' = \mathfrak{T}/\mathfrak{P}$ tem o radical $\mathfrak{K}'^* = \mathfrak{K}^*/\mathfrak{P}$. Em particular, $\mathfrak{T}/\mathfrak{K}$ tem o radical $\mathfrak{K}'^* = \mathfrak{K}^*/\mathfrak{K}$. De resto, a existência de $\mathfrak{K}'^*$ arrasta a de $\mathfrak{K}^*$.

Uma noção de radical ($\mathfrak{K}^{**}$) intermédio entre $\mathfrak{K}$ e $\mathfrak{K}^*$ pode dar-se como vai vêr-se. Como sucede com o conjunto unido dos ideais direitos nilpotentes, o conjunto unido dos ideais direitos semi-nilpotentes dum anel $\mathfrak{T}$ é também o conjunto unido dos ideais bilaterais semi-nilpotentes. A êsse conjunto unido chamaremos radical $\mathfrak{K}^{**}$. A semelhança de $\mathfrak{K}$ e $\mathfrak{K}^*$, $\mathfrak{K}^{**}$ é ainda o conjunto dos elementos de $\mathfrak{T}$ que geram ideais bilaterais ou ideais direitos semi-nilpotentes.

<u>Teorema</u>:- <u>O radical $\mathfrak{K}^{**}$ é um ideal bilateral semi-nilpotente</u>. Consideremo-lo como conjunto unido dos ideais bilaterais semi-nilpotentes. A repetição do raciocínio feito para $\mathfrak{K}^*$ (ou, melhor, $\mathfrak{N}$) prova que $\mathfrak{K}^{**}$ é um nilideal bilateral. Mostra-se que é semi-nilpotente, tomando um conjunto qualquer de elementos $a_1, \ldots, a_n \in \mathfrak{K}^{**}$ e notando que êsses elementos pertencem a um ideal bilateral semi-nilpotente $\mathfrak{a} = (\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$, no qual $a_i \in \mathfrak{a}_i$.

Conforme as respectivas definições, valem as relações

$$\mathfrak{K} \subseteq \mathfrak{K}^{**} \subseteq \mathfrak{K}^* \quad \text{(ou, melhor, } \mathfrak{N}\text{)}.$$

<u>Teorema</u>:- <u>No homomorfismo $\mathfrak{T} \sim \mathfrak{T}/\mathfrak{K}^{**} = \mathfrak{T}''$, não pode um ideal não semi-nilpotente $\mathfrak{r}$, de $\mathfrak{T}$, ter um correspondente semi-nilpotente $\mathfrak{r}''$</u>[1]. Suponhamos, com efeito, que $r_1, \ldots, r_n$ são elementos de $\mathfrak{r}$ que geram um anel potente $\mathfrak{T}_1$ e que o anel correspondente $\mathfrak{T}_1'' = (\mathfrak{T}_1, \mathfrak{K}^{**})/\mathfrak{K}^{**}$ é nilpotente. Se fôr $\mathfrak{T}_1''^\sigma = (0)$, ter-se-á $\mathfrak{T}_1^\sigma \subseteq \mathfrak{K}^{**}$. $\mathfrak{T}_1^\sigma$ é, porém, potente como $\mathfrak{T}_1$. Se $v_1, \ldots, v_m$ fôr o conjunto finito de elementos de $\mathfrak{T}_1^\sigma$ da forma $r_{i_1} \ldots r_{i_\sigma}$, $(i_j = 1, 2, \ldots, n)$, $(j = 1, 2, \ldots, \sigma)$, o anel $\mathfrak{T}_2$, gerado pelos v_j, está contido em $\mathfrak{T}_1^\sigma$. Se considerarmos o anel $\mathfrak{T}_1^{\sigma\rho+1}$, cada elemento do mesmo é uma soma de parcelas, cada uma das quais tem necessàriamente (qualquer que seja $\rho = 1, 2, \ldots$) mais do que $\sigma\rho$ factores r_i, de modo que pode escrever-se $\mathfrak{T}_1^{\sigma\rho+1} \subseteq \mathfrak{T}_2 \mathfrak{T}_1$. Nestas condições, $\mathfrak{T}_2$ é um anel potente, o que é absurdo, pelo facto de $\mathfrak{T}_2$ estar contido em $\mathfrak{K}^{**}$.

(1) J. Levitzki, "On the radical of a general ring".

Corolário:- O anel cociente $\mathcal{T}/\mathcal{K}^{**}$ não tem radical.

Quando $\mathcal{K}^*$ existe e é $\mathcal{K}^*=\mathcal{K}$, tem-se também $\mathcal{K}^*=\mathcal{K}^{**}$. Acêrca das relações entre os diferentes radicais, podemos enunciar os três teoremas a seguir.

Teorema 1º:- É necessário e suficiente, para que $\mathcal{K}^*$ exista e seja $\mathcal{K}^*=\mathcal{K}^{**}$, que $\mathcal{T}/\mathcal{K}^{**}$ não tenha nilideal. A demonstração é imediata.

Teorema 2º:- É necessário e suficiente, para que $\mathcal{K}^*$ exista e seja $\mathcal{K}^*=\mathcal{K}^{**}$, que cada elemento pròpriamente nilpotente gere um ideal semi-nilpotente. A demonstração é imediata.

Teorema 3º:- É necessário e suficiente, para que $\mathcal{K}^{**}=\mathcal{K}$, que $\mathcal{T}/\mathcal{K}$ não tenha ideal semi-nilpotente.

Seja $\mathcal{P}$ um ideal bilateral semi-nilpotente de $\mathcal{T}$. O anel $\mathcal{T}''=\mathcal{T}/\mathcal{P}$ tem o radical $\mathcal{K}''^{**}=\mathcal{K}^{**}/\mathcal{P}$. Em particular, $\mathcal{T}/\mathcal{K}$ tem o radical $\mathcal{K}''^{**}=\mathcal{K}^{**}/\mathcal{K}$.

Finalmente, consideremos $\mathcal{T}''=\mathcal{T}/\mathcal{K}^{**}$. Se $\mathcal{K}^*$ existe, sabemos que o radical $\mathcal{K}''^{*}$ é $\mathcal{K}^*/\mathcal{K}^{**}$.

Teorema:- É condição necessária e suficiente, para que $s\in\mathcal{K}^{**}$, que seja $s\mathcal{T}\subseteq\mathcal{K}^{**}$. A condição é necessária, porque, se s pertence ao radical, o ideal direito gerado por s, que contém $s\mathcal{T}$, pertence ao radical. É suficiente, porque, se a condição se verifica, o ideal direito $\mathcal{K}$, gerado por $\geq$, é semi-nilpotente, como se mostra por um processo análogo a um já utilizado. Efectivamente, se um conjunto $st_1+m_1s,\ldots,st_q+m_qs$, de elementos de $\mathcal{K}$, gerasse um anel potente, seria potente o anel gerado por $st_1,\ldots,st_q, m_1s,\ldots,m_qs$. Dado N arbitràriamente grande, haveria sempre um produto

$$P=st'_{i_1}\ st'_{i_2}\ldots st'_{i_N}\neq 0,\quad (t'_{i_j}=\text{um dos elementos } t_1,\ldots,t_q \text{ ou um dos inteiros } m_1,\ldots,m_q).$$

Escrevendo P sob uma das formas possíveis

$$P=s(t'_{i_1}\ st'_{i_2}).\ s(t'_{i_3}\ st'_{i_4})\ldots s(t'_{i_{N-1}}st'_{i_N}),$$

$$P=s(t'_{i_1}\ st'_{i_2})\ldots st'_{i_N},$$

vê-se que ainda seria igualmente potente, contra a hipótese, um anel gerado por um número finito de elementos de $s\mathcal{T}$.

Façamos ainda algumas observações. Vimos que se tinha $\mathcal{R}\supseteq\mathcal{K}^{**}\supseteq\mathcal{K}$. Um elemento de $\mathcal{K}^{**}$ que não pertença a $\mathcal{K}$ gera um ideal direito semi-nilpotente que não é nilpotente, e um elemento $a\in\mathcal{R}$ que não pertença a $\mathcal{K}^{**}$ gera um nilideal direito que não é semi-nilpotente (podemos, mesmo, dizer que o nilideal $a\mathcal{T}$ não é semi-nilpotente). Quando $\mathcal{R}=\mathcal{K}^{**}$, ou se tem $\mathcal{K}^*=\mathcal{R}$ e não há nilideais não semi-nilpotentes, ou não se define $\mathcal{K}^*$ e um nilideal direito não contido em $\mathcal{R}$ contém sempre elementos gerando nilideais não semi-nilpotentes. A existência de nilideais não semi-nilpotentes liga-se a de nilaneis potentes gerados por um número finito de elementos. Inversamente, se um nilanel com um número finito de geradores é potente, êsse nilanel é um nilideal que não é semi-nilpotente.

Terminaremos êste §, considerando um anel $\mathcal{T}$ de matrizes com elementos dum anel $\mathcal{O}$ e demonstrando o seguinte

Teorema:- As matrizes $S=(a_{ik})$ com elementos pertencentes ao radical $\mathcal{K}^{**}_{\mathcal{O}}$, de $\mathcal{O}$, pertencem ao radical $\mathcal{K}^{**}_{s}$, de $\mathcal{T}$. Suponhamos, com efeito, que $S\mathcal{T}$ não é semi-nilpotente. Os elementos $SS_1,\ldots,SS_k,\ldots,SS_n$, de $\mathcal{T}$, nos quais $S_i\in\mathcal{T}$, geram um anel potente. Por maior que seja N, haverá produtos $SS_{i_1}\ldots SS_{i_N}\neq 0$, e, por conseqüência, haverá elementos dessas matrizes produtos que serão $\neq 0$. Tais elementos terão a forma $\Sigma a_{ik}a^{(1)}_{jl}a_{rs}a^{(2)}_{\lambda\mu}\ldots$, onde o índice superior i significa elemento da matriz S_i. Vê-se que o conjunto finito $a_{ik}a^{(1)}_{jl}$, $a_{ik}a^{(2)}_{\lambda\mu}$, ... gera um anel potente, o que é absurdo, pelo facto de todos êstes elementos pertencerem a $\mathcal{K}^{**}_{\mathcal{O}}$.

4) Elementos idempotentes - Um elemento $e\in\mathcal{T}$ diferente do elemento nulo diz-se idempotente, se tôdas as suas potências fôrem iguais. É necessário e basta, para isso, que se tenha $e^2=e$.

Dado o idempotente e, designemos com $\mathcal{O}$ o conjunto dos elementos de $\mathcal{T}$ para os quais $se=0$; com $\mathcal{L}$ o dos elementos s para os quais $es=0$; e, com $\mathcal{J}$, o dos elementos satizfazendo a $es=se=0$.

Dado $s\in\mathcal{T}$, tem-se sempre

(1) $\quad s = e(s - se) + (s - es)e + (s - es - se + ese) + ese,$

com $s - se \in \mathcal{A}$, $s - es \in \mathcal{L}$, $s - es - se + ese = s - es - (s - es)e = s - se - e\,(s - se) \in \mathcal{J}$. A soma (1) é directa, como vamos demonstrar. Se $s = a' + b' + c' + d'$, com $a' \in e\mathcal{A}$, $b' \in \mathcal{L}e$, $c' \in \mathcal{J}$, $d' \in e\mathcal{J}e$, tem-se

$$ese = ed'e\,, \quad d' = ete\,, \quad t \in \mathcal{J},$$

$$ed'e = ete = d' = ese.$$

Obtem-se também

$$es = ea' + ese, \quad a' = er, \quad r \in \mathcal{A},$$

$$ea' = er = a' = e(s - se).$$

O raciocínio é análogo quanto a b'. Finalmente,

$$c' = s - a' - b' - d' = s - es + ese - se + ese - ese =$$

$$= s - es - se + ese.$$

É claro que $\mathcal{A}$, $\mathcal{L}$, $\mathcal{J}$, e $\mathcal{J}$ e são aqui simples módulos sem operadores. $\mathcal{A}$ é, com efeito, um ideal esquerdo, $\mathcal{L}$ um ideal direito, $\mathcal{J}$ a intersecção de $\mathcal{A}$ com $\mathcal{L}$ e $e\mathcal{J}e$ um anel com elemento $u = e$.

Diz-se decomposição de Peirce a decomposição

(2) $\qquad \mathcal{J} = e\mathcal{A} + \mathcal{L}e + \mathcal{J} + e\mathcal{J}e.$

Pode, de resto, demonstrar-se que $\mathcal{A}$ se compõe dos elementos da forma $s - se$, em que $s \in \mathcal{J}$. Disse-se já que $s - se \in \mathcal{A}$. Inversamente, se $x \in \mathcal{A}$, é $xe = 0$, $x = x - xe$. Uma afirmação análoga tem lugar para $\mathcal{L}$. Quanto a $\mathcal{J}$, podemos dizer também

que, para cada $x \in \mathcal{J}$, se tem $x = s - es - se + ese$. De facto, êste elemento pertence a $\mathcal{J}$. Inversamente, se $x \in \mathcal{J}$, pondo $x = s - se = t - et$, vem $ex = es - ese = 0$, $es = ese$, e, portanto, $x = s - se - es + ese$.

Da igualdade (2), tira-se $\mathcal{J}e = \mathcal{L}e + e\mathcal{J}e$, ou seja $\mathcal{J} = e\mathcal{A} + \mathcal{J}e + \mathcal{J}$. Ora, consideremos a soma directa $e\mathcal{A} + \mathcal{J}$. Por um lado, se x pertence a esta soma, tem-se $xe = 0$, pelo que $x \in \mathcal{A}$. Por outro lado, se $x \in \mathcal{A}$, a decomposição (1) dá, pois $xe = 0$, $x = e(x - xe) + (x - ex)$, o que mostra ser x soma de dois elementos, respectivamente pertencentes a $e\mathcal{A}$ e $\mathcal{J}$. Logo, pode escrever-se $e\mathcal{A} + \mathcal{J} = \mathcal{A}$,

(3) $\qquad \mathcal{J} = \mathcal{J}e + \mathcal{A} = e\mathcal{J} + \mathcal{L}$,

visto que pode raciocinar-se igualmente com $\mathcal{L}$.(1)

As decomposições (3) dizem-se, respectivamente, decomposição esquerda e decomposição direita de Peirce. Sob esta forma, aparece $\mathcal{J}$ como soma de dois ideais esquerdos ou direitos. Pode enunciar-se o

Teorema:- Se e é idempotente, pondo $\mathfrak{K} = e\mathcal{J}$, tem-se

$$\mathcal{J} = e\mathcal{J} + \mathfrak{K}' = \mathfrak{K} + \mathfrak{K}',$$

como soma de dois ideais direitos, valendo, para $x \in \mathfrak{K}$, $ex = x$; para $x' \in \mathfrak{K}'$, $ex' = 0$. A êste teorema corresponde outro relativo a ideais esquerdos. Ambos os teoremas subsistem quando $\mathcal{J}$ admite um domínio operatório estranho, pois, $\lambda.es = e.\lambda s$, $\lambda(s - es) = \lambda s - e.\lambda s$.

Teorema:- Se $\mathcal{J}$ é simples, $e\mathcal{J}e$ é igualmente simples. Se $\mathfrak{a}$ fôr ideal bilateral não nulo de $e\mathcal{J}e$, tem-se

$$e\mathfrak{a} = \mathfrak{a}e = \mathfrak{a}\,, \qquad e\mathcal{J}e.\mathfrak{a}.e\mathcal{J}e = \mathfrak{a}\,,$$

$$e\mathcal{J}.e\mathfrak{a}e.\mathcal{J}e = e\mathcal{J}\mathfrak{a}\mathcal{J}e = e\mathcal{J}e = \mathfrak{a}\,.$$

(1) O raciocínio feito pode comparar-se com L.E.Dickson, "Algebras and their Arithmetics", Chicago, 1923, pgs. 48 e 49.

O ideal direito gerado por um idempotente e é simplesmente o conjunto $e\mathfrak{J}$.

Um idempotente e diz-se primitivo, se não existir outro idempotente $e' \neq e$ tal que $ee' = e'e = e'$. Tem lugar o

Teorema:- É necessário e basta, para que e seja primitivo, que o anel $e\mathfrak{J}e$ apenas possua o idempotente principal (elemento um). Se existisse $e' \in e\mathfrak{J}e$, ter-se-ia, com $t \in \mathfrak{J}$, $e' = ete$, $ee' = ete = e'e = e'$, contra a hipótese. Inversamente, supondo que $e\mathfrak{J}e$ apenas possui o idempotente e, não pode haver $e' \in \mathfrak{J}$ tal que $ee' = e'e = e'$, pois que seria $ee'e = e'e = e'$ e ter-se-ia $e' \in e\mathfrak{J}e$.

Serão dadas adiante certas propriedades importantes dos idempotentes primitivos. Relativamente à existência de elementos idempotentes, demonstraremos alguns teoremas fundamentais.

Teorema 1º:- Um ideal direito simples $\mathfrak{K}$ ou é nilpotente e de expoente 2 ($\mathfrak{K}^2 = (0)$), ou possui um idempotente e, para o qual $e\mathfrak{J} = \mathfrak{K}$.

Sendo $\mathfrak{K}^2 \neq (0)$, tomemos $r \in \mathfrak{K}$ tal que $r\mathfrak{K} \neq (0)$. O homomorfismo $\mathfrak{K} \sim r\mathfrak{K}$ é um isomorfismo. Sendo, por outro lado, $r\mathfrak{K} \subseteq \mathfrak{K}$, é $r\mathfrak{K} = \mathfrak{K}$. Designando com e o elemento de $\mathfrak{K}$ para o qual $re = r$, conclui-se que será $re^2 = re = r$. Os elementos e^2 e e têm o mesmo correspondente r no isomorfismo, pelo que se terá $e^2 = e$. O facto $e\mathfrak{J} = \mathfrak{K}$ resulta de ser $e\mathfrak{J} \neq (0)$, $e\mathfrak{J} \subseteq \mathfrak{K}$.

Corolário 1º:- Um ideal direito simples que é nilideal é nilpotente e de expoente 2. Com efeito, por ser nilideal, não pode ter elemento idempotente.

Corolário 2º:- Um ideal direito simples que tem elemento não nilpotente tem elemento idempotente. Nêste caso o ideal não pode, de facto, ser nilpotente. Pode dar-se, é claro, uma demonstração directa dêste corolário, raciocinando como no teorema, mas supondo r um elemento não nilpotente. Provaremos adiante uma generalização desta afirmativa (teorema 4º).

Teorema 2º:- Se $a \in \mathfrak{J}$ é tal que $axa = a$, o ideal direito $\mathfrak{K}$ gerado por a contém um idempotente e tal que $\mathfrak{K} = e\mathfrak{J}$.

Com efeito, sendo $axa = a$, com $a \neq 0$, é $ax.ax = ax$, com $ax \neq 0$. O elemento $ax = e$ é idempotente e tem-se $\mathfrak{K} \supseteq e\mathfrak{J}$.

Mas, tendo-se $ea = a$, é também $e\mathfrak{J} \supseteq \mathfrak{K}$, o que dá $e\mathfrak{J} = \mathfrak{K}$, q. e. d.

Teorema 3º:- Um ideal direito $\mathfrak{K}$ que possui um elemento não nilpotente $r = b_{10}$, satisfazendo à igualdade $x^2 - r = t$, com $t^n = 0$, possui um idempotente. [Na demonstração que vai fazer-se, pode substituir-se $\mathfrak{K}$ por um sub-anel de $\mathfrak{J}$]. Se $n = 1$ o facto é trivial. Supondo $n > 1$, ponhamos $b_{11} = b_{10} - 2b_{10}t + t \in \mathfrak{K}$. O elemento b_{11} verifica uma equação da forma $b_{11}^m = b_{10}^m - tb$, onde b e t são comutativos. O elemento tb é nilpotente, o que não sucede com b_{10}. Isto significa $b_{10}^m \neq tb$, qualquer que seja m. O elemento b_{11} não será nilpotente. Tendo em conta a comutabilidade de b_{10} e t, fàcilmente se conclui a relação $t_1 = b_{11}^2 - b_{11} = 4t^3 - 3t^2 \in \mathfrak{K}$. Se fôr $b_{11}^2 - b_{11} = 0$, o teorema está demonstrado. De contrário, ponhamos $b_{12} = b_{11} - 2b_{11}t + t_1 \in \mathfrak{K}$. O elemento b_{12} não é nilpotente. Tendo em conta a comutabilidade de b_{11} e t_1, é, anàlogamente, $t_2 = b_{12}^2 - b_{12} = 4t_1^3 - 3t_1^2 \in \mathfrak{K}$. Como $t, t_1, t_2, \ldots$ são elementos nilpotentes e o expoente que os anula vai diminuindo, chega a encontrar-se $b_{1p}^2 - b_{1p} = t_p = 0$, $b_{1p} \in \mathfrak{K}$, $b_{1p} \neq 0$, como se deseja.

Diz-se que um ideal é regular, se possui elementos não nilpotentes. Um ideal regular é mínimo, se os sub-ideais que contém fôrem todos nilideais. Vale o

Teorema 4º:- Um ideal direito regular mínimo possui um elemento idempotente.(1) Dado $\mathfrak{K}$ nas condições do enunciado, seja $r \in \mathfrak{K}$ um elemento não nilpotente. O ideal direito $r\mathfrak{K}$ está contido em $\mathfrak{K}$ e não é nilideal. Logo tem-se $r\mathfrak{K} = \mathfrak{K}$. Se fôr $e \neq 0$ o elemento de $\mathfrak{K}$ tal que $re = r$, vem $re^2 = re = r$, $r(e^2 - e) = 0$. Supondo $e^2 - e = 0$, e será o idempotente desejado. Tendo-se $e^2 - e \neq 0$, como o conjunto $\mathfrak{S}$ dos elementos de $\mathfrak{K}$ para os quais $r\mathfrak{S} = (0)$ é um nilideal $\mathfrak{S} \subset \mathfrak{K}$, será $e^2 - e = t \in \mathfrak{S}$, com $t^n = 0$, de modo que $\mathfrak{K}$, conforme o teorema anterior, terá igualmente um idempotente.

Teorema:- Todo o idempotente dum ideal regular mínimo $\mathfrak{K}$ é primitivo. $\mathfrak{K}$ tem um idempotente e, sendo $e\mathfrak{J} = \mathfrak{K}$. Se existisse e' tal que $ee' = e'e = e'$, e' pertenceria ao ideal, sendo $e\mathfrak{J} = e'\mathfrak{J}$. Pondo $e = e's$, obter-se-ia $e'e = e's = e = e'$. O teorema vale para um sub-anel regular mínimo.

(1) Seguimos Köthe, loc.cit. Todos os livros e memórias indicados são largamente utilizados. O teorema pode demonstrar-se para sub-anéis com as designações correspondentes.

Teorema:- Se e_1 é primitivo, $e_1\mathcal{J}=\mathfrak{K}_1$ não admite sub-ideal com idempotente. Suponhamos $e_2\,\mathcal{J}\subset e_1\,\mathcal{J}$, onde e_2 é idempotente. Façamos a decomposição direita de Peirce $\mathcal{J}=$ $= e_2\mathcal{J} + \mathcal{L}_2$ e escrevamos $e_1\mathcal{J} = e_2\mathcal{J} + \mathcal{L}_2$, $e_1 = e_2\,e_1 +$ $+ (e_1 - e_2\,e_1)$. Tendo em conta que é $e_2 = e_1 s$, $(s\in\mathcal{J})$, conclui-se que $f = e_1 - e_2\,e_1 \in \mathcal{L}_2 \subset e_1\mathcal{J}$ é idempotente satisfazendo a $fe_1 = f$, $e_1 f = e_1 - e_1\,e_2\,e_1 = e_1 - e_2\,e_1 = f$, contra a hipótese, visto não poder admitir-se a relação $e_1 = e_2\,e_1$. O teorema está provado.(1)

Em correlação com a ideia de radical, demonstraremos, em seguida, algumas afirmações.

Teorema:- No homomorfismo $\mathcal{J}\sim\mathcal{J}/\mathcal{R}^* = \mathcal{J}'$, a todo o elemento primitivo de $\mathcal{J}$ corresponde um elemento primitivo de $\mathcal{J}'$, e reciprocamente. Dizer que e é primitivo equivale a dizer que $e\mathcal{J}e$ apenas tem o idempotente principal. Dado o idempotente primitivo $e_1\in\mathcal{J}$, se $e_1'\in\mathcal{J}'$ é correspondente de e_1 não fôsse primitivo, existiria $f_1'\in e_1'\,\mathcal{J}'\,e_1'$ tal que $e_1'\,f_1' = f_1'\,e_1' = f_1'$. Poderia encontrar-se, então, nos termos do anterior teorema 3º, um idempotente $f_1\in e_1\mathcal{J}e_1$ que teria f' como correspondente. Seria $f_1 = e_1$, e, portanto, $f_1' = e_1'$. Inversamente, se e_1' é primitivo, construamos e_1. Se êste último não é primitivo, pondo $e_1 f_1 = f_1\,e_1 = f_1$, vem $e_1' = f_1'$, e, por conseqüência, $e_1 - f_1 = r\in\mathcal{R}^*$. Ora, sendo $(e_1 - f_1) = e_1 - f_1$, vem $e_1 = f_1$, o que prova o teorema.

Teorema:- Em $\mathcal{J}\sim\mathcal{J}'$ a um ideal regular mínimo corresponde um ideal simples idempotente, e, reciprocamente, todo o ideal simples de $\mathcal{J}'$ é correspondente dum ideal regular mínimo de $\mathcal{J}$. Supondo $e_1\mathcal{J}$ regular mínimo, $e_1'\,\mathcal{J}'$, que não contém sub-nilideal, também não contém sub-ideal regular, visto serem incompatíveis as condições $\mathfrak{K}_1'\subset e_1'\,\mathcal{J}'$, $\mathfrak{K}_1 = e_1\mathcal{J}$, onde $\mathfrak{K}_1$ é o ideal direito composto pelos elementos de e que têm correspondentes em $\mathfrak{K}_1'$. Reciprocamente, se $e_1'\,\mathcal{J}'$ é simples, $e_1\mathcal{J}$ é regular mínimo, visto que, se o ideal regular $\mathfrak{K}_2$ estivesse contido em $e_1\mathcal{J}$, seria $\mathfrak{K}_2' = e_1'\,\mathcal{J}'$, e haveria idempotente em $\mathfrak{K}_2$, contra o facto de e_1 ser primitivo.

(1) Seguimos Almeida Costa, "Sôbre os aneis semi-primários"; vidè "Anais da Faculdade de Ciências do Pôrto", tomo XXIX, pgs. 283 a 314, 1944.

Teorema:- Se os ideais regulares mínimos $e_1\mathcal{J}=\mathfrak{K}_1$, $e_2\mathcal{J}=\mathfrak{K}_2$, têm correspondentes em $\mathcal{J}'$ que sejam operatòriamente isomorfos, vale a igualdade $\mathfrak{K}_1\,\mathfrak{K}_2 = \mathfrak{K}_1$. De facto, tem-se $\mathfrak{K}_1'\,\mathfrak{K}_2' = \mathfrak{K}_1'$(1), pois que o isomorfismo $\mathfrak{K}_2'\cong\mathfrak{K}_1'$ determina as correspondências $e_2'\longrightarrow\rho_1'$, $e_2'^2\longrightarrow\rho_1'\,e_2' = \rho_1'$, o que mostra ser diferente de (0) o produto dos dois ideais. É válida a relação $\rho_1'\,\mathfrak{K}_2' = \mathfrak{K}_1'$. Supondo $\rho_1'\,r_2' = e_1'$, os elementos ρ_1, r_2 são tais que $\rho_1\,r_2$ não é nilpotente. Será $\mathfrak{K}_1\mathfrak{K}_2\subseteq\mathfrak{K}_1$ um ideal regular, valendo, assim, a igualdade do teorema.

Teorema:- Dois ideais regulares mínimos como os do teorema anterior (de correspondentes operatòriamente isomorfos) são operatòriamente isomorfos. Acabamos de vêr que $\rho_1 r_2$ não é nilpotente. Será $\rho_1\mathfrak{K}_2 = \mathfrak{K}_1$, pois que o primeiro membro não é nilideal. Supondo $\rho_1 t_2 = e_1$, com $t_2\in\mathfrak{K}_2$, o facto de ser, para qualquer $r_1\in\mathfrak{K}_1$, $\rho_1 t_2\,r_1 = e_1\,r_1 = r_1$ mostra que t_2 não é divisor de zero à esquerda de r_1. A igualdade $t_2\,r_1 = 0$ arrasta $r_1 = 0$. Então, tem-se o isomorfismo $\mathfrak{K}_1\cong t_2\mathfrak{K}_1$. Êste último ideal está contido em $\mathfrak{K}_2$, não podendo ter-se $t_2\,\mathfrak{K}_1\subset\mathfrak{K}_2$, visto que, de contrário, $t_2\mathfrak{K}_1$ seria nilideal, estaria contido em $\mathcal{R}^*$ e o mesmo sucederia a $\rho_1 t_2\,\mathfrak{K}_1 = e_1\mathfrak{K}_1 = \mathfrak{K}_1$, o que é absurdo. Logo, como se queria, é $\mathfrak{K}_1\cong t_2\mathfrak{K}_1 = \mathfrak{K}_2$.

Suponhamos agora que $\mathcal{J}'$ tem elemento um, u'. Vale a seguinte recìproca da proposição que acaba de demonstrar-se:

Teorema:- Dois ideais regulares mínimos operatòriamente isomorfos de $\mathcal{J}$ têm correspondentes operatòriamente isomorfos em $\mathcal{J}'$. Comecemos por uma observação. Dado o ideal regular mínimo $\mathfrak{K}_1 = e_1\mathcal{J}$, seja um elemento r_1 do mesmo, não pertencente ao radical do anel. O ideal direito $r_1'\,\mathcal{J}'\subseteq e_1'\,\mathcal{J}'$ contém $r_1'\neq 0$. Será $r_1'\,\mathcal{J}' = e_1'\,\mathcal{J}'$, o que mostra haver em $r_1\mathcal{J}$ um elemento idempotente. Tem-se $r_1\mathcal{J} = \mathfrak{K}_1$. Posto isto, supondo que se tem o isomorfismo $\mathfrak{K}_1\cong\mathfrak{K}_2$ entre dois ideais regulares mínimos, a um elemento do radical contido no primeiro corresponde um elemento do radical contido no segundo, e reciprocamente, visto que, supondo $r_1\longrightarrow r_2$, com $r_1\notin\mathcal{R}^*$ e $r_2\in\mathcal{R}^*$, será $r_1\mathcal{J}\longrightarrow r_2\mathcal{J}$; $r_1\mathcal{J} = \mathfrak{K}_1$, enquanto que $r_2\mathcal{J}$, como nilideal, é uma parte de $\mathfrak{K}_2$. Se agora considerármos uma correspondência $r_1'\longrightarrow r_2'$, defini-

(1) As letras acentuadas referem-se a elementos (ou ideais) de $\mathcal{J}'$, que correspondem a elementos (ou ideais) de $\mathcal{J}$, com a designação análoga não acentuada.

da a partir da correspondência isomorfa dada $r_1 \longrightarrow r_2$, vê-se que se tem um homomorfismo operatório. Em particular, de $e_1 \longrightarrow \rho_2$, tira-se $e_1' \longrightarrow \rho_2'$, com $\rho_2' e_1' = \rho_2'$. Vamos vêr que a hipótese $\rho_2' s' = 0$ arrasta $e_1' s' = 0$. Efectivamente, sendo $\rho_2 s \in \mathscr{K}^*$, é $e_1 s \in \mathscr{K}^*$, e, portanto, $e_1' s' = 0$. O teorema está demonstrado.

Continuando a supor que $\mathscr{Y}$ tem radical $\mathscr{K}^*$ e que $\mathscr{Y}'$ tem elemento u', pode enunciar-se o seguinte

Teorema:- É condição necessária e suficiente, para que dois ideais regulares mínimos $\mathfrak{K}_1$ e $\mathfrak{K}_2$ sejam operatòriamente isomorfos, que tenha lugar a relação $\mathfrak{K}_1 \mathfrak{K}_2 = \mathfrak{K}_1$. Que a condição é necessária, resulta imediatamente da combinação do teorema anterior com o ante-penúltimo. Inversamente, se $\mathfrak{K}_1 \mathfrak{K}_2 = \mathfrak{K}_1$, é $\mathfrak{K}_1' \mathfrak{K}_2' = \mathfrak{K}_1'$. Há um elemento $b' \in \mathfrak{K}_1'$ tal que $b_1' \mathfrak{K}_2' = \mathfrak{K}_1'$, visto que o produto de dois elementos dos ideais de $\mathscr{Y}'$ não é sempre nulo. Supondo $b_1' r_2' = e_1'$, a relação $b_1' r_2' r_1' = e_1' r_1' = r_1'$ mostra que a hipótese $r_2' r_1' = 0$ arrasta $r_1' = 0$. A correspondência $\mathfrak{K}_1' \sim r_2' \mathfrak{K}_1'$ é um isomorfismo. Por outro lado, na relação $r_2' \mathfrak{K}_1' \subseteq \mathfrak{K}_2'$, valerá necessàriamente a igualdade, visto que $\mathfrak{K}_2'$ é mínimo. O teorema está provado.

Teorema:- Se $e \in \mathscr{Y}$, os idempotentes primitivos de $e\mathscr{Y}$, $\mathscr{Y}e$, e $e\mathscr{Y}e$ são-no também de $\mathscr{Y}$. Tomemos $\mathscr{Y}e$, por ex. Se e_1 é primitivo em $\mathscr{Y}e$, não existe $e' \in \mathscr{Y}$ tal que $e_1 e' = e' e_1 = e'$, visto que, pondo $e_1 = se$, seria $e' = e'se$, ou seja $e' \in \mathscr{Y}e$.

Teorema:- A soma de dois nilideais não pode ter idempotente. Sejam $\mathfrak{K}_1$ e $\mathfrak{K}_2$ os nilideais em causa. Suponhamos que a sua soma tem um elemento idempotente $e = r_1 + r_2$, $(r_1 \in \mathfrak{K}_1, r_2 \in \mathfrak{K}_2)$. Será

$$r_1 + r_2 \quad e, \quad r_1 e + r_2 e = e, \quad (r_1 e)^2 + r_1 e . r_2 e = r_1 e,$$

$$(r_1 e)^2 = (r_1 e)^3 + (r_1 e)^2 . r_2 e; \ldots; (r_1 e)^{n-1} = (r_1 e)^n + (r_1 e)^{n-1} . r_2 e =$$

$$= (r_1 e)^{n-1} . r_2 e,$$

se $(r_1 e)^n = 0$, $(r_1 e)^{n-1} \neq 0$. Bem entendido que a hipótese $r_1 e = 0$, $r_2 e = e$, é de excluir. Nessas condições, supondo $(r_2 e)^m = 0$, $(r_2 e)^{m-1} \neq 0$, será também $(r_1 e)^{n-1} = (r_1 e)^{n-1} . (r_2 e) =$

$= \ldots = (r_1 e)^{n-1} . (r_2 e)^m = 0$, o que é absurdo.

Observação:- O teorema não prova que a diferença entre um idempotente e um nilpotente (pertencente, ou não, a um nilideal) é um "não nilpotente". O facto de e ser elemento um de $e\mathscr{Y}e$, combinado com o raciocínio do último teorema do § 2, permite afirmar que a diferença entre e e um elemento dum nilideal de $e\mathscr{Y}e$ é sempre "não nilpotente".

Corolário 1º:- Num anel $\mathscr{Y}$ para o qual todo o ideal regular direito possui elemento idempotente, a soma dum número finito de nilideais direitos é um nilideal direito ($\mathscr{K}^*$ existe). De facto, a soma de dois nilideais $\mathfrak{K}_1$ e $\mathfrak{K}_2$, se não fôsse nilideal, seria um ideal regular e teria um elemento idempotente.

Corolário 2º:- Um anel $\mathscr{Y}$ para o qual todo o ideal direito regular possui um ideal direito regular mínimo tem radical $\mathscr{K}^*$.

Teorema:- Se x' é um elemento dum nilideal direito $\mathfrak{K}'$ de $e\mathscr{Y}e$, $x'\mathscr{Y}$ é um nilideal direito de $\mathscr{Y}$. Dado o elemento $x' \in \mathfrak{K}'$, tem-se

$$x' = ete, \quad x' = x'e = ex' = ex'e, \quad (t \in \mathscr{Y}),$$

e, para cada $r \in \mathscr{Y}$,

$$(x'r)^\sigma = x'r.x'r \ldots = x'er.ex'er \ldots ex'er.ex'r =$$

$$= (x'ere)^{\sigma-1} . x'r.$$

Ora $x'ere = x'.ere \in \mathfrak{K}'$, pêlo que será nilpotente. $x'r$ é nilpotente, e o ideal $x'\mathscr{Y}$ é nilideal. Observe-se que $x' \in x'\mathscr{Y}$.

Corolário:- Se $\mathscr{K}^*$ existe, tem-se $\mathfrak{K}'\mathscr{Y} \subseteq \mathscr{K}^*$ e $\mathfrak{K}' \subseteq e\mathscr{K}^*e$. Um elemento de $\mathfrak{K}'\mathscr{Y}$ pertence sempre a uma soma finita $\Sigma x'\mathscr{Y} \subseteq \mathscr{K}^*$. Logo, $\mathfrak{K}'\mathscr{Y}$ é nilideal de $\mathscr{Y}$ e está contido em $\mathscr{K}^*$. Tendo em conta que $\mathfrak{K}' = \mathfrak{K}'e$, vê-se que $\mathfrak{K}' \subseteq \mathfrak{K}'\mathscr{Y} \subseteq \mathscr{K}^*$, e que $\mathfrak{K}' = e\mathfrak{K}'e \subseteq e\mathscr{K}^*e$.

Teorema:- O radical $\mathscr{R}'^*$ de $e\mathscr{T}e$ é $e\mathscr{R}^*e$, se $\mathscr{R}^*$ existe.[1] Em primeiro lugar, $e\mathscr{R}^*e$ é um nilideal bilateral de $e\mathscr{T}e$, pois, por ex.,

$$e\mathscr{R}^*e.e\mathscr{T}e = e.\mathscr{R}^*e\mathscr{T}.e \subseteq e\mathscr{R}^*e.$$

Assim, será $e\mathscr{R}^*e \subseteq \mathscr{R}'$ = nilideal bilateral máximo de $e\mathscr{T}e$. O corolário anterior diz-nos que $\mathscr{R}' \subseteq e\mathscr{R}^*e$. Será, pois, $\mathscr{R}' = e\mathscr{R}^*e$. Ora $\mathscr{R}' = \mathscr{R}'^*$, porque, ainda pelo corolário anterior, $\mathscr{R}'$ contém todos os nilideais direitos.

Teorema:- Se x'' é um elemento dum nilideal direito $\mathscr{r}''$ de $\mathscr{J}$, $x''\mathscr{T}$ é um nilideal direito de $\mathscr{T}$. Dado o elemento $x'' \in \mathscr{r}''$, tem-se $x''e = ex'' = 0$. Vê-se que é, para cada $r \in \mathscr{T}$,

$$(x''(r - re - er + ere))^\sigma = (x''(r - re))^\sigma = (x''r - x''re)^\sigma =$$

$$= (x''r)^\sigma - (x''r)^\sigma e .$$

Portanto, podemos escrever

$$(x''r)^{\sigma+1} = (x''r)^\sigma.x''r = \{(x''r)^\sigma e + [x''(r - re - er + ere)]^\sigma\}.x''r =$$

$$= [x''(r - re - er + ere)]^\sigma .x''r.$$

A circunstância de ser $r - re - er + ere \in \mathscr{J}$ mostra que o primeiro factor do último membro pertence a $\mathscr{r}''$, e é, pois, nilpotente. O produto $x''r$ é nilpotente e o ideal $x''\mathscr{T}$, de $\mathscr{T}$, é nilideal.

Corolário:- Se $\mathscr{R}^*$ existe, tem-se $\mathscr{r}''\mathscr{T} \subseteq \mathscr{R}^*e$ $\mathscr{r}'' \subseteq [\mathscr{R}^*, \mathscr{J}]$. Um elemento de $\mathscr{r}''\mathscr{T}$ pertence sempre a uma soma finita $\Sigma x''\mathscr{T} \subseteq \mathscr{R}^*$. Portanto, $\mathscr{r}''\mathscr{T} \subseteq \mathscr{R}^*$. A soma $(\mathscr{r}'', \mathscr{r}''\mathscr{T})$ é nilideal de $\mathscr{T}$, e, por consequência, $\mathscr{r}'' \subseteq \mathscr{R}^*$. Logo tem-se $\mathscr{r}'' \subseteq [\mathscr{R}^*, \mathscr{J}]$.

Teorema:- O radical $\mathscr{R}'^*$ de $\mathscr{J}$ é $\Delta = [\mathscr{R}^*, \mathscr{J}]$, se $\mathscr{R}^*$ existe.

(1) Confronte com M.Deuring, "Algebren", "Ergebnisse der Mathematik und ihrer Grenzgebiete", IV Band, 1935, Cap. II.

Em primeiro lugar, Δ é um nilideal bilateral de $\mathscr{J}$, pois, por ex., se a lhe pertence e $b \in \mathscr{J}$, é $ab \in \mathscr{R}^*$, $ab \in \mathscr{J}$. Assim, será $\Delta \subseteq \mathscr{R}''$ = nilideal bilateral máximo de $\mathscr{J}$. O corolário anterior diz-nos que $\mathscr{R}'' \subseteq \Delta$. Será, pois, $\mathscr{R}'' = \Delta$. Ora $\mathscr{R}'' = \mathscr{R}'''^*$, porque, ainda pelo corolário anterior, $\mathscr{R}''$ contém todos os nilideais direitos de $\mathscr{J}$.

Passando ao radical $\mathscr{R}^{**}$, valem algumas proposições análogas às anteriores.

Teorema:- Se x' é um elemento dum ideal direito semi-nilpotente $\mathscr{r}'$, de $e\mathscr{T}e$, x' pertence a $\mathscr{R}^{**}$. Por hipótese, com efeito, $x'\mathscr{T}e$ é um ideal semi-nilpotente de $e\mathscr{T}e$. Vê-se que $x'\mathscr{T}$ é ideal semi-nilpotente de $\mathscr{T}$, tendo em conta igualdades como a seguinte:

$$x's_{l_1}.x's_{l_2} \ldots x's_{l_N} = x's_{l_1} e.x's_{l_2} e \ldots x's_{l_{N-1}}e.x's_{l_N}.$$

Corolário:- O radical de $e\mathscr{T}e$ é $e\mathscr{R}^{**}e$. Acaba de mostrar-se que, na realidade, $x' \in \mathscr{R}^{**}$, e que, portanto, $x' = ex' e \in e\mathscr{R}^{**}e$.

Teorema:- Se x'' é um elemento dum ideal direito semi-nilpotente $\mathscr{r}''$, de $\mathscr{J}$, x'' pertence a $\mathscr{R}^{**}$. Demonstra-se notando que, se fôr potente o anel gerado por $x''s_1, \ldots, x''s_n$, é potente um anel gerado por $x''b_1 e, \ldots, x''b_n e$; $x''i_1, \ldots, x''i_n$, onde $b_j \in \mathscr{B}$, $i_k \in \mathscr{J}$, da decomposição de Peirce relativa a e. Ora a última afirmação é absurda.

Corolário:- O radical de $\mathscr{J}$ é $[\mathscr{J}, \mathscr{R}^{**}]$.

5) O centro de $\mathscr{T}$ - Diz-se centro de $\mathscr{T}$ o conjunto $\mathscr{Z}$ dos elementos $z \in \mathscr{T}$ que comutam contados os elementos de $\mathscr{T}$. $\mathscr{Z}$ é um anel comutativo. Mesmo que haja um domínio operatório estranho, o sub-anel é admissível: $zx = xz$, $(x \in \mathscr{T})$, $\lambda z.x = \lambda.zx = \lambda.xz = x.\lambda z$.

A cada ideal direito $\mathscr{r}$, de $\mathscr{T}$, corresponde um ideal contraído de $\mathscr{Z}$, que se representa com $[\mathscr{r}, \mathscr{Z}]$. A cada ideal $\mathscr{L}$, de $\mathscr{Z}$, corresponde um ideal ampliado de $\mathscr{T}$, que é o ideal direito $\mathscr{m}$ gerado pelos elementos de $\mathscr{L}$: $\mathscr{m} = (\mathscr{L}, \mathscr{L}\mathscr{T}) = (\mathscr{L}, \mathscr{T}\mathscr{L})$. Êste ideal é bilateral.

Teorema:- O centro dum anel $\mathfrak{T}$ tem um radical $[\mathfrak{R}, \mathfrak{z}] = [\mathfrak{R}^*, \mathfrak{z}]$. Em primeiro lugar é válida a igualdade, pois um elemento do 2º membro é nilpotente, e, pertencendo a $\mathfrak{z}$, gera um ideal direito (bilateral) nilpotente, pelo que pertencerá a $\mathfrak{R}$. Em seguida, $[\mathfrak{R}, \mathfrak{z}]$ é nilideal de $\mathfrak{z}$. Como $\mathfrak{z}$ é comutativo, pertencerá ao radical de $\mathfrak{z}$. Inversamente, se $\mathfrak{a}'$ é um ideal nilpotente de $\mathfrak{z}$, o ideal bilateral de $\mathfrak{T}$, $(\mathfrak{a}', \mathfrak{a}'\mathfrak{T})$, é também nilpotente, como fàcilmente se verifica. Isto dá $\mathfrak{a}' \subseteq \mathfrak{R}$, como se deseja. Bem entendido que se supôs existir $\mathfrak{R}^*$. De contrário, deveria substituir-se, na demonstração, $\mathfrak{R}^*$ por $\mathfrak{M}$.

Corolário:- Se $\mathfrak{R}^* = (0)$, ou se $\mathfrak{R} = (0)$, $\mathfrak{z}$ não tem radical.

6) Decomposição de $\mathfrak{T}$ em ideais bilaterais - Se um anel é uma soma directa de ideais bilaterais:

$$(4) \qquad \mathfrak{T} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n,$$

têm lugar as relações $\mathfrak{a}_i \mathfrak{a}_k = (0)$, se $i \neq k$, visto que o produto $\mathfrak{a}_i \mathfrak{a}_k$ está contido em $\mathfrak{a}_i$ e $\mathfrak{a}_k$. A decomposição de $\mathfrak{T}$ pode considerar-se como uma decomposição em anéis que mutuamente se anulam. Inversamente, se existe uma decomposição de $\mathfrak{T}$ em anéis que tenha a forma

$$\mathfrak{T} = (\mathfrak{a}_1, \ldots, \mathfrak{a}_n), \quad \text{com} \quad \mathfrak{a}_i \mathfrak{a}_k = (0), \quad \text{se} \quad i \neq k,$$

os anéis são ideais bilaterais de $\mathfrak{T}$. De facto, vem imediatamente

$$\mathfrak{a}_i \mathfrak{T} = \mathfrak{a}_i^2 \subseteq \mathfrak{a}_i \quad , \qquad \mathfrak{T}\mathfrak{a}_i \subseteq \mathfrak{a}_i \quad .$$

Pode imaginar-se uma definição de $\mathfrak{T}$, a partir dos $\mathfrak{a}_i$, prèviamente dados. Tomando, então, $a_i, a_i' \in \mathfrak{a}_i$, pôr-se-à Σa_i como expressão do elemento geral de $\mathfrak{T}$, definir-se-à a soma pela igualdade $\Sigma a_i + \Sigma a_i' = \Sigma(a_i + a_i')$ e o produto pela relação $\Sigma a_i \cdot \Sigma a_i' = \Sigma a_i a_i'$. A igualdade $\Sigma a_i = \Sigma a_i'$ implicará $a_i = a_i'$ e $\mathfrak{T}$ será uma soma directa.

Teorema:- Os ideais direitos ou bilaterais dos $\mathfrak{a}_i$ são ideais análogos de $\mathfrak{T}$. Se, por ex., $\mathfrak{l}_1$ é ideal direito de $\mathfrak{a}_1$, tem-se

$$\mathfrak{l}_1 \mathfrak{T} = (\mathfrak{l}_1 \mathfrak{a}_1, \ldots, \mathfrak{l}_1 \mathfrak{a}_n) = \mathfrak{l}_1 \mathfrak{a}_1 \subseteq \mathfrak{l}_1 .$$

Daqui se conclui que, se os ideais bilaterais $\mathfrak{a}_i$ não contêm qualquer ideal bilateral diferente de $\mathfrak{a}_i$ ou do ideal nulo (isto é, são bilateralmente simples), são anéis simples. A inversa é clara: se os $\mathfrak{a}_i$ são anéis simples, considerados como ideais bilaterais de $\mathfrak{T}$ são bilateralmente simples.

Teorema:- A tôda a decomposição (4) corresponde uma decomposição do centro $\mathfrak{z}$. Vamos vêr que a (4) corresponde

$$(5) \qquad \mathfrak{z} = \mathfrak{z}_1 + \cdots + \mathfrak{z}_n,$$

onde $\mathfrak{z}_i = [\mathfrak{a}_i, \mathfrak{z}]$. Em primeiro lugar, os $\mathfrak{z}_i$ são os centros dos anéis $\mathfrak{a}_i$. E isto porque os elementos de $\mathfrak{z}$ que pertencem a $\mathfrak{a}_i$ pertencem certamente ao centro de $\mathfrak{a}_i$ e os elementos de $\mathfrak{a}_i$ que comutam com todos os elementos de $\mathfrak{T}$, em face de (4) e da propriedade $\mathfrak{a}_i \mathfrak{a}_k = (0)$. Seja agora $z \in \mathfrak{z}$. Pondo, conforme (4), $z = z_1 + z_2 + \cdots + z_n$, tem-se, se $a \in \mathfrak{T}$,

$$az = az_1 + \cdots + az_n = za = z_1 a + \cdots + z_n a \ ,$$

e, conseqüentemente, $az_i = z_i a$. Isto significa que os elementos z_i pertencem ao centro, e que, portanto, $z_i \in [\mathfrak{a}_i, \mathfrak{z}]$. Inversamente, uma soma de elementos z_i nestas condições dá um elemento de $\mathfrak{z}$. Por isso, tem-se

$$\mathfrak{z} = (\mathfrak{z}_1, \ldots, \mathfrak{z}_n).$$

Esta soma é directa, visto ser $\mathfrak{z}_i \subseteq \mathfrak{a}_i$.

7) Aneis com elemento u - Quando um anel tem elemento u, êste diz-se idempotente principal. Em tal caso, os dois elementos e, u-e, são simultâneamente idempotentes. Suponhamos que, em $\mathcal{T}$, é possível uma decomposição de u sob a forma

$$u = e_1 + \cdots + e_n ,$$

com $e_i^2 = e_i$, $e_i e_k = 0$ (se $i \neq k$). Vamos demonstrar que $\mathcal{T}$ é uma soma directa dos ideais direitos gerados pelos e_i: $\mathcal{T} = e_1\mathcal{T} + \cdots + e_n\mathcal{T}$.

De facto, cada elemento $s \in \mathcal{T}$ é da forma $s = e_1 s + \cdots + e_n s$, e a soma dos elementos $e_i\mathcal{T}$ pertence a $\mathcal{T}$. Por outro lado, se fôr $e_1 s_1 + \cdots + e_n s_n = 0$, $(s_i \in \mathcal{T})$, deduz-se $e_i^2 s_i = e_i s_i = 0$.

Inversamente, se $\mathcal{T}$ tem elemento u e é soma directa de ideais direitos, $\mathcal{T} = \mathcal{K}_1 + \cdots + \mathcal{K}_n$, os elementos e_i da decomposição $u = e_1 + \cdots + e_n$, $(e_i \in \mathcal{K}_i)$, verificam as condições $e_i^2 = e_i$, $e_i e_k = 0$, (se $i \neq k$), $\mathcal{K}_i = e_i\mathcal{T}$. Seja $r_i \in \mathcal{K}_i$. Tem-se $r_i = u\, r_i = e_1 r_i + \cdots + e_n r_i$, e, portanto, $e_i r_i = r_i$, $e_k r_i = 0$. Tomando $r_i = e_i$, vem $e_i^2 = e_i$, $e_k e_i = 0$. Finalmente, sendo $e_i\mathcal{T} \subseteq \mathcal{K}_i$, e $e_i r_i = r_i$, tem-se $\mathcal{K}_i = e_i\mathcal{K}_i \subseteq e_i\mathcal{T}$, ou seja $\mathcal{K}_i = e_i\mathcal{T}$, q. e. d.

No caso da decomposição supra de $\mathcal{T}$, se $\mathcal{L}_1$ é o ideal direito que anula e_1, vê-se que se tem $\mathcal{L}_1 \supseteq e_2\mathcal{T} + \cdots + e_n\mathcal{T}$. Inversamente, se $b_1 \in \mathcal{L}_1$, pondo $b_1 = u\, b_1 = e_1 b_1 + \cdots + e_n b_1$, vê-se que é $b_1 = e_2 b_1 + \cdots + e_n b_1$, pelo que se terá $\mathcal{L}_1 = e_2\mathcal{T} + \cdots + e_n\mathcal{T}$.

É claro que há uma decomposição de $\mathcal{T}$ em ideais esquerdos:

$$(6) \qquad \mathcal{T} = \mathcal{T}e_1 + \cdots + \mathcal{T}e_n = \mathcal{W}_1 + \cdots + \mathcal{W}_n ,$$

nas mesmas condições que anteriormente.

As matrizes e_{ii} do anel $\mathcal{M}$ das matrizes quadradas dos elementos dum corpo estão precisamente nas condições dos elementos e_i a que se referem os teoremas acabados de demonstrar.

Os elementos e, u-e permitem a decomposição

$$\mathcal{T} = e\,\mathcal{T} + (u-e)\,\mathcal{T} .$$

Estudemos as homomorfias operatórias $\mathcal{K}_j \sim \mathcal{K}_i$. Dada uma tal homomorfia, ela fará corresponder ao elemento $e_j \in \mathcal{K}_j$ um elemento $\rho_i \in \mathcal{K}_i$. Ter-se-á, se $r_j \in \mathcal{K}_j$,

$$e_j \longrightarrow \rho_i , \quad r_j = e_j r_j \longrightarrow \rho_i r_j , \quad e_j e_j = e_j \longrightarrow \rho_i e_j = \rho_i .$$

Isto significa que é $\rho_i = \rho_i e_j \in \mathcal{K}_i \mathcal{W}_j = e_i\mathcal{T}\mathcal{T} e_j = e_i\mathcal{T} e_j = \mathcal{T}_{ij}$. Assim, a nossa homomorfia é definida por um elemento $a_{ij} \in \mathcal{T}_{ij}$, conforme a correspondência $r_j \longrightarrow a_{ij} r_j \in \mathcal{K}_i$.

Em particular, consideremos os endomorfismos operatórios $\mathcal{K}_i \sim \mathcal{K}_i$. Serão definidos pelos elementos de $\mathcal{T}_{ii} = e_i\mathcal{T} e_i = \mathcal{K}_i\mathcal{W}_i$. Mais precisamente, vamos demonstrar que há isomorfismo entre o anel endomórfico do grupo abeliano com operadores, $\mathcal{K}_i$, e o anel $\mathcal{T}_{ii}$. De facto, o endomorfismo soma e o endomorfismo produto de dois endomorfismos a_{ii} e b_{ii} são, respectivamente, definidos por $a_{ii} + b_{ii}$, $a_{ii} b_{ii}$:

$$r_i \longrightarrow a_{ii} r_i + b_{ii} r_i = (a_{ii} + b_{ii})\, r ,$$

$$r_i \longrightarrow a_{ii} \cdot b_{ii} r_i = a_{ii} b_{ii} \cdot r_i .$$

Cada elemento $a_i \in \mathcal{K}_i$ determina também um endomorfismo $\mathcal{K}_i \sim a_i \mathcal{K}_i$, mediante a correspondência $r_i \longrightarrow a_i r_i$. O anel $\mathcal{T}_{ii}$ é homomorfo de $\mathcal{K}_i$ (êste último considerado como anel). Em $\mathcal{K}_i$ existe um ideal bilateral $\mathcal{A}_i$ (de $\mathcal{K}_i$) tal que $\mathcal{T}_{ii} \cong \mathcal{K}_i / \mathcal{A}_i$. Pertencem a $\mathcal{A}_i$ os elementos α_i, de $\mathcal{K}_i$, tais que $\alpha_i e_i = 0$, e apenas êsses elementos. Da decomposição 2, § 4, conclui-se que $\mathcal{A}_i$ é uma parte de $\mathcal{U}$. Pode escrever-se $\mathcal{A}_i = [\mathcal{U}, \mathcal{K}_i]$. Tem lugar o

Teorema:- Dado o anel $\mathcal{T}$ com elemento u, se e_i fôr um idempotente de $\mathcal{T}$, o ideal esquerdo $\mathcal{U}$, da decomposição $\mathcal{T} = e_i\mathcal{U} + \mathcal{A}_i e_i + \mathcal{J} + e_i\mathcal{T}e_i$, é tal que $[\mathcal{U}, e_i\mathcal{T}]$ é um ideal bilateral de $e_i\mathcal{T}$, e tem lugar a relação de isomorfismo anular $e_i\mathcal{T}e_i \cong e_i\mathcal{T}/[\mathcal{U}, e_i\mathcal{T}] \cong \mathcal{T}e_i/[\mathcal{L}, \mathcal{T}e_i]$ (1). A verificação directa de que $\mathcal{A}_i$ é ideal bilateral de $\mathcal{K}_i$ resulta simplesmente do facto de ser $\mathcal{U}\, e_i = (0)$ e de ser $\mathcal{U}$ ideal esquerdo de $\mathcal{T}$.

(1) Observe-se que u admite a decomposição $u = e + (u-e)$.

Vamos demonstrar agora o seguinte

Teorema:- Se o anel $\mathcal{J}$ com elemento u admite a decomposição $\mathcal{J} = \mathfrak{K}_1 + \ldots + \mathfrak{K}_n$, na qual os $\mathfrak{K}_i$ são directamente indecomponíveis, a decomposição correspondente (6) determina ideais esquerdos $\mathfrak{N}_i = \mathcal{J} e_i$, também directamente indecomponíveis. Se fôsse, com efeito, por ex.,

$$\mathfrak{N}_1 = \mathcal{J} e_1 = \mathcal{J} e_1' + \mathcal{J} e_1'' ,$$

ter-se-ia também

$$\mathcal{J} = e_1' \mathcal{J} + e_1'' \mathcal{J} + e_2 \mathcal{J} + \ldots + e_n \mathcal{J} = \mathfrak{K}_1' + \mathfrak{K}_1'' + e_2 \mathcal{J} + \ldots + e_n \mathcal{J} .$$

Daqui se concluia, tendo em vista o primeiro teorema da isomorfia dos grupos,

$$\mathcal{J} / e_2 \mathcal{J} + \ldots + e_n \mathcal{J} \cong \mathfrak{K}_1' + \mathfrak{K}_1'' \cong \mathfrak{K}_1 ,$$

o que mostraria ser $\mathfrak{K}_1$ directamente decomponível, contra a hipótese.

No tocante à decomposição de $\mathcal{J}$ em ideais bilaterais, a existência de u permite-nos precisar alguns resultados do § anterior.

Teorema:- Um ideal direito $\mathfrak{K}$, de $\mathcal{J}$, é uma soma de ideais direitos da forma $\mathfrak{K} = \mathfrak{K} \alpha_1 + \ldots + \mathfrak{K} \alpha_n$. Na verdade, por um lado, é $\mathfrak{K} = \mathfrak{K} \mathcal{J} = (\mathfrak{K} \alpha_1, \ldots, \mathfrak{K} \alpha_n)$; por outro, o último membro é uma soma directa, visto que $\mathfrak{K} \alpha_i$ é um ideal direito de $\mathcal{J}$ contido em α_i. Por conseqüência, se $\mathfrak{K}$ é directamente indecomponível (à direita), será necessàriamente, por ex., $\mathfrak{K} = \mathfrak{K} \alpha_i \cong \alpha_i$. Um ideal direito simples de $\mathcal{J}$ está, assim, contido sempre num α_i.

Teorema:- Se os α_i são bilateral e directamente indecomponíveis, a decomposição (4) é univocamente determinada. Se se tivesse, com efeito, $\mathcal{J} = \alpha_1' + \ldots + \alpha_m'$, deduzia-se, sucessivamente:

$$\alpha_1' = \alpha_1' \mathcal{J} = (\alpha_1' \alpha_1 , \ldots , \alpha_1' \alpha_n) = \alpha_1' \alpha_1 + \ldots + \alpha_1' \alpha_n ,$$

visto que $\alpha_1' \alpha_i \subseteq \alpha_i$. Como, por hipótese, α_1' é indecomponível, será, por ex., $\alpha_1' = \alpha_1' \alpha_R \subseteq \alpha_R$. Poderia concluir-se analogamente, $\alpha_R \subseteq \alpha_i'$, e, portanto, $\alpha_1' \subseteq \alpha_R \subseteq \alpha_i'$, o que daria $\alpha_1' = \alpha_i' = \alpha_R$. Isto significa que cada α_i' é idêntico a um α_R q. e. d. .

Teorema:- A decomposição (5) corresponde, de modo biunívoco, à decomposição (4). Dado (4), passa-se a (5). E, supondo $u = e_1 + \ldots + e_n$, tem-se

$$\mathfrak{z}_i = \mathfrak{z} e_i , \qquad \alpha_i = \mathcal{J} e_i = e_i \mathcal{J} .$$

Inversamente, dado (5), pondo $u = e_1 + \ldots + e_n$, será $e_i^2 = e_i$, $e_i e_k = 0, (i \neq k)$,

$$\mathcal{J} = \mathcal{J} e_1 + \ldots + \mathcal{J} e_n = \alpha_1 + \ldots + \alpha_n , \qquad (\alpha_i = \mathcal{J} e_i = e_i \mathcal{J}) .$$

Daqui tira-se agora

$$\mathfrak{z} = \mathfrak{z}_1' + \ldots + \mathfrak{z}_n' , \qquad \mathfrak{z}_i' = \mathfrak{z} e_i = \mathfrak{z}_i .$$

Qualquer outra decomposição de $\mathcal{J}$ em n ideais bilaterais, que leve a $u = e_1 + \ldots + e_n$, dará para êsses ideais a expressão $\alpha_i' = \mathcal{J} e_i = \alpha_i$.

Teorema:- Dois ideais direitos contidos em dois α_i diferentes não podem ser operatòriamente isomorfos. Sejam $\mathfrak{K}_1 \subseteq \alpha_1$, $\mathfrak{K}_2 \subseteq \alpha_2$. Se a $r_1 \neq 0$, e pertencente a $\mathfrak{K}_1$, corresponde $r_2 \in \mathfrak{K}_2$, a $r_1 e_1 = r_1$ corresponderá $r_2 e_1 = 0$. Assim, será $\mathfrak{K}_2 = (0)$, contra a hipótese. Podemos dizer, pois, que uma homomorfia $\mathfrak{K}_1 \sim \mathfrak{K}_2$, nas condições do teorema, só pode ser a homomorfia nula.

Posto isto, suponhamos que se tem uma decomposição de $\mathcal{J}$, como (4), e que os α_i são bilateralmente indecomponíveis. O estudo dos ideais (direitos ou esquerdos) de $\mathcal{J}$, conforme os resultados adquiridos, pode fazer-se à custa do estudo dos ideais dos α_i . Suponhamos, em segundo lugar, que se faz a decomposição de cada α_i numa soma de ideais direitos directamente indecomponíveis (à direita); os ideais direitos isomorfos pertencem a um mesmo α_i, mas não existe proposição inver-

sa geral, segundo a qual tôdas as parcelas do mesmo $\mathfrak{a}_i$ são isomorfas.

Terminaremos êste §, fazendo ainda uma observação. Consideremos, no anel $\mathfrak{J}$ com elemento $u = e_1 + \ldots + e_n$, o anel $\mathfrak{Z} = \sum_{i,j} e_i \mathfrak{J} e_j = \sum_{i,j} \mathfrak{z}_{ij}$. Vê-se imediatamente que se tem $\mathfrak{Z}^h = (0)$, em face das relações $e_i e_k = 0$, $e_i^2 = e_i$.

8) Aneis regulares[1]. Diz-se regular, todo o anel $\mathfrak{J}$ para o qual, dado $a \neq 0$, pertencente a $\mathfrak{J}$, existe um elemento x tal que $a\,x\,a = a$. O ideal direito gerado por a tem o elemento idempotente $ax = e$, de modo que é $\mathfrak{K} = \mathfrak{K}^* = (0)$.

Teorema:- Um idempotente primitivo dum anel regular gera um ideal simples. O ideal gerado pelo idempotente não pode ter sub-ideal próprio, visto que êste teria idempotente.

Teorema:- Um ideal principal direito (ou esquerdo) é sempre gerado por um idempotente. Seja $(a)_d$ o ideal direito gerado por a. Se fôr $axa = a$, $ax = e$, tem-se $(e)_d \subseteq (a)_d$. sendo, por outro lado, $ea = a$, é também $(a)_d \subseteq (e)_d$, pelo que o teorema está demonstrado.

Procuremos agora o aniquilador esquerdo de $(a)_d$, ou seja o ideal esquerdo composto pelos elementos $x \in \mathfrak{J}$ tais que $x.(a)_d = (0)$. Pondo $(a)_d = (e)_d$, a decomposição $\mathfrak{J} = \mathfrak{J}e + \mathfrak{U}$ contém o ideal $\mathfrak{U}$ tal que $\mathfrak{U}e = (0)$. Vê-se imediatamente que $\mathfrak{U}$ é o aniquilador procurado.

Nêste §, suporemos que $\mathfrak{J}$ tem elemento u e que $\mathfrak{k}, \mathfrak{k}', \ldots; \mathfrak{h}, \mathfrak{h}', \ldots$ representam, respectivamente, ideais principais, direitos ou esquerdos:

$$\mathfrak{k} = (a)_d = (e)_d \; ; \qquad \mathfrak{h} = (a)_l = (e)_l .$$

O aniquilador esquerdo de $\mathfrak{k}$ representa-se por $\mathfrak{k}^l$ e o aniquilador direito de $\mathfrak{h}$ por $\mathfrak{h}^d$.

(1) Cfr. J.von Neumann, "On regular rings", Proceedings of the National Academy of Sciences of the U.S.A., vol.22, nº 12, 1936. Para uma extensão, pode vêr-se N.H.McCoy, "Generalized regular rings", Bulletin of the American Mathematical Society, vol.45, 1939, pgs.175-178.

Teorema:- O aniquilador esquerdo de $\mathfrak{k}$ é o ideal principal esquerdo gerado pelo idempotente u-e. Efectivamente, tem-se $\mathfrak{k}^l = \mathfrak{J}(u-e)$.

Corolário:- Tem lugar a igualdade $\mathfrak{k}^{ld} = \mathfrak{k}$. De facto, o aniquilador direito de $\mathfrak{k}^l$ (conforme o teorema anterior, suposto aplicado a um ideal principal esquerdo $\mathfrak{h}$) é o ideal principal direito gerado pelo idempotente $u-(u-e) = e$. É claro ainda que, ao lado de $\mathfrak{k}^{ld} = \mathfrak{k}$, deve fixar-se a igualdade $\mathfrak{h}^{dl} = \mathfrak{h}$.

Teorema:- Se $\mathfrak{k}$ e $\mathfrak{k}'$ são dois ideais principais gerados por e e e', existe um idempotente f tal que $ef = fe = 0$, para o qual $(\mathfrak{k}, \mathfrak{k}') = (e)_d + (f)_d$. Se $\mathfrak{k}'$ está contido em $\mathfrak{k}$, podemos tomar $f = 0$. Não sendo assim, vamos vêr que se tem

$$(\mathfrak{k}, \mathfrak{k}') = (e)_d + \big((u-e).e'\big)_d .$$

Um elemento do 2º membro é da forma $es + (u-e)e't = e(s-e't) + e't$, com $s, t \in \mathfrak{J}$, o que mostra pertencer ao 1º. Inversamente, um elemento do 1º membro é da forma $es+e't = es+e't-ee't + ee't = e(s + e't) + (u-e)e't$, o que mostra pertencer ao 2º. Posto isto, seja e_1 o idempotente que gera $\big((u-e)e'\big)_d$. Tem-se $ee_1 = 0$, de modo que, pondo $f = e_1 - e_1 e$, vem imediatamente $ef = fe = 0$, $ff = f$, $fe_1 = e_1$, $e_1 f = f$, donde se conclui o teorema.

Corolário:- Num anel regular, a soma de dois ideais principais direitos é um ideal principal direito. O idempotente $e + f$ é, com efeito, gerador da soma: $(e + f)_d = (e)_d + (f)_d$.

Posto isto, consideremos a soma $(\mathfrak{k}, \mathfrak{k}')$ de dois ideais principais direitos e o ideal esquerdo $[\mathfrak{k}^l, \mathfrak{k}'^l]$ que é intersecção dos respectivos aniquiladores esquerdos. Um elemento da intersecção anula $\mathfrak{k}$ e $\mathfrak{k}'$, e, portanto, anula a soma. Inversamente, se um elemento anula a soma, anula $\mathfrak{k}$ e $\mathfrak{k}'$, pelo que pertence à intersecção. Pode, pois, enunciar-se o

Teorema:- É válida a igualdade $(\mathfrak{k}, \mathfrak{k}')^l = [\mathfrak{k}^l, \mathfrak{k}'^l]$.

Corolário 1º:- Tem lugar a igualdade $[\mathfrak{k}, \mathfrak{k}']^l = (\mathfrak{k}^l, \mathfrak{k}'^l)$. Com efeito, podemos escrever, sucessivamente:

Se um anel regular é redutível (veja-se o § 1), pondo $\mathfrak{r} = \mathfrak{a} + \mathfrak{a}'$, a decomposição correspondente de u, sob a forma $u = e + (u-e)$, mostra que $e \in \mathfrak{z}$. Inversamente, a cada $e \in \mathfrak{z}$ corresponde uma redução do anel. Tem lugar o

Teorema:- É condição necessária e suficiente, para que um anel regular seja totalmente redutível, que todo o seu ideal bilateral seja um ideal principal direito. Acabamos de vêr que a condição é necessária. A condição é suficiente, pois que, então, cada ideal bilateral é gerado por um idempotente $e \in \mathfrak{z}$, e a igualdade $\mathfrak{r} = e\mathfrak{r} + (u-e)\mathfrak{r}$ tem lugar com $u-e \in \mathfrak{z}$.

Teorema:- É condição necessária e suficiente, para que um anel regular seja irredutível, que o centro seja um corpo. Se $\mathfrak{z}$ é um corpo, apenas tem o idempotente u, não havendo decomposição de $\mathfrak{r}$ em ideais bilaterais. Inversamente, se uma tal decomposição não pode ter lugar, $\mathfrak{z}$ apenas pode ter o idempotente u. Como é regular, será um corpo (todo o seu elemento tem inverso).

Teorema:- Se e e f são dois idempotentes pertencentes ao centro, tem-se $(ef)_d = [(e)_d, (f)_d]$ e $(e+f-ef)_d = ((e)_d, (f)_d)$. Na verdade $(ef)_d = (fe)_d$ está contido na intersecção de $(e)_d$ com $(f)_d$. Por outro lado, se g é um idempotente gerador da intersecção, tem-se $g = es = ft$, e também

$$fg = ft = g = eg = efg.$$

Conclui-se que $(g)_d \subseteq (ef)_d$, e, portanto, a primeira afirmação do teorema. É claro que deverá ser $ef = g$, pelo facto de ef ser um idempotente do centro. Relativamente, à segunda afirmação do teorema, tem-se, com $(e)_d = \mathfrak{k}$, $(f)_d = \mathfrak{k}'$:

$$(\mathfrak{k}, \mathfrak{k}')^l = [\mathfrak{k}^l, \mathfrak{k}'^l] = [(u-e)_l, (u-f)_l] = ((u-e)(u-f))_l =$$

$$= (u-e-f+ef)_l \ ;$$

$$(\mathfrak{k}, \mathfrak{k}')^{ld} = (\mathfrak{k}, \mathfrak{k}') = (u-(u-e-f+ef))_d = (e+f-ef)_d .$$

Teorema:- Num anel regular, o conjunto dos elementos s, tais que $se = es = s$, constitui um anel regular. Se s é um tal elemento, ponhamos $sxs = s$. Vamos vêr que x pode substituir-se por um elemento x' tal que $x'e = ex' = x'$. De facto, tem-se $ese = s$, e, portanto,

$$esxse = s = s.exe.s \ .$$

Fazendo $x' = exe$, resulta o teorema, pois que o produto de dois elementos do conjunto em questão é um elemento do mesmo conjunto.

9) Anéis com n^2 matrizes unidades[1]- No que vai seguir-se, o anel $\mathfrak{r}$, além de possuir elemento u, contém n^2 elementos e_{ik} (matrizes unidades) verificando as duas relações seguintes: 1ª) $e_{ik}e_{jl} = \delta_{kj} \cdot e_{il}$, ($\delta_{kj}$ = símbolo de Kronecker); 2ª) $u = e_{11} + \ldots + e_{nn}$. Verifica-se, então, que são válidas as igualdades $\mathfrak{r} e_k \mathfrak{r} = \mathfrak{r}$, ($k = 1, \ldots, n$; $e_k = e_{kk}$). Basta notar com efeito, que $\mathfrak{r} e_k \mathfrak{r}$ é um ideal bilateral contendo tôdas as matrizes e_{ij} (e, portanto, o elemento u): $e_{ij} = e_{ik} e_{kk} e_{kj}$, $u = e_{11} + \ldots + e_{nn}$.

Ponhamos $\mathfrak{r}_{ij} = e_i \mathfrak{r} e_j$. São válidas as igualdades

$$\mathfrak{r} = \sum_i e_i \mathfrak{r} \ , \quad e_i \mathfrak{r} = \sum_j e_i \mathfrak{r} e_j \ , \quad \mathfrak{r} = \sum_{ij} \mathfrak{r}_{ij} \ ,$$

onde os somatórios se referem a somas directas. Os sub-anéis $\mathfrak{r}_{ij}$ verificam as igualdades $\mathfrak{r}_{ij}\mathfrak{r}_{kl} = \delta_{jk}\mathfrak{r}_{il}$. Os sub-aneis $\mathfrak{r}_{ii}$ admitem e_i como elemento um e nunca se reduzem ao único elemento nulo. As igualdades $\mathfrak{r}_{ij}\mathfrak{r}_{ji} = \mathfrak{r}_{ii}$ mostram que os $\mathfrak{r}_{ij}$ também não podem reduzir-se a (0). Seja $x_{11} \in \mathfrak{r}_{11}$. Façamos corresponder a x_{11} o elemento $a \in \mathfrak{r}$, $a = \sum e_{i1} x_{11} e_{1i}$. Esta correspondência é biunívoca. De facto a x_{11} corresponde um elemento a bem determinado. Inversamente, a todo o elemento a da forma anterior, onde $x_{11} \in \mathfrak{r}_{11}$, corresponde um x_{11} bem determinado, pois $e_{11} a e_{11} = x_{11}$. O conjunto $\mathfrak{U}$ dos elementos

(1) Cfr. Almeida Costa, "Sôbre os grupos abelianos", Anais da Faculdade de Ciências do Pôrto, tomo XXVII, 1942. A 3ª condição indicada no começo do § 16 dêsse artigo, é supérflua.

a constitui um anel isomorfo de $\mathcal{Y}_{11}$:

$$x_{11} \longrightarrow a = \sum_i e_{i1} x_{11} e_{1i} \ , \qquad x_{11} + y_{11} \longrightarrow a + b \ ,$$

$$y_{11} \longrightarrow b = \sum_i e_{i1} y_{11} e_{1i} \ ,$$

$$x_{11}\, y_{11} \longrightarrow \sum_i e_{i1} x_{11} y_{11} e_{1i} = \sum_i e_{i1} x_{11} e_{1i} e_{i1} y_{11} e_{1i} = \sum_i e_{i1} x_{11} e_{1i} \cdot$$

$$\cdot \sum_i e_{i1} y_{11} e_{1i} = ab.$$

Em particular, ao elemento e_{11} corresponde

$$\sum_i e_{i1} e_{11} e_{1i} = \sum_i e_{i1} e_{1i} = \sum_i e_{ii} = u \ .$$

O anel $\mathcal{U}$ tem, assim, como elemento um, o elemento um de $\mathcal{Y}$. Os elementos de $\mathcal{U}$ comutam com tôdas as matrizes unidades:

$$a e_{kl} = e_{k1} x_{11} e_{1l} \ , \qquad e_{kl} a = e_{k1} x_{11} e_{1l} \ .$$

Um elemento $x \in \mathcal{Y}$ pode pôr-se sob a forma

$$x = \sum_{p,q} x_{pq} e_{pq} \ , \qquad x_{pq} = \sum_i e_{ip} x e_{ql} \ ,$$

pois é $\sum_{p,q,i} e_{ip} x e_{ql} e_{pq} = \sum_{p,q} e_{pp} x e_{qq} = \sum_p e_{pp} x = x$. Os coeficientes x_{pq} comutam com todos os e_{ij}:

$$x_{pq} e_{ij} = \sum_k e_{kp} x e_{qk} e_{ij} = e_{ip} x e_{qj} = e_{ij} \sum_k e_{kp} x e_{qk} = e_{ij} x_{pq} \cdot$$

Mas, escrevendo $x_{pq} = \sum_i e_{i1} e_{ip} x e_{q1} e_{1i}$, vê-se que $x_{pq} \in \mathcal{U}$. Isto significa que o anel $\mathcal{Y}$ se pode considerar como um módulo finito relativamente ao anel $\mathcal{U}$. A representação de cada elemento de $\mathcal{Y}$ é, então, única. De facto, vamos vêr que uma igualdade do tipo

$$\sum_{p,q} a_{pq} e_{pq} = \sum_{p,q} a'_{pq} e_{pq} \ ,$$

onde os a_{pq} e os a'_{pq} comutam com tôdas as matrizes unidades, leva necessàriamente, a $a_{pq} = a'_{pq}$. Tem-se sucessivamente:

$$\sum_{p,q} a_{pq} e_{pq} e_{ij} = \sum_{p,q} a'_{pq} e_{pq} e_{ij} \ , \qquad \sum_p a_{pi} e_{pj} = \sum_p a'_{pi} e_{pj} \ ,$$

$$e_{ki} \sum_p a_{pi} e_{pj} = e_{ki} \sum_p a'_{pi} e_{pj} \ , \qquad a_{ii} e_{kj} = a'_{ii} e_{kj} \ ,$$

$$a_{ii} e_{kk} = a'_{ii} e_{kk} \ , \qquad \sum_k a_{ii} e_{kk} = \sum_k a'_{ii} e_{kk} = a_{ii} = a'_{ii} \ ,$$

quaisquer que sejam i e j, como se deseja. Atendendo a que se tem

$$x_{pq} e_{pq} = \sum_i e_{ip} x e_{qi} e_{pq} = e_{pp} x e_{qq} \in \mathcal{Y}_{pq} \ ,$$

pode agora afirmar-se ser $\mathcal{Y}_{pq} = \mathcal{U} e_{pq}$. Com Wedderburn[1], diz-se que $\mathcal{Y}$ é o produto directo de $\mathcal{U}$ pelo sistema dos e_{ik}. Procuremos ainda os elementos de $\mathcal{Y}$ que comutam com todos os e_{ik}. Se x é um tal elemento, vem $e_{ij} x = \sum_{p,q} e_{ij} x_{pq} e_{pq} =$ $= \sum_{p,q} x_{pq} e_{ij} e_{pq} = \sum_q x_{jq} e_{iq}$, $x e_{ij} = \sum_{p,q} x_{pq} e_{pq} e_{ij} = \sum_p x_{pi} e_{pj}$, $\sum_q x_{jq} e_{iq} = \sum_p x_{pi} e_{pj}$, o que leva a $q = j$, $p = i$, $x_{jj} = x_{ii}$, $x_{ji} = 0$ $(j \neq i)$. Por aqui se vê que x é da forma $x = \sum x' e_{ii} =$ $= x'$, com $x' \in \mathcal{U}$. Podemos enunciar o

Teorema:- Sob as duas condições indicadas, o anel $\mathcal{Y}$ é um módulo finito (produto directo de Wedderburn) com respeito aos elementos de $\mathcal{Y}$ que comutam com as matrizes unidades, as quais representam uma base correspondente de $\mathcal{Y}$.

É válida a proposição a seguir.

(1) M. Wedderburn, "On hypercomplex numbers", Proceedings of the London Mathematical Society, II series, vol. 6, 1908.

Teorema:- Se $\mathfrak{Y}$ possui o radical $\mathfrak{K}_s^*$, $\mathfrak{A}$ possui o radical $[\mathfrak{A}, \mathfrak{K}_s^*]$.(1) Na verdade tem-se $\mathfrak{A} \cong \mathfrak{A}\, e_{11} = e_{11}\mathfrak{Y}\, e_{11}$, como imediatamente se verifica. O radical de $\mathfrak{Y}_{11}$ é $e_{11}\mathfrak{K}_s^* e_{11} \subseteq \mathfrak{K}_s^*$. Dado um elemento w do radical de $\mathfrak{A}$, tem-se $w\, e_{11} \in e_{11}\mathfrak{K}_s^* e_{11}$. E, sendo $w = we_{11} + \ldots + we_{nn}$, é também $w \in \sum e_{ii}\mathfrak{K}_s^* e_{ii} \subseteq \mathfrak{K}_s^*$, o que mostra ter-se $w \in [\mathfrak{A}, \mathfrak{K}_s^*]$. Inversamente, um elemento dêste último nilideal bilateral de $\mathfrak{A}$ pertence ao radical de $\mathfrak{A}$.

Aplicação:- Consideremos, por ex., um anel $\mathfrak{Z}$ com elemento U e o anel completo, $\mathfrak{Y}$, das matrizes quadradas do grau n com elementos de $\mathfrak{Z}$. Existem, como se sabe, as n^2 matrizes e_{ik}, que verificam as duas condições impostas no começo do §. O anel $\mathfrak{A}$ é composto de elementos da forma

$$a = \sum_i e_{i1} s\, e_{1i} = \sum_{i,j,k} \alpha_{jk} e_{i1} e_{jk} e_{1i} = \alpha_{11} \sum_i e_{ii} = \alpha_{11} u ,$$

$(s \in \mathfrak{Y}, \alpha_{jk} \in \mathfrak{Z})$, e apenas dêsses. Isto significa $\mathfrak{A} = \mathfrak{Z} u \cong e_{11} \cdot \mathfrak{Y} e_{11}$. Se $\mathfrak{Y}$ possui o radical $\mathfrak{K}_s^*$, o radical de $\mathfrak{Z} u$ é $[\mathfrak{Z} u, \mathfrak{K}_s^*] \cong e_{11}\mathfrak{K}_s^* e_{11} \cong$ radical de $\mathfrak{Z}$. Uma proposição que demonstraremos ainda é a seguinte:

Teorema:- O anel $\mathfrak{Y}' = \mathfrak{Y}/\mathfrak{K}_s^*$ é o anel completo de matrizes de $\mathfrak{Z}' = (\mathfrak{Z} u, \mathfrak{K}_s^*)/\mathfrak{K}_s^*$. Na verdade, consideremos e_{ik} e e_{jm}. Se $i \neq j$, as igualdades $e_{ik} - e_{jm} = r \in \mathfrak{K}_s^*$, $e_{ki}(e_{ik} - e_{jm}) = e_{kk} = e_{ki} r$ mostram uma parte do que se deseja. Se $i = j$, pondo $(e_{ik} - e_{im})\, e_{ki} = e_{ii} = r\, e_{ki}$, a conclusão é a mesma, salvo se $m = k$, caso em que as duas matrizes de que se partiu são idênticas. $\mathfrak{Z}'$ é um anel sem radical, precisamente pelo facto de $\mathfrak{Y}'$ não ter radical. De resto, pode observar-se que se tem

$$\mathfrak{Z}' = (\mathfrak{Z} u, \mathfrak{K}_s^*) / \mathfrak{K}_s^* \cong \mathfrak{Z} u / [\mathfrak{Z} u, \mathfrak{K}_s^*].$$

(1) O teorema subsiste quando se substitui $\mathfrak{K}_s^*$ pelo radical $\mathfrak{K}_s^{**}$.

Capítulo II

Aneis com condição dupla de cadeia

1) A condição dupla de cadeia - Diz-se que o anel $\mathfrak{Y}$ verifica a condição de cadeia múltipla (ou condição de cadeia descendente), se, para um conjunto de ideais direitos $\mathfrak{k}$, satisfazendo a

$$\mathfrak{k}_1 \supseteq \mathfrak{k}_2 \supseteq \mathfrak{k}_3 \supseteq \cdots ,$$

tem necessàriamente lugar o sinal =, a partir de determinada ordem.

Podemos também dizer que se introduziu uma condição de mínimo para os ideais direitos. Isto significa que, num conjunto dos mesmos, há, pelo menos, um ideal mínimo, que não pode conter outro ideal qualquer do conjunto. A equivalência das duas condições é imediata.

Ao lado da condição de cadeia múltipla, juntaremos ainda a seguinte, de cadeia divisora (ou ascendente): o anel $\mathfrak{Y}$ é tal que, para um conjunto de ideais direitos $\mathfrak{k}$, satisfazendo a

$$\mathfrak{k}_1 \subseteq \mathfrak{k}_2 \subseteq \mathfrak{k}_3 \subseteq \cdots ,$$

tem necessàriamente o sinal = , a partir de determinada ordem.

Podemos também dizer que se introduziu uma condição de máximo para os ideais direitos. Isto significa que, num conjunto dos mesmos, há, pelo menos, um ideal máximo, ou seja um ideal que não pode pertencer a outro qualquer. A equivalência das duas condições é imediata.

Um anel com condições de mínimo e de máximo diz-se com condição dupla de cadeia. Consideremos os ideais direitos como sub-módulos admissíveis de $\mathfrak{Y}$, tem lugar o

Teorema:- A condição dupla de cadeia determina a existência duma série de composição para cada ideal direito, e inversamente. De facto, se fôsse possível dilatar indefinidamente, sem repetições, uma série normal de $\mathfrak{Y}$, essa dilatação contradiria a condição imposta. Inversamente, dado um conjunto qualquer de ideais direitos, tomemos como "comprimento" de cada ideal o comprimento da sua série de composição. Como existe no

conjunto um ideal de comprimento máximo ($\leqq$ que o comprimento da série de composição de $\mathfrak{r}$),êsse ideal será máximo no conjunto. Anàlogamente,pode afirmar-se que um ideal direito de comprimento mínimo do nosso conjunto é um ideal mínimo.

Os resultados da Teoria dos Grupos[1] permitem afirmar que as condições de máximo e de mínimo se transportam de $\mathfrak{r}$ a um anel factor $\mathfrak{r}/\mathfrak{a}$.

Num anel $\mathfrak{r}$ completamente redutível (soma dum número finito de ideais direitos simples) é válida a condição dupla de cadeia.

Teorema:- A condição dupla de cadeia transporta-se de $\mathfrak{r}$ para os aneis $e\mathfrak{r}e$ e $\mathfrak{J}$ duma decomposição de Peirce. Façamos corresponder aos ideais direitos $\mathfrak{d}$, $\mathfrak{d}'$,..., de $e\mathfrak{r}e$, ideais direitos $\mathfrak{k}$, $\mathfrak{k}'$,..., de $\mathfrak{r}$,de tal sorte que $\mathfrak{d}\subset\mathfrak{d}'$ arraste $\mathfrak{k}\subset\mathfrak{k}'$. Basta tomar para $\mathfrak{k}$ o ideal gerado pelos elementos de $\mathfrak{d}$:

$$\mathfrak{k} = (\mathfrak{d}, \mathfrak{d}\mathfrak{r}) = (\mathfrak{d}, \mathfrak{d}\mathfrak{a}) .$$

Para se verificar a última igualdade,observemos que é $\mathfrak{d}e = \mathfrak{d}$, $\mathfrak{d}.e\mathfrak{L}e = (0)$, $\mathfrak{d}.e\mathfrak{J} = (0)$, $\mathfrak{d}.e\mathfrak{r}e = \mathfrak{d}$. Tendo agora em conta a igualdade $\mathfrak{k}e = \mathfrak{d}e = \mathfrak{d}$,vê-se que a hipótese $\mathfrak{d}\subset\mathfrak{d}'$ não pode dar $\mathfrak{k} = \mathfrak{k}'$. Daqui se tira o teorema,quanto a $e\mathfrak{r}e$.

Passando a $\mathfrak{J}$,seja $\mathfrak{d}$ ideal direito em $\mathfrak{J}$. Anàlogamente, formemos

$$\mathfrak{k} = (\mathfrak{d}, \mathfrak{d}\mathfrak{r}) = (\mathfrak{d}, \mathfrak{d}\mathfrak{L}e, \mathfrak{d}\mathfrak{J}) = (\mathfrak{d}, \mathfrak{d}\mathfrak{L}e),$$

como resulta de $\mathfrak{d}e = (0)$. Vê-se que é $\mathfrak{d} = [\mathfrak{k}, \mathfrak{J}]$, pois um elemento de $\mathfrak{d}$ pertence a $\mathfrak{k}$ e a $\mathfrak{J}$,e,se $a \in \mathfrak{k}, \mathfrak{J}$, pondo $a = d + \Sigma d'be$, com $d, d' \in \mathfrak{d}$, $b \in \mathfrak{L}$, vem $ae = \Sigma d'be = 0$, $d = a \in \mathfrak{d}$. A hipótese $\mathfrak{d}\subset\mathfrak{d}'$ não pode dar $\mathfrak{k} = \mathfrak{k}'$,o que demonstra a segunda parte do teorema.[2]

(1) Veja-se Almeida Costa, "Elementos da Teoria dos Grupos", pgs.78. Veja-se também B.van der Waerden,"Moderne Algebra", I Teil,1930,Cap.VI.

(2) Conforme E.Artin,"Zur Theorie der hyperkomplexen Zahlen", Abhanlungen des mathematischem Seminars,Hamburg,Band 5,1927, pgs.251 a 260.

Corolário:- A condição dupla de cadeia transporta-se de $\mathfrak{r}$ para $e\mathfrak{r}e$ / $e\mathfrak{K}^*e$ e para $\mathfrak{J}/[\mathfrak{J}, \mathfrak{K}^*]$.

Teorema:- A condição dupla de cadeia transporta-se de $\mathfrak{r}/\mathfrak{K}^*$ para $e\mathfrak{r}e$ / $e\mathfrak{K}^*e = \mathfrak{r}'$. Para fazer a demonstração (Deuring, loc.cit.), vamos determinar uma certa correspondência biunívoca entre ideais direitos dos dois aneis factores,precisando que os ideais de $\mathfrak{r}'$ são quaisquer. De facto,se $\mathfrak{k}'$ é ideal direito de $\mathfrak{r}'$,corresponde-lhe $\mathfrak{K}' \supset e\mathfrak{K}^*e$, tal que $\mathfrak{K}'/e\mathfrak{K}^*e = \mathfrak{k}'$. Ao ideal direito $\mathfrak{K}'$ de $e\mathfrak{r}e$, façamos corresponder o ideal $(\mathfrak{K}', \mathfrak{K}'\mathfrak{r}) = (\mathfrak{K}', \mathfrak{K}'\mathfrak{a})$ de $\mathfrak{r}$, e,em seguida,o ideal $\Delta' = (\mathfrak{K}', \mathfrak{K}'\mathfrak{r}, \mathfrak{K}^*) \supseteq \mathfrak{K}^*$,também ideal direito de $\mathfrak{r}$. Finalmente,tomaremos em $\mathfrak{r}/\mathfrak{K}^*$ o ideal $\Delta'/\mathfrak{K}^*$ como correspondente de $\mathfrak{k}'$. Se $\mathfrak{k}''$ e $\Delta''/\mathfrak{K}^*$, com $\Delta'' = (\mathfrak{K}'', \mathfrak{K}''.\mathfrak{r}, \mathfrak{K}^*)$ forem outros correspondentes,a igualdade $\Delta''/\mathfrak{K}^* = \Delta'/\mathfrak{K}^*$ arrasta $\Delta' = \Delta''$, e,por conseqüência, $e\Delta''e = (\mathfrak{K}'', e\mathfrak{K}^*e) = \mathfrak{K}'' = e\Delta'e = \mathfrak{K}'$, $\mathfrak{k}' = \mathfrak{k}''$. Daqui se tira a demonstração desejada[1].

Teorema:- Num anel $\mathfrak{r}$ com condição dupla de cadeia,cada ideal direito não nilpotente, $\mathfrak{k}$, tem um elemento idempotente (Artin, loc.cit.). Imaginemos ser possível encontrar um elemento $s \in \mathfrak{s} \subseteq \mathfrak{k}$, que não seja divisor de zero à esquerda do ideal direito $\mathfrak{s}$,e tal que $se = s$, com $0 \neq e \in \mathfrak{s}$. O teorema ficará demonstrado,pois a relação $se = se^2$ dará $s(e^2 - e) = 0$, ou $e^2 = e$. Ora,consideremos o conjunto dos ideais direitos de $\mathfrak{r}$ não nilpotentes contidos em $\mathfrak{k}$,depois o ideal mínimo, $\mathfrak{s}$,dêsse conjunto. Se $a \in \mathfrak{s}$,tem-se $a\mathfrak{r} \subseteq \mathfrak{s}$. Existe pelo menos um elemento $a' \in \mathfrak{s}$ para o qual $a'\mathfrak{r} = \mathfrak{s}$,como vamos vêr. Se,para todos os elementos de $\mathfrak{s}$,fôsse $a\mathfrak{s} \subset \mathfrak{s}$,do conjunto dos ideais nilpotentes

$$(1) \qquad a\mathfrak{s},\ a'\mathfrak{s},\ \ldots$$

(1) O mesmo teorema tem lugar substituindo $\mathfrak{K}^*$ pelo radical $\mathfrak{K}^{**}$.

deduzia-se um ideal nilpotente

$$(2) \qquad (a_1\mathfrak{r}, \ldots, a_n\mathfrak{r})$$

que continha todos os ideais (1). Bastaria, para isso, tomar um ideal direito nilpotente máximo no conjunto dos ideais nilpotentes que fôssem soma dum número finito de ideais (1). Êsse ideal máximo seria da forma (2) e conteria todos os ideais (1), visto que, de contrário, a sua soma com um ideal (1), que êle não contivesse, daria um ideal nilpotente que conteria o máximo.

O ideal (2), assim construido, conteria $\mathfrak{r}^2$, pela circunstância seguinte: um elemento de $\mathfrak{r}^2$ seria da forma $\Sigma a\,a'$ e pertenceria, por isso, a uma certa soma de ideais (1); $\mathfrak{r}^2$ e $\mathfrak{r}$ seriam nilpotentes, contra a hipótese.

Seja, assim, $a'\mathfrak{r} = \mathfrak{r}$. Designando com e um elemento de $\mathfrak{r} \subseteq \mathfrak{R}$ para o qual $a'e = a'$, resta verificar não ser a' um divisor de zero à esquerda de $\mathfrak{r}$. Consideremos o ideal direito de $\mathfrak{T}$ composto doe elementos t que satisfazem à condição $a'^n t = 0$. Representando-o com $\mathfrak{R}_n$, tem-se $\mathfrak{R}_n \subseteq \mathfrak{R}_{n+1}$. Se imaginarmos que a' pode ser um divisor de zero à esquerda de $\mathfrak{r}$, existe $0 \neq s' \in \mathfrak{r}$, para o qual é $a's' = 0$. Sendo, porém, $a'^n\mathfrak{r} = \mathfrak{r}$, existe $t \in \mathfrak{r}$, com $a'^n t = s'$. Assim, será

$$a's' = a'^{n+1}t = 0, \qquad a'^n t = s' \neq 0 ,$$

o que mostra ser $t \in \mathfrak{R}_{n+1}$ um elemento não pertencente a $\mathfrak{R}_n$. Dêste modo não haverá ideal máximo no conjunto

$$\mathfrak{R}_1 \subset \mathfrak{R}_2 \subset \cdots \subset \mathfrak{R}_n \subset \mathfrak{R}_{n+1} \subset \cdots ,$$

contra o suposto. O teorema está demonstrado.

Corolário:- Num anel com condição dupla de cadeia, é $\mathfrak{R}^* = \mathfrak{R}$ e $\mathfrak{T}/\mathfrak{R}$ não tem radical. Basta ter em conta, com efeito, que a soma dum número finito de nilideais direitos é a soma dum número finito de ideais direitos nilpotentes, e, conseqüentemente, que tal soma, como nilpotente, é nilideal. Por outro lado, $\mathfrak{T}/\mathfrak{R}$ não tem nilideal.

2) Os sub-nilaneis - No caso de anéis $\mathfrak{T}$ sujeitos à condição dupla de cadeia e com uma série de composição de comprimento n, podem estabelecer-se os dois teoremas seguintes:

Teorema 1º:- Dado um ideal $\mathfrak{R}$ de comprimento $\leqq c$, se $a_1, \ldots, a_c$ são elementos de $\mathfrak{T}$ tais que $a_1 \ldots a_c\mathfrak{R} \neq (0)$ e $a_1\mathfrak{R} \subseteq \mathfrak{R}$, existe um ideal $\mathfrak{R}_1$ para o qual $(0) \subset \mathfrak{R}_1 \subseteq \mathfrak{R}$, $\mathfrak{R}_1 = (a_1\mathfrak{R}_1, \ldots, a_c\mathfrak{R}_1)$.(1)

Teorema 2º:- Dado um ideal $\mathfrak{R} \neq (0)$, de comprimento $\leqq c$, se $a_1, \ldots, a_c$ são elementos de $\mathfrak{T}$ tais que $a_1 \ldots a_c \neq 0$ e $\mathfrak{R} = (a_1\mathfrak{R}, \ldots, a_c\mathfrak{R})$, pode construir-se em $\mathfrak{T}$ um elemento não nilpotente de potências dos a_i.

Antes de demonstrarmos êstes teoremas, vamos tirar algumas consequências importantes.

Corolário 1º:- É condição necessária e suficiente, para que $\mathfrak{T}$ seja nilanel, que se tenha $\mathfrak{T}^{n+1} = (0)$. Que a condição é suficiente, é um facto banal. Para se vêr que é necessária, provaremos que é nulo o produto de $n+1$ elementos quaisquer de $\mathfrak{T}$. Se pudesse ser $a_1 \ldots a_{n+1} \neq 0$, o ideal $a_1 \ldots a_n\mathfrak{T}$ seria $\neq 0$. Em virtude de se ter $a_i\mathfrak{T} \subseteq \mathfrak{T}$, o teorema 1º garantiria a existência de $\mathfrak{R}_1$ tal que

$$0 \subset \mathfrak{R}_1 \subseteq \mathfrak{T}, \qquad \mathfrak{R}_1 = (a_1\mathfrak{R}_1, \ldots, a_n\mathfrak{R}_1) .$$

Em seguida, o teorema 2º afirmaria a existência de elemento não nilpotente em $\mathfrak{T}$, que não seria, pois, nilanel. Logo é $\mathfrak{T}^{n+1} = (0)$.

Corolário 2º:- É condição necessária e suficiente, para que o sub-anel $\mathfrak{T}'$, de $\mathfrak{T}$, seja sub-nilanel, que se tenha $\mathfrak{T}'^{n+1} = (0)$. Que a condição é suficiente, é um facto banal. Que a condição é necessária, resulta, como no corolário 1º, tomando $0 \neq a'_1 \ldots a'_{n+1} \in \mathfrak{T}'$ e raciocinando com o ideal $a'_1 \ldots a'_n\mathfrak{T} \neq (0)$. O elemento não nilpotente formado à custa dos a'_i pertenceria a $\mathfrak{T}'$.

(1) Os resultados dêste § são devidos a J.Levitzki, "Über nilpotente Unterringe", Mathematische Annalen, Band 105, 1931, pags. 620 a 627.

Corolário 3º:- Todo o sub-anel $\mathcal{Y}'$, de $\mathcal{Y}$, tem um radical $\mathcal{R}'^{*} = \mathcal{R}'$, tal que $\mathcal{R}'^{\rho} = (0)$, com $\rho \leq n+1$. De facto, um ideal de $\mathcal{Y}'$ é um sub-anel de $\mathcal{Y}$; por conseqüência, um nilideal de $\mathcal{Y}'$ é nilpotente.

Corolário 4º:-Se $\mathcal{Y}$ tem elemento u, o sub-nilanel $\mathcal{Y}'$ é tal que $\mathcal{Y}'^{n} = (0)$. Prova-se que o produto $a'_1 \dots a'_n$ de n quaisquer elementos de $\mathcal{Y}'$ é nulo, tendo em conta que é $a'_1 \dots a'_n u = a'_1 \dots a'_n$ e que, portanto, os dois teoremas enunciados, para o caso $a'_1 \dots a'_n \neq 0$, permitiriam afirmar a existência de elemento não nilpotente em $\mathcal{Y}'$.

Façamos agora a demonstração do teorema 1º. Ponhamos

$$\mathfrak{k} \supseteq \mathfrak{k}' = (a_1 \mathfrak{k}, \dots, a_c \mathfrak{k}).$$

O ideal $\mathfrak{k}'$ é $\neq (0)$, visto que $\mathfrak{k}' \supseteq a_c \mathfrak{k} \neq (0)$. Ponhamos, depois,

$$\mathfrak{k} \supseteq \mathfrak{k}' \supseteq \mathfrak{k}'' = (a_1 \mathfrak{k}', \dots, a_c \mathfrak{k}'), \text{ com } a_l \mathfrak{k}' \subseteq a_l \mathfrak{k}.$$

O ideal $\mathfrak{k}''$ é $\neq (0)$, visto que $\mathfrak{k}'' \supseteq a_{c-1} \mathfrak{k}' \supseteq a_{c-1} a_c \mathfrak{k} \neq (0)$. Podemos prosseguir e estabelecer a série normal

$$\left\{ \mathfrak{k} \supseteq \mathfrak{k}' \supseteq \mathfrak{k}'' \supseteq \dots \supseteq \mathfrak{k}^{(c)} \supset (0) \right\},$$

com $\mathfrak{k}^{(c)} \supseteq a_1 \dots a_c \mathfrak{k} \neq (0)$. Como o comprimento desta série normal é $c+1$ e o comprimento de $\mathfrak{k}$ é $\leq c$, haverá repetições. Pondo

$$\mathfrak{k}^{(l+1)} = (a_1 \mathfrak{k}^{(l)}, \dots, a_c \mathfrak{k}^{(l)}) = \mathfrak{k}^{(l)},$$

fica demonstrado o teorema.

A demonstração do teorema 2º é um pouco mais longa. Destaquemos, de entre os $a_l \mathfrak{k}$, todos os que podem ser desprezados, sem que a soma dos demais deixe de ser $\mathfrak{k}$. Será, por ex., $\mathfrak{k} = (b_1 \mathfrak{k}, \dots, b_d \mathfrak{k})$, com $d \leq c$, e onde os b_j são elementos a_l. Se fôsse $d = 1$, a relação $\mathfrak{k} = b_1 \mathfrak{k}$ daria $b_1^m \mathfrak{k} = \mathfrak{k} \supset (0)$, e b_1 seria um elemento nas condições do teorema.

Supondo $d > 1$, formemos as relações

$$(0) \subset \mathfrak{k} \supset b_d \mathfrak{k} = (b_d b_1 \mathfrak{k}, \dots, b_d b_d \mathfrak{k}) \supset (0),$$

e, escrevendo $b_d = b_{m_1}$, designemos com b_{m_2} um elemento b_j tal que

$$(0) \subset b_{m_1} b_{m_2} \mathfrak{k} = (b_{m_1} b_{m_2} b_1 \mathfrak{k}, \dots, b_{m_1} b_{m_2} b_{m_1} \mathfrak{k}).$$

Vê-se existir uma sucessão $b_{m_1}, b_{m_2}, \dots$ tal que $\prod_{k=l}^{l+\sigma} b_{m_k} \cdot \mathfrak{k} \supset (0)$, quaisquer que sejam os inteiros positivos l e σ. Tomemos $i = 1$, $\sigma = c^2 - 1$. Vamos verificar a existência dum ideal $\mathfrak{k}'$ e de elementos $a'_1, \dots, a'_c$, formados por produtos dos a_j, satisfazendo às condições

$$(0) \subset \mathfrak{k}' \subset \mathfrak{k}, \qquad a'_1 \dots a'_c \neq 0, \qquad \mathfrak{k}' = (a'_1 \mathfrak{k}', \dots, a'_c \mathfrak{k}').$$

Levitzki distingue dois casos. No primeiro admite que há um produto de c dos b_{m_k}, que sejam consecutivos em $P = \prod_{k=1}^{c^2} b_{m_k}$, o qual não contém $b_{m_1} = b_d$. No segundo, faz a hipótese contrária. Se se dá o primeiro caso, suponhamos $a'_1 \dots a'_c$ o produto em causa. Tem-se

$$a'_1 \dots a'_c \mathfrak{k} \supset (0), \qquad a'_i \mathfrak{k} \subseteq \mathfrak{k},$$

e, conforme o teorema primeiro,

$$(0) \subset \mathfrak{k}' \subseteq \mathfrak{k}, \qquad \mathfrak{k}' = (a'_1 \mathfrak{k}', \dots, a'_c \mathfrak{k}').$$

Como em $a'_1, \dots, a'_c$ não figura b_d, será

$$(a'_1 \mathfrak{k}, \dots, a'_c \mathfrak{k}) \subset \mathfrak{k}, \text{ e, portanto, } \mathfrak{k}' \subset \mathfrak{k}.$$

Se em $\mathfrak{k}'$ há um elemento nas condições do teorema em demons-

tração, está o mesmo provado. Não sendo assim, a demonstração continua. Se, nos termos do 2º caso, cada c factores consecutivos de P contêm $b_{m_1} = b_d$, podemos escrever $P = b_{m_1} p_1 . b_{m_1} p_2 . b_{m_1} p_3 \ldots$, onde $p_1, p_2, \ldots$ são produtos dos a_i, pela ordem por que figuram em P, contendo cada p_j menos de c factores. A decomposição supra de P contém c factores, pelo menos, de modo que existe sempre uma parte de P, $P_1 = a'_{i_1} a'_{i_2} \ldots a'_{i_c}$, onde $a'_{ij} = b_{m_1} p_{ij}$, e onde os a'a' são consecutivos em P. Como no primeiro caso, tem-se agora

$$P_1 \mathfrak{K} \supset (0), \qquad a'_{ij} \mathfrak{K} \subseteq \mathfrak{K},$$

de sorte que existe $\mathfrak{K}'$, nos termos do teorema 1º, satisfazendo a

$$(0) \subset \mathfrak{K}' \subseteq \mathfrak{K}, \qquad \mathfrak{K}' = (a'_{i_1} \mathfrak{K}', \ldots, a'_{i_c} \mathfrak{K}').$$

Para se vêr que $\mathfrak{K}' \subset \mathfrak{K}$, basta ter em conta que

$$a'_{ij} \mathfrak{K} = b_{m_1} p_{ij} \mathfrak{K} \subseteq b_{m_1} \mathfrak{K}.$$

Em resumo: quando $d > 1$, há sempre um ideal $\mathfrak{K}'$ nas condições seguintes:

$$(0) \subset \mathfrak{K}' \subset \mathfrak{K}, \qquad (a'_1 \mathfrak{K}', \ldots, a'_c \mathfrak{K}') = \mathfrak{K}', \quad a'_1 \ldots a'_c \neq 0,$$

em que os a'_i são produtos dos a_j.

Partindo de $\mathfrak{K}'$, o raciocínio anterior repete-se. Obtem-se a sucessão de ideais

$$(3) \qquad \mathfrak{K} \supset \mathfrak{K}' \supset \mathfrak{K}'' \supset \cdots,$$

que prossegue enquanto não fôr possível chegar a

$$(4) \qquad (0) \subset \mathfrak{K}^{(t)} \subset \mathfrak{K}^{(t-1)}, \quad b\,\mathfrak{K}^{(t)} = \mathfrak{K}^{(t)},$$

com b = produto dos a_j. A condição de mínimo limita a cadeia (3) e da última igualdade (4) conclui-se o teorema. b é o elemento procurado.

Corolário 5º:- O ideal direito $\mathfrak{K}_1$ gerado pelos elementos $a_1, \ldots, a_c$ contém um elemento idempotente. Acabamos de verificar, com efeito, que $\mathfrak{K}_1$ não é nilpotente.

3) Aneis semi-simples - Diz-se que $\mathfrak{R}$ é um anel semi-simples quando verifica a condição de mínimo para ideais direitos e não tem radical $\mathfrak{N}$. Do estudo que vai ser feito (E.Noether, loc.cit.), resultará ser $\mathfrak{R}$ completamente redutível e ter elemento um. Será verificada, pois, a condição dupla de cadeia.

Teorema 1º:- O anel semi-simples $\mathfrak{R} \neq (0)$ é soma directa de ideais direitos simples. Tomemos, em $\mathfrak{R}$, um ideal direito mínimo $\mathfrak{K}_1 \neq (0)$. Como ideal simples, $\mathfrak{K}_1$ contém um elemento idempotente e_1, visto não poder ter-se $\mathfrak{K}_1^2 = (0)$, pois que $\mathfrak{R}$ não tem radical. Sabemos que é

$$\mathfrak{R} = e_1 \mathfrak{R} + \mathfrak{K}' = \mathfrak{K}_1 + \mathfrak{K}', \quad e_1^2 = e_1, \quad e_1 x' = 0 \qquad (x' \in \mathfrak{K}').$$

Em $\mathfrak{K}'$, se $\mathfrak{K}' \neq (0)$ não é simples, procuremos um ideal de $\mathfrak{R}$ que seja mínimo. Êsse ideal mínimo $\mathfrak{K}_2$ é necessàriamente simples. Se e_2 fôr um elemento idempotente de $\mathfrak{K}_2$, tem-se

$$\mathfrak{R} = e_2 \mathfrak{R} + \mathfrak{K}'' = \mathfrak{K}_2 + \mathfrak{K}'', \quad e_2^2 = e_2, \quad e_1 e_2 = 0, \quad e_2 x'' = 0 \quad (x'' \in \mathfrak{K}'').$$

Em particular, é

$$\mathfrak{K}' = \mathfrak{K}_2 + \mathfrak{o}_1, \quad (0) \neq \mathfrak{o}_1 \subset \mathfrak{K}'', \quad \mathfrak{o}_1 \subset \mathfrak{K}', \quad (\mathfrak{o}_1 = \text{ideal direito}),$$

pelo que vem $\mathfrak{R} = \mathfrak{K}_1 + \mathfrak{K}_2 + \mathfrak{o}_1$. Toma-se em $\mathfrak{o}_1$, se $\mathfrak{o}_1 \neq (0)$ não é simples, um ideal mínimo $\mathfrak{K}_3$ de $\mathfrak{R}$. Depois, como anteriormente, tem-se

$$\mathfrak{R} = e_3 \mathfrak{R} + \mathfrak{K}''' = \mathfrak{K}_3 + \mathfrak{K}''', \quad e_3^2 = e_3, \quad e_1 e_3 = 0, \quad e_2 e_3 = 0,$$

$e_3 x^{i''} = 0 \quad (x^{i''} \in \mathfrak{K}^{i''})$, $\mathfrak{r}_1 = \mathfrak{K}_3 + \mathfrak{r}_2$, $\mathfrak{J} = \mathfrak{K}_1 + \mathfrak{K}_2 + \mathfrak{K}_3 + \mathfrak{r}_3$,

$\mathfrak{r}_2 \subset \mathfrak{K}^{i''}$, $\mathfrak{r}_3 \subset \mathfrak{r}_2$, ($\mathfrak{r}_k$ = ideal direito). O raciocínio prossegue-se. Sendo $\mathfrak{J} \supset \mathfrak{K}^i \supset \mathfrak{r}_1 \supset \mathfrak{r}_2 \supset \mathfrak{r}_3 \supset \ldots$, a condição de mínimo garante que se chega a uma relação $\mathfrak{r}_{n-2} = \mathfrak{K}_n + \mathfrak{r}_{n-1}$, com $\mathfrak{r}_{n-1} = (0)$, e a uma decomposição

$$\mathfrak{J} = \mathfrak{K}_1 + \ldots + \mathfrak{K}_n + \mathfrak{r}_{n-1} = \mathfrak{K}_1 + \ldots + \mathfrak{K}_n ,$$

como se deseja. Os elementos idempotentes e_i satisfazem, assim, às condições

$$e_i^2 = e_i \ , \quad e_i e_k = 0 \quad (k > i) \ , \quad \mathfrak{K}_i = e_i \mathfrak{J} .$$

Teorema 2º:- Se um ideal direito $\mathfrak{K} = e\mathfrak{J} \neq \mathfrak{J}$ possui uma unidade esquerda e, existe um ideal direito $\mathfrak{K}^i = E\mathfrak{J}$, do qual $\mathfrak{K}$ é divisor normal autêntico, que possui igualmente uma unidade esquerda. A decomposição direita de Peirce,

$$s = es + (s - es) \ , \quad (s \in \mathfrak{J}) \quad \text{ou} \quad \mathfrak{J} = e\mathfrak{J} + \mathfrak{L} ,$$

contém uma parcela $\mathfrak{L}$ com um idempotente $e' \neq e$ tal que $ee' = 0$. Pondo $e_1 = e$, $e_2 = e' - e'e$, vê-se que é

$$e_2 e_1 = (e' - e'e)\, e = 0, \quad e_1 e_2 = 0, \quad e_2^2 = e_2 .$$

O elemento $E = e_1 + e_2$ é idempotente e constitui uma unidade esquerda para o ideal direito $\mathfrak{K}^i = E\mathfrak{J} = e_1\mathfrak{J} + e_2\mathfrak{J}$. Ora é $\mathfrak{K}^i \supset \mathfrak{K}$.

Corolário:- $\mathfrak{J}$ tem uma unidade esquerda - De facto, a construção sucessiva de $\mathfrak{K}, \mathfrak{K}', \mathfrak{K}'', \ldots$ satisfazendo a

$$\mathfrak{K} \subset \mathfrak{K}' \subset \mathfrak{K}'' \subset \ldots ,$$

é forçosamente limitada, pois, sendo $\mathfrak{J}$ completamente redutível, $\mathfrak{J}$ tem uma série de composição de comprimento limitado.

Teorema 3º:- O anel semi-simples $\mathfrak{J} \neq 0$ tem elemento um. Designemos com u a unidade esquerda de $\mathfrak{J}$, anteriormente construida, e façamos a decomposição esquerda de Peirce, $\mathfrak{J} = \mathfrak{J}u + \mathfrak{N}$. Sabemos que é $\mathfrak{N}u = (0)$, $u\mathfrak{N} = \mathfrak{N}$, e, portanto, $\mathfrak{N} = \mathfrak{N}\cdot u\,\mathfrak{N} = \mathfrak{N}u\cdot\mathfrak{N} = (0)$. Como $\mathfrak{J}$ não possui radical, deverá ser $\mathfrak{N} = (0)$, $\mathfrak{J} = \mathfrak{J}u$. Daqui se conclui o teorema.

Teorema 4º:- Se $\mathfrak{J} \neq (0)$ é uma soma directa de ideais direitos simples e tem elemento um, é semi-simples. A redutibilidade completa, como já anteriormente se assinalou, arrasta a condição dupla de cadeia. Em particular, arrasta a condição de mínimo. Para se concluir que não há radical, raciocina-se como segue. Seja $\mathfrak{K}$ tal que $\mathfrak{K}^2 = (0)$. Pondo $\mathfrak{J} = \mathfrak{K} + \mathfrak{K}'$, $u = e + e'$, sabemos que é $\mathfrak{K} = e\mathfrak{J}$, $e^2 = e$. Ora $e \in \mathfrak{K}$, o que leva a um absurdo.

Teorema 5º:- Um anel semi-simples $\mathfrak{J}$ é uma soma directa de aneis simples que mutuamente se anulam. Para fazer a demonstração, basta provar que $\mathfrak{J}$ é uma soma directa de ideais bilaterais, bilateralmente simples. Seja $\mathfrak{a}$ um ideal bilateral mínimo de $\mathfrak{J}$. Considerado como ideal direito, leva a

$$\mathfrak{J} = \mathfrak{a} + \mathfrak{C} = e_1\mathfrak{J} + e_2\mathfrak{J}, \qquad u = e_1 + e_2 \ ,$$

existindo também a decomposição

$$\mathfrak{J} = \mathfrak{b} + \mathfrak{r} = \mathfrak{J}e_1 + \mathfrak{J}e_2 .$$

Vamos vêr que $\mathfrak{C}$ é um ideal bilateral, mostrando ser $\mathfrak{C} = \mathfrak{r}$. Tem-se, com efeito, $\mathfrak{r} = \mathfrak{J}\mathfrak{r} = (\mathfrak{a}\,\mathfrak{r}, \mathfrak{C}\,\mathfrak{r})$, e, sendo $\mathfrak{r}\mathfrak{a} = \mathfrak{J}e_2 \cdot e_1\mathfrak{J} = (0)$, tem-se ainda $(\mathfrak{a}\,\mathfrak{r})^2 = \mathfrak{a}\,\mathfrak{r}\cdot\mathfrak{a}\,\mathfrak{r} = \mathfrak{a}\cdot\mathfrak{r}\mathfrak{a}\cdot\mathfrak{r} = (0)$. Será, pois, $\mathfrak{a}\,\mathfrak{r} = (0)$, e, por conseqüência, $\mathfrak{r} = \mathfrak{C}\mathfrak{r}$. Ora $\mathfrak{C} = \mathfrak{C}\mathfrak{J} = (\mathfrak{C}\mathfrak{b}, \mathfrak{C}\mathfrak{r})$, de modo que, tendo em conta ser $e_1 \in \mathfrak{a}$, ser $\mathfrak{a}$ bilateral e ser

$$\mathfrak{b} = \mathfrak{J}e_1 \subseteq \mathfrak{a} \ , \quad \mathfrak{C}\mathfrak{b} \subseteq \mathfrak{C}\,\mathfrak{a} \subseteq [\mathfrak{C}\ ,\ \mathfrak{a}] = (0) \ ,$$

vem $\mathfrak{C} = \mathfrak{C}\mathfrak{r} = \mathfrak{r}$, q. e. d. .

O ideal bilateral $\mathfrak{C}$ tem e_2 como elemento um. Considerando $\mathfrak{C}$ como um anel, os ideais direitos de $\mathfrak{C}$ são ideais direitos de $\mathfrak{I}$. A condição de mínimo transporta-se, pois, de $\mathfrak{I}$ para $\mathfrak{C}$. Decompondo $\mathfrak{C}$ sob a forma $\mathfrak{C} = \mathfrak{A}' + \mathfrak{C}'$, onde $\mathfrak{A}'$ é um ideal bilateral mínimo de $\mathfrak{C}$, o raciocínio anterior repete-se e prossegue-se, até ser obtido o resultado desejado. O número de ideais bilaterais $\mathfrak{A}, \mathfrak{A}', \ldots$ é, quando muito, igual ao número de ideais direitos da decomposição de $\mathfrak{I}$.

Com êste teorema, reduz-se o estudo dos aneis semi-simples ao estudo de aneis simples completamente redutíveis com elemento um.

Teorema 6º:- Um anel semi-simples comutativo $\mathfrak{I}$ é uma soma de corpos comutativos que se anulam simultâneamente. $\mathfrak{I}$ é uma soma de ideais bilaterais que se anulam simultâneamente, que são aneis simples e que têm elemento um. Ora um tal anel simples $\mathfrak{A}$ é um corpo, pois que a equação $ax = b$, com $a \neq 0$, é solúvel em $\mathfrak{A}$, pelo facto de se ter $a\mathfrak{A} = \mathfrak{A}a = \mathfrak{A}$.

Teorema 7º:- É condição necessária e suficiente, para que um anel seja semi-simples, que verifique a condição de mínimo e seja regular.

A condição é necessária. Se $\mathfrak{I}$ é semi-simples, tem lugar a condição de mínimo. Tomando um elemento $a \neq 0$, o ideal principal direito gerado por a, $(a)_d$, é uma soma directa de ideais direitos simples, visto que $\mathfrak{I}$ é completamente redutível:

$$(a)_d = (e_1)_d + \ldots + (e_k)_d \ .$$

Os idempotentes $e_1, \ldots, e_k$ podem supôr-se ortogonais, de modo que o idempotente $f = e_1 + \ldots + e_k$ satisfaz à igualdade $(f)_d = (a)_d$. Nessas condições, é $f = as$, $a = ft$, e, portanto,

$$fa = asa = ft = a.$$

Assim, $\mathfrak{I}$ é regular.

A condição é suficiente. Se $\mathfrak{I}$ é regular, não há radical. O teorema fica provado.

Visto que os aneis semi-simples possuem radical $\mathfrak{R}^* = \mathfrak{R} = (0)$, podem ser definidos finalmente como aneis que verificam a condição de mínimo para ideais direitos e que não possuem nilideal direito.

São válidas ainda as duas proposições a seguir.

Teorema:- Num anel para o qual $\mathfrak{I}/\mathfrak{R} = \mathfrak{I}'$ é semi-simples, $\mathfrak{R}^*$ existe e é $\mathfrak{R}^* = \mathfrak{R}$. Resulta imediatamente da proposição 1ª citada no §3 do Capítulo anterior (relações entre $\mathfrak{R}^*$ e $\mathfrak{R}$).

Teorema:- Se e é idempotente, as parcelas $e\mathfrak{I}e$ e $\mathfrak{J}$, da decomposição de Peirce, são aneis semi-simples. A condição de mínimo transporta-se de $\mathfrak{I}$ para $e\mathfrak{I}e$ e $\mathfrak{J}$. Resta vêr que êstes últimos não têm radical. Ora isso resulta de se ter $e\mathfrak{R}^*e = (0)$, $[\mathfrak{J}, \mathfrak{R}^*] = (0)$, pois $\mathfrak{R}^* = (0)$, e do facto do radical sem asterisco estar contido no radical com asterisco. Uma demonstração directa simples é a seguinte. Seja $\delta \neq (0)$ um ideal direito de $e\mathfrak{I}e$ tal que $\delta^2 = (0)$. Então, $\mathfrak{K} = (\delta, \delta\mathfrak{A})$ daria, tendo em vista que $\mathfrak{A}e = (0)$, $\mathfrak{K}^2 = (\delta^2, \delta^2\mathfrak{A}) = (0)$, o que seria absurdo. Se δ fôsse um ideal direito de $\mathfrak{J}$ e se tivesse $\delta^2 = (0)$, tendo em conta que $e\delta = (0)$, viria $\mathfrak{K}^2 = (\delta^2, \delta^2\mathfrak{J}e) = (0)$, com $\mathfrak{K} = (\delta, \delta\mathfrak{J}e)$, o que seria absurdo.

Antes de passarmos ao estudo dos aneis simples, daremos agora um certo número de teoremas que envolvem ainda aneis semi-simples e tratam com elementos idempotentes.

Teorema 1º:- Um anel semi-simples $\mathfrak{I} \neq (0)$ tem um elemento primitivo. Tomemos em $\mathfrak{I}$ um anel direito mínimo $\neq (0)$. Como êsse ideal não é nilpotente, terá elemento idempotente. Um teorema do §4 do Cap. anterior garante que êsse idempotente é primitivo.

Teorema 2º:- Um idempotente não primitivo, e é soma dum certo número de elementos primitivos que se anulam dois a dois.

Ponhamos $\mathfrak{I} = e\mathfrak{I}e + \mathfrak{K}' = \mathfrak{r}_1 + \ldots + \mathfrak{r}_r + \mathfrak{C}_1 + \ldots + \mathfrak{C}_q$, com

$$e\mathfrak{I}e = \mathfrak{r}_1 + \ldots + \mathfrak{r}_r \ , \qquad \mathfrak{K}' = \mathfrak{C}_1 + \ldots + \mathfrak{C}_q \ ,$$

onde os $\mathfrak{r}_i$ e os $\mathfrak{C}_j$ são ideais direitos simples. Sabemos que é

$$u = e + (u - e) = e_1 + \ldots + e_r + f_1 + \ldots + f_q \ ,$$

com $u - e \in \mathfrak{K}'$, $e_i \in \mathfrak{k}_i$, $f_j \in \mathfrak{k}_j$. A relação $e = e_1 + \ldots + e_r$ demonstra o teorema. Tem-se, mesmo, $e_i f_j = 0$.

Teorema 3º:- Se $e_1, \ldots, e_r$ são elementos primitivos de $\mathfrak{J}$ verificando as condições $e_i e_k = 0$, se $i \neq k$, e se $e = \sum e_i$ não é o elemento u, então u pode decompôr-se numa soma de mais do que r elementos primitivos (entre os quais os r dados) que se anulam dois a dois. De facto, tem-se aqui

$$e\mathfrak{J} = e_1\mathfrak{J} + \ldots + e_r\mathfrak{J},$$

e, como no teorema anterior, $u = e + (u - e) = e_1 + \ldots + e_r + f_1 + \ldots + f_q$.

4) Aneis simples completamente redutíveis com elemento um

A estrutura dêstes aneis (E. Noether), loc. cit.) resulta como conseqüência dum certo número de proposições que vamos estabelecer.

Teorema 1º:- O anel endomórfico dum módulo simples é um corpo. Se $\mathfrak{M}$ é o módulo em questão, um endomorfismo operatório só pode levar ao sub-módulo nulo ou ao próprio módulo. Nêste último caso, há um automorfismo operatório inverso, o que mostra haver no anel endomórfico do módulo um inverso de cada elemento não nulo, q. e. d.

Teorema 2º:- Os ideais direitos $\mathfrak{k}_i$ da decomposição dum anel simples completamente redutível são operatòriamente isomorfos. Dados $\mathfrak{k}_j$ e $\mathfrak{k}_i$ da decomposição de $\mathfrak{J}$, vamos precisar alguns dos resultados estabelecidos no § 7 do Cap. anterior. Tomemos $a_{ij} \in \mathfrak{J}_{ij} \subseteq \mathfrak{k}_i$. A correspondência $\mathfrak{k}_j \sim a_{ij}\mathfrak{k}_j \subseteq \mathfrak{k}_i$ não é a homomorfia nula, se fôr $a_{ij} \neq 0$. De facto, tem-se $e_j \rightarrow a_{ij}.e_j = a_{ij}$. Só pode ser, pois, $a_{ij}\mathfrak{k}_j = \mathfrak{k}_i$, visto que $\mathfrak{k}_i$ é simples. Os ideais $\mathfrak{k}_j$ e $\mathfrak{k}_i$ são operatòriamente isomorfos.

Corolário:- Todos os ideais direitos simples não nulos dum anel nas condições do são operatòriamente isomorfos. Se $\mathfrak{K}$ e $\mathfrak{K}'$ são dois dêsses ideais, é claro que não têm elemento comum, salvo o elemento nulo. Mas, então, a soma directa $\mathfrak{K} + \mathfrak{K}'$ pode aparecer como parcela na decomposição do anel completamente redutível.

Teorema 3º:- O anel $\mathfrak{J}_{ii}$ é um corpo. Vê-se, com efeito, que $\mathfrak{J}_{ii}$ é isomorfo do anel endomórfico de $\mathfrak{k}_i$. Êste último, conforme o teorema 1º, é um corpo.

Representemos com $x_{ij}, y_{ij}, \ldots$ elementos de $\mathfrak{J}_{ij}$. Um elemento x_{ij} diz-se regular, se verificar a igualdade $x_{ij}\mathfrak{J}_{ji} = \mathfrak{J}_{ii}$. Dado $x_{ij} \neq 0$, vimos que era $x_{ij}\mathfrak{k}_j = \mathfrak{k}_i$. Assim, $x_{ij}\mathfrak{k}_j\mathfrak{M}_i = \mathfrak{k}_i\mathfrak{M}_i$, ou seja $x_{ij}\mathfrak{J}_{ji} = \mathfrak{J}_{ii}$. Todos os elementos $x_{ij} \neq 0$ são, pois, elementos regulares. Pode enunciar-se o

Teorema 4º:- Os elementos $x_{ij} \in \mathfrak{J}_{ij}$ não nulos são elementos regulares, isto é, verificam a igualdade $x_{ij}\mathfrak{J}_{ji} = \mathfrak{J}_{ii}$.

A circunstância de $\mathfrak{J}_{jj}$ ser um corpo permite demonstrar ainda o

Teorema:- Se $\mathfrak{J}_{ij}\, x_{ij} \neq (0)$, tem-se $\mathfrak{J}_{ij}\, x_{ij} = \mathfrak{J}_{jj}$. Na verdade

$$\mathfrak{J}_{ji}\, x_{ij} \subseteq \mathfrak{J}_{ji}\mathfrak{J}_{ij} = \mathfrak{J}_{jj}.$$

Qualquer que seja z_{jj}, a equação $z.y_{ji}\, x_{ij} = z_{jj}$ é solúvel em $\mathfrak{J}_{jj}$, desde que se tenha $y_{ji}\, x_{ij} \neq 0$. E como, nêsse caso, $z.y_{ji} \in \mathfrak{J}_{ji}$, segue-se $zy_{ji}.x_{ij} = z_{jj}$, donde se tira a afirmação. Tem-se também o seguinte

Teorema:- Se os elementos x_{ij}, x_{ji} são diferentes de zero, o seu produto também o é. De verdade pode escrever-se $x_{ij}.\mathfrak{J}_{jj} = \mathfrak{J}_{ij}$, e, portanto, existe $y_{ij} \in \mathfrak{J}_{ij}$ tal que $x_{ji}y_{ij} = e_j$. Em seguida, tem-se

$$x_{ij}\, x_{ji}\, y_{ij} = x_{ij}\, e_j = x_{ij} \neq 0.$$

Como conseqüência, tira-se que a relação $\mathfrak{J}_{ji}\, x_{ij} = \mathfrak{J}_{jj}$ tem lugar, sempre que $x_{ij} \neq 0$. E isso porque, sendo $\mathfrak{J}_{ji} \neq (0)$, existe sempre um elemento $x_{ji} \neq 0$ tal que $x_{ji}\, x_{ij} \neq 0$, não podendo ser, pois, $\mathfrak{J}_{ji}\, x_{ij} \neq (0)$. Em resumo: Se $x_{ij} \neq 0$, têm lugar as igualdades

$$x_{ij}\mathfrak{J}_{ji} = \mathfrak{J}_{ii}, \qquad \mathfrak{J}_{ii}\, x_{ij} = \mathfrak{J}_{ij}.$$

Teorema 5º:- O anel $\mathfrak{J}$ tem n^2 matrizes unidades. Se $\mathfrak{J}$ é um corpo, o teorema está demonstrado. No caso contrário, u é soma dos elementos primitivos e_l, que se anulam dois a dois. Ponhamos $e_l = e_{ll}$. Em seguida, em cada $\mathfrak{J}_{l1}$ tomemos um elemento $e_{1l} \neq 0$. Visto que $e_{1l}\mathfrak{J}_{l1} = \mathfrak{J}_{ll}$, tomemos em $\mathfrak{J}_{l1}$ o elemento e_{l1} tal que $e_{1l}e_{l1} = e_{ll}$. Interessam-nos, depois, os produtos $e_{1l}e_{l1}$. Tem-se

$$(e_{1l}e_{l1})^2 = e_{1l}e_{l1}e_{1l}e_{l1} = e_{1l}e_{ll}e_{l1} = e_{1l}e_{l1},$$

e, por conseqüência, $e_{1l}e_{l1} = e_{11}$, visto que $e_{1l}e_{l1} \in \mathfrak{J}_{11}$ e êste anel é um corpo. É claro que não poderia admitir-se $e_{1l} \cdot e_{l1} = 0$, pois

$$e_{1l}e_{l1}e_{1l} = e_{1l}e_{ll} = e_{1l} \neq 0.$$

Para prosseguirmos na construção das matrizes, poremos, por definição, $e_{lk} = e_{l1}e_{1k}$. Vê-se imediatamente que $e_{lk} \neq 0$. De facto

$$e_{lk}e_{ki} = e_{l1}e_{1k}e_{ki}e_{1l} = e_{l1}e_{11}e_{1l} = e_{l1}e_{1l} = e_{ll}.$$

Finalmente, tem-se

$$e_{lk}e_{kf} = e_{l1}e_{1k}e_{ki}e_{1f} = e_{l1}e_{11}e_{1f} = e_{l1}e_{1f} = e_{lf},$$

$$e_{lk}e_{jf} = e_{lk}e_{kk}e_{jj}e_{jf} = 0, \qquad (j \neq k).$$

Os elementos e_{lk} constituem o sistema de n^2 matrizes que tinhamos em vista.(1)

(1) O processo de construção, que voltará a ser utilizado adiante, é devido a Artin, loc.cit.

Teorema 6º:- O conjunto dos elementos de $\mathfrak{J}$ que comutam com as matrizes unidades constitui um corpo. O anel $\mathfrak{A}$ do § 9 do Cap. anterior é, de facto, isomorfo do corpo $\mathfrak{J}_{11}$.

Teorema fundamental:- Um anel simples completamente redutível com elemento um é isomorfo dum anel completo $\mathfrak{M}$, de matrizes, com elementos dum corpo, e reciprocamente. Para a demonstração, só resta provar que o anel $\mathfrak{M}$ é completamente redutível(1). Ora consideremos o conjunto de elementos de $\mathfrak{M}$,

$$\mathfrak{K}_1 = \mathfrak{K}e_{11} + \mathfrak{K}e_{12} + \ldots + \mathfrak{K}e_{1n}, \qquad (\mathfrak{K} = \text{corpo fundamental}).$$

Êste conjunto constitui um ideal direito, pois, se

$$r_1 = \lambda_1 e_{11} + \ldots + \lambda_n e_{1n} \in \mathfrak{K}_1,$$

tem-se (com $\alpha_{1k} \in \mathfrak{K}$)

$$r_1 \sum_{1,k} \alpha_{1k}e_{1k} = \sum_{1,k,j} \lambda_j e_{1j}\alpha_{1k}e_{1k} = \sum_{1,k} \lambda_1 \alpha_{1k}e_{1k} \in \mathfrak{K}_1.$$

O ideal $\mathfrak{K}_1$ é simples. Se o elemento supra r_1 não é nulo, o ideal direito que êle gera é $\mathfrak{K}_1$, como vamos vêr. $\mathfrak{K}_1$ contém, com efeito, se $\lambda_k \neq 0$, o elemento $\sum_j \lambda_j e_{1j} \cdot \lambda_k^{-1} e_{k\mu} = e_{1\mu}$, qualquer que seja $\mu = 1, 2, \ldots, n$.

Pondo, geralmente,

$$\mathfrak{K}_\mu = \mathfrak{K}e_{\mu 1} + \mathfrak{K}e_{\mu 2} + \ldots + \mathfrak{K}e_{\mu n},$$

o anel $\mathfrak{M}$ é a soma directa

$$\mathfrak{M} = \mathfrak{K}_1 + \ldots + \mathfrak{K}_n, \qquad \text{q. e. d.}$$

Podemos afirmar agora que todos os ideais direitos simples de $\mathfrak{M}$ são operatòriamente isomorfos e que o corpo automórfico de cada ideal direito simples é isomorfo de $e_{11}\mathfrak{M}$.

(1) Viu-se no § 3 do Cap. anterior que $\mathfrak{M}$ é simples.

$e_{11} = M_{11}$. Sendo $m \in \mathfrak{M}$, é $m = \sum_{i,k} \lambda_{ik} e_{ik}$, e

$$e_{11} m . e_{11} = \sum_{i,k} \lambda_{ik} e_{11} e_{ik} e_{11} = \lambda_{11} e_{11} = e_{11} \cdot \lambda_{11} e_{11} \cdot e_{11} .$$

Assim ,o corpo automórfico de cada ideal direito simples é isomorfo do corpo $M_{11} = \mathfrak{k} e_{11}$, ou seja do corpo $\mathfrak{k}$.

Se quizermos construir o corpo $\mathcal{C}$,temos de considerar os elementos de $\mathfrak{M}$ que comutam com todos os e_{ik} ,ou seja os elementos

$$a = \sum_i e_{i1} \lambda_{11} e_{11} e_{1i} = \sum_i \lambda_{11} e_{ii} = \lambda_{11} u .$$

É,assim, $\mathcal{C} = \mathfrak{k} u$.

Uma questão importante a tratar respeita ao estudo da passagem dum sistema de matrizes unidades a um segundo sistema nas mesmas condições (mudança de base). Podemos,a êsse respeito,enunciar o

Teorema:- Dadas duas representações de $\mathcal{T}$,

$$\mathcal{T} = \sum_{i,k} \mathcal{C} e_{ik} , \qquad \mathcal{T} = \sum_{i,k} \mathcal{C}' e'_{ik} ,$$

existe um automorfismo interno tal que

$$\mathcal{C}' = x^{-1} \mathcal{C} x , \qquad e'_{ik} = x^{-1} e_{ik} x .$$

Se pômos $e_{ii} \mathcal{T} = \mathfrak{K}_i$, $e'_{ii} \mathcal{T} = \mathfrak{K}'_i$, sabemos que os ideais direitos simples $\mathfrak{K}_i$ e $\mathfrak{K}'_i$ são operatòriamente isomorfos. Estudemos por ex., $\mathfrak{K}_1 \cong \mathfrak{K}'_1$. Tem-se

$$e_{11} = e_1 \longrightarrow a' \in \mathfrak{K}'_1 , \qquad a' \mathfrak{K}_1 = \mathfrak{K}'_1$$

$$a = e_1 a \longrightarrow a'a = e'_{11} = e'_1 \in \mathfrak{K}'_1 , \quad a \in \mathfrak{K}_1 , \quad a \mathfrak{K}'_1 = \mathfrak{K}_1 ,$$

pois $a' \mathfrak{K}_1$ e $a \mathfrak{K}'_1$ não podem ser os ideais nulos,visto que

$$a'a = e'_1 , \qquad aa' \longrightarrow e'_1 a' = a' , \quad aa' = e_1 .$$

Nestas condições,pondo $x = \sum_i e_{i1} a e'_{1i}$, $y = \sum_j e'_{j1} a' e_{1j}$,vê-se que é

$$xy = \sum_i e_{i1} a e'_{i1} a' e_{1i} = \sum_i e_{i1} aa' e_{1i} = \sum_i e_{ii} = u ,$$

$$yx = \sum_j e'_{j1} a' e_{11} a e'_{1j} = \sum_j e'_{jj} = u , \qquad y = x^{-1} ,$$

$$x^{-1} e_{ik} x = e'_{i1} a' e_{1k} e_{k1} a e'_{ik} = e'_{i1} a'a e'_{ik} = e'_{ik} .$$

No tocante aos corpos $\mathcal{C}$ e $\mathcal{C}'$,observemos que,se $\alpha \in \mathcal{C}$, $\alpha' \in \mathcal{C}'$, é,para $s,t \in \mathcal{T}$,

$$\alpha = \sum_i e_{i1} s e_{1i} , \qquad \alpha' = \sum_i e'_{i1} t e'_{1i} .$$

Ora $x^{-1} \alpha x = \sum_{j,i} e'_{j1} a' e_{ij} \alpha e_{i1} a e'_{1i} = \sum_j e'_{j1} a' e_{11} \alpha a e'_{1j} \in \mathcal{C}'$.
Isto mostra que o automorfismo interno em causa leva de cada elemento de $\mathcal{C}$ a um elemento de $\mathcal{C}'$. Inversamente,é

$$\alpha' = \sum_i x^{-1} e_{i1} x t x^{-1} e_{1i} x = x^{-1} \left(\sum_i e_{i1} x t x^{-1} e_{1i} \right) x ,$$

onde o elemento entre parêntesis pertence a $\mathcal{C}$, q. e. d.

Sem necessidade de demonstração,podemos enunciar o

Teorema:- Um anel simples completamente redutível à direita,com elemento um,é também completamente redutível à esquerda,e inversamente (sempre sob a hipótese da existência de u). Basta ter em conta que o anel é isomorfo do anel $\mathfrak{M}$ de matrizes.

Teorema:- O centro $\mathfrak{z}_{\mathfrak{M}\mathcal{C}}$,de $\mathfrak{M}$,é o centro $\mathfrak{z}_{\mathcal{C}}$,de $\mathcal{C}$.Se uma matriz $m = \sum_{i,k} \lambda_{ik} e_{ik}$ pertence a $\mathfrak{z}_{\mathfrak{M}\mathcal{C}}$,comuta com os e_{ik} , pelo que pertence a $\mathcal{C}$. Será a matriz diagonal $m = \lambda u = \lambda e_{11} + \ldots + \lambda e_{nn}$. Devendo ter-se,porém,para cada elemento $m' = \lambda' u$, onde $\lambda' \in \mathfrak{k}$ é qualquer, $\lambda u . \lambda' u = \lambda \lambda' u = \lambda' \lambda u$, vê-se que deve ser $\lambda \lambda' = \lambda' \lambda$. Assim,só podem intervir na expressão de m os elementos do centro de $\mathfrak{k}$. Será,pois, $\mathfrak{z}_{\mathfrak{M}\mathcal{C}} = \mathfrak{z}_{\mathfrak{k}} u$, q. e. d.. É claro que $\mathfrak{z}_{\mathfrak{M}\mathcal{C}}$ é um corpo.

Corolário:- O centro dum anel semi-simples $\mathcal{T}$ é uma soma directa de corpos comutativos. Cada corpo é centro dum $\mathcal{A}_\nu$ (ideal bilateral simples da decomposição de $\mathcal{T}$) e tem, assim, a forma $\mathcal{Z}_{\mathcal{A}_\nu} = \mathcal{Z}_{\mathcal{C}_\nu} u_\nu$, onde u_ν é o elemento um de $\mathcal{A}_\nu$ e $\mathcal{C}_\nu$ é o corpo fundamental das matrizes $\mathcal{A}_\nu$, corpo que é isomorfo do corpo automórfico de cada ideal direito simples de $\mathcal{A}_\nu$.

É interessante precisar agora um resultado obtido anteriormente, estabelecendo o seguinte

Teorema:- Num anel simples completamente redutível, com elemento um, um sub-nilanel está sempre contido num sub-nilanel máximo e todos os sub-nilâneis máximos resultam dum dêles por um automorfismo interno. A existência de sub-nilaneis foi demonstrada no § 7 do Cap. anterior. Seja φ um sub-nilanel de expoente r. Consideremos os ideais

$$\mathcal{T},\ \varphi\mathcal{T} = \mathfrak{K}_1,\quad \varphi^2\mathcal{T} = \mathfrak{K}_2,\ \ldots,\ \varphi^{r-1}\mathcal{T} = \mathfrak{K}_{r-1},\ \varphi^r\mathcal{T} = (0).$$

Não pode ser, para $k < r-1$, $\mathfrak{K}_k = \mathfrak{K}_{k+1}$, pois que se teria então $\mathfrak{K}_k = \varphi^k\mathcal{T} = \varphi^{k+1}\mathcal{T} = \ldots = (0)$, o que não é válido, pelo facto de ser $\varphi^k\varphi = \varphi^{k+1} \supset (0)$. É, assim,

$$\mathcal{T} \supset \mathfrak{K}_1 \supset \cdots \supset \mathfrak{K}_{r-1} \supset (0),$$

onde a circunstância $\mathfrak{K}_{r-1} \supset (0)$ resulta de $\mathcal{T}$ ter elemento um. A redutibilidade completa de $\mathcal{T}$ permite escrever

$$\mathcal{T} = \mathfrak{K}_1 + \overline{\mathfrak{K}}'_r = \mathfrak{K}_2 + \overline{\mathfrak{K}}'_{r-1} = \cdots = \mathfrak{K}_{r-1} + \overline{\mathfrak{K}}'_2,$$

$$\mathfrak{K}_1 = \mathfrak{K}_2 + \overline{\mathfrak{K}}_{r-1},\ \mathfrak{K}_2 = \mathfrak{K}_3 + \overline{\mathfrak{K}}_{r-2},\ \ldots,\ \mathfrak{K}_{r-2} = \mathfrak{K}_{r-1} + \overline{\mathfrak{K}}_2,\ \mathfrak{K}_{r-1} = \overline{\mathfrak{K}}_1,$$

$$\mathfrak{K}_{r-\rho} = \overline{\mathfrak{K}}_1 + \ldots + \overline{\mathfrak{K}}_\rho,\quad \mathcal{T} = \overline{\mathfrak{K}}_1 + \ldots + \overline{\mathfrak{K}}_r,\qquad (\overline{\mathfrak{K}}'_r = \overline{\mathfrak{K}}_r).$$

Poremos $u = \sum_{i=1}^{r} \overline{e}_i$, $e_{r-\rho} = \overline{e}_1 + \ldots + \overline{e}_\rho$, onde $\overline{e}_i \in \overline{\mathfrak{K}}_i$. Seja, então, $a \in \varphi \subseteq \mathfrak{K}_1$. É claro que se tem $a\,\mathfrak{K}_{r-\rho} = a\varphi^{r-\rho}\mathcal{T} \subseteq$

$\subseteq \varphi^{r-\rho+1}\mathcal{T} = \mathfrak{K}_{r-\rho+1}$, e, por conseqüência, $a e_{r-\rho} \in \mathfrak{K}_{r-\rho+1}$. Pondo $a = \sum_{i=1}^{r-1} \overline{a}_i$, com $\overline{a}_i \in \overline{\mathfrak{K}}_i$, tem-se

$$\sum_{i=1}^{r-1} \overline{a}_i \cdot \sum_{j=1}^{\rho} \overline{e}_j \in \sum_{k=1}^{\rho-1} \overline{e}_k\,\mathcal{T}.$$

Quando $i < \rho - 1$, a parcela correspondente do primeiro membro da relação anterior é nula, pois que a soma dos $\overline{\mathfrak{K}}_i$ é directa. Temos, pois,

$$\overline{a}_s \cdot \sum_{j=1}^{\rho} \overline{e}_j = 0, \qquad \text{se} \qquad s = \rho, \rho+1, \ldots, r-1,$$

$$\overline{a}_s \cdot \sum_{j=1}^{r} \overline{e}_j = \overline{a}_s, \qquad \overline{a}_s = \overline{a}_s \cdot \sum_{j=\rho+1}^{r} \overline{e}_j \in \overline{e}_s\,\mathcal{T} \cdot \sum_{j=\rho+1}^{r} \overline{e}_j.$$

Façamos, nesta última relação, sucessivamente, $\rho = 1$, $s = 1$; $\rho = 2$, $s = 2$; $\ldots$; $\rho = r-1$, $s = r-1$. Vem

$$\overline{a}_s \in \overline{e}_s\,\mathcal{T} \cdot \sum_{j=s+1}^{r} \overline{e}_j, \qquad a \in \sum_{s=1}^{r-1} \sum_{j=s+1}^{r} \overline{e}_s\,\mathcal{T}\,\overline{e}_j = \sum_{s<j} \overline{e}_s\,\mathcal{T}\,\overline{e}_j = \mathcal{J}.$$

Conclui-se, assim, $\varphi \subseteq \mathcal{J}$. Pelo facto de $\mathcal{T}$ ser uma soma de ideais direitos simples, cada $\overline{\mathfrak{K}}_j$ é também uma soma de ideais direitos simples. Decompondo, sucessivamente, $\overline{\mathfrak{K}}_1, \ldots, \overline{\mathfrak{K}}_r$, obtem-se

$$\mathcal{T} = \sum_{j=1}^{r} \overline{\mathfrak{K}}_j = \sum_{i=1}^{h} E_i\,\mathcal{T}.$$

Substituindo em $\mathcal{J}$ os $\overline{e}_s$, $\overline{e}_j$ por somas dos E_i correspondentes, vê-se que é $\mathcal{J} \subseteq \sum_{i<j} E_i\,\mathcal{T}\,E_j = \mathcal{P}$, e, portanto, $\varphi \subseteq \mathcal{P}$. Vamos verificar agora que $\mathcal{P}$ é sub-nilanel máximo. Seja $\mathcal{P}' \supset \mathcal{P}$, onde $\mathcal{P}'$ é sub-nilanel. Existe $\mathcal{P}'' \supseteq \mathcal{P}'$, com $\mathcal{P}'' = \sum_{i<j} E''_i\,\mathcal{T}\,E'_j$, construido a partir de $\mathcal{P}'$, como $\mathcal{P}$ se construiu a partir de φ. A existência dum automorfismo interno definido por um elemento

$x \in \mathfrak{r}$ tal que

$$x^{-1} E_i x = E_i' , \qquad x^{-1} \mathfrak{p} x = \mathfrak{p}''$$

é um facto conhecido. Como $\mathfrak{r}$ é um módulo relativamente a um corpo, o sub-módulo $\mathfrak{p}''$, que, em virtude do automorfismo, teria uma base com o mesmo número de elementos que $\mathfrak{p}$, teria, por outro lado, uma base com um número maior de elementos. Conclui-se, assim, $\mathfrak{p}' = \mathfrak{p}$, q. e. d.

Capítulo III

Aneis semi-primários[1]

1) Sôbre alguns teoremas gerais relativos a aneis - Diz-se que e é um idempotente especial, se não existir idempotente $f \neq 0$ tal que $ef = fe = 0$. Se um anel tem elemento u, êste é sempre um idempotente especial.

Teorema:- Um anel com elemento u apenas tem u como idempotente especial. Se e fôr idempotente especial, pondo $\mathfrak{r} = e\mathfrak{r} + \mathfrak{L}$, tem-se $u = e + (u - e)$. O elemento $v = u - e$ é idempotente, valendo $ev = ve = 0$, ou seja $v = 0$, $e = u$.

Dado um anel $\mathfrak{r}$, nêste Capítulo poremos sempre $\mathfrak{r}/\mathfrak{K}^* = \mathfrak{r}'$.

(1) Compare Köthe, loc.cit. e Deuring, loc.cit. Veja-se também Almeida Costa, "Sôbre os aneis semi-primários", atrás citado.

Teorema:- Se se conhecem em $\mathfrak{r}'$ os idempotentes e_i' $(i=1,2,\ldots,n)$ ortogonais dois a dois, podem construir-se em $\mathfrak{r}$ os idempotentes correspondentes e_i, também ortogonais dois a dois. Tomemos e_i' e construamos e_i a partir dum elemento $r = b_{10}$, de correspondente e_i' (Cap.I, § 4). Se $e_1, \ldots, e_{m-1}$ são elementos idempotentes, já determinados sob as condições

$$e_i e_k = 0 , \quad \text{se } i \neq k , \quad e_i^2 = e_i , \quad e_i \rightarrow e_i' ,$$

a construção de e_m faz-se do modo seguinte. Designemos com $f_m \in \mathfrak{r}$ um elemento de correspondente e_m' e ponhamos

$$b_{10} = f_m - f_m(e_1+\ldots+e_{m-1}) - (e_1+\ldots+e_{m-1}) f_m + (e_1+\ldots+e_{m-1}) \cdot f_m(e_1+\ldots+e_{m-1}) .$$

Vê-se que b_{10} tem e_m' como correspondente e satisfaz às condições

$$b_{10} e_i = e_i b_{10} = 0 , \quad (i = 1,2,\ldots,m-1) .$$

A partir de b_{10} faz-se, como anteriormente, a construção dum idempotente e_m, de correspondente e_m'. As condições $e_i e_m = e_m e_i = 0$ são asseguradas, pois que

$$e_i b_{11} = e_i(b_{10} - 2b_{10} t + t) = e_i t = e_i(b_{10}^2 - b_{10}) = 0 ,$$

$$b_{11} e_i = (b_{10} - 2b_{10} t + t) e_i = 0 ,$$

o mesmo sucedendo com todos os b_{1j}.

Corolário:- No homomorfismo $\mathcal{T} \sim \mathcal{T}'$, a todo o idempotente especial e corresponde um idempotente especial e', e reciprocamente. A demonstração é imediata.

Diz-se que em $\mathcal{T}$ é válida a propriedade P, quando se realiza a seguinte condição: se $e_1, \ldots, e_r$ são elementos primitivos de $\mathcal{T}$ verificando as condições $e_i e_k = 0$, se $i \neq k$, e se $e = \Sigma e_i$ não é um idempotente especial, existe em $\mathcal{T}$ um idempotente que pode decompôr-se numa soma de mais do que r elementos primitivos (entre os quais os r anteriores) que se anulam dois a dois.

No final do § 3 do Cap. anterior, viu-se que a propriedade em referência tem lugar num anel semi-simples. De facto, na decomposição $e = \Sigma e_i$, que existe, se e não é primitivo, supôr que e não é idempotente especial é supôr $e \neq u$. Ora u decompõe-se em mais parcelas ortogonais do que e, figurando em u as parcelas de e.

Pode enunciar-se imediatamente o seguinte

Teorema:- Se a propriedade P é válida em $\mathcal{T}$ e $\mathcal{K}^*$ existe, a propriedade P é válida em $\mathcal{T}'$, e reciprocamente.

Posto isto, consideremos um idempotente especial $e \in \mathcal{T}$ e a decomposição $\mathcal{T} = e\mathcal{A} + \mathcal{L} e + \mathcal{J} + e\mathcal{T}e$. Vale o

Teorema:- É necessário e suficiente, para que e seja especial, que $\mathcal{L}$ (ou $\mathcal{A}$) não tenha idempotente. Comecemos por observar que e é idempotente especial quando $\mathcal{J}$ não tem idempotente e reciprocamente. Então, se $\mathcal{L}$ não tem idempotente, $\mathcal{J}$ não tem idempotente e e é especial. Inversamente, a não existência de idempotente em $\mathcal{J}$ arrasta a não existência em $\mathcal{L}$, pelo seguinte: se existisse o idempotente $f \in \mathcal{L}$, ter-se-ia $f = fe + i$, $(i \in \mathcal{J})$, $i = f - fe$, $i^2 = (f - fe)(f - fe) = f - fe = i$, e viria, assim,

$$i = 0 , \quad f = fe , \quad f^2 = f = fe \cdot fe = 0 , \quad \text{q. e. d.}$$

Teorema:- Se um anel regular tem idempotente especial, êste só pode ser o elemento u. Seja e o idempotente em causa. A decomposição $\mathcal{T} = e\mathcal{T} + \mathcal{L}$, visto que $\mathcal{L}$ não pode ter idempotente, leva a $\mathcal{L} = (0)$, $\mathcal{T} = e\mathcal{T}$. Verificava-se analogamente a

relação $\mathcal{T} = \mathcal{T}e$. O elemento e, como unidade direita e esquerda, é elemento u.

Terminaremos o § com o seguinte

Teorema:- Se um idempotente $e \in \mathcal{T}$ pode decompôr-se numa soma de idempotentes e_i ortogonais dois a dois, os diferentes e_i pertencem a $e\mathcal{T}e$. Pondo $e = e_1 + \ldots + e_n$, tem-se por ex.,

$$e\, e_1 = e_1 , \quad e_1 e = e_1 , \quad e\, e_1 e = e_1 , \quad \text{q. e. d.}$$

2) Primeiras propriedades dos aneis semi-primários - Diz-se que um anel $\mathcal{T}$ é semi-primário, se tem radical $\mathcal{K}^*$ e se $\mathcal{T}'$ é semi-simples.

Como num anel semi-simples há idempotente primitivo e idempotente especial, o mesmo sucede em $\mathcal{T}$. Para as decomposições de Peirce relativas a um idempotente especial e, vale o

Teorema:- Os ideais $\mathcal{A}$ e $\mathcal{L}$ estão contidos no radical. Consideremos $\mathcal{L}$, por ex.. Em $\mathcal{T} \sim \mathcal{T}'$ corresponde-lhe $\mathcal{L}'$. Visto que $\mathcal{L}$ não tem idempotente, o mesmo sucede em $\mathcal{L}'$. Será $\mathcal{L}' = (0)$ e ter-se-à $\mathcal{L} \subseteq \mathcal{K}^*$.

Corolário:- Em $\mathcal{T}'$ há apenas o idempotente especial u'. Se e fôr um idempotente especial qualquer de $\mathcal{T}$, tem-se $s = es + (s - es)$, com $s - es \in \mathcal{L}$. Os correspondentes em $\mathcal{T}'$ dão $s' = e's'$, e, portanto, $e' = u'$. É um resultado conhecido.

Teorema:- Um elemento primitivo de $\mathcal{T}$ determina um ideal regular mínimo. No anel semi-simples $\mathcal{T}'$, um idempotente primitivo e_1' determina, com efeito, um ideal mínimo $e_1'\mathcal{T}'$. O teorema resulta agora duma proposição demonstrada no § 4 do Cap. I.

Corolário:- Todo o ideal regular $\mathcal{K}$, de $\mathcal{T}$, tem um ideal regular mínimo. Basta passar ao ideal correspondente $\mathcal{K}'$, de $\mathcal{T}'$, e tomar nele um ideal mínimo não nulo $e_1'\mathcal{T}'$. O ideal $e_1\mathcal{T}$, com $e_1 \in \mathcal{K}$, está nas condições exigidas.

Em $\mathcal{T}$ é válida a propriedade P, como se viu no § anterior. Podemos também afirmar que há sempre um idempotente espe-

pecial que é soma de idempotentes primitivos ortogonais. A êste respeito, enuncia-se o

Teorema:- O número de idempotentes primitivos ortogonais em que pode decompôr-se um idempotente especial é um invariante. Dado um idempotente especial e, para o qual $e = e_1+\ldots+e_n$ é uma decomposição como a referida no teorema, tem-se $\mathfrak{r}' = e_1'\mathfrak{r}' + \ldots + e_n'\mathfrak{r}'$. Os ideais $e_i'\mathfrak{r}'$ são mínimos. O seu número é bem determinado.

3) Estrutura dos anéis semi-primários - Tomemos um idempotente especial e, susceptível de ser decompôsto em idempotentes primitivos ortogonais: $e = e_1+\ldots+e_n$. Ponhamos $\mathfrak{L} = e_1\mathfrak{r}' + \ldots + e_n\mathfrak{r}' = e\mathfrak{r}'$, $\mathfrak{r}' = \mathfrak{L} + \mathfrak{L} = e\mathfrak{r}' + \mathfrak{L}$. Podemos enunciar o seguinte

Teorema:- Um anel semi-primário $\mathfrak{r}'$ é soma dum número finito de ideais regulares mínimos e dum nilideal. Na demonstração, supôs-se que os e_i eram ortogonais. Essa hipótese garante o seguinte

Aditamento:- O número de ideais regulares da soma é bem determinado.

Do exposto, resulta que um anel semi-primário verifica as duas condições seguintes:

A) todo o ideal regular tem um ideal regular mínimo;

B) uma cadeia de ideais regulares mínimos $e_2\mathfrak{r}' \subset e_1\mathfrak{r}' + e_2\mathfrak{r}' \subset \ldots$, onde $e_i e_k = 0$, é finita. Basta mesmo supôr que $i < k$. Então, com efeito, duma soma directa $e_1\mathfrak{r}'+\ldots+e_n\mathfrak{r}'$ passa-se ainda a uma soma directa correspondente em $\mathfrak{r}'$.

Caracterizando um anel semi-primário $\mathfrak{r}'$ como sendo aquele para o qual são válidas A) e B), com $i < k$, vamos provar, seguindo Kothe, que $\mathfrak{r}'$ tem radical $\mathfrak{K}^*$ e que $\mathfrak{r}'/\mathfrak{K}^*$ é semi-simples. Seja $\mathfrak{r}' \supset (0)$. Como a soma de dois nilideais direitos é um nilideal direito, $\mathfrak{K}^*$ existe. Sob o ponto de vista em que nos temos colocado, $\mathfrak{r}'$ não é nilideal. Será $\mathfrak{r}' \supset \mathfrak{K}^*$.

Teorema:- Um anel semi-primário $\mathfrak{r}'$ é soma directa de ideais regulares mínimos indecomponíveis e dum nilideal $\mathfrak{s}'$:

$$\mathfrak{r}' = \mathfrak{k}_1' + \ldots + \mathfrak{k}_n' + \mathfrak{s}' . \qquad (1)$$

Tomemos, em $\mathfrak{r}'$, um ideal regular mínimo $\mathfrak{k}_1' = e_1\mathfrak{r}'$ e escrevamos $\mathfrak{r}' = \mathfrak{k}_1' + \mathfrak{r}_1'$. Se $\mathfrak{r}_1'$ é nilideal, o teorema está demonstrado. No caso contrário, tomemos em $\mathfrak{r}_1'$ um ideal direito regular mínimo $\mathfrak{k}_2' = e_2\mathfrak{r}'$ e ponhamos

$$\mathfrak{r}' = \mathfrak{k}_2' + \mathfrak{r}_1' , \quad \mathfrak{r}_1' = \mathfrak{k}_2' + \mathfrak{r}_2' , \quad \mathfrak{r}' = \mathfrak{k}_1' + \mathfrak{k}_2' + \mathfrak{r}_2' .$$

Sabemos que se tem $e_1 e_2 = 0$. Se $\mathfrak{r}_2'$ é nilideal, o teorema está demonstrado. De contrário, o processo continua. Êle é limitado, a cadeia $\mathfrak{k}_1' \subset \mathfrak{k}_1' + \mathfrak{k}_2' \subset \mathfrak{k}_1' + \mathfrak{k}_2' + \mathfrak{k}_3' \subset \ldots$ é finita. Depois de n operações chega-se, pois, a $\mathfrak{r}' = \mathfrak{k}_1' + \ldots + \mathfrak{k}_n' + \mathfrak{s}'$, com $\mathfrak{s}'$ = nilideal. É claro que cada $\mathfrak{k}_i'$ é indecomponível, visto que uma soma de dois nilideais direitos não poderia levar a $\mathfrak{k}_i'$ e uma soma em que interviesse um ideal direito regular contrariaria a hipótese de $\mathfrak{k}_i'$ ser regular mínimo.

Teorema:- O anel factor $\mathfrak{r}'$ é semi-simples. Tem-se, de facto, pondo $\mathfrak{k}_i^* = (\mathfrak{k}_i', \mathfrak{K}^*)$,

$$\mathfrak{r}' = \mathfrak{k}_1^*/\mathfrak{K}^* + \ldots + \mathfrak{k}_n^*/\mathfrak{K}^* , \qquad (2)$$

onde as parcelas são ideais simples.[1] Observemos que é

$$\mathfrak{k}^*/\mathfrak{K}^* \cong \mathfrak{k}'/[\mathfrak{k}', \mathfrak{K}^*].$$

Ora $[\mathfrak{k}_1', \mathfrak{K}^*]$ é o nilideal direito máximo contido em $\mathfrak{k}_1'$. Se o último grupo factor não é simples, há um ideal entre $\mathfrak{k}_1'$ e $[\mathfrak{k}_1', \mathfrak{K}^*]$, que não será nilideal, o que contraria o facto de $\mathfrak{k}_1'$ ser ideal regular mínimo. Assim, $\mathfrak{k}_1^*/\mathfrak{K}^*$ é simples. $\mathfrak{r}'$, conforme (2), é soma de ideais direitos simples. Trata-se dum anel com condição dupla de cadeia, que também não tem nilideal, o que estabelece o teorema.

(1) É um resultado conhecido, aqui demonstrado doutra maneira.

Caracterizando por A) e B), com $i < k$, os aneis semi-primários, pode, pois, enunciar-se o

Teorema fundamental:- É condição necessária e suficiente, para que $\mathfrak{r}$ seja semi-primário, que haja radical $\mathfrak{K}^*$ e que $\mathfrak{r}/\mathfrak{K}^*$ seja semi-simples.

Demonstraremos agora a proposição a seguir.

Teorema:- Um anel semi-primário $\mathfrak{r}$ sem nilideal direito é semi-simples. Em primeiro lugar, $\mathfrak{r}$ é uma soma directa de ideais direitos simples não nilpotentes. Para se provar que existe elemento u, comecemos por observar que a decomposição $\mathfrak{r} = e_1\mathfrak{r} + \ldots + e_n\mathfrak{r}$ define um elemento $u' = e_1 + \ldots + e_n$ que é uma unidade esquerda. A decomposição de Peirce, $\mathfrak{r} = \mathfrak{r}u' + \mathfrak{A}$, com $\mathfrak{A}u' = (0)$, $u'\mathfrak{A} = \mathfrak{A}$, mostra ter-se $\mathfrak{A}^2 = \mathfrak{A}$. $u'\mathfrak{A} = \mathfrak{A}u' \cdot \mathfrak{A} = (0)$. Daqui tira-se $\mathfrak{A} = (0)$, visto que, não havendo ideal direito nilpotente também não pode haver ideal esquerdo nilpotente. Será $u' = u$. Mais simplesmente é $\mathfrak{r} \cong \mathfrak{r}/\mathfrak{K}^*$.

Teorema:- O anel $e\mathfrak{r}e = \mathfrak{r}_1$ duma decomposição de Peirce é semi-primário, se $\mathfrak{r}$ é semi-primário. Sabemos que $\mathfrak{r}_1$ tem o radical $e\mathfrak{K}^*e = \mathfrak{K}_1^*$. Também sabemos que a condição dupla de cadeia se transporta de $\mathfrak{r}/\mathfrak{K}^*$ para $\mathfrak{r}_1/\mathfrak{K}_1^*$. Como êste último não tem nilideal, é semi-simples, o que demonstra o teorema.

Corolário:- Um anel semi-primário $\mathfrak{r}$ é soma directa dum anel semi-primário $\mathfrak{r}_1$, com elemento um, e dum módulo $\mathfrak{M}_1$ contido no radical. O radical $\mathfrak{K}^*$ é soma directa de $\mathfrak{M}_1$ e do radical de $\mathfrak{r}_1$. De facto, basta tomar, em $\mathfrak{r}$, um idempotente especial e e escrever

$$\mathfrak{r} = e\mathfrak{r}e + (e\mathfrak{A} + \mathfrak{B}e + \mathfrak{J}). \qquad (3)$$

A parcela entre parêntesis é $\mathfrak{M}_1$. A primeira parcela é $\mathfrak{r}_1$. Se $r \in \mathfrak{K}^*$, pondo $r = ere + m_1$, $m_1 \in \mathfrak{M}_1$, reconhece-se a afirmação relativa ao radical.

Um caso interessante é aquele para o qual, em (3), se tem $e\mathfrak{A} = (0)$. Verifica-se, então, que $\mathfrak{r}_1$ é um ideal direito de $\mathfrak{r}$ e que todo o ideal direito de $\mathfrak{r}_1$ é ideal direito de $\mathfrak{r}$. Feita a decomposição de $\mathfrak{r}_1$ em ideais regulares mínimos com idempotentes ortogonais, fica feita a decomposição de $\mathfrak{r}$. É $\mathfrak{M}_1 = \mathfrak{B}$. Realizam-se estas condições se existe, por ex., uma unidade direita e.

4) Aneis completamente primários - Diz-se anel completamente primário um anel $\mathfrak{r}$ com elemento u tal que todo o ideal $\mathfrak{k} \neq \mathfrak{r}$ é nilideal.

Teorema:- $\mathfrak{r}$ tem radical $\mathfrak{K}^*$ e $\mathfrak{r}/\mathfrak{K}^*$ é um corpo. Tomemos com efeito, dois nilideais $\mathfrak{k}_1$ e $\mathfrak{k}_2$. A soma $(\mathfrak{k}_1, \mathfrak{k}_2)$ será nilideal, visto que, se o não fôsse, seria igual a $\mathfrak{r}$. E isto não pode dar-se, pelo facto de a soma de dois nilideais direitos não poder conter elemento idempotente. Posto isto, estudemos o homomorfismo $\mathfrak{r} \sim \mathfrak{r}/\mathfrak{K}^* = \mathfrak{r}'$. Dado $\mathfrak{k}' \neq (0)$, o ideal $\mathfrak{k}$ que lhe corresponde conterá $\mathfrak{K}^*$. Como nêste último estão contidos todos os nilideais unilaterais, é $\mathfrak{k} = \mathfrak{r}$. O anel $\mathfrak{r}'$, por conseqüência, que tem elemento um, só tem os ideais direitos nulo e unidade. É um corpo, como se deseja.

A proposição anterior admite inversa. Vamos provar o

Teorema:- Se um anel $\mathfrak{r}$ com elemento u tem radical $\mathfrak{K}^*$ e $\mathfrak{r}/\mathfrak{K}^*$ é um corpo, $\mathfrak{r}$ é completamente primário. O homomorfismo $\mathfrak{r} \sim \mathfrak{r}'$ faz corresponder a $\mathfrak{k}'$ o ideal $\mathfrak{k} \supset \mathfrak{K}^*$, só podendo ter-se $\mathfrak{k} = \mathfrak{K}^*$ ou $\mathfrak{k} = \mathfrak{r}$. Se $\mathfrak{k}_1$ é um ideal de $\mathfrak{r}$ diferente do radical ou do anel, tem-se $(\mathfrak{k}_1, \mathfrak{K}^*) = \mathfrak{K}^*$, pois que $(\mathfrak{k}_1, \mathfrak{K}^*) = \mathfrak{r}$ daria $\mathfrak{k}_1 = \mathfrak{r}$, (Cap.I, § 2). Daqui se conclui a afirmação.

Teorema:- Um anel completamente primário apenas tem o idempotente principal. Na verdade, se o idempotente e_1 pertence a $\mathfrak{r}$, deverá ter-se $e_1\mathfrak{r} = \mathfrak{r}$, $e_1 s = u$, com $s \in \mathfrak{r}$. Assim, é $e_1^2 s = e_1 s = u = e_1$.

Pode enunciar-se o seguinte inverso:

Teorema:- Um anel semi-primário que apenas tem o elemento um como idempotente é completamente primário. Se $\mathfrak{k} \subset \mathfrak{r}$ fôr um ideal direito, é nilideal, visto que, se o não fôsse, teria idempotente $= u$ e seria $\mathfrak{k} = \mathfrak{r}$.

Teorema:- O anel dos endomorfismos dum ideal regular mínimo, $\mathfrak{k} = e\mathfrak{r}$, dum anel $\mathfrak{r}$ com radical $\mathfrak{K}^*$, é completamente primário.

O anel dos endomorfismos é isomorfo de $e\mathfrak{J}e$[1]. Êste anel tem radical e elemento um. Um seu ideal $\mathfrak{k}' \neq e\mathfrak{J}e$ é nilideal, como vamos vêr. Se $a' \in \mathfrak{k}'$ fôsse regular,[2] $a'\mathfrak{J}$ seria regular e teria lugar $a'\mathfrak{J} = \mathfrak{k}$. Em particular, poderia escrever-se $a't=e$, e, portanto, como $a'e = a'$, seria $a'ete = e$. O ideal $\mathfrak{k}'$ conteria e e seria igual a $e\mathfrak{J}e$, contra a hipótese.

Pode chamar-se incidentalmente a atenção para o facto seguinte: se dois idempotentes e e e' geram o mesmo ideal direito, os aneis $e\mathfrak{J}e$ e $e'\mathfrak{J}e'$ são isomorfos.

5) Aneis primários - Diz-se anel primário um anel $\mathfrak{J}$ com elemento u tal que todo o ideal bilateral $\mathfrak{a} \neq \mathfrak{J}$ é nilideal.

Teorema:- $\mathfrak{J}$ tem radical $\mathfrak{R}^*$ e $\mathfrak{J}^1$ é um anel simples.

Para demonstrarmos que $\mathfrak{R}^*$ existe, provaremos que todo o nilideal direito $\mathfrak{k}$, de $\mathfrak{J}$, está contido num nilideal bilateral. Dado $\mathfrak{k}$, tomemos o ideal bilateral que êle gera: $\mathfrak{a} = (\mathfrak{k}, \mathfrak{J}\mathfrak{k})$. Vamos vêr que $\mathfrak{a}$ é nilideal. Com r, r', r'', ..., afectados ou não de índices, significaremos elementos de $\mathfrak{k}$; as outras letras serão elementos de $\mathfrak{J}$. Se $\mathfrak{a}$ não fôsse nilideal, ter-se-ia $\mathfrak{J}\mathfrak{k} = \mathfrak{J}$ e existiria uma igualdade $\sum s_i r_{r_i} = u$. Pondo $\sum_1 s_i r_i = a$, $s_1 r_1 = b$, a relação $a = u - b$ mostraria que a teria inverso direito v. Escrevendo $\sum_1 s_i r_i v = \sum_1 s_i r_i' = u$, vêr-se-ia, anàlogamente, que $\sum_1 s_i r_i'$ teria inverso direito. O processo levaria a concluir-se que um elemento nilpotente teria um inverso direito, o que é absurdo. A demonstração de que $\mathfrak{J}^1$ apenas tem os ideais bilaterais nulo e unidade faz-se estudando o homomorfismo $\mathfrak{J} \sim \mathfrak{J}^1$. Podemos também enunciar o

Teorema:- Se um anel com elemento u tem radical $\mathfrak{R}^*$ e $\mathfrak{J}^1$ é simples, $\mathfrak{J}$ é primário.

Uma outra afirmação é a seguinte:

Teorema:- Se $\mathfrak{a}$ é um ideal bilateral do anel primário $\mathfrak{J}$, o anel $\mathfrak{J}/\mathfrak{a} = \mathfrak{J}''$ é primário e tem o radical $\mathfrak{R}^*/\mathfrak{a} = \mathfrak{R}''^*$. Tomemos o ideal bilateral $\mathfrak{a}' \neq \mathfrak{J}''$ e seja $\mathfrak{b} \supset \mathfrak{a}$ o ideal bilateral de $\mathfrak{J}$ tal que $\mathfrak{a}' = \mathfrak{b}/\mathfrak{a}$. É necessàriamente $\mathfrak{b} \neq \mathfrak{J}$. $\mathfrak{b}$ é nilideal e $\mathfrak{a}'$ é também nilideal. $\mathfrak{J}''$ tem elemento u' e tem radical $\mathfrak{R}''^*$. No raciocínio anterior supõe-se, é claro, $\mathfrak{a} \neq \mathfrak{J}$. Então é $\mathfrak{a} \subseteq \mathfrak{R}^*$, $\mathfrak{b} \subseteq \mathfrak{R}^*$, e tem-se $\mathfrak{R}''^* = \mathfrak{R}^*/\mathfrak{a}$, visto que êste último nilideal bilateral contém $\mathfrak{a}'$.

(1) Êste resultado não exige que $\mathfrak{J}$ tenha elemento um. No § 7 do Cap.I não se torna necessário que haja elemento um para concluir $\rho_i \in \mathfrak{J}_{ij}$.

(2) Significa "não nilpotente".

Postas estas considerações, vamos vêr que é possível prosseguir no estudo da estrutura dos aneis primários admitindo que êles são semi-primários. Em primeiro lugar, a decomposição (1) do § 3 não introduz o nilideal $\mathfrak{k}$, visto existir elemento um. Será

$$\mathfrak{J} = e_1\mathfrak{J} + \ldots + e_n\mathfrak{J}. \qquad (4)$$

O ideal bilateral $\mathfrak{J}e_k\mathfrak{J}$ não é nilideal, tendo-se $\mathfrak{J}e_k\mathfrak{J} = \mathfrak{J}$. Se pusermos $e_i\mathfrak{J}e_k = \mathfrak{J}_{ik}$, são válidas as igualdades $\mathfrak{J}_{ik}\mathfrak{J}_{kj} = \mathfrak{J}_{ij}$. Podemos, mesmo, afirmar o

Teorema:- Cada $\mathfrak{J}_{ik}$ possui um elemento regular x_{ik}, ou seja um elemento verificando a condição $x_{ik}\mathfrak{J}_{ki} = \mathfrak{J}_{ii}$. Na verdade, tem-se $x_{ik}\mathfrak{J}_{ki} \subseteq \mathfrak{J}_{ii}$. Sendo, porém, $x_{ik}\mathfrak{J}_{ki}\mathfrak{J}_{ii} = x_{ik}\mathfrak{J}_{ki}$, vê-se que $x_{ik}\mathfrak{J}_{ki}$ é ideal direito de $\mathfrak{J}_{ii}$. O sinal $\subset$ não pode subsistir para todos os x_{ik}, como vamos vêr. O anel $\mathfrak{J}_{ii}$ tem como nilideal bilateral máximo o seu ideal $e_i\mathfrak{R}^*e_i$ e é um anel completamente primário. Para se concluir esta última afirmação, basta ter em conta que $e_i\mathfrak{J}e_i$ é semi-primário e que e_i é primitivo. Uma outra demonstração dêste facto é a seguinte. Tem-se

$$e_i\mathfrak{J}e_i / e_i\mathfrak{R}^*e_i = e_i\mathfrak{J}e_i / [e_i\mathfrak{J}e_i, \mathfrak{R}^*] \cong (e_i\mathfrak{J}e_i, \mathfrak{R}^*)/\mathfrak{R}^*,$$

de modo que há necessidade de verificar, por ex., a solubilidade da equação

$$(e_i a e_i + \mathfrak{R}^*)(e_i x e_i + \mathfrak{R}^*) = e_i b e_i + \mathfrak{R}^*,$$

onde se supõe $e_i a e_i \notin \mathfrak{R}^*$ (ou $\notin e_i\mathfrak{R}^*e_i$). Na correspondência $\mathfrak{J} \sim \mathfrak{J}/\mathfrak{R}^*$, ao ideal regular mínimo $e_i\mathfrak{J}$ corresponde o ideal simples $e_i\mathfrak{J}^1$. Supondo $e_ia'e_i \neq 0$, tem-se $e_ia'e_i.e_i\mathfrak{J}^1 = e_i\mathfrak{J}^1$. Dado e_ib', existe x' tal que $e_ia'e_i.e_ix' = e_ib'$, e, por conseqüência, é, como se quere, $e_ia'e_i.e_ix'e_i = e_ib'e_i$.

Posto isto, regressemos ao teorema proposto. Sempre que subsistir o sinal $\subset$ em $x_{iR}\mathfrak{J}_{Ri} \subset \mathfrak{J}_{ii}$, o ideal $x_{iR}\mathfrak{J}_{Ri}$ é nilideal direito de $\mathfrak{J}_{ii}$ e tem-se $x_{iR}\mathfrak{J}_{Ri} \equiv e_i \mathcal{R}^* e_i$. Se, com todos os x_{iR}, se obtivessem nilideais, $\mathfrak{J}_{ii} = \mathfrak{J}_{iR}\mathfrak{J}_{Ri}$ seria nilanel de $\mathfrak{J}$, o que é absurdo. O teorema enunciado é, pois, válido. Quando x_{iR} é um elemento regular, tem-se, assim,

$$x_{iR}\mathfrak{J}_{Ri} = \mathfrak{J}_{ii}\,, \qquad x_{iR}\mathfrak{J}_{Rj} = \mathfrak{J}_{ij}\,.$$

Ponhamos $e_i\mathfrak{J} = \mathfrak{K}_i$, $\mathfrak{J}e_i = \mathfrak{N}_i$. É

$$e_i\mathfrak{J}\cdot\mathfrak{J}e_R = e_i\mathfrak{J}e_R = \mathfrak{J}_{iR} = \mathfrak{K}_i\,\mathfrak{N}_R\,.$$

Vamos vêr que um elemento regular x_{iR} verifica a relação $x_{iR}\mathfrak{K}_R = \mathfrak{K}_i$. O ideal $x_{iR}\mathfrak{K}_R$ está contido em $\mathfrak{K}_i$, pois $x_{iR} \in \mathfrak{K}_i$. Ora é

$$x_{iR}\mathfrak{K}_R \supseteq x_{iR}\mathfrak{K}_R\,\mathfrak{J} \supseteq x_{iR}\mathfrak{K}_R\,\mathfrak{N}_i = \mathfrak{J}_{ii}\,.$$

Isto significa que o nosso ideal contém um elemento idempotente, não podendo ser $x_{iR}\mathfrak{K}_R \subset \mathfrak{K}_i$, visto que $\mathfrak{K}_i$ é regular mínimo.

Teorema:- Na decomposição (4) as diferentes parcelas são operatòriamente isomorfas. É o que resulta do facto de $\mathfrak{J}'$ ser simples e semi-simples, conforme se viu no § 4 do Cap.I.

A proposição fundamental relativa a aneis primários constitui o seguinte

Teorema:- Um anel primário $\mathfrak{J}$ tem uma base de n^2 matrizes unidades, reduzindo-se a um módulo finito com respeito a um anel $\mathcal{O}$, completamente primário. Se $\mathfrak{J}$ é completamente primário, o teorema está demonstrado. No caso contrário, u, como nos aneis semi-simples, é soma dos elementos primitivos e_i, que se anulam dois a dois. Ponhamos $e_i = e_{ii}$. Em seguida, em cada $\mathfrak{J}_{ii}$, tomemos um elemento regular e_{i1}. Visto que $e_{i1}\mathfrak{J}_{ii} = \mathfrak{J}_{i1}$, tomemos em $\mathfrak{J}_{1i}$ o elemento e_{1i} tal que $e_{i1}\,e_{1i} = e_{ii}$. É claro que os elementos e_{1i} também são regulares, pois $e_{1i}\,\mathfrak{J}_{iR} = e_{1i}\mathfrak{J}_{ii}\,\mathfrak{J}_{iR} = \mathfrak{J}_{1i}\,\mathfrak{J}_{iR} = \mathfrak{J}_{1R}$. Interessam-nos, depois, os produtos $e_{1i}\,e_{i1}$. Tem-se

$$(e_{1i}\,e_{i1})^2 = e_{1i}\,e_{i1}\,e_{1i}\,e_{i1} = e_{1i}\,e_{i1}\,,$$

o que mostra ser $e_{1i}\,e_{i1}$ um idempotente de $\mathfrak{J}_{1i}$. Como a relação $e_{1i}\,e_{i1} = 0$ arrastaria $e_{1i}\,e_{i1}\,\mathfrak{J}_{1i} = e_{1i}\,\mathfrak{J}_{ii} = (0)$, que não pode ter lugar, visto ser, por ex., $e_{1i}\,e_{i1} = e_{11} \neq 0$, segue-se que deverá ter-se $e_{1i}\,e_{i1} = e_{11}$. Para prosseguirmos na construção das matrizes, poremos, por definição, $e_{iR} = e_{i1}\,e_{1R}$. Vê-se imediatamente que $e_{iR} \neq 0$. De facto

$$e_{iR}\,e_{Ri} = e_{i1}\,e_{1R}\,e_{R1}\,e_{1i} = e_{i1}\,e_{11}\,e_{1i} = e_{i1}\,e_{1i} = e_{ii}\,.$$

Em seguida tem-se $e_{iR}\,e_{Rj} = e_{ij}$. Chegámos, assim, a introduzir n elementos que são, na verdade, matrizes unidades: $e_{iR}\,e_{Rj} = \delta_{Rj}\,e_{ij}$. O estudo que fizemos no § 9 do Cap.I diz-nos que $\mathfrak{J}$ é um módulo relativamente a um anel $\mathcal{O}$ isomorfo de $\mathfrak{J}_{11}$, q. e. d.

Tem também lugar a proposição inversa seguinte:

Teorema:- Um anel completo, $\mathfrak{J}$, de matrizes formadas com elementos dum anel completamente primário, $\mathcal{O}$, é um anel primário, se $\mathfrak{J}$ tem radical. O anel $\mathfrak{J}$, com efeito, é um anel com elemento u e com n^2 matrizes unidades, nos têrmos do § 9, Cap.I (Aplicação). Se $\mathfrak{M}$ é o anel que comuta com tôdas as matrizes e_{iR}, sabemos ser $\mathfrak{M} = \mathcal{O}u \cong e_1\mathfrak{J}e_{11}$ e que o radical de $\mathfrak{M}$ é $[\mathfrak{M}, \mathcal{R}^*]$. Também sabemos que é $\mathfrak{J}' = \mathfrak{J}/\mathcal{R}^*$ um anel com elementos de $\mathcal{O}' = (\mathcal{O}u, \mathcal{R}^*)/\mathcal{R}^* \cong \mathcal{O}u/[\mathcal{O}u, \mathcal{R}^*]$. A demonstração do teorema reduz-se agora a provar que êste último anel factor é um corpo. Ora isso é imediato, porque $\mathcal{O}u \cong \mathcal{O}$ é completamente primário.

Nêste § demonstraremos ainda duas proposições.

Teorema:- Os ideais de duas decomposições (4) são operatòriamente isomorfos. Passando ao anel factor $\mathfrak{J}'$, as duas decomposições levam a duas decomposições de $\mathfrak{J}'$ em ideais regulares mínimos isomorfos. Os ideais das decomposições (4) serão, pois, isomorfos (Cap.I, § 4).

Teorema:- O número n é um invariante da decomposição (4) e as n matrizes relativas a duas decomposições resultam umas das outras por um automorfismo interno. O mesmo automorfismo

leva do anel completamente primário $\mathcal{O}$ duma decomposição ao anel $\mathcal{O}'$ da segunda. Sabemos que n é, realmente, um invariante. Admitamos a existência dum segundo sistema de matrizes f_{ik} e ponhamos $u = f_1 + \dots + f_n$, com $f_i = f_{ii}$. Fazendo $e_{ii}\mathfrak{J} = \mathfrak{k}_i$, $f_{ii}\mathfrak{J} = \mathfrak{r}_i$, sabemos que os ideais direitos regulares mínimos $\mathfrak{k}_i$ e $\mathfrak{r}_i$ são isomorfos. Estudemos, por ex., $\mathfrak{k}_1 \cong \mathfrak{r}_1$. Tem-se

$$e_{11} = e_1 \longrightarrow \alpha \in \mathfrak{r}_1, \qquad \alpha\,\mathfrak{k}_1 = \mathfrak{r}_1 ,$$

$$a = e_1 a \longrightarrow \alpha a = f_1 \in \mathfrak{r}_1 , \qquad a \in \mathfrak{k}_1, \qquad a\,\mathfrak{r}_1 = \mathfrak{k}_1 ,$$

pois $\alpha\,\mathfrak{k}_1$ e $a\,\mathfrak{r}_1$ são ideais regulares, visto que

$$\alpha a = f_1 , \qquad a\alpha \longrightarrow f_1\alpha = \alpha , \qquad a\alpha = e_1 .$$

Os elementos

$$x = \sum_i e_{i1}\, a\, f_{1i} , \qquad y = \sum_j f_{j1}\, \alpha\, e_{1j}$$

verificam as relações $xy = u$, $yx = u$; pelo que é $y = x^{-1}$. E é

$$x^{-1} e_{ik}\, x = f_{i1}\alpha\, e_{1k}\, e_{k1}\, a\, f_{1k} = f_{i1}\, f_{11}\, f_{1k} = f_{ik}.$$

O anel $\mathcal{O}'$, composto de todos os elementos de $\mathfrak{J}$ que comutam com as matrizes f_{ik} é isomorfo de $f_1\mathfrak{J}f_1$, e, portanto, completamente primário. A demonstração termina, como no § 4 do Cap. anterior, verificando que é

$$x^{-1}\mathcal{O}x = \mathcal{O}' .$$

6) Continuação do estudo dos anéis semi-primários – Todos os teoremas dados no Cap. I, § 4, àcêrca de ideais regulares mínimos de $\mathfrak{J}$ e de ideais mínimos idempotentes de $\mathfrak{J}'$ são válidos aqui.

Regressemos ao estudo da decomposição

$$\mathfrak{J} = e_1\mathfrak{J} + \dots + e_n\mathfrak{J} + \mathfrak{P} , \qquad (5)$$

dada no comêço do § 3. Tem ainda lugar, se fôr $e_i\mathfrak{J} \cong e_k\mathfrak{J}$, o

Teorema:- Cada $\mathfrak{J}_{ik} = e_i\mathfrak{J}e_k$ possui um elemento regular x_{ik} tal que $x_{ik}\mathfrak{J}_{ki} = \mathfrak{J}_{ii} = e_i\mathfrak{J}e_i$. Na verdade, tem-se $x_{ik}\mathfrak{J}_{ki} \subseteq \mathfrak{J}_{ii}$. Como $\mathfrak{k}_k = e_k\mathfrak{J}$ e $\mathfrak{k}_i = e_i\mathfrak{J}$ são isomorfos, vale $e_k\mathfrak{J}\cdot e_i\mathfrak{J} = \mathfrak{k}_k\mathfrak{k}_i = \mathfrak{k}_k = e_k\mathfrak{J}$, de modo que $x_{ik}\mathfrak{J}_{ki}\,\mathfrak{J}_{ii} = x_{ik}\mathfrak{J}_{ki}$, e êste último é ideal direito de $\mathfrak{J}_{ii}$. O sinal $\subset$ não pode subsistir para todos os x_{ik}, como vai vêr-se. O anel $\mathfrak{J}_{ii}$ é semi-primário, e, como e_i é primitivo, é completamente primário. A demonstração continua como para os aneis primários, pois é também aqui

$$\mathfrak{J}_{ik}\mathfrak{J}_{ki} = \mathfrak{k}_i\, e_k\mathfrak{J}e_i = \mathfrak{k}_i\,\mathfrak{k}_k e_i = \mathfrak{k}_i\, e_i = e_i\,\mathfrak{J}e_i = \mathfrak{J}_{ii} .$$

Suponhamos que os t primeiros ideais regulares mínimos da decomposição (5) são isomorfos, não havendo outros isomorfos dêles. Fazendo $i,k = 1,2,\dots,t$, podemos, como no caso dos anéis primários (§ anterior), construir t^2 matrizes unidades e_{ik}, as quais estão contidas no anel $f_1\mathfrak{J}$, com $f_1 = e_1 + \dots + e_t$. O idempotente f_1 é simplesmente unidade esquerda de $f_1\mathfrak{J}$.

Quando se faz a decomposição de Peirce relativa ao elemento f_1 :

$$\mathfrak{J} = f_1\mathfrak{J} + \mathfrak{P}_1 = (f_1\mathfrak{J}f_1 + f_1\mathcal{O}_1) + \mathfrak{P}_1 ,$$

tem-se $f_1\mathfrak{J} = e_1\mathfrak{J} + \dots + e_t\mathfrak{J} = f_1\mathfrak{J}f_1 + f_1\mathcal{O}_1$. Fàcilmente se reconhece que as matrizes e_{ik}, assim como os $\mathfrak{J}_{ik}$, pertencem a $f_1\mathfrak{J}f_1$. Por ex.:

$$f_1 e_{ik}\, f_1 = e_{ik} , \qquad \mathfrak{J}_{ik} = f_1\mathfrak{J}_{ik}f_1 .$$

De resto, pelo que respeita aos e_{ii}, foi êste resultado estabelecido já no § 1 dêste Capítulo. O anel $f_1 \mathcal{Y} f_1$ tem radical $f_1 \mathcal{K}^* f_1$ e é anel de matrizes com elementos dum anel $\mathcal{W}$ nêle contido e isomorfo dum anel completamente primário. Como se viu no § anterior, $f_1 \mathcal{Y} f_1$ é primário. A parcela $f_1 \mathcal{O}_1$, de $f_1 \mathcal{Y}$, está contida no radical $\mathcal{K}^*$, como se verifica tendo em conta ser f_1' elemento um de $f_1' \mathcal{Y}'$, pelo facto dêste último ser anel simples com elemento um, parcela da decomposição do anel semi-simples $\mathcal{Y}'$ em anéis simples. Procedendo em (5) com tôdas as classes de ideais regulares mínimos operatòriamente isomorfos como acaba de fazer-se com uma delas, chega-se a

$$\mathcal{Y} = f_1 \mathcal{Y} f_1 + \ldots + f_p \mathcal{Y} f_p + (f_1 \mathcal{O}_1 + \ldots + f_p \mathcal{O}_p) + \mathcal{G}.$$

Daqui o seguinte

Teorema:- Um anel semi-primário $\mathcal{Y}$ é soma dum número finito de anéis primários $f_i \mathcal{Y} f_i$ e dum módulo $\mathcal{M}$ contido no radical. O radical $\mathcal{K}^*$ é soma directa de $\mathcal{M}$ e dos radicais $f_i \mathcal{K}^* f_i$.

Para se reconhecer a afirmação relativa ao radical, escrevamos, se $r \in \mathcal{K}^*$,

$$r = f_1 s_1 f_1 + \ldots + f_p s_p f_p + m \ , \quad (m \in \mathcal{M} = f_1 \mathcal{O}_1 + \ldots + f_p \mathcal{O}_p + \mathcal{G}).$$

Tem-se

$$f_i r f_i = f_i s_i f_i + f_i m f_i \ , \quad f_i s_i f_i = f_i (r-m) f_i \ , \quad r = \sum f_i (r-m) f_i + m,$$

como se deseja. Incidentalmente, podemos fazer as duas observações seguintes: 1ª) não apenas para os elementos do radical, mas para qualquer $s \in \mathcal{Y}$ se tem $s = \sum f_i (s - r) f_i + m$, $(r \in \mathcal{K}^*)$; 2ª) o aniquilador esquerdo $\mathcal{O}_l$ de $e = f_1 + \ldots + f_p$, é dado por $\mathcal{O}_l = [\mathcal{O}_{l_1}, \ldots, \mathcal{O}_{l_p}]$.

Para terminarmos as considerações dêste §, digamos ainda que podemos substituir as condições A) e B), características de anel semi-primário, pelas duas condições seguintes: α) cada ideal regular tem um idempotente primitivo que gera um ideal regular mínimo; β) existe idempotente especial decomponível em idempotentes primitivos ortogonais.
A verificação é fácil de fazer.

7) Estudo de algumas circunstâncias particulares - Se em $\mathcal{Y}$ existe u, designemos com e um idempotente especial qualquer e ponhamos

$$\mathcal{Y} = e \mathcal{Y} + \mathcal{G} \ , \qquad u = e + (u - e) \ .$$

Como $u - e$ pertence ao radical, escrevendo $e = u - r$, $r \in \mathcal{K}^*$, vê-se que e tem inverso. Isto significa $e\mathcal{Y} = \mathcal{Y}$, $\mathcal{G} = (0)$, $u = e$. Daqui (conforme já se viu de modo mais geral) o

Teorema:- Num anel semi-primário com elemento u, apenas existe êste idempotente especial, o qual pode decompôr-se em elementos primitivos ortogonais. Supõe-se, bem entendido, que o anel não é completamente primário.
Dêste enunciado resulta que, num anel semi-primário, um idempotente não primitivo é soma de idempotentes ortogonais. Podemos precisar. Seja e um idempotente qualquer de $\mathcal{Y}$. Escrevendo $\mathcal{Y} = e \mathcal{Y} e + e\mathcal{O}_l + \mathcal{G}$, no anel semi-primário $e \mathcal{Y} e$, supondo e não primitivo em $\mathcal{Y}$, tem-se $e = e_1 + \ldots + e_n$, onde os $e_i \in e\mathcal{Y}e$ são ortogonais e primitivos nêste último e em $\mathcal{Y}$. Pode enunciar-se o

Teorema:- Num anel semi-primário, todo o idempotente não primitivo é soma de idempotentes primitivos ortogonais.

Seja e um idempotente especial de $\mathcal{Y}$. Pelo facto de ser $\mathcal{Y} = e \mathcal{Y} + \mathcal{G}$, $\mathcal{G} \subseteq \mathcal{K}^*$, sabemos que $e\mathcal{Y}$ tem o radical $[e\mathcal{Y}, \mathcal{K}^*]$, (Cap.I, § 3). É, de resto, $\mathcal{K}^* = \mathcal{G} + [e\mathcal{Y}, \mathcal{K}^*]$. A relação de isomorfismo

$$(e\mathcal{Y}, \mathcal{K}^*)/\mathcal{K}^* = \mathcal{Y}/\mathcal{K}^* \cong e\mathcal{Y}/[e\mathcal{Y}, \mathcal{K}^*]$$

prova que $e\mathcal{Y}$ é semi-primário. O mesmo se diz de $\mathcal{Y}e$. Pode escrever-se

$$\mathcal{Y} = e \mathcal{Y} + \mathcal{G} = e \mathcal{Y} e + e\mathcal{O}_l + \mathcal{G} \ ,$$

$$\mathcal{K}^* = [e\mathcal{Y}, \mathcal{K}^*] + \mathcal{G} = [e \mathcal{Y} e, \mathcal{K}^*] + e\mathcal{O}_l + \mathcal{G} = e\mathcal{K}^* e + e\mathcal{O}_l + \mathcal{G} \ .$$

Fixaremos, assim, o

Teorema:- Se e é um idempotente especial dum anel semi-primário $\mathcal{R}$, e $\mathcal{R}$ é um anel semi-primário (assim como $\mathcal{R}e$). Podemos dizer, mais geralmente ainda:

Teorema:- Se o anel semi-primário $\mathcal{R} = (\mathcal{R}_1, \mathcal{R}_1)$ é soma dum seu sub-anel $\mathcal{R}_1$ e dum módulo $\mathcal{R}_1$ contido no radical, $\mathcal{R}_1$ é semi-primário.

Suponhamos agora o caso especial de $\mathcal{R}$ ser um anel com condição de mínimo para ideais regulares. Um tal anel é semi-primário, porque a soma de dois nilideais direitos é um nil-ideal direito e porque a correspondência $\mathcal{R} \sim \mathcal{R}'$ mostra ter lugar em $\mathcal{R}'$ a condição de mínimo. Consideremos, então, a cadeia de ideais regulares direitos

$$\mathcal{R} \supseteq \mathcal{R}^2 \supseteq \mathcal{R}^3 \supseteq \dots$$

e ponhamos $\mathcal{R}^k = \mathcal{R}^{k+1}$. Se e é um idempotente especial de $\mathcal{R}$, $e^k = e$ é um idempotente especial de $\mathcal{R}^k$. Escrevamos as decomposições correspondentes

$$\mathcal{R} = e\mathcal{R}e + e\mathcal{A} + \mathcal{L}e + \mathcal{J}, \qquad \mathcal{R}^k = e\mathcal{R}^k e + e\mathfrak{a} + \mathfrak{b}e + \mathfrak{i}.$$

Tem-se

$$e\mathcal{R}^k e = e\mathcal{R}.\mathcal{R}^{k-1}e = e\mathcal{R}e,$$

$$e\mathcal{A} = e^k\mathcal{A} = e.e^{k-1}\mathcal{A}, \quad e^{k-1}\mathcal{A} \subseteq \mathcal{R}^k, \quad e^{k-1}\mathcal{A} \subseteq \mathfrak{a},$$

$$e\mathcal{A} = e\mathfrak{a}, \quad \mathcal{L}e = \mathfrak{b}e, \quad \mathcal{R} = (\mathcal{R}^k, \mathcal{J}).$$

O teorema anterior garante ser $\mathcal{R}^k$ um anel semi-primário. Podemos enunciar o seguinte

Teorema:- Um anel com condição de mínimo para ideais regulares é soma dum anel semi-primário idempotente e dum sub-anel contido no radical.

No caso de $\mathcal{R}^k$ ter elemento um = U, não pode haver um idempotente especial $e \neq U$ no anel $\mathcal{R}$, visto que os idempotentes dos dois anéis são os mesmos e da mesma natureza. Valerá a igualdade $\mathcal{R} = \mathcal{R}^k + \mathcal{J}$, pois $e\mathcal{R}e = e\mathcal{R}^k e = \mathcal{R}^k$, $e\mathfrak{a} = \mathfrak{b}e = \mathfrak{i} = (0)$.

Dissemos já que a condição de mínimo para ideais regulares é suficiente para garantir ser $\mathcal{R}$ um anel semi-primário (ou anel-A generalizado).(1) Uma condição necessária e suficiente é dada pelo

Teorema:- É condição necessária e suficiente, para que $\mathcal{R}$ seja um anel - A generalizado, que $\mathcal{K}^*$ exista e tenha lugar a condição de mínimo para ideais direitos contendo $\mathcal{K}^*$.

Seria obtida uma classe mais restrita de anéis semi-primários (anéis - A), se êstes fôssem definidos pela condição de $\mathcal{R}/\mathcal{K}^{**}$ ser semi-simples. De facto, existiria $\mathcal{K}^* = \mathcal{K}^{**}$ e $\mathcal{R}/\mathcal{K}^*$ seria semi-simples. Pode enunciar-se um teorema análogo ao anterior:

Teorema:- É condição necessária e suficiente, para que $\mathcal{R}$ seja um anel - A, que tenha lugar a condição de mínimo para ideais direitos contendo $\mathcal{K}^{**}$.

Finalmente, mais restrita ainda seria a classe dos anéis semi-primários, se êstes se definissem pela condição de $\mathcal{R}/\mathcal{K}$ ser semi-simples. De facto, existiria $\mathcal{K}^* = \mathcal{K}^{**} = \mathcal{K}$ e $\mathcal{R}/\mathcal{K}^*$ seria semi-simples. Como, em geral, $\mathcal{R}/\mathcal{K}$ tem ainda ideais nilpotentes, é natural, na definição de anel - A (especial), exigir que $\mathcal{K}$ seja nilpotente. Dessa maneira $\mathcal{R}/\mathcal{K}$ não terá radical. A proposição a enunciar, correspondente aos dois teoremas anteriores, é, então, a mesma:

Teorema:- É condição necessária e suficiente, para que $\mathcal{R}$ seja um anel - A especial, que tenha lugar a condição de mínimo para ideais direitos contendo $\mathcal{K}$. Em seguida é válido o seguinte

Teorema:- É condição necessária e suficiente, para que $\mathcal{R}/\mathcal{K}$ seja semi-simples e $\mathcal{K}$ seja nilpotente, que tenha lugar

(1) J. Levitzki, "On the radical of a general ring", atrás citado.

a condição de mínimo para ideais direitos contendo $\mathcal{R}$ e que seja finita tôda a cadeia descendente de ideais bilaterais contidos em $\mathcal{R}$ da forma $\mathcal{L}_0 \supset \mathcal{L}_0\mathcal{L}_1 \supset \ldots$[1]. A demonstração é imediata, se se tiverem em conta resultados estabelecidos no Cap. I, § 3.

8) Nota sôbre anéis completamente primários e primários - Entre as definições especiais de Artin (veja-se o final do tomo I) e as definições generalizadas de Köthe (dadas atrás), há lugar para definições intermediárias. Um anel completamente primário $\mathcal{T}$ é um anel com elemento u tal que cada $\mathcal{K} \neq \mathcal{T}$ é semi-nilpotente, ou um anel com elemento u tal que $\mathcal{T}/\mathcal{K}^{**}$ é um corpo. Um anel primário é um anel $\mathcal{T}$ com elemento u tal que cada ideal bilateral $\mathcal{A} \neq \mathcal{T}$ é semi-nilpotente ou um anel com elemento u tal que $\mathcal{T}/\mathcal{K}^{**}$ é simples e semi-simples.

Teorema:- Se $\mathcal{T}/\mathcal{K}^{**}$ é semi-simples, cada ideal $\mathcal{K}$ não semi-nilpotente do anel semi-primário $\mathcal{T}$ tem idempotente. Na verdade, $\mathcal{K}^{*}$ existe e é igual a $\mathcal{K}^{**}$. Todo o nilideal é semi-nilpotente, de modo que, por hipótese, todo o ideal não semi-nilpotente é regular. O teorema é conhecido.

Corolário:- Um anel semi-primário (anel - A) que apenas tem o idempotente principal é completamente primário.

Teorema:- É condição necessária e suficiente, para que um anel $\mathcal{T}$ seja primário, que seja um anel completo de matrizes com elementos dum anel completamente primário. Que a condição é necessária, resulta, como no teorema de Köthe, do facto de se tratar dum anel de matrizes quadradas com elementos dum anel $\mathcal{O}$ isomorfo de $e_1\mathcal{T}e_1$ (e_1 primitivo) e de $e_1\mathcal{T}e_1 / e_1\mathcal{K}^{**}e_1$ ser um corpo. Esta última afirmação prova-se assim[2]: a condição dupla de cadeia transporta-se de $\mathcal{T}/\mathcal{K}^{**}$ para $e_1\mathcal{T}e_1 / e_1\mathcal{K}^{**}e_1$ e êste último não tem ideal nilpotente, pelo que é semi-simples; dêste modo, $e_1\mathcal{T}e_1$ é semi-primário, e, como não tem idempotente diferente de e_1, é completamente primário. Que a condição é suficiente, mostra-se ainda como no caso mais geral anterior, aplicando os mesmos teoremas, que são realmente válidos.

(1) J. Levitzki, "A characteristic condition for semi-primary rings", atrás citado.
(2) Bastaria notar que é $\mathcal{K}^{*} = \mathcal{K}^{**}$.

Capítulo IV

Aneis com condição de mínimo

1) Módulos com respeito a aneis - Se bem que o conteúdo dêste § pudesse ser reduzido a um mínimo indispensável, a importância do assunto obriga-nos a ser mais extensos do que se tornaria necessário[1]

Sejam o módulo $\mathcal{M} = \{\theta, \alpha, \beta, \tau, \ldots\}$ e o anel operatório $\mathcal{T} = \{u, a, b, c, \ldots\}$. Nada nos permite afirmar que o elemento u seja operador unitário do módulo, isto é, que se tenha $\alpha u = \alpha$. Escrevendo $\alpha = (\alpha - \alpha u) + \alpha u$, cada elemento de $\mathcal{M}$ pode considerar-se como soma de dois, o primeiro dos quais, $\beta = \alpha - \alpha u$, satisfaz à condição $\beta a = 0$, qualquer que seja $a \in \mathcal{T}$, e o segundo, $\tau = \alpha u$, admite u como operador unitário. O conjunto dos elementos β constitui um sub-módulo admissível $\mathcal{M}'$, o conjunto dos τ um sub-módulo admissível $\mathcal{M}''$, valendo a igualdade $\mathcal{M} = \mathcal{M}' + \mathcal{M}''$, como se verifica fàcilmente.

Suponhamos que $\mathcal{M}$ é um módulo finito relativo a $\mathcal{T}$. Isto significa, como se sabe, que existem elementos $m_1, \ldots, m_n$, de $\mathcal{T}$, tais que qualquer $m \in \mathcal{M}$ se pode escrever sob a forma

$$m = m_1 a_1 + \ldots + m_n a_n + i_1 m_1 + \ldots + i_n m_n ,$$

onde $a_i \in \mathcal{T}$ e i_k é inteiro.

Procuremos, nêste caso, o sub-módulo $\mathcal{M}'$. Os seus elementos são da forma

$$m_1 a_1 + \ldots + m_n a_n + i_1 m_1 + \ldots + i_n m_n - (m_1 a_1 + \ldots + i_1 m_1 + \ldots) u =$$

$$= i_1 m_1 + \ldots + i_n m_n - (i_1 m_1 + \ldots + i_n m_n) u . \qquad (1)$$

Os elementos de $\mathcal{M}''$ são da forma

(1) Veja-se Almeida Costa, "Sôbre os grupos abelianos" e "Grupos abelianos e Aneis...", já citados.

$$(m_1a_1+\ldots+ m_na_n)\ u + (i_1m_1+\ldots+ i_nm_n)\ u\ =$$

$$= m_1(a_1+ i_1u) +\ldots+ m_n(a_n+ i_nu)\ =$$

$$= m_1b_1+\ldots+ m_nb_n\ ,\quad (b_i\in \mathfrak{Y})\ , \qquad (2)$$

verificando-se que u é operador unitário.

Quando se diz, pois, que o módulo $\mathfrak{M}$ é formado por elementos do tipo (2), o carácter unitário do operador u tem de ser concebido. Os elementos $m_1,\ldots, m_n$ não têm a forma (2) não pertencendo a $\mathfrak{M}$. Os geradores são os elementos $m_1u,\ldots, m_nu$, geralmente representados por $m_1,\ldots, m_n$.

Sempre que uma relação da forma

$$m_1a_1+\ldots+ m_na_n = 0$$

apenas tem lugar se $a_1 = \cdots = a_n = 0$, os elementos m_l dizem-se independentes. O seu número é a ordem ou dimensionalidade de $\mathfrak{M}$.

O estudo de módulos com respeito a corpos é fácil de fazer, no caso de haver uma ordem.(1)

Num módulo finito $\mathfrak{M}$ relativamente a um anel, diz-se que tem lugar a condição de base, quando é válida a propriedade de ser um módulo finito relativamente ao anel cada sub-módulo de $\mathfrak{M}$. Pode enunciar-se o seguinte

Teorema:- É necessário e basta, para que um módulo finito $\mathfrak{M}$ relativo a um anel $\mathfrak{Y}$ goze da propriedade da cadeia ascendente para os sub-módulos admissíveis, que tenha lugar a condição de base para os referidos sub-módulos. A condição é necessária, porque, se a propriedade da cadeia ascendente tem lugar, tomemos um sub-módulo $\mathfrak{M}'$; se $a'\in\mathfrak{M}'$ é um elemento que não gera $\mathfrak{M}'$, tomemos um segundo elemento $a''\in\mathfrak{M}'$, que não esteja em (a') = módulo gerado por a'. Se (a',a'') = módulo gerado por a'

(1) Veja-se Almeida Costa, "Elementos da Teoria dos Aneis", pgs. 170 e seguintes.

e a'' não é $\mathfrak{M}'$, prossegue-se o raciocínio, de modo a construir a cadeia

$$(a') \subset (a',a'') \subset (a',a'',a''') \subset \ldots\ .$$

Por hipótese, esta cadeia não é infinita, de sorte que tem de chegar-se a $(a',a'',\ldots, a^{(n)}) = \mathfrak{M}'$. Inversamente, se a condição de base tem lugar, não pode haver uma cadeia infinita de sub-módulos de $\mathfrak{M}$, visto que o conjunto unido de todos os módulos da cadeia seria um sub-módulo sem uma base finita.

O anel do § 2 do Cap. I não goza da propriedade da condição de base, quando se considera como um módulo relativamente a si mesmo. Não vale nele, por conseqüência, a condição de máximo. A condição de mínimo tambem não é válida nêsse anel, como se vê considerando a cadeia descendente infinita

$$(r_1) \supset (r_1r_2r_3) \supset (r_1r_2r_3r_4r_5) \supset \ldots\ .$$

Designaremos por anel - O direito um anel com condição de máximo para ideais direitos. Um anel com condição de mínimo designar-se-à também por anel - U direito.

São teoremas importantes da teoria dos módulos os que vão seguir-se.

Teorema:- Se $\mathfrak{Y}$ é um anel com condição de base para ideais direitos, um módulo finito $\mathfrak{M}$ relativo a $\mathfrak{Y}$ é um módulo com condição de base. Seja $\mathfrak{N}$ um sub-módulo de $\mathfrak{M}$. Para se exprimirem os elementos de $\mathfrak{N}$ podem ser ou não necessários todos oe elementos $u_1, u_2, \ldots, u_N$, da base de $\mathfrak{M}$. Suponhamos carecer dos primeiros $r \leqq N$, de sorte que cada elemento de $\mathfrak{N}$ é da forma

$$n = u_1s_1+\ldots+ u_rs_r+ n_1u_1+\ldots+ n_ru_r\ .$$

O conjunto dos inteiros n_r, que figuram nas expressões dos nn, constitui um ideal (i_r) = grupo cíclico do anel I dos números inteiros. Se considerarmos o elemento de $\mathfrak{N}$,

$$P_r = u_1 t_{r_1} + \ldots + u_r t_{r_r} + D_{r_1} u_1 + \ldots + i_r u_r$$

e pusermos $n_r = k\, i_r$, tem-se

$$n - k\, P_r = u_1 S_1 + \ldots + u_r S_r + N_1 u_1 + \ldots + N_{r-1}\, u_{r-1} ,$$

onde o segundo membro pertence a $\mathfrak{M}$. O conjunto dos segundos membros constitui um sub-módulo admissível, $\mathfrak{M}_1$, de $\mathfrak{M}$, e o conjunto dos N_{r-1} constitui um ideal (i_{r-1}) = grupo cíclico do anel dos números inteiros. Introduzindo o elemento de N_1,

$$P_{r-1} = u_1 t_{r-1,1} + \ldots + u_r t_{r-1,r} + D_{r-1} u_1 + \ldots + i_{r-1} u_{r-1} ,$$

e prosseguindo, chega a estabelecer-se que os elementos de $\mathfrak{M}$ se exprimem como soma de dois elementos: um da forma $n' = u_1 S_1 + \ldots + u_r S_r$, $(S_j \in \mathfrak{O})$, outro pertencente ao módulo gerado por P_r, $P_{r-1}, \ldots, P_1$. Os elementos $\underline{n}'$ pertencem a $\mathfrak{M}$, onde definem outro sub-módulo admissível $\mathfrak{M}'$. Se encontrarmos uma base para $\mathfrak{M}'$, só temos que juntar aos elementos dessa base os os elementos P. Ora o conjunto dos S_r, que figuram nas expressões dos $\underline{n}'$, constitui um ideal direito $\mathfrak{k}$, de $\mathfrak{O}$. Se se tiver

$$\mathfrak{k} = (\sigma_r^1, \ldots, \sigma_r^\alpha) ,$$

tomemos os elementos seguintes de $\mathfrak{M}'$:

$$N_r^\mu = u_1 T_1^\mu + \ldots + u_{r-1} T_{r-1}^\mu + u_r\, \sigma_r^\mu , \quad (\mu = 1, \ldots, \alpha) .$$

Os elementos de $\mathfrak{M}'$ podem escrever-se como soma de dois elementos: um pertencente ao módulo gerado pelos N_r^μ, e o outro pertencente a um sub-módulo $\mathfrak{M}''$, de $\mathfrak{M}$, cujos elementos $\underline{n}''$ se exprimem em $u_1, \ldots, u_{r-1}$. Repetindo o processo sôbre

$$n'' = u_1 T_1 + \ldots + u_{r-1} T_{r-1} ,$$

e prosseguindo, chega-se, finalmente, a um sub-módulo de $\mathfrak{M}$, cujos

elementos se exprimem à custa de elementos da forma $u_1 r'$, com $r' \in \mathfrak{O}$, êstes últimos figurando também na base procurada.

Se $\mathfrak{O}$ tem elemento um, operador unitário do módulo, não comparecem na base os elementos P_j.

Posto isto, seja $\mathfrak{M}$ um módulo finito relativamente a um anel semi-simples $\mathfrak{O}$. Podemos supôr $\mathfrak{M}$ reduzido à sua parte para a qual $\underline{u}$ é operador unitário. O teorema anterior garante que continua a ser módulo finito. Vamos demonstrar o seguinte

Teorema:- $\mathfrak{M}$ é completamente redutível e cada sub-módulo simples é operatòriamente isomorfo dum ideal direito simples de $\mathfrak{O}$.

Por hipótese, tem-se

$$\mathfrak{M} = (m_1 \mathfrak{O}, \ldots, m_n \mathfrak{O}) , \quad \mathfrak{O} = \mathfrak{k}_1 + \ldots + \mathfrak{k}_t ,$$

e, conseqüentemente,

$$\mathfrak{M} = (\ldots, m_l \mathfrak{k}_k, \ldots) . \qquad (3)$$

Ora, estudando a correspondência $\mathfrak{k}_k \longrightarrow m_l \mathfrak{k}_k$, vê-se imediatamente que é um homomorfismo operatório, no qual $\mathfrak{O}$ se considera operando à direita. Se $f_k \in \mathfrak{k}_k$ é diferente do elemento nulo, não pode ser $m_l f_k = 0$, pois, se assim fôsse, ter-se-ia $m_l \mathfrak{k}_k = (0)$, visto que $f_k \mathfrak{O} = \mathfrak{k}_k$, $m_l \mathfrak{k}_k = m_l f_k \mathfrak{O} = (0)$. Deixando de parte, em (3), as parcelas nulas, a correspondência em causa é um isomorfismo. O sub-módulo $m_l \mathfrak{k}_k$, de $\mathfrak{M}$, é um sub-módulo admissível simples. Consideremos, em (3), o sub-módulo admissível constituido pela soma das parcelas que antecedem $m_l \mathfrak{k}_k$. A sua intersecção com $m_l \mathfrak{k}_k$ só pode ser o sub-módulo nulo ou o próprio $m_l \mathfrak{k}_k$. Excluindo da soma (3) as parcelas contidas na soma das parcelas anteriores, obtem-se $\mathfrak{M}$ sob a forma de soma directa, nos termos do teorema.

A última proposição que vamos demonstrar nêste § é a seguinte:

Teorema:- Um módulo $\mathfrak{M}$ relativo a um anel semi-simples $\mathfrak{O}$, se nele tiver lugar a condição de mínimo para os seus sub-

-módulos admissíveis, e se $u \in \mathfrak{T}$ fôr operador unitário, é completamente redutível. Escrevamos $\mathfrak{T} = e_1\mathfrak{T} + \ldots + e_n\mathfrak{T}$, sob a forma de soma de ideais direitos simples, e tomemos $m \in \mathfrak{M}$ diferente de zero. Será $m\mathfrak{T} \neq (0)$, e, portanto, existe um sub-módulo $m\,e_i\mathfrak{T} \neq (0)$. Para êsse sub-módulo, tem-se $m\,e_i = m_1 \neq 0$. Se $m_1\mathfrak{T} \neq \mathfrak{M}$, tomemos $m' \in \mathfrak{M}$, mas tal que $m' \notin m_1\mathfrak{T}$. Existirá um sub-módulo $m'e_k\mathfrak{T} \neq (0)$, com $m'e_k \neq 0$. Poremos $m'e_k = m_2$ e consideraremos a soma $m_1\mathfrak{T} + m_2\mathfrak{T}$, que é directa, pelo facto de cada parcela ser **módulo-simples**. Basta ter em conta, com efeito, que $m_1\mathfrak{T} = m\,e_i\mathfrak{T} \cong e_i\mathfrak{T}$. Proseguindo o raciocínio, forma-se uma cadeia

$$m_1\mathfrak{T} \subset m_1\mathfrak{T} + m_2\mathfrak{T} \subset m_1\mathfrak{T} + m_2\mathfrak{T} + m_3\mathfrak{T} \subset \ldots ,$$

que é finita pela razão seguinte. Se fôsse infinita, pondo

$$m_1\mathfrak{T} + m_2\mathfrak{T} + \ldots = \mathfrak{M}_1 , \quad m_2\mathfrak{T} + \ldots = \mathfrak{M}_2 , \ldots ,$$

seria também infinita a cadeia

$$\mathfrak{M}_1 \supset \mathfrak{M}_2 \supset \ldots ,$$

contra a hipótese. Chega-se, assim, a uma soma

$$m_1\mathfrak{T} + \ldots + m_n\mathfrak{T} ,$$

a qual contém todos os elementos de $\mathfrak{M}$, como se deseja.

2) A condição de mínimo - Embora o objectivo principal dêste Capítulo seja o estudo dos aneis $\mathfrak{T}$ com condição de mínimo para ideais direitos (ou aneis - U direitos), vamos nêste momento coordenar certos resultados já assinalados anteriormente, que respeitam principalmente à nilpotência do radical $\mathfrak{K}$. São sucessivamente mais fracas as condições seguintes:

I) a condição de mínimo para os ideais direitos de $\mathfrak{T}$;

II) a condição de mínimo para os ideais bilaterais de $\mathfrak{T}$ e condição de mínimo para os ideais direitos de $\mathfrak{T}/\mathfrak{F}$, em que $\mathfrak{F}$

é um ideal primo arbitrário de $\mathfrak{T}$ (§ 5 deste Capítulo);

III) a condição de mínimo para os ideais bilaterais de $\mathfrak{T}$;

IV) a condição de mínimo para os nilideais bilaterais de $\mathfrak{T}$;

V) a condição de mínimo para os ideais bilaterais semi-nilpotentes;

VI) a condição de mínimo para os ideais bilaterais de $\mathfrak{T}$ contidos em $\mathfrak{K}$.

Em todos êstes casos, o radical $\mathfrak{K}$ é nilpotente. No caso VI), com efeito, é finita tôda a cadeia de ideais bilaterais $\mathfrak{L}_i$, de $\mathfrak{T}$, contidos em $\mathfrak{K}$, da forma $\mathfrak{L}_0 \supset \mathfrak{L}_0\mathfrak{L}_1 \supset \ldots$ (Levitzki). Nos casos I - V, pode demonstrar-se que o radical $\mathfrak{K}^{**}$ é nilpotente e que coincide, portanto, com $\mathfrak{K}$ (Levitzki)[1]. A afirmação é conseqüência imediata da seguinte proposição relativa a V:

Teorema:- Se num anel $\mathfrak{T}$ é válida a condição de mínimo para os ideais bilaterais semi-nilpotentes, $\mathfrak{K}^{**}$ é nilpotente (ou todo o ideal semi-nilpotente é nilpotente). Suponhamos $\mathfrak{K}^{**}$ não nilpotente. Entre os ideais bilaterais semi-nilpotentes que não são nilpotentes, escolhamos um ideal semi-nilpotente mínimo $\mathfrak{a}$. Tem-se $\mathfrak{a} = \mathfrak{a}^2 = \mathfrak{a}^3 = \ldots$, visto que não pode ser $\mathfrak{a}^2 \subset \mathfrak{a}$, pois isso mostraria que $\mathfrak{a}^2$ era nilpotente e $\mathfrak{a}$ seria nilpotente. Existe uma infinidade numerável $a_1, a_2, \ldots, a_n, \ldots$, de elementos de $\mathfrak{a}$, tais que o produto de qualquer número deles consecutivos é diferente de zero. Pondo $\mathfrak{a}\,a_{2+sk}\,\mathfrak{a} = \mathfrak{a}_k$, é $\mathfrak{a}_0\,\mathfrak{a}_1 \ldots \mathfrak{a}_q \neq (0)$, qualquer que seja r. Como a cadeia

$$\mathfrak{a}_0 \supset \mathfrak{a}_0\mathfrak{a}_1 \supset \ldots \supset \mathfrak{a}_0\mathfrak{a}_1 \ldots \mathfrak{a}_i \supset \ldots$$

é finita, suponhamos

$$\mathfrak{a}_0\,\mathfrak{a}_1 \ldots \mathfrak{a}_{q-1} = \mathfrak{L} = \mathfrak{L}\,\mathfrak{a}_q .$$

O ideal $\mathfrak{a}_q$ não pode ser nilpotente, de contrário ter-se-ia $\mathfrak{L} = (0)$. Como $\mathfrak{a}_q$ está contido em $\mathfrak{a}$, será $\mathfrak{a}_q = \mathfrak{a}$, em virtude da propriedade de mínimo dêste último.

(1) J. Levitzki, "Semi-nilpotente ideals", Duke Mathematical Journal, vol. 10, 1943, pgs. 553 - 556.

A relação

$$\mathfrak{a} = \mathfrak{a}\, a_{2+sq}\, \mathfrak{a} = \mathfrak{a}\, b\, \mathfrak{a} \ , \quad (b = a_{2+sq}) \ ,$$

vai levar-nos a um absurdo. Efectivamente, seja

$$b = \sum_l a_l b\, a'_l \ , \qquad (a_l, a'_l \in \mathfrak{a}) \ .$$

Tira-se daqui, sucessivamente:

$$a_j b\, a'_j = \sum_l a_j a_l b\, a'_l\, a'_j \ , \qquad b = \sum_j a_j b\, a'_j = \sum_{l,j} a_j a_l b\, a'_l\, a'_j \ ,$$

$$a_k a_m b\, a'_m\, a'_k = \sum_{l,j} a_k a_m a_j a_l b\, a'_l\, a'_j\, a'_m\, a'_k \ ,$$

$$b = \sum_{k,m} a_k a_m b\, a'_m\, a'_k = \sum_{l,j,k,m} a_k a_m a_j a_l b\, a'_l\, a'_j\, a'_m\, a'_k \ , \text{ etc.}$$

Conclui-se dêste modo que o anel gerado pelos elementos b, a_l, a'_l não pode ser nilpotente, pois $b \neq 0$ pode escrever-se sob a forma de soma de produtos daqueles elementos, cada produto ($\neq 0$) com um número de factores tão grande quanto se queira. O absurdo está em evidência, pelo facto de b, a_l, a'_l pertencerem a $\mathfrak{a}$, que é semi-nilpotente.

Corolário:- Um anel $\mathfrak{r}$ para o qual valem a condição de mínimo para os ideais $\mathfrak{K}$ contendo $\mathfrak{K}^{**}$ e a condição de mínimo para os ideais bilaterais semi-nilpotentes é um anel - A especial.

Nos casos I) e II), tem-se $\mathfrak{K}^* = \mathfrak{K}^{**} = \mathfrak{K}$. Deixaremos para o final do Capítulo a demonstração relativa a II) (Asano). Quanto a I), tem lugar o

Teorema:- Um anel - U direito é um anel - A especial. Com efeito, $\mathfrak{K}$ é nilpotente e em $\mathfrak{r}/\mathfrak{K}$ (que não tem radical) vale a condição de mínimo. Acrescente-se que $\mathfrak{r}/\mathfrak{K}$ não tem nil-ideal e que, portanto, $\mathfrak{K}^*$ existe e é $= \mathfrak{K}$. De resto, a existência de $\mathfrak{K}^*$ decorre imediatamente do facto de a soma de dois nilideais direitos ser um nilideal direito.

Hopkins[1] provou o teorema supra como conseqüência da demonstração que vai seguir-se.

Teorema:- Um anel com condição de mínimo para ideais direitos tem um radical $\mathfrak{K} = \mathfrak{K}^*$, que é nilpotente. A condição de mínimo garante a existência dum inteiro positivo k tal que $\mathfrak{K}^k = \mathfrak{K}^{k+1} = \ldots$. Vamos vêr que a hipótese $\mathfrak{K}^\rho \supset (0)$ arrasta a existência de elementos de $\mathfrak{K}^\rho$ que não pertencem a $\mathfrak{K}^{\rho+1}$. O teorema resultará, então, imediatamente. Consideremos os elementos a de $\mathfrak{K}$ tais que $a\mathfrak{K}^\rho = (0)$. O seu conjunto constitui um ideal bilateral $\mathfrak{a}_\rho$, de $\mathfrak{r}$. Em $\mathfrak{K}$ tomemos um ideal direito mínimo não nulo $\mathfrak{k}$, de $\mathfrak{r}$. Valerá a relação $\mathfrak{k}\mathfrak{K}^\rho = (0)$, de sorte que é $\mathfrak{a}_\rho \neq (0)$. Se $\mathfrak{K}^{\rho+1} = (0)$, o resultado desejado é trivial. Se $\mathfrak{K}^{\rho+1} \supset (0)$, ponhamos $\mathfrak{a}_{\rho+1}\mathfrak{K}^{\rho+1} = (0)$. Um teorema demonstrado no Cap.I, § 3, continuando a designar com $\mathfrak{P}$ o ideal bilateral de $\mathfrak{r}$ contido em $\mathfrak{K}$ tal que $\mathfrak{P}^\nu \mathfrak{K}^\nu = (0)$, dá aqui, pondo $\mathfrak{P} = \mathfrak{a}_\rho$, para expressão do radical de $\mathfrak{r}/\mathfrak{a}_\rho$, o anel $\mathfrak{K}/\mathfrak{a}_\rho = \mathfrak{K}'$. No homomorfismo $\mathfrak{r} \sim \mathfrak{r}/\mathfrak{a}_\rho$, tem-se $\mathfrak{K} \to \mathfrak{K}' \supset (0)$. Se fôr $\mathfrak{n}' \supset (0)$ o ideal bilateral de $\mathfrak{r}'$, contido em $\mathfrak{K}'$, tal que $\mathfrak{n}'\mathfrak{K}' = (0)$, e se $\mathfrak{n} \to \mathfrak{n}'$, o ideal $\mathfrak{n} \supset \mathfrak{a}_\rho$, de $\mathfrak{r}$, satisfaz a

$$\mathfrak{n} \subseteq \mathfrak{K} \ , \quad \mathfrak{n}\mathfrak{K} \subseteq \mathfrak{a}_\rho \ , \quad \mathfrak{n}\mathfrak{K}^{\rho+1} = (0) \ .$$

Conclui-se daqui $\mathfrak{n} \subseteq \mathfrak{a}_{\rho+1}$, $\mathfrak{a}_{\rho+1} \supset \mathfrak{a}_\rho$, $\mathfrak{K}^\rho \supset \mathfrak{K}^{\rho+1}$, como se quere. Podemos precisar que é $\mathfrak{n} = \mathfrak{a}_{\rho+1}$. Tendo em conta as relações

$$\mathfrak{a}_{\rho+1} \subseteq \mathfrak{K}, \quad \mathfrak{a}_{\rho+1}\mathfrak{K}^{\rho+1} = \mathfrak{a}_{\rho+1}\mathfrak{K}.\mathfrak{K}^\rho = (0), \quad \mathfrak{a}_{\rho+1}\mathfrak{K} \subseteq \mathfrak{a}_\rho \ ,$$

vê-se que cada $x \in \mathfrak{a}_{\rho+1}$ tem, no homomorfismo em causa, um correspondente $x' \in \mathfrak{K}'$, para o qual $x'\mathfrak{K}' = (0)$. Será, portanto, $x' \in \mathfrak{n}'$, o que dá $x \in \mathfrak{n}$, ou seja $\mathfrak{n} = \mathfrak{a}_{\rho+1}$.

(1) C.Hopkins, "Nil-rings with minimal condition for admissible left ideals", Duke Mathematical Journal, vol 4, 1938, pgs. 664 a 667.

Do que acaba de dizer-se, podemos concluir que, se $\mathfrak{K}^k = (0)$, é $\mathfrak{K} \cdot \mathfrak{K}^{k-1} = (0)$, $\mathfrak{a}_{k-1} = \mathfrak{K}$.

Procuremos agora o aniquilador direito, $\mathfrak{b}_\rho$, de $\mathfrak{K}^\rho$, ou seja o conjunto dos elementos de $\mathfrak{K}$ tais que $\mathfrak{K}^\rho \mathfrak{b}_\rho = (0)$. Vê-se imediatamente que $\mathfrak{b}_\rho$ é um ideal bilateral. E, sendo $\mathfrak{K}^k = \mathfrak{K}^\rho \cdot \mathfrak{K}^{k-\rho} = (0)$, conclui-se que $\mathfrak{K}^{k-\rho} \subseteq \mathfrak{b}_\rho$, $\mathfrak{b}_\rho \subseteq \mathfrak{b}_{\rho+1}$, podendo precisar-se que $\mathfrak{b}_\rho \subset \mathfrak{b}_{\rho+1}$, pelo facto de $\mathfrak{b}_{\rho+1}$ conter $\mathfrak{K}^{k-\rho-1}$, mas ser $\mathfrak{K}^\rho \cdot \mathfrak{K}^{k-\rho-1} = \mathfrak{K}^{k-1} \supset (0)$, e, portanto, $\mathfrak{K}^{k-\rho-1} \notin \mathfrak{b}_\rho$. Nestas condições é $\mathfrak{b}_{k-1} = \mathfrak{K}$.

Aos aneis -U podem estender-se certos resultados de Levitzki, expostos no Cap.II. Assim, tratando de sub-nilaneis é válido o

Teorema:- Todo o sub-nilanel $\mathfrak{J}_1$, dum anel com condição de mínimo[1], é nilpotente. No homomorfismo $\mathfrak{J} \sim \mathfrak{J}/\mathfrak{K}$, seja $\mathfrak{J}_1'$ o correspondente de $\mathfrak{J}_1$. $\mathfrak{J}_1'$ é nilpotente, como sub-nilanel dum anel com condição dupla de cadeia. Pondo $\mathfrak{J}_1'^r = (0)$, vê-se que $\mathfrak{J}_1^r \subseteq \mathfrak{K}$, e $\mathfrak{J}_1^{rk} \subseteq \mathfrak{K}^k = (0)$. O teorema está demonstrado.

Teorema:- Um anel -U direito $\mathfrak{J}$ que tenha um elemento não divisor de zero possui elemento um. Seja $a \in \mathfrak{J}$ um elemento não divisor de zero. Por hipótese, a cadeia $\mathfrak{J} \supseteq a\mathfrak{J} \supseteq a^2\mathfrak{J} \supseteq \cdots$ é limitada. Supondo $a^k\mathfrak{J} = a^{k+1}\mathfrak{J}$, vale, para cada $x \in \mathfrak{J}$, $a^k x = a^{k+1} y$, ou seja $x = ay$. Se fôr agora $a = au$, tem-se $a(x - ux) = 0$, $x = ux$, o que mostra ser u uma unidade esquerda. Escrevendo, em seguida,

$$(x - xu)a = xa - x.ua = xa - xa = 0 ,$$

vê-se que é $x = xu$, o que demonstra a afirmação.

(1) Quando se falar em anel com condição de mínimo, sem nada especificar, subentender-se-á "condição de mínimo para ideais direitos".

Corolário:- Um anel -U direito sem divisores de zero é um corpo. Dado $a \neq 0$, sabemos, com efeito, que a equação $ax = b$ é solúvel em $\mathfrak{J}$, qualquer que seja b. Em particalar, suponhamos $at = u$. Vê-se que é $t \neq 0$, e, por conseqüência,

$$(ta - u)t = tat - t = 0 , \qquad ta = u .$$

A equação $ya = b$ é também solúvel, para o que basta pôr $y = bt$.

Teorema:- Um anel -U que tenha uma unidade direita é um anel -O[1] Provaremos o teorema mostrando que a série normal $\{\mathfrak{J} \supset \mathfrak{K} \supset \cdots \supset \mathfrak{K}^k = (0)\}$ se pode dilatar e tornar numa série de composição de $\mathfrak{J}$ (para ideais direitos). Estudemos a parte $\{\mathfrak{K}^\rho \supset \mathfrak{K}^{\rho+1}\}$. Comecemos por observar que $\mathfrak{K}^\rho$ é um grupo abeliano com o domínio operatório $\mathfrak{J}$, e que o mesmo sucede com o sub-grupo admissível $\mathfrak{K}^{\rho+1}$. Dêsse modo, $\Delta = \mathfrak{K}^\rho/\mathfrak{K}^{\rho+1}$ é um grupo abeliano com o domínio operatório $\mathfrak{J}$. Os sub-grupos admissíveis de $\mathfrak{K}^\rho$ são os ideais direitos que contém. Como a todo o sub-grupo de Δ corresponde um e um só de $\mathfrak{K}^\rho$ que contém $\mathfrak{K}^{\rho+1}$, o estudo dos sub-grupos de Δ é o estudo dos ideais direitos de $\mathfrak{J}$ contidos em $\mathfrak{K}^\rho$ que contêm $\mathfrak{K}^{\rho+1}$. Consideremos dois elementos $s, t \in \mathfrak{J}$, tais que $s - t \in \mathfrak{K}$. Tem-se, se $a_\rho \in \mathfrak{K}^\rho$,

$$(a_\rho + \mathfrak{K}^{\rho+1})s = a_\rho s + \mathfrak{K}^{\rho+1} , \quad (a_\rho + \mathfrak{K}^{\rho+1})t = a_\rho s + \mathfrak{K}^{\rho+1} .$$

Isto significa que podemos, no estudo de Δ, substituir o domínio operatório $\mathfrak{J}$ pelo domínio $\mathfrak{J}/\mathfrak{K}$. A unidade direita de $\mathfrak{J}$ (ou o elemento um de $\mathfrak{J}/\mathfrak{K}$) funciona de operador unitário. O último

(1) Conforme C.Hopkins, "Rings with minimal condition for left ideals", Annals of Mathematics, II series, vol.40, 1939, pgs.712 a 730, e K.Asano, "Uber Ringe mit Vielfachenkettensatz", Proceedings of the Imperial Academy, Tokyo, vol.XV, nº 9, 1939, pgs.288 a 291.

teorema do § anterior, tendo em conta que vale em Δ a condição de mínimo para os sub-módulos admissíveis, diz que Δ é completamente redutível. A uma série de composição

$$\left\{\mathfrak{K}^0/\mathfrak{K}^{\rho+1} \supset \mathfrak{k}_1/\mathfrak{K}^{\rho+1} \supset \ldots \supset \mathfrak{K}^{\rho+1}/\mathfrak{K}^{\rho+1} = (0)\right\}$$

corresponde uma série normal

$$\left\{\mathfrak{K}^0 \supset \mathfrak{k}_1 \supset \ldots \supset \mathfrak{K}^{\rho+1}\right\} .$$

Esta última, como a anterior, não pode ser dilatada, pelo que o teorema está demonstrado, tendo em conta que $\mathfrak{o}/\mathfrak{K}$ também possui série de composição.

3) Os ideais mínimos dum anel com condição de mínimo-Seja $\mathfrak{k}_1$ um ideal mínimo de $\mathfrak{o}$. Procuremos a soma $\mathfrak{M}_1$ de todos os ideais mínimos de $\mathfrak{o}$ isomorfos de $\mathfrak{k}_1$. Se $m_1 \in \mathfrak{M}_1$, m_1 pertence a uma soma Δ_1 dum número finito de tais ideais, e a essa mesma soma, e conseqüentemente a $\mathfrak{M}_1$, pertence $m_1 s$, com $s \in \mathfrak{o}$. A correspondência $\mathfrak{k}_1 \sim s\ \mathfrak{k}_1$ é um isomorfismo, salvo se $s\mathfrak{k}_1 = (0)$. Daqui se conclui que sm_1 pertence a uma soma do tipo Δ_1, e, portanto, a $\mathfrak{M}_1$. Esta última é, pois, um ideal bilateral. Seja $\mathfrak{k}_1$, $\mathfrak{k}_1'$, ... o conjunto dos ideais isomorfos de $\mathfrak{k}_1$. Suponhamos possível tirar dêsse conjunto uma infinidade numerável de ideais, de tal sorte que uma parte finita qualquer da soma dessa infinidade constitua uma soma directa. Escrevendo

$$\mathfrak{k}_1 + \mathfrak{k}_1' + \mathfrak{k}_1'' + \ldots \supset \mathfrak{k}_1' + \mathfrak{k}_1'' + \ldots \supset \mathfrak{k}_1'' + \ldots \supset \ldots ,$$

vê-se que se contradiz a condição de mínimo. Isto significa que $\mathfrak{M}_1$ é uma soma dum número finito de ideais isomorfos de $\mathfrak{k}_1$:

$$\mathfrak{M}_1 = \mathfrak{k}_1^{(1)} + \ldots + \mathfrak{k}_1^{(n)} . \qquad (4)$$

Designaremos com $\mathfrak{N}_1 \subseteq \mathfrak{M}_1$ a soma dos ideais isomorfos de $\mathfrak{k}_1$ de quadrado nulo, e poremos

$$\mathfrak{M}_1 = \mathfrak{L}_1 + \mathfrak{N}_1 , \qquad (5)$$

onde $\mathfrak{L}_1$ é uma parte dos ideais idempotentes que figuram em (4). Suponhamos $\mathfrak{L}_1 = e_1\mathfrak{o} + e_1'\mathfrak{o} + \ldots + e_1^{(k)}\mathfrak{o}$. Vamos vêr que os idempotentes $e_1, \ldots$ podem ser substituidos por outros, $E_1, \ldots$ de tal modo que sejam ortogonais dois a dois.

Ponhamos $\mathfrak{o} = e_1\mathfrak{o} + \mathfrak{L}_1$ (decomposição direita de Peirce) e $\mathfrak{L}_1 = e_1\mathfrak{o} + \mathfrak{b}_1$. Se o ideal direito $\mathfrak{b}_1$ é mínimo, será necessàriamente isomorfo de $e_1\mathfrak{o} = \mathfrak{k}_1$. Não pode então ter-se $\mathfrak{b}_1^2 = (0)$, pois $\mathfrak{b}_1$ pertenceria a $\mathfrak{N}_1$ e a soma (5) não seria directa. Designando com E_2' um idempotente de $\mathfrak{b}_1$, seria (com $e_1 = E_1$)

$$\mathfrak{L}_1 = E_1\mathfrak{o} + E_2'\mathfrak{o} , \qquad E_1 E_2' = 0 .$$

Pondo $E_2 = E_2' - E_2' E_1 \in \mathfrak{b}_1$, a soma $\mathfrak{L}_1 = E_1\mathfrak{o} + E_2\mathfrak{o}$, com $E_2^2 = E_2$ $E_1E_2 = E_2E_1 = 0$ estaria nas condições desejadas. Não sendo $\mathfrak{b}_1$ mínimo, tomaríamos um ideal mínimo contido em $\mathfrak{b}_1$, escolheríamos ainda E_2' pertencente a êsse ideal mínimo $\mathfrak{b}_1'$, poriamos

$$\mathfrak{o} = E_2'\mathfrak{o} + \mathfrak{L}_2 , \quad \mathfrak{b}_1 = E_2'\mathfrak{o} + \mathfrak{b}_2 , \quad E_2 = E_2' - E_2' E_1 ,$$

e teríamos em conta que seria $E_2'\mathfrak{o} = E_2\mathfrak{o}$. Viria, como se deseja,

$$\mathfrak{L}_1 = E_1\mathfrak{o} + E_2\mathfrak{o} + \mathfrak{b}_2 , \quad E_2^2 = E_2 , \quad E_1E_2 = E_2E_1 = 0.$$

Se $\mathfrak{b}_2$ fôsse mínimo, deveria tomar-se um idempotente $E_3' \in \mathfrak{b}_2$, e, em seguida, $E_3 = E_3' - E_3'(E_1 + E_2)$. Seria

$$E_1E_3' = 0 , \quad E_2' E_3' = 0 , \quad E_2E_3' = 0, \quad E_1E_3 = 0 , \quad E_2E_3 = 0,$$

$$E_3E_1 = 0 , \quad E_3E_2 = 0 , \quad E_3^2 = E_3 , \quad \mathfrak{L}_1 = E_1\mathfrak{o} + E_2\mathfrak{o} + E_3\mathfrak{o}.$$

Se $\mathfrak{b}_2$ não fôsse mínimo, o processo continuaria, até ser obtida a decomposição desejada de $\mathfrak{L}_1$. De futuro, suporemos que em

$$\mathcal{L}_1 = e_1\mathcal{J} + \ldots + e_1^{(k)}\mathcal{J}$$

os idempotentes $e_1^{(i)}$ verificam as condições de ortogonalidade. Poderá escrever-se simplesmente $\mathcal{L}_1 = E_1\mathcal{J}$, com $E_1 = e_1 + \ldots + e_1^{(k)}$.

Escrevendo

$$\mathcal{N}_1 = \mathcal{K}_1^{(i_1)} + \ldots + \mathcal{K}_1^{(i_\rho)},$$

vê-se imediatamente que é $\mathcal{N}_1^2 = (0)$. $\mathcal{N}_1$ é, de resto, um ideal bilateral. Para o vêr, basta ter em conta que s $\mathcal{K}_1^{(i)}$ é nilpotente, por ser nilideal. Demonstraremos a seguinte tabela de multiplicações:

	$\mathcal{L}_1$	$\mathcal{N}_1$
$\mathcal{L}_1$	$\mathcal{L}_1$	(0)
$\mathcal{N}_1$	$\mathcal{N}_1$	(0)

(6)

A relação $\mathcal{L}_1\mathcal{N}_1 = (0)$ é imediata. Estudemos $\mathcal{N}_1$ um pouco mais em detalhe. Têm-se as decomposições de Peirce

$$\mathcal{J} = E_1\mathcal{O}_1 + \mathcal{G}_1E_1 + \mathcal{J}_1 + E_1\mathcal{J}E_1 = E_1\mathcal{J} + \mathcal{G}_1 = \mathcal{J}E_1 + \mathcal{O}_1,$$

onde $E_1\mathcal{O}_1 + \mathcal{J}_1 = \mathcal{O}_1$, $\mathcal{G}_1E_1 + \mathcal{J}_1 = \mathcal{G}_1$, $\mathcal{G}_1E_1 + E_1\mathcal{J}E_1 = \mathcal{J}E_1$, $E_1\mathcal{O}_1 + E_1\mathcal{J}E_1 = E_1\mathcal{J}$, $\mathcal{J}_1 = [\mathcal{O}_1, \mathcal{G}_1]$, $\mathcal{O}_1$ = aniquilador esquerdo de E_1, $\mathcal{G}_1$ = aniquilador direito de E_1.

Vamos vêr que é $E_1\mathcal{O}_1 = (0)$.[1] A demonstração resultará do facto de se verificar que $E_1\mathcal{O}_1$ pertence a um ideal direito nilpotente contido em $\mathcal{L}_1$. Consideremos $\mathcal{O}_1^* = (E_1\mathcal{O}_1, \mathcal{J}E_1\mathcal{O}_1) = \mathcal{J}E_1\mathcal{O}_1$.

(1) Em todo êste § é utilizada a última memória citada de C.Hopkins.

Vê-se que é $\mathcal{O}_1^{*2} = \mathcal{J}E_1\mathcal{O}_1.(\mathcal{G}_1E_1 + E_1\mathcal{J}E_1)\mathcal{O}_1 = \mathcal{J}E_1\mathcal{O}_1\mathcal{G}_1E_1\mathcal{O}_1 = (\mathcal{G}_1E_1\mathcal{O}_1)^2, E_1\mathcal{J}E_1\mathcal{O}_1\mathcal{G}_1E_1\mathcal{O}_1)$. Provaremos, dentro dum instante, a igualdade $(\mathcal{G}_1E_1\mathcal{O}_1)^2 = (0)$. Nessas condições, tem-se

$$\mathcal{O}_1^{*2} \subseteq E_1\mathcal{O}_1, \qquad \mathcal{O}_1^{*4} = (0).$$

O ideal esquerdo $\mathcal{O}_1^*$ está contido num ideal bilateral nilpotente $\mathcal{J}$, e sendo $\mathcal{L}_1 = E_1\mathcal{J} \supseteq E_1\mathcal{O}_1$, êste último conjunto pertencerá a $\mathcal{J}$ e a $\mathcal{L}_1$, e, portanto, pertencerá a um ideal direito nilpotente contido em $\mathcal{L}_1$. Resta verificar a igualdade $(\mathcal{G}_1E\mathcal{O}_1)^2 = (0)$. Ora tem-se $\mathcal{G}_1E_1\mathcal{O}_1 \subseteq \mathcal{G}_1$, $E_1\mathcal{O}_1 \subseteq E_1\mathcal{J} = \mathcal{L}_1 \subseteq \mathcal{N}_1$, donde se tira $\mathcal{G}_1E_1\mathcal{O}_1 \subseteq \mathcal{N}_1$, ou seja $\mathcal{G}_1E_1\mathcal{O}_1 \subseteq [\mathcal{G}_1, \mathcal{N}_1] = [\mathcal{G}_1, \mathcal{L}_1 + \mathcal{N}_1]$. Um elemento desta última intersecção será da forma

$$b_1 = \ell_1 + n_1, \quad \text{com} \quad E_1b_1 = 0 = E_1\ell_1 + E_1n_1 = \ell_1,$$

onde b_1, ℓ_1, n_1 pertencem aos ideais com designações correspondentes. Será, pois, $b_1 = n_1$, e, portanto, como se quere,

$$\mathcal{G}_1E_1\mathcal{O}_1 \subseteq [\mathcal{G}_1, \mathcal{N}_1], \quad (\mathcal{G}_1E_1\mathcal{O}_1)^2 \subseteq \mathcal{N}_1^2 = (0).$$

Conclui-se agora que se tem

$$\mathcal{L}_1 = E_1\mathcal{J} = E_1\mathcal{J}E_1, \qquad \mathcal{L}_1^2 = \mathcal{L}_1.$$

Como o radical $\mathcal{R}$ de $\mathcal{J}$ verifica a relação $\mathcal{L}_1\mathcal{R} = (0)$, segue-se que é $E_1\mathcal{R} = (0)$. O radical de $\mathcal{L}_1$ será nulo e como a condição de mínimo se transporta para $E_1\mathcal{J}E_1$, conclui-se que $\mathcal{L}_1$ é um anel simples e semi-simples (de futuro, apenas simples). Resta mostrar, na tabela (6), a relação $\mathcal{N}_1\mathcal{L}_1 = \mathcal{N}_1$. Ora é $\mathcal{N}_1\mathcal{L}_1 \subseteq \mathcal{N}_1$, $\mathcal{N}_1\mathcal{L}_1E_1 = \mathcal{N}_1\mathcal{L}_1 \subseteq \mathcal{N}_1E_1$, assim como $\mathcal{N}_1\mathcal{L}_1 \supseteq \mathcal{N}_1E_1$. Portanto, tem-se $\mathcal{N}_1\mathcal{L}_1 = \mathcal{N}_1E_1$. Sejam $\mathcal{K}_1$ e $\mathcal{K}_1'$ dois ideais simples isomorfos, respectivamente pertencentes a $\mathcal{L}_1$ e $\mathcal{N}_1$. A correspondência $a_1 \to a_1'$ entre os seus elementos dá $a_1E_1 = a_1 \to a_1'E_1 = a_1'$. Daqui se conclui que E_1 é unidade direita de $\mathcal{N}_1$ (e, portanto, de $\mathcal{N}_1$), o que demonstra a igualdade $\mathcal{N}_1\mathcal{L}_1 = \mathcal{N}_1$.

Teorema:- Os ideais direitos de $\mathcal{L}_1$ e $\mathfrak{M}_1$ são ideais direitos de $\mathcal{T}$. Seja $\mathfrak{r}$ um ideal direito de $\mathcal{L}_1$. Tem-se

$$\mathfrak{r}\mathcal{T} = (\mathfrak{r}\mathcal{L}_1, \mathfrak{r}\mathcal{G}_1) = \mathfrak{r}\mathcal{L}_1 \subseteq \mathfrak{r} \ , \quad \text{pois} \quad \mathfrak{r}\mathcal{G}_1 = (0).$$

Seja $\mathfrak{r}$ um ideal direito de $\mathfrak{M}_1$. Tem-se

$$\mathfrak{r}\mathfrak{M}_1 \subseteq \mathfrak{r} \ , \ \mathfrak{r}\mathcal{T} = (\mathfrak{r}\mathcal{L}_1, \mathfrak{r}\mathcal{G}_1) \subseteq (\mathfrak{r}\mathfrak{M}_1, \mathfrak{r}\mathcal{G}_1) \subseteq \mathfrak{r},$$

pois $\mathfrak{r}\mathcal{G}_1 \subseteq \mathfrak{M}_1\mathcal{G}_1 = (\mathcal{L}_1\mathcal{G}_1, \mathfrak{N}_1\mathcal{G}_1) = (0)$.

Podemos enunciar o

Teorema:- Um anel $\mathcal{T}$ com condição de mínimo para ideais direitos é a soma directa do ideal direito $\mathcal{L}_1$ (soma de ideais direitos mínimos isomorfos dum dado ideal mínimo), que é um anel simples, e do ideal direito $\mathcal{G}_1$, êste último constituindo o aniquilador direito de $\mathcal{L}_1$. O radical está contido em $\mathcal{G}_1$, que é um ideal bilateral. Observemos que se tem $\mathcal{L}_1\mathcal{G}_1 = (0)$, de modo que o aniquilador de $\mathcal{L}_1$ contém $\mathcal{G}_1$. Como êsse aniquilador está contido no aniquilador de E_1, a afirmação correspondente do teorema é exacta. Como é $\mathcal{T}\mathcal{G}_1 = (\mathcal{L}_1 + \mathcal{G}_1)\mathcal{G}_1 = \mathcal{L}_1\mathcal{G}_1 \subseteq \mathcal{G}_1$, vê-se que êste último é ideal bilateral de $\mathcal{T}$. Finalmente, o radical está contido em $\mathcal{G}_1$, porque $E_1\mathcal{K} = (0)$.

Uma conseqüência imediata exprime-se pelo seguinte

Corolário:- Se um anel $\mathcal{T}$ com condição de mínimo é soma dos seus ideais direitos mínimos, supostos todos isomorfos, ou é igual ao seu radical, ou é simples, ou é soma directa dum anel simples e do seu radical. Êste último é de expoente 2(1)

Na verdade, é $\mathcal{T} = \mathfrak{M}_1 = \mathcal{L}_1 + \mathfrak{N}_1$. Se não há radical, tem-se $\mathfrak{N}_1 = (0)$, $\mathcal{T} = \mathcal{L}_1$. Se $\mathcal{K} \supset (0)$, notemos que, sendo $E_1\mathcal{K} = (0)$, é $\mathfrak{N}_1 \subseteq \mathcal{K} \subseteq \mathcal{G}_1$. As igualdades $\mathcal{T} = \mathcal{L}_1 + \mathcal{G}_1 = \mathcal{L}_1 + \mathfrak{N}_1$ dão $\mathcal{G}_1 = \mathfrak{N}_1 = \mathcal{K}$.

(1) Conforme J.Dieudonné, "Sur les systemes hyperkomplexes", Journal für die reine und angewandte Mathematik, Band 184, 1942.

Se $\mathcal{L}_1 = (0)$, é $\mathcal{T} = \mathcal{K}$. De contrário, é $\mathcal{T} = \mathcal{L}_1 + \mathcal{K}$, e o corolário está demonstrado. A tabela (6) é agora relativa às duas parcelas de $\mathcal{T}$.

Os aneis referidos no corolário, ou aneis quási-simples, consideram-se de estrutura conhecida, pelo menos no que respeita ao produto dos seus elementos. Para isso, deve ter-se em conta a tabela (6) e o que se sabe àcêrca da estrutura de $\mathcal{L}_1$.

Posto isto, consideremos os ideais mínimos não operatòriamente isomorfos, $\mathfrak{k}_1, \mathfrak{k}_2, \ldots$. Escolhamos de entre êles, se fôr possível, uma infinidade numerável $\mathfrak{k}_1, \mathfrak{k}_2, \ldots$. A soma dêstes é directa, visto que $\mathfrak{k}_1 + \mathfrak{k}_2$ é soma directa e a prova por indução é imediata. Conclui-se daqui haver um número finito de classes de ideais mínimos isomorfos. A essas diferentes classes correspondem somas $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_q$ e $\mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{N}_q$. Tanto $\sum \mathfrak{M}_i$ como $\sum \mathfrak{N}_i$ são somas directas. De facto, $\mathfrak{M}_1 + \mathfrak{M}_2$ está nessas condições, visto que $[\mathfrak{M}_1, \mathfrak{M}_2]$ é um ideal direito de $\mathfrak{M}_1$ e $\mathfrak{M}_2$, simultâneamente igual a uma soma de ideais direitos isomorfos dos que figuram em $\mathfrak{M}_1$ e em $\mathfrak{M}_2$. Por outro lado, a indução é fácil de estabelecer. É claro que

$$\mathfrak{M} = \sum \mathfrak{M}_i, \qquad \mathfrak{N} = \sum \mathfrak{N}_i,$$

representemos, respectivamente, a soma de todos os ideais direitos mínimos de $\mathcal{T}$ e a de todos os ideais direitos mínimos nilpotentes. São imediatas as relações $\mathfrak{M}_i\mathfrak{M}_j = (0)$, se $i \neq j$. Delas se deduzem outras. Têm também lugar tabelas análogas a (6). Escrevendo $\mathcal{L} = \sum \mathcal{L}_i$, tem-se $\mathfrak{M} = \mathcal{L} + \mathfrak{N}$. Desde que se escolha uma base ortogonal de elementos idempotentes em cada $\mathcal{L}_i$, obtem-se, pelo conjunto dessas bases, uma base ortogonal para $\mathcal{L}$. É válida a tabela

	$\mathcal{L}$	$\mathfrak{N}$
$\mathcal{L}$	$\mathcal{L}$	(0)
$\mathfrak{N}$	$\mathfrak{N}$	(0)

(7)

Para se reconhecer a relação $\mathfrak{N}\mathcal{L} = \mathfrak{N}$, basta escrever

$$\mathfrak{N}\mathfrak{L} = (\mathfrak{N}_1 + \ldots + \mathfrak{N}_q)(\mathfrak{L}_1 + \ldots + \mathfrak{L}_q) = \mathfrak{N}_1\mathfrak{L}_1 + \ldots + \mathfrak{N}_q\mathfrak{L}_q =$$

$$= \mathfrak{N}_1 + \ldots + \mathfrak{N}_q = \mathfrak{N} .$$

Se representarmos com E a soma dos diferentes elementos um dos $\mathfrak{L}_i$, E é o elemento um de $\mathfrak{L}$ e é unidade direita de $\mathfrak{N}$ (e, portanto, de $\mathfrak{M}$). $\mathfrak{L}$ é um anel semi-simples. Evidentemente que $\mathfrak{L}_i$ é ideal bilateral de $\mathfrak{L}$.

Vamos reconhecer algumas circunstâncias interessantes. Tendo em conta a ortogonalidade dos $\mathfrak{L}_i$ e pondo

$$\mathfrak{Y} = (E_1 + E_2)\mathfrak{N}_{12} + \mathfrak{L}_{12}(E_1 + E_2) + \mathfrak{I}_{12} + (E_1 + E_2)\mathfrak{Y}(E_1 + E_2) ,$$

mostram-se fàcilmente as relações

$$(E_1 + E_2)\,\mathfrak{Y}\,(E_1 + E_2) = \mathfrak{L}_1 + \mathfrak{L}_2 ,$$

$$\mathfrak{Y} = (E_1 + E_2)\,\mathfrak{Y} + \mathfrak{L}_{12} , \qquad \mathfrak{L}_{12} = [\mathfrak{L}_1 , \mathfrak{L}_2] ,$$

$$(E_1 + E_2)\,\mathfrak{Y} = E_1\mathfrak{Y} + E_2\mathfrak{Y} = \mathfrak{L}_1 + \mathfrak{L}_2 = (E_1 + E_2)\,\mathfrak{Y}\,(E_1 + E_2) + (E_1 + E_2)\mathfrak{N}_{12} ,$$

$$(E_1 + E_2)\mathfrak{N}_{12} = (0), \qquad \mathfrak{N}_{12} = [\mathfrak{N}_1 , \mathfrak{N}_2] = \mathfrak{I}_{12} .$$

Duma maneira geral, escrevendo $E = E_1 + \ldots + E_q$, tem-se

$$\mathfrak{Y} = E\mathfrak{N} + \mathfrak{L}E + \mathfrak{I} + E\,\mathfrak{Y}E ,$$

$$E\,\mathfrak{Y}E = \mathfrak{L} , \qquad \mathfrak{Y} = E\,\mathfrak{Y} + \mathfrak{L} , \qquad \mathfrak{L} = [\mathfrak{L}_1 , \ldots , \mathfrak{L}_q] ,$$

$$E\mathfrak{Y} = E_1\mathfrak{Y} + \ldots + E_q\mathfrak{Y} = \mathfrak{L}_1 + \ldots + \mathfrak{L}_q = E\,\mathfrak{Y}E + E\mathfrak{N} ,$$

$$E\mathfrak{N} = (0), \qquad \mathfrak{N} = \mathfrak{I} = [\mathfrak{N}_1 , \ldots , \mathfrak{N}_q] .$$

Podemos enunciar algumas proposições.

Teorema:- Os ideais direitos de $\mathfrak{L}$ e $\mathfrak{M}$ são ideais direitos de $\mathfrak{Y}$. A demonstração faz-se como numa proposição análoga anterior.

Teorema:- Um anel $\mathfrak{Y}$ com condição de mínimo para ideais direitos é a soma directa do ideal direito $\mathfrak{L}$ (soma de ideais direitos mínimos), que é um anel semi-simples, e do ideal direito $\mathfrak{G}$, êste último constituindo o aniquilador direito de $\mathfrak{L}$. O radical está contido em $\mathfrak{G}$, que é um ideal bilateral.

Uma conseqüência imediata exprime-se pelo seguinte

Corolário:- Se um anel $\mathfrak{Y}$ com condição de mínimo é soma dos seus ideais direitos mínimos, ou é igual ao seu radical, ou é semi-simples, ou é soma directa dum anel semi-simples e do seu radical. Êste último é de expoente 2.

Um anel como o referido no corolário pode chamar-se quási-semi-simples. A tabela (7) é então relativa às duas parcelas de $\mathfrak{Y}$. O produto dos elementos de $\mathfrak{N}$ pelos elementos de $\mathfrak{L}$ esclarece-se notando que é $\mathfrak{N}_i\mathfrak{L}_j = (0)$, se $i \neq j$.

Consideremos um anel quási-semi-simples $\mathfrak{Y} = \mathfrak{M} = \Sigma\mathfrak{M}_i$. Como um ideal direito de $\mathfrak{M}_i$ é ideal direito de $\mathfrak{Y}$, podemos enunciar o

Teorema:- Um anel quási-semi-simples é soma directa dum número finito de aneis quási-simples que mutuamente se anulam. O radical daquele é soma directa dos radicais dêstes últimos e o seu expoente é 2.

Êste teorema traduz também uma propriedade da soma $\mathfrak{M}$ dos ideais direitos mínimos dum anel qualquer.

Regressemos ao estudo de algumas propriedades de $\mathfrak{L}_1$. Enquanto que $\mathfrak{M}_1$ e $\mathfrak{N}_1$ têm significado preciso, é evidente que $\mathfrak{L}_1$ depende do modo como se faz a decomposição de $\mathfrak{M}_1$ numa soma de ideais direitos mínimos.

Teorema:- Se fôr $\mathfrak{M}_1 = \mathfrak{L}_1 + \mathfrak{N}_1$, pode escrever-se também $\mathfrak{M}_1 = \mathfrak{L}_1' + \mathfrak{N}_1$, onde $\mathfrak{L}_1' = (E_1 + D_1)\mathfrak{L}_1$, com $D_1 \in \mathfrak{N}_1$. Reciprocamente, se $\mathfrak{M}_1 = \mathfrak{L}_1' + \mathfrak{N}_1$, $\mathfrak{L}_1'$ é necessàriamente da forma indi-

cada. E_1+D_1 é o elemento um de $\mathcal{L}_1'$. Que E_1+D_1 é o elemento um de $\mathcal{L}_1'$ é imediato, se nos lembrarmos de que E_1 é unidade direita de $\mathcal{M}_1$ e de $\mathcal{L}_1$. Vamos passar ao resto do teorema. Em primeiro lugar, $\mathcal{L}_1'$ está contido em $\mathcal{M}_1$. Se fôr $m_1 = \ell_1 + n_1^{(1)}$, $\ell_1' = E_1\ell_1 + D_1\ell_1$, pode escrever-se também $m_1 = \ell_1' - D_1\ell_1 + n_1 = \ell_1' + n_1'$, onde $n_1' \in \mathcal{M}_1$. Para se vêr que é $[\mathcal{L}_1', \mathcal{M}_1] = (0)$, ponhamos $n_1 = E_1\ell_1 + D_1\ell_1$ um elemento da intersecção. Tem-se $E_1 n_1 = 0 = E_1\ell_1 = \ell_1$, e, portanto, $n_1 = 0$. Passemos à recíproca. Ponhamos $E_1 = \ell_1' + n_1$. Tem-se $\mathcal{L}_1'\mathcal{M}_1 = (0)$, e, por conseqüência,

$$E_1^2 = E_1 = \ell_1'^2 + n_1\ell_1' = \ell_1' + n_1, \qquad \ell_1'^2 = \ell_1', \quad n_1\ell_1' = n_1.$$

Ora, sendo $\ell_1' = E_1 - n_1$, é $\ell_1'\mathcal{L}_1 + \mathcal{M}_1 = \mathcal{L}_1 + \mathcal{M}_1$. Como $\ell_1'\mathcal{L}_1 \subseteq \mathcal{L}_1'$, tem necessàriamente lugar o sinal = entre êles. Sabemos agora, de resto, que ℓ_1' é o elemento um de $\mathcal{L}_1'$. O teorema está demonstrado.

Teorema:- Os ideais direitos $\mathcal{L}_1'$ e os elementos $D_1 \in \mathcal{M}_1$ estão em correspondência biunívoca. Em face dos resultados anteriores, bastará estabelecer que, supondo $D_1 \neq D_1'$, também $(E_1+D_1)\mathcal{L}_1 \neq (E_1+D_1')\mathcal{L}_1$. Se houvesse igualdade entre êstes dois últimos, o elemento E_1+D_1' pertenceria ao primeiro. Ter-se-ia

$$(E_1+D_1)(E_1+D_1') = E_1+D_1 = E_1+D_1', \qquad D_1' = D_1.$$

Teorema:- Os ideais $\mathcal{L}_1$ e $\mathcal{L}_1'$ são isomorfos. Na correspondência homomorfa $\ell_1 \longrightarrow (E_1+D_1)\ell_1 = \ell_1 + D_1\ell_1$, se supomos $\ell_1 + D_1\ell_1 = 0$, o facto de ser directa a soma $\mathcal{L}_1 + \mathcal{M}_1$ mostra que deve ter-se $\ell_1 = 0$.

Finalmente, demonstraremos nêste § o seguinte

Teorema:- O ideal bilateral $\mathcal{G}_1$ verifica as igualdades $\mathcal{T} = \mathcal{L}_1 + \mathcal{G}_1 = \mathcal{L}_1' + \mathcal{G}_1$. Tudo está em provar-se que o aniquilador

(1) As letras latinas minúsculas significam elementos pertencentes aos ideais designados pelas letras góticas maiúsculas correspondentes.

direito de $\mathcal{L}_1$ é o aniquilador direito de $\mathcal{L}_1'$. Tem-se

$$\mathcal{L}_1\mathcal{G}_1 = (0), \qquad \mathcal{L}_1'\mathcal{G}_1 = (E_1+D_1)\mathcal{L}_1\mathcal{G}_1 = (0).$$

O aniquilador direito de $\mathcal{L}_1'$ verifica as mesmas igualdades, o que demonstra o teorema. Podemos precisar, dizendo que $\mathcal{G}_1E_1 = \mathcal{G}_1(E_1+D_1)$, pelo facto de ser $\mathcal{G}_1(E_1+D_1) \subseteq \mathcal{G}_1$, $\mathcal{G}_1(E_1+D_1)E_1 = \mathcal{G}_1(E_1+D_1) \subseteq \mathcal{G}_1E_1$, e de terem lugar as relações em sentido inverso: $\mathcal{G}_1E_1 \subseteq \mathcal{G}_1$, $\mathcal{G}_1E_1(E_1+D_1) = \mathcal{G}_1E_1 \subseteq \mathcal{G}_1(E_1+D_1)$.

O que acabamos de dizer para $\mathcal{L}_1, \mathcal{L}_1', \mathcal{G}_1$ repete-se para $\mathcal{L}, \mathcal{L}', \mathcal{G}$, onde $\mathcal{L}'$ é uma parcela directa na soma $\mathcal{M} = \mathcal{L}' + \mathcal{N}$.

4) Sôbre os anéis semi-primários - Comecemos por lembrar alguns resultados e demonstrar certos teoremas preliminares. Um ideal bilateral $\mathcal{J}$, dum anel $\mathcal{T}$, diz-se primo, se, dados dois ideais bilaterais $\mathfrak{a}$ e $\mathfrak{b}$ tais que $\mathfrak{a}\mathfrak{b} \equiv 0(\mathcal{J})$, tiver lugar uma (pelo menos) das relações $\mathfrak{a} \equiv 0(\mathcal{J})$, $\mathfrak{b} \equiv 0(\mathcal{J})$.

Teorema 1º:- O radical $\mathcal{R}$ está contido em qualquer ideal primo $\mathcal{J}$. Tomemos, na verdade, $a \in \mathcal{R}$. O ideal bilateral $\mathfrak{a}$, gerado por a, é nilpotente, de modo que $(0) = \mathfrak{a}^s \subset \mathcal{J}$. Tira-se daqui $\mathfrak{a} \subseteq \mathcal{J}$, e, portanto, $a \in \mathcal{J}$, ou seja $\mathcal{R} \subseteq \mathcal{J}$.

Corolário:- Se $\mathcal{R} \neq (0)$, (0) não é ideal primo. Sob forma afirmativa, podemos também dizer: se (0) é primo, é $\mathcal{R} = (0)$.

Teorema 2º:- Há correspondência biunívoca completa entre os ideais primos de $\mathcal{T}$ que contêm o ideal bilateral $\mathfrak{a}$ e os ideais primos de $\mathcal{T}/\mathfrak{a}$. A demonstração faz-se estudando o homomorfismo $\mathcal{T} \sim \mathcal{T}/\mathfrak{a}$.

Teorema 3º:- Se $\mathfrak{a} \supset \mathcal{P}$ é um ideal bilateral mínimo dos ideais de $\mathcal{T}$ que contêm $\mathcal{P}$, o ideal bilateral $\mathcal{J}$, conjunto dos elementos p tais que $p\mathfrak{a} \subseteq \mathcal{P}$, é um ideal bilateral primo. É imediato que $\mathcal{J}$ é um ideal bilateral. Para se vêr que é primo, suponhamos $\mathfrak{b}z \equiv 0(\mathcal{J})$ e $\mathfrak{b} \not\equiv 0(\mathcal{J})$. Trata-se de provar que $z \equiv 0(\mathcal{J})$. Se fôsse $z \not\equiv 0(\mathcal{J})$, em virtude de se ter

$$\mathfrak{b}z\mathfrak{a} \subseteq \mathcal{P}, \quad z\mathfrak{a} \not\subset \mathcal{P}, \quad \mathcal{P} \subset (\mathcal{P}, z\mathfrak{a}) \subseteq \mathfrak{a},$$

conclui-se $(\varphi, z\alpha) = \alpha$, $(\beta\varphi, \beta z\alpha) = \beta\alpha \equiv \varphi$, $\beta \equiv 0(\mathcal{P})$, contra a hipótese.

Corolário 1º:- Se α é um ideal bilateral mínimo de $\mathcal{J}$, o ideal $\mathcal{P}$, conjunto dos elementos p tais que $p\alpha = (0)$, é um ideal bilateral primo. Podemos precisar que $\mathcal{P}$ representa também o conjunto $\mathfrak{r}$ dos elementos q tais que $\alpha q = (0)$, se não há radical $\mathcal{R}$. De facto, é $\alpha\mathcal{P}.\alpha\mathcal{P} = \alpha.\mathcal{P}\alpha.\mathcal{P} = (0)$. Como não há radical, tem-se $\alpha\mathcal{P} = (0)$, ou seja $\mathcal{P} \subseteq \mathfrak{r}$. Prova-se anàlogamente que $\mathfrak{r} \subseteq \mathcal{P}$, e conclui-se, assim, $\mathcal{P} = \mathfrak{r}$.

Corolário 2º:- Se num anel $\mathcal{J}$ todos os ideais bilaterais diferentes de (0) são primos, o radical $\mathcal{R}$ ou é nulo ou é uma álgebra zero (de expoente 2). Se (0) é primo, é $\mathcal{R} = (0)$. Suponhamos (0) não primo. Se $\mathcal{R}$ não é nulo, em virtude do teorema 1º, $\mathcal{R} = \alpha$ é um ideal bilateral mínimo. Então, a igualdade $\mathcal{R}^2 = \mathcal{R}$ não pode ter lugar, pelo facto de ser $\mathcal{R}.\mathcal{R} \subseteq \mathcal{P}.\mathcal{R} = (0)$. Será $\mathcal{R}^2 = (0)$, q. e. d.

Um ideal bilateral $\mathcal{P} \neq \mathcal{J}$ diz-se sem divisor, se o anel cociente $\mathcal{J}/\mathcal{P} = \mathcal{J}'$ fôr simples e semi-simples. Um ideal sem divisor é primo, como vamos vêr. No homomorfismo $\mathcal{J} \sim \mathcal{J}'$, tomemos os ideais bilaterais correspondentes $\alpha \longrightarrow \alpha'$, $\beta \longrightarrow \beta'$, com $\alpha\beta \equiv 0(\mathcal{P})$. Tem-se $\alpha'\beta' = (0)$. Se fôr $\alpha' = (0)$ ou $\beta' = (0)$, é $\alpha \equiv 0(\mathcal{P})$ ou $\beta \equiv 0(\mathcal{P})$. O caso $\alpha' = \mathcal{J}'$, $\beta' = \mathcal{J}'$ não pode dar-se, pelo facto de $\mathcal{J}'$ ter elemento um.

No geral, não vale a circunstância inversa, de ser um ideal sem divisor todo o ideal primo. Tem todavia lugar o seguinte

Teorema 4º:- É necessário e suficiente, para que o ideal primo $\mathcal{P}$ seja um ideal sem divisor, que tenha lugar em $\mathcal{J}$ a condição de mínimo para os ideais direitos que contenham $\mathcal{P}$. A condição é necessária: Seja $\mathcal{J}/\mathcal{P} = \mathcal{J}'$. O homomorfismo $\mathcal{J} \sim \mathcal{J}'$ faz corresponder a cada ideal direito de $\mathcal{J}'$ um único ideal $\equiv \mathcal{P}$; e a condição de mínimo em $\mathcal{J}'$ arrasta a condição de mínimo para os ideais $\equiv \mathcal{P}$. A condição é suficiente: Vale, em $\mathcal{J}$, a condição de mínimo para os ideais $\kappa \equiv \mathcal{P}$. Trata-se de provar que $\mathcal{J}'$ é simples e semi-simples. A condição de mínimo é válida em $\mathcal{J}'$. Êste tem, assim, um radical nilpotente $\mathcal{R}' = \mathcal{R}'^{\kappa}$. Seja $\mathcal{R}'^{\kappa} = (0)$. Em $\mathcal{J}'$, se o produto de dois ideais bilaterais é nulo, um deles é nulo. Será, pois, $\mathcal{R}' = (0)$. $\mathcal{J}'$ é semi-simples. Seja, agora, $\alpha' \supset (0)$ o ideal bilateral mínimo não nulo

de $\mathcal{J}'$. Vamos vêr que é $\alpha' = \mathcal{J}'$. Se assim não fôsse, a decomposição de $\mathcal{J}'$ em anéis simples levaria à existência dum ideal bilateral $\alpha'' \supset (0)$ tal que $\alpha''\alpha' = \alpha'\alpha'' = (0)$.

Teorema 5º:- Se num anel $\mathcal{J}$ todos os ideais bilaterais diferentes de (0) são sem divisor, $\mathcal{J}$ é um anel - A especial. Supõe-se $\mathcal{R} \neq (0)$, se $\mathcal{J}$ é simples e semi-simples. Se $\mathcal{R} \supset (0)$, tem-se $\mathcal{R}^2 = (0)$ e $\mathcal{J}/\mathcal{R}$ é simples e semi-simples. Podemos precisar que, no caso de haver $u \in \mathcal{J}$, êste é anel primário especial.

Consideremos agora os anéis $\mathcal{J}$ para os quais são válidas as duas propriedades seguintes: I) a condição de mínimo para os ideais bilaterais de $\mathcal{J}$; II) cada ideal primo é um ideal sem divisor.(1)

Teorema 6º:- As condições I) e II) transportam-se de $\mathcal{J}$ para $\mathcal{J}/\mathcal{R}$. Relativamente a I), o teorema é imediato. Quanto a II), basta ter em conta os teoremas 2º e 4º.

Teorema 7º:- É condição necessária e suficiente, para que um anel $\mathcal{J}$ seja semi-simples, que tenham lugar as condições I) e II) e seja $\mathcal{R} = (0)$. É imediato que a condição é necessária. Para se vêr que é suficiente, raciocina-se como segue. Seja $\alpha \supset \supset (0)$ um ideal bilateral mínimo de $\mathcal{J}$. O ideal bilateral $\mathcal{P}$ tal que $\mathcal{P}\alpha = (0)$ é um ideal primo, e, portanto, sem divisor. E, sendo $[\mathcal{J}, \alpha] \subseteq \mathcal{P}, \alpha$; $[\mathcal{P}, \alpha]^2 \subseteq \mathcal{P}\alpha$; vê-se que se tem $[\mathcal{P}, \alpha] = (0)$. A soma $\mathcal{P} + \alpha$ é directa, valendo $\mathcal{J} = \alpha + \mathcal{P}$, visto que $\mathcal{P}$ é sem divisor. α é simples e semi-simples, por ser isomorfo de $\mathcal{J}/\mathcal{P}$. Todos os ideais bilaterais de $\mathcal{P}$ são ideais bilaterais de $\mathcal{J}$. Tomando em $\mathcal{P}$, suposto $\neq (0)$, um ideal bilateral mínimo β, é $\mathcal{J} = \beta + \mathcal{P}_{11}$, $\mathcal{P} = \beta + \mathcal{P}_1$, $\mathcal{J} = \alpha + \beta + \mathcal{P}_1$, etc. A cadeia $\mathcal{J} \supset \mathcal{P} \supset \mathcal{P}_1 \supset \ldots$ é limitada, devendo chegar-se a um ideal nulo. aparece, então, como soma de ideais simples e semi-simples, pelo que é semi-simples.

Teorema:- As condições I) e II) bastam para que um anel $\mathcal{J}$ seja um anel - A especial. A condição I), com efeito, garante

(1) K. Asano, "Über Ringe mit Vielfachenkettensatz", atrás citado.

que $\mathfrak{K}$ é nilpotente e que, portanto, $\mathfrak{r}/\mathfrak{K}$ não tem radical. Em virtude do teorema 6º, valem em $\mathfrak{r}/\mathfrak{K}$ as condições I) e II). Assim, conforme o teorema anterior, $\mathfrak{r}/\mathfrak{K}$ é semi-simples, e, como $\mathfrak{K}$ é nilpotente, o teorema está demonstrado.

Corolário:- As condições I) e II) garantem que $\mathfrak{K}^*$ existe e é igual a $\mathfrak{K}$. Observe-se que um nilideal bilateral $\mathfrak{n} \supset (0)$ goza da propriedade $\mathfrak{n} \supset \mathfrak{n}^2$.

Vale, mesmo, o teorema preciso seguinte:

Teorema:- Se valem em $\mathfrak{r}$ as condições I) e II), todo o sub-nilanel é nilpotente. A demonstração é a mesma que para os anéis com condição de mínimo (§ 2 dêste Cap.).

Teorema:- É condição necessária e suficiente, para que $\mathfrak{r}$ seja um anel-A, que valha a condição de mínimo para os ideais bilaterais de $\mathfrak{r}$ que contêm $\mathfrak{K}^{**}$ e que cada ideal primo contendo $\mathfrak{K}^{**}$ seja um ideal sem divisor. É imediato que a condição é necessária. Para se vêr que é suficiente, notemos que a condição em causa garante as condições I) e II) em $\mathfrak{r}/\mathfrak{K}^{**}$. Como êste anel cociente não tem radical (com ou sem asteriscos), é um anel semi-simples. O teorema está provado.

Corolário:- Quando $\mathfrak{K}^{**}$ fôr nilpotente, as condições do teorema anterior garantem que $\mathfrak{r}$ é um anel - A especial. Mais geralmente do que no corolário, seja $\mathfrak{r}$ de radical nilpotente. Condições mais fracas que I) e II) [não só suficientes, mas também necessárias]; para $\mathfrak{r}$ ser anel-A especial, são enunciadas como no último teorema, apenas pondo $\mathfrak{K}$ em vez de $\mathfrak{K}^{**}$.

Finalmente, $\mathfrak{r}$ será anel-A generalizado, ainda nas mesmas condições do último teorema, se se supõe que $\mathfrak{K}^*$ existe e se substitui no enunciado $\mathfrak{K}^{**}$ pelo radical $\mathfrak{K}^*$.

SISTEMAS HIPER-COMPLEXOS

Capítulo V

Matrizes

1) Recapitulação de alguns resultados do tomo I - Uma grande parte do tomo anterior foi dedicada ao estudo de matrizes. Interessa-nos aqui ter presentes os resultados do Cap. IV do referido tomo. Viu-se no citado Capítulo que, dada uma matriz rectangular A, com elementos pertencentes a um anel de ideais principais $\mathfrak{o}$, era possível reduzir essa matriz à forma

$$A \longrightarrow \begin{pmatrix} b_{11} \dots & 0 & \dots 0 \\ \hline 0 & \dots & b_{rr} \dots 0 \\ \hline 0 & \dots & 0 \dots 0 \end{pmatrix} = B , \quad (b_{ii} \in \mathfrak{o}), \quad (1)$$

na qual $b_{ii} \equiv 0 \ (b_{i-1,i-1})$. Essa redução tinha lugar à custa das seguintes operações elementares: I) troca de linhas ou de colunas; II) adição, a uma linha ou a uma coluna, dos elementos doutra linha ou doutra coluna, multiplicados por um elemento do anel; III) substituição dos elementos a, b, duma linha ou duma coluna, pelos elementos o, d, em que d significa o máximo divisor comum (m.d.c.) de a e b. A estas operações pode juntar-se IV): multiplicação dos elementos duma linha ou duma coluna por uma unidade de $\mathfrak{o}$. Tôdas elas equivalem a multiplicar A por matrizes quadradas invertíveis Π (à direita ou à esquerda), de modo que, finalmente, se encontra $B = P\,A\,Q$, onde P e Q são invertíveis (produtos de matrizes Π). Os elementos b_{ii} chamaram-se divisores elementares de A. Quando a matriz A vem multiplicada por uma matriz Π, a matriz $C = A\,\Pi$ (ou $\Pi\,A$) goza da propriedade seguinte: os determinantes de ordem k que podem extrair-se de C são combinações lineares dos determinantes de ordem k que podem extrair-se de A, e reciprocamente. A matriz B está, por consequência, nas mesmas condições. Se designarmos por d_{ss} o m.d.c. dos determinantes de ordem s extraidos de B, tem-se

$$d_{11} = b_{11} , \quad d_{22} = b_{11}\,b_{22} , \dots , \quad d_{rr} = b_{11} \dots b_{rr} , \quad (1')$$

pondo de parte unidades de $\mathcal{O}$. Isto significa que, a partir de A, podem determinar-se os b_{ii}, calculando os d_{ss} (divisores determinantes). Basta pôr

$$b_{11} = d_{11}, \quad b_{22} = \frac{d_{22}}{d_{11}}, \ldots, \quad b_{rr} = \frac{d_{rr}}{d_{r-1,r-1}}.$$

O número inteiro r representa também a característica de A.

Seja P uma matriz invertível. O seu determinante é uma unidade. As relações (1') mostram que os d_{jj}, assim como os b_{ii}, são unidades, sempre que a matriz A é invertível.

Se A e D forem duas matrizes (do mesmo número de linhas e de colunas) com os mesmos divisores elementares, tem-se

$$P\,A\,Q = A', \qquad P_1\,D\,Q_1 = D',$$

onde A' e D' são da forma (1). Podemos supôr A' = D', desde que A' se multiplique por uma matriz quadrada diagonal conveniente de elementos diagonais todos diferentes de zero e iguais a unidades. Então será

$$P\,A\,Q = P_1\,D\,Q_1, \qquad A = P^{-1}P_1 . D . Q_1 Q^{-1} = R\,D\,S,$$

onde R e S são invertíveis. Reciprocamente, se se multiplica uma matriz A por uma matriz invertível R (à direita ou à esquerda), a matriz produto tem os mesmos divisores elementares que A. De facto sendo B = A R, a igualdade P R Q = U, com P e Q invertíveis (e produtos de matrizes Π, como sempre se tem suposto) e U = matriz unidade, dá

$$B = A\,P^{-1}Q^{-1}, \quad B\,Q\,P = A, \quad B.\text{matrizes } \Pi = A,$$

donde se conclui o que se deseja. Podemos fixar o

Teorema:- É condição necessária e suficiente, para que duas matrizes A e D, com o mesmo número de linhas e de colunas, tenham os mesmos divisores elementares, que existam duas matrizes invertíveis, R e S, tais que A = R D S.[1]

Teorema:- A característica dum produto de duas matrizes é igual ou menor que a característica dos factores. Representemos por E_r uma matriz quadrada de ordem r, só com elementos diagonais diferentes de zero e iguais a unidades. Se o produto AB de duas matrizes tem a característica r", existem matrizes invertíveis R e S tais que

$$R.AB.S = \begin{pmatrix} E_{r''} & 0 \\ 0 & 0 \end{pmatrix}.$$

Existem também matrizes invertíveis P e Q tais que

$$P\,R\,A\,Q = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}, \quad (r = \text{característica de A ou de R A}).$$

Nestas condições, pode escrever-se

$$P^{-1}\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}Q^{-1}B\,S = \begin{pmatrix} E_{r''} & 0 \\ 0 & 0 \end{pmatrix}.$$

Esta igualdade mostra que a característica de

$$\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}Q^{-1}B = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} F & G \\ H & K \end{pmatrix} = \begin{pmatrix} E_r F & E_r G \\ 0 & 0 \end{pmatrix}$$

é igual a r". Como o número de linhas diferentes de zero da última matriz é igual a r, quando muito, vê-se que deverá ter $r'' \leqslant r$, como se afirmou.

---

(1) O leitor que não possuir o nosso tomo I encontra as demonstrações invocadas nêste § no livro de A.A.Albert, "Modern Higher Algebra", Chicago, 1937, pgs. 59 e seguintes.

2) Matrizes quadradas com elementos de $\mathcal{K}[x]$ [1] - Nêste §, $\mathcal{K}$ é um corpo e $\mathcal{K}[x]$ [2] é o domínio de integridade que resulta de $\mathcal{K}$ por adjunção anular da indeterminada x. $\mathcal{K}$, considerado como uma parte de $\mathcal{K}[x]$, é composto de elementos que são unidades de $\mathcal{K}[x]$ ou que são polinómios do grau zero dêste último domínio. Tomemos o anel $\mathcal{K}_n$, de matrizes quadradas de grau n com elementos de $\mathcal{K}$. A cada elemento a do côrpo façamos corresponder a matriz diagonal de elementos iguais a a. Essa correspondência é um isomorfismo. Podemos substituir em $\mathcal{K}_n$ tais matrizes diagonais pelos elementos do corpo, de modo que $\mathcal{K} \equiv \mathcal{K}_n$. Se A fôr uma matriz, tem sentido uma soma $a + A$ ou um produto aA.

Passemos agora de $\mathcal{K}[x]$ ao anel $\mathcal{M}_n$ de matrizes quadradas do grau n com elementos dêsse domínio. Pode supôr-se anàlogamente $\mathcal{K}[x] \equiv \mathcal{M}_n$. Uma soma da forma $x + A$, por ex., em que A é a matriz acima mencionada, tem aqui sentido. O mesmo se diz duma soma $x + a$, considerada como uma soma de matrizes. Uma expressão do tipo $x^n A_n + x^{n-1} A_{n-1} + \ldots + x A_1 + A_0$,

(1) Indicamos no prefácio a ordem pela qual devem ser lidas as nossas publicações, a fim de ser feita uma leitura completa de tôdas elas, incluindo esta. Também dissémos que os quatro primeiros cadernos de Álgebra moderna, saídos no Pôrto por iniciativa da Junta de Investigação Matemática, bastavam à compreensão duma grande parte do que aqui escrevemos. Juntando ao texto dêsses 4 cadernos (que podem substituir-se por uma parte do nosso volumesito "Elementos da Teoria dos Grupos") a doutrina exposta de pgs. 1 a 54, 72 a 79, 86 a 91, 113 a 123 e Cap. V do nosso livro "Elementos da Teoria dos Anéis", e bem assim as 40 primeiras páginas do tomo I desta obra e o Cap. IV dêsse mesmo tomo, pode lêr-se todo êste volume, crêmos que sem excepção. O leitor que tiver presentes as pgs. 4 a 6, 14 a 67 e 131 a 144 do livro de van der Waerden, "Moderne Algebra", I Teil, 1930, está também habilitado a compreender quási tôda a matéria. É fácil, de resto, encontrar em qualquer publicação de Álgebra moderna (van der Waerden, A.A.Albert, Mac Duffee, G.Birkhoff, etc.) os elementos de que o leitor carece para nos seguir. O conteúdo dêste Capítulo, e bem assim uma parte importante do do seguinte, é extraído principalmente dos Cap. IV e X do livro de A.A.Albert, "Modern Higher Algebra", já mencionado.

(2) $\mathcal{K}$ é comutativo.

onde as matrizes A_i são compostas de elementos de $\mathcal{K}$ é ainda de fácil interpretação em $\mathcal{M}_n$. Por ex., $x^R A_R$ é o produto de k matrizes diagonais de elementos iguais a x pela matriz A_R. Vê-se que todo o elemento de $\mathcal{M}_n$ se pode escrever sob a forma $\sum x^R A^R$. Êsse facto faz com que se possa interpretar $\mathcal{M}_n$ como o anel $\mathcal{K}_n[x]$, resultante de $\mathcal{K}_n$ pela adjunção anular da transcendente x: $\mathcal{M}_n = (\mathcal{K}[x])_n = \mathcal{K}_n[x]$. Uma observação a fazer é a de que os anéis de matrizes não são comutativos.

3) Divisão por $x - A$ - Seja $\mathcal{J}$ um anel com elemento u. Um elemento $a \in \mathcal{J}$ é regular se tem inverso. Dado o anel $\mathcal{J}[x]$, tomemos dois polinómios $P(x)$, $D(x)$, de graus n e m, respectivamente:

$$P(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n ,$$

$$D(x) = b_0 x^m + b_1 x^{m-1} + \ldots + b_{m-1} x + b_m .$$

Suponhamos b_0 um elemento regular. Existe um algoritmo de divisão, pois podem determinar-se sempre, de modo unívoco, dois polinómios $Q_d(x)$, $R_d(x)$ (ou $Q_e(x)$, $R_e(x)$) tais que

$$P(x) = Q_d(x) . D(x) + R_d(x),$$

$$P(x) = D(x) . Q_e(x) + R_e(x) .$$

Se fôr, em particular, $D(x) = x - \alpha$, podem dar-se expressões simples para $R_d(x)$ e $R_e(x)$. Observemos, com efeito, as igualdades

$$x^n - \alpha^n = (x^{n-1} + \alpha x^{n-2} + \ldots + \alpha^{n-2} x + \alpha^{n-1}) (x - \alpha),$$

$$x^n - \alpha^n = (x - \alpha) (x^{n-1} + \alpha x^{n-2} + \ldots + \alpha^{n-2} x + \alpha^{n-1}).$$

Tem-se, então,

$$P(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n ,$$

$$R_d(x) = a_0 \alpha^n + a_1 \alpha^{n-1} + \ldots + a_{n-1} \alpha + a_n ,$$

pois

$$P(x) - R_d(x) = a_0(x^n - \alpha^n) + a_1(x^{n-1} - \alpha^{n-1}) + \ldots + a_{n-1}(x - \alpha) =$$

$$= Q(x).(x - \alpha) .$$

Vê-se anàlogamente que é

$$R_e(x) = \alpha^n a_0 + \alpha^{n-1} a_1 + \ldots + \alpha a_{n-1} + a_n ,$$

para o que basta ter em conta a comutabilidade da indeterminada x com os elementos de $\mathcal{F}$.

Regressemos ao anel $\mathcal{M}_n = \mathcal{A}_n[x]$ do § anterior. Sabemos o que significa a divisão por $x - A$ duma matriz qualquer com elementos de $\mathcal{A}[x]$.

4) Matrizes semelhantes - Duas matrizes A , $B \in \mathcal{A}_n$ dizem-se semelhantes, se existe uma matriz invertível P tal que

$$B = P A P^{-1} .$$

Teorema:- É condição necessária e suficiente, para que duas matrizes A e B sejam semelhantes, que tenham os mesmos divisores elementares as matrizes $x - A$ e $x - B$.

A condição é necessária - Supondo $B = P A P^{-1}$, tem-se

$$x - B = x - P A P^{-1} = P(x - A) P^{-1} ,$$

donde se conclui a afirmação.

A condição é suficiente - Suponhamos que $x - A$ e $x - B$ têm os mesmos divisores elementares. Existem matrizes invertíveis $R, S \in \mathcal{A}_n[x]$ tais que

$$x - B = R(x - A)S . \qquad (2)$$

Ponhamos $R = (x - B).Q_1 + R_1$, $S = Q_2.(x - B) + R_2$, onde pode

ser, incidentalmente, $Q_1 = 0$, ou $Q_2 = 0$, ou $Q_1 = Q_2 = 0$. As matrizes R_1 e R_2 são compostas de elementos de $\mathcal{A}$. De (2) tira-se

$$R(x - A)S = \left[(x - B)Q_1 + R_1\right].(x - A).\left[Q_2(x - B) + R_2\right] =$$

$$= (x - B)Q_1(x - A)Q_2(x - B) + (x - B)Q_1(x - A)R_2 + R_1(x - A)Q_2(x - B) +$$

$$+ R_1(x - A)R_2 = (x - B)Q_1(x - A)Q_2(x - B) + (x - B)Q_1(x - A) .$$

$$.\left[S - Q_2(x - B)\right] + \left[R - (x - B)Q_1\right].(x - A)Q_2(x - B) + R_1(x - A)R_2 =$$

$$= (x - B)Q_1(x - A)S + R(x - A)Q_2(x - B) - (x - B)Q_1(x - A)Q_2 .$$

$$.(x - B) + R_1(x - A)R_2 = (x - B)Q_1R^{-1}(x - B) + (x - B)S^{-1} .$$

$$. Q_2(x - B) - (x - B)Q_1(x - A)Q_2(x - B) + R_1(x - A)R_2 =$$

$$= (x - B).\left[Q_1R^{-1} + S^{-1}Q_2 - Q_1(x - A)Q_2\right].(x - B) + R_1(x - A)R_2 .$$

Conclui-se, pois, uma relação da forma

$$R(x - A)S = (x - B).\ominus.(x - B) + R_1(x - A)R_2 ,$$

onde a matriz $\ominus$ está indicada no último parêntesis recto das igualdades anteriores. Se fôsse $\ominus \neq 0$, o segundo membro da igualdade supra seria, pelo menos, um polinómio do 2º grau, o que é absurdo. Ter-se-á simplesmente

$$x - B = R_1(x - A)R_2 = xR_1R_2 - R_1A R_2 ,$$

o que dá $R_1R_2 = U$, $B = R_1A R_2$. Como R_1 e R_2 são matrizes de determinante não nulo com elementos dum corpo, são invertíveis. Assim, tem-se

$$B = R_1A R_1^{-1} , \qquad \text{q.e.d.}$$

Os divisores elementares de $x - A$ e $x - B$ calculam-se por meio de operações envolvendo apenas polinómios com coeficientes pertencentes a um sub-corpo de $\mathfrak{K}$ que contém os elementos de A e de B. É válido, por isso, o seguinte

Teorema:- Duas matrizes semelhantes em $\mathfrak{K}$ são semelhantes em qualquer corpo (sub-corpo de $\mathfrak{K}$) que contenha os elementos das matrizes.

5) Polinómios mínimo e característico duma matriz - Da definição de $\mathfrak{K}_n$, conclui-se que êste anel é módulo finito relativamente ao corpo $\mathfrak{K}$.[1] Se A fôr uma matriz, as potências sucessivas U, A, A^2, A^3, ... não podem ser tôdas linearmente independentes, pelo que haverá uma relação

$$\alpha_t' A^t + \dots + \alpha_1' A + \alpha_0' = 0 , \qquad (\alpha_i' \in \mathfrak{K} \subseteq \mathfrak{K}_n) ,$$

sem que todos os α_i' sejam nulos. α_t' supõe-se diferente de zero e a relação anterior pode tomar ainda a forma

$$A^t + \alpha_{t-1} A^{t-1} + \dots + \alpha_1 A + \alpha_0 = 0 .$$

Seja $\psi(x)$ um polinómio normado[2], de grau mínimo, tal que $\psi(A) = 0$. Êsse polinómio diz-se polinómio mínimo de A. É bem determinado, pois que, se $D(x)$ fôsse um segundo polinómio mínimo, a equação $\psi(x) - D(x) = 0$, de grau inferior ao de cada um dos polinómios, seria ainda verificada por A. Se $\Phi(x)$ fôr um polinómio qualquer a que satisfaça A, efectuemos a divisão de $\Phi(x)$ por $\psi(x)$: $\Phi(x) = \psi(x).q(x) + r(x)$. Substituindo aqui x por A, vê-se que $r(A) = 0$. Como $r(x)$ é de grau inferior ao grau de $\psi(x)$, será $r(x) = 0$. Assim, vale o

(1) As propriedades dos módulos relativos a corpos foram dados no Cap.II do tomo anterior.

(2) O coeficiente do têrmo de mais alto grau é $u \in \mathfrak{K}$.

Teorema:- O polinómio mínimo duma matriz divide qualquer polinómio a que satisfaça a matriz.

Consideremos, em particular, o polinómio normado

$$f(x) = |x - A| = \text{determinante da matriz } x - A \in \mathfrak{K}_n[x].$$

É um polinómio de grau n (grau da matriz). Designando com B_a a matriz adjunta duma matriz B, tem-se

$$(x - A)_a . (x - A) = |x - A| = f(x) \in \mathfrak{K}_n[x] . \qquad (3)$$

Esta igualdade mostra que $f(x)$ é divisível por $x - A$, e que, portanto, o resto direito $f(A) = A^n + \dots + (-1)^n |A|$ é nulo. $f(x)$ diz-se o polinómio característico de A, e enuncia-se o

Teorema:- Toda a matriz A satisfaz à sua equação característica $f(x) = 0$.

Uma outra proposição é a seguinte:

Teorema:- O polinómio mínimo duma matriz A é o último divisor elementar da matriz $x - A$. Trata-se de demonstrar que

$$a_{nn}(x) = \frac{d_{nn}(x)}{d_{n-1,n-1}(x)} = \frac{f(x)}{d_{n-1,n-1}(x)} = \psi(x). \qquad (4)$$

Em primeiro lugar, como é $|x - A| = f(x) \neq 0$, o determinante da matriz da forma (1) deduzida de $x - A$ é também $\neq 0$ e $x-A$ tem n divisores elementares. O divisor determinante $d_{n-1,n-1}(x)$ é o m.d.c. dos elementos da matriz adjunta de $x - A$. Pode escrever-se, em virtude disso,

$$(x - A)_a = d_{n-1,n-1}(x) . B,$$

onde $B \in \mathfrak{K}_n[x]$. Daqui tira-se, tendo em conta (3) e (4):

$$a_{nn}(x) \; (x - A)_a = f(x) . B,$$

$$a_{nn}(x) \; (x - A)_a (x - A) = f(x) . B . (x - A),$$

$$a_{nn}(x).f(x) = f(x).B.(x - A),$$

$$a_{nn}(x) = B.(x - A).$$

A matriz $a_{nn}(x)$ é divisível por $x - A$, e, por consequência, tem-se

$$a_{nn}(x) = \psi(x).q(x). \qquad (5)$$

Efectuemos a divisão de $\psi(x)$ por $x - A$ sob a forma $\psi(x) = C\,(x - A)$. Vem imediatamente

$$a_{nn}(x) = C\ q(x).(x - A),$$

de sorte que $B = C\ q(x)$, pelo facto de o algoritmo de divisão em $\mathfrak{K}_n[x]$ levar a um resultado determinado. B, por construção, admite como m.d.c. dos seus elementos o elemento $u \in \mathfrak{K}$. Não pode deixar de ser $q(x) \in \mathfrak{K}$, e, portanto, independente de x. A relação (5) dá agora $a_{nn}(x) = \psi(x).q$. Se $a_{nn}(x)$ é normado, como pode admitir-se, ter-se-á $a_{nn}(x) = \psi(x)$, q.e.d.

Corolário 1º:- O polinómio mínimo duma matriz A é independente do corpo a que se supõem pertencer os elementos de A.

Esclareçamos. Se os elementos de A pertencem a $\mathfrak{K}$, pertencem a qualquer ampliação Ω, de $\mathfrak{K}$. O polinómio mínimo de A, com elementos de Ω, calcula-se pelas operações indicadas pelo teorema, efectuadas sobre a matriz $x - A$. Essas operações apenas exigem que se utilize o algoritmo de divisão em $\mathfrak{K}[x]$, de modo que o referido polinómio fica o mesmo.

Corolário 2º:- O polinómio característico duma matriz é divisor duma potência do polinómio mínimo da referida matriz.

É o que se conclui das relações

$$a_{11}(x) = d_{11}(x),\quad a_{22}(x) = \frac{d_{22}(x)}{d_{11}(x)},\ \ldots,\ a_{nn}(x) = \psi(x) =$$

$$= \frac{f(x)}{d_{n-1,n-1}(x)},\quad a_{ll}(x) \equiv 0\left((a_{l-1,l-1}(x)\right).$$

De facto, tem-se, para cada i, $\psi(x) = a_{ll}(x).q_l(x)$, e é

$$a_{11}\,a_{22}\ldots a_{n-1,n-1}(x)\,\psi(x) = f(x).$$

Logo virá

$$\left(\psi(x)\right)^n = f(x).\prod_{l=1}^{n-1} q_l(x).$$

Se, em particular, $\psi(x)$ for irredutível, $f(x)$ será uma potência de $\psi(x)$.

6) Regresso ao estudo da noção de semelhança - Tomemos o anel $\mathfrak{K}_n$ das matrizes quadradas, de grau n, com elementos de $\mathfrak{K}$, e consideremos como equivalentes as matrizes semelhantes. Na relação de equivalência assim definida, vamos procurar um tipo canónico para a representante de cada classe. Os resultados do § 4 deste Cap. mostram que a classe a que pertence a matriz M é definida pelos divisores elementares de $x - A$, em que A é uma matriz qualquer da referida classe. Dum modo preciso, o nosso objectivo é aqui estabelecer o seguinte

Teorema:- Dada a matriz A, se $x - A$ admite como divisores elementares dependentes de x os polinómios $\psi_1(x), \ldots, \psi_R(x)$ (1), A é semelhante à matriz

$$A' = \begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_R \end{pmatrix}, \qquad (6)$$

na qual A_l é de grau n_l, igual ao grau de $\psi_l(x)$, e tem o polinómio característico $f_l(x) = \psi_l(x)$. Além disso, se for $\psi_l(x) = x^{n_l} + \alpha_1 x^{n_l-1} + \ldots + \alpha_{n_l}$, pode supor-se

(1) Outros divisores elementares que existam são elementos de $\mathfrak{K}$, que podem, aliás, supor-se iguais a u.

$$A_l = \begin{pmatrix} 0 & u & 0 & \dots & 0 \\ 0 & 0 & u & \dots & 0 \\ \hline 0 & 0 & 0 & \dots & u \\ -\alpha_{n_l} & -\alpha_{n_l-1} & -\alpha_{n_l-2} & & -\alpha_1 \end{pmatrix}. \qquad (7)$$

Comecemos por verificar que, em (7), se tem $f_l(x) = x^{n_l} + \dots + \alpha_{n_l}$. Supondo $n_l = 1$, é, de facto, $A = (-\alpha_1)$, $f_l(x) = |x - A_l| = x + \alpha_1$. Imaginemos agora que a igualdade é válida para $n_l - 1$. Tem-se

$$|x-A_l| = x \begin{vmatrix} x & -u & 0 & \dots & 0 \\ 0 & x & -u & \dots & 0 \\ \hline \alpha_{n_l-1} & \alpha_{n_l-2} & \alpha_{n_l-3} & \dots & x+\alpha_1 \end{vmatrix} + (-1)^{n_l-1}\alpha_{n_l} \cdot \begin{vmatrix} -u & 0 & \dots & 0 & 0 \\ x & -u & \dots & 0 & 0 \\ \hline 0 & 0 & \dots & x & -u \end{vmatrix}.$$

O 1º determinante do 2º membro é de ordem $n_l - 1$, pelo que é igual, por hipótese, a $x^{n_l-1} + \alpha_1 x^{n_l-2} + \dots + \alpha_{n_l-1}$. O outro determinante do 2º membro, desenvolvido segundo os elementos da 1ª linha, dá imediatamente $(-1)^{n_l-1} u$. É, pois,

$$f_l(x) = |x-A_l| = x(x^{n_l-1} + \alpha_1 x^{n_l-2} + \dots + \alpha_{n_l-1}) + \alpha_{n_l} = x^{n_l} + \alpha_1 x^{n_l-1} + \dots + \alpha_{n_l}.$$

Para se reconhecer a relação $\psi_l(x) = f_l(x)$, basta ter em conta que na matriz $x - A_l$ se pode encontrar um determinante de ordem $n_l - 1$ que é igual a $(-1)^{n_l-1} u$. Vem, então, $\psi_l(x) = \frac{f_l(x)}{u} = f_l(x)$. A demonstração de que $\underline{A}$ é semelhante a $\underline{A}'$, de (6), resulta de se verificar que $x - A'$ tem os divisores elementares $\psi_l(x)$. Supõe-se, bem entendido, que é $\psi_l(x) \equiv 0 \left(\psi_{l-1}(x)\right)$. Em virtude de ser $\mathfrak{K}[x]$ um anel de ideais principais, existem, por hipótese, matrizes invertíveis $C_1, \dots, C_R$ e $D_1, \dots, D_R$, com elementos de $\mathfrak{K}[x]$, tais que

$$C_1(x-A_1)D_1 = \begin{pmatrix} u & 0 & \dots & 0 \\ 0 & u & \dots & 0 \\ \hline 0 & 0 & \dots & \psi_1(x) \end{pmatrix}, \dots, C_R(x-A_R)D_R = \begin{pmatrix} u & 0 & \dots & 0 \\ 0 & u & \dots & 0 \\ \hline 0 & 0 & \dots & \psi_R(x) \end{pmatrix},$$

$$\begin{pmatrix} C_1 & \dots & 0 \\ \hline 0 & \dots & C_R \end{pmatrix} \begin{pmatrix} x-A_1 & \dots & 0 \\ \hline 0 & \dots & x-A_R \end{pmatrix} \begin{pmatrix} D_1 & \dots & 0 \\ \hline 0 & \dots & D_R \end{pmatrix} = \begin{pmatrix} u & & & & \\ & \ddots & & & 0 \\ & & \psi_1 & & \\ & & & \ddots & \\ 0 & & & & u \\ & & & & & \ddots \\ & & & & & & \psi_R \end{pmatrix}.$$

Como $\{C_1, \dots, C_R\}$[1] e $\{D_1, \dots, D_R\}$ são invertíveis, os divisores elementares de $\{x - A_1, \dots, x - A_R\} = x - A'$ são os de $\{u, \dots, \psi_1, \dots, u, \dots, \psi_R\}$. Ora estes últimos são precisamente $u, \dots, u$ (repetido $n-k$ vezes) e $\psi_1, \dots, \psi_R$, como se quer. É claro que se tiveram em conta os factos de ser do grau n o produto $\psi_1 \dots \psi_R = f(x) = |x - A|$ e de ser $x - A$ uma matriz com n divisores elementares.

Façamos uma aplicação às matrizes nilpotentes. Supondo $A^r = 0$, o polinómio $\psi(x)$ dividirá x^r. Será $\psi(x) = x^q$, com $q \leqslant r$. Diz-se índice da matriz o menor expoente que a anula. Se r é o índice, tem-se necessàriamente $q = r$. Os divisores elementares de $x - A$, dependentes de x, são da forma x^{α_i}, ($i = 1, 2, \dots, k$), com $\alpha_i \leqslant q$ e $\sum \alpha_i = n$ = grau da matriz. A matriz (7) é da forma

$$A = \begin{pmatrix} 0 & u & 0 & \dots & 0 \\ \hline 0 & 0 & 0 & \dots & u \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Os expoentes α_i, que verificam as condições $0 < \alpha_1 \leqslant \alpha_2 \leqslant \dots \leqslant \alpha_R = q$, dizem-se índices de $\underline{A}$. É válido o seguinte

Teorema:- É condição necessária e suficiente, para que duas matrizes nilpotentes sejam semelhantes, que tenham os mesmos índices.

Suponhamos $q = 2$. Os divisores elementares de $\underline{A}$, dependentes de x, só podem ser x e x^2. Se é $\psi_l(x) = x$, a matriz $\underline{A}_l$ é nula; se se tem $\psi_l(x) = x^2$, a matriz $\underline{A}_l$ é da forma $A_l = \begin{pmatrix} 0 & u \\ 0 & 0 \end{pmatrix}$.

---

(1) Representaremos abreviadamente por $\{B_1, \dots, B_R\}$ uma matriz quadrada em escada diagonal, de matrizes quadradas diagonais $B_1, \dots, B_R$. Também se diz que a matriz é "soma directa dos B_l".

A matriz $\underline{A}$ é semelhante a

$$\left\{0\ ,\ldots,0\ ;\begin{pmatrix}0 & u\\ 0 & 0\end{pmatrix},\ \ldots\ ,\ \begin{pmatrix}0 & u\\ 0 & 0\end{pmatrix}\right\}. \qquad (8)$$

É evidente que a característica é dada pelo número de matrizes $\underline{A}_i$ do 2º grau. Quando duas matrizes do mesmo grau, $\underline{A}$ e $\underline{B}$, de índice 2, têm a mesma característica, em (8) figuram exactamente as mesmas matrizes do 2º grau e os mesmos zeros (matrizes do 1º grau), de modo que $\underline{A}$ e $\underline{B}$ são semelhantes. Pode enunciar-se o

Teorema:- É condição necessária e suficiente, para que duas matrizes nilpotentes do mesmo grau e de índice 2 sejam semelhantes, que tenham a mesma característica.

7) Representantes indecomponíveis duma classe - O tipo canónico (6) para a representante duma classe de matrizes semelhantes mostra que cada matriz é uma soma directa de matrizes da forma (7). Os $\underline{A}_i$ podem, porém, ser ainda semelhantes a matrizes somas directas de outras. É possível encontrar uma representante da forma

$$A' = \left\{D_1^{(1)},\ \ldots,\ D_1^{(h_1)}\ ;\ \ldots\ ;\ D_k^{(1)},\ \ldots,\ D_k^{(h_k)}\right\}, \qquad (9)$$

onde cada $D_j^{(i)}$ é da forma (7), mas não é semelhante a uma soma directa.

Comecemos por demonstrar o seguinte

Lema:- É condição necessária e suficiente, para que uma matriz $\underline{A}$ seja semelhante a $\{G,H\}$, onde G e H são matrizes cujos polinómios mínimos, $g(x)$ e $h(x)$, são primos entre si, que o seu polinómio mínimo $\psi(x)$ seja da forma $\psi(x) = g(x).h(x)$.

Se $\underline{A}$ é semelhante a $\{G,H\}$, com $g(x)$ e $h(x)$ primos entre si, pondo $\psi(x) = g(x).h(x)$, tem-se, para $A' = \{G,H\}$,

$$\psi(A') = g(A').h(A') = \{g(G),g(H)\}.\{h(G),h(H)\} =$$

$$= \{0,g(H)\}.\{h(G),0\} = 0,$$

o que prova ser $\psi(x)$ divisível pelo polinómio mínimo de $\underline{A}$.

Por outro lado, se $\psi_0(x)$ é esse polinómio mínimo, tem-se

$$\psi_0(A) = \psi_0(A') = \left(\psi_0(G),\ \psi_0(H)\right) = 0,$$

o que dá $\psi_0(G) = 0$, $\psi_0(H) = 0$. Daqui conclui-se que $\psi_0(x)$ é divisível por $g(x)$ e $h(x)$, e, portanto, pelo seu produto. É, assim, $\psi_0(x) = \psi(x) = g(x).h(x)$.

Inversamente, se $\psi(x) = g(x).h(x)$, com $\underline{g}$ e $\underline{h}$ primos entre si, é polinómio mínimo duma matriz $\underline{A}$, designemos com $\psi_1(x),\ldots,$ $,\ \psi_k(x) = \psi(x)$ os divisores elementares de $\underline{A}$ dependentes de $\underline{x}$ e ponhamos

$$\text{m.d.c.}\left(\psi_j(x),g(x)\right) = g_j(x),$$
$$\text{m.d.c.}\left(\psi_j(x),h(x)\right) = h_j(x).$$

Chamando G_j e H_j a duas matrizes da forma (7), de polinómios mínimos g_j e h_j, a matriz $\{G_j,\ H_j\}$ tem o polinómio mínimo $g_j(x).h_j(x)$, visto que os factores deste produto são primos entre si. Mas é $g_j(x).h_j(x) = \psi_j(x)$, pois que $\psi_j(x)$ divide $\psi(x)$ e os factores indecomponíveis de ψ_j hão-de figurar em $g(x)$, constituindo $g_j(x)$, ou em $h(x)$, constituindo $h_j(x)$. Se agora considerarmos as matrizes

$$G = \{G_1,\ \ldots,\ G_k\},\qquad H = \{H_1,\ \ldots,\ H_k\},$$

sabemos que os divisores elementares de $x - G$ são $g_1(x),\ldots$ $\ldots,\ g_k(x)$ e os de $x - H$ são $h_1(x),\ \ldots,\ h_k(x)$. O polinómio mínimo de G é $g_k(x) = g(x)$ e o de H é $h_k(x) = h(x)$. A matriz $\{G,H\}$ tem o polinómio mínimo $g(x).h(x)$. Por hipótese, $\underline{A}$ é semelhante a $A' = \{A_1,\ldots,\ A_k\}$, onde A_j, da forma (7), tem o polinómio mínimo $\psi_j(x)$. A matriz $\{G_j,H_j\}$ tem o mesmo polinómio mínimo que A_j e tem o polinómio característico

$$\left|x - \{G_j,H_j\}\right| = \left|x - G_j\right|.\left|x - H_j\right| = \psi_j(x).$$

A_j é, pois, semelhante a $\{G_j,\ H_j\}$, e $\underline{A}'$, ou $\underline{A}$, é semelhante a

$$\{G_1,\ H_1;\ \ldots\ ;\ G_k,\ H_k\}. \qquad (10)$$

Seja P_{k_j} (como no tomo anterior, pgs. 21 e 22) a matriz de grau n = grau de $\underline{B}$, obtida da matriz unidade trocando as linhas

de ordem k e j. Vê-se imediatamente que é

$$P_{R_j} = P_{R_j}^{-1}, \qquad P_{R_j} B = B', \qquad B\, P_{R_j} = B'',$$

onde B' resulta de B por troca das linhas de ordem k e j e B'' resulta de B por troca das colunas k e j. A matriz

$$P_{R_j} B\, P_{R_j}^{-1} = P_{R_j} B\, P_{R_j}$$

é semelhante a B e resulta desta por uma certa troca de linhas e a mesma troca de colunas. Dum modo geral, duas matrizes B e B'', que resultam uma da outra pelas mesmas trocas de linhas e de colunas são semelhantes. A matriz (10) é semelhante a

$$\{G_1, \ldots, G_R; H_1, \ldots, H_R\} = \{G, H\},$$

de modo que A, como se quer, é semelhante a $\{G, H\}$.

Teorema:- É condição necessária e suficiente, para que uma matriz A seja semelhante a $\{R, S\}$, onde R e S são matrizes cujos polinómios característicos, $\rho(x)$ e $\sigma(x)$, são primos entre si, que o seu polinómio característico $f(x)$ seja da forma $f(x) = \rho(x).\sigma(x)$. A condição é necessária, porque, se A é semelhante a $\{R, S\}$, o polinómio característico $f(x) = |x - A|$ pode escrever-se

$$f(x) = |x - A| = |x - R|.\,|x - S| = \rho(x).\sigma(x).$$

Inversamente, se A tem o polinómio característico $f(x) = \rho(x).\sigma(x)$, com ρ e σ primos entre si, designemos com $\psi(x)$ o polinómio mínimo de A e ponhamos

$$\text{m.d.c.}\,(\psi(x), \rho(x)) = g(x),$$
$$\text{m.d.c.}\,(\psi(x), \sigma(x)) = h(x).$$

Como $\psi(x)$ divide $f(x)$, tem-se $\psi(x) = g(x).h(x)$. Nessas condições, em virtude do lema, A é semelhante a $\{G, H\}$. E sabe-se que se tem

$$|x - G| = g_1(x) \ldots g_R(x),$$
$$|x - H| = h_1(x) \ldots h_R(x).$$

Será, pois,

$$|x - A| = |x - G|.\,|x - H| = \Pi\, g_l(x).\Pi\, h_l(x) = f(x) = \rho(x).\sigma(x)$$

Como cada $g_l(x)$ divide $g(x)$, dividirá também $\rho(x)$. Nenhum $g_l(x)$ poderá figurar em $\sigma(x)$ e nenhum $h_l(x)$ poderá figurar em $\rho(x)$. Ter-se-á

$$\Pi\, g_l(x) = \rho(x), \qquad \Pi\, h_l(x) = \sigma(x).$$

O teorema fica demonstrado, pondo $R = G$, $S = H$.

Para se chegar agora à forma canónica desejada (9), baseamo-nos no seguinte

Teorema:- É condição necessária e suficiente, para que uma matriz da forma (7) não seja semelhante a uma soma directa (isto é, seja indecomponível), que o seu polinómio mínimo $\psi(x) = f(x)$ seja uma potência dum polinómio primo normado. Se este teorema for válido, então basta encontrar uma matriz A', da forma (9), semelhante da matriz A, de tal modo que os $D_j^{(l)}$ tenham como polinómio mínimo determinadas potências dos factores primos da decomposição do polinómio característico de A. Isso consegue-se fàcilmente, raciocinando como vai ver-se. Dada a matriz A, consideremos a decomposição em factores primos normados

$$f(x) = |x - A| = \left(p_1(x)\right)^{\sigma_1} \ldots \left(p_r(x)\right)^{\sigma_r}. \qquad (11)$$

A é semelhante à matriz

$$\{R_1, \ldots, R_r\}, \qquad (12)$$

onde R_l tem o polinómio característico $\left(p_l(x)\right)^{\sigma_l}$. Os divisores elementares de $x - R_l$ serão

$$\left(p_l(x)\right)^{\alpha_{l1}}, \ldots, \left(p_l(x)\right)^{\alpha_{lq_l}}, \qquad (\Sigma \alpha_{lj} = \sigma_l),$$

e R_l será semelhante a

$$\left\{D_l^{(1)}, \ldots, D_l^{(q_l)}\right\},$$

onde $D_l^{(k)}$, da forma (7), tem o polinómio mínimo e característi-

co $\left(p_t(x)\right)^{\alpha_{ik}}$. A matriz $\underline{A}$ será, pois, semelhante a

$$\left\{D_1^{(1)}, \ldots, D_1^{(\rho_1)}; \ldots; D_r^{(1)}, \ldots, D_r^{(\rho_r)}\right\},$$

que tem precisamente a forma desejada (9).

Resta demonstrar o teorema. Seja $\underline{M}$ uma matriz da forma (7), não decomponível. O seu polinómio mínimo ou característico não pode decompor-se num produto de polinómios primos, pois, se assim fosse, $\underline{M}$ seria decomponível. Inversamente, se $\underline{M}$, da forma (7), tem o polinómio mínimo $\left(p(x)\right)^{\lambda}$, onde $p(x)$ é um polinómio primo normado, não pode ser semelhante a $\{G, H\}$, visto que, se o fosse, ter-se-ia

$$|x-M| = |x-G| \cdot |x-H| = \left[p(x)\right]^{\alpha} \cdot \left[p(x)\right]^{\beta},$$

onde $|x-G| = \left[p(x)\right]^{\alpha}$, $|x-H| = \left[p(x)\right]^{\beta}$, $\alpha+\beta=\lambda$. Supondo, por ex., $\beta \geqslant \alpha$, tem-se

$$\left(p(M)\right)^{\beta} = \{p(G)^{\beta}, p(H)^{\beta}\} = 0,$$

de modo que $\beta = \lambda$. Será $\alpha = 0$, a matriz $\underline{G}$ não existe e $\underline{M}$ é indecomponível.

Poder-se-ia, dada a matriz $\underline{A}$, considerar o seu polinómio mínimo normado $\psi(x)$, que se decomporia em polinómios primos normados:

$$\psi(x) = \left(q_1(x)\right)^{\tau_1} \ldots \left(q_s(x)\right)^{\tau_s}.$$

$\underline{A}$ seria ainda semelhante a uma matriz

$$\{S_1, \ldots, S_s\}, \qquad (12')$$

onde S_j teria o polinómio mínimo $\left(q_j(x)\right)^{\tau_j}$. Convém, todavia, observar que, tanto aqui como no raciocínio anterior, as matrizes S_j (ou R_l) não são ainda, geralmente, da forma (7). Para prosseguirmos na decomposição, tornar-se-ia necessário, do mesmo modo, recorrer agora aos divisores elementares de S_j. O conhecimento destes é que permitiria encontrar uma matriz semelhante a S_j, soma directa de matrizes da forma (7).

Façamos uma aplicação. Seja $A = E$ uma matriz idempotente. Tendo-se $E^2 = E$, a equação $x^2 - x = 0$ é satisfeita pela matriz,

de modo que o polinómio mínimo só pode ser x, $x-u$ ou x^2-x. Excluindo os casos de ser $E = 0$ ou $E = u$, tem-se $\psi(x) = x^2-x$. Mas, sendo $\psi(x) = x(x-u)$, a matriz (12') tem a forma $\{S_1, S_2\}$, onde S_1 e S_2 possuem os polinómios mínimos respectivos x e $x-u$. Pelo facto de S_1 e S_2 serem idempotentes, conclui-se que S_1 é semelhante a $\{0, \ldots, 0\}$ e S_2 semelhante a $\{u, \ldots, u\}$, de sorte que $\underline{E}$ é semelhante a $\{0, \ldots, 0; u, \ldots, u\}$.

Se quisermos utilizar o polinómio característico de $\underline{E}$, faremos

$$f(x) = \psi_1(x) \ldots \psi_k(x) = x^{\sigma_1}(x-u)^{\sigma_2}; \qquad (\sigma_1 + \sigma_2 = n),$$

onde $\underline{n}$ é o grau da matriz. Na decomposição (11) deverá pôr-se

$$p_1(x) = x, \qquad p_2(x) = x-u, \qquad (r = 2).$$

A forma (12) para à matriz semelhante de $\underline{E}$ escreve-se

$$\{R_1, R_2\}, \quad \text{com} \quad |x-R_1| = x^{\sigma_1}, \quad |x-R_2| = (x-u)^{\sigma_2}.$$

Os divisores elementares de $x-R_1$ são $x^{\alpha_1}, \ldots, x^{\alpha_r}$, com $\sum \alpha_l = \sigma_1$, de sorte que R_1 é semelhante a $\{D_1^{(1)}, \ldots, D_1^{(r)}\}$. Cada $D_1^{(l)}$ é idempotente. Tem-se $|x-D_1^{(l)}| = x^{\alpha_l}$. Como o polinómio mínimo duma matriz idempotente é do 1º ou do 2º grau, ou é $\alpha_l = 1$, ou $\alpha_l = 2$. Se fosse $\alpha_l = 2$, ter-se-ia

$$D_1^{(l)} = \begin{pmatrix} 0 & u \\ 0 & 0 \end{pmatrix}.$$

Esta matriz não é, porém, idempotente. Assim, ter-se-á

$$|x-D_1^{(l)}| = x, \qquad D_1^{(l)} = 0, \qquad (i = 1, 2, \ldots, r).$$

Um raciocínio análogo mostra que $\underline{R_2}$ é semelhante a

$$\{D_2^{(1)}, \ldots, D_2^{(t)}\}, \text{ com } |x-D_2^{(l)}| = x-u, \quad D_2^{(t)} = u,$$

visto que, pôr $|x-D_2^{(l)}| = (x-u)^2$ daria uma das igualdades

$$(x-u)^2 = x^2-2ux+u = x, \; x-u, \; x^2-x.$$

Fica demonstrado, assim, que uma matriz idempotente é semelhan-

te a uma matriz $\{o, \dots, o ; u, \dots, u\}$ e conclui-se o

Teorema:- É condição necessária e suficiente, para que duas matrizes idempotentes do mesmo grau sejam semelhantes, que tenham a mesma característica.

Usaremos adiante este outro

Teorema:- A soma de duas matrizes idempotentes ortogonais tem uma característica igual à soma das características. Sejam E e F as matrizes idempotentes do grau n tais que $EF = FE = 0$. Se r e r são as respectivas características e usarmos o sinal $\approx$ para significar semelhança, temos

$$E \approx \begin{pmatrix} 0 & 0 \\ 0 & U_{r_1} \end{pmatrix}, \qquad F \approx \begin{pmatrix} U_{r_2} & 0 \\ 0 & 0 \end{pmatrix},$$

onde U designa matriz unidade. Supondo E, por ex., de característica n, E será invertível e ter-se-á $E E^{-1} = U$, donde se conclui

$$E E E^{-1} = E E^{-1} = U = E U = E.$$

Nesse caso será $F = 0$ e o teorema está demonstrado. Admitindo, porém, que r_1 e r_2 são diferentes de n, suponhamos que é

$$P E P^{-1} = \begin{pmatrix} 0 & 0 \\ 0 & U_{r_1} \end{pmatrix}, \qquad P F P^{-1} = \begin{pmatrix} F_1 & F_2 \\ F_3 & F_4 \end{pmatrix},$$

onde F_1 é uma matriz quadrada de grau $n - r_1$. Como se tem

$$P E P^{-1} . P F P^{-1} = P E F P^{-1} = 0 = \begin{pmatrix} 0 & 0 \\ F_3 & F_4 \end{pmatrix},$$

vê-se que é $F_3 = 0$, $F_4 = 0$. A característica r_2, de F, não pode exceder $n - r_1$. Sendo ainda

$$P F P^{-1} . P E P^{-1} = 0 = \begin{pmatrix} F_1 & F_2 \\ F_3 & F_4 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & U_{r_1} \end{pmatrix} = \begin{pmatrix} 0 & F_2 \\ 0 & 0 \end{pmatrix},$$

deverá ter-se $F_2 = 0$, de sorte que as duas matrizes ortogonais podem supor-se da forma

$$E = \begin{pmatrix} 0 & 0 \\ 0 & U_{r_1} \end{pmatrix}, \qquad F = \begin{pmatrix} F_1 & 0 \\ 0 & 0 \end{pmatrix},$$

onde F_1 é de grau $n - r_1$ e tem a característica $r_2 \equiv n - r_1$. Designemos por B_1 uma matriz invertível de grau $n - r_1$ e escrevamos as igualdades

$$\begin{pmatrix} B_1 & 0 \\ 0 & U_{r_1} \end{pmatrix} \begin{pmatrix} F_1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} B_1^{-1} & 0 \\ 0 & U_{r_1} \end{pmatrix} = \begin{pmatrix} B_1 F_1 B_1^{-1} & 0 \\ 0 & 0 \end{pmatrix}, \qquad (13)$$

$$\begin{pmatrix} B_1 & 0 \\ 0 & U_{r_2} \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & U_{r_1} \end{pmatrix} \begin{pmatrix} B_1^{-1} & 0 \\ 0 & U_{r_1} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & U_{r_1} \end{pmatrix}.$$

Escolhendo B_1 de modo que (13) se reduza à forma

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & U_{r_2} & 0 \\ 0 & 0 & 0_{r_1} \end{pmatrix},$$

na qual 0_{r_1} significa a matriz quadrada nula de ordem r_1, obtem-se

$$\begin{pmatrix} B_1 & 0 \\ 0 & U_{r_1} \end{pmatrix} \left[\begin{pmatrix} F_1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & U_{r_1} \end{pmatrix} \right] \begin{pmatrix} B_1^{-1} & 0 \\ 0 & U_{r_1} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & U_{r_2} & 0 \\ 0 & 0 & U_{r_1} \end{pmatrix} = \Delta .$$

Em suma: pondo $\begin{pmatrix} B_1 & 0 \\ 0 & U_{r_1} \end{pmatrix} = Q$, vê-se que as matrizes iniciais E e F se reduzem conforme as relações

$$Q P^{-1} F P^{-1} Q^{-1} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & U_{r_2} & 0 \\ 0 & 0 & 0_{r_1} \end{pmatrix}, \qquad Q P E P^{-1} Q^{-1} = \begin{pmatrix} 0 & 0 \\ 0 & U_{r_1} \end{pmatrix},$$

$$Q\,P\,(F+E)\,(Q\,P)^{-1} = \Delta\,,$$

o que demonstra o teorema.

Se G for uma nova matriz idempotente, ortogonal às duas primeiras, tem-se também $G(E+F) = (E+F)G = 0$. Nesse caso, a característica r_3, de G, verifica a desigualdade $r_3 \leqq n-(r_1+r_2)$. Supondo

$$R\,E\,R^{-1} = \begin{pmatrix} 0 & 0 \\ 0 & U_{r_1} \end{pmatrix}, \qquad R\,F\,R^{-1} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & U_{r_2} & 0 \\ 0 & 0 & 0_{r_1} \end{pmatrix},$$

$$R(E+F)R^{-1} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & U_{r_2} & 0 \\ 0 & 0 & U_{r_1} \end{pmatrix}, \qquad R\,G\,R^{-1} = \begin{pmatrix} G_1 & 0 \\ 0 & 0 \end{pmatrix},$$

onde G_1 é de grau $n-(r_1+r_2)$ e tem a característica r_3, cheja-se a encontrar uma matriz invertível S tal que

$$S\,E\,S^{-1} = \begin{pmatrix} 0 & 0 \\ 0 & U_{r_1} \end{pmatrix}, \qquad S\,F\,S^{-1} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & U_{r_2} & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$S\,G\,S^{-1} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & U_{r_3} & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad S(E+F+G)S^{-1} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & U_{r_3} & 0 & 0 \\ 0 & 0 & U_{r_2} & 0 \\ 0 & 0 & 0 & U_{r_1} \end{pmatrix}.$$

Vêem-se claramente as condições em que o processo pode continuar-se.

+

\+ +

Capítulo VI

Álgebras e matrizes

1) Definição duma álgebra sobre um corpo - O anel $\mathfrak{A}_n$, de matrizes com elementos dum corpo comutativo $\mathfrak{K}$, constitui uma álgebra sobre $\mathfrak{K}$. É uma álgebra extremamente importante, que, servindo-nos de modelo no estudo das álgebras, permite, por outro lado, recorrendo à noção de isomorfismo, o enunciado de muitas proposições gerais. Vamos proceder a uma construção abstracta das álgebras, o que faremos com certo pormenor.

Seja $\mathfrak{M} = \{0, v, w, \ldots, e_1, \ldots, e_n\}$ um módulo relativo a um anel $\mathfrak{r} = \{u, \alpha, \beta, \ldots, \lambda, \mu, \ldots\}$. Tem-se

$$\alpha v \in \mathfrak{M}, \qquad \alpha(v+w) = \alpha v + \alpha w\,, \tag{1}$$

$$(\alpha+\beta)v = \alpha v + \beta v\,, \quad \alpha\,\beta.v = \alpha.\,\beta v\,. \tag{2}$$

Vamos introduzir em $\mathfrak{M}$ um produto associativo

$$v\,w \in \mathfrak{M}, \qquad v\,w.e_i = v.w\,e_i\,; \tag{3}$$

e pôr também a hipótese seguinte:

$$\lambda(v\,w) = \lambda v.w = v.\lambda w\,. \tag{4}$$

Decompondo $\mathfrak{M}$ sob a forma $\mathfrak{M} = \mathfrak{M}' + \mathfrak{M}''$, a parte $\mathfrak{M}''$, para a qual u é operador unitário (§ 1, Cap. IV) é um módulo no qual é válida a noção de produto introduzida em (3): $uv.uw = u(v.uw) = u(u.vw) = u.vw$. Em suma: em $\mathfrak{M}''$ verificam-se (1), (2), (3) e (4).

É de especial interesse o caso em que $\mathfrak{r}$ se reduz a um corpo comutativo $\mathfrak{K}$. A comutatividade neste último permite que se possa escrever

$$\alpha v = v\alpha\,. \tag{5}$$

As igualdades (4) podem substituir-se pelas seguintes:

$$\lambda(vw) = \lambda v.w\,, \qquad (vw)\lambda = v.w\,\lambda\,. \tag{6}$$

De facto, tira-se daqui, tendo em conta (5)

$$\lambda(vw) = \lambda v.w = (vw)\lambda = v.w\lambda = v.\lambda w .$$

Inversamente, estabelece-se (6), a partir de (4) e (5), pois

$$\lambda(vw) = \lambda v.w , \qquad \lambda(vw) = (vw)\lambda = v.\lambda w = v.w\lambda .$$

Diz-se uma <u>álgebra $\mathcal{U}$ [ou $\mathcal{U}/\mathcal{K}$] sobre o corpo $\mathcal{K}$</u> um conjunto em que se verificam os seguintes postulados:

I) $\mathcal{U}$ é um anel [$\mathcal{U}$ é, então, um módulo para o qual valem (3) e as propriedades distributivas];

II) $\mathcal{U}$ é um módulo relativo a $\mathcal{K}$ [em $\mathcal{U}$ ficam valendo as igualdades (1) e (2)];

III) vale a igualdade $\lambda v = v\lambda$ [trata-se de (5), que provém da comutatividade de $\mathcal{K}$];

IV) valem as igualdades $\lambda(vw) = \lambda v.w = v.\lambda w$ [trata-se de (4) ou de (6)];

V) vale a igualdade $ua = au = a$, $(a \in \mathcal{U})$.

Se a álgebra $\mathcal{U}$ é um módulo finito de ordem <u>n</u>, diz-se que se tem uma <u>álgebra linear associativa finita de ordem n</u> ou <u>um sistema hiper-complexo de ordem n</u>. Introduziremos, então, indiferentemente, os símbolos $\mathcal{U}$ ou $\mathcal{L}$ para representar o sistema. Vamos dar alguns exemplos.

1º)- Um corpo comutativo $\mathcal{K}$ é uma álgebra finita sobre $\mathcal{K}$. Qualquer elemento de $\mathcal{K}$ não nulo constitui uma base da álgebra. Uma ampliação finita, Ω, de $\mathcal{K}$, é igualmente uma álgebra sobre $\mathcal{K}$, com uma ordem igual à ordem ou grau de Ω.

2º)- Dado $\mathcal{K}$, tomemos o grupo abeliano $\mathcal{M}$ constituido pelos elementos da forma $v = (\alpha_1, \ldots, \alpha_n)$, com $\alpha_i \in \mathcal{K}$. A relação $(\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n) = (\alpha_1+\beta_1, \ldots, \alpha_n+\beta_n)$ define o preceito de soma em $\mathcal{M}$. Se tomarmos um elemento $\alpha \in \mathcal{K}$, escreveremos $\alpha v = (\alpha\alpha_1, \ldots, \alpha\alpha_n)$, onde $\alpha\alpha_i$ é o produto considerado em $\mathcal{K}$. Sabemos que $\mathcal{M}$ verifica os postulados II), III) e V). Para se introduzir em $\mathcal{M}$ um produto associativo e distributivo, que o torne num anel $\mathcal{L}$, ponhamos

$$e_1 = (u, o, \ldots, o), \ldots, e_n = (o, \ldots, u), \quad e_i e_k = \sum_{j=1}^{n} a_{ikj} e_j . \qquad (7)$$

O elemento <u>v</u> pode tomar a forma $v = \alpha_1 e_1 + \cdots + \alpha_n e_n$. Admitindo a distributividade necessária para que $\mathcal{L}$ seja um anel, devemos exigir aos <u>n^3</u> coeficientes a_{ikj} que seja satisfeita a propriedade associativa para os <u>e_i</u>. Isso implicará as condições

$$\alpha e_i . \beta e_k = \alpha\beta e_i e_k , \qquad \text{(pròpriamente uma definição)},$$

$$\sum_j a_{ikj} e_j . e_m = \sum_j a_{ikj} e_j e_m = \sum_l a_{kml} e_i e_l .$$

Tiram-se daqui as igualdades a verificar pelos a_{ikj}:

$$\sum_j a_{ikj} a_{jmn} = \sum_j a_{kmj} a_{ijn} .$$

O postulado I) é agora verificado. Quanto a IV), basta observar que se tem

$$\lambda(\alpha e_i . \beta e_j) = \lambda(\alpha\beta . e_i e_j) = \lambda\alpha\beta e_i e_j = \lambda\alpha e_i . \beta e_j = \alpha e_i . \lambda\beta e_j .$$

Se supusermos $e_i e_k = 0$, se $i \neq k$, e $e_i^2 = e_i$, obtem-se simplesmente

$$(\alpha_1, \ldots, \alpha_n).(\beta_1, \ldots, \beta_n) = (\alpha_1\beta_1, \ldots, \alpha_n\beta_n).$$

O sistema $\mathcal{L}$ tem, neste caso, elemento um = U, para o qual vale

$$U = e_1 + \cdots + e_n .$$

Como $\mathcal{L}$ é anel, pode escrever-se

$$\mathcal{L} = e_1\mathcal{L} + \cdots + e_n\mathcal{L} = \mathfrak{N}_1 + \cdots + \mathfrak{N}_n , \quad (\mathfrak{N}_i = e_i\mathcal{L}).$$

Sob esta forma de escrita, sugere-se indagar se $\mathcal{L}$, considerado como módulo relativamente a si mesmo, ainda admite os geradores independentes $e_1, \ldots, e_n$. Ora, notando as relações $e_i^2 = e_i$, $e_i(e_i - U) = 0$, vê-se que a resposta é negativa. $\mathcal{L}$ aparece como soma directa de grupos cíclicos, cada um dos quais com uma base que se anula para elementos não nulos de $\mathcal{L}$. Tais elementos constituem um ideal direito. Se $\mathcal{R}_1$ é o ideal direito que anula e_1, vê-se que se tem

$$\mathcal{R}_1 \supseteq e_2\mathcal{L} + \cdots + e_n\mathcal{L} .$$

Inversamente, se $\beta_1 \in \mathcal{L}_1$, pondo

$$\beta_1 = U\beta_1 = e_1\beta_1 + \cdots + e_n\beta_1 = e_2\beta_1 + \cdots + e_n\beta_1 ,$$

conclui-se ser $\beta_1 \in e_2\mathcal{G} + \cdots + e_n\mathcal{G}$, e, portanto, $\mathcal{L}_1 = e_2\mathcal{G} + \cdots + e_n\mathcal{G}$.

3º)- Consideremos um grupo $\mathcal{G}$ com um número finito, N, de elementos. Supondo $g_l \in \mathcal{G}$; $x_l, y_j \in \mathcal{A}$; ponhamos $X = (x_1 g_1, \ldots, x_N g_N)$, $Y = (y_1 g_1, \ldots, y_N g_N)$, $X+Y = ((x_1+y_1)g_1, \ldots, (x_N+y_N)g_N)$, $\alpha X = (\alpha x_1 \cdot g_1, \ldots, \alpha x_N \cdot g_N)$, $(\alpha \in \mathcal{A})$. As igualdades (1) e (2) têm lugar. No módulo $\mathcal{M}$, constituido pelos elementos X, podemos introduzir o simbolismo seguinte:

$$(x_1 g_1, \ldots, 0 \cdot g_N) = x_1 g_1 ; \quad (0 \cdot g_1, x_2 g_2, \ldots, 0 \cdot g_N) = x_2 g_2 ; \ \ldots ,$$

$$X = (x_1 g_1, \ldots, x_N g_N) = x_1 g_1 + \cdots + x_N g_N .$$

Este simbolismo é apropriado para a definição do produto em $\mathcal{M}$. Começaremos por escrever $x_l g_l \cdot x_j g_j = x_l x_j \cdot g_l g_j = z_k g_k$, onde $x_l x_j = z_k$ é calculado em $\mathcal{A}$ e $g_l g_j = g_k$ é determinado em $\mathcal{G}$. Em seguida exige-se a distributividade esquerda e direita. Por fim, ser-se-á levado à regra geral de produto, pondo

$$X \cdot Y = \sum_l x_l g_l \cdot \sum_j x_j g_j = \sum_{i,j} x_l x_j \cdot g_l g_j .$$

A propriedade associativa do produto resulta imediatamente dos factos de ela ter lugar em $\mathcal{A}$ e em $\mathcal{G}$.

A álgebra finita $\mathcal{A}$, assim introduzida, diz-se uma <u>álgebra do grupo</u> ou um <u>sistema hiper-complexo do grupo</u>. A base de $\mathcal{A}$ é constituida pelos elementos $ug_1, \ldots, ug_N$, ou, simplesmente, $g_1, \ldots, g_N$.

4º)- Sejam os símbolos <u>1</u> e <u>i</u>, e ponhamos

$$1.1 = 1, \quad i.1 = i,$$
$$1.i = i, \quad i.i = -u.1, \quad (u = \text{elemento um de } \mathcal{A}).$$

Por meio deste quadro associativo, define-se, dado um corpo qualquer, um sistema hiper-complexo de 2ª ordem. Se o corpo é o dos números reais, o anel obtido é o dos <u>números complexos</u> da Álgebra elementar. Se o corpo é o dos números racionais, o

anel obtido é o <u>anel dos números de Gauss</u>.

Este último também constitui um corpo. De facto, supondo que <u>a</u> e <u>b</u> são números racionais não simultâneamente nulos, ponhamos

$$(a.1 + b.i)(x.1 + y.i) = c.1 + d.i .$$

Efectuando o produto indicado no primeiro membro e igualando os coeficientes de <u>1</u> e de <u>i</u>, tem-se

$$ax - by = c$$
$$bx + ay = d .$$

Como $a^2 + b^2 \neq 0$, este sistema admite uma e uma só solução constituida por números racionais, como se deseja.

5º)- Os <u>quaterniões</u> constituem um sistema hiper-complexo de <u>4ª ordem</u> relativamente ao corpo dos números reais. Se i, j, k, l são os elementos base, o produto associativo destes elementos é introduzido, relativamente a um corpo qualquer, segundo a tabela

$i.i = i$,	$j.i = j$,	$k.i = k$,	$l.i = l$,
$i.j = j$,	$j.j = -u.i$,	$k.j = -u.l$,	$l.j = k$,
$i.k = k$,	$j.k = l$,	$k.k = -u.i$,	$l.k = -u.j$,
$i.l = l$,	$j.l = -u.k$,	$k.l = j$,	$l.l = -u.i$,

onde se pode fazer $u = 1$,(1) no caso vulgar dos quaterniões. Verifiquemos, por ex., a igualdade

$$lj.l = l.jl .$$

O primeiro membro é igual a $kl = j$. O segundo membro é também igual a j: $l(-u.k) = -u.lk = -u(-u.j) = (-u.-u)j = j$, pois $-u.-u = -(-u.u) = -(-u) = u$.

Os quaterniões constituem um corpo. O elemento <u>i</u> é, de facto, o elemento um. A existência do inverso dum quarténio $a.i + b.j + c.k + d.l$ vê-se do modo seguinte. Tomemos o elemento

(1) Trata-se da letra <u>l</u> e não do número um.

$$Q = \frac{a}{a^2+b^2+c^2+d^2}\cdot i - \frac{b}{a^2+b^2+c^2+d^2}\cdot j - \frac{c}{a^2+b^2+c^2+d^2}\cdot k -$$

$$- \frac{d}{a^2+b^2+c^2+d^2}\cdot l \ ,$$

que existe sempre que o quatérnio não é o elemento nulo (o corpo fundamental é agora o corpo dos números reais). Fàcilmente se vê que o produto $Q.(ai + bj + ck + dl)$ é igual a i. A afirmação subsiste para um corpo qualquer, quando este satisfaz à única condição de não poder ser o elemento nulo a soma de quatro quadrados de elementos não todos nulos.

6º)- Um exemplo importante de sistema hiper-complexo é formado pelo anel completo, M, das matrizes quadradas dum corpo comutativo, como já tínhamos dito. A característica ou ordem do sistema é n^2.

Dados estes exemplos, podemos indicar o processo geral da construção duma álgebra associativa finita, à custa de n símbolos independentes e_i. Põe-se

$$e_i e_j = \sum_k a_{ijk} e_k \ , \qquad (a_{ijk} \in \mathfrak{K}) \ ,$$

$$\lambda e_i . \mu e_j = \lambda \mu . e_i e_j = \sum_k \lambda \mu a_{ijk} e_k \ .$$

Têm-se em seguida em conta as propriedades distributivas e restringem-se os n^3 coeficientes a_{ijk} pela condição da associatividade dos produtos dos e_i. O módulo finito $\sum \lambda_i e_i$ (onde se subentende $ue_i = e_i$) constitui uma álgebra finita $\mathfrak{G} = \mathfrak{O}/\mathfrak{K}$. A ordem ou característica da álgebra é n.

Uma álgebra pode definir-se ainda do modo seguinte:

I) é um módulo finito relativo a um corpo comutativo $\mathfrak{K}$, cujos elementos têm a forma:

$$\lambda_1 e_1 + \cdots + \lambda_n e_n = e_1 \lambda_1 + \cdots + e_n \lambda_n , \qquad (\lambda_i \in \mathfrak{K}) \ ;$$

II) é um anel com o domínio operatório $\mathfrak{K}$:

$$\lambda(ab) = \lambda a.b = a.\lambda b \ , \qquad (a,b \in \text{à álgebra}).$$

Considerada a álgebra como grupo com operadores, há dois domínios operatórios: o corpo fundamental e a álgebra.

No geral, contràriamente ao que sucede em quase todos os exemplos do § anterior, a álgebra finita $\mathfrak{G}$ não tem elemento um = U. Obtem-se uma álgebra $\mathfrak{G}'$ com elemento um, ampliação de $\mathfrak{G}$, introduzindo U por meio das igualdades $U\,U = U$, $U\,e_i = e_i U = e_i$ e tomando os símbolos base $(e_1, \ldots, e_n; U)$. Se U existe, os elementos λU, com $\lambda \in \mathfrak{K}$, constituem um corpo isomorfo de $\mathfrak{K}$, que pode tomar-se como corpo fundamental. Então, os dois domínios operatórios da álgebra pertencem à álgebra.

Duas álgebras, como anéis, podem ser isomorfas. Se admitem o mesmo corpo fundamental e se o isomorfismo é operatório relativamente a esse corpo, dizem-se equivalentes. As considerações deste Cap.e dos seguintes respeitam a álgebras finitas.

2) A representação regular duma álgebra finita - Tomemos um sistema hiper-complexo $\mathfrak{G}$, de ordem n, de corpo fundamental $\mathfrak{K}$, e designemos com a, b, ... os elementos de $\mathfrak{G}$. Se for

$$a\,e_1 = \sum_j e_j \alpha_{j1}, \ldots, \ a\,e_n = \sum_j e_j \alpha_{jn}, \qquad (\alpha_{jk} \in \mathfrak{K}), \qquad (8)$$

faz-se corresponder a cada elemento a uma matriz $A = (\alpha_{ik})$. Em virtude de terem lugar as relações

$$(a+b)e_i = a\,e_i + b\,e_i = \sum_j e_j (\alpha_{ji} + \beta_{ji}) \ ,$$

$$ab.e_i = a.be_i = a \sum_k e_k \beta_{ki} = \sum_k a e_k . \beta_{ki} =$$

$$= \sum_k \Big(\sum_j e_j \alpha_{jk}\Big)\beta_{ki} = \sum_j e_j \Big(\sum_k \alpha_{jk} \beta_{ki}\Big) \ ,$$

$$\lambda a.e_i = \lambda(a\,e_i) = \lambda \sum_j e_j \alpha_{ji} = \sum_j e_j . \lambda \alpha_{ji} \ ,$$

nas quais $\lambda \in \mathfrak{K}$, $(\beta_{ik}) = B$ = matriz correspondente de b, vê-se que a correspondência $a \rightarrow A$ é um homomorfismo operatório relativamente a $\mathfrak{K}$. O conjunto das matrizes A, como sub-módulo do módulo das matrizes quadradas de grau n, formadas com elementos de $\mathfrak{K}$, é um módulo finito relativamente a $\mathfrak{K}$. Se supômos que $\mathfrak{G}$ tem elemento U, o homomorfismo torna-se num isomorfismo, visto que imaginar A = 0 equivale a admitir a $e_i = 0$, para todos os i, e, portanto, a admitir que é

$$ab = a(e_1 \beta_1 + \cdots + e_n \beta_n) = 0, \qquad (\beta_i \in \mathfrak{K}) \ ,$$

qualquer que seja b. Em particular, ter-se-á aU = a = 0, o que prova a afirmação. Neste caso, o conjunto das matrizes A constitui um sistema hiper-complexo equivalente de $\mathcal{G}$. Se se tomassem as igualdades

$$ae_1 = \sum a_{1j} e_j, \ \ldots, \ ae_n = \sum_j a_{nj} e_j \ , \quad (a_{kj} \in \mathcal{K}), \tag{9}$$

teriam lugar resultados análogos. A matriz correspondente de a seria neste caso $\tilde{A}$ = matriz transposta de A.

O teorema da homomorfia permite enunciar imediatamente o seguinte

Teorema:- É condição necessária e suficiente, para que a correspondência $a \longrightarrow A$ seja um isomorfismo, que uma igualdade $ax = o$, com a fixo e $x \in \mathcal{G}$ qualquer, apenas possa ser satisfeita se $a = o$.

Se designarmos por $\mathcal{U}$ o conjunto das matrizes A, o homomorfismo $\mathcal{G} \sim \mathcal{U}$, definido através das relações (8), dá a chamada 1ª representação regular do sistema $\mathcal{G}$. O corpo de representação é o corpo fundamental da álgebra.

Poderíamos ter escrito, em vez de (8),

$$e_1 a = \sum_j \alpha^*_{1j} e_j, \ \ldots, \ e_n a = \sum_j \alpha^*_{nj} e_j, \quad (\alpha^*_{jk} \in \mathcal{K}). \tag{10}$$

Valeriam, então, os dois resultados seguintes para $ae_l b$:

$$ae_l b = \sum_j \beta^*_{lj} . ae_j = \sum_{j,k} \beta^*_{lj} e_k \alpha_{kj} = \sum_k e_k \sum_j \beta^*_{lj} \alpha_{kj},$$

$$ae_l b = \sum_j e_j b . \alpha_{jl} = \sum_{j,k} \beta^*_{jk} e_k \alpha_{jl} = \sum_k e_k \sum_j \beta^*_{jk} \alpha_{jl} \ .$$

Daqui se concluiam as igualdades

$$\sum_j \alpha_{kj} b^*_{jl} = \sum_j b^*_{kj} \alpha_{jl} \ , \qquad (b^*_{kj} = \beta^*_{jk}) \ .$$

Designando por $A^*, B^*, \ldots$ as matrizes da representação (10), seria, pois, $A \tilde{B}^* = \tilde{B}^* A$, o que exprimiria serem comutáveis as matrizes de (8) e as transpostas de (10). As igualdades (10) definem a chamada 2ª representação regular.

Dadas duas álgebras $\mathcal{G}$ e $\mathcal{G}'$, com o mesmo corpo fundamental, diz-se que elas são recíprocas, se forem verificadas as correspondências

$$a \longrightarrow a', \ b \longrightarrow b', \ \lambda a \longrightarrow \lambda a', \ a+b \longrightarrow a'+b', \ ab \longrightarrow b'a'.$$

Seja $\mathcal{G}$ uma álgebra com elemento um. Se a 1ª representação regular é definida pelas igualdades (8), a álgebra $\mathcal{G}$ e a álgebra $\mathcal{U}$, das matrizes A, são equivalentes (rep. directa). Utilizando (9) para definir a 1ª representação regular, a álgebra $\mathcal{G}$ e a álgebra $\mathcal{U}' = \tilde{\mathcal{U}}$, das matrizes $\tilde{A}$ (ainda correspondentes dos elementos de $\mathcal{G}$), são recíprocas (rep. recíproca). Anàlogamente, por meio de (10), a 2ª representação regular dá, se $\mathcal{G}$ tem elemento um, uma álgebra $\mathcal{U}''$ equivalente de $\mathcal{G}$ (rep. directa), mas se se escreve $e_l a = \sum e_j a^*_{jl}$, a 2ª representação regular leva a uma álgebra recíproca de $\mathcal{G}$ (rep. recíproca). Da combinação destas últimas igualdades com (8) resulta, formando de dois modos diferentes os produtos $ae_l b$, que as matrizes da 2ª representação regular recíproca comutam com as matrizes da 1ª representação regular directa. Se $\mathcal{U}'''$ é a álgebra daquelas matrizes (de ordem n, igual à ordem de $\mathcal{G}$), tanto $\mathcal{U}$ como $\mathcal{U}'''$ são sub-álgebras da álgebra completa das matrizes de grau n, $\mathcal{K}_n = \mathcal{M}_n$. Vamos ver que, se $M \in \mathcal{M}_n$ comuta com todas as matrizes de $\mathcal{U}$, é $M \in \mathcal{U}'''$. Ponhamos $M e_l = \sum e_j m^*_{jl}$. Supondo A, B, $\ldots \in \mathcal{U}$, tem-se, para cada $x \in \mathcal{G}$, AM.x = MA.x = M(ax), e, em particular, se x = U, AM.U = a.MU = Ma. Conclui-se daqui que a aplicação de M a qualquer $a \in \mathcal{G}$ é sempre uma multiplicação de a por um elemento bem determinado $MU \in \mathcal{G}$, colocado à direita de a ($M e_l = e_l . MU = \sum e_j m^*_{jl}$). A matriz M é a matriz que representa MU na 2ª representação regular recíproca. Podemos enunciar o seguinte

Teorema:- Se uma álgebra $\mathcal{G}$, de ordem n, tem elemento um, a álgebra $\mathcal{U}$, de ordem n, definida pela 1ª representação regular directa de $\mathcal{G}$, é composta das matrizes, da álgebra total das matrizes $\mathcal{M}_n$, que comutam com as matrizes da 2ª representação regular recíproca $\mathcal{U}'''$, e inversamente. É claro que, supondo $A''', B''', \ldots \in \mathcal{U}'''$ e M comutável com estas matrizes, o raciocínio faz-se como segue. Para cada $x \in \mathcal{G}$, tem-se $A'''M.x = MA'''.x = M(xa)$; e, portanto, com x = U, $A'''M.U = MU.a = Ma$.

Conclui-se daqui que a aplicação de $\underline{M}$ a qualquer $a \in \mathcal{H}$ é sempre uma multiplicação de a por um elemento bem determinado $MU \in \mathcal{H}$ colocado à esquerda de a ($M\,e_l = MU.e_l = \sum_j e_j m_{jl}$). A matriz $\underline{M}$ representa MU na 1ª representação regular directa. As álgebras $\mathcal{U}$ e $\mathcal{U}''$ são recíprocas. O teorema anterior tem um análogo, no qual entram as álgebras $\mathcal{U}'$ e $\mathcal{U}''$.

Teorema:- Duas representações regulares duma álgebra são semelhantes. Façamos duas observações. A representação regular (8) depende da base da álgebra. Tem sentido, pois, falar de duas representações regulares. Em seguida, dizer que duas representações são semelhantes (empregaremos também a designação de representações equivalentes) é dizer que existe uma matriz fixa $\underline{P}$, com inverso, tal que as matrizes A_1 e A_2, correspondentes do mesmo elemento $a \in \mathcal{H}$, nas duas representações, estão relacionadas pela igualdade $A_2 = P A_1 P^{-1}$. A_1 e A_2 são, assim, matrizes semelhantes. A busca de A_2, a partir de A_1, equivale à determinação da nova matriz dum endomorfismo, quando se pratica uma mudança de base (tomo I, § 12, Cap. I). Em notação de matrizes, tem-se

$$a.(e_1,\dots,e_n) = (e_1,\dots,e_n).A = (E_1,\dots,E_n),$$

$$(e'_1,\dots,e'_n) = (e_1,\dots,e_n).Q, \quad (e'_l = \text{elemento da nova base}),$$

$$a.(e'_1,\dots,e'_n) = (E_1,\dots,E_n).Q = (e_1,\dots,e_n).AQ =$$

$$= (e'_1,\dots,e'_n).Q^{-1}AQ,$$

de sorte que basta pôr $P = Q^{-1}$.

Viu-se que a representação regular duma álgebra com elemento um era um isomorfismo $\mathcal{H} \sim \mathcal{U}$. Se $\mathcal{H}$ não tem elemento um, consideremos a álgebra de ordem $n+1$, $\mathcal{H}' = (U; e_1,\dots,e_n)$, já referida anteriormente. Os elementos de $\mathcal{H}$ pertencem a $\mathcal{H}'$, tendo-se, para $a \in \mathcal{H}$,

$$a\,U = a = \sum_l e_l \alpha_l, \qquad a\,e_j = \sum_{k=1}^{n} e_k \alpha_{kj},$$

de modo que a nova representação regular determina a correspondência

$$a \longrightarrow \begin{pmatrix} 0 & 0 & \dots & 0 \\ \alpha_1 & \alpha_{11} & \dots & \alpha_{1n} \\ \hline \alpha_n & \alpha_{n1} & \dots & \alpha_{nn} \end{pmatrix} = A_1 .$$

Tem-se aqui um isomorfismo operatório $a \longrightarrow A_1$, pelo que pode enunciar-se o

Teorema:- Uma álgebra $\mathcal{H}$ de ordem n é sempre equivalente a uma sub-álgebra duma álgebra de matrizes. Este enunciado pode precisar-se ainda dizendo: uma álgebra de ordem n é sempre equivalente a uma álgebra de matrizes de ordem n ou de ordem $n+1$.

3) Soma directa de duas álgebras - Dadas duas álgebras $\mathcal{H}(u_1,\dots,u_n)$ e $\mathcal{H}'(v_1,\dots,v_m)$, com o mesmo corpo fundamental $\mathcal{K}$, a soma directa[1] $\mathcal{H} + \mathcal{H}'$ é a álgebra $\mathcal{H}''(u_1,\dots,u_n; v_1,\dots,v_m)$, de ordem $n+m$, na qual a tabela do produto dos elementos base é a seguinte:

$u_l u_j$ é calculado em $\mathcal{H}$; $v_r v_s$ é calculado em $\mathcal{H}'$;

$$u_p v_q = v_q u_p = 0.$$

Se as álgebras iniciais têm ambas elemento um, sejam $u_1 k_1 + \dots + u_n k_n$ e $v_1 x_1 + \dots + v_m x_m$ esses elementos. O elemento $u_1 k_1 + \dots + u_n k_n + v_1 x_1 + \dots + v_m x_m$ é elemento um da soma. Se $\mathcal{U}$ e $\mathcal{U}'$ forem duas álgebras de matrizes equivalentes a $\mathcal{H}$ e $\mathcal{H}'$, respectivamente, consideremos o conjunto de matrizes

$$\Delta = \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix}, \qquad \begin{cases} A \in \mathcal{U} \text{ é correspondente de } a \in \mathcal{H}; \\ A' \in \mathcal{U}' \text{ é correspondente de } a' \in \mathcal{H}'. \end{cases}$$

A correspondência $a + a' \longrightarrow \Delta$ é ainda uma equivalência, pois

[1] A designação fica de acordo com o significado dado a esta expressão na Teoria dos Grupos.

$$(a+a')+(b+b') = (a+b)+(a'+b') \longrightarrow \begin{pmatrix} A+B & 0 \\ 0 & A'+B' \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix} + \begin{pmatrix} B & 0 \\ 0 & B' \end{pmatrix},$$

$$(a+a').(b+b') = ab + a'b' \longrightarrow \begin{pmatrix} AB & 0 \\ 0 & A'B' \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix} \begin{pmatrix} B & 0 \\ 0 & B' \end{pmatrix},$$

$$(a+a')k = ak + a'k \longrightarrow \begin{pmatrix} Ak & 0 \\ 0 & A'k \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix} . k \ ,$$

onde $b \in \mathcal{G}$, $b' \in \mathcal{G}'$, $k \in \mathcal{K}$, e $b \longrightarrow B \in \mathcal{U}$, $b' \longrightarrow B' \in \mathcal{U}'$. Quando uma matriz é da forma

$$A = \{P, Q\} = \begin{pmatrix} P & 0 \\ 0 & Q \end{pmatrix},$$

usa-se também (Cap.anterior, § 6) a expressão "A é soma directa de P e Q" para o significar. Extremamente importante é a noção de produto (produto directo de Kronecker) de duas álgebras, que será objecto do § seguinte. Nele faremos também aplicações imediatas às álgebras de matrizes.

4) Produto de sistemas hiper-complexos - Dados os sistemas $\mathcal{G}_1(u_1, \ldots, u_n)$ e $\mathcal{G}_2(v_1, \ldots, v_m)$, com o mesmo corpo fundamental $\mathcal{K}$, consideremos os n m símbolos $u_i v_j$ e tomemo-los como bases dum novo sistema hiper-complexo com o corpo fundamental $\mathcal{K}$. Nesta hipótese, supor-se-á ainda que é $u_i v_j = v_j u_i$ e condicionar-se-á a tabela da multiplicação dos elementos base $u_i v_j$ pelas relações associativas $u_i v_j . u_k v_l = u_i u_k . v_j v_l$. É claro que pode escrever-se também

$$u_i v_j . u_k v_l = v_j u_i . v_l u_k = v_j v_l . u_i u_k .$$

Representando o produto pelo símbolo $\mathcal{G}_1 \times \mathcal{G}_2$, tem-se imediatamente

$$\mathcal{G}_1 \times \mathcal{G}_2 = \mathcal{G}_2 \times \mathcal{G}_1 . \qquad (11)$$

Quando se utiliza uma nova base $(u'_1, \ldots, u'_h)$ para $\mathcal{G}_1$, o produto passa a ter os elementos base $u'_i v_j$. Recorrendo às expressões dos u'_i em função dos u_j e às destes em função daqueles, obtêm-se relações formais entre os $u'_i v_j$ e os $u_k v_l$, que permitem passar duns aos outros. Em vez de considerarmos o sistema de base $(\ldots, u'_i v_j, \ldots)$ como equivalente do sistema $\mathcal{G}_1 \times \mathcal{G}_2$, diremos que se trata deste próprio sistema. A equivalência resulta evidentemente do facto de sabermos procurar a expressão $\sum u'_i v_j \alpha'_{ij}$ dum elemento $\sum u_i v_j \alpha_{ij}$, e reciprocamente. De resto verifica-se imediatamente a invertibilidade da matriz que figura nas equações que relacionam os $u'_i v_j$ e os $u_k v_l$. Na expressão de cada elemento do produto, podemos agora fazer desaparecer a base utilizada para $\mathcal{G}_1$ ou para $\mathcal{G}_2$. Basta pôr

$$\sum_{i,j} u_i v_j \lambda_{ij} = \sum_i u_i \sum_j v_j \lambda_{ij} = \sum_j \left(\sum_i u_i \lambda_{ij}\right) v_j = \sum_i u_i c'_i = \sum_j b'_j v_j \ , \qquad (12)$$

onde $b'_j \in \mathcal{G}_1$, $c'_i \in \mathcal{G}_2$. O produto goza ainda da propriedade expressa pela relação $\mathcal{G}_1 \times (\mathcal{G}_2 \times \mathcal{G}_3) = (\mathcal{G}_1 \times \mathcal{G}_2) \times \mathcal{G}_3$, da qual se deduzem várias outras, tendo em conta (11).

Admitamos que $\mathcal{G}_1$ tem elemento U. O conjunto dos elementos Uc, onde $c \in \mathcal{G}_2$, é um sub-anel do produto. A correspondência $c \longrightarrow Uc$ é um isomorfismo, pois que $U(c + c') = Uc + Uc'$, $Uc.Uc' = Ucc'$, e a relação $Uc = 0$, escrita sob a forma $U(\mu_1 v_1 + \cdots + \mu_m v_m) = 0$, dá, supondo $U = a_1 u_1 + \cdots + a_n u_n$,

$$a_1 \mu_1 = \cdots = a_1 \mu_m = 0 \ ; \ \cdots \ ; \ a_n \mu_1 = \cdots = a_n \mu_m = 0 \ ;$$

donde se tira, se um dos μ_l for diferente de zero, $a_1 = \cdots = a_n = 0$, o que é absurdo. No anel produto, podemos, assim, substituir os elementos Uc pelos elementos c e supor $\mathcal{G}_2$ contido no referido produto.

Em todo este §, suporemos agora que ambos os factores de (11) têm elemento um. Admitindo que u_1 e v_1 são esses elementos, vê-se que $u_1 v_1$ é elemento um do produto. Pondo $u_1 \mathcal{G}_2 = \mathcal{G}'_2$, $\mathcal{G}_1 v_1 = \mathcal{G}'_1$, tem-se

$$\mathcal{G}_1 \times \mathcal{G}_2 = \mathcal{G}'_1 \times \mathcal{G}'_2 .$$

Dum modo geral, se $\mathcal{U}_1$, $\mathcal{U}_2$ são duas álgebras com o corpo fundamental $\mathfrak{K}$ das álgebras $\mathcal{Y}_1$, $\mathcal{Y}_2$, e respectivamente equivalentes a estas últimas, tem-se

$$\mathcal{Y}_1 \times \mathcal{Y}_2 \cong \mathcal{U}_1 \times \mathcal{U}_2 .$$

Tendo em conta os resultados do § 9 do Cap.I, podemos enunciar o seguinte

Teorema:- Se $\mathcal{Y}$ é uma álgebra de ordem n com elemento um e $\mathcal{U}_s$ uma sub-álgebra de $\mathcal{Y}$ com o mesmo elemento um e isomorfa dum anel completo de matrizes de ordem s, tem-se $\mathcal{Y} = \mathcal{U}_s \times \mathcal{G}$, onde $\mathcal{G}$ é uma sub-álgebra de $\mathcal{Y}$, ainda com o mesmo elemento um, composta dos elementos de $\mathcal{Y}$ que comutam com todos os elementos de $\mathcal{U}_s$.

Façamos duas observações. Quando utilizarmos um dos símbolos $\mathcal{M}_s$, $\mathcal{M}_t$, ..., significaremos álgebra completa de matrizes pròpriamente ditas, de grau dado pelo índice, e com elementos dum corpo (corpo fundamental da álgebra). Se usarmos $\mathcal{U}_s$, $\mathcal{U}_t$, $\mathcal{U}'_s$, $\mathcal{U}'_t$, $\mathcal{G}_s$, $\mathcal{G}_t$, ..., significaremos álgebra equivalente a uma álgebra $\mathcal{M}_s$, $\mathcal{M}_t$, ... do mesmo índice da álgebra dada.

No teorema que acabámos de enunciar, a existência de s^2 matrizes e_{ij} em $\mathcal{Y}$ (que constituem a base de $\mathcal{U}_s$) mostra que $\mathcal{Y}$ é o produto directo de Wedderburn, simbòlicamente representado por

$$\mathcal{Y} = (\ldots e_{ij} \ldots) \times \mathcal{G} , \qquad (13)$$

onde $\mathcal{G}$ é o conjunto de elementos de $\mathcal{Y}$ que comutam com todos os e_{ij}. É imediato que tais elementos são os mesmos que comutam com todos os elementos de $\mathcal{U}_s$. Por outro lado formam uma álgebra $\mathcal{G}$, à qual pertence o elemento um de $\mathcal{Y}$. Os elementos do 2º membro de (13) constituem precisamente a álgebra $\mathcal{U}_s \times \mathcal{G}$, como se vê tendo em conta a independência dos produtos dos e_{ij} pelos elementos duma base de $\mathcal{G}$ e recorrendo a (12). Pode verificar-se que os únicos elementos comuns a $\mathcal{U}_s$ e $\mathcal{G}$ são as matrizes diagonais de $\mathcal{U}_s$ de elementos iguais, as quais formam uma álgebra isomorfa do corpo fundamental $\mathfrak{K}$ (Cap.II, § 4). Convém talvez precisar que, nesta demonstração do teorema supra, $\mathcal{U}_s$ é álgebra sobre $\mathfrak{K}$.

Como caso particular, trataremos aquele em que se tem $\mathcal{Y} = \mathcal{M}_r$, r = st. Começaremos por demonstrar dois teoremas.

Teorema 1º:- A álgebra completa de matrizes, $\mathcal{M}_r$, se for r = st, é um produto de duas sub-álgebras da forma $\mathcal{M}_r = \mathcal{U}_s \times \mathcal{U}_t$, onde $\mathcal{U}_t$, que substitui a sub-álgebra $\mathcal{G}$ do teorema anterior, é o conjunto de elementos de $\mathcal{M}_r$ que comutam com todos os elementos de $\mathcal{U}_s$. Decomponhamos as matrizes de $\mathcal{M}_r$ em matrizes quadradas de grau t, de modo que cada matriz $M \in \mathcal{M}_r$ se considera de grau s. Pode escrever-se, assim, $M = (a_{ij})$, (i,j = 1, 2, ..., s), onde a_{ij} é matriz de grau t da forma

$$a_{ij} = \sum_{p,q=1}^{t} \varepsilon_{pq} \alpha_{pq}^{(ij)} ,$$

com $\alpha_{pq}^{(ij)} \in \mathfrak{K}$, e ε_{pq} = matriz de grau t de elementos nulos, salvo o elemento da linha de ordem p e coluna de ordem q, que é $u \in \mathfrak{K}$. Entre as matrizes M figuram as matrizes U_{ij}, de elementos nulos, salvo o da linha de ordem i e coluna de ordem j, que se supõe a matriz unidade de grau t. As matrizes U_{ij} constituem um sistema de s^2 matrizes unidades pertencentes a $\mathcal{M}_r$, pelo que se terá, conforme o teorema anterior,

$$\mathcal{M}_r = \mathcal{U}_s \times \mathcal{G} ,$$

subentendendo por $\mathcal{U}_s$ a álgebra de elementos base U_{ij}, que tem o mesmo elemento um que $\mathcal{M}_r$. Vamos proceder à construção de $\mathcal{G}$. Consideremos as matrizes diagonais M da forma

$$E_{pq} = \{\varepsilon_{pq}, \ldots, \varepsilon_{pq}\} .$$

Tem-se

$$U_{ij} E_{pq} = E_{pq} U_{ij} .$$

O único elemento deste produto que não é nulo é o elemento (i,j), precisamente igual à matriz ε_{pq}. A álgebra $\mathcal{U}_t$, de base formada pelos elementos E_{pq}, é uma sub-álgebra de $\mathcal{M}_r$ comutá-

vel com $\mathcal{U}_s$. Provaremos, inversamente, que um elemento pertencente a $\mathcal{M}_r$, comutável com a álgebra $\mathcal{U}_s$, pertence a $\mathcal{U}_t$. Se $\underline{M}$ for um tal elemento, tem-se

$$MU_{ij} = U_{ij} M = \begin{pmatrix} 0 & (a_{1l}) & 0 \\ \hline 0 & (a_{sl}) & 0 \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 \\ a_{j1} & \cdots & a_{js} \\ 0 & \cdots & 0 \end{pmatrix},$$

onde os $a_{\kappa l}$ pertencem à coluna de ordem $\underline{j}$ e os $a_{j\kappa}$ à linha de ordem $\underline{i}$. Conclui-se que deve ser $a_{\lambda l} = 0$, se $\lambda \neq i$, $a_{j\mu} = 0$, se $\mu \neq j$, e $a_{ll} = a_{jj}$. A matriz $\underline{M}$ tem o aspecto de matriz diagonal de elementos iguais:

$$M = \{a_{ll}, \ldots, a_{ll}\}.$$

Ora esta matriz pode escrever-se

$$M = \left\{ \sum_{p,q} \varepsilon_{pq} \alpha_{pq}^{(1l)}, \ldots, \sum_{p,q} \varepsilon_{pq} \alpha_{pq}^{(jl)} \right\} = \sum_{p,q} \left\{ \varepsilon_{pq}, \ldots, \varepsilon_{pq} \right\} \alpha_{pq}^{(il)} = \sum_{p,q} E_{pq} \alpha_{pq}^{(il)},$$

de modo que é, efectivamente, $\mathcal{L} = \mathcal{U}_t$, como se quer.

Corolário:- O produto de duas álgebras $\mathcal{U}_s', \mathcal{U}_t'$ é uma álgebra $\mathcal{U}_{st}'$. Pondo, com efeito, $m = st$, consideremos a álgebra $\mathcal{M}_m = \mathcal{U}_s \times \mathcal{U}_t$. Como $\mathcal{U}_s'$ e $\mathcal{U}_t'$ são isomorfas dos respectivos factores do produto, o corolário fica provado.

Teorema 2º:- Se uma álgebra $\mathcal{M}_r$ contém uma sub-álgebra $\mathcal{U}_s'$ com o mesmo elemento um que $\mathcal{M}_r$, s é divisor de r, e existe um automorfismo interno de $\mathcal{M}_r$ que faz passar de $\mathcal{U}_s'$ à sub-álgebra $\mathcal{U}_s$ do teorema anterior. Designemos com e_{ij}' as matrizes unidades de $\mathcal{U}_s'$. Em virtude de se ter $e_{il}' = e_{ij}' e_{jl}'$. e_{jl}', a característica t_j, de e_{ll}', é $\geq t_j$. Sendo analogamente $t_j \geq t_i$, resulta $t_1 = t_2 = \cdots = t_s$. Por outro lado, como os e_{ii}' $(i = 1, 2, \ldots, s)$ são ortogonais e idempotentes, tem-se (§ 7 do Cap. anterior): $t_1 + t_2 + \cdots + t_s = st$ = característica da matriz unidade $U_r = r$. Seja $\underline{S}$ uma matriz invertível (ainda § 7 do Cap. anterior) tal que

$$S e_{11}' S^{-1} = \begin{pmatrix} U_t & 0 \\ 0 & 0_{r-t} \end{pmatrix} = U_{11}, \qquad S e_{22}' S^{-1} = \begin{pmatrix} 0_t & 0 & 0 \\ 0 & U_t & 0 \\ 0 & 0 & 0_{r-2t} \end{pmatrix} = U_{22},$$

etc. Por meio do automorfismo interno S, a sub-álgebra $\mathcal{U}_s'$ transforma-se numa sub-álgebra $\mathcal{U}_s''$, de matrizes unidades e_{ij}'', para as quais $e_{ii}'' = U_{ii}$. Vejamos a expressão geral dum e_{ij}''. Tem-se

$$U_{ii} e_{ij}'' = e_{ij}'', \qquad e_{ij}'' U_{jj} = e_{ij}''.$$

A matriz e_{ij}'', do grau $\underline{s}$, apenas pode ter diferente de zero a matriz ε_{ij}'', de ordem $\underline{t}$, do cruzamento da sua linha de ordem $\underline{i}$ e da sua coluna de ordem $\underline{j}$. São válidas as igualdades

$$\{\varepsilon_{ij}'', \ldots, \varepsilon_{ij}''\} \cdot U_{ij} = e_{ij}'',$$

$$\{\varepsilon_{j\kappa}'', \ldots, \varepsilon_{j\kappa}''\} \cdot U_{j\kappa} = e_{j\kappa}'',$$

$$\{\varepsilon_{ij}'' \ \varepsilon_{j\kappa}'', \ldots, \varepsilon_{ij}'' \varepsilon_{j\kappa}''\} \cdot U_{l\kappa} = e_{ij}'' e_{j\kappa}'' = e_{i\kappa}'',$$

pois que as matrizes U_{ij} comutam com as matrizes diagonais de elementos iguais. Conclui-se da última igualdade que é

$$\varepsilon_{ij}'' \ \varepsilon_{j\kappa}'' = \varepsilon_{i\kappa}'', \qquad (i,j,k = 1, 2, \ldots, s).$$

Consideremos agora as matrizes

$$T = \{U_t, \varepsilon_{12}'', \ldots, \varepsilon_{1s}''\}, \qquad T^{-1} = \{U_t, \varepsilon_{21}'', \ldots, \varepsilon_{s1}''\}.$$

Verifica-se que a segunda é inversa da primeira, em virtude de se ter $\varepsilon_{ij}'' \varepsilon_{jl}'' = \varepsilon_{il}'' = U_t$. E tem-se imediatamente

$$T e_{ii}'' T^{-1} = T U_{ii} T^{-1} = e_{ii}''' = U_{ii}, \qquad T e_{ij}'' T^{-1} = e_{ij}''' = U_{ij}.$$

Por meio do automorfismo interno de $\mathcal{M}_r$ definido por $V = T S$, vem, assim:

$$V e_{ij}' V^{-1} = T S . e_{ij}' . S^{-1} T^{-1} = T e_{ij}'' T^{-1} = e_{ij}''' = U_{ij}.$$

O teorema está demonstrado.

Regressando à questão que nos tínhamos proposto, podemos enunciar o

Teorema:- Se a álgebra $\mathcal{M}_r$ tem a sub-álgebra $\mathcal{U}_s'$, com o mesmo elemento um que $\mathcal{M}_r$, vale $\mathcal{M}_r = \mathcal{U}_s' \times \mathcal{U}_t'$. Em primeiro lu-

$\mathfrak{K}[x_1,\ldots,x_n]$) e é de ordem $n = m^2$. Se a álgebra quadrada for de divisão, vale ainda o

Teorema:- Uma álgebra quadrada de divisão (de ordem $n = m^2$) sobre um corpo infinito $\mathfrak{K}$ possui elementos b cujo polinómio mínimo é de grau m e tais que $\mathfrak{K}(b)$ é álgebra separável sobre $\mathfrak{K}$ (ampliação separável de $\mathfrak{K}$).

11) As álgebras como anéis - No § 1 dissemos já que uma álgebra finita $\mathfrak{Z}$ é um módulo finito relativamente ao seu corpo comutativo fundamental $\mathfrak{K}$ e um anel com o domínio operatório estranho constituido pelo mesmo corpo. Considerada a álgebra como grupo com operadores, há dois domínios operatórios: o corpo $\mathfrak{K}$ e a própria álgebra. Os sub-grupos admissíveis são ideais que, além de ideais ordinários, contêm, com cada elemento a, o elemento λa, em que $\lambda \in \mathfrak{K}$. Trata-se de ideais admissíveis, no sentido do § 1 do Cap. I. São os ideais que estarão em causa em tudo o que vai seguir-se. Quando há elemento um, todos os ideais são admissíveis, como sabemos.

Um ideal próprio duma álgebra finita é uma álgebra finita de ordem inferior à daquela. Como já dissemos, apenas temos como objecto o estudo das álgebras finitas.

Teorema:- Uma álgebra sem divisores de zero é uma álgebra de divisão. Seja $a \in \mathfrak{Z}$. O conjunto dos elementos $a\mathfrak{Z}$ constitui um ideal direito de $\mathfrak{Z}$ (é, de facto, um ideal admissível, pois $\lambda.a\mathfrak{Z} = a.\lambda\mathfrak{Z}$, se $\lambda \in \mathfrak{K}$). Trata-se dum sub-módulo com respeito a um corpo. Se a ordem do sub-módulo for a de $\mathfrak{Z}$ (e o mesmo suceder a $\mathfrak{Z}a$), o teorema resultará das igualdades $a\mathfrak{Z} = \mathfrak{Z}$, $\mathfrak{Z}a = \mathfrak{Z}$, válidas para qualquer $a \neq 0$. Ora, se for e_i ($i = 1, 2, \ldots, n$) uma base de $\mathfrak{Z}$, vamos ver que os elementos ae_i são, efectivamente, linearmente independentes, em face de $\mathfrak{K}$. Uma relação

$$\lambda_1.a\,e_1 + \cdots + \lambda_n.a\,e_n = a(\lambda_1 e_1 + \cdots + \lambda_n e_n) = 0$$

dá $\lambda_1 e_1 + \cdots + \lambda_n e_n = 0$, e, portanto, como se quer, $\lambda_1 = \cdots = \lambda_n = 0$. Vê-se, mesmo, conforme anunciámos no começo do § 8, que, quando a não é divisor de zero, as equações $ax = b$, $ya = b$ ($a, b \in \mathfrak{Z}$, $a \neq 0$) são soluveis em $\mathfrak{Z}$, qualquer que seja esta álgebra (Veja-se o teorema análogo para anéis - U).

Teorema:- Uma sub-álgebra duma álgebra de divisão $\mathfrak{D}$ é uma álgebra de divisão com o mesmo elemento um que $\mathfrak{D}$ e com uma ordem que divide a desta última. A sub-álgebra $\mathfrak{D}'$ não tem divisores de zero. É um corpo. Se u' é o seu elemento um e se $u \in \mathfrak{K} \subseteq \mathfrak{D}$, tem-se $u'u' = u'$, $uu' = u'$; $(u'-u)u' = 0$, $u' = u$. O último teorema do § 8 mostra-nos, por fim, que a ordem de $\mathfrak{D}'$ divide a de $\mathfrak{D}$.

Consideremos o caso mais simples, de uma álgebra de 1ª ordem: $\mathfrak{Z} = (u_1)$. Tem lugar o

Teorema:- Uma álgebra de 1ª ordem ou é nilpotente, e de expoente 2 (álgebra zero), ou é equivalente ao corpo fundamental. Seja $u_1^2 = \alpha u_1$, $(\alpha \in \mathfrak{K})$, a tabela de multiplicação. Se for $\alpha = 0$, o produto de dois quaisquer elementos da álgebra é nulo, e a álgebra é nilpotente, de expoente 2. Se é $\alpha = 0$, observemos que, tendo-se

$$\alpha^{-1}u_1.\alpha^{-1}u_1 = \alpha^{-1}\alpha^{-1}.\alpha u_1 = \alpha^{-1}u_1 ,$$

o elemento $v_1 = \alpha^{-1}u_1$ é um idempotente da álgebra. Considerando, então, a correspondência $\lambda \to \lambda v_1$, $(\lambda \in \mathfrak{K})$, tem-se uma equivalência entre $\mathfrak{Z}$ e $\mathfrak{K}$, pois:

$$\lambda \to \lambda v_1 , \qquad \lambda.\rho \to \lambda\rho v_1 = \lambda v_1.\rho ,$$
$$\rho \to \rho v_1 , \qquad \lambda\rho \to \lambda\rho v_1 = \lambda v_1.\rho v_1 ,$$

e $\lambda v_1 = 0$ implica $\lambda = 0$.

Estudemos a noção de radical. Não pode dizer-se que um certo elemento seja uma raiz. Pode definir-se, porém, ideal direito nilpotente, $\mathfrak{r}$, e considerar-se o ideal $\mathfrak{n} = (\mathfrak{r};\mathfrak{Z}\mathfrak{r})$, que é ainda um ideal bilateral nilpotente. O conjunto unido dos ideais bilaterais nilpotentes é o conjunto unido de todos os ideais nilpotentes e é um nilideal bilateral.

Num conjunto qualquer de ideais direitos (ou esquerdos), de $\mathfrak{Z}$, consideremos um ideal de maior e outro de menor ordem. Esses ideais são, respectivamente, um ideal máximo e um ideal mínimo. A condição dupla de cadeia é verificada em $\mathfrak{Z}$. A simples condição de máximo garante que o radical $\mathfrak{R}$ é nilpotente. Tomemos, com efeito, um ideal nilpotente $\mathfrak{r}$ que seja máxi-

mo. Um ideal nilpotente qualquer $\mathfrak{N}_1$ está contido em $\mathfrak{N}$, pois que a soma $(\mathfrak{N}, \mathfrak{N}_1)$ é nilpotente e contém $\mathfrak{N}$, o que dá $(\mathfrak{N}, \mathfrak{N}_1) = \mathfrak{N}$, $\mathfrak{N}_1 \subseteq \mathfrak{N}$.

Os raciocínios do § 1 do Cap.II são aqui aplicáveis. A demonstração de Artin prova que numa álgebra todo o nilideal é nilpotente e que, portanto, $\mathcal{R}^* = \mathcal{R}^{**} = \mathcal{R}$. Conforme o § 3 do Cap.I, pode também enunciar-se o seguinte

Teorema:- O radical duma álgebra é o conjunto $\mathfrak{N}_1$ dos seus elementos pròpriamente nilpotentes.

Se uma álgebra não tem radical, o seu centro $\mathfrak{z}$ também não tem radical. $\mathfrak{z}$ reduz-se a um anel semi-simples comutativo, sendo, por isso, uma soma de corpos comutativos que se anulam mutuamente.

Falemos aqui das álgebras nilpotentes. Se n for a ordem da álgebra, a sua série de composição não pode ter um comprimento superior a n. Como se viu no Cap.II, será necessàriamente $\mathfrak{g}^{n+1} = (0)$. A álgebra confunde-se com o seu radical.

Teorema:- É necessário e suficiente, para que uma álgebra nilpotente tenha uma sub-álgebra própria, que não seja de 1ª ordem. É necessário, porque, se $\mathfrak{g}$ tem sub-álgebra $\neq (0)$, a ordem da sub-álgebra, inferior à da álgebra, é um, pelo menos. É suficiente, porque, supondo $\mathfrak{g} = (u_1, \ldots, u_n)$, $(n > 1)$, o sub-conjunto de $\mathfrak{g}$ de base $u_1, \ldots, u_{n-1}$ constitui uma sub-álgebra de $\mathfrak{g}$, se esta é de expoente 2 $(u_i u_j = o)$. No caso de ser $\mathfrak{g}^2 \neq (0)$, $\mathfrak{g}^2$ é uma sub-álgebra própria, visto que a igualdade $\mathfrak{g}^2 = \mathfrak{g}$ levaria a $\mathfrak{g} = (0)$.

Teorema:- Um anel cociente dum sistema hiper-complexo é um sistema hiper-complexo com o mesmo corpo fundamental. Se $\mathfrak{a}$ é um ideal bilateral, o anel cociente $\mathfrak{g}/\mathfrak{a}$ [que alguns autores, pelo facto de se estar trabalhando com grupos abelianos aditivos, representam por $\mathfrak{g} - \mathfrak{a}$ e chamam anel diferença ou álgebra diferença] é homomorfo de $\mathfrak{g}$. O corpo $\mathfrak{K}$ é também domínio operatório do anel cociente, pois, pondo $\lambda(a + \mathfrak{a}) = \lambda a + \mathfrak{a}$, e, em seguida, $\overline{a} = a + \mathfrak{a}$, $\overline{b} = b + \mathfrak{a}$, vem imediatamente $\lambda(\overline{a}\,\overline{b}) = \lambda\overline{a}.\overline{b} = \overline{a}.\lambda\overline{b}$. Verifica-se que o anel cociente é módulo finito relativamente a $\mathfrak{K}$, tomando a base (embora compos-

ta de elementos não linearmente independentes) $e_1 + \mathfrak{a}, \ldots, e_n + \mathfrak{a}$, que pressupõe os e_i constituirem uma base de $\mathfrak{g}$. Todos os postulados das álgebras têm lugar e o teorema está provado. Podemos, todavia, precisar que, se $\mathfrak{a}$ é de ordem r, a álgebra cociente é de ordem $n - r$. É o que se vê tomando uma base $(e_1, \ldots, e_n)$ da álgebra, na qual os r primeiros elementos constituam uma base de $\mathfrak{a}$. A ordem do anel cociente é $n - r$.

Aplicação:- Seja $\mathfrak{g}'$ uma sub-álgebra de $\mathfrak{g}$ isomorfa de $\mathfrak{g}/\mathcal{R}$. Pode escrever-se imediatamente $\mathfrak{g} = \mathfrak{g}' + \mathcal{R}$. Basta notar, com efeito, que as duas parcelas do 2º membro não têm elemento comum diferente de zero, visto que um tal elemento geraria em $\mathfrak{g}'$ um ideal nilpotente, contra a hipótese de a sub-álgebra não ter radical.

Definição:- Diz-se que uma álgebra $\mathfrak{g}$ é soma directa de várias sub-álgebras $\mathfrak{g}_{\gamma_i}$:

$$\mathfrak{g} = \mathfrak{g}_{\gamma_1} + \cdots + \mathfrak{g}_{\gamma_s}, \qquad (16)$$

quando as sub-álgebras satisfazem à condição $\mathfrak{g}_{\gamma_i}\mathfrak{g}_{\gamma_j} = (0)$, $(i \neq j)$. É uma definição concordante com a do § 3 deste Capítulo. Sabemos que as sub-álgebras $\mathfrak{g}_{\gamma_i}$ são ideais bilaterais de $\mathfrak{g}$. Uma álgebra é redutível ou irredutível conforme se pode ou não exprimir como soma directa de sub-álgebras (Cap.I, § 1).

Teorema:- Se $\mathfrak{g}$ é uma álgebra com elemento U e com a decomposição (16), o radical $\mathcal{R}$ é da forma $\mathcal{R} = \mathcal{R}_1 + \cdots + \mathcal{R}_s$, onde $\mathcal{R}_i = [\mathcal{R}, \mathfrak{g}_{\gamma_i}]$ é o radical de $\mathfrak{g}_{\gamma_i}$. Sabemos que se tem (Cap. I, § 7)

$$\mathcal{R} = \mathcal{R}\,\mathfrak{g} = \mathcal{R}\,\mathfrak{g}_{\gamma_1} + \cdots + \mathcal{R}\,\mathfrak{g}_{\gamma_s}.$$

$\mathcal{R}\,\mathfrak{g}_{\gamma_i}$ é um ideal bilateral nilpotente de $\mathfrak{g}$ e de $\mathfrak{g}_{\gamma_i}$ que está contido em $[\mathcal{R}, \mathfrak{g}_{\gamma_i}]$. Este último é também ideal bilateral de $\mathfrak{g}_{\gamma_i}$ e de $\mathfrak{g}$, e, portanto, uma soma de ideais da forma $[\mathcal{R}, \mathfrak{g}_{\gamma_i}]\mathfrak{g}_{\gamma_j}$, o que dá $\mathcal{R}\mathfrak{g}_{\gamma_i} = [\mathcal{R}, \mathfrak{g}_{\gamma_i}]$. Como $[\mathcal{R}, \mathfrak{g}_{\gamma_i}]$ é o ideal nilpotente máximo contido em $\mathfrak{g}_{\gamma_i}$, representa, de facto, o radical deste anel.

Nas álgebras redutíveis tem lugar o seguinte

Teorema:- Uma álgebra redutível com elemento um é uma soma directa de álgebras irredutíveis bem determinadas. Façamos uma primeira decomposição (16). Se as parcelas forem todas irredutíveis, o teorema está provado (Cap.I, § 7). Se uma parcela $\mathcal{G}_i$ for redutível, façamos a sua decomposição e repitamos o raciocínio para as novas parcelas obtidas. O processo acaba, pelo facto de ser finita a ordem da álgebra.

Exemplo de álgebra finita:(1) Seja o sistema $\mathcal{G}$ de 3ª ordem, com a seguinte tabela para a multiplicação dos elementos base:

	e_1	e_2	e_3
e_1	e_1	o	e_3
e_2	o	e_2	o
e_3	o	e_3	o

Procuremos o seu radical. Seja $w = \alpha e_1 + \beta e_2 + \gamma e_3$, onde α, β, $\gamma \in \mathfrak{K}$, uma raiz (esta afirmação tem sentido porque $e_1 + e_2$ é elemento um do sistema). O ideal direito que ela gera é nilpotente. Ora $we_1 = \alpha e_1$. Se $\alpha \neq o$, não pode ser nula uma potência de αe_1, o que mostra dever ter-se $w = \beta e_2 + \gamma e_3$. Mas, sendo também nilpotente o ideal esquerdo gerado por w, a relação $e_2 w = \beta e_2$ leva a uma conclusão análoga, se $\beta \neq o$. Assim, se há elementos raizes, a sua forma será $w = \gamma e_3$. O conjunto de elementos de tal forma é um ideal bilateral nilpotente, como imediatamente se vê. É o radical procurado. Como se tem $U = e_1 + e_2$, $e_1^2 = e_1$, $e_2^2 = e_2$, $e_1 e_2 = e_2 e_1 = o$, será

$$\mathcal{G} = \mathcal{G} e_1 + \mathcal{G} e_2 = e_1 \mathcal{G} + e_2 \mathcal{G} .$$

O ideal esquerdo $\mathcal{G} e_1$, considerado como módulo com respeito a $\mathfrak{K}$, tem um único elemento base. É simples, e, portanto, indecomponível. Mas, então, $e_1 \mathcal{G}$ é igualmente indecomponível. O mesmo se diz de $e_2 \mathcal{G}$ e de $\mathcal{G} e_2$. O anel cociente $\mathcal{G}/\mathcal{G} e_3$ é um anel sem radical. É um sistema hiper-complexo no qual a base é constituida pelos elementos $e_1 + \mathcal{G} e_3$, $e_2 + \mathcal{G} e_3$, visto que $e_3 + \mathcal{G} e_3 = 0$. A base referida é composta de elementos

(1) Tirado de E.Noether, "Hyperkomplexe Grössen und Darstellungstheorie".

linearmente independentes. Pondo

$$\mathcal{G}/\mathcal{G} e_3 = \mathfrak{K}(e_1 + \mathcal{G} e_3) + \mathfrak{K}(e_2 + \mathcal{G} e_3) ,$$

tem-se uma decomposição do anel cociente numa soma de dois corpos. De facto, e por ex.,

$$\lambda(e_1 + \mathcal{G} e_3) \cdot \mu(e_1 + \mathcal{G} e_3) = \lambda \mu e_1 + \mathcal{G} e_3 .$$

Terminaremos o §, dando algumas propriedades do sistema hiper-complexo $\mathcal{G}_{\mathcal{P}}$, que resulta de $\mathcal{G}$ por ampliação do corpo fundamental $\mathfrak{K}$ para o corpo $\mathcal{P} \supset \mathfrak{K}$.

Teorema:- Se $\mathcal{G}$ tem radical, $\mathcal{G}_{\mathcal{P}}$ tem radical. Tomemos, com efeito, como base de $\mathcal{G}$, os elementos $v_1, \ldots, v_r$; $e_{r+1}, \ldots, e_n$, dos quais os r primeiros constituem uma base do radical $\mathcal{R}$. Os elementos de $\mathcal{R}$ são da forma $v_1 k_1 + \cdots + v_r k_r$, $(k_i \in \mathfrak{K})$. Ao passar-se para $\mathcal{G}_{\mathcal{P}}$, os elementos base substituem-se por $\overline{v}_i$, $\overline{e}_j$, com a antiga tabela de multiplicação. Então, os elementos $\overline{v}_1 p_1 + \cdots + \overline{v}_r p_r$, $(p_r \in \mathcal{P})$, constituem um ideal bilateral nilpotente, como se reconhece imediatamente tendo em conta a multiplicação dos $\overline{v}_i$ (um produto que contenha σ factores $\overline{v}_i$ é nulo, se for $\mathcal{R}^{\sigma} = (0)$. Reduzindo ao absurdo, conclui-se também que $\mathcal{G}$ não tem radical, se $\mathcal{G}_{\mathcal{P}}$ não tem radical.

O centro dum sistema hiper-complexo é um anel que admite o corpo fundamental como domínio operatório:

$$a \cdot \lambda z = \lambda \cdot az = \lambda \cdot za = \lambda z \cdot a \qquad (z \in \mathcal{Z} = \text{centro}).$$

Sejam, então, $z_1, \ldots, z_R, \underline{k}$ elementos do centro, número máximo de elementos independentes com respeito a $\mathfrak{K}$. Os elementos do centro são da forma $z = z_1 \lambda_1 + \cdots + z_R \lambda_R$ e todos os elementos desta forma pertencem ao centro. $\mathcal{Z}$ é, assim, um sistema hiper-complexo com o corpo fundamental $\mathfrak{K}$.

Procuremos o centro da álgebra dum grupo $\mathcal{G}$. Seja $g \in \mathcal{G}$. Se s é um elemento qualquer de $\mathcal{G}$, os conjugados de g são da forma $s^{-1} g s$. Eles constituem uma classe de elementos equivalentes em $\mathcal{G}$. Poremos

$K_g = \frac{h_g}{h} \sum_s s^{-1} g\, s$ = soma dos conjugados distintos de g ,

significando com h_g o número de elementos conjugados de g, com h a ordem do grupo (e, portanto, com $\frac{h}{h_g}$ a ordem do normalizador de g[1]) e estendendo a soma a todos os elementos de $\mathcal{G}$. Vê-se fàcilmente que se tem $K_g \cdot g_i = g_i K_g$, isto é, que os K_g pertencem ao centro da álgebra do grupo. De facto,

$$K_g \cdot g_i = \frac{h_g}{h} \sum s^{-1} g\, s\, g_i , \qquad g_i \cdot K_g = \frac{h_g}{h} \sum g_i t^{-1} g\, t .$$

Ora, quando $sg_i = t$, é $s^{-1} = g_i t^{-1}$. Por isso, as duas somas anteriores são iguais, como se deseja.

Posto isto, vamos mostrar que $\mathcal{Z}$ se compõe de todos os elementos da forma $\sum_g \lambda_g K_g$ e só desses. Se um elemento $\sum \lambda_i g_i$ pertence ao centro, comuta com qualquer $s \in \mathcal{G}$, pelo que pode escrever-se

$$\sum_i \lambda_i g_i = s^{-1} \cdot \sum_i \lambda_i g_i \cdot s = \sum_i \lambda_i s^{-1} g_i s ,$$

$$h \cdot \sum_i \lambda_i g_i = \sum_i \lambda_i \left(\sum_s s^{-1} g_i s \right) ,$$

$$\sum_i \lambda_i g_i = \frac{1}{h} \sum_i \lambda_i \sum_s \left(s^{-1} g_i s \right) = \frac{1}{h} \sum_i \lambda_i \frac{h}{h_{g_i}} K_{g_i} =$$

$$= \frac{1}{h} \sum_i \left(\frac{h}{h_{g_i}} \lambda_i \right) K_{g_i} = \sum_g \lambda_g K_g , \qquad \text{q. e. d.}$$

Tira-se como conclusão que a característica do centro é dada pelo número de classes de elementos conjugados em que pode decompor-se o grupo.

Teorema:- O sistema ampliado, $\mathcal{Z}_\mathcal{F}$, do centro $\mathcal{Z}$, é o centro de $\mathcal{G}_\mathcal{F}$. Visto que $\mathcal{Z}$ é um sistema hiper-complexo com o corpo fundamental $\mathcal{F}$, tomemos uma base independente em $\mathcal{G}$ sob a forma $(z_1, \ldots, z_r ; e_1, \ldots, e_{n-r})$, onde $(z_1, \ldots, z_r)$ constitui

(1) Veja-se, por ex., Almeida Costa, "Elementos da Teoria dos Grupos", nº 1 desta Colecção, pgs. 65 e 66.

uma base independente de $\mathcal{Z}$. Os elementos do sistema $\mathcal{G}_\mathcal{F}$ são da forma

$$\sum_{i=1}^{r} \overline{z}_i p_i + \sum_{j=1}^{n-r} \overline{e}_j p_j \quad . \tag{17}$$

Todos os elementos de $\mathcal{G}_\mathcal{F}$ da forma $\sum \overline{z}_i p_i$ comutam evidentemente com todos os elementos (17), pelo que o centro $\mathcal{Z}'$, de $\mathcal{G}_\mathcal{F}$, contém aqueles elementos. Basta agora ver que um elemento $\overline{a} = \sum \overline{e}_j p_j$ não pode pertencer a $\mathcal{Z}'$, para se concluir o teorema. Comecemos por observar que, no caso de se ter simplesmente $\overline{a} = \overline{e}_1 p_1$, se fosse $\overline{a} \in \mathcal{Z}'$, seria $\overline{a}\, p_1^{-1} = \overline{e}_1 \in \mathcal{Z}'$, e $\overline{e}_1$ comutaria com todos os elementos $\overline{z}_i$, $\overline{e}_i$. O mesmo sucederia com e_1 e os elementos z_i, e_i, o que é absurdo. Suponhamos ainda, para ver claramente o espírito da demonstração, que $a = \overline{e}_1 p_1 + \overline{e}_2 p_2 \notin \mathcal{Z}'$. Para cada $\overline{e}_\lambda$, são válidas as igualdades

$$(\overline{e}_1 p_1 + \overline{e}_2 p_2)\overline{e}_\lambda = \overline{e}_\lambda (\overline{e}_1 p_1 + \overline{e}_2 p_2) ,$$

$$(\overline{e}_1 \overline{e}_\lambda - \overline{e}_\lambda \overline{e}_1) p_1 = (\overline{e}_\lambda \overline{e}_2 - \overline{e}_2 \overline{e}_\lambda) p_2 ,$$

$$(\overline{e}_1 \overline{e}_\lambda - \overline{e}_\lambda \overline{e}_1) p_1 p_2^{-1} = \overline{e}_\lambda \overline{e}_2 - \overline{e}_2 \overline{e}_\lambda .$$

Supondo $\overline{e}_\lambda$ escolhido de modo a não comutar com $\overline{e}_2$, vê-se que $p_1 p_2^{-1} = \alpha$ pertence ao corpo $\mathcal{F}$ e que $a\, p_2^{-1} = \overline{e}_1 \alpha + \overline{e}_2 \in \mathcal{Z}'$. O elemento $e_1 \alpha + e_2$ pertenceria igualmente ao centro de $\mathcal{G}$, o que não pode ter lugar.

Seja $\mathcal{G}$ uma soma directa de ideais bilaterais: $\mathcal{G} = \mathcal{A}_1 + \ldots + \mathcal{A}_s$. Sabemos que se tem $\mathcal{Z} = \mathcal{Z}_1 + \ldots + \mathcal{Z}_s$. É, então, válido o

Teorema:- O centro $\mathcal{Z}_\mathcal{F}$, de $\mathcal{G}_\mathcal{F}$, é da forma $\mathcal{Z}_\mathcal{F} = \mathcal{Z}_{1\mathcal{F}} + \ldots + \mathcal{Z}_{s\mathcal{F}}$. De facto, tem-se $\mathcal{G}_\mathcal{F} = \mathcal{A}_{1\mathcal{F}} + \ldots + \mathcal{A}_{s\mathcal{F}}$, como se reconhece tomando para base de $\mathcal{G}_\mathcal{F}$ o conjunto das s bases independentes dos $\mathcal{A}_i$. Os $\mathcal{A}_{i\mathcal{F}}$ continuam a ser ideais bilaterais de $\mathcal{G}_\mathcal{F}$, valendo $\mathcal{Z}_\mathcal{F} = \mathcal{Z}_{1\mathcal{F}} + \ldots + \mathcal{Z}_{s\mathcal{F}}$, onde os $\mathcal{Z}_{i\mathcal{F}}$ são, simultâneamente, centros dos $\mathcal{A}_{i\mathcal{F}}$ e ampliação dos centros $\mathcal{Z}_i$.

Se $\mathcal{G}$ é semi-simples e os $\mathcal{A}_i$ são simples, a decomposição de $\mathcal{G}$ é bem determinada. Os $\mathcal{Z}_i$ são corpos comutativos, como já dissemos. Ao passarmos ao sistema ampliado $\mathcal{G}_\mathcal{F}$, continua a haver elemento um, mas não podemos afirmar que $\mathcal{G}_\mathcal{F}$ subsista como

anel completamente redutível.

Em qualquer álgebra $\mathcal{A}$, o conjunto dos seus elementos que comutam com cada elemento dum sub-conjunto $\mathcal{L}$, de $\mathcal{A}$, constitui uma sub-álgebra de $\mathcal{A}$, chamado o comutador de $\mathcal{L}$. O centro duma álgebra é, assim, o seu próprio comutador.

12) Álgebras normais - Uma álgebra com elemento um diz-se normal, quando o seu centro se reduz ao corpo fundamental (estamos supondo, como sempre se tem feito, que $\mathcal{K}$ pertence à álgebra).

Tomemos uma álgebra $\mathcal{A}$, de ordem n, com elemento um, e suponhamos que o seu centro $\mathcal{Z}$ é uma álgebra de divisão. $\mathcal{Z}$ é uma ampliação finita de $\mathcal{K}$ e $\mathcal{A}$ é uma álgebra de ordem s sobre $\mathcal{Z}$. $\mathcal{A}$ e $\mathcal{Z}$ têm o mesmo elemento um, valendo a relação $n = ms$. Pode enunciar-se o

Teorema:- Se $\mathcal{A}$ é uma álgebra de ordem n, com elemento um, sobre $\mathcal{K}$, e se o seu centro $\mathcal{Z}$ é uma álgebra de divisão de ordem m, $\mathcal{A}$ é uma álgebra normal sobre $\mathcal{Z}$, de ordem s, tal que $n=sm$.

Uma álgebra de divisão, por ex., é sempre uma álgebra normal sobre o seu centro.

São de interesse as proposições a seguir, relativas a produtos directos de álgebras normais.

Teorema:- Se $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2$ for o produto directo de duas sub-álgebras, a primeira das quais é normal, a álgebra $\mathcal{A}_2$ é o comutador de $\mathcal{A}_1$ e o centro de $\mathcal{A}$ é o centro de $\mathcal{A}_2$. O corpo fundamental $\mathcal{K}$ está contido em $\mathcal{A}_1$, por hipótese. $\mathcal{A}_2$ é sub-álgebra de $\mathcal{A}$. Um elemento $\alpha \in \mathcal{A}$ tem a forma $\alpha = \sum_j b'_j v_j$, com $b'_j \in \mathcal{A}_1$ (§ 4 deste Capítulo). Esta representação de α é única, pois que, pondo $\sum b'_j v_j = \sum b_j v_j$, $b'_j = \sum_i u_i \lambda'_{ij}$, $b_j = \sum_i u_i \lambda_{ij}$, onde λ'_{ij} , $\lambda_{ij} \in \mathcal{K}$, tem-se $\sum_{ij} u_i v_j (\lambda'_{ij} - \lambda_{ij}) = 0$, ou seja $\lambda'_{ij} = \lambda_{ij}$. Suponhamos α pertencente ao comutador de $\mathcal{A}_1$. Para cada $h_1 \in \mathcal{A}_1$, tem-se

$$\alpha h_1 = h_1 \alpha = \sum_j b'_j h_1 v_j = \sum h_1 b'_j v_j , \quad \sum_j (b'_j h_1 - h_1 b'_j) v_j = 0 .$$

Conclui-se, assim, $b'_j h_1 = h_1 b'_j$, e, portanto, os coeficientes b'_j

pertencem ao centro de $\mathcal{A}_1$, ou seja a $\mathcal{K}$. O elemento α pertencerá a $\mathcal{A}_2$. Como os elementos deste último comutam com os de $\mathcal{A}_1$, segue-se que $\mathcal{A}_2$ é o comutador de $\mathcal{A}_1$. Os elementos do centro de $\mathcal{A}$ comutam com os elementos de $\mathcal{A}_1$, e, por isso, o centro de $\mathcal{A}$ está em $\mathcal{A}_2$. Será o centro de $\mathcal{A}_2$.

Teorema:- O produto directo de duas álgebras normais é uma álgebra normal, e, inversamente, posta uma álgebra normal sob a forma de produto directo, em que um dos factores é uma sub-álgebra com o elemento um da álgebra, cada factor é uma álgebra normal. Se, em $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2$, os dois factores directos forem normais, ambos eles se podem considerar sub-álgebras de $\mathcal{A}$. Nesse caso, o centro de $\mathcal{A}$, como centro de $\mathcal{A}_2$ (por ex.), é o corpo $\mathcal{K}$. Logo, $\mathcal{A}$ é normal. Inversamente, se $\mathcal{A}$ é normal e tem a citada forma de produto, $\mathcal{A}_2$ também é sub-álgebra de $\mathcal{A}$. O centro de $\mathcal{A}_1$ pertence ao centro de $\mathcal{A}$ e é, pois, o corpo fundamental. Como $\mathcal{A}_1$ é normal, o centro de $\mathcal{A}$ é o centro de $\mathcal{A}_2$, de modo que esta é também uma álgebra normal.

Consideremos a álgebra $\mathcal{A}$. Se $\mathcal{A}_1$ e $\mathcal{A}_2$ são sub-álgebras, o produto $\mathcal{A}_1 \mathcal{A}_2$ não é geralmente uma sub-álgebra. No caso de se ter $\mathcal{A}_1 \mathcal{A}_2 = \mathcal{A}_2 \mathcal{A}_1$, estamos já em presença duma sub-álgebra. Se o produto tiver uma ordem com respeito ao corpo fundamental que seja o produto das ordens dos factores, vê-se que se tem $\mathcal{A}_1 \mathcal{A}_2 = \mathcal{A}_1 \times \mathcal{A}_2$. Podemos fixar o

Teorema:- Se duas sub-álgebras comutam, o seu produto é directo, se tiver por ordem o produto das ordens dos factores.

Teorema:- Se $\mathcal{A}_1 = \mathcal{J}$ é uma sub-álgebra normal de divisão de $\mathcal{A}$ e se $\mathcal{A}_2$ é uma segunda sub-álgebra, de elementos individualmente comutáveis com os da primeira e com o mesmo elemento um que esta, o produto $\mathcal{J}\mathcal{A}_2$ é directo. A álgebra $\mathcal{J}\mathcal{A}_2$ é módulo com respeito a $\mathcal{J}$. O teorema reduz-se a provar que a sua ordem relativamente a $\mathcal{J}$ é a mesma que a ordem de $\mathcal{A}_2$ relativamente ao corpo fundamental inicial $\mathcal{K}$. Pondo $\mathcal{A}_2 = \mathcal{A}_2(u_1, \ldots, u_n)$, tem-se $\mathcal{J}\mathcal{A}_2 = (\mathcal{J}u_1, \ldots, \mathcal{J}u_n)$. No caso de, apenas, os primeiros r dos u_i serem independentes relativamente a $\mathcal{J}$, é mais simplesmente,

$$\mathcal{J}\mathcal{A}_2 = \mathcal{J}u_1 + \cdots + \mathcal{J}u_r .$$

Se pudesse supor-se $r < n$, seria, por ex.,

$$u_{r+i} = d_1 u_1 + \cdots + d_r u_r \ , \qquad (d_i \in \mathfrak{D}) \ ,$$

e, para cada $d \in \mathfrak{D}$, ter-se-ia

$$d u_{r+i} = u_{r+i} d \ , \qquad d d_i = d_i d \ ,$$

de sorte que os coeficientes d_i pertenceriam ao centro de $\mathfrak{D}$, ou seja a $\mathfrak{K}$. O elemento u_{r+i} não seria, em face de $\mathfrak{K}$, independente dos primeiros r dos u_i, contra a hipótese. O teorema está provado.

Seja $\mathfrak{D}$ uma álgebra normal de divisão. Se $\mathfrak{U}$ é a sua 1ª representação regular (directa) e $\mathfrak{U}'''$ a sua 2ª representação regular (recíproca), as duas sub-álgebras $\mathfrak{U}$ e $\mathfrak{U}'''$, da álgebra total $\mathfrak{M}_n$ de matrizes, estão nas condições do teorema anterior, de modo que o produto $\mathfrak{U} \times \mathfrak{U}'''$ é de ordem n^2. Isto significa $\mathfrak{U} \times \mathfrak{U}''' = \mathfrak{M}_n$ e permite enunciar o seguinte

Teorema:- Se $\mathfrak{D}$ é uma álgebra normal de divisão e $\mathfrak{D}^{-1}$ a sua álgebra recíproca, o produto $\mathfrak{D} \times \mathfrak{D}^{-1}$ é uma álgebra completa de matrizes.(1)

Terminaremos o § com algumas observações úteis, que relembram factos anteriormente demonstrados. Seja $\mathfrak{Y}$ um anel simples. Sabemos que $\mathfrak{Y}$ admite uma base de n^2 matrizes e_{ij} e é um módulo finito relativamente a um corpo $\mathfrak{L}$, conjunto dos elementos de $\mathfrak{Y}$ que comutam com todos os e_{ij}. Não se trata duma álgebra sobre $\mathfrak{L}$, visto que este não é geralmente comutativo. Considerando, porém, um anel completo de matrizes, $\mathfrak{M}_n = \mathfrak{K}_n$, com elementos do corpo comutativo $\mathfrak{K}$, estamos na presença dum anel simples que é uma álgebra sobre $\mathfrak{K}$. O centro da álgebra é formado pelas matrizes diagonais de elementos iguais. É isomorfo de $\mathfrak{K}$, de modo que $\mathfrak{K}_n$ se pode considerar álgebra normal sobre $\mathfrak{K}$. Se uma álgebra qualquer $\mathfrak{Y}$, sobre $\mathfrak{K}$, com elemento um, tem uma sub álgebra $\mathfrak{U}_n$, isomorfa dum anel completo de matrizes $\mathfrak{K}_n$, e com o mesmo elemento um que $\mathfrak{Y}$, vimos no § 4 que vale a igualdade $\mathfrak{Y} = \mathfrak{U}_n \times \mathfrak{L}$, onde os elementos de $\mathfrak{L} \cong \mathfrak{Y}$ comutam indi-

(1) Os teoremas sobre álgebras normais são tirados de A.A.Albert, "Structure of algebras", pgs.41 e 42.

vidualmente com os de $\mathfrak{U}_n$, e o elemento um de $\mathfrak{L}$ é o de $\mathfrak{Y}$. Sabemos agora que o centro de $\mathfrak{Y}$ é o centro de $\mathfrak{L}$, pois, ao escrever-se $\mathfrak{Y} = \mathfrak{Y}_1 \times \mathfrak{Y}_2$, com $\mathfrak{Y}_1$ = sub-álgebra normal de $\mathfrak{Y}$ e $\mathfrak{Y}_2$ sub-álgebra de $\mathfrak{Y}$, $\mathfrak{Y}_2$ é necessàriamente o comutador de $\mathfrak{Y}_1$, e, além disso, tem por centro o centro de $\mathfrak{Y}$.

Seja $\mathfrak{Y} \cong \mathfrak{K}$ uma álgebra simples sobre $\mathfrak{K}$. Escrevendo, sob a forma de produto de Wedderburn, $\mathfrak{Y} = (\ldots e_{ij} \ldots) \times \mathfrak{L}$, o corpo $\mathfrak{L}$ contém necessàriamente o corpo $\mathfrak{K}$. Se considerarmos a álgebra $\mathfrak{Y}' = (\ldots e_{ij} \ldots) \times \mathfrak{K}$, vê-se que $\mathfrak{Y}$ aparece como o produto directo $\mathfrak{Y} = \mathfrak{Y}' \times \mathfrak{L}$, da sub-álgebra normal $\mathfrak{Y}'$ e da sub-álgebra de divisão $\mathfrak{L}$ (sobre $\mathfrak{K}$). Tem lugar o

Teorema:- Uma álgebra simples $\mathfrak{Y}$, sobre $\mathfrak{K}$, é o produto directo duma álgebra normal $\mathfrak{Y}'$ sobre $\mathfrak{K}$ (álgebra completa de matrizes) e duma álgebra de divisão $\mathfrak{L}$. $\mathfrak{L}$ é o comutador de $\mathfrak{Y}'$; o centro $\mathfrak{Z}$, de $\mathfrak{Y}$, é o centro de $\mathfrak{L}$. $\mathfrak{Z}$ é um corpo comutativo intermédio entre $\mathfrak{K}$ e $\mathfrak{L}$, e a álgebra $\mathfrak{Y}$, como álgebra sobre $\mathfrak{Z}$, é normal e simples.

Imaginemos duas decomposições da álgebra simples $\mathfrak{Y}$, da forma

$$\mathfrak{Y} = \mathfrak{U}_n \times \mathfrak{L} = \mathfrak{U}'_m \times \mathfrak{L}' \ ,$$

onde $\mathfrak{L}$ e $\mathfrak{L}'$ são álgebras de divisão sobre $\mathfrak{K}$ e $\mathfrak{U}_n, \mathfrak{U}'_m$ são sub-álgebras de $\mathfrak{Y}$ com o mesmo elemento um que esta, ambas elas álgebras completas de matrizes com elementos de $\mathfrak{K}$. Então, tem-se

$$\mathfrak{Y} = \mathfrak{L}_n = \mathfrak{L}'_m \ .$$

Sob esta forma, vê-se que $\mathfrak{L}$ e $\mathfrak{L}'$ são isomorfas, pois ambas elas são isomorfas dos corpos endomórficos dos ideais direitos simples em que pode decompor-se $\mathfrak{Y}$. É, portanto, $\mathfrak{L} \cong \mathfrak{L}'$. Neste isomorfismo, o corpo fundamental $\mathfrak{K}$ é conservado, de modo que se trata dum isomorfismo operatório relativamente a $\mathfrak{K}$. Se for N a ordem de $\mathfrak{Y}$ e r a ordem comum de $\mathfrak{L}$ e $\mathfrak{L}'$, ter-se-à $N = n^2 r = m^2 r$, e, pois, $n = m$. Sabemos agora que existe um automorfismo interno levando de $\mathfrak{U}_n$ a $\mathfrak{U}'_n$ e de $\mathfrak{L}$ a $\mathfrak{L}'$. Enuncia-se o seguinte

Teorema:- Uma decomposição duma álgebra simples $\mathcal{G}$, sobre $\mathcal{K}$, sob a forma de produto directo duma álgebra completa de matrizes por uma álgebra de divisão, é uma decomposição unívoca, pondo de parte os automorfismos internos de $\mathcal{G}$. Pode dizer-se, de resto, que se põem de parte todos os automorfismos da álgebra, pelo facto de haver apenas automorfismos internos de $\mathcal{G}$.

Corolário:- Se o produto $\mathcal{G}\times\mathcal{L}=\mathcal{O}_n$, da álgebra normal de divisão $\mathcal{G}$, sobre $\mathcal{K}$, pela álgebra de divisão $\mathcal{L}$, for uma álgebra completa de matrizes (sobre $\mathcal{K}$), $\mathcal{L}$ é equivalente a $\mathcal{G}^{-1}$.

De facto, tem-se

$$\mathcal{G}^{-1}\times\mathcal{G}\times\mathcal{L}=\mathcal{O}_m^i\times\mathcal{L}=\mathcal{O}_n\times\mathcal{G}^{-1}.$$

Portanto, é $m = n$, $\mathcal{L}\cong\mathcal{G}^{-1}$, com conservação de $\mathcal{K}$ no isomorfismo.

Capítulo VII

Sobre as álgebras simples

1) Sobre as ampliações algébricas dos corpos comutativos- O objectivo deste Capítulo é a indicação das propriedades mais elementares das álgebras simples, no tocante a ampliações e a produtos directos em que as mesmas intervenham. Uma ampliação comutativa dum corpo $\mathcal{K}$ é uma álgebra sobre $\mathcal{K}$. Se a ampliação é algébrica e finita, tem-se uma álgebra associativa finita ou um sistema hiper-complexo sobre $\mathcal{K}$. Estas ampliações realizam os primeiros exemplos de álgebras simples sobre $\mathcal{K}$.

Partiremos aqui das noções elementares seguintes:(1) 1) de ampliação dum corpo por adjunção de elementos (A, pgs.23 a 27); 2) de corpo primo e de característica dum corpo (A, pgs.43 a 45); 3) de ampliação algébrica (A, pgs.166 a 180); 4) de grau, grau reduzido e de expoente dum elemento algébrico relativamente a um corpo $\mathcal{K}$ (A, pgs.72 a 78); 5) de corpo de decomposição duma função inteira (A, pgs.180 a 183).

A letra $\mathcal{L}$ designará neste § uma ampliação finita dum corpo $\mathcal{K}$, de característica p. Como se disse, uma tal ampliação é uma álgebra finita sobre $\mathcal{K}$. O número de elementos independentes de $\mathcal{L}$ diz-se grau e representa-se por $(\mathcal{L}/\mathcal{K})$. Se $u_1,\ldots,u_n$ constituirem uma base de $\mathcal{L}$, escreveremos $\mathcal{L}=\mathcal{K}\{u_1,\ldots,u_n\}$. A notação $\mathcal{K}(u_1,\ldots,u_n)$ fica reservada para o corpo que resulta de $\mathcal{K}$ por adjunção algébrica dos elementos $u_1,\ldots,u_n$. Por ex., fazendo a adjunção a $\mathcal{K}$ dum elemento algébrico Θ, raiz duma equação irredutível em $\mathcal{K}$, do grau n, tem-se

$$\mathcal{K}(\Theta)=\mathcal{K}\left\{u,\Theta,\ldots,\Theta^{n-1}\right\}.$$

(1) Utilizaremos aqui a designação de "A, pgs.23", etc., para significar "Elementos da Teoria dos Anéis, pgs.23". A doutrina que vai ser exposta neste §, devida a E. Steinitz, constitui uma parte da memória deste grande algebrista publicada no "Journal für die reine und angewandte Mathematik", Band 137, 1910, sob o título "Algebraische Theorie der Körper". Aqui cingimo-nos a van der Waerden, "Moderne Algebra", I Teil, Cap.V, pgs.86 a 122, e a A.A.Albert, "Structure of algebras", pgs.32 a 35.

Seja α um elemento algébrico relativamente a $\mathcal{K}$. Se n é o seu grau, n_0 o grau reduzido e t o expoente, tem-se

$$n = n_0 p^t, \qquad (\mathcal{K}(\alpha^{p^t}) : \mathcal{K}) = n_0.$$

Lema 1:- Se é $\Theta \in \Omega \supset \mathcal{K}$, com $\Theta^{p^t} \in \mathcal{K}$, $\Theta^{p^{t-1}} \notin \mathcal{K}$, a equação $f(x) = x^{p^t} - \Theta^{p^t} = x^{p^t} - k = 0$, $(k \in \mathcal{K})$, é irredutível em $\mathcal{K}$. Se fosse $f(x) = (x - \Theta)^{p^t} = g(x).h(x)$, com $g(x)$ irredutível em $\mathcal{K}$, seria $g(x) = (x - \Theta)^{p^{t-s}} = x^{p^{t-s}} - \Theta^{p^{t-s}}$, $(s \geq 1)$, e $\Theta^{p^{t-s}} \in \mathcal{K}$, contra a hipótese.

Teorema 1:- É condição necessária e suficiente, para que $f(x) = x^{p^t} - k = 0$, $(k \in \mathcal{K})$, seja irredutível em $\mathcal{K}$, que, para cada $\beta \in \mathcal{K}$, seja $\beta^p \neq k$. A condição é necessária: se $f(x) = x^{p^t} - k$ é irredutível, se fosse $\beta^p = k$, ter-se-ia $f(x) = x^{p^t} - k = x^{p^t} - \beta^p = (x^{p^{t-1}} - \beta)^p$, $(\beta \in \mathcal{K})$, e, consequentemente, $f(x)$ seria redutível. A condição é suficiente: se não existe $\beta \in \mathcal{K}$ tal que $\beta^p = k$, designemos por Θ uma raiz da equação $x^{p^t} - k = 0$. Será $\Theta^{p^t} = k$, e $\Theta^{p^{t-1}} \notin \mathcal{K}$. Então, em face do lema, a equação é irredutível em $\mathcal{K}$.

Dado um corpo $\mathcal{K}$, seja Θ uma raiz dum polinómio irredutível de $\mathcal{K}[x]$. Se esse polinómio só tiver raizes simples, diz-se um elemento separável relativamente a $\mathcal{K}$. Se Ω é uma ampliação algébrica de $\mathcal{K}$ e se todos os seus elementos são separáveis, Ω diz-se uma ampliação separável de $\mathcal{K}$. Uma ampliação algébrica não separável diz-se inseparável.

Teorema 2:- É condição necessária e suficiente, para que Θ seja separável relativamente a $\mathcal{K}$, que se tenha $\mathcal{K}(\Theta^p) = \mathcal{K}(\Theta)$. Se Θ é separável, não pode ser $\mathcal{K}(\Theta^p) \subset \mathcal{K}(\Theta)$, visto que, de contrário, a equação $x^p - \Theta^p = 0$ seria irredutível em $\mathcal{K}(\Theta^p)$, e, portanto, Θ seria inseparável relativamente a este último corpo e a $\mathcal{K}$. A suficiência resulta do facto de ser $\left(\mathcal{K}(\Theta) : \mathcal{K}(\Theta^p) \right) = p$, quando Θ é inseparável.

Teorema 3:- Se Θ é um elemento separável relativamente a $\mathcal{K}$, $\mathcal{K}(\Theta)$ é uma ampliação separável de $\mathcal{K}$. (A, pgs. 194 e 195).

Teorema 4:- Se $\Theta_1, \ldots, \Theta_r$ são elementos algébricos relativamente a $\mathcal{K}$, de tal sorte que Θ_i seja do grau reduzido n_i relativamente a $\mathcal{K}(\Theta_1, \ldots, \Theta_{i-1})$, é possivel construir um corpo $\Omega \supseteq \mathcal{L} = \mathcal{K}(\Theta_1, \ldots, \Theta_r)$ no qual $\mathcal{L}$ admite $T = \prod_{i=1}^{r} n_i$ isomorfismos relativos com respeito a $\mathcal{K}$, não existindo corpo contendo $\mathcal{K}$ e $\mathcal{L}$ onde haja mais do que esse número de isomorfismos relativos (A, pgs. 200 a 202).

Teorema 5:- A ampliação finita $\mathcal{L} = \mathcal{K}(\alpha, \beta, \ldots, \lambda)$, na qual $\beta, \ldots, \lambda$ são elementos separáveis relativamente a $\mathcal{K}$, é uma ampliação simples de $\mathcal{K}$ (A, pgs. 199 e 200). Deve notar-se que nenhuma hipótese se faz quanto ao elemento algébrico α.

Teorema 6:- A ampliação finita $\mathcal{L} = \mathcal{K}(\alpha, \beta, \ldots, \lambda)$, na qual $\alpha, \ldots, \lambda$ são elementos separáveis relativamente a $\mathcal{K}$, é uma ampliação separável simples de $\mathcal{K}$. O teorema 5 garante que a ampliação é simples. O teorema 4 garante que existe um corpo Ω onde o número de isomorfismos relativos de $\mathcal{L}$ com respeito a $\mathcal{K}$ é igual ao grau $(\mathcal{L} : \mathcal{K})$. Como uma tal propriedade é independente dos elementos de $\mathcal{L}$ que se adjuntam a $\mathcal{K}$, seja $\Theta \in \mathcal{L}$ um elemento qualquer e ponhamos $\mathcal{L} = \mathcal{K}(\Theta, \Theta', \ldots, \Theta^{(s)})$. Θ é separável relativamente a $\mathcal{K}$, porque, se fosse inseparável, o número máximo possível de isomorfismos relativos de $\mathcal{L}$ com respeito a $\mathcal{K}$ seria inferior ao grau $(\mathcal{L} : \mathcal{K})$.

Numa ampliação qualquer Ω, de $\mathcal{K}$, o conjunto dos elementos de Ω que são separáveis relativamente a $\mathcal{K}$ constitui um corpo $\Omega_0 \subseteq \Omega$. Seja a ampliação $\mathcal{L}$ e ponhamos $(\mathcal{L} : \mathcal{K}) = N$. Para a ampliação separável finita $\mathcal{L}_0$, de $\mathcal{K}$, contida em $\mathcal{K}$, poremos $(\mathcal{L}_0 : \mathcal{K}) = N_0$. N_0 diz-se grau reduzido de $\mathcal{L}$ relativamente a $\mathcal{K}$. Seja $\alpha \in \mathcal{L}$ e t o seu expoente. Diz-se expoente de $\mathcal{L}$, e representa-se por e, o valor máximo (limitado) de t.

Teorema 7:- O grau reduzido dum elemento $\alpha \in \mathcal{L}$ divide o grau reduzido de $\mathcal{L}$. De facto verifica-se imediatamente que $\alpha^{p^t} \in \mathcal{L}_0$ e que $\alpha^{p^{t-1}} \notin \mathcal{L}_0$. Nessas condições tem-se, como se quer,

$$N_0 = \left(\mathcal{L}_0 / \mathcal{K}(\alpha^{p^t})\right) . n_0 .$$

Teorema 8:- O grau $(\mathcal{L}/\mathcal{L}_0)$ é uma potência p^f, com $f \geqq e$. Designemos por Θ_1 um elemento de $\mathcal{L}$ de expoente e, ponhamos $\mathcal{L}_0(\Theta_1) = \mathcal{L}_1$ e admitamos que é $\mathcal{L} = \mathcal{L}_0(\Theta_1, \Theta_2, \ldots, \Theta_r)$, onde Θ_2 não pertence a $\mathcal{L}_1$, Θ_3 não pertence a $\mathcal{L}_1(\Theta_2) = \mathcal{L}_2$, etc. Por ser Θ_1 raiz da equação irredutível em $\mathcal{L}_0$, $x^{p^e} - \Theta_1^{p^e} = 0$, vê-se que é $(\mathcal{L}_1/\mathcal{L}_0) = p^e$. Se $\Theta_2 \notin \mathcal{L}_1$ é um elemento de expoente t_2 relativamente a $\mathcal{K}$, tem-se $\Theta_2^{p^{t_2}} \in \mathcal{L}_0, \mathcal{L}_1$, e existe um inteiro mínimo $\theta_2 \leqq t_2$ tal que $\Theta_2^{p^{\theta_2}} \in \mathcal{L}_1$ e tal que $x^{p^{\theta_2}} - \Theta_2^{p^{\theta_2}} = 0$ é uma equação irredutível em $\mathcal{L}_1$. Será $(\mathcal{L}_2/\mathcal{L}_1) = p^{\theta_2}$. A continuação do raciocínio leva ao teorema.

Como consequência dos teoremas 7) e 8), tira-se agora o

Teorema 9:- N é múltiplo de $N_0 p^e$ e $n = n_0 p^t$ é sub-múltiplo do mesmo número. Vimos, com efeito, que era

$$N = (\mathcal{L}/\mathcal{K}) = (\mathcal{L}/\mathcal{L}_0)\,(\mathcal{L}_0/\mathcal{K}) = p^f . N_0 , \qquad (f \geqq e),$$

$$N_0 p^e = \left(\mathcal{L}_0 / \mathcal{K}(\alpha^{p^t})\right) . n_0 . p^e = \left(\mathcal{L}_0 / \mathcal{K}(\alpha^{p^t})\right) . n . p^{e-t} , \quad (n = n_0 p^t ; t \leqq e).$$

Teorema 10:- É condição necessária e suficiente, para que $\mathcal{L}$ seja simples, que se tenha $f = e$. Se é $\mathcal{L} = \mathcal{K}(\alpha)$, tem-se

$$N = (\mathcal{L}/\mathcal{K}) = \left(\mathcal{K}(\alpha)/\mathcal{K}\right) = N_0 p^f = n_0 p^t ,$$

e, portanto, visto ser $n_0 \leqq N_0$, $t \leqq e \leqq f$, conclui-se $n_0 = N_0$, $t = e = f$. Inversamente, supondo $N = N_0 p^e$, tomemos um elemento $\Theta \in \mathcal{L}$ de expoente e. Sendo $\left(\mathcal{L}(\Theta)/\mathcal{L}_0\right) = p^e$, a relação $\left(\mathcal{L}_0(\Theta)/\mathcal{K}\right) = p^e . N_0$ mostra que é $\mathcal{L} = \mathcal{L}_0(\Theta)$. Ora $\mathcal{L}_0$ é uma ampliação simples de $\mathcal{K}$ da forma $\mathcal{L}_0 = \mathcal{K}(\Theta')$, de modo que $\mathcal{L} = \mathcal{K}(\Theta, \Theta') = \mathcal{K}(\Theta'')$, visto que Θ' é separável relativamente

a $\mathcal{K}$. O teorema está demonstrado.

Em $\mathcal{L}$ há sempre, por definição, elementos de expoente igual ao expoente e, de $\mathcal{L}$. Há também elementos de expoente reduzido $n_0 = N_0$, em virtude do seguinte

Teorema 11:- É condição necessária e suficiente, para que $\alpha \in \mathcal{L}$ seja do grau reduzido N_0, que se tenha $\mathcal{L}_0(\alpha) = \mathcal{K}(\alpha)$. Se é $n_0 = N_0$, tem-se $\left(\mathcal{K}(\alpha)/\mathcal{K}\right) = N_0 p^t$. Como $\left(\mathcal{L}_0(\alpha)/\mathcal{L}_0\right) = p^t$, vem $\left(\mathcal{L}_0(\alpha)/\mathcal{K}\right) = N_0 p^t$, de modo que a condição é necessária. Inversamente, supondo $\mathcal{L}_0(\alpha) = \mathcal{K}(\alpha)$, é $\left(\mathcal{K}(\alpha)/\mathcal{K}\right) = n_0 = n_0 p^t = \left(\mathcal{L}_0(\alpha)/\mathcal{K}\right) = p^t N_0$.

Existem elementos separáveis Θ que satisfazem ao teorema: são todos aqueles para os quais é $\mathcal{L}_0 = \mathcal{K}(\Theta)$ e apenas esses. Há também elementos inseparáveis μ nas condições do teorema: são todos aqueles para os quais é $\mathcal{K}(\mu) \supset \mathcal{L}_0$, e apenas esses. Se supusermos $\mathcal{L}_0 = \mathcal{K}(\Theta)$, é, para cada elemento inseparável $\alpha \in \mathcal{L}$,

$$\mathcal{K}(\Theta, \alpha) = \mathcal{K}(\alpha, \Theta) = \mathcal{L}_0(\alpha) = \mathcal{K}(\mu) \supset \mathcal{L}_0 .$$

Teorema 12:- Em $\mathcal{L}$ há elementos simultâneamente de grau reduzido N_0 e de expoente t = expoente dum elemento arbitrário $\alpha \in \mathcal{L}$. Ponhamos $\mathcal{L}_0 = \mathcal{K}(\Theta)$ e tomemos $\alpha \in \mathcal{L}$, de expoente t. Tem-se $\mathcal{L}_0(\alpha) = \mathcal{K}(\Theta, \alpha) = \mathcal{K}(\lambda)$. O elemento λ é de grau reduzido N_0. Como $\mathcal{K}(\lambda)$ é uma ampliação simples, na qual o corpo separável relativamente a $\mathcal{K}$ é ainda $\mathcal{L}_0$, pode escrever-se, se e' é o seu expoente,

$$\left(\mathcal{K}(\lambda)/\mathcal{K}\right) = N_0 p^{e'} = \left(\mathcal{L}_0(\alpha)/\mathcal{L}_0\right) . N_0 = p^t N_0 ,$$

donde se conclui o teorema. Em particular, há em $\mathcal{L}$ elementos de grau reduzido N_0 e de expoente $t = e$ = expoente de $\mathcal{L}$. O número t toma, de resto, todos os valores inteiros satisfazendo a $0 \leqq t \leqq e$, visto que, se α é de expoente e, α^p é de expoente $e-1$, α^{p^2} de expoente $e-2$, etc.

Seja Ω uma ampliação algébrica de $\mathcal{K}$. Representaremos por $\Omega^{(p)}$ o corpo que resulta de $\mathcal{K}$ por adjunção de todas as potências ω^p dos elementos $\omega \in \Omega$. Mais geralmente, escreveremos $\Omega^{(p^t)}$ para significar o corpo que resulta de $\mathcal{K}$ por adjun-

ção das potências ω^{p^r}.

Teorema 13:- Se Ω é uma ampliação separável de $\mathcal{K}$, tem-se $\Omega^{(p)} = \Omega$. De facto, seja $\alpha \in \Omega$. Como é $\mathcal{K}(\alpha^p) = \mathcal{K}(\alpha)$, é $\alpha \in \mathcal{K}(\alpha^p) \equiv \Omega^{(p)}$, q. e. d.

Suponhamos $\Omega = \mathcal{L} = \mathcal{K}\{u_1, \ldots, u_n\}$ uma ampliação inseparável. Se fizermos a adjunção a $\mathcal{K}$ dos elementos $u_1^{p^r}, \ldots, u_n^{p^r}$, obtem-se um corpo $\triangle = \mathcal{K}(u_1^{p^r}, \ldots, u_n^{p^r})$, contido em $\mathcal{L}^{(p^r)}$. Um elemento deste último pertence, porém, a um corpo $\mathcal{K}(\xi_1^{p^r}, \ldots, \xi_s^{p^r})$, no qual se tem $\xi_i^{p^r} = u_1^{p^r} k_1^{p^r} + \ldots + u_n^{p^r} k_n^{p^r}$, pondo $\xi_i = u_1 k_1 + \ldots + u_n k_n$, $(k_i \in \mathcal{K})$. Sendo $\mathcal{K}(\xi_1^{p^r}, \ldots, \xi_n^{p^r}) \equiv \triangle$, tem-se $\mathcal{L}^{(p^r)} \equiv \equiv \triangle$, e, portanto, $\mathcal{L}^{(p^r)} = \triangle$. Também se demonstram relações como a seguinte: $\mathcal{L}^{(p)(p)} = \mathcal{L}^{(p^2)}$. Na verdade, pondo $\mathcal{L}^{(p)} = \mathcal{K}(u_1^p, \ldots, u_n^p) = \mathcal{K}\{x_1, \ldots, x_t\}$, tem-se $\mathcal{L}^{(p)(p)} = \mathcal{K}(x_1^p, \ldots, x_t^p)$. Ora $u_i^{p^2}$ pertence a este último corpo, em virtude de ser $u_i^p \in \mathcal{K}\{x_1, \ldots, x_t\}$, e, portanto, é $\mathcal{L}^{(p^2)} \equiv \mathcal{L}^{(p)(p)}$. Inversamente, se tomarmos o polinómio nos u_k,

$$x_j = \sum b_{i_1 \ldots i_n}^{(j)} (u_1^p)^{i_1} \cdots (u_n^p)^{i_n},$$

com coeficientes em $\mathcal{K}$, vê-se ser x_j^p um polinómio nos $u_i^{p^2}$, com coeficientes em $\mathcal{K}$, pelo que se terá $\mathcal{L}^{(p)(p)} \equiv \mathcal{L}^{(p^2)}$. Podemos enunciar o seguinte

Teorema 14:- Se $\mathcal{L} = \mathcal{K}\{u_1, \ldots, u_n\}$ é uma ampliação finita de $\mathcal{K}$, tem-se $\mathcal{L}^{(p^r)} = \mathcal{K}(u_1^{p^r}, \ldots, u_n^{p^r})$ e $\mathcal{L}^{(p^{r+1})} = \mathcal{L}^{(p^r)(p)}$. A afirmação é também válida se supusermos $\mathcal{L} = \mathcal{K}(u_1, \ldots, u_n)$.

Teorema 15:- Se $\mathcal{L}$ é inseparável, tem lugar a relação $\mathcal{L} \supset \mathcal{L}^{(p)}$. Seja e o expoente de $\mathcal{L}$. Imaginando que poderia ter-se $\mathcal{L} = \mathcal{L}^{(p)} = \ldots = \mathcal{L}^{(p^e)} = \mathcal{K}(u_1^{p^e}, \ldots, u_n^{p^e})$, como os $u_i^{p^e}$ são elementos separáveis relativamente a $\mathcal{K}$, $\mathcal{L}$ seria uma ampliação separável, contra a hipótese.

Teorema 16:- É válida a igualdade $\mathcal{L}_0 = \mathcal{L}^{(p^e)}$. Já sabemos que se tem $\mathcal{L}^{(p^e)} \equiv \mathcal{L}_0$. A relação inversa tem também lugar, porque, se $\alpha \in \mathcal{L}_0$, valem as igualdades $\mathcal{K}(\alpha) = \mathcal{K}(\alpha^p) = \ldots = \mathcal{K}(\alpha^{p^e}) = \equiv \mathcal{L}^{(p^e)}$, o que mostra ser $\alpha \in \mathcal{L}^{(p^e)}$.

Resulta daqui que, se considerarmos a cadeia

$$\mathcal{L} \supset \mathcal{L}^{(p)} \supset \mathcal{L}^{(p^2)} \supset \ldots, \qquad (1)$$

a mesma, que é necessàriamente finita, termina na ampliação separável $\mathcal{L}_0 = \mathcal{L}^{(p^e)}$, de $\mathcal{K}$. O expoente e, além de poder caracterizar-se com o comprimento da cadeia (1), pode também definir-se como o máximo dos expoentes t_i dos elementos u_i, da base de $\mathcal{L}$. Se e' for esse máximo, tem-se, com efeito, $\mathcal{L}^{(p^{e'-1})} \supset \mathcal{L}_0 \equiv \mathcal{L}^{(p^{e'})}$.

Um teorema que pode enunciar-se é o seguinte:

Teorema 17:- É condição necessária e suficiente, para que $\mathcal{L}$ seja ampliação simples de $\mathcal{K}$, que se tenha $\triangle = \left(\mathcal{L}^{(p^i)} / \mathcal{L}^{(p^{i+1})}\right) = p$, para cada $i \equiv e-1$. É claro, com efeito, que o grau $\triangle$ é uma potência de p. Por ex., de

$$(\mathcal{L}/\mathcal{K}) = (\mathcal{L}/\mathcal{L}^{(p)})\ (\mathcal{L}^{(p)}/\mathcal{L}_0)\ (\mathcal{L}_0/\mathcal{K}) = N_0 p^f,$$

tira-se $(\mathcal{L}/\mathcal{L}^{(p)})\ (\mathcal{L}^{(p)}/\mathcal{L}_0) = p^f$.

No caso das ampliações simples, cada corpo $\mathcal{L}^{(p^{e-k})}$ é também o corpo $\mathcal{L}_k$, conjunto dos elementos de $\mathcal{L}$ de expoente $\equiv k$. Para o ver, basta notar que, na cadeia $\mathcal{L}_0 \subset \mathcal{L}_1 \subset \mathcal{L}_2 \subset \ldots \subset \mathcal{L}_e = \mathcal{L}$, não pode ter lugar o sinal =, pois, se α é de expoente e, $\alpha^{p^e} \in \mathcal{L}_0$; $\alpha^{p^{e-1}} \in \mathcal{L}_1$, mas não a $\mathcal{L}_0$; $\alpha^{p^{e-2}} \in \mathcal{L}_2$, mas não a $\mathcal{L}_1$, etc.; e notar ainda que o grau dum $\mathcal{L}_i$ relativamente a $\mathcal{K}$ é necessàriamente uma potência de p.

Seja Ω uma ampliação algébrica inseparável de $\mathcal{K}$, finita ou não. Se o grau reduzido de cada elemento $\alpha \in \Omega$ for a

unidade, Ω diz-se uma ampliação inseparável pura (abrev. ampliação pura) de $\mathcal{K}$. Quando $\underline{\alpha}$ pertence a $\mathcal{K}$, é verificada a equação irredutível em $\mathcal{K}$, $x-\alpha=0$; mas, se $\alpha \notin \mathcal{K}$, como a equação irredutível tem as raizes todas iguais, ela será da forma $x^{p^t}-\alpha^{p^t}=0$. Reciprocamente, se cada elemento $\alpha \in \Omega \supset \mathcal{K}$ verifica uma equação irredutível em $\mathcal{K}$ da forma anterior ($t \neq 0$), o grau reduzido de $\underline{\alpha}$ é a unidade e a ampliação algébrica é pura. Vale o

Teorema 18:- É condição necessária e suficiente, para que a ampliação algébrica Ω, de $\mathcal{K}$, seja pura, que cada $\alpha \in \Omega$ verifique uma equação irredutível em $\mathcal{K}$ da forma $x^{p^t}-\alpha^{p^t}=0$.

Quando o corpo separável Ω_0 é idêntico a $\mathcal{K}$, cada elemento $\alpha \in \Omega$ satisfaz a uma equação irredutível em $\mathcal{K}$ da forma $x^{p^t}-\alpha^{p^t}=0$, de modo que Ω é ampliação pura. Inversamente, se Ω é ampliação pura, um elemento $\alpha \in \Omega$ que seja separável satisfaz a $x-\alpha=0$, de sorte que $\alpha \in \mathcal{K}$, $\Omega_0=\mathcal{K}$. Pode, pois, enunciar-se o

Teorema 19:- É condição necessária e suficiente, para que a ampliação algébrica Ω, de $\mathcal{K}$, seja pura, que se tenha $\Omega_0=\mathcal{K}$.

É claro que Ω é sempre ampliação pura de Ω_0. No caso duma ampliação finita $\mathcal{L}$, de $\mathcal{K}$, podemos caracterizá-la como ampliação pura pelo

Teorema 20:- É condição necessária e suficiente, para que a ampliação finita $\mathcal{L}$, de $\mathcal{K}$, seja pura, que o seu grau reduzido seja a unidade.

Corolário 1:- Se Θ satisfaz a uma equação irredutível em $\mathcal{K}$ da forma $x^{p^e}-\Theta^{p^e}=0$, a ampliação $\mathcal{K}(\Theta)$ é inseparável pura. Escrevendo, com efeito, $(\mathcal{K}(\Theta)/\mathcal{K}) = N_0 p^f = p^e$, ($f \neq e$), vê-se que se tem $N_0=1$.

Lema 2:- Se $\varphi(x)=0$ é uma equação do grau $n=n_0 p^t$, irredutível em $\mathcal{K}$, não pode, numa ampliação separável $\mathcal{M}$, de $\mathcal{K}$, ter-se $\varphi(x)=f(x).g(x)$, onde $f(x)$ é irredutível em $\mathcal{M}$ e

admite todas as raizes de $\varphi(x)$. Para o caso de se ter $t=0$, o teorema é banal. Se $t \neq 0$, ponhamos

$$\varphi(x)=\prod_{i=1}^{n_0}(x-\alpha_i)^{p^t}=\prod_{i=1}^{n_0}(x^{p^t}-\alpha_i^{p^t}), \qquad (\alpha_i \neq \alpha_j).$$

Se for

$$f(x)=\prod_{i=1}^{n_0}(x-\alpha_i)^{p^{t-k}}=\prod_{i=1}^{n_0}(x^{p^{t-k}}-\beta_i), \quad \begin{cases} \beta_i=\alpha_i^{p^{t-k}} \neq \beta_j, \\ k>0, \end{cases}$$

consideremos o polinómio

$$F(x)=\prod_{i=1}^{n_0}(x^{p^k}-\beta_i^{p^k})=\prod_{i=1}^{n_0}(x^{p^k}-\alpha_i^{p^t}) \in \mathcal{K}[x].$$

Vê-se que $F(x)$ é irredutível em $\mathcal{K}$, pelo facto de se ter $F(x^{p^{t-k}})=\varphi(x)$. Nessas condições, os elementos $\beta_1, \ldots, \beta_{n_0}$ são inseparáveis relativamente a $\mathcal{K}$. Ora a equação $\tau(x)=(x-\beta_1)\ldots(x-\beta_{n_0})=0$, com coeficientes pertencentes a $\mathcal{M}$, mostra que os elementos β_i são separáveis relativamente a $\mathcal{K}$, visto que são separáveis relativamente a $\mathcal{M}$ e esta é ampliação separável de $\mathcal{K}$.(1)

Teorema 21:- Se a equação $\varphi(x)=x^{p^t}-\alpha=0$ é irredutível em $\mathcal{K}$, é irredutível em qualquer ampliação separável, $\mathcal{M}$, daquele corpo. Supondo $\varphi(x)=x^{p^t}-\alpha=(x-\Theta)^{p^t}$, não pode, em $\mathcal{M}$, em virtude do lema, admitir $\varphi(x)$ um factor $f(x)$ com a raiz Θ. $f(x)$ será uma constante. E conclui-se deste modo que é $(\mathcal{M}(\Theta)/\mathcal{M}) = (\mathcal{K}(\Theta)/\mathcal{K}) = p^t$.

Corolário 2:- Se Ω é uma ampliação pura e $\mathcal{M}$ uma ampliação separável de $\mathcal{K}$, cada elemento $\alpha \in \Omega$ tem o mesmo expoente e o mesmo grau relativamente a $\mathcal{K}$ e a $\mathcal{M}$.

(1) "A, pgs. 203".

Teorema 22:- Se for $\mathfrak{M} \supset \Omega \supset \mathfrak{K}$, é condição necessária e suficiente, para que $\mathfrak{M}$ seja ampliação inseparável pura de $\mathfrak{K}$, que Ω seja ampliação pura de $\mathfrak{K}$ e $\mathfrak{M}$ ampliação pura de Ω. É imediato que a condição é necessária. Para se ver que é suficiente, suponhamos que $\alpha \in \mathfrak{M}$ satisfaz a uma equação $x^{p^t} - \omega = 0$, irredutível em Ω. Como $\omega \in \Omega$ satisfaz a uma equação $x^{p^s} - k = 0$, irredutível em $\mathfrak{K}$, vê-se que α satisfaz à equação de $\mathfrak{K}[x]$, $x^{p^{t+s}} - k = 0$. α tem, pois, relativamente a $\mathfrak{K}$, um grau reduzido igual à unidade, como se quer. Podemos precisar, dizendo: o expoente de α, relativamente a $\mathfrak{K}$, é a soma dos expoentes t e s. Se pudesse ser $\alpha^{p^{t+s-j}} \in \mathfrak{K}$, $(j \geqslant 1)$, como é $\alpha^{p^t} = \omega$, ter-se-ia $\omega^{p^{s-j}} \in \mathfrak{K}$, o que é absurdo.

Corolário 3:- É condição necessária e suficiente, para que uma ampliação finita $\mathfrak{L}$, de $\mathfrak{K}$, seja pura, que o único isomorfismo relativo de $\mathfrak{L}$ com respeito a $\mathfrak{K}$ seja o isomorfismo idêntico. Se $\mathfrak{L}$ é ampliação pura, os graus reduzidos n_i, do teorema 4, são todos iguais à unidade. Inversamente, se os n_i são todos iguais à unidade, pondo $\mathfrak{L} = \mathfrak{K}(\Theta_1, \ldots, \Theta_r)$, é $\mathfrak{K}(\Theta_1)$ ampliação pura de $\mathfrak{K}$; $\mathfrak{K}(\Theta_1, \Theta_2)$ ampliação pura de $\mathfrak{K}(\Theta_1)$, e, portanto, de $\mathfrak{K}$; etc.

Teorema 23:- O grupo $\mathcal{G}$, dos automorfismos de $\mathfrak{L}$ com respeito a $\mathfrak{K}$, é sub-grupo do grupo $\mathcal{G}_0$ dos automorfismos de $\mathfrak{L}_0$ com respeito a $\mathfrak{K}$, e a ordem dum elemento $g' \in \mathcal{G}$ divide os graus de $\mathfrak{L}$ e de $\mathfrak{L}_0$ relativamente a $\mathfrak{K}$. Seja $g' \in \mathcal{G}$. Um elemento separável $\alpha \in \mathfrak{L}$, $\mathfrak{L}_0$ é transformado, por via de g', num elemento de $\mathfrak{L}$, que representaremos por $g'\alpha$. As correspondências $\mathfrak{K} \to \mathfrak{K}$, $\alpha \to g'\alpha$ determinam um isomorfismo relativo de $\mathfrak{K}(\alpha)$ com respeito a $\mathfrak{K}$. O elemento $g'\alpha$, como conjugado de α, é um elemento separável $(g'\alpha \in \mathfrak{L}_0)$. Assim, tem-se $\mathcal{G} \leqq \mathcal{G}_0$. Seja ainda $g' \in \mathcal{G}$. Como se tem $\mathfrak{L}_0 = \mathfrak{K}(\lambda)$, g' transforma λ num conjugado $g'\lambda$. Pondo $g'^n\lambda = g'g'^{n-1}\lambda$, suponhamos μ a ordem de g', e, por consequência, $g'^\mu\lambda = \lambda$. Os conjugados $\lambda, g'\lambda, \ldots, g'^{\mu-1}\lambda$ são todos distintos.

Seja $\mathfrak{L}_1 \supseteq \mathfrak{K}$ o corpo contido em $\mathfrak{L}_0$ que fica conservado por g'. A equação $f(x) = (x-\lambda)(x-g'\lambda)\ldots(x-g'^{\mu-1}\lambda) = 0$ tem coeficientes pertencentes a $\mathfrak{L}_1$. Se fosse $\lambda \in \mathfrak{L}_1$, ter-se-ia $\mathfrak{L}_1 = \mathfrak{L}_0$ e o teorema estaria demonstrado. No geral $\lambda \notin \mathfrak{L}_1$, de modo que se tem $\mathfrak{L}_0 = \mathfrak{L}_1(\lambda)$. A equação irredutível em $\mathfrak{L}_1$ a que satisfaz λ é precisamente $f(x) = 0$, em virtude do seguinte: se ela fosse $\Psi(x) = 0$, ter-se-ia $\Psi(\lambda) = \Psi(g'\lambda) = \ldots = 0$, pelo que $\Psi(x)$ seria também divisível por $f(x)$. Nestas condições, é $(\mathfrak{L}_0/\mathfrak{L}_1) = \mu$ e $(\mathfrak{L}_0/\mathfrak{K}) = \mu.(\mathfrak{L}_1/\mathfrak{K})$, o que demonstra o teorema.

Teorema 24:- Se $\mathfrak{M}$ é uma ampliação separável de $\mathfrak{K}$ e se $\mathfrak{L} = \mathfrak{K}\{\alpha_1, \ldots, \alpha_n\}$ é uma ampliação pura do mesmo corpo, $\Omega = \mathfrak{M}\{\alpha_1, \ldots, \alpha_n\}$ é uma ampliação pura de $\mathfrak{M}$. Os expoentes t_i, dos α_i, relativamente a $\mathfrak{K}$, são também os expoentes dos α_i relativamente a $\mathfrak{M}$. Sabe-se que é $\Omega_0 = \mathfrak{M}(\alpha_1^{p^e}, \ldots, \alpha_n^{p^e})$, se e é o expoente de $\mathfrak{L}$ relativamente a $\mathfrak{K}$ (ou de Ω relativamente a $\mathfrak{M}$). Como, porém, $\alpha_i^{p^e} \in \mathfrak{K}$, é $\Omega_0 = \mathfrak{M}$, como se quer.

Lema 3:- Se $\mathfrak{M}$ é uma ampliação separável de $\mathfrak{K}$, $\Delta \neq \mathfrak{M}(\beta_1, \ldots, \beta_s)$ é uma ampliação separável de $\Omega = \mathfrak{K}(\beta_1, \ldots, \beta_s)$. Tomemos $\alpha \in \Delta$. α é um polinómio nos β_i, com coeficientes pertencentes a $\mathfrak{M}$. Ponhamos $\alpha = \sum m_{i_1 \ldots i_s} \beta_1^{i_1} \ldots \beta_s^{i_s}$. Vê-se que α pertence ao corpo $\Phi(\beta_1, \ldots, \beta_s)$, onde $\Phi = \mathfrak{K}(\ldots, m_{i_1 \ldots i_s}, \ldots)$ resulta de $\mathfrak{K}$ por adjunção dos coeficientes que figuram na expressão supra de α. Como Φ é uma ampliação simples $\mathfrak{K}(\lambda)$, de $\mathfrak{K}$, tem-se $\alpha \in \mathfrak{K}(\lambda, \beta_1, \ldots, \beta_s) = \Omega(\lambda)$. Por ser λ separável relativamente a $\mathfrak{K}$ e a Ω, o corpo $\Omega(\lambda)$ é uma ampliação separável de Ω. Assim, qualquer elemento $\alpha \in \Delta$ é separável relativamente a Ω, pelo que Δ é ampliação separável deste último, como se afirmou.

Teorema 25:- Os corpos $\mathfrak{L}$ e Ω do teorema 24 verificam a relação $(\mathfrak{L}/\mathfrak{K}) = (\Omega/\mathfrak{M})$. Ponhamos, com efeito, $\mathfrak{L} = \mathfrak{K}(\beta_1, \ldots, \beta_s)$. Podemos supor $\beta_1, \ldots, \beta_s$ elementos inseparáveis relativamente a $\mathfrak{K}$ e a $\mathfrak{M}$, satisfazendo às mesmas equações irredutíveis nesses corpos, $x^{p^{t_i}} - \gamma_i = 0$, $(i = 1, 2, \ldots, s)$. É claro que se tem $\Omega = \mathfrak{M}(\beta_1, \ldots, \beta_s)$. Ora é

$$(\mathcal{K}(\beta_1)/\mathcal{K}) = (\mathcal{M}(\beta_1)/\mathcal{M}).$$

Fazendo $\mathcal{K}(\beta_1,\ldots,\beta_l) = \mathcal{L}_l$, $\mathcal{M}(\beta_1,\ldots,\beta_l) = \Omega_l$, admitamos que tem lugar a relação $(\mathcal{L}_{l-1}/\mathcal{K}) = (\Omega_{l-1}/\mathcal{M})$. Para se verificar que é também

$$(\mathcal{L}_l/\mathcal{K}) = (\Omega_l/\mathcal{M}) \qquad (2)$$

raciocina-se como segue. O elemento β_l satisfaz a uma equação irredutível em $\mathcal{L}_{l-1}$, $x^{p^{\theta_l}} - \delta_l = 0$. Como Ω_{l-1} é ampliação separável de $\mathcal{L}_{l-1}$, segue-se que a referida equação é irredutível em Ω_{l-1}. A igualdade (2) resulta desse facto.

Corolário 4:- Pondo ainda, como no teorema 24, $\mathcal{L} = \mathcal{K}\{\alpha_1, \ldots, \alpha_n\}$, $\Omega = \mathcal{M}\{\alpha_1,\ldots,\alpha_n\}$, e supondo $\mathcal{M}$ ampliação finita separável de $\mathcal{K}$, tem lugar a igualdade $\Omega = \mathcal{M}\times\mathcal{L}$. Neste enunciado, bem entendido, supõe-se $(\mathcal{L}/\mathcal{K}) = (\Omega/\mathcal{M}) = n$. Ω, como álgebra sobre $\mathcal{K}$, é da ordem $m = n.(\mathcal{M}/\mathcal{K})$. O produto directo $\mathcal{M}\times\mathcal{L}$, como álgebra sobre $\mathcal{K}$, é também da ordem m. Os elementos deste produto podem supor-se efectuados, porém, dentro da álgebra Ω (corpo), porque, supondo

$$\mathcal{M} = \mathcal{K}(\lambda) = \mathcal{K}\{u, \lambda, \ldots, \lambda^{r-1}\},\ (u = \text{elemento um de } \mathcal{K}),$$

os elementos $\lambda^i \alpha_j \in \Omega$, como vamos ver, são linearmente independentes relativamente a $\mathcal{K}$. Duma relação $\sum_{ij} \lambda^i \alpha_j k_{ij} = 0$, $(k_{ij} \in \mathcal{K})$, deduz-se

$$\sum_j \alpha_j \Big(\sum_i \lambda^i k_{ij}\Big) = 0\ , \qquad \sum_i \lambda^i k_{ij} = 0\ ,$$

pois, como se verificou no teorema anterior, os α_j são independentes em face de $\mathcal{M}$. Ora a última igualdade escrita dá $k_{ij} = 0$, como se quer.

Uma ampliação algébrica Ω, de $\mathcal{K}$, diz-se normal, se todo o polinómio irredutível em $\mathcal{K}$ com uma raiz em Ω é completamente decomponível em Ω.

Teorema 26:- O corpo de decomposição $\mathcal{M}_s$ (A, pgs. 180) dum polinómio qualquer $f(x) \in \mathcal{K}[x]$ é uma ampliação normal do

corpo $\mathcal{K}$. Construida a decomposição $f(x) = (x-\Theta_1)\ldots(x-\Theta_s)$, tomemos um polinómio irredutível $\varphi(x) \in \mathcal{K}[x]$ com uma raiz $\alpha \in \mathcal{M}_s = \mathcal{K}(\Theta_1,\ldots,\Theta_s)$. α é um polinómio nos Θ_i da forma $\alpha = P(\Theta_1, \ldots, \Theta_s)$. Representando por α', α'', ... as outras raizes de $\varphi(x) = 0$, construamos, por ex., os corpos $\mathcal{K}(\alpha)$ e $\mathcal{K}(\alpha')$. No corpo $\Omega = \mathcal{M}_s(\alpha')$ podemos definir o isomorfismo seguinte, relativo a $\mathcal{K}$: $\mathcal{L} = \mathcal{K}(\alpha) \cong \mathcal{K}(\alpha') = \mathcal{L}'$. Como $f(x)$ pertence a $\mathcal{L}[x]$ e $\mathcal{L}'[x]$, é possível prolongar o isomorfismo anterior (A., pgs. 181 e 182) e determinar, em Ω, o isomorfismo $\mathcal{M} = \mathcal{K}(\alpha, \Theta_1, \ldots, \Theta_s) \cong \mathcal{K}(\alpha', \Theta_1, \ldots, \Theta_s) = \mathcal{M}'$. Pelo facto de α ser uma expressão racional nos Θ_i, com coeficientes de $\mathcal{K}$, e de ser $\mathcal{M} \cong \mathcal{M}'$ um isomorfismo relativo a $\mathcal{K}$, no qual $\alpha \longrightarrow \alpha'$, $\Theta_i \longrightarrow \Theta_j$, $(i,j = 1, 2, \ldots, s)$, segue-se que α' é a mesma expressão racional dos Θ_j que α é dos Θ_i. Logo $\alpha' \in \mathcal{M}_s$. q. e. d.

Seja $\mathcal{L} = \mathcal{K}(\lambda)$ uma ampliação separável de $\mathcal{K}$ e suponhamos $\varphi(x) = 0$ a equação irredutível, de grau r, em $\mathcal{K}[x]$, a que satisfaz λ. O corpo de decomposição $\mathcal{M}$, de $\varphi(x)$, é uma ampliação normal separável, $\mathcal{M} = \mathcal{K}(\alpha_1)$, de $\mathcal{K}$. Designemos com $\alpha_1, \alpha_2, \ldots, \alpha_n$ os conjugados de α_1. Se tivermos em conta que é $\mathcal{K}(\alpha_i) = \mathcal{K}(\alpha_1)$, podemos afirmar que os isomorfismos relativos de $\mathcal{M}$ com respeito a $\mathcal{K}$ são obtidos por qualquer das correspondências

$$\mathcal{K} \longrightarrow \mathcal{K}\ , \qquad \alpha_i \longrightarrow \alpha_1, \alpha_2, \ldots, \alpha_n\ .$$

Esta afirmação equivale a dizer que uma correspondência que conserva $\mathcal{K}$ e muda α_i em α_k é uma correspondência que conserva $\mathcal{K}$ e muda α_1 em α_j.

Admitamos agora que $\mathcal{K}(\Theta_1)$ é um corpo intermediário entre $\mathcal{K}$ e $\mathcal{M}$. Se $\varphi_1(x) = 0$ for a equação irredutível em $\mathcal{K}$ a que satisfaz Θ_1, os corpos conjugados $\mathcal{K}(\Theta_1)$, $\mathcal{K}(\Theta_2)$, ..., de $\mathcal{K}(\Theta_1)$, são igualmente intermediários entre $\mathcal{K}$ e $\mathcal{M}$. É válido o seguinte

Teorema 27:- O número de isomorfismos relativos $\mathcal{K} \longrightarrow \mathcal{K}$, $\alpha_1 \longrightarrow \alpha_j$, que conservam um corpo $\mathcal{N} = \mathcal{K}(\Theta_m)$, é um divisor do grau $n = (\mathcal{M}/\mathcal{K})$, precisamente o grau $q = (\mathcal{M}/\mathcal{N})$. Efectivamente, os isomorfismos em causa são isomorfismos relativos de $\mathcal{M}$ com respeito a $\mathcal{N}$. Eles constituem um sub-grupo $\mathcal{Y}$, do grupo $\mathcal{G}$ dos isomorfismos relativos de $\mathcal{M}$ com respeito a $\mathcal{K}$.

O número de elementos de $\mathcal{G}$ é n e o dos elementos de $\mathcal{Y}$ é q, visto que $\mathfrak{M}$ é também ampliação separável de $\mathcal{N}$ (normal).

Se for $\mathcal{N}'$ um segundo corpo intermédio entre $\mathfrak{K}$ e $\mathfrak{M}$, ao qual corresponda o mesmo grupo $\mathcal{Y}$ que corresponde a $\mathcal{N}$, então $\tau' \in \mathcal{N}'$ é conservado, por hipótese, por todos os isomorfismos de $\mathcal{Y}$, os quais conservam $\mathcal{N}(\tau')$. Como o número dos isomorfismos que conservam $\mathcal{N}(\tau')$ não pode exceder o número de elementos de $\mathcal{Y}$, deve ter-se $(\mathfrak{M}/\mathcal{N}(\tau')) = (\mathfrak{M}/\mathcal{N})$, e, portanto, $\mathcal{N}(\tau') = \mathcal{N}$, $\tau' \in \mathcal{N}$, $\mathcal{N}' = \mathcal{N}$. Daqui se tira o

Corolário 5:- Entre $\mathfrak{K}$ e $\mathfrak{M}$ há um número finito de corpos intermédios.

E pode enunciar-se o

Teorema 28:- Entre $\mathfrak{K}$ e uma ampliação separável, $\mathcal{L} = \mathfrak{K}(\lambda)$ de $\mathfrak{K}$, há um número finito de corpos intermédios.

A questão dos corpos intermédios é resolvida por esta proposição: é necessário e basta, para que, entre $\mathfrak{K}$ e a sua ampliação Ω, haja um número finito de corpos intermédios, que Ω seja uma ampliação algébrica simples de $\mathfrak{K}$ (A, pgs. 238).

Teorema 29:- É condição necessária e suficiente, para que uma ampliação inseparável finita $\mathcal{L}$, de $\mathfrak{K}$, seja simples, que se tenha $(\mathcal{L}/\mathcal{L}^{(p)}) = p$.

Já sabemos que a condição é necessária. Para se ver que é suficiente, ponhamos

$$\mathcal{L} = \mathfrak{K}(a_1, \dots, a_r), \qquad \mathcal{L}^{(p)} = \mathfrak{K}(a_1^p, \dots, a_r^p).$$

Um dos elementos a_i, a_1 por ex., não pertence a $\mathcal{L}^{(p)}$. Por isso, tem-se

$$\mathcal{L} = \mathcal{L}^{(p)}(a_1) = \mathfrak{K}(a_1, a_2^p, \dots, a_r^p), \quad \mathcal{L}^{(p)} = \mathfrak{K}(a_1^p, a_2^{p^2}, \dots, a_r^{p^2}).$$

Daqui tira-se agora

$$\mathcal{L} = \mathfrak{K}(a_1, a_2^{p^2}, \dots, a_r^{p^2}) = \dots = \mathfrak{K}(a_1, a_2^{p^e}, \dots, a_r^{p^e}),$$

ou seja

$$\mathcal{L} = \mathcal{L}_0(a_1) = \mathfrak{K}(\Theta, a_1) = \mathfrak{K}(\mu),$$

se $\mathcal{L}_0 = \mathfrak{K}(\Theta)$.

Corolário 6:- A condição $(\mathcal{L}/\mathcal{L}^{(p)}) = p$ arrasta $(\mathcal{L}^{(p^t)}/\mathcal{L}^{(p^{t+1})}) = p$.

Seja $\mathcal{L}$ uma ampliação pura de $\mathfrak{K}$. Se o grau de $\mathcal{L}$ é p, tem-se $\mathcal{L} \supset \mathcal{L}^{(p)} = \mathcal{L}_0 = \mathfrak{K}$. $\mathcal{L}$ é ampliação simples de $\mathfrak{K}$ e não há, efectivamente, corpo intermédio entre um e outro. No caso da ampliação pura $\mathcal{L}$ ser de grau p^r $(r>1)$, suponhamos $\alpha^p \in \mathfrak{K}$, para cada $\alpha \in \mathcal{L}$. A cadeia $\mathcal{L} \supset \mathcal{L}^{(p)} = \mathcal{L}_0 = \mathfrak{K}$ diz-nos que $\mathcal{L}$ não pode ser ampliação simples de $\mathfrak{K}$. Dum modo preciso, é fácil encontrar r elementos tais que $\mathcal{L} = \mathfrak{K}(\alpha_1, \dots, \alpha_r)$, e verificar que um número de elementos inferior a r não pode gerar $\mathcal{L}$, a partir de $\mathfrak{K}$. Este resultado fixa-se no seguinte

Teorema 30:- Se $\mathcal{L}$ é ampliação pura de $\mathfrak{K}$, de grau p^r, e se, para cada $\alpha \in \mathcal{L}$, se tem $\alpha^p \in \mathfrak{K}$, o número mínimo de elementos a adjuntar a $\mathfrak{K}$ para obter $\mathcal{L}$ é igual a r.

Neste caso expresso pelo teorema, façamos $\mathfrak{K}(\alpha_1, \dots, \alpha_s) = \psi_s$. Se considerarmos a cadeia

$$\mathcal{L} = \psi_r \supset \psi_{r-1} \supset \dots \supset \psi_1 \supset \mathfrak{K} = \mathcal{L}^{(p)},$$

sabemos que não é possível encontrar corpo intermédio entre dois corpos consecutivos. Mas, entre dois não consecutivos, há uma infinidade de corpos intermédios. Tomemos por ex., ψ_3 e ψ_1. Sejam ρ, ρ', $\dots$ elementos de ψ_1 (em número infinito) e consideremos

$$\beta = \alpha_2 + \rho\,\alpha_3, \qquad \beta' = \alpha_2 + \rho'\alpha_3, \quad \dots .$$

Os corpos $\psi_1(\beta)$, $\psi_1(\beta')$, $\dots$ não estão contidos em ψ_2, mas estão contidos em ψ_3. Eles são diferentes, se for $\rho \neq \rho'$. Efectivamente, se pudesse ser $\beta' \in \psi_1(\beta)$, como se tem $\beta' - \beta = (\rho' - \rho)\alpha_3$, ter-se-ia $\alpha_3 \in \psi_1(\beta)$. Então, α_2 pertenceria a $\psi_1(\beta)$, seria

$\psi_1(\beta) = \psi_3$, o que não pode ter lugar, pelo facto de ser $(\psi_1(\beta)/\psi_1) = p$. Passando a uma ampliação finita qualquer Ω , de $\mathcal{K}$, os raciocínios feitos permitem enunciar, de facto, o seguinte

Teorema 31:- Se a ampliação finita Ω , de $\mathcal{K}$ (este suposto com uma infinidade de elementos), não é simples, há entre $\mathcal{K}$ e Ω uma infinidade de corpos intermédios.

Dada a ampliação finita Ω , de $\mathcal{K}$, consideremos a cadeia

$$\Omega \supset \Omega^{(p)} \supset \cdots \supset \Omega_0 \supset \mathcal{K}, \qquad (3)$$

e suponhamos $(\Omega/\Omega^{(p)}) = p^r$. Pondo

$$\Omega = \mathcal{K}(a_1, \ldots, a_\lambda), \qquad \Omega^{(p)} = \mathcal{K}(a_1^p, \ldots, a_\lambda^p),$$

concluimos imediatamente que não pode ser $\lambda < r$. Admitindo, pois, que é $\lambda \geqq r$, designemos por $a_1, \ldots, a_r$ elementos a_i, em número de r, não pertencentes a $\Omega^{(p)}$, os quais existem certamente. Tem-se

$$\Omega = \Omega^{(p)}(a_1, \ldots, a_r) = \mathcal{K}(a_1, \ldots, a_r, a_{r+1}^p, \ldots, a_\lambda^p) .$$

Como no teorema 29, chega-se a estabelecer

$$\Omega = \mathcal{K}(a_1, \ldots, a_r, a_{r+1}^{p^e}, \ldots, a_\lambda^{p^e}) = \Omega_0(a_1, \ldots, a_r) =$$

$$= \mathcal{K}(\Theta, a_1, \ldots, a_r) = \mathcal{K}(b_1, \ldots, b_r) .$$

Tem lugar este

Teorema 32:- Se na cadeia (3) se tiver $(\Omega/\Omega^{(p)}) = p^r$, Ω resulta de $\mathcal{K}$ por adjunção de r elementos e nunca por menos do que r elementos.

Na cadeia (3), o grau de $\Omega^{(p)}$ relativamente a $\Omega^{(p^2)}$ não pode exceder r. Se excedesse, $\Omega^{(p)}$ só poderia resultar de $\mathcal{K}$ por adjunção de mais do que r elementos e não seria $\Omega^{(p)} = \mathcal{K}(b_1^p, \ldots, b_r^p)$. Dum modo geral, na referida cadeia, o grau de cada corpo relativamente ao seguinte nunca pode aumentar. Se todos os graus são iguais a p, salvo $(\Omega/\Omega^{(p)}) = p^r$ [bem entendido que $(\Omega_0/\mathcal{K})$ não está em causa], $\Omega^{(p)}$ é uma ampliação simples de $\mathcal{K}$, o mesmo podendo dizer-se de $\Omega^{(p)}(b_i)$, se b_i é de expoente e (um dos elementos b_i é necessàriamente de expoente e). Efectivamente, tem-se

$$(\Omega^{(p)}(b_1)/\mathcal{K}) = (\Omega^{(p)}(b_1)/\Omega^{(p)})(\Omega^{(p)}/\mathcal{K}) = p \cdot N_0 p^{e-1} = N_0 p^e .$$

Vamos fazer mais duas observações. Primeiramente, quando Ω, nas condições do teorema 32, resulta de $\mathcal{K}$ por adjunção dum certo número de elementos ($s \geqq r$), r dos referidos elementos não pertencem a $\Omega^{(p)}$, e entre os elementos não pertencentes a $\Omega^{(p)}$ há $x-1$ que podem fazer-se figurar nos r elementos que levam de $\mathcal{K}$ a Ω . A segunda observação vem a seguir. Ponhamos, em (3), $\Omega^{(p^i)} = \Delta$, $\Omega^{(p^k)} = \Phi$, $(i < k)$. Considerando $\Delta = \Phi(\alpha_1, \ldots, \alpha_t)$ como ampliação finita de Φ , a cadeia $\Delta \supset \Delta^{(p)} \supset \cdots \supset \Delta_0 = \Phi$ é precisamente a parte de (3) intermediária entre Φ e Δ. Na verdade, tendo-se

$$\Delta \supset \Omega^{(p^{i+1})} \equiv \Phi \equiv \mathcal{K} ,$$

pode escrever-se

$$\Delta = \mathcal{K}(x_1, \ldots, x_\rho) = \Phi(x_1, \ldots, x_\rho),$$

e, em seguida,

$$\Omega^{(p^{i+1})} = \mathcal{K}(x_1^p, \ldots, x_\rho^p) = \Phi(x_1^p, \ldots, x_\rho^p) = \Delta^{(p)} ,$$

como se deseja.

Consideremos a ampliação algébrica $\mathcal{L} = \mathcal{K}(\alpha_1, \ldots, \alpha_r)$, de $\mathcal{K}$, e tomemos um corpo $\mathcal{M} = \mathcal{K}(x_1, \ldots, x_t)$, intermediário entre $\mathcal{K}$ e $\mathcal{L}$. Pondo

$$\mathcal{L} = \mathcal{M}(\beta_1, \ldots, \beta_s) = \mathcal{K}(x_1, \ldots, x_t, \beta_1, \ldots, \beta_s),$$

tem-se imediatamente

$$\mathcal{L}^{(p^r)} = \mathcal{K}(x_1^{p^r}, \ldots, \beta_s^{p^r}) = \mathcal{M}^{(p^r)}(\beta_1^{p^r}, \ldots, \beta_s^{p^r}),$$

a que podemos dar ainda a forma

$$\mathfrak{M}(\beta_1,\dots,\beta_s)^{(p^r)} = \mathfrak{M}^{(p^r)}(\beta_1^{p^r},\dots,\beta_s^{p^r}).$$

Em particular será

$$\mathfrak{L}^{(p)} \triangleq \mathfrak{M}(\beta_1,\dots,\beta_s)^{(p)} = \mathfrak{M}^{(p)}(\beta_1^p,\dots,\beta_s^p).$$

Suponhamos $\beta_1,\dots,\beta_s$ elementos em número mínimo a adjuntar a $\mathfrak{M}$ para obter $\mathfrak{L}$. Se β_1 verifica a equação irredutível em $\mathfrak{M}$,

$$\varphi_1(x) = x^n + \alpha_1 x^{n-1} + \dots + \alpha_{n-1} x + \alpha_n = 0, \qquad (3')$$

o elemento β_1^p verifica a equação seguinte, com coeficientes de $\mathfrak{M}^{(p)}$:

$$\Phi_1(x) = x^n + \alpha_1^p x^{n-1} + \dots + \alpha_n^p = 0. \qquad (3'')$$

Por isso, será

$$\left(\mathfrak{M}^{(p)}(\beta_1^p)/\mathfrak{M}^{(p)}\right) \cong \left(\mathfrak{M}(\beta_1)/\mathfrak{M}\right). \qquad (4)$$

Anàlogamente, β_2 satisfaz à equação irredutível em $\mathfrak{M}(\beta_1)$,

$$\varphi_2(x) = x^m + \alpha_1' x^{m-1} + \dots + \alpha_m' = 0,$$

e β_2^p à equação

$$\Phi_2(x) = x^m + \alpha_1'^p x^{m-1} + \dots + \alpha_m'^p = 0.$$

Os coeficientes desta última equação pertencem a $\mathfrak{M}(\beta_1)^{(p)} = \mathfrak{M}^{(p)}(\beta_1^p)$, de sorte que se tem

$$\left(\mathfrak{M}^{(p)}(\beta_1^p,\beta_2^p)/\mathfrak{M}^{(p)}(\beta_1^p)\right) \cong \left(\mathfrak{M}(\beta_1,\beta_2)/\mathfrak{M}(\beta_1)\right).$$

Continuando o processo, chega-se, por combinação das diferentes desigualdades obtidas, à relação

$$(\mathfrak{L}^{(p)}/\mathfrak{M}^{(p)}) \cong (\mathfrak{L}/\mathfrak{M}),$$

e, em seguida, das igualdades

$$(\mathfrak{L}/\mathfrak{M}^{(p)}) = (\mathfrak{L}/\mathfrak{M})\,(\mathfrak{M}/\mathfrak{M}^{(p)}) = (\mathfrak{L}/\mathfrak{L}^{(p)})\,(\mathfrak{L}^{(p)}/\mathfrak{M}^{(p)}),$$

tira-se a relação

$$(\mathfrak{M}/\mathfrak{M}^{(p)}) \cong (\mathfrak{L}/\mathfrak{L}^{(p)}).$$

Podemos enunciar, assim, o seguinte

Teorema 33:- Se $\mathfrak{L}$ é uma ampliação algébrica finita de $\mathfrak{K}$, que resulta deste pela adjunção dum número mínimo de elementos = r, um corpo $\mathfrak{M}$, intermediário entre $\mathfrak{K}$ e $\mathfrak{L}$, pode fazer-se resultar de $\mathfrak{K}$ pela adjunção dum número de elementos $\cong$ $\cong$ r.

Tira-se daqui o

Corolário 7:- Se $\mathfrak{L}$ é ampliação algébrica simples de $\mathfrak{K}$, um corpo $\mathfrak{M}$, intermediário entre $\mathfrak{K}$ e $\mathfrak{L}$, é também ampliação simples de $\mathfrak{K}$.(1)

Um caso em que, em (4), vale a igualdade, é aquele em que $\mathfrak{L}$ é ampliação simples de $\mathfrak{K}$. Se for $\mathfrak{L} = \mathfrak{K}(\alpha) \supset \mathfrak{M} \supset \mathfrak{K}$, e $\mathfrak{L} = \mathfrak{M}(\beta)$, a equação (3'') a que satisfaz β^p é irredutível em $\mathfrak{M}^{(p)}$, tal como (3') é irredutível em $\mathfrak{M}$. Efectivamente, dum modo geral, o elemento β^{p^k} satisfaz à equação

$$\Phi_k(x) = x^n + \alpha_1^{p^k} x^{n-1} + \dots + \alpha_n^{p^k} = 0,$$

com coeficientes pertencentes a $\mathfrak{M}^{(p^k)}$. Ora, tendo-se

$$(\mathfrak{L}/\mathfrak{M}^{(p^k)}) = (\mathfrak{L}/\mathfrak{M})\,(\mathfrak{M}/\mathfrak{M}^{(p)}) \dots (\mathfrak{M}^{(p^{k-1})}/\mathfrak{M}^{(p^k)}) = n\cdot p^k =$$

$$= (\mathfrak{L}/\mathfrak{L}^{(p)}) \dots (\mathfrak{L}^{(p^{k-1})}/\mathfrak{L}^{(p^k)}).(\mathfrak{L}^{(p^k)}/\mathfrak{M}^{(p^k)}) = p^k(\mathfrak{L}^{(p^k)}/\mathfrak{M}^{(p^k)}),$$

conclui-se imediatamente a afirmação supra. Podemos fixar o seguinte

(1) Às indicações bibliográficas dadas no começo do §, podemos juntar Almeida Costa, "Sobre os corpos comutativos", "Anais da Faculdade de Ciências do Porto", tomo XXXI, 1946. A redacção do § é quase totalmente extraída desse artigo.

Teorema 34:- Se $\varphi(x) = x^n+\alpha_1 x^{n-1}+\cdots+\alpha_n = 0$ é uma equação irredutível em $\mathfrak{M}$, e se β é uma raiz desta equação tal que $\mathfrak{M}(\beta) = \mathfrak{N}(\alpha)$ é ampliação simples de $\mathfrak{N}$, a equação $\varphi_R(x) = x^{n_R}+\alpha_1^{p^R} x^{n-1}+\cdots+\alpha_n^{p^R} = 0$ é irredutível em $\mathfrak{M}^{(p^R)}$.

2) Sobre os módulos com respeito a corpos - Daremos neste § algumas indicações que completam a exposição feita no tomo I, Cap. II, pgs. 25 e seguintes. Os resultados a indicar são devidos a E. Noether.(1) Trataremos com corpos não comutativos, contràriamente ao que aconteceu no § anterior.

Seja $\mathfrak{M} = u_1\Omega+\cdots+u_n\Omega$ um módulo de ordem n com respeito a um corpo Ω e suponhamos que este contém um corpo $\mathfrak{N} \cdot \mathfrak{M}$ diz-se uma ampliação do módulo $\mathfrak{M} = u_1\mathfrak{N}+\cdots+u_n\mathfrak{N}$. Inversamente, dado um módulo $\mathfrak{M}$ relativo a $\mathfrak{N}$, como o anterior, se Ω contiver $\mathfrak{N}$, o módulo $\mathfrak{M} = u_1\Omega+\cdots+u_n\Omega$ é ampliação dum módulo isomorfo de $\mathfrak{M}$.

Teorema 1:- Se $\mathfrak{M}$ é ampliação de $\mathfrak{M}$, dados m elementos $v_1,\ldots,v_m \in \mathfrak{M}$, independentes relativamente a $\mathfrak{N}$, os mesmos elementos são independentes relativamente a Ω. Se n é a ordem comum dos dois módulos, juntaremos aos v_j n-m elementos de modo a formar uma base de $\mathfrak{M}$. Esta base é equivalente à base comum dos dois módulos em causa.

Teorema 2:- Dado o sub-módulo $\mathfrak{M}' = v_1\mathfrak{N}+\cdots+v_m\mathfrak{N}$, de $\mathfrak{M}$, o sub-módulo $\mathfrak{M}' = v_1\Omega+\cdots+v_m\Omega$, de $\mathfrak{M}$, ampliação daquele, tem de comum com $\mathfrak{M}$ o sub-módulo $\mathfrak{M}'$: $\mathfrak{M}' \cap \mathfrak{M} = \mathfrak{M}'$. É claro que vale $\mathfrak{M}' \subseteq \mathfrak{M}' \cap \mathfrak{M}$. Se for $a \in \mathfrak{M}' \cap \mathfrak{M}$, como $\mathfrak{M}'$ é, por hipótese, ampliação dum sub-módulo $\mathfrak{M}'$, a exprime-se nos elementos $v_1,\ldots,v_m$, que constituem uma base comum a $\mathfrak{M}'$ e $\mathfrak{M}'$. Será $a = \sum v_l\omega_l$, $(\omega_l \in \Omega)$. Os elementos $a, v_1,\ldots,v_m \in \mathfrak{M}$ não podem ser independentes em face de $\mathfrak{N}$, visto que, pelo teorema anterior, seriam também independentes em face de Ω. Deste modo é $a \in \mathfrak{M}'$, como se quer.

(1) Veja-se E. Noether, "Nichtkommutative Algebra", Mathematische Zeitschrift, Band 37, 1933, pgs. 523 a 525.

Convém observar, todavia, que, dado um sub-módulo $\mathfrak{M}'$, não é geralmente $(\mathfrak{M}' \cap \mathfrak{M})_\Omega = \mathfrak{M}'$. Vamos ver, por ex., que pode ter-se $\mathfrak{M}' \cap \mathfrak{M} = (0)$, com $\mathfrak{M}' \neq (0)$. Seja $u_1,\ldots,u_n$ uma base de $\mathfrak{M}$ e $\mathfrak{M}$. Ponhamos

$$v = u_1k_1+\cdots+u_{n-1}k_{n-1}+u_n\omega, \qquad (k_l \in \mathfrak{N},\ 0 \neq \omega \notin \mathfrak{N}).$$

O elemento v não pode pertencer a $\mathfrak{M}$. O módulo $\mathfrak{M}' = v\Omega$ não possui elemento diferente de zero pertencente a $\mathfrak{M}$, pois que, se o possuisse, seria

$$v\alpha = u_1k_1\alpha+\cdots+u_n\omega\alpha = u_1K_1+\cdots+u_nK_n, \qquad (\alpha \in \Omega,\ K_l \in \mathfrak{N}).$$

Daqui tirar-se-ia $k_1\alpha = K_1,\ldots,k_{n-1}\alpha = K_{n-1}$, e, supondo um $k_j \neq 0$, viria $\alpha \in \mathfrak{N}$, $\omega\alpha = K_n, \omega \in \mathfrak{N}$, contra a hipótese.

Lema 1:- Dado $\mathfrak{M} = u_1\Omega+\cdots+u_n\Omega$, se $\mathfrak{M}' = v_1\Omega+\cdots+v_m\Omega$ for um sub-módulo de $\mathfrak{M}$, existe uma base $x_1,\ldots,x_m$, de $\mathfrak{M}'$, da forma

$$x_l = u_l - \sum_{R=m+1}^{n} u_R\omega_{R_l}, \qquad (\omega_{R_l} \in \Omega),$$

desde que os u_l se suponham ordenados de modo conveniente.

Completemos, com efeito, os v_j com os u_R necessários à construção duma base de $\mathfrak{M}$. Ordenando os uu de modo que os u_R u_R sejam $u_{m+1},\ldots,u_n$, a base de $\mathfrak{M}$ será $(v_1,\ldots,v_m; u_{m+1},\ldots,u_n)$. Se for

$$u_i = \sum_{j=1}^{m} v_j\alpha_j + \sum_{R=m+1}^{n} u_R\alpha_{R_i}, \qquad (i = 1, 2,\ldots,m;\ \alpha_j, \alpha_{R_i} \in \Omega),$$

vê-se que é

$$x_l = u_l - \sum_{R=m+1}^{n} u_R\alpha_{R_i} = \sum_{j=1}^{m} v_j\alpha_j \in \mathfrak{M}'. \qquad (5)$$

Os elementos x_l, pertencentes a $\mathfrak{M}'$, são linearmente independentes, como resulta da sua expressão nos uu. O lema está demonstrado. A base dos x_lx_l diz-se uma base normal de $\mathfrak{M}'$.

Consequência:- Se $a, a' \in \mathfrak{M}'$, e se é

$$a = \sum_1^m u_l \alpha_l + \sum_{m+1}^n u_k \alpha_k , \qquad a' = \sum_1^m u_l \alpha_l + \sum_{m+1}^q u_k \alpha'_k ,$$

tem-se $a = a'$. Recorrendo a (5), vê-se que tem lugar a igualdade

$$a = \sum_1^m x_l \alpha_l + \sum_{m+1}^n u_k r_k .$$

Como o sistema $(x_1, \ldots, x_m ; u_{m+1}, \ldots, u_n)$ constitui uma base de $\mathfrak{M}$, segue-se que é simplesmente $a = \sum_1^m x_l \alpha_l$. Anàlogamente, tem-se $a' = \sum_1^m x_l \alpha_l = a$, q. e. d.

Consideremos um grupo $\mathcal{G}$ de automorfismos de Ω tal que os elementos de $\mathfrak{o}$, e apenas esses, fiquem invariantes para as operações de $\mathcal{G}$. O módulo $\mathfrak{M}$ torna-se num módulo que admite o domínio operatório $\mathcal{G}$, mediante as seguintes convenções:

se $G \in \mathcal{G}$, $a \in \mathfrak{M}$, põe-se $Ga = a$;

se $a = \sum u_l \omega_l \in \mathfrak{M}$, $u_l \in \mathfrak{N}$, põe-se $Ga = \sum u_l G(\omega_l)$.

Pode, então, enunciar-se o

Lema 2:- É necessário e suficiente, para que um elemento de $\mathfrak{M}$ seja invariante em face do grupo $\mathcal{G}$, que esse elemento pertença a $\mathfrak{N}$.

Vimos que um elemento de $\mathfrak{N}$ é invariante. Inversamente, se $a \in \mathfrak{M}$ é invariante, escolhamos uma base u_l, de $\mathfrak{M}$, que seja base de $\mathfrak{N}$. Será $a = \sum u_l \omega_l$, $Ga = \sum u_l G(\omega_l) = \sum u_l \omega_l$. Conclui-se $G(\omega_l) = \omega_l$, e, portanto, $\omega_l \in \mathfrak{o}$, q. e. d.

Teorema 3:- É condição necessária e suficiente, para que um sub-módulo $\mathfrak{M}'$ seja admissível em face de $\mathcal{G}$, que $\mathfrak{M}'$ seja ampliação dum sub-módulo $\mathfrak{N}'$. Se $\mathfrak{M}'$ é ampliação de $\mathfrak{N}'$, tomando uma base $x_1, \ldots, x_m \in \mathfrak{N}'$, tem-se, para cada $a \in \mathfrak{M}'$, $Ga = G. \sum x_i \omega_l = \sum x_i G(\omega_i) \in \mathfrak{M}'$. Inversamente, se $\mathfrak{M}'$ é admissível, tomemos uma base u_j, comum a $\mathfrak{M}$ e $\mathfrak{N}$, e, depois, uma base normal

x_l de $\mathfrak{M}'$. Tem-se, conforme (5),

$$G(x_l) = u_l - \sum_{k=m+1} u_k G(\alpha_{kl}) \in \mathfrak{M}' ,$$

$$G(x_l) = x_l + \sum_{k=m+1} u_k \left(\alpha_{kl} - G(\alpha_{kl}) \right) .$$

Desta última relação conclui-se $\alpha_{kl} - G(\alpha_{kl}) = 0$, $G(x_l) = x_l$, e, portanto (lema 2), $x_l \in \mathfrak{N}$. $\mathfrak{M}'$ é ampliação de $x_1 \mathfrak{o} + \cdots + x_m \mathfrak{o}$, q. e. d.

No § próximo, faremos uma importante aplicação dos raciocínios que acabamos de expor.

3) Demonstração dum teorema fundamental - É susceptível de aplicações muito variadas no estudo das ampliações das álgebras (particularmente das álgebras simples) o seguinte

Teorema fundamental[1]:- Se $\mathfrak{A}$ é uma álgebra com elemento um sobre $\mathfrak{o}$ e se Ω é um corpo de centro $Z \supseteq \mathfrak{o}$, o anel $\mathfrak{A}_\Omega = \mathfrak{M}$ tem o centro do anel $\mathfrak{A}_z = \mathfrak{N}$ e os ideais bilaterais destes dois últimos anéis estão em correspondência biunívoca, de tal modo que cada ideal bilateral de $\mathfrak{M}$ é ampliação dum ideal bilateral de $\mathfrak{N}$. Na definição de $\mathfrak{M}$, são comutáveis os elementos de $\mathfrak{A}$ e de Ω. Tanto $\mathfrak{A}$ como Ω pertencem a $\mathfrak{M}$. Se x é um elemento do centro deste, vale, para cada $\omega \in \Omega$, tomando uma base u_j de $\mathfrak{A}$,

$$\omega^{-1} x \omega = \omega^{-1} . \sum u_j \alpha_j . \omega = \sum u_j \omega^{-1} \alpha_j \omega = \sum u_j \alpha_j , \qquad (x = \sum u_j \alpha_j) .$$

Será, assim, $\omega^{-1} u_j \omega = \alpha_j$, ou $\alpha_j \omega = \omega \alpha_j$, o que mostra ser $\alpha_j \in Z$. Portanto, é $x = \sum u_j \alpha_j \in \mathfrak{N}$, de modo que x pertence ao centro de $\mathfrak{N}$. Por outro lado, um elemento do centro de $\mathfrak{N}$ comuta com os elementos de $\mathfrak{M}$. Se $\mathfrak{z}$ é o centro de $\mathfrak{A}$, podemos precisar, dizendo que o centro de $\mathfrak{M}$ é $\mathfrak{z}_z$. Basta ter em conta que $\mathfrak{N} = \mathfrak{A}_z$ é uma álgebra ampliada da álgebra $\mathfrak{A}$.

(1) Cfr. van der Waerden, "Moderne Algebra", II Teil, pgs. 174 e seguintes. Veja-se também M. Deuring, loc. cit., pgs. 36 e 37.

Seja agora $\mathcal{G}$ o grupo dos automorfismos internos de Ω. Os elementos de Z, e apenas esses, ficam invariantes para as operações de $\mathcal{G}$. O módulo $\mathfrak{M}$ com respeito a Ω admite o domínio operatório $\mathcal{G}$, no sentido mencionado no § anterior. Vamos ver que os ideais bilaterais, como $\mathfrak{a}$, de $\mathfrak{M}$, são sub-módulos admissíveis. De facto, tem-se $\omega^{-1}\mathfrak{a}\omega \equiv \mathfrak{a}$, $(\omega \in \Omega \subseteq \mathfrak{M})$. Nestas condições, $\mathfrak{a}$ é ampliação de $\mathfrak{a}_0 = \mathfrak{a} \cap \mathfrak{N}$. Inversamente, partindo dum ideal bilateral $\mathfrak{a}_0$, de $\mathfrak{N}$, o módulo ampliado $\mathfrak{a}$, em $\mathfrak{M}$, é um ideal bilateral deste último, pois, se $v_1, \ldots, v_m$ são elementos base de $\mathfrak{a}_0$, tem-se, por ex., para cada $\alpha = \sum u_j \omega_j' \in \mathfrak{M}$,

$$\alpha \cdot \sum_l v_l \omega_l = \sum_{l,j} u_j v_l \omega_j' \omega_l = \sum_k v_k \omega_k'' , \quad (\omega_l, \omega_j', \omega_k'' \in \Omega),$$

visto que os elementos ω_j' comutam com os v_l, pelo facto de estes se exprimirem nos $u_{j,s}$ com coeficientes pertencentes a Z. O teorema está demonstrado.

Teorema:- É condição necessária e suficiente, para que $\mathcal{A}_\Omega$ seja semi-simples, que $\mathcal{A}_z$ seja semi-simples. Se $\mathcal{A}_\Omega$ é semi-simples, uma vez decomposto em ideais bilaterais simples, cada ideal bilateral é ampliação dum ideal bilateral de $\mathcal{A}_z$. A soma correspondente destes últimos ideais bilaterais leva a $\mathcal{A}_z$ e cada ideal bilateral é simples, visto que, se o não fosse e tivesse um ideal bilateral próprio, poderíamos passar, por ampliação, a um ideal bilateral próprio dum ideal bilateral simples da decomposição de $\mathcal{A}_\Omega$. Inversamente, se $\mathcal{A}_z$ é semi-simples, $\mathcal{A}_\Omega$ é semi-simples.

Corolário:- Se $\mathcal{A}$ é uma álgebra simples e Ω tem o centro $Z = \mathfrak{K}$, o anel $\mathcal{A}_\Omega$ é simples e tem o mesmo centro que $\mathcal{A}$.

O teorema fundamental demonstrado permite-nos tratar imediatamente o estudo do produto directo de duas álgebras simples $\mathcal{A}$ e $\mathcal{B}$, sobre $\mathfrak{K}$. Ponhamos, com efeito, conforme se viu no final do Cap. anterior,

$$\mathcal{A} = (\ldots e_{ij} \ldots) \times \mathcal{L} = \mathfrak{K}_r \times \mathcal{L}, \qquad \mathcal{B} = \mathfrak{K}_s \times \Delta,$$

onde figuram as álgebras normais de matrizes, $\mathfrak{K}_r$ e $\mathfrak{K}_s$, e as álgebras de divisão $\mathcal{L}$ e Δ. Tem-se imediatamente

$$\mathcal{A} \times \mathcal{B} = \mathfrak{K}_{rs} \times (\mathcal{L} \times \Delta) .$$

O estudo em causa reduz-se, assim, ao do produto $\mathcal{L} \times \Delta$. Por ser $\mathfrak{K}_{rs}$ uma álgebra normal, o centro de $\mathcal{A} \times \mathcal{B}$ é o centro de $\mathcal{L} \times \Delta$. O centro desta última é o centro de $\mathcal{L}_{z'}$, se Z' é o centro de Δ. O centro de $\mathcal{L}_{z'}$ é $Z_{z'}$, se Z é o centro de $\mathcal{L}$. Por outro lado, é condição necessária e suficiente para que $\mathcal{L}_\Delta = \mathcal{L} \times \Delta$ seja semi-simples, que $\mathcal{L} \times Z' = Z' \times \mathcal{L}$ seja semi-simples. Ora esta última é semi-simples, se $Z' \times Z$ for semi-simples, e apenas nesse caso. Podemos, por isso, enunciar o seguinte

Teorema:- É condição necessária e suficiente, para que o produto de duas álgebras simples $\mathcal{A}$ e $\mathcal{B}$, sobre $\mathfrak{K}$, seja semi-simples, que seja semi-simples o produto dos respectivos centros. Em todos os casos, o centro do produto é o produto dos centros. Se se puser

$$\mathcal{L} \times \Delta = \mathfrak{K}_1 \times \Phi + \mathfrak{K}_1 \times \Phi' + \cdots ,$$

vê-se que é

$$\mathcal{A} \times \mathcal{B} = \mathfrak{K}_{rst} \times \Phi + \mathfrak{K}_{rst} \times \Phi' + \cdots .$$

O número de álgebras simples em que se decompõe $\mathcal{A} \times \mathcal{B}$ é o mesmo em que se decompõe $\mathcal{L} \times \Delta$ ou $Z \times Z'$. Tiram-se daqui as seguintes proposições:

Corolário 1º :- O produto directo de duas álgebras simples sobre $\mathfrak{K}$, a segunda das quais é normal, é uma álgebra simples sobre $\mathfrak{K}$. O centro do produto é o centro do 1º factor.

Corolário 2º :- O produto directo duma álgebra simples $\mathcal{A}$ e duma álgebra normal de divisão Ω, sobre $\mathfrak{K}$, é uma álgebra simples, isomorfa dum anel de matrizes com elementos duma álgebra de divisão Σ, sobre $\mathfrak{K}$. O centro de $\mathcal{A} \times \Omega$ é o centro de Σ.

Na teoria das álgebras, uma questão muito importante é a do estudo das ampliações duma álgebra $\mathcal{A}$, quando se passa do corpo fundamental $\mathfrak{K}$ ao corpo fundamental $\mathfrak{P} \supset \mathfrak{K}$. No § 5 ocupar-nos-emos desse problema, especialmente no caso de alge-

bras simples. Os resultados deste § encontrarão aí muitas aplicações. A álgebra $\mathcal{A}_{\mathfrak{P}}$ não é, geralmente, álgebra sobre $\mathfrak{K}$. Se $\mathcal{A}$ tem elemento um, os ideais ordinários de $\mathcal{A}_{\mathfrak{P}}$ são ideais admissíveis. No caso de $\mathfrak{P}$ ser uma ampliação finita (comutativa) de $\mathfrak{K}$, $\mathcal{A}_{\mathfrak{P}}$ é álgebra s/$\mathfrak{K}$, e o facto de haver elemento um em $\mathcal{A}$ é suficiente para garantir que os ideais ordinários de $\mathcal{A}_{\mathfrak{P}}$ são ideais admissíveis desta álgebra, tanto considerada sobre $\mathfrak{P}$ como sobre $\mathfrak{K}$.

O § seguinte é dedicado a considerações gerais sobre ideais sem divisor dos anéis comutativos, no sentido de justificar certas afirmações a utilizar também no § 5.

4) Sobre os ideais sem divisor dos anéis comutativos - Seja $\mathcal{J}$ um anel comutativo, com elemento um. Dois ideais $\mathfrak{a}_1, \mathfrak{a}_2$ dizem-se sem divisor comum, se o seu máximo divisor comum for o ideal unidade $\mathcal{J} = (\mathfrak{a}_1, \mathfrak{a}_2)$. Para dois ideais quaisquer $\mathfrak{a}$ e $\mathfrak{b}$, é válida a relação $\mathfrak{a}\mathfrak{b} \equiv [\mathfrak{a}, \mathfrak{b}]$. Se os ideais não têm divisor comum, é precisamente $\mathfrak{a}\mathfrak{b} = [\mathfrak{a}, \mathfrak{b}]$, visto que se tem também

$$[\mathfrak{a}, \mathfrak{b}] = [\mathfrak{a}, \mathfrak{b}].(\mathfrak{a}, \mathfrak{b}) = \big([\mathfrak{a}, \mathfrak{b}].\mathfrak{a}, [\mathfrak{a}, \mathfrak{b}].\mathfrak{b}\big) \equiv (\mathfrak{a}\mathfrak{b}, \mathfrak{a}\mathfrak{b}) = \mathfrak{a}\mathfrak{b}.$$

Lema 1 :- De $(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{z}) = \mathcal{J}$, conclui-se $(\mathfrak{a}, \mathfrak{b}\mathfrak{z}) = \mathcal{J}$.

Este enunciado traduz que um ideal sem divisor comum com cada um de dois outros também não tem divisor comum com o produto destes últimos. De facto é

$$(\mathfrak{a}, \mathfrak{b}).(\mathfrak{a}, \mathfrak{z}) = \mathcal{J} = \big((\mathfrak{a}, \mathfrak{b})\mathfrak{a}, (\mathfrak{a}, \mathfrak{b})\mathfrak{z}\big) = \big(\mathfrak{a}, (\mathfrak{a}\mathfrak{z}, \mathfrak{b}\mathfrak{z})\big) =$$

$$= (\mathfrak{a}, \mathfrak{a}\mathfrak{z}, \mathfrak{b}\mathfrak{z}) = (\mathfrak{a}, \mathfrak{b}\mathfrak{z}) .$$

Esta proposição estende-se ao caso de $\mathfrak{a}$ não ter divisor comum com cada um de vários ideais.

Lema 2:- Se $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ são ideais dois a dois sem divisor comum, tem lugar a igualdade $[\mathfrak{a}_1, \ldots, \mathfrak{a}_n] = \mathfrak{a}_1 \ldots \mathfrak{a}_n$. Como a igualdade é válida para n = 2, suponhamos que é válida para n - 1. Então tem-se

$$[\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1}] = \mathfrak{a}_1 \ldots \mathfrak{a}_{n-1} \; ; \; \big[[\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1}], \mathfrak{a}_n\big] =$$

$$= [\mathfrak{a}_1, \ldots, \mathfrak{a}_n] = [\mathfrak{a}_1 \ldots \mathfrak{a}_{n-1}, \mathfrak{a}_n] = \mathfrak{a}_1 \ldots \mathfrak{a}_{n-1}.\mathfrak{a}_n .$$

Lema 3:- Se $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ são ideais dois a dois sem divisor comum, pondo $\mathfrak{b}_k = \mathfrak{a}_1 \ldots \mathfrak{a}_{k-1}\, \mathfrak{a}_{k+1} \ldots \mathfrak{a}_n$, $(k = 1, 2, \ldots, n)$, tem-se $\mathcal{J} = (\mathfrak{b}_1, \ldots, \mathfrak{b}_n)$.

Para o caso n = 2, é $\mathfrak{b}_1 = \mathfrak{a}_2$, $\mathfrak{b}_2 = \mathfrak{a}_1$, $\mathcal{J} = (\mathfrak{b}_1, \mathfrak{b}_2) = (\mathfrak{a}_1, \mathfrak{a}_2)$. Admitamos, então, que o lema é válido para n - 1. Será

$$\mathcal{J} = (\mathfrak{z}_2, \ldots, \mathfrak{z}_{n-1}), \quad \mathfrak{z}_j = \mathfrak{a}_1 \ldots \mathfrak{a}_{j-1}\mathfrak{a}_{j+1} \ldots \mathfrak{a}_{n-1}, \quad (j = 1, \ldots, n-1).$$

Tem-se também

$$(\mathfrak{b}_1, \ldots, \mathfrak{b}_n) = (\mathfrak{z}_1\mathfrak{a}_n, \ldots, \mathfrak{z}_{n-1}\mathfrak{a}_n, \mathfrak{a}_1 \ldots \mathfrak{a}_{n-1}) = \big((\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1})\mathfrak{a}_n,$$

$$\mathfrak{a}_1 \ldots \mathfrak{a}_{n-1}\big) = (\mathfrak{a}_n, \mathfrak{a}_1 \ldots \mathfrak{a}_{n-1}) = \mathcal{J}, \qquad \text{q. e. d.}$$

Aditamento ao lema 3:- Pondo $\mathfrak{a} = \mathfrak{a}_1 \ldots \mathfrak{a}_n$, a representação de cada elemento de $\mathcal{J}$ como soma de elementos dos $\mathfrak{b}_\nu$ é unívoca, módulo $\mathfrak{a}$.

Seja, para $a \in \mathcal{J}$,

$$a = b_1 + \cdots + b_n , \qquad a = B_1 + \cdots + B_n , \; (b_i , B_i \in \mathfrak{b}_i).$$

No caso n = 2, tem-se

$$a = b_1 + b_2 , \qquad a = B_1 + B_2 , \qquad B_1 - b_1 = b_2 - B_2 = \alpha .$$

O elemento α pertence a $\mathfrak{b}_1$ e a $\mathfrak{b}_2$, ou seja a $\mathfrak{a}_2$ e a $\mathfrak{a}_1$, e pertence, portanto, a $[\mathfrak{a}_1, \mathfrak{a}_2] = \mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}$. Admitindo que o aditamento é válido para n - 1, ponhamos

$$\alpha = b_1 + \cdots + b_{n-1}, \qquad \beta = B_1 + \cdots + B_{n-1} .$$

Vê-se que $\beta = a - B_n = \alpha + (b_n - B_n)$, com $b_n, B_n \in \mathfrak{a}_1 \ldots \mathfrak{a}_{n-1}$. Assim, tem-se

$$\beta \equiv \alpha \,(\mathfrak{a}_1 \ldots \mathfrak{a}_{n-1}) , \qquad \beta = \alpha + (\beta - \alpha) = b_1 + \cdots + b_{n-1} + r = B_1 + \cdots + B_{n-1} .$$

onde $\tau = \beta - \alpha$. Escrevendo, por ex.,

$$\beta = (b_1 + \tau) + b_2 + \cdots + b_{n-1} = B_1 + \cdots + B_{n-1} ,$$

e tendo em conta que é

$$b_1 \in \mathfrak{a}_2 \cdots \mathfrak{a}_n \subseteq \mathfrak{a}_2 \cdots \mathfrak{a}_{n-1} , \quad \tau \in \mathfrak{a}_1 \cdots \mathfrak{a}_{n-1} \subseteq \mathfrak{a}_2 \cdots \mathfrak{a}_{n-1} ,$$

$$B_1 \in \mathfrak{a}_2 \cdots \mathfrak{a}_{n-1} , \quad b_2, B_2 \in \mathfrak{a}_1 \mathfrak{a}_3 \cdots \mathfrak{a}_n \subseteq \mathfrak{a}_1 \mathfrak{a}_3 \cdots \mathfrak{a}_{n-1} , \quad \text{etc.},$$

conclui-se

$$b_i \equiv B_i (\mathrm{mod}\ \mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}) , \qquad (i = 1, 2, \ldots, n-1).$$

Tanto os b_i como os B_i $(i = 1, 2, \ldots, n-1)$ pertencem a $\mathfrak{a}_n$, e, por isso, é $b_i \equiv B_i (\mathrm{mod}\ \mathfrak{a}_n)$. Será

$$b_i \equiv B_i (\mathrm{mod}\ [\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}, \mathfrak{a}_n]), \text{ ou} \quad b_i \equiv B_i (\mathrm{mod}\ \mathfrak{a}).$$

A congruência $b_n \equiv B_n (\mathrm{mod}\ \mathfrak{a})$ resulta do facto de ser

$$B_n - b_n = (b_1 - B_1) + \cdots + (b_{n-1} - B_{n-1}) \in \mathfrak{a}_n ,$$

$$B_n - b_n \in \mathfrak{a}_1 \cdots \mathfrak{a}_{n-1} .$$

Consequências:- Resultam dos raciocínios anteriores algumas consequências importantes que vamos assinalar. Passemos de $\mathfrak{r}$ a $\mathfrak{r}/\mathfrak{a} = \mathfrak{r}'$. Vê-se que vale

$$\mathfrak{r}' = (\mathfrak{f}_1', \ldots, \mathfrak{f}_n'), \quad (\mathfrak{f}_i' = \mathfrak{f}_i/\mathfrak{a} = \text{correspondente de } \mathfrak{f}_i \text{ em } \mathfrak{r} \sim \mathfrak{r}').$$

Como a representação de cada elemento $a' \in \mathfrak{r}'$ na soma anterior é única, segue-se que a referida soma é directa: $\mathfrak{r}' = \mathfrak{f}_1' + \cdots + \mathfrak{f}_n'$. Em particular, a decomposição do elemento um, u', de $\mathfrak{r}'$, dá

$$u' = e_1' + \cdots + e_n', \qquad e_i'^2 = e_i' , \qquad e_i' e_k' = 0, \quad (i \neq k).$$

O idempotente e_i' é elemento um de $\mathfrak{f}_i'$. Consideremos, por ex., a sucessão de homomorfismos $\mathfrak{r} \sim \mathfrak{r}' \sim \mathfrak{o}_1'$. Conclui-se o homomorfismo $\mathfrak{r} \sim \mathfrak{f}_1'$ e o isomorfismo $\mathfrak{f}_1' \cong \mathfrak{r}/\mathfrak{A}$. O ideal bilateral $\mathfrak{A}$ procura-se a partir de $b_1' = 0$. Em $\mathfrak{r}'$ reencontra-se $\mathfrak{f}_2' + \cdots + \mathfrak{f}_n'$. Se pusermos $\mathfrak{a}_j' = \mathfrak{a}_j/\mathfrak{a}$, vê-se que é $\mathfrak{a}_j \mathfrak{f}_j = \mathfrak{a}$ e $\mathfrak{a}_j' \mathfrak{f}_j' = (0)$. Assim, tem-se

$$\mathfrak{a}_1' = \mathfrak{a}_1' \mathfrak{r}' = \mathfrak{a}_1' \mathfrak{f}_2' + \cdots + \mathfrak{a}_1' \mathfrak{f}_n' .$$

Nestas condições é $\mathfrak{a}_1' \equiv \mathfrak{f}_2' + \cdots + \mathfrak{f}_n'$. Como, porém, $\mathfrak{f}_i' \equiv \mathfrak{a}_1'$, $(i = 2, 3, \ldots, n)$, segue-se a igualdade $\mathfrak{a}_1' = \mathfrak{f}_2' + \cdots + \mathfrak{f}_n'$. Será $\mathfrak{A} = \mathfrak{a}_1$ e pode escrever-se

$$\mathfrak{f}_1' \cong \mathfrak{r}/\mathfrak{a}_1 , \quad (\text{analogamente}, \ \mathfrak{f}_i' \cong \mathfrak{r}/\mathfrak{a}_i).$$

A segunda consequência que queremos assinalar é relativa a uma questão incidental, sem uso posterior. Trata-se de verificar que há soluções comuns às congruências

$$x \equiv \alpha_i (\mathrm{mod}\ \mathfrak{a}_i), \qquad (i = 1, 2, \ldots, n), \tag{6}$$

nas quais os α_i são elementos dados de $\mathfrak{r}$. Ponhamos

$$\alpha_1 = b_{11} + \cdots + b_{n1} , \ \ldots , \ \alpha_n = b_{1n} + \cdots + b_{nn} , \quad (b_{ik} \in \mathfrak{f}_i).$$

Vamos mostrar que $x = b_{11} + b_{22} + \cdots + b_{nn}$ é solução de (6). É, por ex.,

$$b_{11} + \cdots + b_{nn} - \alpha_1 = (b_{11} - \alpha_1) + b_{22} + \cdots + b_{nn} .$$

Ora $b_{11} - \alpha_1 = -b_{21} - \cdots - b_{n1} \in \mathfrak{a}_1$, o mesmo sucedendo com $b_{22}, \ldots, b_{nn}$. A conclusão está tirada. Se a $x = b_{11} + \cdots + b_{nn}$ se junta um elemento qualquer de $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_n$, continuamos a obter soluções de (6). Obtêm-se assim todas as soluções de (6), porque, se $\underline{x}$ e $\underline{y}$ são duas soluções, é[1]

$$x \equiv \alpha_i (\mathfrak{a}_i), \quad y \equiv \alpha_i (\mathfrak{a}_i), \quad x - y \equiv 0 (\mathfrak{a}_i), \quad x - y \in \mathfrak{a} .$$

(1) Cfr. com van der Waerden, "Moderne Algebra", II Teil, pgs. 43 a 48.

5) Sobre as ampliações das álgebras simples - Assinalámos no final do § 3 a importância da teoria das ampliações das álgebras. Dada uma álgebra simples $\mathcal{A}$, se pusermos $\mathcal{A} = \mathfrak{K}_r \times \mathcal{L}$, tem-se, quando se passa de $\mathfrak{K}$ ao corpo comutativo $\Omega \supseteq \mathfrak{K}$,

$$\mathcal{A}_\Omega = (\mathfrak{K}_r \times \mathcal{L})_\Omega = \Omega_r \times \mathcal{L}_\Omega . \qquad (6')$$

O estudo da ampliação $\mathcal{A}_\Omega$ reduz-se ao estudo da ampliação $\mathcal{L}_\Omega$, da álgebra de divisão $\mathcal{L}$. Vamos, por isso, ocupar-nos primeiramente das álgebras de divisão. Começaremos pelo caso em que a álgebra $\mathcal{L}$ é um corpo comutativo separável, ampliação finita de $\mathfrak{K}$. Os teoremas relativos a esse caso (e a uma extensão) assentam sobre o conteúdo do § anterior. Passaremos depois à hipótese de $\mathcal{L}$ ser uma ampliação finita inseparável de $\mathfrak{K}$, após o que trataremos então as álgebras de divisão não comutativas.

Pode ter-se já em conta que, se for Ω uma ampliação finita de $\mathfrak{K}$, as relações $\mathcal{L}_\Omega = \mathcal{L} \times \Omega = \Omega \times \mathcal{L}$ reduzem o estudo da questão a um problema resolvido pelo teorema fundamental do § 3. Efectivamente, como há elemento um em $\mathcal{L}$ (e em $\mathcal{L}_\Omega$), os ideais ordinários de $\mathcal{L}_\Omega$ são ideais admissíveis, tanto considerando esta última como álgebra sobre Ω como álgebra sobre $\mathfrak{K}$. Ora, a álgebra $\Omega \times \mathcal{L}$, sobre $\mathfrak{K}$, de centro $\Omega \times Z = Z_\Omega$, é semi-simples, se $\Omega \times Z$ for semi-simples, e apenas nesse caso. Regressando a $\mathcal{A}_\Omega = \mathcal{A} \times \Omega$, pode enunciar-se este

Teorema:- Se Ω é uma ampliação finita de $\mathfrak{K}$, é condição necessária e suficiente, para que a álgebra $\mathcal{A}_\Omega$, sobre Ω, ampliação da álgebra simples $\mathcal{A}$, sobre $\mathfrak{K}$, seja semi-simples, que seja semi-simples o seu centro Z_Ω (Z = centro de $\mathcal{A}$). Efectivamente, $Z_\Omega = \Omega_z$ é centro de $\mathcal{A}_\Omega$ e de $\mathcal{L}_\Omega = \Omega_{\mathcal{L}}$. Se Ω_z é semi-simples, $\Omega_{\mathcal{L}}$ é semi-simples. A igualdade (6') mostra que $\mathcal{A}_\Omega$ é semi-simples. Inversamente, se $\mathcal{A}_\Omega$ é semi-simples, o seu centro é semi-simples (assim como $\mathcal{L}_\Omega$).

O caso em que Ω é uma ampliação qualquer de $\mathfrak{K}$ estuda-se na linha de ideias que já se referiu (teorema 10 deste §).

Teorema 1 :- Se $\mathcal{L} = \mathfrak{K}(\lambda_1)$ é uma ampliação finita separável de $\mathfrak{K}$ e se λ_1 é raiz da equação irredutível em $\mathfrak{K}$, $\varphi(x) = 0$, a álgebra $\mathcal{L}_\Delta$, onde Δ é uma ampliação comutativa de $\mathfrak{K}$, na qual $\varphi(x)$ admite a decomposição em polinómios irredutíveis primos $\varphi(x) = \varphi_1(x) \dots \varphi_\rho(x)$, não tem radical e é uma soma de ρ corpos comutativos que são álgebras sobre Δ.

Sabemos que $\mathcal{L} \cong \mathfrak{K}[x] / (\varphi(x))$ e que $\mathcal{L}_\Delta \cong \Delta[x] / (\varphi(x))$. Ora, por hipótese, $(\varphi_1(x)), \dots, (\varphi_\rho(x))$ são ideais de $\Delta[x]$ que não têm divisor (1). São, portanto, ideais dois a dois sem divisor comum, os quais verificam a igualdade

$$\mathfrak{a} = (\varphi(x)) = (\varphi_1(x)) \dots (\varphi_\rho(x)) = \mathfrak{a}_1 \dots \mathfrak{a}_\rho , \quad (\mathfrak{a}_i = (\varphi_i(x))) .$$

Nessas condições é

$$\mathfrak{I}' = \Delta[x]/(\varphi(x)) = \mathfrak{k}'_1 + \dots + \mathfrak{k}'_\rho , \qquad (\mathfrak{k}'_i \cong \Delta[x]/(\varphi_i(x))) .$$

Cada $\mathfrak{k}'_i$ é um corpo comutativo e álgebra sobre Δ. Pondo

$$\mathcal{L}_\Delta = \mathcal{L}_1 + \dots + \mathcal{L}_\rho ,$$

onde $\mathcal{L}_i \cong \mathfrak{k}'_i$, vê-se que $\mathcal{L}_\Delta$ é uma álgebra redutível cujo radical é soma dos radicais dos $\mathcal{L}_i$. Estes últimos são nulos e o teorema está demonstrado.

Corolário 1 :- Dada a álgebra $\mathcal{L} = \mathfrak{K}(\lambda_1)$ do teorema, a álgebra $\mathcal{A} = \mathcal{L}_\mathfrak{M}$, na qual $\mathfrak{M}$ é o corpo de decomposição de $\varphi(x)$, é uma álgebra diagonal da forma $\mathcal{L}_\mathfrak{M} = \mathcal{L}_\mathfrak{M}^{(1)} + \dots + \mathcal{L}_\mathfrak{M}^{(n)}$, onde $\mathcal{L}^{(i)}$ é uma álgebra de 1ª ordem sobre o corpo fundamental $\mathfrak{K}(\lambda_1)$ [λ_i = conjugado de λ_1] equivalente a $\mathcal{L}$ sobre $\mathfrak{K}$.

(1) Veja-se "A, pgs. 117 e seguintes", assim como "A, pgs. 60 e seguintes".

Como se tem $\varphi(x) = \prod_{i=1}^{n} (x - \lambda_i)$, é

$$\mathcal{L}_n = \mathcal{L}_1 + \cdots + \mathcal{L}_n,$$

com $\mathcal{L}_i \cong \mathcal{R}[x]/(x - \lambda_i)$. $\mathcal{L}_i$ é, deste modo, uma álgebra de 1ª ordem sobre $\mathcal{R}$, equivalente a $\mathcal{R}$. Pondo $u = e_1 + \cdots + e_n$, $(e_i \in \mathcal{L}_i$, $e_i^2 = e_i$, $e_i e_k = 0)$, vem

$$\mathcal{U} = \mathcal{L}_n = \mathcal{L}_n e_1 + \cdots + \mathcal{L}_n e_n = \mathcal{R} e_1 + \cdots + \mathcal{R} e_n .$$

Uma tal álgebra diz-se diagonal. Ela é de ordem n sobre $\mathcal{R}$, que é a ordem de $\mathcal{L}$ sobre $\mathcal{K}$. Pondo $x_0 = e_1\lambda_1 + \cdots + e_n\lambda_n$, vê-se que é $x_0^k = e_1\lambda_1^k + \cdots + e_n\lambda_n^k$. As equações

$$\begin{aligned} u &= e_1 + \cdots + e_n , \\ x_0 &= e_1\lambda_1 + \cdots + e_n\lambda_n , \\ &\cdots\cdots\cdots\cdots \\ x_0^{n-1} &= e_1\lambda_1^{n-1} + \cdots + e_n\lambda_n^{n-1} , \end{aligned} \qquad (7)$$

nas quais os $\lambda_j \in \mathcal{R}$ são os conjugados de λ_1, constituem um sistema Cramer em que as incógnitas são os e_i, visto que o determinante destes é diferente de zero, por ser um determinante de Vandermonde $= \prod_{j>i}(\lambda_j - \lambda_i)$ e ser $\varphi(x)$ um polinómio separável. Por meio de (7), passa-se da base independente $(e_1, \ldots, e_n)$, de $\mathcal{U}$, à base independente $(u, x_0, \ldots, x_0^{n-1})$. O isomorfismo $\mathcal{L}_n \cong \mathcal{R}[x]/(\varphi(x))$ é dado pela correspondência $x + (\varphi(x)) \rightarrow x_0$. A base $(u, x_0, \ldots, x_0^{n-1})$ tem a mesma tabela de multiplicação que a base $(u, \lambda_1, \ldots, \lambda_1^{n-1})$, de $\mathcal{L}$. De (7) deduz-se imediatamente, com efeito, $\varphi(x_0) = 0$.

Tomemos um elemento de $\mathcal{U}$ da forma le_i, onde $l \in \mathcal{U}$ se forma com coeficientes $\beta_i \in \mathcal{K}$. Será

$$le_i = (\beta_0 + \beta_1 x_0 + \cdots + \beta_{n-1} x_0^{n-1})e_i = \beta_0 e_i + \beta_1 \lambda_i e_i + \cdots + \beta_{n-1}\lambda_i^{n-1} e_i =$$

$$= (\beta_0 + \beta_1\lambda_i + \cdots + \beta_{n-1}\lambda_i^{n-1})e_i = K_i e_i , \qquad (K_i \in \mathcal{K}(\lambda_i)) .$$

$\mathcal{U} e_i = \mathcal{R} e_i$ pode considerar-se ampliação da álgebra de 1ª ordem sobre $\mathcal{K}(\lambda_i) = \mathcal{K}_i$, $\mathcal{L}^{(i)} = \mathcal{K}_i e_i$. $\mathcal{L}^{(i)} \cong \mathcal{K}_i$ é equivalente a $\mathcal{L} = \mathcal{K}_1$ sobre $\mathcal{K}$.

Pode dar-se uma generalização do corolário anterior, como vai ver-se em seguida.

Teorema 2 :- Se $\mathcal{U}$ é uma álgebra finita, com elemento um e corpo fundamental $\mathcal{K}$, e se o seu centro $\mathcal{Z}$ contém uma ampliação separável $\mathcal{L} = \mathcal{K}(\lambda_1) = \mathcal{K}_1$, de $\mathcal{K}$, a álgebra $\mathcal{U}_n$ é uma soma directa da forma $\mathcal{U}_n = \mathcal{U}_n^{(1)} + \cdots + \mathcal{U}_n^{(r)}$, na qual $\mathcal{U}_n^{(i)}$ é uma álgebra sobre $\mathcal{K}(\lambda_i) = \mathcal{K}_i$, de ordem igual à ordem de $\mathcal{U}$ sobre $\mathcal{K}$, equivalente a $\mathcal{U}$ sobre $\mathcal{K}_i$. Tem-se, pondo em evidência bases e corpos fundamentais duma álgebra:

$$\begin{aligned} \mathcal{U} &= \mathcal{K}\left\{u, \lambda_1, \ldots, \lambda_1^{n-1}; z_1, \ldots, z_r; v_1, \ldots, v_s\right\} , \\ \mathcal{Z} &= \mathcal{K}\left\{u, \lambda_1, \ldots, \lambda_1^{n-1}; z_1, \ldots, z_r\right\} , \\ \mathcal{L} &= \mathcal{K}\left\{u, \lambda_1, \ldots, \lambda_1^{n-1}\right\} , \end{aligned}$$

$$\mathcal{U} \supseteq \mathcal{Z} \supseteq \mathcal{L} = \mathcal{K}(\lambda_1) \supseteq \mathcal{K} .$$

Quando se passa a $\mathcal{U}_n$, deverá pôr-se:

$$\begin{aligned} \mathcal{U}_n &= \mathcal{R}\left\{u, x_0, \ldots, x_0^{n-1}; \overline{z}_1, \ldots, \overline{z}_r; \overline{\overline{v}}_1, \ldots, \overline{\overline{v}}_s\right\} , \\ \mathcal{Z}_n &= \mathcal{R}\left\{u, x_0, \ldots, x_0^{n-1}; \overline{z}_1, \ldots, \overline{z}_r\right\} , \\ \mathcal{L}_n &= \mathcal{R}\left\{u, x_0, \ldots, x_0^{n-1}\right\} , \end{aligned}$$

(1) Cfr. A.A.Albert, "Structure of algebras", pgs.35 e 36. Para o conteúdo do resto do Cap., cfr. ainda a mesma obra, pgs.41 a 45; van der Waerden, II Teil, pgs.174 a 177; e M.Deuring, "Algebren", pgs.36 e 37.

sem esquecer que os elementos das bases são puros símbolos, com as leis de multiplicação que resultam já de $\mathcal{U}$. Introduzindo os n idempotentes e_i que existem em $\mathcal{L}_n$, podemos escrever

$$\mathcal{U}_n = \mathcal{K}\{e_1,\ldots,e_n;\ \overline{z}_1,\ldots,\overline{z}_r;\ \overline{v}_1,\ldots,\overline{v}_s\}\ ,$$

$$z_n = \mathcal{K}\{e_1,\ldots,e_n;\ \overline{z}_1,\ldots,\overline{z}_r\}\ .$$

Nestas condições, tem lugar a igualdade

$$\mathcal{U}_n = \mathcal{U}_n e_1 + \cdots + \mathcal{U}_n e_n\ . \tag{8}$$

Estudemos a álgebra $\mathcal{U}_n e_i$, de corpo fundamental $\mathcal{K}$. Se a ordem de $\mathcal{U}$ relativamente a $\mathcal{L}$ é igual a m, têm lugar as igualdades

$$\mathcal{U} = \mathcal{L}\{u_1,\ldots,u_m\} = \mathcal{L}u_1 + \cdots + \mathcal{L}u_m\ , \tag{9}$$

e $\mathcal{U}$ aparece como uma álgebra de ordem mn relativamente a $\mathcal{K}$. A ordem de $\mathcal{U}_n$ será também mn. A ordem de $\mathcal{U}_n e_i$ é efectivamente m, como passamos a mostrar. Consideremos os elementos $\overline{u}_j \in \mathcal{U}_n$, que se formam nesta álgebra como os u_j se formam em $\mathcal{U}$. Visto que os elementos

$$u_j,\ u_j\lambda_1,\ldots,\ u_j\lambda_1^{n-1},\qquad (j = 1,\ 2,\ldots,m),$$

formam uma base de $\mathcal{U} = \mathcal{U}_{\mathcal{K}}$, também os elementos

$$\overline{u}_j,\ \overline{u}_j x_0,\ldots,\ \overline{u}_j x_0^{n-1},\qquad (j = 1,\ 2,\ldots,m),$$

formam uma base de $\mathcal{U}_n$. Nessas condições, os elementos

$$\overline{u}_j e_1,\ldots,\ \overline{u}_j e_n,\qquad (j = 1,\ 2,\ldots,m),$$

formam uma base de $\mathcal{U}_n$. Ora em $\mathcal{U}_n e_i$ figuram os elementos

$$\overline{u}_1 e_i,\ldots,\overline{u}_m e_i, \tag{10}$$

pelo que a sua ordem é, pelo menos, igual a m. A igualdade (8) mostra que não pode ser maior. Em (10) define-se uma tabela de multiplicação, a partir da tabela seguinte, válida na álgebra referida em (9):

$$u_r u_s = \sum_{k=1}^{m} \alpha_{rsk} u_k\ , \qquad (\alpha_{rsk} \in \mathcal{L}).$$

Deverá escrever-se

$$u_r u_s = \sum_{k=1}^{m} \sum_{t=0}^{n-1} \lambda_1^t h_{rskt} u_k = \sum_{t,k} h_{rskt}\, \lambda_1^t u_k\ , \qquad (h_{rskt} \in \mathcal{K}),$$

e, depois,

$$\overline{u}_r \overline{u}_s = \sum_{t,k} h_{rskt} x_0^t\, \overline{u}_k\ .$$

Vem, então,

$$\overline{u}_r e_i \cdot \overline{u}_s e_i = \sum_{t,k} h_{rskt} x_0^t\, \overline{u}_k e_i\ . \tag{11}$$

Em virtude de ser $x_0 = e_1\lambda_1 + \cdots + e_n\lambda_n$, $x_0 e_i = e_i \lambda_i$, é também

$$x_0^t e_i = x_0 e_i \cdots x_0 e_i = e_i\, \lambda_i^t\ .$$

A igualdade (11) toma a forma

$$\overline{u}_r e_i \cdot \overline{u}_s e_i = \sum_{t,k} h_{rskt} \lambda_i^t \overline{u}_k e_i\ .$$

Como $h_{rskt}\lambda_i^t \in \mathcal{K}_i$, conclui-se daqui a existência duma álgebra

$$\mathcal{U}^{(i)} = \mathcal{K}_i\{\overline{u}_1 e_i,\ldots,\overline{u}_m e_i\}\ .$$

A álgebra $\mathcal{U}_n e_i$ é uma ampliação de $\mathcal{U}^{(i)}$, obtida ampliando $\mathcal{K}_i$ para $\mathcal{K}$. $\mathcal{U}^{(i)}$, considerada álgebra relativamente a $\mathcal{K}$, é de ordem mn. É evidentemente equivalente à álgebra $\mathcal{U}$, sobre $\mathcal{K}$.

mediante a correspondência

$$\lambda_i^t \overline{u}_R e_i \longrightarrow \lambda_1^t u_R .$$

O teorema está demonstrado.

Teorema 3 :- Se $\mathcal{L} = \mathcal{K}(\alpha_1)$ é uma ampliação finita inseparável de $\mathcal{K}$, e se α_1 é raiz da equação irredutível em $\mathcal{K}$, $\varphi(x) = 0$, a álgebra $\mathcal{L}_{\mathcal{R}}$, onde $\mathcal{R}$ é o corpo de decomposição de $\varphi(x)$, é uma álgebra com radical. Tem-se

$$\mathcal{L} = \mathcal{K}(\alpha_1) \cong \mathcal{K}[x]/(\varphi(x)) , \qquad \mathcal{L}_{\mathcal{R}} \cong \mathcal{R}[x]/(\varphi(x)) .$$

Suponhamos que α_1 tem o expoente $t > 0$ e que o grau de $\varphi(x)$ é $n = n_0 p^t$. No corpo $\mathcal{R} = \mathcal{K}(\alpha_1, \ldots, \alpha_{n_0})$, $\varphi(x)$ tem uma decomposição

$$\varphi(x) = \prod_{i=1}^{n_0} (x - \alpha_i)^{p^t} = \big(\rho(x)\big)^{p^t}, \quad \text{com} \quad \rho(x) = \prod_{i=1}^{n_0} (x - \alpha_i) .$$

O polinómio $\rho(x) \in \mathcal{R}[x]$ verifica as relações

$$\rho(x) \not\equiv 0 \ \big(\varphi(x)\big) , \qquad \big(\rho(x)\big)^{p^t} \equiv 0 \big(\varphi(x)\big) .$$

A álgebra $\mathcal{R}[x]/(\varphi(x))$ sobre $\mathcal{R}$ tem radical. Por ex., o elemento $\rho(x) + (\varphi(x)) \neq 0$, que é nilpotente, gera um ideal nilpotente, visto tratar-se duma álgebra comutativa. O mesmo sucederá na álgebra isomorfa $\mathcal{L}_{\mathcal{R}}$, o que demonstra o teorema. É possível, porém, encontrar um corpo $\mathcal{P} \cong \mathcal{R}$, tal que $\mathcal{L}_{\mathcal{P}}$ já possui radical. Vamos demonstrar, a esse respeito, o seguinte

Teorema 4 :- Se for $\mathcal{P} = \mathcal{K}(\alpha_1^{p^{t-1}}, \ldots, \alpha_{n_0}^{p^{t-1}})$, a álgebra $\mathcal{L}_{\mathcal{P}}$ tem radical. Pondo

$$\varphi(x) = \prod_{i=1}^{n_0} (x - \alpha_i)^{p^t} = \left(\prod_{i=1}^{n_0} (x^{p^{t-1}} - \alpha_i^{p^{t-1}}) \right)^p = \big(\tau(x)\big)^p ,$$

o polinómio $\tau(x)$ pertence a $\mathcal{P}[x]$. A demonstração é agora

a mesma que a do teorema anterior. Mais geralmente ainda, é válido este outro

Teorema 5 :- Se for $\Delta = \mathcal{K}(\alpha_1^{p^{t-1}}, \alpha_2^{p^t}, \ldots, \alpha_{n_0}^{p^t})$, a álgebra $\mathcal{L}_\Delta$ tem radical. Ponhamos $\alpha_1^{p^t} = \lambda_1$, $\alpha_1^{p^{t-1}} = \eta_1$. Tem-se

$$\mathcal{L} = \mathcal{K}(\alpha_1) \supset \mathcal{K}(\lambda_1) = \mathcal{K}_1 \supseteq \mathcal{K} .$$

Admitindo que é $\varphi(x) = \psi(x^{p^t})$, representemos por $\mathcal{R}_0 = \mathcal{K}(\alpha_1^{p^t}, \ldots, \alpha_{n_0}^{p^t}) = \mathcal{K}(\lambda_1, \ldots, \lambda_{n_0})$ o corpo de decomposição de $\psi(x) = 0$. Será

$$\mathcal{L}_{n_0} \supset \mathcal{K}_{1 n_0} \supseteq \mathcal{R}_0 \supseteq \mathcal{K} .$$

A álgebra $\mathcal{K}_{1 n_0}$ tem n_0 idempotentes $e_1, \ldots, e_{n_0}$. Para base da mesma podemos tomar também $u, x_0, \ldots, x_0^{n_0 - 1}$, onde $x_0 = e_1 \lambda_1 + \ldots + e_{n_0} \lambda_{n_0}$. Ao passarmos à álgebra $\mathcal{L}_\Delta$ e a $\mathcal{K}_{1\Delta}$, continuaremos a encontrar elementos $\underline{e_i}$ e $\underline{x_0}$. Em $\mathcal{L}$, tem-se $\eta_1^p = \lambda_1$. Em $\mathcal{L}_\Delta$, ter-se-á $\overline{\eta}_1^p = x_0$, se $\overline{\eta}_1 \in \mathcal{L}_\Delta$ se exprime aqui como η_1 se exprime em $\mathcal{L}$. Pondo

$$a = (\overline{\eta}_1 - \eta_1) e_1 = (\overline{\alpha_1^{p^{t-1}}} - \alpha_1^{p^{t-1}}) e_1 ,$$

vê-se que é

$$a^p = (\overline{\eta}_1 - \eta_1)^p e_1^p = (\overline{\eta}_1^p - \eta_1^p) e_1 = x_0 e_1 - \lambda_1 e_1 = \lambda_1 e_1 - \lambda_1 e_1 = 0$$

O elemento $a \in \mathcal{L}_\Delta$ gera, pois, um ideal nilpotente.

Corolário 2 :- Se $\mathcal{A}$ é uma álgebra finita com elemento um e corpo fundamental $\mathcal{K}$, e se o seu centro $\mathcal{Z}$ contém uma ampliação inseparável $\mathcal{M}$, de $\mathcal{K}$, cada elemento $\alpha_1 \in \mathcal{M}$, de expoente $t > 0$, é tal que, designando por $\mathcal{R}_0$ a ampliação separável de $\mathcal{K}$, definida através da equação irredutível $\psi(x) = 0$ a que satisfaz $\alpha_1^{p^t}$, e pondo $\Delta = \mathcal{R}_0(\alpha_1^{p^{t-1}})$, $\mathcal{L} = \mathcal{K}(\alpha_1)$, o elemento

$$a = \left(\alpha_1^{p^{t-1}} - \alpha_1^{p^{t-1}}\right) e_1 \in \mathcal{L}_\Delta \equiv \mathfrak{w}_\Delta \equiv \mathfrak{z}_\Delta \subseteq \mathfrak{o}_\Delta$$

é nilpotente e de expoente $\leq p$.

$\mathcal{L}$ passará a ser agora uma álgebra de divisão não comutativa sobre $\mathfrak{K}$. Se Δ é uma ampliação algébrica (finita ou infinita) comutativa de $\mathfrak{K}$, a álgebra $\mathcal{L}_\Delta$, sobre Δ, gosa da propriedade expressa no seguinte

Teorema 6 :- Se a álgebra $\mathcal{L}$ de divisão sobre $\mathfrak{K}$ tem o centro Z, cada ideal bilateral $\mathfrak{a}$, de $\mathcal{L}_\Delta$, é gerado por um ideal $\mathfrak{a}' = [\mathfrak{a}, Z_\Delta]$, de Z_Δ. Sem dúvida que o ideal $\mathfrak{f}$, de $\mathcal{L}_\Delta$, gerado por $\mathfrak{a}'$, está contido em $\mathfrak{a}$. O teorema demonstra-se procurando um ideal $\mathfrak{f}' \equiv \mathfrak{a}'$, que gera precisamente o ideal $\mathfrak{a}$. Ponhamos $\mathcal{L}_\Delta = \Delta\{u_1, \ldots, u_n\}$, $\mathfrak{a} = \Delta\{v_1, \ldots, v_m\}$, com

$$v_l = \sum_{j=1}^{n} u_j \alpha_{jl}, \qquad v_l u_k = \sum_{i=1}^{m} v_i \beta_{lik}, \qquad u_k v_l = \sum_{i=1}^{m} v_i \beta'_{lki},$$

onde os $\alpha, \beta, \beta' \in \Delta$. Em seguida, tomemos a ampliação $\Phi = \mathfrak{K}(\ldots, \alpha_{jl}, \ldots, \beta_{lik}, \ldots, \beta'_{lki}, \ldots)$, de $\mathfrak{K}$. A álgebra $\mathcal{L}_\Phi$ é álgebra sobre Φ e sobre $\mathfrak{K}$. Consideremos o módulo $\mathfrak{a}_0 = \Phi\{v_1, \ldots, v_m\}$, do qual $\mathfrak{a}$ é uma ampliação. $\mathfrak{a}$ é um ideal bilateral de $\mathcal{L}_\Phi = \mathcal{L} \times \Phi = \mathcal{L} \times \Omega = \Phi_\mathcal{L}$, como se reconhece imediatamente. O teorema fundamental do § 3, pondo $\mathfrak{o} = \Phi$, $\Omega = \mathcal{L}$, afirma-nos que $\mathfrak{a}_0$ é ampliação do ideal $\mathfrak{a}'_0 = [\mathfrak{a}_0, \Phi_z]$, de $\Phi_z = \Phi \times Z = Z_\Phi$. Ter-se-á

$$\mathfrak{a}'_0 = \Phi\{z_1, \ldots, z_r\} = Z\{\varphi_1, \ldots, \varphi_t\},$$

onde se põem em evidência bases do ideal, que tanto podem ser compostas de elementos pertencentes a Z como a Φ, conforme se considera módulo relativamente a Φ ou a Z. Conclui-se que é

$$\mathfrak{a}_0 = \mathcal{L}\{\varphi_1, \ldots, \varphi_t\} = \Phi\{v_1, \ldots, v_m\}.$$

Passemos de $\mathfrak{a}'_0 = \Phi\{z_1, \ldots, z_r\}$ a $\mathfrak{f}' = \Delta\{z_1, \ldots, z_r\}$. $\mathfrak{f}'$ é ideal bilateral de Z_Δ. Estudemos a correspondência $\mathfrak{a} \longrightarrow \mathfrak{f}'$. Fàcilmente se vê que o ideal bilateral de $\mathcal{L}_\Delta$, gerado por $\mathfrak{f}'$, é o

ideal $\mathfrak{a}$. Com efeito, o ideal gerado por $\mathfrak{f}'$ contém $\mathfrak{a}'_0 = \Phi\{z_1, \ldots, z_r\} = Z\{\varphi_1, \ldots, \varphi_t\}$, e contém, portanto, $\mathcal{L}\{\varphi_1, \ldots, \varphi_t\} = \Phi\{v_1, \ldots, v_m\} = \mathfrak{a}_0$, e também $\Delta\{v_1, \ldots, v_m\} = \mathfrak{a}$. Deste modo, tendo em vista que é $\mathfrak{f}' \equiv [\mathfrak{a}, Z_\Delta]$, o teorema está demonstrado. Pode observar-se que $\mathfrak{a}$ é gerado pelos elementos $z_1, \ldots, z_r$.

Teorema 7 :- Se $\mathfrak{a}'$ é simples, tem-se $\mathfrak{f}' = \mathfrak{a}'$ e $\mathfrak{a}$ é um ideal bilateral simples. Se $\mathfrak{a}'$ é simples, como se tem $\mathfrak{f}' \equiv \mathfrak{a}'$, será $\mathfrak{f}' = \mathfrak{a}'$. O ideal $\mathfrak{a}$ é simples, pois, se o não fosse, existiria $\mathfrak{f} \subset \mathfrak{a}$, e o processo que levou de $\mathfrak{a}$ a $\mathfrak{f}'$ levaria de $\mathfrak{f}$ a $\mathfrak{f}'$, com $\mathfrak{f}'' \equiv \mathfrak{f}'$, e, portanto, com $\mathfrak{f}'' = \mathfrak{f}'$. Daqui tirava-se $\mathfrak{f} = \mathfrak{a}$.

Corolário 3 :- Se Z_Δ é semi-simples, $\mathcal{L}_\Delta$ é semi-simples. Ponhamos $Z_\Delta = \mathfrak{a}'_1 + \cdots + \mathfrak{a}'_s$, onde os $\mathfrak{a}'_l$ são simples. Como Z_Δ é o centro de $\mathcal{L}_\Delta$, há uma decomposição correspondente

$$\mathcal{L}_\Delta = \mathfrak{a}_1 + \cdots + \mathfrak{a}_s.$$

Os ideais bilaterais $\mathfrak{a}_l$ são gerados pelos $\mathfrak{a}'_l$ e tem-se $\mathfrak{a}'_l = [\mathfrak{a}_l, Z_\Delta]$. Em virtude do teorema anterior, os $\mathfrak{a}_l$ são simples.

Se Δ não é ampliação algébrica de $\mathfrak{K}$, mas uma ampliação transcendente pura,(1) isto é, se resulta de $\mathfrak{K}$ por adjunção dum número finito ou infinito de indeterminadas, tem lugar o seguinte

Teorema 8 :- É condição necessária e suficiente, para que $\mathcal{L}_\Delta$ seja uma álgebra de divisão, que $\mathcal{L}$ seja uma álgebra de divisão.(2) Efectivamente, supondo $u_1, \ldots, u_n$ uma base de $\mathcal{L}$, um elemento $a \in \mathcal{L}_\Delta$ é da forma $a = \sum u_l \delta_l$, onde $\delta_l \in \Delta$. Dois elementos $a, b \in \mathcal{L}_\Delta$ têm um produto

$$ab = \sum u_l \delta_l \cdot \sum u_j \delta'_j = \sum_k u_k \left(\sum_{l,j} \alpha_{klj} \delta_l \delta'_j \right), \quad (\alpha_{klj} \in \mathfrak{K}).$$

(1) Veja-se van der Waerden, "Moderne Algebra", I Teil, pgs. 205.

(2) Cfr. A. Albert, "Structure of algebras", pgs. 16.

Se este produto é nulo, será também

$$\sum_{ij} \alpha_{Rij}\delta_l\delta'_j = 0 \ .$$

Uma tal igualdade é impossível, a não ser que sejam nulos todos os α_{Rij}, visto que Δ é transcendente pura. Mas, então, $\mathcal{L}$ seria uma álgebra zero, o que é absurdo.

Podemos associar as afirmações do corolário 3 e do teorema anterior, sem fazer qualquer restrição sobre o corpo Δ, e enunciar o seguinte

Teorema 9 :- Se uma álgebra de divisão $\mathcal{L}$ sobre $\mathfrak{K}$ se amplia para $\mathcal{L}_\Delta$, é condição necessária e suficiente, para que $\mathcal{L}_\Delta$ seja semi-simples (qualquer que seja Δ), que Z_Δ seja semi-simples. Na verdade, obtém-se Δ começando por fazer a adjunção a $\mathfrak{K}$ dum número finito ou infinito de indeterminadas, o que leva a $\sum \supset \mathfrak{K}$, e, em seguida, fazendo adjunções algébricas a $\sum$. Se Z_Δ é semi-simples, $Z_{\sum} = Z'$, $\mathcal{L}_{\sum} = \mathcal{L}'$ são semi-simples, pois são álgebras de divisão. Mas, então, $\mathcal{L}'_\Delta = \mathcal{L}_\Delta$ é semi-simples, visto que $Z'_\Delta = Z_\Delta$ é semi-simples.

O teorema com que abrimos o § enuncia-se agora mais geralmente:

Teorema 10 :- É condição necessária e suficiente, para que a ampliação $\mathcal{A}_\Omega$, da álgebra simples $\mathcal{A}$, seja semi-simples, que seja semi-simples a ampliação Z_Ω, do centro Z, de $\mathcal{A}$.

Suponhamos $\mathcal{A}$ uma álgebra semi-simples. Quando se passa de $\mathfrak{K}$ a Ω, pode $\mathcal{A}_\Omega$ ficar ou não semi-simples. Recorrendo à decomposição de $\mathcal{A}$ em álgebras simples, pode enunciar-se o

Teorema 11 :- É condição necessária e suficiente, para que a ampliação $\mathcal{A}_\Omega$, da álgebra semi-simples $\mathcal{A}$, seja semi-simples, que seja semi-simples a ampliação do centro de $\mathcal{A}$.

Se uma álgebra $\mathcal{A}$ (necessàriamente semi-simples) fica semi-simples qualquer que seja o modo como se amplia o corpo fundamental, diz-se separável. Tem lugar o seguinte

Teorema 12 :- É condição necessária e suficiente, para que a álgebra semi-simples $\mathcal{A}$ seja separável, que seja separável o seu centro Z.

6) Detalhes sobre as ampliações das álgebras simples - Consideremos uma álgebra de divisão $\mathcal{L}$, de centro separável $Z \supseteq \mathfrak{K}$. Z_Δ é, então, uma soma de corpos comutativos. $\mathcal{L}_\Delta$ será semi-simples, soma de tantas álgebras simples sobre Δ quantas aqueles corpos. O número máximo de parcelas é dado pelo grau $(Z/\mathfrak{K})$. Podemos dar este enunciado:

Teorema 1 :- Se $\mathcal{L}$ é uma álgebra de divisão sobre $\mathfrak{K}$, cujo centro é uma ampliação separável do corpo fundamental, a álgebra $\mathcal{L}_\Delta$, qualquer que seja Δ, é uma álgebra semi-simples, soma de tantas álgebras simples quantas aquelas em que se decompõe Z_Δ. O número máximo de álgebras simples parcelas é dado pelo grau $(Z/\mathfrak{K})$.

Lema 1 :- Uma álgebra de divisão sobre um corpo algèbricamente fechado Ω é necessàriamente de 1ª ordem. Um elemento a da álgebra satisfaz a uma equação da forma

$$x^r + x^{r-1}\omega_{r-1} + \cdots + \omega_\Delta = 0, \qquad (\omega_l \in \Omega).$$

Considerado o 1º membro como polinómio em x, visto que Ω é algèbricamente fechado, a equação anterior pode escrever-se

$$(x-\omega') \ \ldots \ (x-\omega^{(r)}) = 0, \qquad (\omega^{(l)} \in \Omega).$$

Se agora x volta a ser o elemento a da álgebra, o facto de x comutar com os $\omega^{(l)}$ permite afirmar que a última equação é a mesma que aquela de que se partiu, sendo, portanto, a igual a um dos $\omega^{(l)}$.

Admitamos que $\mathcal{L}$ é uma álgebra normal de divisão. Será $Z = \mathfrak{K}$. $\mathcal{L}_\Delta$ é uma álgebra simples, visto que $Z_\Delta = \Delta$. $\mathcal{L}_\Delta$ é uma álgebra isomorfa dum anel de matrizes com elementos dum corpo Ω que contém o corpo comutativo Δ. Se, em particular, Δ for

algèbricamente fechado, tem-se $\Delta = \Omega$. Podemos dar o seguinte enunciado:

Teorema 2 :- Uma álgebra normal de divisão $\mathcal{L}$ tem uma ordem que é um quadrado perfeito m^2. Se o corpo fundamental se amplia para um corpo algèbricamente fechado Ω, a álgebra torna-se num anel completo de matrizes do grau m com elementos de Ω. A demonstração repousa ainda sobre o facto de $\mathcal{L}_\Omega$ ter, relativamente a Ω, a mesma ordem que $\mathcal{L}$ relativamente ao seu centro (corpo fundamental). O número m diz-se índice da álgebra.

Se $\mathcal{A}$ é álgebra normal simples, ao escrever-se

$$\mathcal{A}_\Omega = (\mathfrak{K}_r \times \mathcal{L})_\Omega = \Omega_r \times \mathcal{L}_\Omega,$$

concluimos que a ordem de $\mathcal{A}$ é também um quadrado perfeito e que, se Ω é algèbricamente fechado, $\mathcal{A}_\Omega$ é um anel completo de matrizes com elementos de Ω. Vamos precisar este resultado. Se a nossa álgebra normal simples $\mathcal{A}$, sobre $\mathfrak{K}$, é de ordem n, sabemos que $n = r^2m^2$, onde m^2 é a ordem de $\mathcal{L}$ sobre $\mathfrak{K}$. Supondo $m^2 = 1$, é $m = 1$, $\mathcal{L} = \mathfrak{K}$. Nesse caso, $\mathcal{A}$ é anel completo de matrizes com elementos de $\mathfrak{K}$. Sucede assim, por ex., se for $\mathfrak{K}$ algèbricamente fechado. Não supondo $\mathfrak{K}$ algèbricamente fechado e admitindo que é $\mathcal{L} \neq \mathfrak{K}$, tomemos uma ampliação algébrica finita Δ, de $\mathfrak{K}$. A álgebra $\mathcal{A}_\Delta$, normal sobre Δ, tem a ordem n. Pondo $\mathcal{A}_\Delta = \Delta_r \times \mathcal{L}_\Delta = \Delta_r \times \Delta_s \times \Sigma = \Delta_{rs} \times \Sigma = \Sigma_{rs}$, onde Σ é uma álgebra normal de divisão sobre Δ, tem-se $n = r^2s^2t^2$, se t^2 é a ordem de Σ relativamente a Δ. Supondo $t^2 = 1$, é $t = 1$, $\Sigma = \Delta$. $\mathcal{A}_\Delta$ é anel completo de matrizes com elementos de Δ. É o que sucede se Δ for algèbricamente fechado. Não supondo Δ algèbricamente fechado e admitindo que é $\Sigma \neq \Delta$, tomemos uma ampliação algébrica finita Ψ, de Δ. Fazendo $\mathcal{A}_\Delta = \mathcal{A}'$, a álgebra $\mathcal{A}'_\Psi = \mathcal{A}_\Psi$, normal sobre Ψ, tem a ordem n. E é

$$\mathcal{A}_\Psi = \mathcal{A}'_\Psi = (\Delta_{rs} \times \Sigma)_\Psi = \Psi_{rs} \times \Sigma_\Psi = \Psi_{rs} \times \ominus_\rho = \Psi_{rs\rho} \times \ominus = \ominus_{rs\rho},$$

onde a álgebra $\ominus$, sobre Ψ, se pode supor de ordem σ^2. Então

tem-se $n = r^2s^2t^2 = r^2s^2\rho^2\sigma^2$. Como a decomposição de n não pode prolongar-se indefinidamente, suponhamos, por ex., $\sigma^2 = 1$, $\sigma = 1$, $\ominus = \Psi$. Vê-se que é $\mathcal{A}_\Psi = \Psi_{rs\rho}$. É válido o

Teorema 3 :- Uma álgebra normal simples sobre $\mathfrak{K}$, $\mathcal{A} = \mathfrak{K}_r \times \mathcal{L} = \mathcal{L}_r$, fica normal simples quando se amplia o corpo fundamental. É álgebra separável e quadrada. Se Δ é uma ampliação finita de $\mathfrak{K}$ tal que $\mathcal{L}_\Delta$ é anel de matrizes de grau s, Δ_s, a álgebra $\mathcal{A}_\Delta$ é um anel Δ_{rs}.

7) Detalhes sobre o produto directo de duas álgebras simples - Estamos de posse dum teorema geral dado no § 3. Se quisermos estudar $\mathcal{L} \times \Delta$, quando os factores são álgebras quaisquer de divisão sobre $\mathfrak{K}$, sabemos que é condição necessária e suficiente, para que $\mathcal{L} \times \Delta$ seja semi-simples, que seja semi-simples o produto $Z \times Z'$ dos respectivos centros. É o que sucede se um dos centros for ampliação separável finita de $\mathfrak{K}$. Podemos dar o

Teorema 1 :- O produto directo de duas álgebras de divisão sobre $\mathfrak{K}$ é uma álgebra semi-simples, se um dos centros dos factores for uma ampliação separável finita de $\mathfrak{K}$. O número de álgebras simples em que, nesse caso, se decompõe o produto, é igual ao número de corpos em que se decompõe o produto dos centros.

É claro que, se $\Delta = \Omega$ for simplesmente um corpo não comutativo de centro $Z' \supseteq \mathfrak{K}$, $\mathcal{L}_\Omega$ será ou não semi-simples (§ 3), conforme $\mathcal{L}_{z'}$ for ou não semi-simples. É, então, válido o

Teorema 2 :- Se $\mathcal{L}$ é uma álgebra de divisão sobre $\mathfrak{K}$ e se Ω é um corpo não comutativo de centro $Z' \supseteq \mathfrak{K}$, é condição necessária e suficiente, para que $\mathcal{L}_\Omega$ seja semi-simples, que seja semi-simples o seu centro $Z_{z'}$ (Z = centro de $\mathcal{L}$).

Admitamos que $\mathcal{L}$ e Δ são álgebras normais de divisão. O seu produto é uma álgebra normal simples. Um teorema mais preciso é obtido, quando $\Delta = \mathcal{L}^{-1}$. Vimos no Cap. anterior que $\mathcal{L} \times \mathcal{L}^{-1}$ é, então, uma álgebra completa de matrizes.

Passemos agora ao produto directo $\mathcal{U}\times\Omega$, em que $\mathcal{U}$ é uma álgebra simples e Ω uma álgebra de divisão sobre $\mathfrak{K}$. Tem-se $\mathcal{U}\times\Omega=\mathfrak{K}_r\times\mathcal{L}\times\Omega$. Se o produto $Z\times Z'$ dos centros de $\mathcal{U}$ e de Ω for semi-simples (como sucede se um dos centros for uma ampliação separável de $\mathfrak{K}$), $\mathcal{L}\times\Omega$ é semi-simples e pode escrever-se

$$\mathcal{L}\times\Omega = \Phi'_{r'} + \Phi''_{r''} + \cdots,$$

onde Φ', Φ'', ... são álgebras de divisão sobre $\mathfrak{K}$. Nessas condições, tem-se

$$\mathcal{U}\times\Omega = (\Phi'_{r'} + \Phi''_{r''} + \cdots)\times\mathfrak{K}_r = \Phi'\times\mathfrak{K}_r\times\mathfrak{K}_r + \Phi''\times\mathfrak{K}_{r''}\times\mathfrak{K}_r + \cdots =$$

$$= \Phi'\times\mathfrak{K}_{rr'} + \Phi''\times\mathfrak{K}_{rr''} + \cdots = \Phi'_{rr'} + \Phi''_{rr''} + \cdots .$$

É válido o

Teorema 3 :- O produto directo $\mathcal{U}\times\Omega$ duma álgebra simples $\mathcal{U}=\mathfrak{K}_r\times\mathcal{L}$ e duma álgebra de divisão Ω sobre $\mathfrak{K}$ é uma álgebra semi-simples, soma de tantos anéis de matrizes quantos os da decomposição da álgebra semi-simples $\mathcal{L}\times\Omega$, pressuposto que o produto dos centros Z e Z', de $\mathcal{L}$ e Ω, é uma álgebra semi-simples. Os graus das matrizes das álgebras simples em que se decompõe $\mathcal{U}\times\Omega$ obtêm-se fazendo os produtos de r pelos graus das matrizes das álgebras simples em que se decompõe $\mathcal{L}\times\Omega$.

Corolário 1 :- O produto directo duma álgebra normal simples $\mathcal{U}=\mathcal{L}_r$ por uma álgebra de divisão Ω, sobre $\mathfrak{K}$, é uma álgebra simples Σ_{rs}, se $\Sigma_s=\mathcal{L}\times\Omega$.

Os teoremas 2 e 3 do § 6 (relativos a ampliações de algebras normais simples) e os teoremas 11 e 12 do § 5 (relativos a ampliações de álgebras semi-simples) são os resultados essenciais obtidos até aqui sobre a teoria das ampliações das álgebras simples (ou semi-simples). No § que vai seguir-se, serão estabelecidos os mesmos resultados por uma via diferente, que apenas utiliza de todo este Capítulo os teoremas 1 a 3 do já citado § 5[1]

(1) Cfr. A.Albert, "Structure of algebras", pgs.42 a 45.

8) Outro modo de estabelecer certas proposições relativas às ampliações das álgebras simples. Comecemos por certos esclarecimentos preliminares. Seja $\mathcal{M}$ uma álgebra completa de matrizes. Se a cada matriz $A\in\mathcal{M}$ fizermos corresponder a matriz transposta $A'\in\mathcal{M}$, a correspondência obtida é um isomorfismo operatório inverso:

$$AB \to (AB)' = B'A', \qquad kA \to kA', \qquad (k\in\mathfrak{K}).$$

A álgebra $\mathcal{M}$ é, assim, recíproca de si mesma. Em segundo lugar, tomemos uma álgebra normal $\mathcal{G}$. Na passagem desta para a sua recíproca $\mathcal{G}^{-1}$, os elementos do centro ficam em correspondência biunívoca. O centro da segunda será um corpo, precisamente o corpo fundamental da 1ª. A 2ª álgebra é também normal. Por último, observe-se que a recíproca duma álgebra simples é uma álgebra simples.

Posto isto, seja $\mathcal{U}$ uma álgebra normal simples. Ponhamos $\mathcal{U}=\mathcal{U}'\times\mathcal{L}$. Será $\mathcal{U}^{-1}=\mathcal{U}'^{-1}\times\mathcal{L}^{-1}$. Visto que $\mathcal{U}'$ é álgebra completa de matrizes, o mesmo se diz de $\mathcal{U}'^{-1}=\mathcal{U}'=\mathfrak{K}_r$. Escrevendo $\mathcal{U}\times\mathcal{U}^{-1}=\mathcal{U}'\times\mathcal{U}'^{-1}\times(\mathcal{L}\times\mathcal{L}^{-1})$, como $\mathcal{L}$ e $\mathcal{L}^{-1}$ são álgebras normais de divisão sobre $\mathfrak{K}$, o seu produto é uma álgebra completa de matrizes com elementos de $\mathfrak{K}$, de modo que $\mathcal{U}\times\mathcal{U}^{-1}$ é o produto de tres álgebras completas de matrizes com elementos de $\mathfrak{K}$, e pode enunciar-se o seguinte

Teorema 1 :- O produto duma álgebra normal simples pela sua recíproca é uma álgebra completa de matrizes.

Lema 1 :- Se na igualdade $\mathcal{G}=\mathcal{G}_1\times\mathcal{G}_2$, $\mathcal{G}$ é uma álgebra simples e os factores são sub-álgebras de $\mathcal{G}$, ambos esses factores são sub-álgebras simples. Se existisse um ideal bilateral próprio de $\mathcal{G}_1$, representado por $\mathfrak{a}'_1$, seria

$$\mathfrak{a}'_1\,\mathcal{G}_2\cdot\mathcal{G} = \mathfrak{a}'_1\,\mathcal{G}_2\cdot\mathcal{G}_1\mathcal{G}_2 = \mathfrak{a}'_1\,\mathcal{G}_1\mathcal{G}_2^2 \subseteq \mathfrak{a}'_1\mathcal{G}_2 \subset \mathcal{G},$$

$$\mathcal{G}\cdot\mathfrak{a}'_1\,\mathcal{G}_2 = \mathcal{G}_1\mathcal{G}_2\cdot\mathfrak{a}'_1\,\mathcal{G}_2 = \mathcal{G}_1\mathfrak{a}'_1\,\mathcal{G}_2^2 \subseteq \mathfrak{a}'_1\mathcal{G}_2 \subset \mathcal{G},$$

de sorte que $\mathfrak{a}'_1\,\mathcal{G}_2$ seria igualmente um ideal bilateral pró-

prio de $\mathcal{B}$, contra a hipótese.

Teorema 2 :- Supondo $\mathcal{B} = \mathcal{B}_1 \times \mathcal{B}_2$, $\mathcal{B}$ uma álgebra normal simples e os factores sub-álgebras de $\mathcal{B}$, cada factor é uma álgebra normal simples.

O centro de $\mathcal{B}_2$, com efeito, por estar contido no centro de $\mathcal{B}$ mostra que $\mathcal{B}_2$ é normal. $\mathcal{B}_1$ é também normal. O lema diz-nos agora que cada sub-álgebra factor é simples.

Posto isto, seja $\mathcal{A}$ uma álgebra normal simples sobre $\mathcal{K}$. Pondo

$$\mathcal{A} \times \mathcal{A}^{-1} = \mathcal{K}_t, \qquad (\mathcal{A} \times \mathcal{A}^{-1})_\Delta = \mathcal{A}_\Delta \times \mathcal{A}_\Delta^{-1} = \Delta_t,$$

o teorema anterior, visto que Δ_t é normal simples sobre Δ, mostra que $\mathcal{A}_\Delta$ é normal simples sobre Δ, qualquer que seja Δ (1ª parte do teorema 3 do § 6). Pode dar-se o seguinte enunciado:

Teorema 3 :- É condição necessária e suficiente, para que $\mathcal{B}$ seja uma álgebra normal simples sobre $\mathcal{K}$, que $\mathcal{B}_\Delta$ seja normal simples sobre Δ, qualquer que seja a ampliação comutativa Δ do corpo fundamental.

A 2ª parte do teorema 3 do § 6, no que toca à afirmação de ser uma álgebra quadrada toda a álgebra normal simples, será substituida pelo seguinte

Teorema 4 :- É condição necessária e suficiente, para que $\mathcal{B}$ seja normal simples (sobre $\mathcal{K}$), que haja uma ampliação finita Δ, de $\mathcal{K}$, tal que $\mathcal{B}_\Delta$ seja álgebra completa de matrizes (com elementos de Δ). Se existe a ampliação finita Δ indicada, $\mathcal{B}_\Delta$ tem um centro isomorfo de Δ. Diremos que Δ é o centro de $\mathcal{B}_\Delta$. A ordem do centro de $\mathcal{B}$ relativamente a $\mathcal{K}$ é a unidade. $\mathcal{B}$ será uma álgebra normal. Um ideal bilateral $\neq (0)$ de $\mathcal{B}$, $\mathfrak{a}$ por ex., leva a um ideal bilateral $\neq (0)$, $\mathfrak{a}_\Delta$, de $\mathcal{B}_\Delta$, que é uma álgebra sobre Δ da mesma ordem da álgebra $\mathfrak{a}$ sobre $\mathcal{K}$. A ordem de $\mathfrak{a}$ será, assim, a ordem de $\mathcal{B}$, e tem-se $\mathfrak{a} = \mathcal{B}$, como se quer. Da inversa podemos dar a demonstração que vai ver-se. Seja $\mathcal{B}$ normal e simples. Se é de 1ª ordem, o teorema é evidente. No caso contrário, suponhamos que $\mathcal{B}$ não é álgebra

de divisão e admitamos o teorema para as álgebras de ordem inferior à de $\mathcal{B}$. Vamos ver que o teorema é verdadeiro para $\mathcal{B}$. Escrevendo $\mathcal{B} = \mathcal{A}_1 \times \mathcal{L}$, a álgebra de divisão $\mathcal{L}$ é de ordem inferior à de $\mathcal{B}$, pois que $\mathcal{A}_1$ não pode ser de 1ª ordem. Então, existe uma ampliação finita Δ, de $\mathcal{K}$, tal que $\mathcal{L}_\Delta$ é uma álgebra completa de matrizes. A igualdade $\mathcal{B}_\Delta = \Delta_1 \times \mathcal{L}_\Delta$ mostra que $\mathcal{B}_\Delta$ é igualmente uma álgebra completa de matrizes com elementos de Δ. Se $\mathcal{B}$ é a álgebra de divisão, sabemos do Cap. anterior que a álgebra $\mathcal{B}_\mathcal{P}$, onde $\mathcal{P}$ resulta de $\mathcal{K}$ por adjunção duma raiz dum polinómio irredutível em $\mathcal{K}$ a que satisfaz um elemento de $\mathcal{B}$ não pertencente a $\mathcal{K}$, não é uma álgebra de divisão. Nesse caso, $\mathcal{B}_\mathcal{P}$ está nas condições das álgebras já tratadas, o mesmo se dizendo de $\mathcal{B}$.

Vamos passar agora ao teorema 12 do § 5. Se nos recordarmos do teorema 1 e do corolário 1 do mesmo §, podemos dizer que um corpo separável, de grau n sobre $\mathcal{K}$, constitui o exemplo mais simples nas condições do teorema. Dum modo geral, tomemos uma álgebra semi-simples $\mathcal{B}$. Se o seu centro $\mathcal{Z}$ for uma álgebra separável, considerando as igualdades

$$\mathcal{B} = \mathcal{B}_1 + \cdots + \mathcal{B}_s, \qquad \mathcal{Z} = \mathcal{Z}_1 + \cdots + \mathcal{Z}_s,$$

sabemos que os $\mathcal{Z}_i$ se podem supor ampliações separáveis de $\mathcal{K}$. Seja, então, $\mathcal{Z}_i = \mathcal{K}(\lambda_i)$, onde λ_i satisfaz à equação irredutível separável $\varphi_i(x) = 0$, com coeficientes de $\mathcal{K}$. Se φ_i tiver o grau t e $\mathcal{M}$ for o seu corpo de decomposição, tem-se

$$Z = (\mathcal{Z}_i)_n = \mathcal{M}e_1 + \cdots + \mathcal{M}e_t, \qquad \mathcal{A} = (\mathcal{B}_i)_n = \mathcal{A}e_1 + \cdots + \mathcal{A}e_t, \quad (12)$$

como se viu no teorema 2 do § 5. $\mathcal{A}e_j$, por ex., é uma álgebra contida em $\mathcal{A}$ (não devemos esquecer que os e_i são elementos do centro Z, de $\mathcal{A}$), de corpo fundamental $\mathcal{M}$. O seu centro é $\mathcal{M}e_j$, pois que, dada a decomposição (12), de $\mathcal{A}$, há uma decomposição correspondente do centro Z em parcelas como $[\mathcal{A}e_j, Z] =$ = centro de $\mathcal{A}e_j$. No estudo de $\mathcal{A}e_j$ como álgebra sobre $\mathcal{M}$, aparece a mesma como ampliação duma álgebra $\mathcal{B}_i^{(j)}$, sobre $\mathcal{K}(\lambda_j)$, álgebra que é isomorfa da álgebra $\mathcal{B}_i$ sobre $\mathcal{Z}_i = \mathcal{K}(\lambda_i)$. Isto significa que $\mathcal{B}_i^{(j)}$ é normal simples sobre $\mathcal{K}(\lambda_j)$, permanecendo normal e simples ao passar-se de $\mathcal{K}(\lambda_j)$ para $\mathcal{M}$, ou seja ao

passar-se para $(\mathfrak{F}_i^{(j)})_n = \mathcal{A}e_j$. Podemos encontrar uma ampliação finita Σ_j, de $\mathcal{K}$ (e, portanto, de $\mathcal{A}$) que torna $\mathcal{A}e_j$ num anel completo de matrizes com elementos de Σ_j. Existirá uma ampliação finita $\mathcal{L}_j$, de $\mathcal{L}$, que torna $\mathfrak{F}_{jt}$ numa soma de anéis de matrizes, e uma ampliação finita $\mathcal{L}$, de $\mathcal{A}$, gosando da mesma propriedade quanto a $\mathfrak{F}_{\mathcal{A}\mathcal{L}}$. $\mathfrak{F}$ é uma álgebra sem radical, para a qual $\mathfrak{F}_\Delta$ não tem radical, qualquer que seja Δ, como se verifica recorrendo a um corpo Ψ, que contenha Δ e $\mathcal{L}$, e considerando a álgebra $\mathfrak{F}_\Psi$.

É válido, pois, o

Teorema 5 :- É condição necessária e suficiente, para que a álgebra semi-simples $\mathfrak{F}$ seja separável, que seja separável o seu centro $\mathfrak{Z}$.

Exemplos de álgebras separáveis são fornecidos pelas álgebras que podem tornar-se diagonais (e conter, pois, tantos idempotentes ortogonais dois a dois quantos a ordem da álgebra). Já o vimos, quanto às ampliações separáveis finitas de $\mathcal{A}$. Dum modo mais geral, se, dada a álgebra, de ordem n sobre $\mathcal{A}$, se tem, para $\Delta \supseteq \mathcal{A}$,

$$\mathcal{A}_\Delta = \mathfrak{F}_\Delta = \Delta e_1 + \cdots + \Delta e_n, \qquad (e_i e_k = 0, \quad e_i^2 = e_i),$$

$\mathcal{A}$ é separável. Com efeito, $\mathfrak{F}_\Delta$, como soma de corpos, não tem radical. Logo, $\mathcal{A}$ não tem radical. Se Σ for uma ampliação qualquer de $\mathcal{A}$, verifica-se que $\mathcal{A}_\Sigma$ não tem radical, recorrendo a $\mathcal{A}_\Psi$, onde o corpo Ψ contém Δ e Σ. Podemos dar o seguinte enunciado:

Teorema 6 :- É condição suficiente, para que uma álgebra seja separável, que possa tornar-se numa álgebra diagonal para uma ampliação do corpo fundamental.

Uma álgebra diagonal é sempre comutativa. Se a álgebra $\mathcal{A}$ que pode tornar-se diagonal for um corpo comutativo $\mathcal{L}$, ampliação finita de $\mathcal{A}$, o teorema anterior é substituido por este outro:

Teorema 7 :- É condição necessária e suficiente para que $\mathcal{L}$ seja uma ampliação separável de $\mathcal{A}$, que $\mathcal{L}$ leve a uma álgebra diagonal.

Do teorema 6 não existe, porém, inverso. É válido, com efeito, o seguinte

Teorema 8 :- É condição necessária e suficiente, para que uma álgebra $\mathcal{A}$, sobre $\mathcal{K}$, tenha uma álgebra ampliada diagonal $\mathcal{A}_\Delta$, que $\mathcal{A}$ seja uma soma directa de corpos separáveis, isomorfos de ampliações separáveis de $\mathcal{K}$. Não esqueçamos, com efeito, que, se um corpo $\mathcal{L}$ é ampliação inseparável finita de $\mathcal{K}$, há ampliações $\mathcal{L}_\Delta$ que têm radical.

Dada uma álgebra $\mathfrak{F}$, sobre $\mathcal{K}$, se existir uma ampliação $\Delta \supseteq \mathcal{K}$ tal que $\mathfrak{F}_\Delta$ seja uma soma de anéis completos de matrizes com elementos de corpos isomorfos de Δ, este diz-se um corpo de decomposição de $\mathfrak{F}$. Uma álgebra normal simples, por ex., tem sempre um corpo de decomposição, ampliação finita do corpo fundamental. Pode enunciar-se este

Teorema 9 :- É condição necessária e suficiente, para a existência dum corpo de decomposição Δ, de $\mathfrak{F}$, que $\mathfrak{F}$ seja separável. De facto, as considerações que precederam o teorema 5 provam que a condição é suficiente. É imediato que ela é necessária. Convém observar que este teorema também poderia ser enunciado logo no final do § 6. A demonstração a fazer seria a que vem a seguir. Se $\mathfrak{F}$ é separável, os $\mathfrak{F}_{jt}$ (parcelas simples) são separáveis. Pondo $\mathfrak{F}_{jt} = \mathcal{K}_{jt} \times \mathcal{L}$, como o centro de $\mathfrak{F}_{jt}$ é o centro de $\mathcal{L}$, segue-se que esta última é uma álgebra de divisão de centro separável $\mathfrak{Z}_t$. Qualquer que seja o modo como se amplia $\mathcal{K}$, $(\mathfrak{Z}_t)_\Delta$ é semi-simples, o mesmo se dizendo de $\mathcal{L}_\Delta$ e de $(\mathfrak{F}_{jt})_\Delta$. Se Δ é tal que $(\mathfrak{Z}_t)_\Delta$ é soma de corpos isomorfos de Δ, cada parcela de $(\mathfrak{F}_{jt})_\Delta$, que admite um desses corpos como centro, pode considerar-se normal e simples sobre Δ.

Os raciocínios feitos implicam o seguinte

Teorema 10 :- Se existe um corpo de decomposição duma álgebra, existe um corpo de decomposição que é uma ampliação finita do corpo fundamental. (Revejam-se as considerações que acabaram de introduzir o corpo Δ, na demonstração do teorema 9, corpo que pode supor-se ampliação finita de $\mathcal{K}$, ou retomem-se as reflexões que se fizeram para estabelecer o teorema 5).

Seja $\mathcal{A}$ uma álgebra separável e sejam Δ e Δ' dois corpos de decomposição. Um corpo Ψ que contenha Δ e Δ' é também um corpo de decomposição. O número de parcelas simples em que se decompõe $\mathcal{A}_\Psi$ é o número de parcelas simples em que se decompõem $\mathcal{A}_\Delta$ e $\mathcal{A}_{\Delta'}$. Por isso diremos:

Teorema 11 :- O número de anéis completos de matrizes em que se decompõe uma álgebra separável, quando o corpo fundamental se amplia para um corpo de decomposição, é independente deste último corpo. Pode precisar-se quanto ao citado número. Se Δ é um corpo de decomposição de $\mathcal{F}$, é corpo de decomposição de $\mathcal{F}_{\mathcal{Z}_l}$. O centro $\mathcal{Z}_l$ amplia-se para $(\mathcal{Z}_l)_\Delta$, passando a ser uma soma de corpos comutativos isomorfos de Δ. O número de parcelas da decomposição de $\mathcal{F}$ é igual ao número destes corpos, e, portanto, igual à soma dos graus $(\mathcal{Z}_l/\mathcal{K})$, visto que os $\mathcal{Z}_l$ são ampliações separáveis de $\mathcal{K}$ e $(\mathcal{Z}_l)_\Delta$ atingiu o número máximo de corpos em que pode vir a decompor-se uma ampliação de $\mathcal{Z}_l$. Assim, diremos:

Teorema 12 :- O número de álgebras simples (anéis completos de matrizes) do teorema 11 é igual à soma dos graus $(\mathcal{Z}_l/\mathcal{K})$ dos centros dos $\mathcal{F}_{\mathcal{Z}_l}$.

REPRESENTAÇÕES

Capítulo VIII

Representações de anéis

1) Definição de anéis de representação e de módulos de representação - Seja $\mathcal{K}$ um enel com elemento um (mais frequentemente um corpo) e formemos um anel $\mathcal{A}$ de matrizes quadradas do grau n com elementos de $\mathcal{K}$. Diz-se, dum modo geral, que, dado um anel $\mathcal{R}$, se tem uma representação directa do grau n, de $\mathcal{R}$, por meio de $\mathcal{A}$ (ou em $\mathcal{K}$), se houver um homomorfismo anular $\mathcal{R} \sim \mathcal{A}$. Se $\mathcal{R}$ é um sistema hiper-complexo $\mathcal{F}$, de corpo fundamental $\mathcal{P}$, o homomorfismo anular $\mathcal{F} \sim \mathcal{A}$ toma-se como um homomorfismo operatório, segundo o qual, se $a \in \mathcal{F}$ tem $A \in \mathcal{A}$ como correspondente, $a\rho$, com $\rho \in \mathcal{P}$, tem como correspondente a matriz $A\rho \in \mathcal{A}$.

Pode dar-se também uma definição geral de representação recíproca. Consideremos um anel $\mathcal{R} = \{a, b, \ldots\}$ e um segundo anel $\mathcal{R}' = \{a', b', \ldots\}$, em correspondência biunívoca, $a \rightarrow a'$, com o primeiro. Se tiverem lugar em $\mathcal{R}'$ as seguintes regras de soma e de produto

$$a' + b' = (a + b)', \qquad a'b' = (ba)',$$

diz-se que $\mathcal{R}'$ é isomorfo inverso ou anti-isomorfo de $\mathcal{R}$ (tomo I, pgs. 148). Quando $\mathcal{R}$ é um corpo, $\mathcal{R}'$ é igualmente um corpo.

Posto isto, tomemos um anel de matrizes $\mathcal{A} = \{A, B, \ldots\}$, no qual os elementos de $A, \ldots$ pertencem a $\mathcal{R}$. Se tomarmos o anel $\mathcal{A}' = \{A', B', \ldots\}$, de matrizes com elementos correspondentes de $\mathcal{R}'$, e, em seguida, o anel $\tilde{\mathcal{A}}' = \{\tilde{A}', \tilde{B}', \ldots\}$, das matrizes transpostas de $A', \ldots$, verifica-se que $\mathcal{A}$ e $\tilde{\mathcal{A}}'$ são anti-isomorfos. Se $\mathcal{A}$ é uma representação dum anel $\mathcal{T} = \{\alpha, \beta, \ldots\}$ (é sempre a sua própria representação), $\tilde{\mathcal{A}}'$ diz-se uma representação recíproca do mesmo anel. Têm lugar as seguintes correspondências, características duma representação recíproca:

$$\alpha \rightarrow \tilde{A}', \qquad \beta \rightarrow \tilde{B}', \qquad \alpha + \beta \rightarrow \tilde{A}' + \tilde{B}', \qquad \alpha\beta \rightarrow \tilde{B}'\tilde{A}'.$$

Quando se trata de reprosentações de sistemas hiper-com-

plexos, torna-se necessário, por definição, dar sentido ao símbolo $A\rho$. Esse facto exige que os elementos de $\mathcal{P}$ operem sobre $\mathfrak{A}$. Supor-se-á, por isso, estar $\mathcal{P}$ (que é comutativo) no centro de $\mathfrak{A}$.

Uma representação do grau n dum grupo $\mathcal{G}$ é um homomorfismo $\mathcal{G} \sim \mathcal{H}$ entre dois grupos, no qual o grupo $\mathcal{H}$ é constituido por elementos que são matrizes do grau n com elementos de $\mathfrak{A}$.

Diz-se módulo de representação de $\mathcal{G}$ com respeito a $\mathfrak{A}$ um módulo duplo $\mathfrak{M}$, relativo a $\mathcal{G}$ e $\mathfrak{A}$, finito (de ordem n) relativamente a $\mathfrak{A}$, sobre o qual $\mathcal{G}$ opera à esquerda e $\mathfrak{A}$ à direita, de tal modo que vale a lei associativa

$$a.m\,\lambda = am.\lambda\,, \qquad (a\in\mathcal{G},\ m\in\mathfrak{M},\lambda\in\mathfrak{A}).$$

Esta última condição exprime que os operadores a induzem transformações lineares (endomorfismos operatórios) no módulo $\mathfrak{M}$.

Seja $(u_1,\dots,u_n)$ uma base de $\mathfrak{M}$. A aplicação de a ao elemento u_l leva a

$$a\,u_l = \sum_j u_j \alpha_{jl}\,, \qquad (\alpha_{jl}\in\mathfrak{A}). \tag{1}$$

Se é $v = \sum u_l \alpha_l$ um elemento qualquer de $\mathfrak{M}$, tem-se

$$a\,v = \sum_l a(u_l\alpha_l) = \sum_l a\,u_l.\alpha_l = \sum_{l,j} u_j \alpha_{jl}\,\alpha_l\,. \tag{2}$$

A cada elemento a se faz corresponder, pois, uma matriz $A=(\alpha_{jl})$. Se $b\in\mathcal{G}$, tem-se

$$(a+b)u_l = a\,u_l + b\,u_l = \sum u_j(\alpha_{jl}+\beta_{jl})\,,$$

$$a.b.u_l = a.b\,u_l = \sum_j a(u_j\beta_{jl}) = \sum_{j,k} u_k\alpha_{kj}\beta_{jl} = \sum_k u_k\Big(\sum_j \alpha_{kj}\beta_{jl}\Big).$$

As matrizes A constituem, como se vê, um anel de representação do anel $\mathcal{G}$. Inversamente, partamos duma representação $\mathcal{G}\sim\mathcal{C}$ e construamos um módulo $\mathfrak{M}(u_1,\dots,u_n)$ com respeito a $\mathfrak{A}$. Visto

que a cada elemento $a\in\mathcal{G}$ corresponde uma matriz A, em $\mathcal{C}$, façamos operar $\mathcal{G}$, sobre $\mathfrak{M}$, segundo as leis

$$a\,u_l = \sum_j u_j\alpha_{jl}\,, \qquad a.\sum_l u_l\lambda_l = \sum_l a\,u_l.\lambda_l\,, \qquad (\lambda_l\in\mathfrak{A})\,.$$

Vê-se fàcilmente que $\mathfrak{M}$ passa a ser um módulo relativamente a $\mathcal{G}$ e que é um módulo de representação. De facto,

$$a(v+w) = av + aw\,, \qquad a.v\lambda = av.\lambda\,, \qquad (v,w\in\mathfrak{M}),$$

$$(a+b)u_l = \sum_j u_j(\alpha_{jl}+\beta_{jl}) = au_l + bu_l\,,$$

$$ab.u_l = \sum_k u_k . \sum_j \alpha_{kj}\beta_{jl} = \sum_j \Big(\sum_k u_k\alpha_{kj}\Big)\beta_{jl} =$$

$$= \sum_j au_j.\beta_{jl} = a.\sum_j u_j\beta_{jl} = a.bu_l\,.$$

Do exposto resulta o seguinte

Teorema:- A todo o módulo de representação e a uma dada base do mesmo corresponde uma representação, e, inversamente, toda a representação pertence a um módulo de representação.

A primeira representação regular dum sistema $\mathcal{E}$, referida no Cap. anterior, foi obtida a partir do módulo de representação constituido pelo próprio $\mathcal{E}$.

Diz-se módulo recíproco de representação de $\mathcal{G}$ com respeito a $\mathfrak{A}$ um módulo duplo $\mathfrak{M}'$, relativo a $\mathcal{G}$ e $\mathfrak{A}$, finito (de ordem n) relativamente a $\mathfrak{A}$, sobre o qual $\mathcal{G}$ e $\mathfrak{A}$ operam simultâneamente à esquerda, de tal modo que vale (lei de troca)

$$a.\lambda m = \lambda.am\,.^{(1)}$$

Se for $(u_1,\dots,u_n)$ uma base de $\mathfrak{M}'$, põe-se

(1) Os elementos de $\mathcal{G}$ definem ainda endomorfismos operatórios (relativamente a $\mathfrak{A}$) em $\mathfrak{M}$.

$$a\,u_i = \sum_j a_{ij} u_j, \qquad (a_{ij} \in \mathfrak{A}).$$

Vê-se, então, que se tem

$$ab.u_i = a.bu_i = a.\sum_k b_{ik} u_k = \sum_k b_{ik}\left(\sum_j a_{kj} u_j\right) =$$

$$= \sum_j \left(\sum_k b_{ik} a_{kj}\right) u_j \ .$$

As matrizes $A = (a_{ij})$, correspondentes dos elementos $\underline{a}$, determinam, como se vê, uma representação recíproca de $\mathcal{Y}$.

Inversamente, partamos duma representação recíproca de $\mathcal{Y}$ e construamos um módulo $\mathfrak{M}(u_1, \ldots, u_n)$ com respeito a $\mathfrak{A}$. Visto que a cada elemento $a \in \mathcal{Y}$ corresponde uma matriz $\underline{A}$, façamos operar $\mathcal{Y}$ segundo as leis

$$a\,u_i = \sum_j a_{ij} u_j \ , \qquad a.\sum_i \lambda_i u_i = \sum_i \lambda_i . a u_i , \qquad \left(A = (a_{ij})\right).$$

Vê-se que $\mathfrak{M}$ passa a ser módulo recíproco de representação de $\mathcal{Y}$. Vale, com efeito, a lei de troca, e tem-se, sucessivamente:

$$ab.u_i = \sum_k \left(\sum_j b_{ij} a_{jk}\right) u_k ,$$

$$a.bu_i = a \sum_j b_{ij} u_j = \sum_j b_{ij} . a u_j = \sum_{j,k} b_{ij} a_{jk} u_k ,$$

$$ab.u_i = a.bu_i \ .$$

Uma representação directa diz-se fiel, quando o homomorfismo $\mathcal{Y} \sim \mathcal{O}$ se torna num isomorfismo.

À semelhança do que já se disse para os sistemas hiper-complexos, as noções de representação e de módulo de representação podem estender-se a anéis $\mathcal{Y}$ que admitem um domínio

operatório comutativo $\mathcal{O}$[1], precisamente sob a condição de se tomar o homomorfismo anular $\mathcal{Y} \sim \mathcal{O}$ como operatório relativamente a $\mathcal{O}$. Então, se $\underline{A}$ corresponde a $a \in \mathcal{Y}$, a ρ, com $\rho \in \mathcal{O}$, deverá ter $A\rho$ como correspondente. É necessário admitir que os elementos de $\mathcal{O}$ operam sobre $\mathfrak{A}$. Supõe-se, por isso, $\mathcal{O} \equiv \mathfrak{A}$. No tocante a um módulo $\mathfrak{M}$ de representação, ter-se-á $a\rho.v = av.\rho$. Como é $\rho \in \mathfrak{A}$, deverá ser também $a.v\rho = av.\rho$, pelo que valerá a sucessão de igualdades

$$a.v\rho = av.\rho = a\rho.v \ .$$

Numa representação recíproca, a sucessão anterior será substituida pela seguinte:

$$a.\rho v = \rho.av = a\rho.v \ .$$

2) Representações equivalentes - Efectuemos, num módulo $\mathfrak{M}$ de representação, a mudança de base $(u'_1, \ldots, u'_n) = (u_1, \ldots, u_n).P$, na qual $\underline{P}$ é a matriz quadrada da transformação. Ao elemento $\underline{a}$ corresponderá agora a matriz $A_1 = P^{-1}AP$, em vez de A, como se vê imediatamente. Se se tratar do módulo recíproco $\mathfrak{M}'$, a matriz $\underline{A}$ é substituida por PAP^{-1}, pois tem lugar o seguinte conjunto de igualdades:

---

(1) O método que vamos seguir, como já foi assinalado (veja-se o prefácio do tomo I), é devido a E.Noether, que o deu na sua memória "Hyperkomplexe Grössen und Darstellungstheorie". Nos livros "Algebren", Cap.III, de M.Deuring, e "Moderne Algebra", II Teil, Cap.XVII, de van der Waerden, é exposto também o processo de E.Noether. No trabalho desta última autora "Nichtkommutative Algebra", já referido igualmente (Cap.VII deste tomo), encontram-se, de pgs.517 à 523, as ideias centrais da teoria das representações (directas e recíprocas) que vai ser tratada e assenta sobre o estudo dos endomorfismos dum grupo abeliano aditivo. Dedicaremos um certo número de parágrafos (desde o próximo § 3 até voltarmos pròpriamente às representações) à exposição detalhada dessas ideias.

$$u'_i = \sum_j p_{ij} u_j \ ,$$

$$a\,u'_i = \sum_j p_{ij} \cdot a u_j = \sum_{j,R} p_{ij} a_{jR} u_R = \sum_{j,R,\ell} p_{ij} a_{jR} p^{-1}_{R\ell}\, u'_\ell =$$

$$= \sum_\ell \Big(\sum_{j,R} p_{ij} a_{jR} p^{-1}_{R\ell} \Big) u'_\ell \ , \qquad \Big((P^{-1} = (p^{-1}_{R\ell})) \Big) .$$

Sempre que as matrizes de duas representações estão ligadas por qualquer das relações dadas (em que P é uma matriz fixa), as representações dizem-se equivalentes ou pertencentes à mesma classe de representação. Um módulo de representação conduz a uma dada classe. Vamos demonstrar o seguinte

Teorema:- Se dois módulos de representação geram representações equivalentes, são isomorfos, no duplo sentido operatório. Designemos com $\mathfrak{M}(u_1,\ldots,u_n)$ e $\mathfrak{N}(v_1,\ldots,v_n)$ os módulos em questão. Façamos no primeiro uma mudança de base, por forma que as matrizes de representação passem a ser as mesmas que no segundo. A correspondência

$$u'_i \rightleftarrows v_i \ , \quad \sum u'_i \alpha_i \rightarrow \sum v_i \alpha_i \ , \qquad (\alpha_i \in \mathfrak{k}) \ ,$$

define o isomorfismo do enunciado. O facto é evidente, pelo que respeita a $\mathfrak{k}$. No tocante a $\mathfrak{Y}$, seja $a \in \mathfrak{Y}$. Sendo

$$a\,u'_i = \sum u'_j \alpha_{ji} \ , \qquad a\,v_i = \sum v_j \alpha_{ji} \ ,$$

vê-se que $a\,u'_i \rightleftarrows a\,v_i$.

O teorema inverso tem também lugar. Para o demonstrar, façamos uma observação. Sejam $\mathfrak{M}$ e $\mathfrak{N}$ os dois módulos de representação, isomorfos no duplo sentido operatório. Designando com $V_1,\ldots,V_n$ os correspondentes, em $\mathfrak{N}$, dos vectores fundamentais u_i, podemos tomar os V_i como base de $\mathfrak{N}$ (que é módulo finito relativamente a $\mathfrak{k}$). Para cada $a \in \mathfrak{Y}$, é, depois,

$$a\,u_i = \sum_j u_j \alpha_{ji} \ , \qquad a\,V_i = \sum_j V_j \alpha'_{ji} .$$

Por hipótese, $a u_i$ tem $a V_i$ como correspondente e $\sum u_j \alpha_{ji}$ tem o correspondente $\sum V_j \alpha_{ji}$. Será como se quer, $(\alpha_{ji}) = (\alpha'_{ji})$.

3) Os anéis $\mathcal{O}$ e $\mathcal{O}'$ - Vamos reentrar na teoria dos endomorfismos dum grupo abeliano $\mathfrak{M}$. O conjunto dos endomorfismos constitui um anel.(1) Se $\sigma, \tau, \ldots$ representam endomorfismos e m, $m', \ldots$ elementos de $\mathfrak{M}$, tem-se $m \rightarrow m\sigma$, $(m+m')\sigma \rightarrow m\sigma + m'\sigma$. No referido conjunto, que pode designar-se por absoluto dos endomorfismos,(2) define-se um produto segundo a lei $m(\sigma\tau) = (m\sigma)\tau$. Tira-se daqui que o símbolo $\sigma\tau$ significa dever efectuar-se primeiramente σ depois τ. Se imaginarmos a hipótese contrária, será mais conveniente escrever $(\sigma\tau)m = \sigma(\tau m)$. A fim de evitar confusões, utilizaremos os símbolos $\sigma', \tau', \ldots$ para designar os endomorfismos colocados à esquerda dos elementos de $\mathfrak{M}$, de modo que poremos $(\sigma'\tau')m = \sigma'(\tau' m)$. O anel $\mathcal{O}$, dos endomorfismos $\sigma, \tau, \ldots$, pode designar-se por anel dos endomorfismos à direita de $\mathfrak{M}$; e o anel $\mathcal{O}'$, dos endomorfismos $\sigma', \tau', \ldots$, por anel dos endomorfismos à esquerda de $\mathfrak{M}$. $\mathcal{O}$ e $\mathcal{O}'$ são anéis anti-isomorfos.(3)

(1) Veja-se Almeida Costa, "Elementos da Teoria dos Grupos", pgs. 130 e 131.

(2) A terminologia a introduzir concordará com a dos dois §§ anteriores e com a do Cap. VI, utilizada a propósito das representações regulares dum sistema hiper-complexo.

(3) Tratando-se de grupos não comutativos, podem ver-se indicações quanto a endomorfismos nas publicações seguintes: Almeida Costa, "Elementos da Teoria dos Anéis", pgs. 14 a 22; H. Fitting, "Die Theorie der Automorphismenringe Abelscher Gruppen und ihr Analogon bei nichtkommutativen Gruppen", Mathematische Annalen, Band 107, 1932, pgs. 514 a 542; Nathan Jacobson, "The Theory of rings", nº II da colecção Mathematical Surveys da American Mathematical Society, 1943. Nesta última obra desenvolvem-se profundamente os raciocínios que vamos fazer nos §§ próximos, raciocínios que, como dissemos em nota final do § 1, constituem uma exposição detalhada de certas ideias que encontrámos na memória de E. Noether, "Nichtkommutative Algebra".

4) Os módulos redutíveis - Suponhamos $\mathfrak{M}$ uma soma directa da forma

$$\mathfrak{M} = \mathfrak{M}_1 + \cdots + \mathfrak{M}_t . \qquad (3)$$

Dado $m \in \mathfrak{M}$, escrevamos $m = n_1 + \cdots + n_t$, com $n_i \in \mathfrak{M}_i$. A correspondência $m \to n_i$ é um endomorfismo $G_i \in \mathcal{O}$. Pondo $G_i^2 = G_i . G_i$, vê-se imediatamente que G_i é idempotente. Também se verificam as relações $G_i G_j = 0$, se $i \neq j$. O endomorfismo idêntico $U \in \mathcal{O}$ tem a seguinte decomposição: $U = G_1 + \cdots + G_t$. Quanto a $\mathcal{O}$ valem as igualdades

$$\mathcal{O} = G_1\mathcal{O} + \cdots + G_t\mathcal{O} = \mathcal{O}G_1 + \cdots + \mathcal{O}G_t .$$

Uma homomorfia $\mathfrak{M}_i \sim \mathfrak{M}_j$, representada, dum modo geral, por Σ_{ij}, prolonga-se e torna-se num endomorfismo de $\mathfrak{M}$, considerando o símbolo $G_i \Sigma_{ij} = \sigma_{ij}$. Um endomorfismo $\sigma \in \mathcal{O}$ determina sempre t^2 homomorfias σ_{ij}, pois que, por via de σ, se tem, em primeiro lugar,

$$m\sigma = n_1\sigma + \cdots + n_t\sigma , \qquad n_i\sigma = n'_{i1} + \cdots + n'_{it} ,$$

com $n'_{ji} \in \mathfrak{M}_j$. Depois, a correspondência $n_i \to n'_{ji}$ define uma homomorfia Σ_{ij}, de sorte que pode escrever-se, sucessivamente,

$$m\sigma = \sum_i n_i\sigma = \sum_i (mG_i)\sigma = \sum_i m(G_i\sigma) = \sum_{i,j} n'_{ji} = \sum_{i,j} n_i\Sigma_{ij} =$$

$$= \sum_{i,j} (mG_i)\Sigma_{ij} = \sum_{i,j} m\,(G_i\Sigma_{ij}) = \sum_{i,j} m\,\sigma_{ij} = m . \sum_{i,j} \sigma_{ij},$$

e pôr-se

$$\sigma = \sum_{i,j} \sigma_{ij}, \qquad (i,j = 1, 2, \ldots, t). \qquad (4)$$

Em particular, tem-se

$$G_R\sigma = \sum_{i,j} G_R\sigma_{ij} = \sum_{i,j} G_R G_i \Sigma_{ij} = \sum_j G_R \Sigma_{Rj} = \sum_j \sigma_{Rj} .$$

A representação (4), de σ, é unívoca. Inversamente, o 2º membro de (4) define σ. Se pusermos ainda

$$m\sigma = \sum_i n_i\sigma = \sum_{i,j} n_i\sigma_{ij}G_j = \sum_{i,j} m(G_i\sigma G_j),$$

é possível escrever também $\sigma_{ij} = G_i\,\sigma\,G_j$. Os anéis $\mathcal{O}_{ij} = G_i\mathcal{O}G_j$ levam imediatamente, de resto, às somas directas

$$\mathcal{O} = \sum_i G_i\mathcal{O} = \sum_{i,j} G_i\mathcal{O}G_j = \sum_{i,j} \mathcal{O}_{ij},$$

tendo lugar as relações

$$\mathcal{O}_{ij}\,\mathcal{O}_{jl} \cong \mathcal{O}_{il} , \qquad \mathcal{O}_{ij}\,\mathcal{O}_{ki} = 0, \qquad (j \neq k). \qquad (5)$$

De (4) tira-se

$$\sigma + \tau = \sum_{i,j} (\sigma_{ij} + \tau_{ij})$$

$$\theta = \sigma\tau = \sum_{i,j,k,l} \sigma_{ij}\tau_{kl} = \sum_{i,j,l} \sigma_{ij}\tau_{jl} = \sum_{i,l} \theta_{il} , \qquad (\theta_{il} = \sum_j \sigma_{ij}\tau_{jl}).$$

Embora bastante vago, tem lugar o seguinte

Teorema 1 :- O anel $\mathcal{O}$ dos endomorfismos dum módulo, soma directa de t sub-módulos, é uma soma directa de t^2 sub-anéis $\mathcal{O}_{ij}$ (ou um anel de matrizes com elementos dos $\mathcal{O}_{ij}$, sob a condição de cada elemento σ_{ij} da matriz pertencer ao referido $\mathcal{O}_{ij}$).

Imaginemos que, em (3), os $\mathfrak{M}_i$ são todos isomorfos. Representemos por Δ_{ij} o isomorfismo conhecido $\mathfrak{M}_1 \cong \mathfrak{M}_i$. O símbolo Δ_{1i} representará o isomorfismo inverso. Ponhamos $G_1\Delta_{1i} = G_{1i}$, $G_i\Delta_{i1} = G_{i1}$. Tanto os G_{1i} como os G_{i1} pertencem a $\mathcal{O}$, sendo

$$mG_{1i}\,G_{i1} = mG_1\Delta_{1i}G_i\Delta_{i1} = n_1\Delta_{1i}G_i\Delta_{i1} = n'_iG_i\Delta_{i1} = n'_i\Delta_{i1} = n_1 ,$$

se n'_i representa o correspondente de n_1 por via de Δ_{1i}.

Vê-se que é

$$G_{11}\,G_{11} = G_{11} = G_1 .$$

Por definição, poremos

$$G_{ij} = G_{i1}\,G_{1j} .$$

Têm lugar, então, as relações

$$G_{ij}\,G_{j\ell} = G_{i\ell}, \qquad G_{ij}\,G_{k\ell} = 0, \qquad (\text{se } k \neq j).$$

Em $\mathcal{U}$, por consequência, há elemento um e um sistema de t^2 matrizes unidades G_{ij}. $\mathcal{U}$ é um produto directo de Wedderburn, nos termos do § 9 do Cap.I. Pode enunciar-se a proposição a seguir, bastante mais precisa que a anterior:

Teorema 2 :- O anel $\mathcal{U}$ dos endomorfismos dum módulo, soma directa de t sub-módulos isomorfos, é um anel completo de matrizes de grau t com elementos dum sub-anel $\mathcal{Y}$, de $\mathcal{U}$[1] Os elementos de $\mathcal{Y}$ são da forma $T = \sum_i G_{i1}\,\sigma\,G_{1i}$. $\mathcal{Y}$ é isomorfo de $\mathcal{U}_{11} = G_1\mathcal{U}G_1$.

Neste caso as primeiras relações (5) escrevem-se

$$\mathcal{U}_{ij}\mathcal{U}_{j\ell} = G_i\,\mathcal{U}\,G_j\,\mathcal{U}\,G_\ell = \mathcal{U}_{i\ell} ,$$

em virtude de ser $\mathcal{U}\,G_j\,\mathcal{U} = \mathcal{U}$. Esta última igualdade resulta do facto de ser $\mathcal{U}\,G_j\,\mathcal{U}$ um ideal bilateral de $\mathcal{U}$ que contém os elementos da forma $G_{ij}\,G_{jj}\,G_{jk} = G_{ik}$, e contém, portanto $U \in \mathcal{U}$.

(1) O processo de estudo é semelhante ao que foi dado por van der Waerden, de pgs.165 a 169, da 2ª parte da sua "Moderne Algebra", por nós já reproduzido no tomo I, de pgs.140 a 148.

Tenhamos presente que são válidas aqui as igualdades

$$\sigma_{ij} = G_i\,\sigma\,G_j = G_{ij}\,T_{ij}, \qquad T_{ij} = \sum_k G_{ki}\,\sigma\,G_{jk}.$$

Posto isto, suponhamos que as parcelas $\mathfrak{M}_i$, de (3), além de isomorfas, são simples. O anel $\mathcal{Y}$ é um corpo, porque $\mathcal{U}_{11}$ é um corpo, como vamos ver. Um símbolo $G_{11}\sigma G_{11}^{(1)}$, aplicado aos elementos de $\mathfrak{M}_1$, leva deste a $\mathfrak{M}_i$. A cada símbolo corresponde um automorfismo de $\mathfrak{M}_1$ (se não se tratar do endomorfismo nulo). Inversamente, qualquer que seja o automorfismo Σ_{11}, de $\mathfrak{M}_i$, é o mesmo correspondente do símbolo $G_{11}\,.\,G_{11}\,\Sigma_{11}\,.\,G_{11}$. A correspondência em causa é biunívoca, visto que, se for $G_{11}\,\sigma\,G_{11} \neq G_{11}\,\tau\,G_{11}$, também são diferentes os respectivos automorfismos de $\mathfrak{M}_1$, como resulta da própria definição dos símbolos. $\mathcal{U}_{11}$ é, portanto, isomorfo do corpo dos endomorfismos de $\mathfrak{M}_1$. Pode enunciar-se o

Teorema 3 :- O anel $\mathcal{U}$ dos endomorfismos dum módulo completamente redutível, soma directa de t sub-módulos isomorfos, é um anel completo de matrizes do grau t com elementos dum corpo isomorfo do corpo endomorfico de cada sub-módulo.

Consideremos ainda o caso em que a decomposição (3) tem o aspecto

$$\mathfrak{M} = \mathfrak{M}_1 + \dots + \mathfrak{M}_h + \mathfrak{M}_{h+1} + \dots + \mathfrak{M}_{h+m} + \dots \qquad (6)$$

onde os $\mathfrak{M}_i$ são simples, nas condições seguintes: os h primeiros são isomorfos, os m imediatos são também isomorfos, mas não isomorfos dos anteriores, etc. Designemos por α e β dois índices de dois $\mathfrak{M}_i$ que não pertençam ao mesmo sistema de sub-módulos isomorfos. Uma homomorfia $\mathfrak{M}_\alpha \sim \mathfrak{M}_\beta$, já representada por $\Sigma_{\alpha\beta}$ só pode ser a homomorfia nula. A soma (4) deverá escrever-se

(1) É claro que, em geral, há elementos diferentes $\sigma, \tau, \dots \in \mathcal{U}$ que levam ao mesmo símbolo. No isomorfismo $\mathcal{Y} \cong \mathcal{U}_{11}$, podemos supor cada elemento T da forma $\sum_i G_{i1}\sigma_{11}G_{1i}$.

$$\sigma = \sum_{i,j} \sigma_{ij} + \sum_{k,l} \sigma_{kl} + \cdots, \qquad (7)$$

com $(i,j = 1, 2, \ldots, h;\ k, l = h+1, \ldots, h+m;$ etc.). Efectivamente, tem-se

$$\sigma_{\alpha\beta} = G_\alpha \Sigma_{\alpha\beta} = 0.$$

O anel $\mathcal{O}$ aparece como soma directa de tantos anéis quantos os sistemas de sub-módulos isomorfos distintos de (6): $\mathcal{O} = \mathcal{O}_1 + \ldots + \mathcal{O}_s$. A estrutura de cada sub-anel $\mathcal{O}_l$ esclarece-se tendo em conta que cada $\mathcal{O}_l$ é isomorfo dum anel como o referido no teorema 3. Assim:

Teorema 4 :- O anel $\mathcal{O}$ dos endomorfismos dum módulo $\mathfrak{M}$ completamente redutível é uma soma de anéis completos de matrizes que se anulam mutuamente. O número de parcelas é o número de sistemas de sub-módulos isomorfos em que se decompõe $\mathfrak{M}$, pressuposto que em cada sistema figuram todos os sub-módulos isomorfos, e os graus das diferentes matrizes são dados pelos números de sub-módulos de cada sistema. Finalmente, os elementos das matrizes dum anel parcela pertencem a corpos isomorfos dos corpos endomórficos de cada sub-módulo simples do sistema a que corresponde a referida parcela.

Observações:- O anel $\mathcal{O}'$ estudar-se-ia sucessivamente como o anel $\mathcal{O}$. Passando a $\mathcal{O}'$ por anti-isomorfismo, poremos $G_i \rightarrow G'_i$, $G_{ij} \rightarrow G'_{ji}$, por forma que se tenha

$$G_{ij} G_{jl} = G_{il} \rightarrow G'_{li} = G'_{ij} G'_{jl}, \qquad G'_{ij} G'_{ki} = 0, \quad (\text{se } k \neq j).$$

Convém notar, de resto, que uma homomorfia $\mathfrak{M}_i \sim \mathfrak{M}_j$ deveria ser representada, dum modo geral, por Σ'_{jl}, e que o prolongamento desta, de modo a torná-la num endomorfismo de $\mathfrak{M}$, se faria pelo símbolo $\Sigma'_{jl} G'_l = \sigma'_{jl}$. Uma outra observação é esta: se $\mathfrak{M}$ admite a decomposição (6), nas mesmas condições, salvo que os $\mathfrak{M}_l$ não são considerados simples, a igualdade (7) não pode escrever-se, pois que não têm lugar as igualdades $\Sigma_{\alpha\beta} = 0$.

5) Os anéis $\mathcal{O}_\mathcal{R}$ e $\mathcal{O}'_\mathcal{R}$ - Imaginemos agora que o módulo admite um sistema de operadores: $\mathcal{R} = \{R_1, R_2, \ldots, R, \ldots\}$. Isto significa, como se sabe, que se define uma aplicação de $R \in \mathcal{R}$ a $m \in \mathfrak{M}$, segundo a qual

$$m^R \in \mathfrak{M}, \qquad (m + m')^R = m^R + m'^R.$$

Os elementos R definem endomorfismos de $\mathfrak{M}$, os quais não são necessàriamente distintos. O sistema $\mathcal{R}$ tem imagens unívocas $\mathcal{R}_1$ e $\mathcal{R}'_1$, em $\mathcal{O}$ e $\mathcal{O}'$, respectivamente. Um endomorfismo $\sigma \in \mathcal{O}$ diz-se endomorfismo - $\mathcal{R}$, se for operatório relativamente a $\mathcal{R}$, isto é, se tiverem lugar as correspondências

$$m \rightarrow m\sigma, \qquad m^R \rightarrow (m^R)\sigma = (m\sigma)^R. \qquad (8)$$

Anàlogamente, $\sigma' \in \mathcal{O}'$ é um endomorfismo - $\mathcal{R}$, se

$$m \rightarrow \sigma' m, \qquad m^R \rightarrow \sigma'(m^R) = (\sigma' m)^R.$$

O anel $\mathcal{O}_\mathcal{R}$ é o conjunto dos elementos de $\mathcal{O}$ que são endomorfismos - $\mathcal{R}$. Nas aplicações que temos em vista, interessa-nos especialmente o caso em que $\mathcal{R}$ se encontra algebrizado por um produto (domínio multiplicativo). É claro que o produto $R_1 R_2$ de dois operadores representa um endomorfismo que pode não ser o produto dos endomorfismos correspondentes. A esse respeito tem lugar o seguinte

Teorema 1 :- É condição necessária e suficiente, para que a imagem $\mathcal{R}_1$, de $\mathcal{R}$, em $\mathcal{O}$, seja homomorfa (multiplicativa), que se tenha $m^{(R_1 R_2)} = (m^{R_1})^{R_2}$.

Neste caso, escreveremos mR em vez de m^R, de modo que teremos $m(R_1 R_2) = (mR_1)R_2$. O domínio $\mathcal{R}$ diz-se um domínio operatório direito. De resto, em vez de utilizarmos $R_1, R_2, \ldots$ podemos utilizar as suas imagens $\rho_1, \rho_2, \ldots \in \mathcal{R}_1$. As relações (8) tomarão a forma

$$m \rightarrow m\sigma, \qquad mR = m\rho \rightarrow (m\rho)\sigma = (m\sigma)\rho,$$

valendo esta proposição:

Teorema 2 :- Dado o módulo $\mathfrak{M}$ com um domínio operatório direito $\mathcal{R}$, o anel $\mathcal{O}_{\mathcal{R}}$, dos endomorfismos - $\mathcal{R}$, compõe-se dos elementos de $\mathcal{O}$ que comutam com os elementos da imagem $\mathcal{R}_1$, de $\mathcal{R}$, em $\mathcal{O}$, e apenas desses elementos.

Define-se anàlogamente o anel $\mathcal{O}'_{\mathcal{R}}$ como o conjunto dos elementos de $\mathcal{O}'$ que são endomorfismos - $\mathcal{R}$. Valem os seguintes teoremas:

Teorema 3 :- É condição necessária e suficiente, para que a imagem $\mathcal{R}'_1$, de $\mathcal{R}$, em $\mathcal{O}'$, seja anti-homomorfa (multiplicativa), que se tenha $m(R_1R_2) = (mR_1)R_2$.

Teorema 4 :- Dado o módulo $\mathfrak{M}$ com um domínio operatório direito $\mathcal{R}$, o anel $\mathcal{O}'_{\mathcal{R}}$, dos endomorfismos - $\mathcal{R}$, compõe-se dos elementos de $\mathcal{O}'$ que comutam com os elementos da imagem $\mathcal{R}'_1$, de $\mathcal{R}$, em $\mathcal{O}'$, e apenas desses elementos. Se σ' é um endomorfismo - $\mathcal{R}$, tem-se, com efeito,

$$m \longrightarrow \sigma' m, \qquad mR = \rho' m \longrightarrow \sigma'(\rho' m) = (\sigma' m)R = \rho'(\sigma' m).$$

Bem entendido que $\rho', \rho'_1, \rho'_2, \ldots \in \mathcal{R}'_1$ são imagens de $R, R_1, R_2, \ldots$

É evidente que $\mathcal{O}_{\mathcal{R}}$ e $\mathcal{O}'_{\mathcal{R}}$ são anti-isomorfos.

Tratando-se dum módulo $\mathfrak{M}$ com um domínio operatório $\mathcal{L} = \{L_1, L_2, \ldots, L, \ldots\}$, algebrizado por um produto, mas de tal modo que $m^{(L_1L_2)} = (m^{L_2})^{L_1}$, diremos que $\mathcal{L}$ é um domínio operatório esquerdo e escreveremos $(L_1L_2)m = L_1(L_2m)$. Há igualmente imagens $\mathcal{L}_1, \mathcal{L}'_1$, em $\mathcal{O}$ e $\mathcal{O}'$, a primeira anti-homomorfa, a segunda homomorfa. Fixaremos esta proposição:

Teorema 5 :- Dado o módulo $\mathfrak{M}$ com um domínio operatório esquerdo $\mathcal{L}$, o anel $\mathcal{O}_{\mathcal{L}}$ (anel $\mathcal{O}'_{\mathcal{L}}$), dos endomorfismos - $\mathcal{L}$, compõe-se dos elementos de $\mathcal{O}$ (de $\mathcal{O}'$) que comutam com os elementos da imagem $\mathcal{L}_1$ (imagem $\mathcal{L}'_1$), de $\mathcal{L}$, em $\mathcal{O}$ (em $\mathcal{O}'$), e apenas desses elementos.

6) Exemplos - Para aplicação dos resultados do § anterior, tomemos um módulo $\mathfrak{M}$, suposto módulo direito relativamente a $\mathcal{R}$. Isto significa que $\mathfrak{M}$ admite o domínio operatório direito $\mathcal{R}$, e que, portanto, se tem

$$mR \in \mathfrak{M}, \qquad (m + m')R = mR + m'R, \qquad m(R_1R_2) = (mR_1)R_2,$$

valendo além disso a igualdade ($\mathcal{R}$ supõe-se um anel)

$$m(R_1 + R_2) = mR_1 + mR_2.$$

A imagem $\mathcal{R}_1 \subseteq \mathcal{O}$ é homomorfa, tanto multiplicativa como aditiva. $\mathcal{R}_1$ é um sub-anel de $\mathcal{O}$. $\mathcal{R}'_1$ é igualmente um sub-anel de $\mathcal{O}'$. Pode dar-se o seguinte enunciado:

Teorema 1 :- Num módulo $\mathfrak{M}$ com um domínio operatório anular $\mathcal{R}$ (ou $\mathcal{L}$), é condição necessária e suficiente, para que $\mathcal{R}$ (ou $\mathcal{L}$) tenha uma imagem anular homomorfa $\mathcal{R}_1 \subseteq \mathcal{O}$ (ou imagem anular homomorfa $\mathcal{L}'_1 \subseteq \mathcal{O}'$), que $\mathfrak{M}$ seja módulo direito relativamente a $\mathcal{R}$ (ou esquerdo relativamente a $\mathcal{L}$).

Tomemos um anel qualquer $\mathcal{G} = \mathfrak{M}$. Pondo $\mathcal{G} = \mathcal{R}$, sabemos que $\mathcal{R}_1 \subseteq \mathcal{O}$ é imagem anular homomorfa de $\mathcal{G}$. Pondo $\mathcal{G} = \mathcal{L}$, sabemos que $\mathcal{L}_1 \subseteq \mathcal{O}$ é imagem anti-homomorfa de $\mathcal{G}$. Um elemento $L \in \mathcal{L}$ define, porém, um endomorfismo - $\mathcal{R}$, visto que

$$m \longrightarrow Lm = m\sigma, \qquad mR = m\rho \longrightarrow L(mR) = (Lm)R = (m\sigma)\rho = (m\rho)\sigma$$

Vê-se, deste modo, que é $\mathcal{L}_1 \subseteq \mathcal{O}_{\mathcal{R}}$. Podemos dizer:

Teorema 2 :- Um anel $\mathcal{G}$ tem uma imagem anular homomorfa $\mathcal{R}_1 \subseteq \mathcal{O}$ (anti-homomorfa $\mathcal{R}'_1 \subseteq \mathcal{O}'$) e uma imagem anular anti-homomorfa $\mathcal{L}_1 \subseteq \mathcal{O}$ (homomorfa $\mathcal{L}'_1 \subseteq \mathcal{O}'$), de tal modo que $\mathcal{L}_1 \subseteq \mathcal{O}_{\mathcal{R}}$ ($\mathcal{L}'_1 \subseteq \mathcal{O}'_{\mathcal{R}}$) e $\mathcal{R}_1 \subseteq \mathcal{O}_{\mathcal{G}}$ ($\mathcal{R}'_1 \subseteq \mathcal{O}'_{\mathcal{G}}$).

Na hipótese de $\mathcal{G}$ ser tal que, para cada par de elementos b e $c \neq b$, de $\mathcal{G}$, existe um elemento $s \in \mathcal{G}$ para o qual

$(c-b)s \neq 0$, a imagem $\mathcal{L}_1'$ é isomorfa. De facto, por meio de c, cada elemento $t \in \mathcal{G}$ é transformado em ct; e, por meio de b, tem-se $b \rightarrow bt$. Ora não pode ser $bt = ct$, qualquer que seja t, em virtude da hipótese. Vale o seguinte

Teorema 3 :- Um anel $\mathcal{G}$ tal que, dados $b, c \in \mathcal{G}$, com $c \neq b$, existe $s \in \mathcal{G}$ para o qual $(c-b)s \neq 0$, pode mergulhar-se sempre num anel com elemento um. É sempre um anel de endomorfismos de si mesmo. Também vale este outro

Teorema 4 :- Um anel $\mathcal{G}$ sem divisores de zero pode mergulhar-se sempre no anel $\mathcal{O}'$, onde tem uma imagem isomorfa, e no anel $\mathcal{O}$, onde tem igualmente uma imagem isomorfa. O anel $\mathcal{G}$ tem ainda em $\mathcal{O}$ e $\mathcal{O}'$ imagens anti-isomorfas.

Quando $\mathcal{G}$ tem elemento um, este mesmo teorema é verdadeiro. O teorema 2 pode, porém, precisar-se sob esta forma:

Teorema 5 :- Dado um anel $\mathcal{G}$ com elemento um, as suas imagens isomorfas $\mathcal{K}_1$ e $\mathcal{L}_1'$ verificam as relações $\mathcal{K}_1 = \mathcal{O}_{\mathcal{G}}$, $\mathcal{L}_1' = \mathcal{O}_{\mathcal{K}}'$ [e as suas imagens anti-isomorfas $\mathcal{K}_1'$, $\mathcal{L}_1$ as relações $\mathcal{K}_1' = \mathcal{O}_{\mathcal{G}}'$, $\mathcal{L}_1 = \mathcal{O}_{\mathcal{K}}$]. Verifiquemos, por ex., a igualdade $\mathcal{K}_1' = \mathcal{O}_{\mathcal{G}}'$. Temos de mostrar que um elemento σ' do segundo membro pertence ao 1º membro. Para $m = u$ e $L \in \mathcal{L}$, é

$$u \rightarrow \sigma' u = b, \qquad Lu = L \rightarrow \sigma'(Lu) = L(\sigma' u) = Lb .$$

O endomorfismo σ' é, pois, definido pela multiplicação à direita pelo elemento $b \in \mathcal{G}$. Escrevendo $Lb = L\rho = \rho' L$, reconhece-se que o endomorfismo σ' é o mesmo que o endomorfismo $\rho' \in \mathcal{O}'$, correspondente de b, de sorte que $\rho' \in \mathcal{K}_1'$, q. e. d.

Observação:- Façamos uma observação importante. Seja $\mathcal{M}$ um módulo com um domínio operatório esquerdo $\mathcal{L}$, por ex.. Pode suceder que $\mathcal{M}$ se encontre em qualquer das condições referidas no § 4, quanto à sua decomposição como soma directa de sub-módulos admissíveis em face de $\mathcal{L}$. Os teoremas 1, 2, 3 e 4 do referido § são válidos, substituindo $\mathcal{O}$ e $\mathcal{O}'$ por $\mathcal{O}_{\mathcal{G}}$ e $\mathcal{O}_{\mathcal{G}}'$ respectivamente.

Suponhamos que se trata dum ideal direito simples dum anel $\mathcal{G}$. Os anéis $\mathcal{O}_{\mathcal{K}}$ e $\mathcal{O}_{\mathcal{K}}'$ são corpos anti-isomorfos. Tem lugar o

Teorema 6 :- O anel dos endomorfismos dum ideal mínimo é um corpo.

Tomemos um ideal direito $\mathcal{K}$ gerado por um idempotente e dum anel $\mathcal{G} = \mathcal{K}$. É muito fácil de verificar que $\mathcal{O}_{\mathcal{K}}$ e $\mathcal{O}_{\mathcal{K}}'$ são, respectivamente, anti-isomorfo e isomorfo de e $\mathcal{G}$ e. Em particular, admitamos que $\mathcal{K} = e\mathcal{G}$ é um ideal direito regular mínimo, de $\mathcal{G}$. Podemos dizer (como se viu no § 4 do Cap. III):

Teorema 7 :- O anel dos endomorfismos dum ideal regular mínimo é completamente primário.

No § próximo, vamos reencontrar resultados muito nossos conhecidos. Certos detalhes, que, porém, precisaremos, serão úteis posteriormente.

7) Anéis simples, semi-simples e primários - Consideremos um anel simples $\mathcal{G}$ completamente redutível e com elemento um, caracterizado simplesmente como anel com elemento um, soma directa de ideais direitos simples isomorfos:

$$\mathcal{G} = \mathcal{K}_1 + \cdots + \mathcal{K}_n .$$

Pondo $\mathcal{G} = \mathcal{M} = \mathcal{K} = \mathcal{L}$, sabemos que é $\mathcal{L}_1' = \mathcal{O}_{\mathcal{K}}'$. Visto ser $\mathcal{L}_1'$ isomorfo de $\mathcal{G}$ e $\mathcal{O}_{\mathcal{K}}'$ um anel completo de matrizes do grau n com elementos do corpo $\mathcal{K}' = G_{11}' \mathcal{O}_{\mathcal{K}}' G_{11}'$, que é isomorfo do corpo dos endomorfismos - $\mathcal{K}$ à esquerda de $\mathcal{K}_1$, podemos dizer que um anel simples tem a estrutura dum anel completo de matrizes com elementos dum corpo isomorfo do corpo dos endomorfismos - - $\mathcal{K}$ à esquerda dum dos $\mathcal{K}_i$ (ou dum ideal direito simples qualquer de $\mathcal{G}$, pelo facto de serem $\mathcal{K}$- isomorfos todos os ideais direitos simples). Analogamente, a relação $\mathcal{L}_1 = \mathcal{O}_{\mathcal{K}}$ mostra que o anel $\mathcal{G}$ é anti-isomorfo dum anel completo de matrizes com elementos dum corpo isomorfo do corpo dos endomorfismos - $\mathcal{K}$ à direita dum dos $\mathcal{K}_i$. Do estudo dos anéis completos de matrizes, sabe-se que $\mathcal{O}_{\mathcal{K}}'$ é também soma de n ideais esquerdos simples,

o mesmo podendo dizer-se de $\mathscr{G}$, que toma, assim, a forma

$$\mathscr{G} = \mathscr{U}_1 + \cdots + \mathscr{U}_n ,$$

onde $\mathscr{U}_i$ significa ideal esquerdo (simples). Então tem-se

$$\mathscr{R}_1 = \mathscr{O}_{\mathscr{G}} , \qquad \mathscr{R}'_1 = \mathscr{O}'_{\mathscr{G}} .$$

Por consequência, enuncia-se o

Teorema 1 :- Um anel $\mathscr{G} = \mathscr{R} = \mathscr{L}$ completamente redutível em ideais direitos todos $\mathscr{R}$-isomorfos, e com elemento um, é também completamente redutível em ideais esquerdos todos $\mathscr{L}$-isomorfos. A estrutura do anel é a dum anel completo de matrizes com elementos dum corpo isomorfo do corpo dos endomorfismos - $\mathscr{R}$ à esquerda dum ideal direito simples de $\mathscr{G}$, ou a dum anel completo de matrizes com elementos dum corpo isomorfo do do corpo dos endomorfismos - $\mathscr{L}$ à direita dum ideal esquerdo simples de $\mathscr{G}$. Ou ainda: $\mathscr{G}$ é isomorfo dum anel completo de matrizes com elementos dum corpo anti-isomorfo do corpo dos endomorfismos - $\mathscr{R}$ à direita dum ideal direito simples de $\mathscr{G}$, e também isomorfo dum anel completo de matrizes com elementos dum corpo anti-isomorfo do corpo dos endomorfismos - $\mathscr{L}$ à esquerda dum ideal esquerdo simples de $\mathscr{G}$.

Esclarecida a estrutura dos anéis simples, passa-se aos anéis semi-simples. Os resultados anteriores permitem dar a seguinte proposição, na qual se subentende o anel semi-simples definido como anel completamente redutível com elementos um:

Teorema 2 :- Um anel semi-simples é soma directa de anéis simples que mutuamente se anulam. O número de anéis simples parcelas é o número de sistemas de ideais simples direitos isomorfos em que se decompõe o anel (pressuposto que em cada sistema figuram todos os ideais isomorfos). De facto, a existência de elemento um, conforme o § 6, permite que

se escreva $\mathscr{L}'_1 = \mathscr{O}'_{\mathscr{R}}$. A estrutura de $\mathscr{O}'_{\mathscr{R}}$ é consequência dos raciocínios do § 2.

Sabemos que um anel primário tem elemento um e é soma directa de ideais regulares mínimos isomorfos. É válido, assim, o seguinte

Teorema 3 :- Um anel primário tem a estrutura dum anel completo de matrizes com elementos dum anel completamente primário.

8) Caso em que existem dois domínios operatórios - Até aqui esteve em causa um único domínio operatório de $\mathscr{M}$, salvo no caso dos anéis. Suponhamos agora que existem dois anéis operatórios $\mathscr{R}$ e $\mathscr{L}$, o primeiro dos quais opera à direita de $\mathscr{M}$, o segundo à esquerda. Para as aplicações que temos em vista, vamos admitir já (como sucede no caso dos anéis) que $\mathscr{M}$ é módulo relativamente aos dois anéis. Levanta-se a questão de saber se os elementos de $\mathscr{L}$ definirão endomorfismos - $\mathscr{R}$ e os elementos de $\mathscr{R}$ definirão endomorfismos - $\mathscr{L}$. Podemos também dizer que se trata de saber se $\mathscr{L}_1 \subseteq \mathscr{O}_{\mathscr{R}}$ e $\mathscr{R}_1 \subseteq \mathscr{O}_{\mathscr{L}}$. Respondemos imediatamente com o

Teorema 1 :- Se $\mathscr{M}_{\mathscr{R}}$ é um módulo relativo ao anel $\mathscr{R}$ (que opera à direita) e ao anel $\mathscr{L}$ (que opera à esquerda), é condição necessária e suficiente, para que os elementos de $\mathscr{R}$ definam endomorfismos - $\mathscr{L}_1$ (1) que a imagem $\mathscr{R}_1 \subseteq \mathscr{O}$ seja composta de elementos individualmente comutáveis com $\mathscr{L}_1 \subseteq \mathscr{O}$. De facto, se os operadores $\mathscr{R}$ e $\mathscr{L}$ estão na situação recíproca do enunciado, é $\mathscr{R}_1 \subseteq \mathscr{O}_{\mathscr{L}}$ e os elementos de $\mathscr{R}_1$ comutam com os de $\mathscr{L}_1$. Inversamente, supondo $\mathscr{R}_1 \subseteq \mathscr{O}_{\mathscr{L}}$, sem dúvida que os elementos de $\mathscr{R}$ definem endomorfismos - $\mathscr{L}$. Para se ver que é também $\mathscr{L}_1 \subseteq \mathscr{O}_{\mathscr{R}}$, observemos que esta condição se exprime pela igualdade $(m\,\rho_1)\,\lambda_1 = (m\,\lambda_1)\,\rho_1$ [com $\lambda_1 \in \mathscr{L}_1$], a qual é precisamente a mesma que exprime ser $\mathscr{R}_1 \subseteq \mathscr{O}_{\mathscr{L}}$. Também se pode substituir esta última relação por qualquer das duas seguintes:

$$\mathscr{R}'_1 \subseteq \mathscr{O}'_{\mathscr{L}} , \qquad \mathscr{L}'_1 \subseteq \mathscr{O}'_{\mathscr{R}} .$$

(1) [e os elementos de $\mathscr{L}$ definam endomorfismos - $\mathscr{R}$]

Para verificar esta afirmação, basta observar que qualquer das quatro relações de inclusão indicadas traduz a igualdade (associativa)

$$(Lm)R = L(mR), \qquad (9)$$

e que, inversamente, esta igualdade traduz qualquer das quatro relações citadas. Diz-se, então, que $\mathfrak{M}$ é módulo duplo relativamente a $\mathfrak{K}$ e a $\mathfrak{L}$. Por isso, podemos dar ao teorema anterior esta forma:

Teorema 2 :- Se $\mathfrak{M}$ é módulo relativo a $\mathfrak{K}$ e a $\mathfrak{L}$, é condição necessária e suficiente, para que os elementos de $\mathfrak{K}$ definam endomorfismos - $\mathfrak{L}$ e os de $\mathfrak{L}$ definam endomorfismos - $\mathfrak{K}$, que $\mathfrak{M}$ seja módulo duplo relativamente aos dois anéis. A propriedade associativa traduzida em (9) foi precisamente a que se utilizou ao tratarmos os anéis $\mathfrak{L}$ com os seus próprios elementos a operar à direita e à esquerda [teorema 2 do § 6].

Se dois domínios operatórios $\mathfrak{L}$ e $\mathfrak{T}$ são esquerdos (por ex.), é claro, sob a hipótese de $\mathfrak{M}$ ser módulo esquerdo relativamente aos dois anéis (domínios), a comutabilidade dos elementos de $\mathfrak{T}_1$ e de $\mathfrak{L}_1$ traduz-se pela condição seguinte, que substitui (9):

$$\mathfrak{T}_1(L_1 m) = L_1(S_1 m) .$$

Esta condição (lei de troca) resulta pondo $(m\lambda_1)\sigma_1 = (m\sigma_1)\lambda_1$ [com $\sigma_1 \in \mathfrak{T}_1$]. Ela exprime, por definição, que $\mathfrak{M}$ é módulo duplo relativamente a $\mathfrak{T}$ e a $\mathfrak{L}$. Poderiam enunciar-se ainda, exactamente do mesmo modo, os dois teoremas que acabamos de referir.

9) Os módulos finitos - Coloquemo-nos na hipótese de $\mathfrak{M}$ ter a forma $\mathfrak{M} = u_1\mathfrak{K} + \cdots + u_n\mathfrak{K}$, onde os u_i são puros símbolos e $\mathfrak{K}$ é um anel. O módulo aparece como soma directa de n grupos cíclicos isomorfos, não geralmente simples. Se $\mathfrak{K}$ tem elemento um, é verdadeira a seguinte proposição:

Teorema 1 :- O grupo cíclico $u_1\mathfrak{K}$ tem um anel $\mathfrak{O}_{u_1}$ de endomorfismos, no qual a imagem $\mathfrak{K}_1$, de $\mathfrak{K}$, é isomorfa deste último, e no qual o sub-anel $\mathfrak{O}_{1\mathfrak{K}}$, dos endomorfismos - $\mathfrak{K}$, é anti-isomorfo de $\mathfrak{K}$. Portanto:

Teorema 2 :- O módulo finito $\mathfrak{M} = u_1\mathfrak{K} + \cdots + u_n\mathfrak{K}$, relativo ao anel $\mathfrak{K}$ com elemento um, tem um anel $\mathfrak{O}_{\mathfrak{K}}$ (anel $\mathfrak{O}_{\mathfrak{K}}$) de endomorfismos cuja estrutura é a dum anel completo de matrizes com elementos dum anel isomorfo de $\mathfrak{O}_{1\mathfrak{K}}$, ou seja anti-isomorfo de $\mathfrak{K}$ (isomorfo de $\mathfrak{O}'_{1\mathfrak{K}}$, ou seja isomorfo de $\mathfrak{K}$).

Em vez do enunciado anterior, pode dar-se este outro:

Teorema 2' :- O módulo finito $\mathfrak{M} = u_1\mathfrak{K} + \cdots + u_n\mathfrak{K}$, relativo ao anel $\mathfrak{K}$ com elemento um, tem um anel $\mathfrak{O}_{\mathfrak{K}}$ (anel $\mathfrak{O}_{\mathfrak{K}}$) de endomorfismos, que é anti-isomorfo do anel completo de matrizes com elementos de $\mathfrak{K}$ (dum anel anti-isomorfo de $\mathfrak{K}$). Esta forma do teorema reencontra-se imediatamente como segue. Tomemos os elementos $u_1 u, \ldots, u_n u \in \mathfrak{M}$ e endomorfismos $\sigma, \tau \in \mathfrak{O}_{\mathfrak{K}}$. Tem-se

$$(u_i u)\sigma = (u_1 u)s_{1i} + \cdots + (u_n u)s_{ni} = \sum_j (u_j u)s_{ji} , \quad (s_{ji} \in \mathfrak{K}),$$

$$(u_i u)\sigma\tau = \sum_j (u_j u)\tau . s_{ji} = \sum_{j,k} (u_k u)t_{kj}\, s_{ji} = \sum_k (u_k u)\Big(\sum_j t_{kj}\, s_{ji}\Big).$$

Fazendo corresponder ao elemento σ a matriz (s_{ij}), vê-se que ao produto $\sigma\tau$ corresponde a matriz produto $(t_{ij})(s_{ij})$.

Posto isto, consideremos a 1ª representação regular dum sistema hiper-complexo $\mathfrak{h}_{\mathfrak{J}}$. Têm-se as igualdades $ae_i = \Sigma e_j \alpha_{ji}$ (§ 2, Cap. VI). Os elementos de $\mathfrak{A}$ operam aqui à direita e os de $\mathfrak{h}_{\mathfrak{J}}$ à esquerda do módulo finito relativo a $\mathfrak{A}$, $\mathfrak{h}_{\mathfrak{J}} = \mathfrak{M} . \mathfrak{h}_{\mathfrak{J}}$ é módulo duplo com respeito aos dois domínios operatórios em causa, de modo que os elementos de $\mathfrak{h}_{\mathfrak{J}}$ definem endomorfismos - $\mathfrak{A}$. Como no começo do § 6, podemos afirmar que $\mathfrak{h}_{\mathfrak{J}}$ tem imagem anti-homomorfa $\mathfrak{h}_{\mathfrak{J}_1} = \mathfrak{L}_1$ no anel $\mathfrak{O}_{\mathfrak{K}}$, e sendo este último anti-isomorfo do anel completo de matrizes com elementos de $\mathfrak{A}$, a 1ª representação regular indicada é, de facto, uma representação

directa de $\mathcal{G}$ em $\mathcal{K}$. A representação torna-se fiel, se $\mathcal{G}$ tem elemento um.

Dum modo geral para a teoria das representações, sejam $\mathcal{Y}$ um anel e $\mathcal{G}$ uma sua representação directa de grau n (em $\mathcal{K}$, ou por meio de $\mathcal{G}$). Se considerarmos um módulo finito $\mathcal{M}$, de ordem n, relativamente a $\mathcal{K}$ (que opera à direita), $\mathcal{Y}$ tem, por hipótese, uma imagem anti-homomorfa $\mathcal{Y}_1$ no anel $\mathcal{O}_{\mathcal{K}}$. $\mathcal{Y}$ pode considerar-se um domínio operatório esquerdo de $\mathcal{M}$. Este último torna-se num módulo duplo (direito - $\mathcal{K}$, esquerdo - $\mathcal{Y}$), que é o módulo de representação correspondente (§ 1). Inversamente, um módulo duplo (direito - $\mathcal{K}$, esquerdo - $\mathcal{Y}$), finito relativamente a $\mathcal{K}$, leva a uma representação de $\mathcal{Y}$ por meio dum anel de matrizes com elementos de $\mathcal{K}$. Podemos, assim, modificar o enunciado do teorema das representações dado no § 1 e dizer:

Teorema 3 :- Todo o módulo duplo $\mathcal{M}$, relativo a $\mathcal{Y}$ (que opera à esquerda) e relativo a $\mathcal{K}$ (que opera à direita e tal que $\mathcal{M}$ é finito relativamente a $\mathcal{K}$), é um módulo de representação directa de $\mathcal{Y}$ em $\mathcal{K}$, ao qual corresponde uma classe de representações equivalentes, e, inversamente, dada uma representação directa de $\mathcal{Y}$ em $\mathcal{K}$, há um módulo duplo relativo a $\mathcal{Y}$ e a $\mathcal{K}$, ao qual pertence uma classe de representações que contém a representação em causa.

Detalhemos ainda os raciocínios que respeitam às representações recíprocas. Eis aqui os teoremas correspondentes aos anteriores:

Teorema 4 :- O grupo cíclico $\mathcal{L}u_1$, se $\mathcal{L}$ possui elemento um, tem um anel $\mathcal{O}_1$ de endomorfismos no qual a imagem $\mathcal{L}_1$, de $\mathcal{L}$, é anti-isomorfa deste último, e no qual o sub-anel $\mathcal{O}_{1\mathcal{G}}$, dos endomorfismos - $\mathcal{L}$, é isomorfo de $\mathcal{L}$.

Teorema 5 :- O módulo finito $\mathcal{M}=\mathcal{L}u_1+\cdots+\mathcal{L}u_n$, relativo ao anel $\mathcal{L}$ com elemento um, tem um anel $\mathcal{O}_{\mathcal{G}}$ (anel $\mathcal{O}_{\mathcal{H}}$) de endomorfismos cuja estrutura é a dum anel completo de matrizes com elementos dum anel isomorfo de $\mathcal{O}_{1\mathcal{G}}$, ou seja isomorfo de $\mathcal{L}$ (isomorfo de $\mathcal{O}_{1\mathcal{G}}$, ou seja anti-isomorfo de $\mathcal{L}$).

Podemos dar uma demonstração mais directa, escrevendo

$$(uu_i)\sigma = s_{i1}(uu_1) + \cdots + s_{in}(uu_n) = \sum_j s_{ij}(uu_j), \quad (s_{ij}\in\mathcal{L}),$$

$$(uu_i)\sigma\tau = \sum_j s_{ij}\cdot(uu_j)\tau = \sum_{j,k} s_{ij}\,t_{jk}(uu_k) = \sum_k\Big(\sum_j s_{ij}\,t_{jk}\Big)(uu_k).$$

Fazendo corresponder ao elemento σ a matriz (s_{ij}), vê-se que ao produto $\sigma\tau$ corresponde a matriz produto $(s_{ij})(t_{ij})$.

Posto isto, consideremos a 2ª representação regular recíproca dum sistema $\mathcal{G}$. Tem-se $e_i a = \sum e_j a^*_{ji}$. Tanto $\mathcal{G}$ como $\mathcal{K}$ operam à direita de $\mathcal{G} = \mathcal{M}$. A lei de troca tem lugar e $\mathcal{G}$ é módulo duplo com respeito aos dois domínios operatórios. Os elementos de $\mathcal{G}$ definem endomorfismos - $\mathcal{K}$, de sorte que $\mathcal{G}$ tem imagem homomorfa $\mathcal{G}_1 = \mathcal{R}_1$ no qual $\mathcal{O}_{\mathcal{K}}$, e sendo este último anti-isomorfo do anel completo de matrizes com elementos de $\mathcal{K}$, a 2ª representação regular indicada é, de facto, uma representação recíproca de $\mathcal{G}$ em $\mathcal{K}$. A representação torna-se fiel, se $\mathcal{G}$ tem elemento um.

Sejam, em geral, $\mathcal{Y}$ um anel e $\mathcal{G}$ uma representação recíproca do mesmo, de grau n, em $\mathcal{K}$ (ou por meio de $\mathcal{G}$). Se considerarmos um módulo finito $\mathcal{M}$, de ordem n, relativamente a $\mathcal{K}$ (que opera à esquerda), $\mathcal{Y}$ tem, por hipótese, uma himagem anti-homomorfa no anel completo de matrizes do grau n com elementos de $\mathcal{K}$, e, portanto, uma imagem anti-homomorfa $\mathcal{Y}_1$ no anel $\mathcal{O}_{\mathcal{K}}$. $\mathcal{Y}$ pode considerar-se um domínio operatório esquerdo de $\mathcal{M}$. Este último torna-se num módulo duplo (esquerdo - $\mathcal{K}$, esquerdo - $\mathcal{Y}$), que é o módulo recíproco de representação correspondente (§ 1). Inversamente, um módulo duplo esquerdo relativamente a $\mathcal{Y}$ e a $\mathcal{K}$ leva a uma representação recíproca de $\mathcal{Y}$ por meio dum anel de matrizes com elementos de $\mathcal{K}$. Tem-se o

Teorema 6 :- Todo o módulo duplo $\mathcal{M}$ relativo a $\mathcal{Y}$ (que opera à esquerda) e relativo a $\mathcal{K}$ (que opera à esquerda e tal que $\mathcal{M}$ é finito relativamente a $\mathcal{K}$) é um módulo recíproco de representação de $\mathcal{Y}$ em $\mathcal{K}$, ao qual corresponde uma classe de representações equivalentes, e, inversamente, dada uma representação recíproca de $\mathcal{Y}$ em $\mathcal{K}$, há um módulo duplo (esquerdo) relativo a

$\mathcal{T}$ e a $\mathcal{A}$, ao qual pertence uma classe de representações que contém a representação em causa.

Supondo que $\mathcal{L}_{\mathcal{T}}$ tem elemento um, podemos dar agora fàcilmente uma nova demonstração do seguinte

Teorema 7 :- As matrizes da 2ª representação regular recíproca de $\mathcal{L}_{\mathcal{T}}$ constituem o conjunto das matrizes, do anel completo de matrizes com elementos de $\mathcal{A}$, que comutam com as matrizes da 1ª representação regular directa de $\mathcal{L}_{\mathcal{T}}$. Efectivamente, tem-se $\mathcal{L}_{\mathcal{T}_1} = \mathcal{L}_1 = \mathcal{O}_{\mathcal{A}}$, quando $\mathcal{L}_{\mathcal{T}} = \mathcal{R}$ se considera operando à direita de si mesmo, e tem-se $\mathcal{L}_{\mathcal{T}_1} = \mathcal{R}_1 = \mathcal{O}_{\mathcal{L}}$, quando $\mathcal{L}_{\mathcal{T}} = \mathcal{L}$ opera à sua esquerda. Por outro lado, os elementos de $\mathcal{L}_1$ são definidos como únicos elementos de $\mathcal{O}_{\mathcal{A}}$ que comutam com $\mathcal{O}_{\mathcal{L}} = \mathcal{R}_1$. Assim, os elementos de $\mathcal{L}_1$ e $\mathcal{R}_1$, em $\mathcal{O}_{\mathcal{A}}$, comutam. Por anti-isomorfismo, passa-se de $\mathcal{O}_{\mathcal{A}}$ ao anel completo de matrizes com elementos de $\mathcal{A}$, e de $\mathcal{L}_1$ e $\mathcal{R}_1$, respectivamente, às matrizes da 1ª representação regular directa e às da 2ª representação regular recíproca.

10) Matrizes comutáveis com as matrizes duma representação - Dada uma representação directa de $\mathcal{T}$ em $\mathcal{A}$, de grau n, é nosso objectivo procurar, no anel completo $\mathcal{A}_n$, de matrizes com elementos de $\mathcal{A}$, as matrizes que comutam com as matrizes do anel $\mathcal{L}$ de representação. Se $\mathcal{M}$ é o módulo de representação, pondo $\mathcal{T} = \mathcal{L}$, $\mathcal{A} = \mathcal{R}$, sabemos que $\mathcal{T}_1 = \mathcal{L}_1 \cong \mathcal{O}_{\mathcal{M}}$. O problema resolve-se procurando em $\mathcal{O}_{\mathcal{A}}$ os elementos que comutam com $\mathcal{T}_1$. No anel $\mathcal{O}$ dos endomorfismos de $\mathcal{M}$, $\mathcal{O}_{\mathcal{T}}$ representa o conjunto de elementos que comutam com $\mathcal{T}_1$, de sorte que os elementos de $\mathcal{O}$ pertencentes à intersecção $\mathcal{O}_{\mathcal{T}} \cap \mathcal{O}_{\mathcal{A}}$ são os elementos procurados. Daqui, este

Teorema:- É condição necessária e suficiente, para que uma matriz comute com as matrizes duma representação directa de $\mathcal{T}$ em $\mathcal{A}$, que a referida matriz corresponda a um endomorfismo - $(\mathcal{T}; \mathcal{A})$ do módulo de representação, na correspondência anti-isomorfa $\mathcal{O}_{\mathcal{A}} \leftrightarrow \mathcal{A}_n$.

O teorema é exactamente o mesmo para as representações recíprocas, como é, aliás, evidente.

Tomemos, por ex., a representação directa de $\mathcal{T}$ em $\mathcal{A}$. Se $u_1, \ldots, u_n$ constituem uma base independente para o módulo $\mathcal{M}$, designemos por $u'_1, \ldots, u'_n$ os elementos correspondentes num endomorfismo - $(\mathcal{T}, \mathcal{A})$: $u_i \rightarrow u'_i$, $Su_i \rightarrow Su'_i$. Pondo $Su_i = \Sigma u_j s_{ji}$, com $s_{ji} \in \mathcal{A}$, vê-se que é $Su'_i = \Sigma u'_j s_{ji}$. Daqui se tira o seguinte

Teorema:- Dada uma representação de $\mathcal{T}$ em $\mathcal{A}$, se $\mathcal{M}(u_1, \ldots, u_n)$ for o módulo de representação correspondente, um endomorfismo - $(\mathcal{T}, \mathcal{A})$, do módulo $\mathcal{M}$, determina uma correspondência $u_i \rightarrow u'_i$ tal que, da aplicação dos elementos $S \in \mathcal{T}$ aos referidos u'_i, resulta ainda a representação em causa.

Deve observar-se, porém, que os u'_i não constituem geralmente uma base de $\mathcal{M}$.

11) Passagem de módulos duplos a módulos unilaterais - Se $\mathcal{M}$ é um módulo duplo esquerdo relativamente a dois anéis $\mathcal{L}$ e $\mathcal{T}$, as imagens $\mathcal{L}_1$ e $\mathcal{T}_1$, em $\mathcal{O}$, compõem-se de elementos individualmente comutáveis. Existe, em $\mathcal{O}$, um sub-anel $\mathcal{T}_1$ gerado pelos sub-anéis $\mathcal{L}_1$ e $\mathcal{T}_1$. Se existir um anel $\mathcal{T}$, do qual $\mathcal{L}$ e $\mathcal{T}$ sejam geradores de elementos individualmente comutáveis, $\mathcal{M}$ torna-se num módulo relativo ao único domínio operatório $\mathcal{T}$, cujos elementos operam como indicam as suas imagens em $\mathcal{T}_1$. O domínio $\mathcal{T}$ prolonga qualquer dos dois domínios $\mathcal{L}$ e $\mathcal{T}$. É o que sucede, por ex., quando se tem uma representação recíproca de $\mathcal{T}$ em $\mathcal{A}$ e $\mathcal{T}$ existe. Inversamente, se $\mathcal{M}$ é um módulo relativo ao único domínio operatório esquerdo $\mathcal{T}$, se neste último há dois sub-anéis $\mathcal{A}$ e $\mathcal{T}$, de elementos individualmente comutáveis, e se $\mathcal{M}$ é módulo finito relativamente a $\mathcal{A}$, está-se em presença duma representação recíproca de $\mathcal{T}$ em $\mathcal{A}$, com $\mathcal{M}$ como módulo recíproco de representação. Neste caso, vale o seguinte

Teorema 1 :- É condição necessária e suficiente, para que um endomorfismo de $\mathcal{M}$ seja um endomorfismo - $(\mathcal{T}, \mathcal{A})$, que seja um endomorfismo - $\mathcal{T}$. Partamos, com efeito, dum endomorfismo $\sigma \in \mathcal{O}$, que seja endomorfismo - $(\mathcal{T}, \mathcal{A})$. Representando por letras latinas minúsculas correspondentes os elementos dos anéis e do

módulo, consideremos o elemento $t = \sum s_l k_l + s + k$. Tem-se imediatamente:

$$m \to m\sigma, \qquad tm \to (tm)\sigma = \big((\sum s_l k_l + s + k)m\big)\sigma = \sum s_l (k_l m)\sigma +$$

$$+ \cdots = \sum s_l (k_l m \cdot \sigma) + \cdots = \sum s_l (k_l \cdot m\sigma) + \cdots = \sum s_l k_l \cdot m\sigma +$$

$$+ s \cdot m\sigma + k \cdot m\sigma = t(m\sigma).$$

Inversamente, um endomorfismo - $\mathcal{Y}$ é endomorfismo - γ e endomorfismo - $\mathfrak{A}$, portanto endomorfismo - $(\gamma, \mathfrak{A})$. Podemos dizer, assim, que, dada uma representação recíproca de γ em $\mathfrak{A}$, se $\mathcal{Y}$ existe, as matrizes comutáveis com as matrizes da representação são as que determinam endomorfismos - $\mathcal{Y}$ do módulo $\mathfrak{M}$, e apenas essas. $\mathcal{Y}$ supõe-se sempre gerado por $\mathfrak{A}$ e γ.

Realizam as condições do teorema os elementos $q \in [\gamma, \mathfrak{A}] = \mathcal{O}$, ainda que esta intersecção tenha elementos diferentes de zero. Um elemento q pertence ao centro de $\mathfrak{A}$. Na representação recíproca de γ por meio de $\mathfrak{A}$, corresponde a q uma matriz diagonal de elementos iguais a q. Pode dizer-se:

Teorema 2 :- Dado o módulo esquerdo $\mathfrak{M}$ relativo ao anel $\mathcal{Y}$, se neste existem dois sub-anéis γ e $\mathfrak{A}$ de elementos comutáveis e se $\mathfrak{M}$ é finito relativamente a $\mathfrak{A}$, a representação recíproca de γ por meio de $\mathfrak{A}$, pertencente a $\mathfrak{M}$, é operatória relativamente a $[\gamma, \mathfrak{A}]$. De facto, designando as matrizes da representação pelas letras latinas maiúsculas correspondentes aos elementos dos diferentes anéis, tem-se

$$s \to S, \qquad qs = sq \to SQ = QS = qS.$$

Precisemos ainda o que vai ver-se. Continuemos a supor o módulo $\mathfrak{M}$ relativo a $\mathcal{Y}$ e a existência de γ e $\mathfrak{A}$ nas condições anteriores. Define-se, por um lado, uma representação recíproca de γ em $\mathfrak{A}$; por outro, se fizermos corresponder a cada elemento $k \in \mathfrak{A}$ a matriz diagonal de elementos iguais kU (U = matriz unidade), tem-se uma representação directa (isomorfa) de $\mathfrak{A}$ em $\mathfrak{A}$. Poderia tentar-se uma representação de $\mathcal{Y}$ em $\mathfrak{A}$, fazendo corresponder a $t = \sum k_l s_l + k + s$ a matriz $T = \sum K_l S_l + K + S$. A referida representação não poderia ser recíproca, pois que deveria ter-se $ks \to KS = kS$, $k's' \to K'S' = k'S'$, $ks \cdot k's = kk' \cdot ss' \to kk' \cdot S'S$, e também $kk' \cdot ss' \to k'S' \cdot kS$, o que é absurdo. Se a representação se imaginasse directa, viria um outro absurdo: $ks \cdot k's' = kk' \cdot ss' \to kk' \cdot S'S = kS \cdot k'S'$.

12) Representações redutíveis - As matrizes duma representação $\mathcal{Y}$ definem transformações lineares do espaço $\mathfrak{M}$ que é módulo de representação. $\mathcal{Y}$ diz-se redutível, se existir um sub-módulo autêntico $\mathfrak{M} \neq (0)$, de $\mathfrak{M}$, que seja invariante em face de $\mathfrak{A}$ e de γ. Esta definição, que é independente da existência de base para $\mathfrak{M}$, ganha interesse, se essa base existe.

Suponhamos $\mathfrak{M} = \mathfrak{M}(u_1, \ldots, u_q)$ e que existem elementos $v_1, \ldots, v_r \in \mathfrak{M}$, tais que este último admite a base formada pelo conjunto dos u_l e dos v_j. Será

$$\mathfrak{M} = u_1\mathfrak{A} + \cdots + u_q\mathfrak{A}, \tag{10}$$

$$\mathfrak{M} = u_1\mathfrak{A} + \cdots + u_q\mathfrak{A} + v_1\mathfrak{A} + \cdots + v_r\mathfrak{A},$$

com $q + r = n$. Como, por hipótese, para cada $a \in \gamma$, vale

$$au_l = u_l A = \sum_{j=1}^{q} u_j p_{jl}, \qquad (i = 1, \ldots, q),$$

$$av_l = v_l A = \sum_{j=1}^{q} u_j q_{jl} + \sum_{j=1}^{r} v_j r_{jl}, \quad (i = 1, \ldots, r), \tag{11}$$

vê-se que a matriz A é da forma

$$A = \begin{pmatrix} P & Q \\ O & R \end{pmatrix}, \tag{12}$$

onde $P = (p_{jl})$, $Q = (q_{jl})$, $R = (r_{jl})$ são matrizes, das quais P e R são quadradas e Q é rectangular. O é a matriz nula. Assim sempre que uma representação $\mathcal{Y}$ é redutível, todas as suas matrizes podem tomar a forma (12). Inversamente, se as matrizes

de $\mathfrak{g}$ têm o aspecto (12), $\mathfrak{g}$ é redutível e existe um sub-módulo de representação para o qual as matrizes correspondentes são as matrizes P.

Em virtude de ser, para duas matrizes A e B da forma (12),

$$AB = \begin{pmatrix} P & Q \\ 0 & R \end{pmatrix} \cdot \begin{pmatrix} S & T \\ 0 & V \end{pmatrix} = \begin{pmatrix} PS & PT + QV \\ 0 & RV \end{pmatrix},$$

vê-se que o produto RV aparece no lugar de R (ou de V). Esta circunstância sugere que as matrizes R possam ser também matrizes duma representação. Ora consideremos o espaço $\mathfrak{M}/\mathfrak{N}$, que é também módulo duplo relativamente a $\mathfrak{A}$ e a $\mathfrak{g}^{\vee}$ e finito com respeito a $\mathfrak{A}$. Os seus elementos base são $v_1 + \mathfrak{N}, \ldots, v_r + \mathfrak{N}$, tendo-se, para $v + \mathfrak{N} \in \mathfrak{M}/\mathfrak{N}$,

$$a(v + \mathfrak{N}) = av + \mathfrak{N} = a \cdot \sum_{i=1}^{q} u_i a_i + a \cdot \sum_{j=1}^{r} v_j b_j + \mathfrak{N} =$$

$$= \sum_{j=1}^{r} av_j \cdot b_j + \mathfrak{N} = \sum_{i=1}^{r} v_i \left(\sum_{j=1}^{r} r_{ij} b_j \right) + \mathfrak{N}.$$

Duma maneira precisa, pois, o elemento $a \in \mathfrak{g}^{\vee}$ transforma o elemento $\sum_{1}^{r} v_j b_j + \mathfrak{N} \in \mathfrak{M}/\mathfrak{N}$ no elemento dado pelo último membro das igualdades anteriores. Considerando, assim, elementos módulo $\mathfrak{N}$, tem-se

$$a \cdot \sum_{j=1}^{r} v_j b_j = \sum_{i=1}^{r} v_i \left(\sum_{j=1}^{r} r_{ij} b_j \right), \qquad a \cdot v_j = \sum_{i=1}^{r} v_i r_{ij}.$$

Portanto: as matrizes $R = (r_{ij})$ definem uma representação pertencente ao módulo de representação $\mathfrak{M}/\mathfrak{N}$.

Para uma representação recíproca, ter-se-ia, correspondentemente a (11) e (12),

$$au_i = \sum_{j=1}^{q} p'_{ij} u_j, \qquad (i = 1, 2, \ldots, q),$$

$$av_i = \sum_{j=1}^{q} q_{ij} u_j + \sum_{j=1}^{r} r_{ij} v_j, \qquad (i = 1, 2, \ldots, r),$$

$$a \longrightarrow A' = \begin{pmatrix} P' & 0 \\ Q' & R' \end{pmatrix}.$$

Todos os demais raciocínios se repetem.

13) Processo de redução - Imaginemos que o sub-módulo duplo invariante $\mathfrak{N}$, referido no § anterior, é máximo. Ponhamos $\mathfrak{N} = \mathfrak{M}_{p-1}$ e introduzamos os sub-módulos sucessivos $\mathfrak{M}_{p-1}$, $\mathfrak{M}_{p-2}, \ldots, \mathfrak{M}_0 = (0)$, cada um dos quais sub-módulo máximo no anterior (admite-se, é claro, que isso é possível). A série

$$\left\{ \mathfrak{M} = \mathfrak{M}_p \supset \mathfrak{M}_{p-1} \supset \mathfrak{M}_{p-2} \supset \cdots \supset \mathfrak{M}_0 = (0) \right\}$$

é uma série de composição. Por meio de escolhas apropriadas dos elementos base, que se admitem também possíveis, as matrizes A da representação tomarão as formas sucessivas

$$\begin{pmatrix} P & Q \\ 0 & R \end{pmatrix}, \qquad \begin{pmatrix} P_1 & Q_1 & & (Q) \\ 0 & R_1 & & \\ & (0) & & (R) \end{pmatrix}, \text{ etc.},$$

até se chegar à expressão final

$$A' = \begin{pmatrix} P_{11} & P_{12} & \cdots & P_{1p} \\ 0 & P_{22} & \cdots & P_{2p} \\ \hline 0 & 0 & \cdots & P_{pp} \end{pmatrix}.$$

As matrizes P_{pp} são matrizes de representação no espaço $\mathfrak{M}/\mathfrak{N} = \mathfrak{M}_p/\mathfrak{M}_{p-1}$, as matrizes $P_{p-1,p-1}$ são matrizes de representação no espaço $\mathfrak{M}_{p-1}/\mathfrak{M}_{p-2}$, e assim, até P_{11}, que são as matrizes de representação no espaço $\mathfrak{M}_1/\mathfrak{M}_0 = \mathfrak{M}_1$. Todos os P_{ii} constituem sistemas irredutíveis de representação, por-

que os $\mathfrak{M}_i/\mathfrak{M}_{i-1}$ são grupos simples. O teorema de Jordan-Hölder garante-nos que os factores de composição $\mathfrak{M}_i/\mathfrak{M}_{i-1}$ são univocamente determinados, desde que se ponham de parte isomorfias e a ordem dos grupos isomorfos. E como a módulos de representação isomorfos correspondem representações equivalentes, podemos afirmar: pondo de parte a ordem e a equivalência, as representações irredutíveis definidas pelos P_{ii} são univocamente determinadas.

Pode suceder que nas fórmulas (11) faltem os u_i nas expressões dos av_i, isto é, que se anulem as matrizes Q. Os v_i definirão também um sub-módulo duplo invariante, $\mathfrak{N}' = v_1\mathfrak{o} + \cdots + v_r\mathfrak{o}$, as matrizes A tomarão o aspecto

$$A = \begin{pmatrix} P & 0 \\ 0 & R \end{pmatrix},$$

e o módulo $\mathfrak{M}$, como o mostra a última das igualdades (10), é uma soma directa: $\mathfrak{M} = \mathfrak{N} + \mathfrak{N}'$. Diz-se, neste caso, que a representação $\mathcal{G}$ se decompõe nas duas representações $\mathcal{G}'$ e $\mathcal{G}''$, determinadas por P e R, respectivamente, nos espaços $\mathfrak{N}$ e $\mathfrak{N}'$, escrevendo-se mesmo $\mathcal{G} = \mathcal{G}' + \mathcal{G}''$. Estas últimas podem, por sua vez, ter a mesma propriedade de $\mathcal{G}$. Quando for possível chegar a estabelecer para as matrizes A a expressão

$$A = \begin{pmatrix} P_{11} & 0 & \cdots & 0 \\ 0 & P_{22} & \cdots & 0 \\ 0 & 0 & & P_{pp} \end{pmatrix};$$

de tal sorte que as representações definidas pelos P_{ii} sejam irredutíveis, diz-se que $\mathcal{G}$ é completamente redutível e escreve-se $\mathcal{G} = \mathcal{G}_1 + \cdots + \mathcal{G}_p$.

Se o anel $\mathfrak{o}$ for um corpo, realizam-se as diferentes hipóteses relativas à existência de bases para os diferentes sub-módulos.

No caso de redutibilidade completa, $\mathfrak{M}$ é soma directa de módulos simples, portanto, completamente redutível: $\mathfrak{M} = \mathfrak{M}_1 + \cdots + \mathfrak{M}_p$. Então, a cada sub-módulo invariante $\mathfrak{N}$ corresponde um sub-módulo invariante $\mathfrak{N}'$ tal que $\mathfrak{M} = \mathfrak{N} + \mathfrak{N}'$. Esta propriedade é característica da completa redução, como vamos ver. Se $\mathfrak{N}$ for um sub-módulo máximo de $\mathfrak{M}$, ponhamos $\mathfrak{M} = \mathfrak{N} + \mathfrak{N}'$. Em seguida, se $\mathfrak{P}$ é um sub-módulo máximo de $\mathfrak{N}$, escrevamos $\mathfrak{M} = \mathfrak{P} + \mathfrak{Q}$. Consideremos aqui apenas os elementos de $\mathfrak{M}$ que pertencem a $\mathfrak{N}$ e tomemos os elementos de $\mathfrak{Q}$ que entram na sua decomposição. Vê-se fàcilmente que esses elementos constituem um sub-módulo admissível, tendo-se $\mathfrak{N} = \mathfrak{P} + \mathfrak{Z}$, $\mathfrak{M} = \mathfrak{P} + \mathfrak{Z} + \mathfrak{N}'$. O raciocínio prossegue-se com $\mathfrak{P}$, até encontrar parcelas sem sub-espaços invariantes ($\mathfrak{Z}$ e $\mathfrak{N}'$ estão já nesse caso).

14) Representações dos grupos e dos sistemas hiper-complexos - Numa representação dum grupo $\mathcal{G}$, o módulo de representação $\mathfrak{M}$ admitirá $\mathcal{G}$ como domínio operatório. Cada $g \in \mathcal{G}$ induz em $\mathfrak{M}$ um endomorfismo operatório relativamente a $\mathfrak{o}$, valendo ainda a relação $g.m\lambda = gm.\lambda$. As definições de representações equivalentes, de redutibilidade e de irredutibilidade transportam-se imediatamente para este caso.

Passemos do grupo $\mathcal{G}$, suposto finito, à álgebra $\mathcal{A}$ do mesmo, para a qual o corpo fundamental é o corpo $\mathfrak{o}$ em que vai fazer-se a representação do grupo, ou, pelo menos, é um corpo $\mathfrak{P}$ contido no centro $\mathfrak{z}$ do anel de representação. Esta será uma parte da representação de $\mathcal{A}$, obtida fazendo corresponder a cada elemento $\sum g_i\lambda_i \in \mathcal{A}$ a matriz $\sum A_i\lambda_i$, na qual A_i corresponde a g_i. Vê-se que, por este último processo, se tem, com efeito, uma representação de $\mathcal{A}$, pois ao produto $\sum_i g_i\lambda_i \cdot \sum_k g_k\mu_k = \sum_{ik} g_ig_k\lambda_i\mu_k$ corresponderá a matriz $\sum_{ik} A_iA_k\lambda_i\mu_k = \sum_i A_i\lambda_i \cdot \sum_k A_k\mu_k$, visto serem $\lambda_i, \mu_k \in \mathfrak{P}$. Vê-se também que tem lugar o homomorfismo operatório referido no § 1.

15) Caso em que $\mathcal{G}$ tem elemento um - O módulo $\mathfrak{M}$ de representação, a que temos sempre aludido, foi imaginado como módulo finito com respeito a $\mathfrak{o}$, para o qual o elemento um deste último é operador unitário. Suponhamos que $\mathcal{G}$ tem igualmente elemento um = U. Dado $m \in \mathfrak{M}$, ponhamos $m = (m - Um) + Um$.

(1) A demonstração exige diferentes hipóteses que se supõem realizadas.

Sob esta forma aparece $\mathfrak{M}$ como soma directa $\mathfrak{M} = \mathfrak{M}'' + \mathfrak{M}'''$, mas importa ver se as parcelas são módulos admissíveis em face de $\mathfrak{A}$. A resposta é afirmativa, como o mostram as igualdades $Um.\lambda = U.m\lambda \in \mathfrak{M}'''$, $(m - Um)\lambda = m\lambda - U.m\lambda \in \mathfrak{M}''$.

Quanto a um módulo recíproco de representação, a conclusão é a mesma: $\lambda.Um = U.\lambda m \in \mathfrak{M}'''$, $\lambda(m - Um) = \lambda m - U.\lambda m \in \mathfrak{M}''$.

Admitamos que $\mathfrak{M}''$ e $\mathfrak{M}'''$ são módulos finitos relativamente a $\mathfrak{A}$. A representação decompõe-se em duas, $\mathfrak{H}''$ e $\mathfrak{H}'''$, a primeira das quais faz corresponder a matriz nula a todo o elemento de $\mathcal{T}$, enquanto que a segunda faz corresponder a matriz unidade ao elemento $U \in \mathcal{T}$.

De futuro serão tratados casos em que a representação se reduz a $\mathfrak{H}''' = \mathfrak{H}$ (pertencente a $\mathfrak{M}'' = \mathfrak{M}$). Imaginemos, nessa hipótese, que $\mathcal{T}$ tem uma decomposição bilateral, $\mathcal{T} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_s$, $(U = e_1 + \cdots + e_s)$. Podemos, então, escrever

$$\mathfrak{M} = \mathcal{T}\mathfrak{M} = (\mathfrak{a}_1\mathfrak{M}, \ldots, \mathfrak{a}_s\mathfrak{M}),$$

onde, bem entendido, $\mathcal{T}\mathfrak{M}$ representa o conjunto de elementos da forma Σsm, $(s \in \mathcal{T};\ m \in \mathfrak{M})$. Cada $\mathfrak{a}_i\mathfrak{M}$ é um sub-módulo admissível em face de $\mathcal{T}$ e de $\mathfrak{A}$. A decomposição supra é, de resto, directa: $\mathfrak{M} = \mathfrak{a}_1\mathfrak{M} + \cdots + \mathfrak{a}_s\mathfrak{M}$. Basta notar, com efeito, que uma relação $(a_1 m_1 + \cdots + a_1' m_1') + \cdots + (a_s m_s + \cdots + a_s' m_s') = 0$, $(a_1, \ldots, a_1' \in \mathfrak{a}_1;\ \ldots;\ a_s, \ldots, a_s' \in \mathfrak{a}_s)$, dá, multiplicando por e_i, $a_i m_i + \cdots + a_i' m_i' = 0$.

Admitindo a existência de bases para os diferentes sub-módulos, a representação $\mathfrak{H}$ pode considerar-se como uma soma de representações. Cada uma destas últimas, pondo de parte elementos de $\mathcal{T}$ que nela são representados pela matriz nula, é uma representação dum anel com elemento um, na qual a este último, como se quer, corresponde a matriz unidade.

Caso importante é aquele em que as parcelas $\mathfrak{a}_i$ da decomposição de $\mathcal{T}$ são ideais bilaterais indecomponíveis.

16) Representações de anéis semi-simples - Seja $\mathcal{T} = \mathcal{L} = \mathcal{K} = \mathcal{L}$ um anel simples completamente redutível, com elemento um. As considerações do § 7 levaram-nos à igualdade $\mathcal{K}_1 = \mathcal{O}_{\mathcal{L}}$. Estamos, deste modo, em presença duma representação directa isomorfa de $\mathcal{T}$ por meio de $\mathcal{O}_{\mathcal{L}}$, ou num corpo $\mathcal{F}$ isomorfo do corpo

dos endomorfismos - $\mathcal{L}$ à direita dum ideal esquerdo simples (corpo que representaremos por Δ). É conveniente entrarmos novamente em contacto com os raciocínios do § 4, os quais, conjuntamente com os do § 7, nos levaram à conclusão assinalada. Partindo de

$$\mathcal{T} = \mathcal{L} = \mathfrak{N}_1 + \cdots + \mathfrak{N}_n, \qquad (t = f_1 + \cdots + f_n), \tag{13}$$

onde $t \in \mathcal{T}$, $f_i \in \mathfrak{N}_i$, o endomorfismo - $\mathcal{L}$, representado por G_1, determina a correspondência $t \to f_1 = tG_1$. Em particular é $u \to \rho_1 = uG_1$. Vê-se, assim, que $t = tu \to t\rho_1 = f_1$, $\rho_1 = \rho_1 u \to \rho_1\rho_1 = \rho_1$. Pondo $\rho_1 = e_{11} = e_1$, conclui-se que, no isomorfismo $(\mathcal{T} =)\ \mathcal{K} \cong \mathcal{K}_1$, se tem $e_{11} \to G_{11} = G_1$. Do mesmo modo se prova $e_{ii} \to G_i$. As matrizes unidades G_{ij} são correspondentes dum certo sistema de matrizes unidades e_{ij} (como é evidente a priori), mas pode precisar-se que estas últimas se derivam da decomposição de $\mathcal{T}$ de que se partiu e levou aos G_{ij}. Por ex.: a partir dum certo isomorfismo $\mathfrak{N}_1 \cong \mathfrak{N}_i$ definiu-se Δ_{i1}. O mesmo isomorfismo é definido por um elemento $e_{1i} \in \mathcal{T}_{1i}$. Quando se escreve $G_{1i} = G_1\Delta_{i1}$, o endomorfismo G_{1i} passa a aplicar-se a todos os elementos de $\mathcal{T}$. O mesmo sucede com e_{1i}, tendo-se

$$te_{1i} = (f_1 + \cdots + f_n)e_{1i} = f_1 e_{1i} = tG_1\Delta_{i1} = tG_{1i}.$$

Posto isto, escrevamos, em correspondência com (13),

$$\mathcal{K}_1 = \mathcal{O}_{\mathcal{L}} = \mathcal{J}_1 + \cdots + \mathcal{J}_n.$$

O ideal esquerdo simples $\mathcal{J}_1$ tem uma base de n elementos $G_{11}, \ldots, G_{n1}$, enquanto que $\mathfrak{N}_1$ tem a base $e_{11}, \ldots, e_{n1}$. Ponhamos

$$\sigma = \sum_{kj} G_{kj}T_{kj}, \qquad s = \sum_{kj} e_{kj}a_{kj}, \qquad (\sigma \in \mathcal{O}_{\mathcal{L}},\ s \in \mathcal{T}), \tag{14}$$

com $T_{kj} \in \mathcal{T}$ e a_{kj} pertencente ao corpo dos elementos de $\mathcal{T}$ comutáveis com os e_{kj} (a que chamaremos $\mathcal{L}$). Tem-se

$$\sigma G_{11} = \sum_{R,j} G_{Rj} T_{Rj} \cdot G_{11} = \sum_{R} G_{R1} T_{R1},$$

$$s e_{11} = \sum_{R} e_{R1} a_{R1} = \sum_{R} e_{R1} \lambda_{R1} \cdot \qquad (15)$$

Para se fazer a substituição de a_{Rl} por $\lambda_{Rl} \in \Lambda$ raciocina-se como segue. No isomorfismo $\mathcal{L} \cong \mathcal{Y}_{11}$, a_{Rl} é correspondente de $e_{11} a_{Rl} e_{11} = e_{1R} s e_{11}$. Ora tem-se $e_{R1} a_{Rl} = e_{RR} s e_{11} = e_{R1} \cdot e_{1R} s e_{11}$, de sorte que a substituição em (15), dos a_{Rl} pelos seus correspondentes em $\mathcal{Y}_{11}$ é imediata. A passagem destes últimos aos λ_{Rl} resulta simplesmente do facto de cada endomorfismo - $\mathcal{L}$, de $\mathcal{U}_1$, ser definido por um elemento de $\mathcal{Y}_{11}$ à direita de $\mathcal{U}_1$. Podemos enunciar o seguinte

Teorema 1 :- Aos ideais esquerdos simples dum anel simples $\mathcal{Y}$ completamente redutível, com elemento um, pertencem representações isomorfas directas irredutíveis de $\mathcal{Y}$. O corpo de representação é o corpo dos endomorfismos - $\mathcal{Y}$ (ou $\mathcal{L}$) = à direita de cada um daqueles ideais. Cada ideal esquerdo simples é módulo duplo para o qual, além de $\Lambda = \mathcal{O}_{1\mathcal{L}}$, tem lugar $\mathcal{L}_1 = \mathcal{Y}_1 = \mathcal{O}_{1\Lambda}$. Por meio da igualdade (15) ficamos a conhecer a matriz correspondente de s: é precisamente a matriz dos elementos que figuram como coeficientes na representação bem determinada (14), de s. Cada elemento s define um endomorfismo - Λ e elementos diferentes de $\mathcal{Y}$ levam a endomorfismos diferentes. $\mathcal{Y}_1$ é imagem anti-isomorfa de $\mathcal{Y}$. Como se obtêm todos os elementos de $\mathcal{O}_{1\Lambda}$, segue-se $\mathcal{Y}_1 = \mathcal{O}_{1\Lambda}$.

Passando de ideais esquerdos simples a ideais direitos simples, podemos dizer, tendo em conta a igualdade $\mathcal{L}_1 = \mathcal{O}_R$ e outros raciocínios análogos aos anteriores:

Teorema 2 :- Aos ideais direitos simples dum anel simples $\mathcal{Y}$ completamente redutível, com elemento um, pertencem representações anti-isomorfas (recíprocas) irredutíveis de $\mathcal{Y}$. O corpo de representação é o corpo dos endomorfismos - $\mathcal{Y}$ (ou $\mathcal{R}$) = = Σ à direita de cada um daqueles ideais. Cada ideal direito simples é módulo duplo para o qual, além de $\Sigma = \mathcal{O}_{\mathcal{R}}$, tem lugar $\mathcal{R}_1 = \mathcal{Y}_1 = \mathcal{O}_{1\Sigma}$.

Devemos dizer ainda que, em correspondência com $\mathcal{R}_1' = \mathcal{O}_{\mathcal{L}}'$, a um ideal esquerdo pode fazer-se pertencer uma representação recíproca, e que, em correspondência com $\mathcal{L}_1' = \mathcal{O}_{\mathcal{R}}'$, a um ideal direito pode fazer-se pertencer uma representação directa.

Um enunciado mais geral que o do teorema 1 é o deste

Teorema 3 :- Dado um ideal esquerdo qualquer dum anel simples $\mathcal{Y}$ (1), pertence ao mesmo uma representação directa completamente redutível com Λ como corpo de representação. O corpo Λ tem uma imagem homomorfa no anel $\mathcal{O}_{\mathcal{L}} = \mathcal{O}_{\mathcal{R}'}$ dos endomorfismos - $\mathcal{L}$ do ideal, e este anel $\mathcal{O}_{\mathcal{L}}$ é um anel completo de matrizes com elementos dum corpo isomorfo de Λ. O grau destas últimas matrizes é dado pelo número de ideais esquerdos simples em que pode decompôr-se o ideal dado (Veja-se o tomo I, pgs. 147).

Postas estas considerações, tomemos um módulo $\mathcal{M}$ que seja finito relativamente a um anel semi-simples $\mathcal{Y}$. Tanto $\mathcal{M}''$ como $\mathcal{M}'''$ são módulos finitos relativos a $\mathcal{Y}$ (§ 1 do Cap. IV). Tomemos $\mathcal{M} = \mathcal{M}'''$. Sabemos, então, que é $\mathcal{M} = \Sigma \mathcal{W}_i m_{Ri}$, onde os $\mathcal{W}_i$ são ideais esquerdos simples de $\mathcal{Y}$ e a soma é directa. Cada parcela é um sub-módulo relativo a $\mathcal{Y}$, de sorte que, se $\mathcal{M}$ se supõe directamente indecomponível, fica idêntico a um módulo $\mathcal{W}_i m_{Ri}$, operatòriamente isomorfo de $\mathcal{W}_i$ (2). Os endomorfismos - $\mathcal{Y}$, de $\mathcal{M}$ e $\mathcal{W}_i$, constituem corpos Ω e Λ (ou $\mathcal{O}_{1\Sigma}$), que são isomorfos. Tanto $\mathcal{M}$ como $\mathcal{W}_i$ são módulos duplos relativamente a $\mathcal{Y}$ e aos corpos endomórficos correspondentes. Trata-se ainda de módulos de representação, no sentido que vai precisar-se. Raciocinemos com $\mathcal{W}_1 = \mathcal{Y} e_1 = \mathcal{Y} e_{11}$, em vez de $\mathcal{W}_i$, e tenhamos em conta a decomposição de $\mathcal{Y}$ em anéis simples: $\mathcal{Y} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_s$. Se $\mathcal{W}_1 \cong \mathfrak{a}_1$, a aplicação dum $\mathfrak{a}_i (i \neq 1)$ a $\mathcal{W}_1$ leva ao elemento nulo. Basta tratarmos a aplicação a $\mathcal{W}_1$ dos elementos de $\mathfrak{a}_1$. Ora, para $\mathfrak{a}_1$, a questão foi já tratada. Para o anel semi-simples $\mathcal{Y}$ encontram-se tantas representações irredutíveis distintas (não equivalentes) quantos os ideais esquerdos simples não isomorfos ou quantos os anéis simples da decomposição de $\mathcal{Y}$. É válido o seguinte

(1) Simples (subentende já completamente redutível, com elemento um).

(2) Observe-se que o módulo, para a hipótese de ser inicialmente simples, quando não se anula para todos os elementos de $\mathcal{Y}$, é necessàriamente um módulo finito (e com um elemento base !).

Teorema 4 :- Dado um anel semi-simples $\mathcal{Y}$, a um módulo simples esquerdo relativo a $\mathcal{Y}$ pertence uma representação directa irredutível, para a qual o corpo de representação é isomorfo do corpo dos endomorfismos - $\mathcal{Y}$ do referido módulo (à direita). O número de representações irredutíveis não equivalentes nestas condições é igual ao número de anéis simples em que pode decompor-se $\mathcal{Y}$.

Voltemos à representação irredutível dum anel simples $\mathcal{Y}$ pertencente a $\mathcal{M}_1$. Se o corpo $\Lambda = \mathcal{O}_{i\Omega}$ é uma ampliação finita dum corpo Γ, isto é, se é possível encontrar r elementos $\lambda_1, \ldots, \lambda_r$ de Λ, tais que os elementos de Λ se exprimem sob a forma $\lambda = \lambda_1 c_1 + \ldots + \lambda_r c_r$, $(c_i \in \Gamma)$, com a hipótese de os λ_j serem independentes relativamente a Γ, podemos obter como segue uma representação do anel simples $\mathcal{Y}$, em Γ. O espaço $\mathcal{M}_1$ é de ordem nr com respeito a Γ, pois que, da relação

$$\sum_{pq} e_{p1}\, \lambda_q \cdot c_{pq} = 0,$$

tira-se sucessivamente

$$\sum_{pq} e_{p1}\, \lambda_q\, c_{pq} = \sum_{p} e_{p1} \cdot \sum_{q} \lambda_q c_{pq} = 0, \quad \sum_{q} \lambda_q\, c_{pq} = 0, \quad c_{pq} = 0.$$

A aplicação dum elemento de $\mathcal{Y}$ aos elementos base $e_{p1}\lambda_q$, resulta tendo em conta que Λ é um módulo de representação de si mesmo, quando o corpo de representação é Γ. Nesta última representação, ao elemento $\lambda \in \Lambda$ corresponde a matriz $C = (c_{ij})$, definida por igualdades da forma

$$\lambda \lambda_m = \sum_{k=1}^{r} \lambda_k c_{km}, \qquad (m = 1, \ldots, r),$$

as quais resultam da estrutura do corpo Λ. Recorramos às igualdades (15). Vem, operando intermediàriamente com os elementos do corpo dos a_{kj} (substituindo, portanto, λ_q por a_q):

$$s \cdot e_{i1}\, \lambda_q = s \cdot e_{i1} a_q = s e_{i1} \cdot a_q = \sum_{k} e_{k1} \cdot a_{ki} a_q = \sum_{k} e_{k1} \lambda_{ki} \lambda_q,$$

$$\lambda_{ki} \lambda_q = \sum_{m=1}^{r} \lambda_m c_{mq}^{(ki)}, \qquad (q = 1, \ldots, r);$$

e, por consequência,

$$s \cdot e_{i1} \lambda_q = \sum_{k,m} e_{k1}\, \lambda_m \cdot c_{mq}^{(ki)}.$$

Assim, a matriz de grau nr, com elementos de Γ, representante de s, constroi-se por via deste

Teorema 5:- A matriz que representa s, por meio de Γ, obtém-se substituindo os elementos λ_{ki}, da matriz que representa s por meio de Λ, por matrizes $C^{(ki)}$, que representam λ_{ki} por meio de Γ.

Façamos algumas observações. 1ª)-A representação referida no teorema 5 é ainda irredutível, como se reconhece tendo em conta que $\mathcal{M}_1$ continua a ser simples relativamente a $\mathcal{Y}$. 2ª)-Todos os resultados obtidos com o tratamento dado a $\mathcal{M}_1$ subsistem, é claro, com a mesma forma, quando $\mathcal{M}_1$ se substitui por um módulo simples $\mathcal{M}$ relativamente a $\mathcal{Y}$. 3ª)-Continuando a admitir que $\mathcal{M}$ é simples relativamente ao anel simples $\mathcal{Y}$, suponhamo-lo módulo de representação, com um corpo qualquer $\mathcal{K}$ como corpo de representação. Vamos ver que não se introduz representação nova. $\mathcal{K}$ tem, com efeito, uma imagem homomorfa $\mathcal{K}_1$ no anel dos endomorfismos - $\mathcal{Y}$ à direita de $\mathcal{M}$. Essa imagem é isomorfa, porque, se u_1 pertencer à base de $\mathcal{M}$, só pode ter-se $u_1 k = u_1 k'$, com $k, k' \in \mathcal{K}$, se for $k = k'$ (resultado que aliás é válido numa representação qualquer por meio dum corpo). Tira-se daqui que $\mathcal{M}$ é finito relativamente a $\mathcal{K}_1$, e que, portanto, $\Omega = \mathcal{O}_{i\omega}$ é ampliação finita de $\mathcal{K}_1$. Efectivamente, se o não fosse, a ordem de $\mathcal{M}$ com respeito a $\mathcal{K}_1$ não seria finita. 4ª)-Se o módulo finito $\mathcal{M}$ relativo a $\mathcal{Y}$ não é simples, pode suceder que, considerado como módulo de representação (introduzindo, pois, em $\mathcal{M}$, os operadores elementos do corpo de representação $\mathcal{K}$), seja um módulo simples. A representação irredutível correspondente não entrará nas que foram estudadas neste §. Que uma tal hipótese é de formular, constata-se supondo $\mathcal{M} = \mathcal{K}$ uma ampliação finita dum sub-corpo $\mathcal{K}'$. Então, $\mathcal{K}$ é um módulo de representação de base dada pelo elemento um, no qual os elementos de $\mathcal{K}'$ operam à esquerda (por ex.) e os de $\mathcal{K}$ operam à direita.

17) Caso em que existe domínio operatório para $\mathcal{T}$ - Se, mantendo as hipóteses do § anterior, existe um domínio operatório $\mathcal{O}$, para o anel simples $\mathcal{T}$, comutativamente ligado a $\mathcal{T}$[1], quais são as representações de $\mathcal{T}$ pertencentes a módulos simples relativamente a $\mathcal{T}$, mas sob a condição das seguintes correspondências: $s \to S$, $s\rho \to S\rho$? Tomemos um ideal esquerdo $\mathcal{U}_1$ (o qual é admissível em face de $\mathcal{O}$). Vamos ver que a representação pertencente a $\mathcal{U}_1$ satisfaz à nova exigência aqui feita. Consideremos $\mathcal{L}$, em vez de Λ, como corpo de representação. Tem-se $sf_1 \cdot \rho = s\rho \cdot f_1 = s \cdot f_1\rho$, e, portanto,

$$s\rho \cdot e_{i1} = se_{i1} \cdot \rho = \sum_k e_{k1} a_{ki} \cdot \rho = \sum_k e_{k1} \cdot a_{ki}\rho ,$$

donde se conclui que, efectivamente, $s\rho$ e $S\rho$ se correspondem. Supondo $\mathcal{L}$ ampliação finita dum corpo $\mathcal{K}$, as igualdades

$$s \cdot e_{i1} a_q = \sum_{k,m} e_{k1} a_m \cdot c_{mq}^{(ki)}, \qquad (a_q \in \mathcal{L},\ c_{mq}^{(ki)} \in \mathcal{K}),$$

$$s\rho \cdot e_{i1} a_q = (s \cdot e_{i1} a_q)\rho = \sum_{k,m} e_{k1} a_m \cdot c_{mq}^{(ki)} \rho,$$

nas quais figuram os a_q que constituem a base de $\mathcal{L}$ relativamente a $\mathcal{K}$, mostram que a representação é ainda a mesma que no § anterior, sob a condição de os operadores $\rho \in \mathcal{O}$ levarem a elementos de $\mathcal{K}$, sempre que se aplicam a elementos de $\mathcal{K}$. Podemos enunciar o seguinte

Teorema:- Se um anel semi-simples está comutativamente ligado a um domínio operatório $\mathcal{O}$, a todo o módulo simples $\mathcal{M}$ relativo a $\mathcal{T}$, para o qual valem $sm \cdot \rho = s\rho \cdot m = s \cdot m\rho$ pertencem representações irredutíveis de $\mathcal{T}$. Os elementos de $\mathcal{O}$ operam necessàriamente sobre o módulo e sobre o corpo de representação. Este último, se não é o corpo dos endomorfismos - $\mathcal{T}(=\mathcal{L})$ à direita de $\mathcal{M}$, é um seu sub-corpo $\mathcal{K}$. As representações em causa são operatòriamente homomorfas relativamente a $\mathcal{O}$, sob a condição de os elementos de $\mathcal{O}$ aplicados a $\mathcal{K}$ levarem a elementos de $\mathcal{K}$. Inversamente, toda a representação irredutível dum anel semi-simples $\mathcal{T}$ com um domínio operatório $\mathcal{O}$, pertencente a um módulo simples relativamente a $\mathcal{T}$, e que é operatória homomorfa relativamente a $\mathcal{O}$, é uma representação pertencente a um ideal esquerdo simples de $\mathcal{T}$, para a qual o corpo de representação é isomorfo dum sub-corpo do corpo dos endomorfismos - $\mathcal{T}$ do ideal.

(1) O domínio $\mathcal{O}$ não carece de ser comutativo. Basta que esteja comutativamente ligado a $\mathcal{T}$, conforme a definição geral: $(st)\rho = (s\rho)t = s(t\rho)$.

18) Sobre as representações dos anéis semi-primários - Seja $\mathcal{M}$ um módulo simples com respeito a um anel semi-primário $\mathcal{T}$ de radical nilpotente (anel -A especial). O radical $\mathcal{R}^* = \mathcal{R}$ verifica a condição $\mathcal{R}\mathcal{M} = (0)$, visto que, de contrário, seria $\mathcal{M} = \mathcal{R}\mathcal{M} = \ldots = \mathcal{R}^s\mathcal{M} = (0)$. É, portanto, equivalente considerar $\mathcal{M}$ como um módulo com respeito a $\mathcal{T}$ ou com respeito ao anel semi-simples $\mathcal{T}/\mathcal{R}$. Sabemos construir as representações irredutíveis de $\mathcal{T}$ pertencentes a módulos simples relativamente a $\mathcal{T}$, qualquer que seja o corpo de representação. O mesmo se diz, no caso de haver domínio operatório $\mathcal{O}$. Podemos enunciar as proposições a seguir:

Teorema:- Se um módulo $\mathcal{M}$ relativo a um anel semi-primário $\mathcal{T}$ com radical nilpotente admite uma série de composição, os seus factores de composição ou são anulados por $\mathcal{T}$ ou são isomorfos de ideais esquerdos simples de $\mathcal{T}/\mathcal{R}$.

Teorema:- Um módulo simples relativo a um anel $\mathcal{T}$ com condição dupla de cadeia é isomorfo dum ideal esquerdo simples de $\mathcal{T}/\mathcal{R}$ e isomorfo dum factor de composição da série de composição entre $\mathcal{T}$ e $\mathcal{R}$.

19) Sobre as representações dum anel qualquer - Antes de enunciarmos as duas proposições que temos em vista, relativas a representações dum anel qualquer, não queremos deixar de nos referir a uma terminologia que pode ser usada e se liga imediatamente às considerações dos §§ 3 e 5. Tomemos um grupo

qualquer $\mathcal{G}$. O conjunto dos seus endomorfismos diz-se absoluto dos endomorfismos de $\mathcal{G}$. Um sistema de operadores tem uma imagem no absoluto. Esse sistema diz-se um sub-absoluto, se a imagem é biunívoca. No caso dum módulo relativo a um anel $\mathcal{Y}$ (que opera à direita), $\mathcal{Y}$ não é geralmente um sub-absoluto. Se $\mathcal{O}$ é o absoluto do módulo, da imagem homomorfa $\mathcal{G}_1 \cong \mathcal{O}$, de $\mathcal{Y}$, passa-se a um isomorfismo anular $\mathcal{G}_1 \cong \mathcal{Y}/\mathfrak{a} = \mathcal{T}$. Este último é um sub-absoluto. O anel $\mathcal{O}_{\mathcal{Y}}$ é também um sub-absoluto.

Imaginemos em seguida que $\mathcal{G}$ se considera um grupo com um sistema $\mathcal{L}$ de operadores. Chamaremos absoluto - $\mathcal{L}$, de $\mathcal{G}$, o conjunto dos endomorfismos - $\mathcal{L}$. Um novo sistema $\mathcal{L}$, de operadores de $\mathcal{G}$, não tem, geralmente, imagem no absoluto - $\mathcal{L}$. Se $\Theta, \ldots \in \mathcal{L}$ e $\Theta', \ldots \in \mathcal{L}$, as igualdades da forma $\Theta'(\Theta g) = \Theta(\Theta' g)$ exprimem a condição necessária e suficiente para que essa imagem exista (os dois sistemas de operadores actuam à esquerda). Um sub-absoluto - $\mathcal{L}$ é um sistema de operadores com imagem biunívoca no absoluto - $\mathcal{L}$. Suponhamos, por ex., $\mathcal{M}$ um módulo simples com respeito a um anel $\mathcal{Y}$, que é um anel -A especial operando à esquerda de $\mathcal{M}$. Nesta definição, toma-se $\mathcal{L} = \mathcal{Y}$. Admitindo que $\mathcal{Y}\mathcal{M} \neq (0)$, sabemos que $\mathcal{M}$ se pode considerar módulo simples relativamente ao anel semi-simples $\mathcal{Y}/\mathcal{R} = \mathcal{Y}'$ e que tem lugar o isomorfismo $\mathcal{M} \cong \mathcal{M}_1'$, onde $\mathcal{M}_1'$ é ideal esquerdo de $\mathcal{Y}'$ contido num ideal bilateral simples $\mathfrak{a}_1'$ da decomposição de $\mathcal{Y}'$ em anéis simples: Fazendo $\Sigma = \mathcal{O}_{\mathcal{M}} = \mathcal{O}_{\mathcal{M}}$, Σ é, por construção, o absoluto - $\mathcal{Y}$ (ou $\mathcal{Y}'$); mas estes anéis não são sub-absolutos - Σ. $\mathfrak{a}_1'$, pelo contrário, é já um tal sub-absoluto (é mesmo, num sentido geral, o absoluto - Σ).

Posto isto, seja $\mathcal{Y}$ um anel qualquer. Vamos limitar-nos às representações de $\mathcal{Y}$ por meio dum corpo $\mathcal{P}$ comutativamente ligado ao anel, que sejam operatórias homomorfas relativamente a $\mathcal{P}$. Se $\mathcal{L}$ é o anel de representação, consideremos o isomorfismo $\mathcal{Y}/\mathfrak{a} = \mathcal{Y}' \cong \mathcal{L}$. O ideal bilateral $\mathfrak{a}$, de $\mathcal{Y}$, é admissível em face de $\mathcal{P}$, pois tem-se, por hipótese, $s \to S$, $s\rho \to S\rho$, se $\rho \in \mathcal{P}$. Assim, $\mathcal{P}$ opera sobre $\mathcal{Y}'$ e estamos em presença duma representação fiel de $\mathcal{Y}'$ (este é um sub-absoluto - $\mathcal{P}$), operatória homomorfa relativamente a $\mathcal{P}$. Pondo em jogo apenas os ideais admissíveis, $\mathcal{Y}'$ é um anel com condição dupla de cadeia, portanto um anel -A especial. Tem lugar o seguinte

Teorema:- Toda a representação directa dum anel $\mathcal{Y}$ por meio dum corpo $\mathcal{P}$ comutativamente ligado a $\mathcal{Y}$, que seja operatória homomorfa relativamente a $\mathcal{P}$, é uma representação fiel dum anel -A especial comutativamente ligado ao mesmo corpo.

Em particular, se $\mathcal{P}$ é comutativo, $\mathcal{L}$ é um sistema hipercomplexo, com $\mathcal{P}$ como corpo fundamental. Vamos ver a este respeito que, sob uma condição muito geral, o corpo $\mathcal{P}$, referido no teorema anterior, não pode deixar de ser comutativo. Daremos o seguinte enunciado:

Teorema:- Uma representação directa dum anel $\mathcal{Y}$ comutativamente ligado a um corpo $\mathcal{P}$, por meio de $\mathcal{P}$, que seja operatória homomorfa relativamente a $\mathcal{P}$, se as representações irredutíveis que aparecem em escada diagonal, quando se procede à redução da representação, não forem todas a representação nula, é uma representação dum sistema hiper-complexo com $\mathcal{P}$ como corpo fundamental. A demonstração do teorema consiste, como já se disse, em provar que o corpo $\mathcal{P}$ é comutativo. Consideremos uma representação irredutível diagonal, diferente da representação nula. Ela é uma representação irredutível fiel dum anel -A especial (que chamaremos $\mathcal{Y}'$), dada por um corpo $\mathcal{P}$ ligado comutativamente ao anel e que opera sobre o módulo de representação $\mathcal{M}$. Se $\mathcal{R}'$ for o radical de $\mathcal{Y}'$, é fácil de ver que $\mathcal{R}'\mathcal{M}$ é sub-módulo admissível em face de $\mathcal{Y}'$ e de $\mathcal{P}$. Basta ter em conta a igualdade

$$\sum r'm.\rho = \sum r'\rho.m \,, \qquad (r' \in \mathcal{R}', \ \rho \in \mathcal{P}, \ m \in \mathcal{M}),$$

que resulta do homomorfismo operatório da representação. Em virtude de ser $\mathcal{R}'\mathcal{M} = (0)$, vê-se que é $\mathcal{R}' = (0)$, de modo que o anel -A especial é aqui semi-simples (mesmo simples, pelas razões abaixo). O elemento $um = U$, de $\mathcal{Y}'$, é operador unitário de $\mathcal{M}$, pois, se o não fosse, ter-se-ia $m = Um + (m - Um)$, ou seja $\mathcal{M} = \mathcal{M}' + \mathcal{M}''$. Tanto $\mathcal{M}''$ como $\mathcal{M}'''$ seriam sub-módulos admissíveis em face de $\mathcal{Y}'$ e de $\mathcal{P}$, visto que $Um.\rho = U.m\rho$, $(m - Um)\rho = m\rho - U.m\rho$. Conclui-se agora que $\mathcal{M}$ é módulo simples relativamente a $\mathcal{Y}'$, dado que, se existisse $\mathcal{M}' \neq \mathcal{M}$, sob as condições $s'm' \in \mathcal{M}'$, $m'\rho \notin \mathcal{M}'$, viria $m'\rho = U.m'\rho = U\rho.m' \in \mathcal{M}'$,

o que é uma contradição. Realizam-se, assim, as diferentes exigências do § 17, no que toca a representações de anéis semi-simples com um domínio operatório. O corpo $\mathcal{P}$ de representação pode considerar-se sub-corpo do corpo Λ dos endomorfismos - $\mathcal{T}'$ dum ideal esquerdo de $\mathcal{T}'$. Se considerarmos a realização $\mathcal{T} = e\mathcal{T}'e$, de Λ, tem-se, para $\rho = et'e \in \mathcal{P}$,

$$es'e.\rho = e.(s'e)\rho = e\rho.s'e = e\rho e.s'e = e\rho.es'e = \rho.es'e .$$

Vê-se que $\mathcal{P}$ está contido no centro de $\mathcal{T}$ (ou de Λ), q. e. d.

Observação:- Se um anel $\mathcal{T}$, com um domínio operatório $\mathcal{O}$ comutativamente ligado ao anel, tem uma representação no corpo $\mathcal{P}$, homorfa relativamente a $\mathcal{O}$, no geral não podemos fazer corresponder à representação um módulo de representação para o qual $s\rho.m = s.m\rho = sm.\rho$. A teoria das representações que foi desenvolvida neste Capítulo só é válida quando o módulo existe. Assim, no teorema anterior, a existência de módulo de representação deve ser uma condição de hipótese. O módulo existe todas as vezes que $\mathcal{O}$ faz parte do centro de $\mathcal{P}$. Pode, neste sentido, precisar-se ainda o seguinte: se $\mathcal{T}$ tem elemento um, ao qual corresponde a matriz unidade, a existência do módulo de representação exige que $\mathcal{O}$ (suposto pertencente a $\mathcal{P}$) esteja contido no centro de $\mathcal{P}$. É o que se vê tendo em conta as relações

$$s\rho.u_l\alpha = (s\rho.u_l)\alpha = (su_l.\rho)\alpha , \qquad (\alpha \in \mathcal{P}),$$
$$s\rho.u_l\alpha = (s.u_l\alpha)\rho = (su_l.\alpha)\rho ,$$

e fazendo $s = U$ = elemento um de $\mathcal{T}$.

Capítulo IX

Representações de sistemas hiper-complexos

1) Generalidades - Seja $\mathcal{H}$ um sistema hiper-complexo de corpo fundamental $\mathcal{P}$. Só nos interessam as representações de $\mathcal{H}$ não nulas, que sejam homomorfas relativamente a $\mathcal{P}$. Este corpo deverá operar sobre o corpo de representação $\mathcal{A}$, que é ou não comutativo. Suporemos, por isso, $\mathcal{P}$ pertencente ao centro Z de $\mathcal{A}$. Se nos encontramos em frente duma representação de ordem n (recíproca, por ex.), tomemos um módulo $\mathcal{M} = \mathcal{A}(u_1, \ldots, u_n)$, finito relativamente a $\mathcal{A}$. Supondo (a_{lR}) a matriz da representação que corresponde a $a \in \mathcal{H}$, façamos operar $\mathcal{H}$ sobre $\mathcal{M}$ de tal sorte que[1]

$$a.\sum_l \lambda_l u_l = \sum_l \lambda_l (\sum_R a_{lR} u_R), \qquad (a_{lR}, \lambda_l \in \mathcal{A}).$$

Verificam-se as seguintes relações:

$$a.\lambda v = \lambda.av, \qquad (\lambda \in \mathcal{A}, \quad v = \sum_l \lambda_l u_l) .$$

E, supondo $\rho \in \mathcal{P}$, tem-se também

$$a\rho.\sum_l \lambda_l u_l = \sum_l \lambda_l (\sum_R \rho a_{lR} u_R) = \rho\Big(\sum_l \lambda_l (\sum_R a_{lR} u_R)\Big),$$

de sorte que valem as igualdades

$$a\rho.v = \rho.av = a.\rho v .$$

Daremos os seguintes enunciados:

Teorema 1:- Uma representação directa do sistema hiper-complexo $\mathcal{H}$, de corpo fundamental $\mathcal{P}$, no corpo não comutativo $\mathcal{A}$, de centro $Z \supseteq \mathcal{P}$, suposta homomorfa relativamente a $\mathcal{P}$,

(1) Que o leitor nos desculpe os raciocínios supérfluos !

pertence a um módulo de representação, que é módulo duplo relativamente a $\mathcal{L}$ e a $\mathcal{A}$, tal que se tem $a.v\lambda = av.\lambda$, $a.v\rho = av.\rho = a\rho.v$, onde $a \in \mathcal{L}$, $v \in \mathcal{M}$, $\lambda \in \mathcal{A}$, $\rho \in \mathcal{P}$.

Teorema 2:- Uma representação recíproca de $\mathcal{L}$ em $\mathcal{A}$, nas mesmas condições do teorema anterior, pertence a um módulo $\mathcal{M}$ para o qual $a.\lambda v = \lambda'.av$, $a.\rho v = \rho.av = a\rho.v$. Reciprocamente:

Teorema 3:- A todo o módulo $\mathcal{M} \neq (0)$ sobre o qual operam $\mathcal{L}$ e $\mathcal{A}$ (à esquerda, por ex.), que é finito relativamente a $\mathcal{A}$, e para o qual valem $a.\lambda v = \lambda.av$, $a.\rho v = \rho.av = a\rho.v$, pertence uma representação (neste caso recíproca) de $\mathcal{L}$ em $\mathcal{A}$, que é operatória homomorfa relativamente a $\mathcal{P}$.

Na hipótese de $\mathcal{A}$ ser comutativo, uma possível representação de $\mathcal{L}$ (não nula) torna-se imediatamente numa representação de $\mathcal{L}_{\mathcal{A}}$, ainda em $\mathcal{A}$. De facto, se $\mathcal{M}$ é módulo de representação directa de $\mathcal{L}$ em $\mathcal{A}$, aproveitando a circunstância de $\mathcal{A}$ ser comutativo, façamos $\mathcal{A}$ operar à esquerda de $\mathcal{M}$. Passa-se da representação directa para uma representação recíproca, mas, ao mesmo tempo, pode conceber-se $\mathcal{M}$ como um módulo esquerdo relativamente a $\mathcal{L}_{\mathcal{A}}$, que é módulo duplo relativamente a este último e a $\mathcal{A}$. Basta, para isso, definir $ak.v$, onde $k \in \mathcal{A}$, pelas relações $ak.v = a.kv = k.av$. Não se sabia, até aqui, o significado de $ak.v$, a não ser no caso em que $k = \rho \in \mathcal{P}$. Agora passa a ter-se para esse símbolo o significado $k.av$ $(= a.kv)$. E vê-se que a nova representação obtida, como deve ser exigido, é homomorfa relativamente a $\mathcal{P}$. Da representação recíproca de $\mathcal{L}_{\mathcal{A}}$, em $\mathcal{A}$, passa-se à representação directa, mudando $\mathcal{A}$, novamente, para a direita do módulo. Pode ver-se ainda que, se $e_1, \ldots, e_n$ constituirem uma base de $\mathcal{L}$, e se $M_1, \ldots, M_n$ forem as matrizes correspondentes dos e_i na representação inicial, basta representar cada elemento $\sum e_i k_i$, $(k_i \in \mathcal{A})$, pela matriz $\sum M_i k_i$, para se obter a representação ampliada. Podemos dar este enunciado:

Teorema 4:- Toda a representação dum sistema hiper-complexo num corpo comutativo $\mathcal{A}$, que contém o corpo fundamental, é uma parte da representação ampliada de $\mathcal{L}_{\mathcal{R}}$, em $\mathcal{A}$.

É assim que nos encontramos em face da questão seguinte: representar um anel $\mathcal{T}$, com condição dupla de cadeia e comutativamente ligado a um corpo $\mathcal{P}$, em $\mathcal{P}$, sob a condição de homomorfismo relativamente a $\mathcal{P}$. Esta questão, como vimos no final do Cap. anterior, é já um problema reduzido dum problema mais geral (se se tratar duma representação fiel).

Recordemos uma observação. Se $\mathcal{M}$ é um módulo com respeito a $\mathcal{T}$ e a $\mathcal{P}$, para o qual $a.v\rho = av.\rho = a\rho.v$, $(a \in \mathcal{T})$, todo o sub-módulo admissível em face de $\mathcal{T}$ e $\mathcal{P}$ satisfaz às mesmas igualdades.

Posto isto, tratemos representações diferentes da representação nula e comecemos pelas representações irredutíveis de $\mathcal{T}$ em $\mathcal{P}$. O módulo $\mathcal{M}$, ao qual pertence a representação, é simples com respeito a $\mathcal{T}$ e a $\mathcal{P}$. Vamos demonstrar que é simples relativamente a $\overline{\mathcal{T}} = \mathcal{T}/\mathcal{R}$, onde $\mathcal{R}$ é o radical de $\mathcal{T}$. De facto, $\mathcal{R}\mathcal{M}$ é um módulo relativamente a $\mathcal{T}$ (que opera à esquerda) e relativamente a $\mathcal{P}$ (que opera à direita). Não pode ter-se $\mathcal{M} = \mathcal{R}\mathcal{M}$, visto que isso arrastaria $\mathcal{M} = (0)$. Será $\mathcal{R}\mathcal{M} = (0)$. Como no final do Cap. anterior, a propósito do último teorema lá demonstrado, verifica-se agora que o módulo simples $\mathcal{M}$ relativo a $\overline{\mathcal{T}}$ e a $\mathcal{P}$ é módulo simples finito relativo a $\mathcal{T}$. Daqui se conclui o

Teorema 5:- As representações irredutíveis (não nulas) dum sistema hiper-complexo $\mathcal{L}$, no seu corpo fundamental $\mathcal{P}$, operatórias homomorfas relativamente a $\mathcal{P}$, são representações pertencentes a um ideal esquerdo simples do sistema hiper-complexo semi-simples $\overline{\mathcal{L}} = \mathcal{L}/\mathcal{R}$. Reciprocamente, a um tal ideal esquerdo corresponde uma representação irredutível não nula de $\mathcal{L}$, operatória homomorfa em face de $\mathcal{P}$. Quando $\mathcal{P}$ é algèbricamente fechado, identifica-se com o corpo dos endomorfismos - $\mathcal{T}$ à direita do ideal esquerdo aludido tanto na proposição directa como na inversa. Em todos os casos, o corpo dos endomorfismos é ampliação finita de $\mathcal{P}$.

Passemos agora às representações completamente redutíveis de $\mathcal{T}$ em, $\mathcal{P}$, sempre sob as hipóteses de $\mathcal{P}$ estar comutativamente ligado a $\mathcal{T}$ e de a representação ser homomorfa relativamente a $\mathcal{P}$. Dada uma tal representação, é claro que $\mathcal{T}$ não é geralmente, como sabemos, um sub-absoluto-$\mathcal{P}$. Não se tratando da representação nula, tem lugar o seguinte

Teorema 6:- Toda a representação completamente redutível dum anel $\mathcal{T}$ comutativamente ligado ao corpo comutativo $\mathcal{P}$ de representação (e homomorfa relativamente a $\mathcal{P}$) tem um sub-absoluto- $\mathcal{P}$ que é um sistema hiper-complexo sem radical. Se $\mathcal{T}/\mathfrak{a}$ é o sub-absoluto em causa, o seu radical, em cada representação irredutível, é representado pela matriz nula. A mesma circunstância terá lugar na representação global. Como se trata dum sub-absoluto, o radical será nulo.

Sob um ponto de vista inverso, consideremos um sistema hiper-complexo sem radical. Uma representação $\mathcal{G}$ dum tal sistema é uma representação dum anel semi-simples $\mathcal{T}$. Pelo facto de ser, por hipótese, s.m ρ = sm. ρ = s ρ.m, a decomposição $\mathfrak{M} = \mathfrak{M}'' + \mathfrak{M}'''$ leva a dois sub-módulos de representação. $\mathfrak{M}'''$, de elementos m - Um, é finito relativamente a $\mathcal{P}$. Decomposto em módulos simples relativamente a $\mathcal{P}$, tais módulos são ainda módulos de representação de $\mathcal{T} = \mathcal{L}_{\mathcal{T}}$ (para a representação nula). $\mathfrak{M}'''$ é, pois, completamente redutível. Relativamente a $\mathfrak{M}''$, observemos que, se for U o elemento um do sistema, é U $\mathcal{P} = \mathcal{P}$. Assim, $\mathfrak{M}''$ é finito relativamente a U $\mathcal{P}$ (U ρ .m'' = Um''. ρ = = U.m'' ρ = m'' ρ), e, portanto, relativamente a $\mathcal{T}$. Nessas condições, será $\mathfrak{M}'' = \sum \mathfrak{N}_i \, m_k$ completamente redutível (Cap.IV, § 1), podendo enunciar-se o

Teorema 7:- Toda a representação dum sistema hiper-complexo sem radical é completamente redutível.(1)

Vamos passar agora ao caso em que o corpo de representação $\mathcal{A} \supseteq Z \supseteq \mathcal{P}$ não é comutativo. Os teoremas 5 e 7 são ainda válidos, como veremos. Dum modo geral, se $\mathfrak{M}$ é um módulo duplo relativamente a $\mathcal{T}$ (que opera à esquerda) e a $\mathcal{L}$ (que

(1) É claro que, quando não se fala do corpo de representação, se subentende que o mesmo é o corpo fundamental.

opera à direita), não há a possibilidade de fazer operar $\mathcal{L}$ à esquerda e passar a um módulo unilateral relativamente a um anel $\mathcal{T}$, gerado por $\mathcal{T}$ e $\mathcal{L}$, supostos comutáveis. Se $\mathcal{A}$ for um anel anti-isomorfo de $\mathcal{L}$ e se se puser k.m = m.l, ($m \in \mathfrak{M}$, $k \in \mathcal{A}$, $l \in \mathcal{L}$), onde k e l se correspondem no anti-isomorfismo, aparece a referida possibilidade relativamente a um anel $\mathcal{Q}$, suposto gerado por $\mathcal{T}$ e $\mathcal{A}$, ambos comutáveis por hipótese. Anàlogamente, se $\mathcal{K}$ for anti-isomorfo de $\mathcal{T}$, o módulo $\mathfrak{M}$ poderá considerar-se módulo unilateral relativamente a um anel $\mathfrak{M}$, gerado pelos anéis comutativos $\mathcal{K}$ e $\mathcal{L}$. Vale o seguinte

Teorema 8:- Se $\mathcal{L}_{\mathcal{T}}$ e $\mathcal{L}$ são dois sistemas hiper-complexos sobre o mesmo corpo fundamental $\mathcal{P}$, todo o módulo duplo $\mathfrak{M}$ relativamente a $\mathcal{L}_{\mathcal{T}}$ (à esquerda) e a $\mathcal{L}$ (à direita) é módulo unilateral relativamente a $\mathcal{L}_{\mathcal{T}} \times \mathcal{A}$ (à esquerda) e módulo unilateral relativamente a $\mathcal{K} \times \mathcal{L}$ (à direita), sob a hipótese de $\mathcal{A}$ ser anti-isomorfo de $\mathcal{L}$ e $\mathcal{K}$ ser anti-isomorfo de $\mathcal{L}_{\mathcal{T}}$.

Posto isto, seja $\mathcal{L}_{\mathcal{T}}$ um sistema hiper-complexo com elemento um = U. As representações de $\mathcal{L}_{\mathcal{T}}$ em $\mathcal{A} \supseteq Z \supseteq \mathcal{P}$, que vamos estudar, supor-se-ão sempre diferentes da representação nula, além de homomorfas relativamente a $\mathcal{P}$. Admitamos que a representação não faz corresponder a matriz unidade ao elemento U. Sabemos então que ela é soma de duas representações: a representação nula e uma representação em que U tem a matriz unidade a corresponder-lhe. Se pusermos de parte a representação nula, podemos supor que o sistema hiper-complexo contém o corpo fundamental $\mathcal{P}$. Nesta hipótese, não há necessidade de falarmos em homomorfismo da representação relativamente a $\mathcal{P}$, pois que esse homomorfismo é uma condição necessária à representação. Dada uma representação recíproca de $\mathcal{L}_{\mathcal{T}}$ em $\mathcal{A}$, o módulo $\mathfrak{M}$ de representação é módulo esquerdo finito relativamente a $\mathcal{L}_{\mathcal{T}\mathcal{A}}$, visto que este último contém $\mathcal{A}$. Se $\mathcal{K}'$ é o radical de $\mathcal{L}_{\mathcal{T}\mathcal{A}}$ e a representação é irredutível, o módulo $\mathcal{K}'\mathfrak{M}$ é admissível em face de $\mathcal{L}_{\mathcal{T}\mathcal{A}}$. Neste último, os ideais ordinários são admissíveis em face de $\mathcal{A}$. A condição dupla de cadeia é válida, de sorte que $\mathcal{K}'$ é nilpotente. $\mathcal{K}'\mathfrak{M}$ será necessàriamente = (0). $\mathfrak{M}$ torna-se, assim, num módulo esquerdo finito simples relativamente ao anel semi-simples $\mathcal{Z}_{\mathcal{T}} = \mathcal{L}_{\mathcal{T}\mathcal{A}}/\mathcal{K}'$, pelo que será isomorfo dum ideal esquerdo simples $\mathfrak{N}$ deste último

anel. Podemos dizer:

Teorema 9:- Toda a representação recíproca irredutível dum sistema hiper-complexo $\mathcal{Z}$ com elemento um, que contenha o seu corpo fundamental $\mathcal{P}$[1] num corpo não comutativo $\mathcal{K}$ de centro $Z \supseteq \mathcal{P}$, é necessàriamente homomorfa relativamente a $\mathcal{P}$ e pertence a um ideal esquerdo simples do anel semi-simples $\overline{\mathcal{Z}} = \mathcal{Z}_{\mathcal{K}} / \mathcal{R}'$ ($\mathcal{R}$ = radical de $\mathcal{Z}_{\mathcal{K}}$). Inversamente, seja $\overline{\mathcal{U}}$ um ideal esquerdo simples do anel semi-simples $\overline{\mathcal{Z}}$. O ideal é também módulo simples relativamente ao anel $\mathcal{Z}_{\mathcal{K}}$, que opera igualmente à esquerda. Como $\mathcal{Z}_{\mathcal{K}}$ é gerado pelos seus sub-anéis comutáveis $\mathcal{Z}$ e $\mathcal{K}$, o ideal é módulo duma representação recíproca irredutível de $\mathcal{Z}$ em $\mathcal{K}$, a qual é necessàriamente homomorfa relativamente a $[\mathcal{Z}, \mathcal{K}]$, e, portanto, relativamente a $\mathcal{P}$. Nunca se trata aqui da representação nula, de sorte que pode enunciar-se o teorema seguinte, inverso do anterior:

Teorema 10:- A todo o ideal esquerdo simples de $\overline{\mathcal{Z}} = \mathcal{Z}_{\mathcal{K}} / \mathcal{R}$ pertence uma representação recíproca irredutível de $\mathcal{Z}$ em $\mathcal{K}$ (não nula), que é operatória homomorfa relativamente a $\mathcal{P}$.

Se o sistema $\mathcal{Z}$ é semi-simples e se $Z = \mathcal{P}$, $\mathcal{Z}_{\mathcal{K}}$ é igualmente semi-simples. O número de classes distintas de representações irredutíveis de $\mathcal{Z}$ em $\mathcal{K}$ é dado pelo número de anéis simples em que se decompõe $\mathcal{Z}$[2]. Toda a representação de $\mathcal{Z}$, em $\mathcal{K}$, é, então, completamente redutível, porque, se $\mathcal{M}$ for um módulo recíproco de representação, como $\mathcal{K}$ está contido em $\mathcal{Z}_{\mathcal{K}}$, $\mathcal{M}$ é módulo finito relativamente a um anel semi-simples, e, portanto, é completamente redutível. Daremos este enunciado:

Teorema 11:- Toda a representação dum sistema hiper-complexo semi-simples $\mathcal{Z}$, de corpo fundamental $\mathcal{P}$, num corpo $\mathcal{K}$ de centro $Z = \mathcal{P}$, é completamente redutível (suposta homomorfa relativamente a $\mathcal{P}$). O número de classes irredutíveis distintas de representação é o número de anéis simples da decomposição de $\mathcal{Z}$.

(1) Se a representação é homomorfa relativamente a $\mathcal{P}$, esta hipótese é sempre admissível.

(2) Se dois módulos duplos $\mathcal{M}$ e $\mathcal{M}'$ são isomorfos relativamente a $\mathcal{Z}$ e a $\mathcal{K}$ são igualmente isomorfos relativamente a $\mathcal{Z}_{\mathcal{K}}$, e reciprocamente.

Corolário 1:- Um sistema simples $\mathcal{Z}$ tem, no corpo $\mathcal{K}$, de centro $Z = \mathcal{P}$, uma única representação irredutível (tanto recíproca como directa). O grau r da representação é bem determinado.

Na mesma ordem de ideias, pode demonstrar-se o seguinte

Teorema 12:- Se $\mathcal{Z}$ e $\mathcal{Y}$ são dois sistemas hiper-complexos simples sobre $\mathcal{P}$, e se o centro Z, de $\mathcal{Y}$, é $\mathcal{P}$, um módulo duplo mínimo esquerdo $\mathcal{M}$ relativo a $\mathcal{Z}$ e a $\mathcal{Y}$ é $\mathcal{Z}_r \mathcal{Y}_s$ - isomorfo dum ideal esquerdo simples de $\mathcal{Z}_r$. Com efeito, é $\mathcal{Z}_r \mathcal{Y}_s = \mathcal{Z} \times \mathcal{Y} = \mathcal{P}_r \times \mathcal{P}_s = \mathcal{P}_{rs} \times (\mathcal{P} \times \mathcal{P}) = \mathcal{P}_{rs} \times \Phi_t = \mathcal{P}_{rst} \times \Phi = \Phi_{rst}$, de modo que pode afirmar-se ser $\mathcal{Z}_r$ uma álgebra simples sobre $\mathcal{P}$. O módulo $\mathcal{M}$, que é mínimo relativamente a $\mathcal{Z}_r$, é, pois, mínimo relativamente a um anel simples.

Se $\mathcal{Y}$ opera à direita, passa-se à álgebra recíproca $\mathcal{L}$, o módulo $\mathcal{M}$ torna-se num módulo simples relativamente à álgebra simples $\mathcal{Z}_{\mathcal{L}}$ e pode dizer-se:

Teorema 13:- Se $\mathcal{Z}$ e $\mathcal{Y}$ são dois sistemas hiper-complexos simples sobre $\mathcal{P}$, e se o centro Z, de $\mathcal{Y}$, é $\mathcal{P}$, um módulo duplo mínimo $\mathcal{M}$ (esquerdo relativamente a $\mathcal{Z}$ e direito relativamente a $\mathcal{Y}$) torna-se num módulo $\mathcal{Z}_{\mathcal{L}}$ - isomorfo dum ideal esquerdo simples de $\mathcal{Z}_{\mathcal{L}}$ ($\mathcal{L}$ = álgebra recíproca de $\mathcal{Y}$), por passagem a um módulo unilateral.

2) Sobre a representação regular - Este § será exclusivamente dedicado a pôr em evidência certos detalhes interessantes relativos à representação regular. Esta representação será completamente redutível, se $\mathcal{Z}$ for completamente redutível, como sucede se não há radical. As representações irredutíveis, bem determinadas, que comparecem na redução da representação regular pertencem a módulos de representação que são factores de composição da série de composição de $\mathcal{Z}$, os quais são isomorfos de ideais esquerdos simples de $\mathcal{Z} / \mathcal{R} = \mathcal{Z}_{\mathcal{P}}$. Vale o seguinte

Teorema 1:- Na redução da representação regular figuram todas as representações irredutíveis de $\mathcal{Z}$. Com efeito, se $\overline{\mathcal{U}}$ for um ideal esquerdo simples de $\mathcal{Z}_{\mathcal{P}}$, a série de composição des-

te anel factor, na qual $\overline{\mathfrak{N}}$ é penúltimo divisor normal, é isomorfa da parte da série de composição de $\mathfrak{H}$ compreendida entre $\mathfrak{H}$ e $\mathfrak{R}$.

Seja $\mathfrak{H}$ um sistema sem radical. Se $n_1, \ldots, n_s$ são os graus das matrizes que constituem os anéis simples $\mathfrak{a}_t$ em que $\mathfrak{H}$ se decompõe e se g_t é a ordem do corpo dos endomorfismos dum ideal esquerdo simples de $\mathfrak{a}_t$ relativamente ao corpo fundamental de $\mathfrak{H}$, a ordem do sistema é $c = \sum n_t^2 g_t$. A representação irredutível de $\mathfrak{H}$ pertencente a $\mathfrak{N}_t$ contém matrizes de grau $n_t g_t = G_t$. No caso dum corpo fundamental algèbricamente fechado, tem-se $c = \sum n_t^2$, $G_t = n_t$. Em todos os casos, a representação regular de $\mathfrak{H}$ contém n_t vezes a representação irredutível pertencente a $\mathfrak{N}_t$, como se reconhece pondo $\mathfrak{H} = \mathfrak{N}_1 + \cdots + \mathfrak{N}_n$ e considerando a série de composição de $\mathfrak{H}$:

$$\left\{\mathfrak{N}_1 + \cdots + \mathfrak{N}_n \supset \mathfrak{N}_2 + \cdots + \mathfrak{N}_n \supset \cdots \supset \mathfrak{N}_n \supset (0)\right\}.$$

Podemos enunciar o seguinte

Teorema 2:- A representação regular dum sistema sem radical é completamente redutível e contém cada representação irredutível tantas vezes quantos os ideais isomorfos do ideal esquerdo a que pertence e que figuram na decomposição do sistema. Se o corpo fundamental é algèbricamente fechado, cada representação irredutível figura tantas vezes quantas o grau das matrizes da representação.

Se o sistema $\mathfrak{H}$ tiver radical e se $\mathfrak{P}$ for algèbricamente fechado, a característica c, de $\mathfrak{H}$, é maior que a característica c', de $\mathfrak{H}/\mathfrak{R}$. Se se consideram a série de composição

$$\left\{\mathfrak{H}/\mathfrak{R} \supset \mathfrak{H}_1/\mathfrak{R} \supset \cdots \supset \mathfrak{R}/\mathfrak{R} = (0)\right\}, \qquad (1)$$

e a série normal de $\mathfrak{H}$ segundo $\mathfrak{R}$,

$$\left\{\mathfrak{H} \supset \mathfrak{H}_1 \supset \cdots \supset \mathfrak{R}\right\},$$

esta segunda é uma parte duma série de composição de $\mathfrak{H}$. A redução da representação regular vai levar às representações irredutíveis definidas por $\mathfrak{H}/\mathfrak{H}_1, \ldots, \mathfrak{H}_t/\mathfrak{R}$, idênticas às definidas pelos factores de composição da série de composição (1), mas dá ainda outras equivalentes às anteriores. Podemos fixar este enunciado:

Teorema 3:- A representação regular dum sistema com radical, de corpo fundamental algèbricamente fechado, contém cada representação irredutível pelo menos tantas vezes quantas indica o seu grau.

Um teorema interessante é o seguinte:

Teorema 4:- A 1ª representação regular directa dum sistema sem radical é equivalente à 2ª representação regular directa do mesmo sistema. Consideremos as decomposições seguintes em ideais simples (direitos ou esquerdos): $\mathfrak{H} = \mathfrak{K}_1 + \cdots + \mathfrak{K}_n = \mathfrak{N}_1 + \cdots + \mathfrak{N}_n$. Suponhamos $\mathfrak{N}_1$ e $\mathfrak{K}_1$ pertencentes ao mesmo ideal bilateral simples $\mathfrak{a}_1$, da decomposição de $\mathfrak{H}$. Se as bases dos citados ideais são, respectivamente, $(e_{11}, \ldots, e_{n1})$ e $(e_{11}, \ldots, e_{1n})$, temos, para as referidas representações, [suposto, por ex., que o corpo fundamental é algèbricamente fechado],

$$a \cdot e_{t1} = \sum_j e_{j1}\, l_{jt}, \qquad e_{1t} \cdot a = \sum_j \lambda_{tj}\, e_{1j}, \qquad (a \in \mathfrak{a}_1),$$

onde os coeficientes l_{jt} e λ_{tj} pertencem ao corpo fundamental. Suponhamos, porém, $a = \sum e_{pq}\, l'_{pq}$. Virá

$$a \cdot e_{t1} = \sum_p e_{p1}\, l'_{pt}, \qquad e_{1t} \cdot a = \sum_q e_{1q}\, l'_{tq},$$

donde se conclui $l_{jt} = l'_{jt}$, $\lambda_{tj} = l'_{tj}$. As duas matrizes A e A* do Cap. VI, § 2, são iguais, q. e. d.

3) Observações - Estudámos representações de $\mathfrak{H}$ no seu corpo fundamental $\mathfrak{P}$. Dissemos também que as representações $\mathfrak{H}$, de $\mathfrak{H}$, no corpo comutativo $\Omega \supseteq \mathfrak{P}$, se ampliam e tornam em representações Δ, de $\mathfrak{H}_\Omega$. Inversamente, uma representação Δ contém uma representação $\mathfrak{H}$. Se $\mathfrak{H}$ é irredutível, Δ é irredutível. Inversamente, se Δ é irredutível, as matrizes $M_1, \ldots,$

M_n , representantes da base e_1 ,..., e_n , constituem um sistema irredutível, e, portanto, $\mathcal{D}$ é irredutível.

Consideremos uma representação irredutível $\mathcal{D}$. A representação irredutível Δ correspondente figura na representação regular de $\mathcal{G}_\Omega$. Nesta, aos elementos e_1 ,..., e_n correspondem matrizes, que são também as matrizes que lhes correspondem na representação regular de $\mathcal{G}$. Façamos a redução desta última. Podemos, depois, ampliá-la e torná-la na representação regular de $\mathcal{G}_\Omega$. Nestas condições, as representações irredutíveis de $\mathcal{G}$ em Ω (ou de $\mathcal{G}_\Omega$) resultam reduzindo ainda representações irredutíveis de $\mathcal{G}$ em $\mathcal{P}$. Estas últimas representações D podem tornar-se, efectivamente, redutíveis em Ω, em virtude das circunstâncias a seguir.

D pertence a um ideal esquerdo simples $\mathcal{H}$, de $\mathcal{G}/\mathcal{R}$, ou dum anel simples $\mathcal{A}$ contido neste anel factor. Considerando $\mathcal{G}_\Omega$ e ampliando $\mathcal{H}$ para $\mathcal{H}_\Omega$, os elementos de $\mathcal{R}_\Omega$ ainda têm, na representação ampliada, a matriz nula como correspondente. A representação de $(\mathcal{G}/\mathcal{R})_\Omega$ é-o de $\mathcal{G}_\Omega$. No geral, $\mathcal{H}_\Omega$ não é isomorfo dum ideal esquerdo simples de $\mathcal{A}_\Omega$ segundo o seu radical.

Suponhamos $\mathcal{A}_\Omega$ um anel simples de matrizes de grau $n+r$ com elementos de Ω (n representa o grau das matrizes de $\mathcal{A}$ com elementos dum corpo $\mathcal{L} \supseteq \mathcal{P}$). À decomposição $\mathcal{A} = \sum \mathcal{H}$, com n parcelas, corresponde uma decomposição $\mathcal{A}_\Omega = \sum \mathcal{H}_\Omega$, na qual não podem ser ideais esquerdos simples todos os $\mathcal{H}_\Omega$, visto que o número destes numa decomposição de $\mathcal{A}_\Omega$ é $n+r$. É o que sucede se $\mathcal{A}$ é uma álgebra normal sobre $\mathcal{P}$ e Ω é um corpo de decomposição da álgebra (Cap.VII, § 8).

Pode também suceder que $\mathcal{A}_\Omega$, continuando a não ter radical, seja uma soma directa de anéis simples. A representação $\mathcal{D}$ (ou Δ) será completamente redutível, como se sabe. É o que acontece se $\mathcal{A}$ é uma álgebra separável.

Finalmente, voltando ao caso em que $\mathcal{A}_\Omega$ tem radical, a representação $\mathcal{D}$ não é geralmente irredutível, pois que, se o fosse, seria também uma representação irredutível do anel factor $\mathcal{A}_\Omega/\mathcal{R}_1$, segundo o radical $\mathcal{R}_1$. A correspondência $\mathcal{A}_\Omega \sim \mathcal{A}_\Omega/\mathcal{R}_1$ e a decomposição $\mathcal{A}_\Omega = \sum \mathcal{H}_\Omega$ mostram que o anel factor se pode escrever como soma de n ideais esquerdos, cada um dos quais com uma ordem relativamente a Ω que não pode exceder a do seu correspondente $\mathcal{H}_\Omega$. Passando à decomposição em ideais esquerdos simples, estes têm ainda a ordem mais baixa (relativamente a Ω), o que precisa a afirmação feita atrás.

Uma representação irredutível D, que se mantém irredutível quando se considera representação num corpo algébrico qualquer $\Omega \supseteq \mathcal{P}$, diz-se absolutamente irredutível. O sistema de matrizes D é absolutamente irredutível. Inversamente, a partir dum tal sistema constroi-se um anel absolutamente irredutível de matrizes, comutativamente ligado ao corpo $\mathcal{P}$. Exemplos de representações absolutamente irredutíveis são dados pelas representações irredutíveis de $\mathcal{G}$ no seu corpo fundamental, suposto algèbricamente fechado. Dada uma representação $\mathcal{D}$, de $\mathcal{G}$, em $\mathcal{K} \supseteq \mathcal{P}$, também se diz que esta representação é absolutamente irredutível, se for irredutível quando se considera representação de $\mathcal{G}$ no corpo algébrico (qualquer) $\Omega \supseteq \mathcal{K} \supseteq \mathcal{P}$. Se $\mathcal{D}$ é absolutamente irredutível, aos elementos base e_i correspondem matrizes com elementos de $\mathcal{K}$ constituindo um sistema absolutamente irredutível. Fazendo a adjunção a $\mathcal{P}$ dos elementos algébricos que figuram em tais matrizes, o corpo correspondente $\mathcal{P}(\omega_1, \ldots, \omega_t) = \mathcal{L}$ pode tomar-se como corpo de representação de $\mathcal{G}$. Essa representação é já absolutamente irredutível [Regressaremos às representações absolutamente irredutíveis no § 1 do Cap.XI].

4) Aplicações da teoria das representações - São variadas as aplicações da teoria das representações. As que vamos fazer aqui darão motivo suficiente para se avaliar da importância da mesma teoria.

1ª aplicação: Teorema de Burnside (A): - Um anel $\mathcal{Y}$ irredutível de matrizes do grau n com elementos dum corpo algèbricamente fechado $\mathcal{P}$, comutativamente ligado ao anel, contém precisamente n^2 matrizes linearmente independentes (em relação a $\mathcal{P}$). $\mathcal{Y}$ é um sistema hiper-complexo. Tomando $\mathcal{Y}$ como a sua própria representação, esta é fiel e irredutível, e, portanto, $\mathcal{Y}$ é um sistema sem radical. A referida representação pertence a um ideal esquerdo simples de $\mathcal{Y}$. Se Ω for o corpo dos endomorfismos- $\mathcal{Y}$ à direita do ideal, tem-se $\Omega = \mathcal{P}$, pelo facto de $\mathcal{P}$ ser algèbricamente fechado. Nestes termos, encontramo-nos em presença da representação fiel em Ω ou seja do anel completo de matrizes com elementos de $\mathcal{P}$, anel que tem precisa-

mente n^2 matrizes linearmente independentes. Podemos também dizer:

Teorema B:- Uma representação irredutível dum anel $\mathcal{Y}$, comutativamente ligado ao corpo algèbricamente fechado $\mathcal{P}$, dada por matrizes de grau n com elementos de $\mathcal{P}$ e homomorfa relativamente a $\mathcal{P}$, contém precisamente n^2 matrizes linearmente independentes; ou ainda:

Teorema C:- Um sistema irredutível de matrizes, com elementos dum corpo algèbricamente fechado, contanto que contenha, com A e B, o produto AB, contém precisamente n^2 matrizes linearmente independentes. De facto, se A_i é uma matriz do sistema e se $\rho_i \in \mathcal{P}$, o anel $\mathcal{Y}$ de elementos da forma $\sum A_i \rho_i$ está nas condições dos teoremas anteriores. Como as matrizes do sistema considerado constituem uma base para $\mathcal{Y}$, haverá entre elas precisamente n^2 que são independentes, q. e. d.

Passando agora ao caso em que os elementos das matrizes em causa pertencem a um corpo $\mathcal{K}$ que não é algèbricamente fechado e compreendendo a designação de sistema absolutamente irredutível de matrizes como deve ter-se feito já no final do § anterior [trata-se dum sistema que permanece irredutível quando se consideram os seus elementos pertencentes a uma ampliação algébrica qualquer $\Omega \supseteq \mathcal{K}$, de $\mathcal{K}$], admitamos que um sistema absolutamente irredutível $\mathcal{T}$ contém, com A e B, o produto AB. Então, se $A_i \in \mathcal{T}$ e se $\omega_i \in \Omega$, o anel $\mathcal{Y}$, de matrizes $\sum A_i . \omega_i$, está nas condições do teorema A (ou: o sistema $\mathcal{T}$ está nas condições do teorema C). As n^2 matrizes linearmente independentes pertencem a $\mathcal{T}$, de modo que tem lugar o seguinte

Teorema D:- Um sistema absolutamente irredutível de matrizes, contanto que, com A e B, contenha AB, possui precisamente n^2 matrizes linearmente independentes.

Os teoremas A, B, C estendem-se a anéis ou sistemas completamente redutíveis de matrizes, mediante raciocínios simples. Façamos uma observação. Vamos tratar com sistemas completamente redutíveis de matrizes nos quais pode haver sistemas irredutíveis equivalentes. Nestes, supostos reduzidos à mesma forma, a dependência linear das matrizes é apreciada conforme se mostra pelo exemplo seguinte:

$$\begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix} = a \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + b \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} + c \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} + d \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

É válido, então, o

Teorema generalizado de Burnside:- Um anel $\mathcal{Y}$ completamente redutível de matrizes com elementos dum corpo algèbricamente fechado, no qual as partes irredutíveis constituem anéis de matrizes de graus $n_1, \ldots, n_r$, nas condições do teorema A, contém precisamente $n_1^2 + \ldots + n_r^2$ matrizes linearmente independentes, supondo, todavia, que as partes irredutíveis equivalentes se contam uma única vez. De facto, $\mathcal{P}$ está comutativamente ligado a $\mathcal{Y}$. Este é um absoluto da representação completamente redutível que ele próprio fornece, e, por isso, não tem radical. As matrizes de cada representação irredutível (supostas completadas com zeros, de modo a ficarem com grau igual ao das matrizes de $\mathcal{Y}$) não podem depender linearmente das matrizes doutra representação irredutível não equivalente, pelo que o teorema resulta imediatamente.

Em correspondência com os aspectos dos teoremas B e C, anteriores, poderíamos dar mais dois enunciados do teorema generalizado de Burnside.

2ª aplicação: Estudo dum exemplo de Dirac:- Tomemos as matrizes

$$\Sigma_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad \Sigma_2 = \begin{pmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{pmatrix}, \quad \Sigma_3 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad \Sigma_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

com elementos do corpo Γ dos números complexos. Pondo $\lambda, \mu = 1, 2, 3, 4$, verificam-se imediatamente as igualdades

$$\Sigma_\lambda^2 = U\,, \qquad \Sigma_\lambda \Sigma_\mu = -\Sigma_\mu \Sigma_\lambda\,, \quad (U = \text{matriz unidade}). \tag{2}$$

Consideremos o sistema das 16 matrizes seguintes:

$$\begin{gathered} U, \Sigma_1, \ldots, \Sigma_4, \Sigma_1\Sigma_2, \ldots, \Sigma_3\Sigma_4, \\ \Sigma_1\Sigma_2\Sigma_3, \ldots, \Sigma_2\Sigma_3\Sigma_4, \Sigma_1\Sigma_2\Sigma_3\Sigma_4\,. \end{gathered} \tag{3}$$

Este sistema, aparte a questão do sinal, contém o produto de duas matrizes que lhe pertençam. As 16 matrizes são linearmente independentes e podem tomar-se como base do anel completo de matrizes de 4ª ordem com elementos de Γ. Este anel só tem representações irredutíveis ou completamente redutíveis. As representações irredutíveis pertencem a um ideal esquerdo simples do anel e têm este como absoluto. A única representação irredutível do anel é o próprio anel.

Quando se quer um sistema de matrizes satisfazendo a (2), a consideração das matrizes (3) leva a um sistema hiper-complexo de base $u, \sigma_1, \ldots, \sigma_4, \sigma_{12}, \ldots, \sigma_{34}, \sigma_{123}, \ldots, \sigma_{234}, \sigma_{1234}$, base na qual os elementos obedecem à lei associativa de multiplicação (2). Se as matrizes de (2) existem, constroi-se, por meio delas, uma representação do sistema hiper-complexo. Inversamente, uma representação do sistema hiper-complexo tem de ser dada por matrizes, entre as quais matrizes como (3) representam os elementos base do sistema. A representação anterior de Dirac mostra que a estrutura do sistema hiper-complexo é a dum anel completo de matrizes de 4ª ordem. Tratando-se, então, dum sistema sem radical, a única representação irredutível é a de Dirac, e o sistema de matrizes satisfazendo a (2) é, pelo menos, de 4ª ordem. Pode haver, porém, matrizes de 8ª ordem, de 12ª ordem, etc., nas condições desejadas.(1)

(1) Cfr. Dirac, "Quantum Mechanics", 1935, pgs. 254. Aqui seguimos van der Waerden, "Die Gruppenthecretische Methode in der Quantenmechanik", 1932, pgs. 55.

3ª aplicação: Álgebras separáveis:(1) Seja $\mathcal{G}$ um sistema hiper-complexo de corpo fundamental $\mathcal{P}$. Se $\Omega \supseteq \mathcal{P}$ é um corpo algèbricamente fechado, pode enunciar-se o seguinte

Teorema:- O anel cociente $\mathcal{G}_\Omega/\mathcal{R}_1$, da álgebra ampliada segundo o seu radical $\mathcal{R}_1$, é isomorfo duma soma directa de anéis completos de matrizes com elementos de Ω. De facto, a álgebra semi-simples $\mathcal{G}_\Omega/\mathcal{R}_1$, uma vez decomposta em álgebras simples, leva a álgebras completas α_i de matrizes com elementos de álgebras de divisão que são ampliações finitas de corpos algèbricamente fechados isomorfos de Ω (da forma $e_i\Omega$, onde e_i representa o elemento um de α_i). Tais ampliações finitas, como sabemos, são idênticas aos próprios corpos algèbricamente fechados (Lema 1, § 6, Cap. VII).

O teorema anterior pode precisar-se, se $\mathcal{G}/\mathcal{R}$ é uma álgebra separável. Quando se passa do corpo fundamental $\mathcal{P}$ a uma ampliação $\Delta \supseteq \mathcal{P}$, verifica-se que o radical de $\mathcal{G}_\Delta$ é $\mathcal{R}_\Delta$, estudando o homomorfismo $\mathcal{G}_\Delta \sim \mathcal{G}_\Delta/\mathcal{R}_\Delta$ e vendo que cada ideal nilpotente de $\mathcal{G}_\Delta$ está contido no ideal bilateral nilpotente $\mathcal{R}_\Delta$. A igualdade geral

$$(\mathcal{G}/\mathcal{R})_\Delta = \mathcal{G}_\Delta/\mathcal{R}_\Delta$$

mostra que é válido o

Teorema:- É condição necessária e suficiente, para que $\mathcal{G}/\mathcal{R}$ (sobre $\mathcal{P}$) seja separável, que o radical de $\mathcal{G}_\Delta$, para $\Delta \supseteq \mathcal{P}$, seja $\mathcal{R}_\Delta$, qualquer que seja o corpo comutativo Δ.

Voltando à questão de precisar o penúltimo teorema, observemos que os resultados sobre álgebras separáveis estabelecidos no Cap. VII, § 8, nos permitem afirmar a existência dum corpo de decomposição de $\mathcal{G}/\mathcal{R}$, corpo que é uma ampliação finita do corpo fundamental $\mathcal{P}$. Servindo-nos da teoria das representações, vamos demonstrar o mesmo facto, enunciando para o efeito este

(1) Seguimos Almeida Costa, "Sobre os anéis semi-primários".

Teorema:- Se $\mathcal{A}/\mathcal{R}$ se conserva semi-simples para qualquer ampliação algébrica Δ, de $\mathcal{P}$, existe uma ampliação algébrica finita $\mathcal{L}$, de $\mathcal{P}$, tal que $\mathcal{A}_{\mathcal{L}}/\mathcal{R}_{\mathcal{L}}$ ($\mathcal{R}$= radical de $\mathcal{A}_{\mathcal{L}}$) é soma de anéis completos de matrizes com elementos de corpos isomorfos de $\mathcal{L}$. Designando por Ω um corpo algèbricamente fechado, ponhamos

$$\mathcal{A}/\mathcal{R} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_s , \qquad \mathfrak{z} = \mathfrak{z}_1 + \cdots + \mathfrak{z}_s ,$$

$$(\mathcal{A}/\mathcal{R})_{\Omega} = \mathfrak{a}_{1\Omega} + \cdots + \mathfrak{a}_{s\Omega}, \quad \mathfrak{z}_{\Omega} = \mathfrak{z}_{1\Omega} + \cdots + \mathfrak{z}_{s\Omega} ,$$

onde os $\mathfrak{a}_i$ são anéis simples e os $\mathfrak{z}_i$ os seus centros. Cada $\mathfrak{a}_{i\Omega}$ decompõe-se, por hipótese, em anéis simples. Por ex.:

$$\mathfrak{a}_{1\Omega} = \mathfrak{A}_{1\Omega}^{(1)} + \cdots + \mathfrak{A}_{1\Omega}^{(p_1)} , \qquad \mathfrak{z}_{1\Omega} = \mathfrak{z}_{1\Omega}^{(1)} + \cdots + \mathfrak{z}_{1\Omega}^{(p_1)} .$$

O número de parcelas destas somas é dado pela ordem da álgebra $\mathfrak{z}_1$ relativamente a $\mathcal{P}$. De facto $\mathfrak{z}_{1\Omega}^{(1)}$ é isomorfo do corpo fundamental da álgebra, portanto é álgebra de 1ª ordem sobre Ω. $\mathfrak{z}_{1\Omega}$ será de ordem p_1, igual à ordem de $\mathfrak{z}_1$ sobre $\mathcal{P}$. Posto isto, sabemos que $\mathfrak{A}_{1\Omega}^{(1)}$ constitui uma representação irredutível de $(\mathcal{A}/\mathcal{R})_{\Omega}$ num corpo (o dos endomorfismos dum ideal esquerdo de $\mathfrak{A}_{1\Omega}^{(1)}$) que que é isomorfo de Ω. Podemos supor que se trata duma representação irredutível de $(\mathcal{A}/\mathcal{R})_{\Omega}$ em Ω, ou também duma representação irredutível de $\mathcal{A}_{\Omega}$ em Ω. Trata-se, em suma, se se quizer, duma representação absolutamente irredutível de $\mathcal{A}$ em Ω. Tomando um ideal esquerdo simples de $\mathfrak{A}_{1\Omega}^{(1)}$ como módulo de representação, os elementos $e_1, \ldots, e_n$, que constituem a base de $\mathcal{A}$ (ou de $\mathcal{A}_{\Omega}$), têm como correspondentes matrizes nas quais figura um número finito de elementos de Ω. Fazendo o mesmo raciocínio para as diferentes parcelas dos diferentes $\mathfrak{a}_{i\Omega}$, define-se uma ampliação algébrica finita $\mathcal{L} = \mathcal{P}(\omega_1, \ldots, \omega_r)$, de $\mathcal{P}$, que contém os elementos de todas as matrizes que correspondem aos elementos de $\mathcal{A}$. As representações absolutamente irredutíveis de $\mathcal{A}$ (aqui encontradas) são, pois, representações irredutíveis distintas de $\mathcal{A}$ em $\mathcal{L}$. Vamos ver que, inversamente, se obtêm assim todas as representações irredutíveis de $\mathcal{A}$ em $\mathcal{L}$. Uma tal representação, ou representação irredutível de $\mathcal{A}_{\mathcal{L}}$, ou de $(\mathcal{A}/\mathcal{R})_{\mathcal{L}}$, é obtida a

partir de

$$(\mathcal{A}/\mathcal{R})_{\mathcal{L}} = \mathfrak{a}_{1\mathcal{L}} + \cdots + \mathfrak{a}_{s\mathcal{L}} ,$$

decompondo os $\mathfrak{a}_{i\mathcal{L}}$ em anéis simples. A decomposição de $\mathfrak{a}_{1\mathcal{L}}$, por ex., não pode dar mais do que p_1 parcelas, pois, de contrário, também $\mathfrak{a}_{1\Omega}$ daria mais do que p_1 parcelas. O número p_1 é certamente atingido, tendo em conta o número de representações irredutíveis distintas de $\mathcal{A}$ em $\mathcal{L}$ que já se sabe existirem. Será, assim,

$$\mathfrak{a}_{1\mathcal{L}} = \mathfrak{A}_{1\mathcal{L}}^{(1)} + \cdots + \mathfrak{A}_{1\mathcal{L}}^{(p_1)} .$$

O grau n_1 das matrizes da representação de $\mathcal{A}$ obtida através de $\mathfrak{A}_{1\mathcal{L}}^{(1)}$, quando os elementos das matrizes se tomam em $\mathcal{L}$, é o mesmo que o das matrizes que representam $\mathcal{A}$ na representação constituida por $\mathfrak{A}_{1\Omega}^{(1)}$, quando os elementos das matrizes se tomam em Ω. Por outro lado, aquele grau é o produto do grau m_1, das matrizes da representação de $\mathcal{A}$ constituida por $\mathfrak{A}_{1\mathcal{L}}^{(1)}$ (na qual o corpo de representação é o corpo $\mathcal{K}_1$ dos endomorfismos dum ideal esquerdo de $\mathfrak{A}_{1\mathcal{L}}^{(1)}$), pelo grau q_1 (ordem) da ampliação finita $\mathcal{K}_1$, de $\mathcal{L}$: $n_1 = m_1 q_1$. A ordem de $\mathfrak{A}_{1\mathcal{L}}^{(1)}$ relativamente a $\mathcal{L}$ é $m_1^2 q_1 = n_1^2$ = ordem de $\mathfrak{A}_{1\Omega}^{(1)}$ relativamente a Ω. Tem-se, portanto, $q_1 = 1$. $\mathcal{K}_1$ é de 1ª ordem relativamente a $\mathcal{L}$ (ou, melhor, relativamente ao corpo $E_1^{(1)}\mathcal{L}$, no qual $E_1^{(1)}$ é elemento um de $\mathfrak{A}_{1\mathcal{L}}^{(1)}$). O teorema está demonstrado.

4ª aplicação:- Os anéis de matrizes[1]:- Representemos por $\mathcal{K}$ e $\mathcal{L}$ dois corpos anti-isomorfos, com o centro comum $\mathcal{P}$. Dado o sistema hiper-complexo simples $\mathcal{A}$, sobre $\mathcal{P}$, diz-se que o mesmo está mergulhado de modo irredutível ou de modo redutível no anel completo $\mathcal{K}_m$ de matrizes do grau m, conforme $\mathcal{A}$ admite uma representação recíproca irredutível ou completamente redutível, de grau m, em $\mathcal{L}$.

(1) E. Noether, "Nichtkommutative Algebra", pgs. 527 a 529.

Se $\mathcal{G}$ está mergulhado de modo irredutível, m é bem determinado e igual ao grau r da única representação irredutível não nula possível. Poderia dizer-se que, então, $\mathcal{G}$ está mergulhado de modo completamente redutível em $\mathfrak{A}_{r+1}$, $\mathfrak{A}_{r+2}$, etc.. Uma observação feita anteriormente (§ 1), segundo a qual ao elemento um de $\mathcal{G}$ deverá fazer-se corresponder inicialmente a matriz unidade, mostra que é de excluir tal raciocínio. $\mathcal{G}$ estará apenas mergulhado de modo redutível em $\mathfrak{A}_{rq}$, qualquer que seja o inteiro positivo q (diz-se também que $\mathcal{G}$ está mergulhado de modo irredutível com a multiplicidade q em $\mathfrak{A}_{rq}$).

Consideremos duas álgebras simples equivalentes $\mathcal{G}_1$ e $\mathcal{G}_2$ (sobre $\mathfrak{P}$), contidas em $\mathfrak{A}_m$ e com o mesmo elemento um que este último. No geral, $\mathfrak{A}_m$ não é álgebra sobre $\mathfrak{P}$, pois que não se faz a hipótese de $\mathfrak{A}$ ser finito sobre $\mathfrak{P}$. Assim, as duas álgebras equivalentes em questão não são sub-álgebras. In abstracto, existe um sistema hiper-complexo simples sobre $\mathfrak{P}$ com duas representações directas completamente redutíveis, de grau m, em $\mathfrak{A}$. Como as componentes irredutíveis das representações se reduzem (aparte equivalências) a uma representação bem determinada, as duas representações (precisamente $\mathcal{G}_1$ e $\mathcal{G}_2$) podem ser reduzidas às mesmas matrizes. É válido, pois, o seguinte

Teorema 1:- Duas álgebras simples equivalentes $\mathcal{G}_1$ e $\mathcal{G}_2$ (sobre $\mathfrak{P}$) contidas no anel de matrizes $\mathfrak{A}_m$, sob as hipóteses de $\mathfrak{A}$ ter o centro $\mathfrak{P}$ e de as álgebras terem o mesmo elemento um que $\mathfrak{A}_m$, deduzem-se uma da outra por um automorfismo interno de $\mathfrak{A}_m$.

Corolário 1:- Se o corpo não comutativo $\mathfrak{A}$, de centro $\mathfrak{P}$, é finito sobre $\mathfrak{P}$, duas sub-álgebras simples equivalentes contidas em $\mathfrak{A}_m$, com o mesmo elemento um que esta última, deduzem-se uma da outra por um automorfismo interno.(1)

Corolário 2:- Se o corpo não comutativo $\mathfrak{A}$, de centro $\mathfrak{P}$, é finito sobre $\mathfrak{P}$, todo o automorfismo de $\mathfrak{A}_m$ que deixa invariantes os elementos de $\mathfrak{P}$ é interno.(2) Em particular é interno todo o automorfismo de $\mathfrak{A}$ que deixa fixos os elementos de $\mathfrak{P}$ (automorfismos relativamente a $\mathfrak{P}$).

(1) Cfr. R.Brauer, pgs.249 de "Über die algebraische Struktur von Schiefkörpern", adiante citado.

(2) Cfr. R.Brauer, pgs.105 da memória seguinte: "Über Systeme hyperkomplexer Zahlen", Mathematische Zeitschrift, Band 30, 1929, pgs.79 a 107.

Corolário 3:- Se o corpo não comutativo $\mathfrak{A}$, de centro $\mathfrak{P}$, é finito sobre $\mathfrak{P}$, dois sub-corpos de $\mathfrak{A}$ que contenham $\mathfrak{P}$, isomorfos relativamente a $\mathfrak{P}$, deduzem-se um do outro por um automorfismo interno de $\mathfrak{A}$.

No caso de ser $\mathfrak{A} = \mathfrak{P}$, e, portanto, $\mathfrak{A}_m = \mathfrak{P}_m$, o corolário 1 reveste-se dum aspecto já encontrado no § 4 do Cap.VI. Conforme o teorema 2º do referido §, se $\mathcal{C}_s$ e $\mathcal{C}'_s$ são duas sub-álgebras de $\mathfrak{P}_m$, com o mesmo elemento um que a álgebra, e se ambas elas forem equivalentes a álgebras completas de matrizes de grau s com elementos de $\mathfrak{P}$, há um automorfismo interno de $\mathfrak{P}_m$ que faz passar de $\mathcal{C}'_s$ a $\mathcal{C}_s$.

Julgamos úteis as considerações que vamos ainda fazer, em relação imediata com o teorema e os corolários acabados de enunciar. Demonstrámos no Cap.II, § 4, que, dadas as duas expressões (por meio de matrizes unidades) dum anel simples $\mathcal{T}$:

$$\mathcal{T} = \sum \mathcal{C} e_{lk} = \mathcal{C}_m , \qquad \mathcal{T} = \sum \mathcal{C}' e'_{lk} = \mathcal{C}'_m ,$$

há sempre um automorfismo interno de $\mathcal{T}$ levando dos e_{lk} aos e'_{lk} e do corpo $\mathcal{C}$ ao corpo $\mathcal{C}'$. Nessas condições, imaginemos um automorfismo qualquer de $\mathcal{T}$. Ele levará dos e_{lk} a um outro sistema e''_{lk}, de $\mathcal{C}$ a um outro corpo $\mathcal{C}''$, e de cada $a \in \mathcal{T}$ a um elemento $a'' \in \mathcal{T}$, com $a = \sum e_{lk} a_{lk}$, $a'' = \sum e''_{lk} a''_{lk}$, ($a_{lk} \in \mathcal{C}$, $a''_{lk} \in \mathcal{C}''$). O automorfismo interno $\ominus$, que leva dos e_{lk} aos e''_{lk} e de $\mathcal{C}$ a $\mathcal{C}''$, não é o automorfismo anterior, visto que o raciocínio do referido § 4, Cap.II, afirma unicamente haver, por virtude de $\ominus$, uma transformação global de $\mathcal{C}$ em $\mathcal{C}''$, sem que a''_{lk} seja correspondente de a_{lk}, como no automorfismo inicial. Não será, assim, geralmente, a'' o correspondente de a, por via de $\ominus$. No caso da correspondência $\mathcal{C} \rightarrow \mathcal{C}''$ ter lugar, elemento por elemento, da mesma maneira nos dois automorfismos, estes são idênticos. Se, por ex., $\mathcal{C}$ for finito sobre o seu centro, e se os elementos do centro ficarem fixos, o automorfismo inicial é necessàriamente interno.

Posto isto, consideremos ainda um anel simples $\mathcal{T}$ e ponhamos $\mathcal{T} = \mathcal{G}_s = \mathcal{F}_s$, onde $\mathcal{G}$ e $\mathcal{F}$ são corpos. Os resultados que estamos invocando, visto tratar-se de duas expressões de $\mathcal{T}$ por meio de matrizes unidades (em número de s^2), garantem-nos que $\mathcal{G}$ e $\mathcal{F}$ são corpos isomorfos. Por outro lado, também não é possível escrever $\mathcal{G}_s = \mathcal{F}_t$, com $s \neq t$, pelo facto de, tanto s como t, representarem o número de ideais esquerdos simples em que se decompõe $\mathcal{T}$.

Pròpriamente em correlação com o corolário 1, usa-se também a terminologia que se segue. Se $\mathcal{H}$ é uma álgebra com elemento um, sobre $\mathcal{P}$, e se $\mathcal{H}_1$ e $\mathcal{H}_2$ são duas sub-álgebras equivalentes, diz-se que a equivalência pode ser estendida à álgebra $\mathcal{H}$, se existir um automorfismo interno de $\mathcal{H}$ por meio do qual os elementos de $\mathcal{H}_1$ se transformam nos elementos de $\mathcal{H}_2$ que lhes correspondem na referida equivalência. O corolário 1 admite, então, este outro enunciado:

Corolário 1":- Se $\mathcal{H}$ é uma álgebra normal simples cujo elemento um é elemento um de duas sub-álgebras equivalentes $\mathcal{H}_1$ e $\mathcal{H}_2$, esta equivalência pode ser estendida à álgebra $\mathcal{H}$.(1)

Voltemos ao caso em que $\mathfrak{h}$ não é ampliação finita de $\mathcal{P}$. Seja $\mathcal{T}$ uma álgebra simples sobre $\mathcal{P}$, de matrizes contidas em $\mathfrak{h}_m$, com o mesmo elemento um que este último anel. É nosso objectivo procurar em $\mathfrak{h}_m$ as matrizes que comutam individualmente com todas as matrizes de $\mathcal{T}$. A álgebra simples $\mathcal{T}$ está mergulhada em $\mathfrak{h}_m$. Ela tem uma representação recíproca isomorfa em $\mathcal{L}$. Se $\mathcal{M}$ for o módulo de representação, são válidas as relações

$$\mathcal{T} \tilde{=} \mathcal{T}_1' \cong \mathcal{O}_{\mathcal{L}}' \not\cong \mathcal{L}_m^{(2)}, \qquad \mathcal{O}_{\mathcal{L}}' \cong \mathfrak{h}_m ,$$

onde $\not\cong$ significa aqui anti-isomorfismo. Por meio delas, passa-se de $\mathcal{T}$ a um anel T de matrizes de $\mathcal{L}_m$. Se procurarmos as matrizes deste último que comutam com as de T, passaremos por anti-isomorfismo para os elementos de $\mathcal{O}_{\mathcal{L}}'$ que comutam com os endomorfismos $\mathcal{T}_1'$, e, depois, por isomorfismo, para as matrizes que comutam, em $\mathfrak{h}_m$, com as de $\mathcal{T}$. O problema reduz-se, assim, a procurar os endomorfismos $\mathcal{O}_{\mathcal{L}}'$ que comutam com os endomorfismos $\mathcal{T}_1'$. Serão, precisamente, os endomorfismos comuns a $\mathcal{O}_{\mathcal{L}}'$ e a $\mathcal{O}_{\mathcal{T}}'$, ou seja os endomorfismos $-(\mathcal{L}, \mathcal{T})$. Como $\mathcal{T} = \mathcal{T}_{\mathcal{L}}$ existe, os endomorfismos em questão são os endomorfismos $\mathcal{O}_{\mathcal{T}}'$ do módulo $\mathcal{M}$. Este é uma soma $\mathcal{M} = \sum \mathcal{M}_t$, de s módulos mínimos relativamente ao anel simples $\mathcal{T}$, módulos que são $\mathcal{T}$- isomorfos dum ideal esquerdo simples de $\mathcal{T}$, de sorte que $\mathcal{O}_{\mathcal{T}}'$ é um anel completo de matrizes do grau s com elementos dum corpo isomorfo do corpo $\mathcal{G}$ dos endomorfismos - $\mathcal{T}$ à esquerda dum ideal esquerdo simples de $\mathcal{T}$. O conjunto $\overline{\mathcal{T}}$, das matrizes comutáveis com $\mathcal{T}$, que estamos procurando, tem a estrutura de $\mathcal{O}_{\mathcal{T}}'$. É, assim,

$$\overline{\mathcal{G}}_s = \overline{\mathcal{T}} \cong \mathcal{O}_{\mathcal{T}}, \qquad \text{com} \quad \overline{\mathcal{G}} \cong \mathcal{G} \not\cong \mathcal{F}, \qquad \mathcal{T} = \mathcal{T}_{\mathcal{G}} = \mathcal{F}_t \not\cong \mathcal{G}_t ,$$

convindo fixar que $\overline{\mathcal{T}}$ e $\mathcal{T}_{\mathcal{G}}$ são anéis completos de matrizes com elementos de corpos anti-isomorfos. Pode dizer-se:

Teorema 2:- Tomemos uma álgebra simples $\mathcal{T}$, sobre $\mathcal{P}$, contida no anel completo $\mathfrak{h}_m$, de matrizes com elementos do corpo não comutativo $\mathfrak{h}$, de centro $\mathcal{P}$, e suponhamos que o elemento um da álgebra é o elemento um de $\mathfrak{h}_m$. As matrizes individualmente comutáveis com cada um dos elementos de $\mathcal{T}$ formam um anel simples $\overline{\mathcal{T}} = \overline{\mathcal{G}}_s$, de matrizes com elementos dum corpo $\overline{\mathcal{G}}$ isomorfo do corpo dos endomorfismos - $\mathcal{T}_{\mathcal{G}}$ à esquerda dum ideal esquerdo simples de $\mathcal{T}_{\mathcal{G}}$. $\overline{\mathcal{T}}$ reduz-se a um corpo se $\mathcal{T}$ estiver mergulhado em $\mathfrak{h}_m$ de modo irredutível, e a intersecção $[\mathcal{T}, \overline{\mathcal{T}}]$ é o centro de $\mathcal{T}$. A afirmação relativa ao caso em que $\mathcal{T}$ é corpo resulta de que esse facto se dá se for $s = 1$, e, portanto, se for $\mathcal{M}$ um módulo mínimo relativamente a $\mathcal{T}$ e a $\mathcal{L}$, isto é, ainda, se a representação de $\mathcal{T}$ em $\mathcal{L}$ for irredutível. Quanto à intersecção $[\mathcal{T}, \overline{\mathcal{T}}]$, o que se afirma é imediato.

Quando se raciocina supondo o módulo de representação directa de $\mathcal{T}$ em $\mathfrak{h}$ como módulo sobre o qual $\mathcal{T}$ opera ainda à es-

(1) Albert, "Structure of algebras", pgs. 54 a 56. As referências a este autor, feitas a seguir, respeitam sempre ao mesmo livro, se não houver indicação precisa.

(2) As notações são as do Capítulo anterior. $\mathcal{O}_{\mathcal{L}}'$ é o anel de endomorfismos - $\mathcal{L}$ à esquerda de $\mathcal{M}$, etc.

querda e $\mathfrak{h}$ à direita, mas o módulo duma representação recíproca como módulo sobre o qual os dois domínios operatórios operam à direita; se introduzirmos $\mathfrak{L}_m$, e, em seguida, a álgebra simples sobre $\mathfrak{p}$, $\mathfrak{R} \neq \mathfrak{r}$, o problema da comutabilidade referido no teorema 2 resolve-se para $\mathfrak{R}$ tendo em conta as relações

$$\mathfrak{R} \cong \mathfrak{R}_1 \subseteq \mathfrak{o}_{\mathfrak{d}} \cong \mathfrak{L}_m,$$

passando-se depois de $\mathfrak{R}$ para $\overline{\mathfrak{r}}$ por anti-isomorfismo. Podemos dar os enunciados seguintes:

Teorema 2':- As matrizes de $\overline{\mathfrak{R}}$ formam um anel simples $\overline{\mathfrak{R}} = \overline{\mathfrak{I}}_s$, de matrizes com elementos dum corpo $\overline{\mathfrak{I}}$, isomorfo do corpo dos endomorfismos - $\mathfrak{R}_{\mathfrak{d}}$ à direita dum ideal direito simples de $\mathfrak{R}_{\mathfrak{d}}$.

Teorema 2":- As matrizes $\overline{\mathfrak{r}}$, do teorema 2, formam um anel de matrizes com elementos dum corpo $\overline{\mathfrak{L}}$ isomorfo dum corpo $\mathfrak{L}$ tal que $\mathfrak{R}_{\mathfrak{d}} = \mathfrak{R} \times \mathfrak{h}$ se pode escrever como anel completo de matrizes com elementos de $\mathfrak{L}$. De facto, sendo $\overline{\mathfrak{R}} = \overline{\mathfrak{I}}_s$, tem-se $\overline{\mathfrak{r}} = \overline{\mathfrak{L}}_s$, com $\overline{\mathfrak{L}} \neq \overline{\mathfrak{I}}$. Ora é $\mathfrak{R} \times \mathfrak{h} \neq \overline{\mathfrak{I}}_t$, portanto $\mathfrak{R} \times \mathfrak{h} \cong \overline{\mathfrak{L}}_t$, ou seja $\mathfrak{R} \times \mathfrak{h} = \mathfrak{L}_t$, com $\mathfrak{L} \cong \overline{\mathfrak{L}}$.

Imaginemos que $\mathfrak{h}$ é ampliação finita de $\mathfrak{p}$, de sorte que $\mathfrak{h}_m$ é um sistema hiper-complexo sobre $\mathfrak{p}$. A álgebra simples $\mathfrak{r}$, referida no teorema 2, é sub-álgebra de $\mathfrak{h}_m$. Podemos, mais precisamente, demonstrar este

Teorema 3:- Se $\mathfrak{h}$ é uma ampliação finita do seu centro $\mathfrak{p}$, toda a sub-álgebra simples $\mathfrak{r}$, sobre $\mathfrak{p}$, do anel completo de matrizes $\mathfrak{h}_m$, que tenha o mesmo elemento um que $\mathfrak{h}_m$, admite neste último uma sub-álgebra simples $\overline{\mathfrak{r}}$, sobre $\mathfrak{p}$, de elementos individualmente comutáveis com os seus elementos, sub-álgebra que tem ainda o mesmo elemento um que $\mathfrak{h}_m$ e que está em situação recíproca relativamente a $\mathfrak{r}$. A ordem $(\mathfrak{h}_m / \mathfrak{p})$, de $\mathfrak{h}_m$ sobre $\mathfrak{p}$, é o produto das ordens $(\mathfrak{r}/\mathfrak{p})$ e $(\overline{\mathfrak{r}} / \mathfrak{p})$. Se uma matriz A pertence a $\overline{\mathfrak{r}}$, tem-se também $A\rho \in \overline{\mathfrak{r}}$, $(\rho \in \mathfrak{p})$. $\overline{\mathfrak{r}}$ será uma sub-álgebra de $\mathfrak{h}_m$ com o mesmo elemento um que esta. A propriedade

enunciada para as ordens resulta como vai ver-se. Tem-se $(\mathfrak{h}_m / \mathfrak{p}) = m^2(\mathfrak{h}/\mathfrak{p})$. A ordem $(\mathfrak{r}/\mathfrak{p})$ é a mesma que a ordem $(\mathfrak{r}_{\mathfrak{L}}/\mathfrak{L})$, de sorte que $(\mathfrak{r}/\mathfrak{p}) = t^2$, onde t dá o número de ideais esquerdos simples em que pode decompor-se $\mathfrak{r}_{\mathfrak{L}}$ e r dá o grau da representação irredutível de $\mathfrak{r}$ em $\mathfrak{L}$. Quanto à ordem $(\overline{\mathfrak{r}}/\mathfrak{p})$, tem-se $(\overline{\mathfrak{r}}/\mathfrak{p}) = s^2(\overline{\mathfrak{L}}/\mathfrak{p}) = s^2(\mathfrak{L}/\mathfrak{p})$. Ora é também $m = sr$,

$$(\mathfrak{r}_{\mathfrak{L}}/\mathfrak{p}) = (\mathfrak{r}_{\mathfrak{L}}/\mathfrak{L})(\mathfrak{L}/\mathfrak{p}) = (\mathfrak{r}/\mathfrak{p})(\mathfrak{L}/\mathfrak{p}) = t^2.(\mathfrak{L}/\mathfrak{p}) = t^2.(\mathfrak{G}/\mathfrak{p}),$$

de sorte que $r.(\mathfrak{L}/\mathfrak{p}) = t.(\mathfrak{G}/\mathfrak{p})$, e

$$(\mathfrak{r}/\mathfrak{p})(\overline{\mathfrak{r}}/\mathfrak{p}) = t^2 s^2(\mathfrak{G}/\mathfrak{p}) = r^2 s^2(\mathfrak{L}/\mathfrak{p}) = m^2(\mathfrak{h}/\mathfrak{p}).$$

Tira-se daqui que a sub-álgebra de $\mathfrak{h}_m$ de elementos individualmente comutáveis com os elementos de $\overline{\mathfrak{r}}$ é precisamente $\mathfrak{r}$. Efectivamente, se fosse $\overline{\overline{\mathfrak{r}}}$, ter-se-ia $(\overline{\overline{\mathfrak{r}}}/\mathfrak{p})(\overline{\mathfrak{r}}/\mathfrak{p}) = m^2(\mathfrak{h}/\mathfrak{p})$, de modo que a ordem de $\overline{\overline{\mathfrak{r}}}$ seria a de $\mathfrak{r}$. Como esta última está contida em $\overline{\overline{\mathfrak{r}}}$, resulta a afirmação. $\mathfrak{r}$ e $\overline{\mathfrak{r}}$ têm o centro comum formado pela sua intersecção.(1)

Corolário 4:- Os comutadores $\overline{\mathfrak{r}}_1$, $\overline{\mathfrak{r}}_2$, de duas sub-álgebras equivalentes $\mathfrak{r}_1$, $\mathfrak{r}_2$ duma álgebra normal simples sobre $\mathfrak{p}$ (sempre sob a hipótese de haver o mesmo elemento um para a álgebra e as sub-álgebras), são sub-álgebras equivalentes. O automorfismo interno que leva de $\mathfrak{r}_1$ a $\mathfrak{r}_2$ leva também de $\overline{\mathfrak{r}}_1$ a $\overline{\mathfrak{r}}_2$. Esta afirmação contém doutrina a ligar imediatamente aos resultados estabelecidos no § 4 do Cap. VI.

Admitamos que é $\mathfrak{h} = \mathfrak{p}$, e, portanto, $\mathfrak{h}_m = \mathfrak{p}_m$. Uma sub-álgebra simples de $\mathfrak{p}_m$, com o mesmo elemento um que este e da forma $\mathfrak{r} = \begin{pmatrix} \cdots & e_{ij} & \cdots \end{pmatrix} \times \mathfrak{p} = \mathfrak{p}_t$, admite a sub-álgebra correspondente $\overline{\mathfrak{r}} = \begin{pmatrix} \cdots & e_{ij} & \cdots \end{pmatrix} \times \overline{\mathfrak{p}} = \overline{\mathfrak{p}}_s = \mathfrak{p}_s \times \mathfrak{D}$, onde $\mathfrak{D}$ é álgebra de di-

(1) Cfr. pgs. 245 e seguintes de R. Brauer : "Über die algebraische Struktur von Schiefkörpern", Journal für die reine und angewandte Mathematik, Band 166, 1932, pgs. 241 a 252. A demonstração de Brauer pressupõe $\mathfrak{p}$ um corpo perfeito.

visão. Como pode escrever-se $\gamma \neq \overline{\mathcal{G}}_t$, segue-se $\gamma \cong \mathcal{L}_t$, com $\mathcal{L} \neq \overline{\mathcal{G}}$. Será, pois, $\mathcal{L} \cong \mathcal{P}$, $\overline{\mathcal{G}} = \mathcal{P}$, visto que $\mathcal{P}$ é comutativo. Pondo ainda $\mathcal{P}_m = (\cdots e_{ij} \cdots)$ $\overline{\gamma} = \mathcal{P}_t \times \overline{\gamma} = \mathcal{P}_t \times \mathcal{P}_s$, reconhece-se a seguinte proposição, também já demonstrada no § 4 do Cap. VI:

Corolário 5:- Se uma álgebra $\mathcal{P}_m$ contém uma sub-álgebra $\mathcal{P}_t$ com o mesmo elemento um que $\mathcal{P}_m$, t é divisor de m, e a sub-álgebra comutável (comutador) $\overline{\mathcal{P}}_t = \mathcal{P}_s$, é tal que $\mathcal{P}_m = \mathcal{P}_t \times \mathcal{P}_s$.

Teorema 4:- É condição necessária e suficiente, para que em $\mathcal{P}_m$ exista uma sub-álgebra comutativa Σ (com o mesmo elemento um que a álgebra normal simples $\mathcal{P}_m$) equivalente a uma álgebra de divisão Ω sobre $\mathcal{P}$, que a ordem $(\Omega/\mathcal{P}) = t$ divida m. O comutador de Σ é uma álgebra completa de matrizes sobre Σ, $\Sigma_s = \overline{\Sigma}$, supondo $m = st$.(1) Se Σ existe, Ω está mergulhada em $\mathcal{P}_m$, o módulo $\mathcal{M}$ de representação de Ω em $\mathcal{L} = \mathcal{P}$ é uma soma de s sub-módulos isomorfos de ideais esquerdos simples de $\Omega_{\mathcal{L}} = \Omega$, ou seja isomorfos de Ω. Ter-se-á $m = s.(\Omega/\mathcal{P})$. Escrevendo $\overline{\Sigma} = \overline{\mathcal{G}}_s$, $\overline{\mathcal{G}}$ é anti-isomorfo de Σ. A comutatividade dá, em seguida, $\overline{\mathcal{G}} \cong \Sigma$. Inversamente, pondo $m = st$, consideremos a álgebra comutativa de divisão Ω, sobre $\mathcal{P}$, de ordem t, e bem assim a sua única representação irredutível em $\mathcal{P}$. Essa representação, que é fiel, pertence ao próprio módulo Ω, de sorte que é do grau t. Isto significa que existe em $\mathcal{P}_t$, e, portanto, em $\mathcal{P}_m$, uma sub-álgebra equivalente a Ω, q. e. d.

A parte directa do teorema anterior pode estender-se a uma álgebra normal simples $\mathcal{A}_m$ sobre $\mathcal{P}$. O comutador $\overline{\Sigma}$ tem precisamente o centro Σ, pelo que é álgebra normal simples sobre Σ. A ordem $(\overline{\Sigma}/\Sigma)$ é um quadrado perfeito n_1^2, podendo escrever-se $(\overline{\Sigma}/\mathcal{P}) = (\overline{\Sigma}/\Sigma)(\Sigma/\mathcal{P}) = n_1^2(\Sigma/\mathcal{P})$. Como, por outro lado, se tem $(\Sigma/\mathcal{P})(\overline{\Sigma}/\mathcal{P}) = (\mathcal{A}_m/\mathcal{P}) = m^2(\mathcal{A}/\mathcal{P}) = N_1^2$, resulta imediatamente $N^2 = n_1^2(\Sigma/\mathcal{P})_1^2$, $N = n_1.(\Sigma/\mathcal{P})$. Vale, assim, o

(1) Albert, pgs. 52 e 53. No enunciado, Σ_s significa anel isomorfo do anel das matrizes de grau s com elementos de Σ. Esse anel é sub-álgebra de $\mathcal{P}_m$.

Teorema 5:- Se a ordem da álgebra normal simples $\mathcal{A}_m$ sobre $\mathcal{P}$ for N_1^2, a ordem duma sub-álgebra comutativa de divisão Σ, com o mesmo elemento um que $\mathcal{A}_m$, divide N, e o comutador $\overline{\Sigma}_1$ de Σ, em $\mathcal{A}_m$, é uma álgebra normal simples sobre Σ, de ordem n_1^2, tal que $N = n_1.(\Sigma/\mathcal{P})$.

Mantendo as hipóteses do teorema 3, é claro que $\overline{\gamma}$ (ou γ), como no teorema 2, será corpo, se γ (ou $\overline{\gamma}$) estiver mergulhada de modo irredutível em $\mathcal{A}_m$ (então ter-se-á $m = r$).

Continuemos com a álgebra simples γ, sobre $\mathcal{P}$, do teorema 3. γ está mergulhada de modo redutível em $\mathcal{A}_m$, com uma multiplicidade s tal que $m = rs$. Em $\mathcal{A}_r$ está γ mergulhada de modo irredutível, e o sistema de matrizes da representação directa correspondente constitui uma representação fiel de γ (razão pela qual será ainda designado por γ). As matrizes de $\mathcal{A}_r$ que comutam com γ formam um corpo (álgebra de divisão sobre $\mathcal{P}$) $\overline{\mathcal{R}} \cong \overline{\mathcal{G}} \neq \mathcal{F}$. Tem-se o seguinte esquema:

$$\gamma, \mathcal{A}_m, \quad s, \quad m = rs, \quad \overline{\gamma} = \overline{\mathcal{G}}_s, \quad \overline{\mathcal{G}} \neq \mathcal{F}, \quad \gamma_{\mathcal{L}} = \mathcal{F}_t;$$

$$\gamma, \mathcal{A}_r, \quad 1 \quad r = r.1, \quad \overline{\mathcal{R}} = \overline{\mathcal{R}}_1, \quad \overline{\mathcal{R}} \neq \mathcal{F}' = \mathcal{F}; \gamma_{\mathcal{L}} = \mathcal{F}_t'.$$

Repitamos o raciocínio sobre $\overline{\mathcal{R}}$. $\overline{\mathcal{R}}$ está mergulhada em $\mathcal{A}_r$ de modo redutível, com uma multiplicidade q tal que $r = pq$. Em $\mathcal{A}_p$ está $\overline{\mathcal{R}}$ mergulhada de modo irredutível. O comutador γ_1 de $\overline{\mathcal{R}}$ em $\mathcal{A}_r$, é da forma $\gamma = \vartheta_q$, onde a álgebra de divisão ϑ, sobre $\mathcal{P}$, é anti-isomorfa dum corpo $\mathcal{F}''$ tal que $\overline{\mathcal{R}}_{\mathcal{L}} = \mathcal{F}_p''$. O comutador de $\overline{\mathcal{R}}$ em $\mathcal{A}_p$ é um corpo $\overline{\overline{\mathcal{R}}}$ (álgebra de divisão sobre $\mathcal{P}$) anti-isomorfo de $\mathcal{F}''$, e, portanto, isomorfo de ϑ. Tem-se o seguinte esquema:

$$\overline{\mathcal{R}}, \mathcal{A}_r, \quad q, \quad r = pq, \quad \gamma = \vartheta_q, \quad \vartheta \neq \mathcal{F}'', \quad \overline{\mathcal{R}}_{\mathcal{L}} = \mathcal{F}_p'';$$

$$\overline{\mathcal{R}}, \mathcal{A}_p, \quad 1 \quad p = p.1, \quad \overline{\overline{\mathcal{R}}} = \overline{\mathcal{R}}_1, \quad \overline{\overline{\mathcal{R}}} \neq \mathcal{F}''' = \mathcal{F}'', \quad \overline{\mathcal{R}}_{\mathcal{L}} = \mathcal{F}_p'''.$$

Do primeiro esquema tira-se $\overline{\mathcal{R}} \cong \mathcal{Z}$. Do segundo tira-se $\mathcal{R} \cong \mathcal{D}$. Assim:

Teorema 6:- Se $\mathcal{A}$ é ampliação finita do seu centro $\mathcal{P}$, toda a sub-álgebra simples $\mathcal{T}$, sobre $\mathcal{P}$, contida em $\mathcal{A}_m$ e com o mesmo elemento um que esta, escrita sob a forma $\mathcal{T} = \mathcal{D}_q$, onde $\mathcal{D}$ é uma álgebra de divisão sobre $\mathcal{P}$, tem um comutador $\overline{\mathcal{T}} = \mathcal{Z}_s$, sub-álgebra sobre $\mathcal{P}$ ainda com o mesmo elemento um que $\mathcal{A}_m$, tal que os corpos $\mathcal{Z}$ e $\mathcal{D}$ são isomorfos de corpos $\mathcal{R}$ e $\overline{\mathcal{R}}$, os quais são comutadores recíprocos contidos em $\mathcal{A}_n$, com $m = sr = s\,q\,p$.

Podemos dar da primeira parte do teorema 3 outro enunciado, que constitui a primeira parte do seguinte

Teorema 3':- As sub-álgebras simples duma álgebra normal simples $\mathcal{A}_\gamma$, quando têm o mesmo elemento um que a álgebra, associam-se em pares $(\mathcal{T}, \overline{\mathcal{T}})$, de tal modo que cada uma delas constitui o comutador da outra. O comutador do centro comum $\mathcal{Z}$, de $\mathcal{T}$ e $\overline{\mathcal{T}}$, é o produto directo $\mathcal{T} \times \overline{\mathcal{T}}$, considerados os factores como álgebras sobre $\mathcal{Z}$.(1) A demonstração da parte final faz-se como segue. $\mathcal{T}$ e $\overline{\mathcal{T}}$ são álgebras normais simples sobre $\mathcal{Z}$ e o produto $\mathcal{T}\,\overline{\mathcal{T}}$ é uma imagem homomorfa, em $\mathcal{A}_\gamma$, do produto directo $\mathcal{T} \times \overline{\mathcal{T}}$ dessas álgebras. Este produto directo é uma álgebra normal simples sobre $\mathcal{Z}$, pelo que uma sua imagem homomorfa será isomorfa. Dentro de $\mathcal{A}_\gamma$ é, pois, $\mathcal{T}\,\overline{\mathcal{T}} = \mathcal{T} \times \overline{\mathcal{T}}$ (Cfr. Cap.VI, § 12). Ora $\mathcal{T}\,\overline{\mathcal{T}}$ faz parte do comutador de $\mathcal{Z}$, e, se considerarmos $\mathcal{Z}$ como sub-álgebra de $\mathcal{A}_\gamma$ (com o mesmo elemento um que $\mathcal{A}_\gamma$), o comutador $\overline{\mathcal{Z}}$ é uma sub-álgebra de $\mathcal{A}_\gamma$ da forma $\overline{\mathcal{Z}} = \mathcal{Z}_n$, com

(1) R.Brauer (última citação, pgs.248) e Albert, pgs.53 e 54. Não esqueçamos que, não obstante a bibliografia indicada, as demonstrações são, no geral, as de E.Noether. No livro de Deuring, Algebren, Cap.IV, pgs.40 a 49, sucede outro tanto.

$$(\overline{\mathcal{Z}}/\mathcal{Z}) = n^2, \quad (\mathcal{A}_\gamma/\mathcal{R}) = N^2, \quad N = n.(\mathcal{Z}/\mathcal{P}).$$

Tendo em conta as relações

$$(\mathcal{T}/\mathcal{Z})(\overline{\mathcal{T}}/\mathcal{Z})(\mathcal{Z}/\mathcal{P})^2 = (\mathcal{A}_\gamma/\mathcal{P}) = N^2 = n^2(\mathcal{Z}/\mathcal{P})^2,$$

conclui-se que é $(\mathcal{T}/\mathcal{Z})(\overline{\mathcal{T}}/\mathcal{Z}) = n^2$, e, portanto, $\overline{\mathcal{Z}} = \mathcal{T} \times \overline{\mathcal{T}}$, q.e.d.

É claro que qualquer outro sistema hiper-complexo simples, contido em $\mathcal{A}_\gamma$, que tenha $\mathcal{Z}$ por centro, pertence necessàriamente a $\overline{\mathcal{Z}}$, o qual é máximo neste sentido.

No caso particular de $\mathcal{T}$ ser normal simples sobre $\mathcal{P}$, o produto directo $\mathcal{T} \times \overline{\mathcal{T}}$ é a própria álgebra $\mathcal{A}_\gamma$, pelo que pode dizer-se:

Corolário 6:- Se uma sub-álgebra simples $\mathcal{T}$ da álgebra normal simples $\mathcal{A}_\gamma$ é normal, o comutador $\overline{\mathcal{T}}$ é tal que $\mathcal{T} \times \overline{\mathcal{T}} = \mathcal{A}_\gamma$.(1)

Este corolário aparece também contido na seguinte proposição, que generaliza o teorema enunciado a pgs.140:

Teorema:- Se $\mathcal{A}_\gamma$ é uma álgebra qualquer (sobre $\mathcal{P}$) com elemento um e se $\mathcal{U}$ é uma sub álgebra normal simples com o mesmo elemento um, pode sempre escrever-se $\mathcal{A}_\gamma = \mathcal{U} \times \mathcal{L}$, onde $\mathcal{L}$ é uma sub-álgebra, precisamente o comutador de $\mathcal{U}$, em $\mathcal{A}_\gamma$.(2) Com efeito, consideremos o produto directo $\mathcal{A}_\gamma \times \mathcal{U}^{-1}$. Ela contém $\mathcal{U} \times \mathcal{U}^{-1} = \mathcal{P}_m$, de sorte que (pgs.140) $\mathcal{A}_\gamma \times \mathcal{U}^{-1} = \mathcal{P}_m \times \mathcal{L}$, onde $\mathcal{L}$ é o comutador de $\mathcal{P}_m$. Tem-se, por consequência, $\mathcal{A}_\gamma \times \mathcal{U}^{-1} = (\mathcal{U} \times \mathcal{L}) \times \mathcal{U}^{-1}$. Como $\mathcal{U}^{-1}$ é normal, segue-se $\mathcal{A}_\gamma = \mathcal{U} \times \mathcal{L}$ (pgs.164); e, como $\mathcal{U}$ é normal, $\mathcal{L}$ é o comutador de $\mathcal{U}$, em $\mathcal{A}_\gamma$ [Bem entendido que o elemento um de $\mathcal{A}_\gamma$ se pode supor elemento um de $\mathcal{U}$, $\mathcal{U}^{-1}$ e $\mathcal{A}_\gamma \times \mathcal{U}$; e, então, $\mathcal{L}$ tem ainda o mesmo elemento um e é sub-álgebra de $\mathcal{A}_\gamma$.

(1) R.Brauer, última citação, pgs.249. $\mathcal{A}_\gamma$ e $\mathcal{T}$ têm o mesmo elemento um.

(2) Albert, pgs.51.

Uma álgebra normal simples $\mathcal{G} = \mathfrak{h}_m$, sobre $\mathfrak{P}$, diz-se primária, se não contiver sub-álgebra normal simples própria. Pondo $\mathfrak{h}_m = \mathfrak{P}_m \times \mathfrak{h}$, $\mathfrak{h}$ é sub-álgebra normal própria de $\mathcal{G}$, salvo se m=1. Supondo que a álgebra primária não é álgebra de divisão, tem-se $\mathfrak{h}_m \neq \mathfrak{h}$, pelo que $\mathfrak{h}$ deverá reduzir-se necessàriamente a $\mathfrak{P}$. Então é $\mathfrak{h}_m = \mathfrak{P}_m$ e m só pode ser um número primo p. Vale o

Teorema 7:- Uma álgebra primária ou é álgebra de divisão ou anel completo de matrizes sobre o corpo fundamental. Neste caso o grau das matrizes é um número primo p.

Reciprocamente, um anel $\mathfrak{P}_p$ é sempre uma álgebra primária sobre $\mathfrak{P}$, pois que, sendo p^2 a sua ordem, uma sub-álgebra normal simples própria teria igualmente uma ordem igual a um quadrado perfeito, isto é, teria a ordem 1 ou p. Dada, portanto, uma álgebra normal simples qualquer, $\mathcal{G} = \mathfrak{h}_m$, ponhamos $\mathcal{G} = \mathfrak{P}_m \times \mathfrak{h}$. Da decomposição $m = p_1 \cdots p_r$ em factores primos (iguais ou não) resulta $\mathfrak{P}_m = \mathfrak{P}_{p_1} \times \cdots \times \mathfrak{P}_{p_r}$. Quanto à álgebra normal de divisão $\mathfrak{h}$, se não se trata de álgebra primária, uma decomposição $\mathfrak{h} = \mathfrak{o}_1 \times \mathfrak{o}_2$ com $\mathfrak{o}_1$ normal simples, implica $\mathfrak{o}_2$ normal e simples. Prosseguindo, chega-se a decompor $\mathfrak{h}$ em álgebras primárias. É claro que a decomposição escrita para $\mathfrak{h}$ é garantida pelo corolário 6. Daqui o

Teorema 8:- Toda a álgebra normal simples é um produto directo de álgebras primárias.

5) Sistemas hiper-complexos comutativos. Representações do centro - Seja $\mathcal{Z}$ um sistema hiper-complexo comutativo qualquer, com o corpo fundamental $\mathfrak{P}$. Dado o corpo comutativo $\mathfrak{h} \supseteq \mathfrak{P}$, vejamos se poderá haver representações do 1º grau de $\mathcal{Z}$ em $\mathfrak{h}$. Essas representações serão homomorfismos anulares operatórios de $\mathcal{Z}$ em $\mathfrak{h}$. Inversamente, um tal homomorfismo determina uma representação do 1º grau. Duas representações equivalentes são iguais:

$$a \longrightarrow A \in \mathfrak{h}, \qquad (a \in \mathcal{Z}),$$

$$a \longrightarrow A' = \lambda^{-1} A \lambda = A, \qquad (\lambda \in \mathfrak{h}).$$

Deste modo, tem lugar o

Teorema 1:- As representações não equivalentes do 1º grau de $\mathcal{Z}$ em $\mathfrak{h} \supseteq \mathfrak{P}$ são os homomorfismos operatórios (relativamente a $\mathfrak{P}$) não iguais de $\mathcal{Z}$ em $\mathfrak{h}$.

As representações assim obtidas são irredutíveis, pelo que figuram na representação regular de $\mathcal{Z}_{\mathfrak{h}}$. Todavia pode haver outras representações irredutíveis.

Suponhamos $\mathfrak{h} = \Omega$ um corpo algèbricamente fechado. Vamos demonstrar o seguinte

Teorema 2:- As representações irredutíveis dum sistema hiper-complexo comutativo num corpo algèbricamente fechado são, necessàriamente, do 1º grau. Uma representação irredutível é uma parte da representação absolutamente irredutível de $\mathcal{Z}_\Omega$, em Ω. Esta última, por sua vez, é a representação irredutível do sistema semi-simples comutativo $\mathcal{Z}' = \mathcal{Z}_\Omega / \mathcal{R}$, ($\mathcal{R}$ = radical de $\mathcal{Z}_\Omega$) ao qual se pode dar a forma

$$\mathcal{Z}' = \mathfrak{o}'_1 + \cdots + \mathfrak{o}'_s , \qquad (4)$$

como soma directa de anéis simples que são corpos comutativos. A representação em causa pertence a um $\mathfrak{o}'_i$. Ora $\mathfrak{o}'_i$, como álgebra de divisão sobre um corpo algèbricamente fechado, é necessàriamente de 1ª ordem. Em (4) encontra-se a decomposição de $\mathcal{Z}'$ necessária à sua representação regular, podendo afirmar-se o

Teorema 3:- O número de representações irredutíveis de $\mathcal{Z}$ em Ω é igual à característica de $\mathcal{Z}_\Omega / \mathcal{R}$ e igual ao número de homomorfismos não iguais de $\mathcal{Z}$ em Ω.

Seja $\mathcal{Z}$ um corpo comutativo finito relativamente a $\mathfrak{P}$, de grau n. As representações do 1º grau de $\mathcal{Z}$ em Ω, ou homomorfismos operatórios $\mathcal{Z} \sim \Omega' \overset{\alpha}{=} \Omega$ (pondo de parte a representação nula), são aqui isomorfismos relativos a $\mathfrak{P}$, isto é, isomorfismos que são o prolongamento do isomorfismo idêntico de $\mathfrak{P}$. Se $\mathcal{Z}$ é uma ampliação separável de $\mathfrak{P}$, o número de representações irredutíveis é dado pela ordem $(\mathcal{Z}/\mathfrak{P}) = n$. Tendo em con-

ta o teorema anterior, deverá ser $(\mathfrak{z}_\Omega/\Omega) = n =$ à característica de $\mathfrak{z}_\Omega/\mathfrak{R}$ relativamente a Ω. Ora isto exige $\mathfrak{R} = (0)$. Tanto $\mathfrak{z}_\Omega$ como $\mathfrak{z}$ não têm radical. Inversamente, se $\mathfrak{z}_\Omega$ não tem radical, o número de representações irredutíveis de $\mathfrak{z}$ em Ω é igual a $(\mathfrak{z}_\Omega/\Omega) = (\mathfrak{z}/\mathfrak{p})$. Como esse número é igual ao número de isomorfismos (em Ω) de $\mathfrak{z}$ relativos a $\mathfrak{p}$, $\mathfrak{z}$ é ampliação separável de $\mathfrak{p}$. Pode enunciar-se a proposição seguinte, conhecida do Cap.VII:

Teorema 4:- Se $\mathfrak{z}$ é um corpo comutativo, ampliação algébrica finita de $\mathfrak{p}$, é necessário e suficiente, para que $\mathfrak{z}_\Omega$ (com Ω algèbricamente fechado) não tenha radical, que $\mathfrak{z}$ seja ampliação separável de $\mathfrak{p}$.

Seja agora $\mathfrak{H}$ um sistema hiper-complexo qualquer, de corpo fundamental $\mathfrak{p}$. Numa representação do sistema, cada elemento do centro é representado por uma matriz que comuta com todas as matrizes da representação. Se se trata duma representação absolutamente irredutível de $\mathfrak{H}$, e, portanto, duma representação irredutível no corpo algèbricamente fechado $\Omega \supseteq \mathfrak{p}$, a representação de $\mathfrak{H}_\Omega$ é um anel completo de matrizes com elementos de Ω e os elementos do centro $\mathfrak{z}_\Omega$ são representados por matrizes múltiplas da matriz unidade. Como o centro $\mathfrak{z}$, de $\mathfrak{H}$, está contido naquele centro, podemos concluir o

Teorema 5:- Numa representação absolutamente irredutível de $\mathfrak{H}$, o centro é representado por matrizes diagonais múltiplas da matriz unidade. Se $\mathfrak{H}$ é comutativo, é o seu próprio centro. Então, como de resto já poderia ter-se concluido do teorema 2, é válida a seguinte afirmação: as representações absolutamente irredutíveis dum sistema hiper-complexo comutativo são do 1º grau.

Postas estas considerações, vamos tratar o problema das representações do centro dum sistema sem radical.(1) Ponhamos

$$\mathfrak{H} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_s, \qquad \mathfrak{z} = \mathfrak{z}_1 + \ldots + \mathfrak{z}_s, \tag{5}$$

(1) Nas considerações deste § e dos dois seguintes, regressámos a E.Noether, "Hyperkomplexe Grössen und Darstellungstheorie." Cfr. também van der Waerden, "Moderne Algebra", II Teil, pgs.184 e seguintes.

onde os $\mathfrak{z}_k$ são os centro dos $\mathfrak{a}_i$, e tenhamos em conta a correspondência biunívoca das duas decomposições. As classes das representações irredutíveis de $\mathfrak{H}$ e de $\mathfrak{z}$ são em número igual a s. Duma maneira precisa, podemos enunciar o seguinte

Teorema 6:- O sistema hiper-complexo $\mathfrak{H}$ sem radical tem tantas representações irredutíveis não equivalentes quantas as do seu centro $\mathfrak{z}$. Decompostos $\mathfrak{H}$ e $\mathfrak{z}$ sob as formas (5), a cada representação $\mathfrak{d}_i$, de $\mathfrak{H}$, pertencente a um ideal esquerdo de $\mathfrak{a}_i$, corresponde uma representação $\mathfrak{d}_i'$, de $\mathfrak{z}$, pertencente ao respectivo centro $\mathfrak{z}_i$. Naquela, os $\mathfrak{a}_k$, com $k \neq i$, são representados por matrizes nulas; em $\mathfrak{d}_i'$ sucede o mesmo aos $\mathfrak{z}_k$.

Se o corpo fundamental e de representação, Ω, é algèbricamente fechado, podemos afirmar que os $\mathfrak{z}_i$ são de característica 1 relativamente a Ω, e, deste modo, afirmar:

Teorema 7:- O número de representações irredutíveis dum sistema hiper-complexo sem radical no seu corpo fundamental, suposto algèbricamente fechado, é igual à característica do centro do sistema. Neste caso, se, na representação $\mathfrak{d}_i$, um elemento $z \in \mathfrak{z}$ é representado pela matriz $\zeta_i E$ (E = matriz unidade), o elemento ζ_i pertence a Ω e a correspondência $z \rightarrow \zeta_i$ define uma representação do 1º grau de $\mathfrak{z}$. Na referida representação, um elemento de $\mathfrak{z}_k$, com $k \neq i$, é representado pelo elemento nulo de Ω. Como a representação irredutível $\mathfrak{d}_i'$, bem determinada, é a única nessas condições, a correspondência $z \rightarrow \zeta_i$ coincide com $\mathfrak{d}_i'$.

Podemos adoptar ainda outra forma de expressão. Seja $\mathfrak{H}$ um sistema sem radical, de corpo fundamental $\mathfrak{p}$, e suponhamos que $\mathfrak{H}_\Omega$ também não tem radical. As representações absolutamente irredutíveis de $\mathfrak{H}$, em Ω (mais simplesmente: representações irredutíveis de $\mathfrak{H}$, em Ω), são em número igual à característica de $\mathfrak{z}_\Omega$ (sobre Ω), ou de $\mathfrak{z}$ (sobre $\mathfrak{p}$). Numa tal representação, os elementos de $\mathfrak{z}$ (os quais estão contidos em $\mathfrak{z}_\Omega$) são representados por matrizes múltiplas da matriz unidade. Se nela se tiver, por ex., $z \rightarrow \zeta_i E$, há uma correspondência biunívoca entre a representação irredutível (em Ω) $z \rightarrow \zeta_i$, de $\mathfrak{z}$, e a representação irredutível correspondente de $\mathfrak{H}$. Em vez do teorema 7, po-

demos dizer:

Teorema 7':- O número de representações irredutíveis duma álgebra separável (sobre $\mathcal{P}$) no corpo algèbricamente fechado $\Omega \supseteq \mathcal{P}$ é igual à característica do centro da álgebra. Cada representação absolutamente irredutível correspondente fica determinada, conhecida a respectiva representação do centro.

6) Traços e caracteres - Numa representação $\mathcal{D}$ do sistema hiper-complexo $\mathcal{H}$, se A for a matriz correspondente ao elemento $a \in \mathcal{H}$, diz-se traço de a o traço da matriz A, e escreve-se $T(a) = T(A) = \sum a_{ii}$ = soma dos elementos diagonais de A. Querendo por em evidência a variabilidade do elemento a e da matriz A, pode também escrever-se $T_{\mathcal{D}}(a) = T_{\mathcal{D}}(A)$. A definição de traço é indiferente à noção de classe de representação, pelo facto de terem o mesmo traço duas matrizes A e $A' = P^{-1}AP$. O traço é uma função linear de a:

$$T(a + b) = T(a) + T(b), \quad T(a\lambda) = T(a).\lambda, \qquad (\lambda \in \mathcal{P}).$$

Uma matriz redutível tem um traço igual à soma dos traços das matrizes irredutíveis que comparecem em escada diagonal, como é imediato.

A definição de traço não implica, é claro, que o corpo de representação seja o corpo fundamental do sistema. Examinemos as noções de traço principal e de traço reduzido. O traço principal é o traço da representação regular do sistema $\mathcal{H}$, e o traço reduzido é a soma dos traços das representações irredutíveis não equivalentes. Quando $\mathcal{H}$, sobre $\mathcal{P}$, se amplia para $\mathcal{H}_\Omega$, com $\mathcal{P} \subseteq \Omega$, a nova representação regular, obtida, como a anterior, à custa das matrizes bases correspondentes aos elementos bases do sistema hiper-complexo, mantém as matrizes representativas dos antigos elementos de $\mathcal{H}$. No tocante ao traço reduzido, embora o seu valor mude como corpo de representação, a definição pode compreender-se qualquer que seja esse corpo.

Teorema 1:- Numa representação dum sistema qualquer $\mathcal{H}$ (sobre $\mathcal{P}$), em $\mathcal{P}$, o radical é representado por elementos de traço nulo. De facto, tendo em conta que, numa representação redutível, o traço é a soma dos traços das irredutíveis que nela comparecem em escada diagonal, vamos fazer a demonstração para uma representação irredutível. Esta pertencerá a um ideal esquerdo simples, $\mathcal{W}'$, de $\mathcal{H}/\mathcal{R}$. Ora é, como se sabe, $\mathcal{R}\mathcal{W}' = (0)$. Para uma representação de $\mathcal{H}$ em $\Delta \supseteq \mathcal{P}$, o teorema é ainda válido.

Seja $\mathcal{H}$ um sistema hiper-complexo simples (sem radical). Se o corpo fundamental Ω é algèbricamente fechado (então é $\mathcal{H} = \Omega_n$), a representação irredutível única de $\mathcal{H}$, em Ω, que faz corresponder ao elemento $a \in \mathcal{H}$ a matriz $A = (a_{ij})$, dá as seguintes relações:

Traço reduzido de $a = \sum_i a_{ii}$; Traço principal de $a = n.\sum a_{ii}$;

Traço de $e_{ij} = 0$; Traço de $e_{ii} = u$; Traço princ. de $e_{ii} = nu$.

Quando se trata de representações absolutamente irredutíveis de $\mathcal{H}$, e, portanto, de representações irredutíveis de $\mathcal{H}_\Omega$, em Ω, os traços dos elementos dizem-se caracteres, escrevendo-se $\chi(a)$ para representar o caracter de a.

Seja $\mathcal{H}$ um sistema sem radical, sobre o corpo algèbricamente fechado Ω. O centro $\mathcal{Z}$, numa representação $\mathcal{D}_\nu$, é representado por matrizes múltiplas da matriz unidade. Se $z \in \mathcal{Z}$, tem-se $z \longrightarrow \Theta_\nu(z)U_{n_\nu}$, onde o índice n_ν, posto na matriz unidade, está a lembrar o grau da representação. É, então,

$$\chi(z) = \chi_\nu(z) = n_\nu \Theta_\nu(z) .$$

Se a característica de Ω não divide n_ν, a igualdade anterior dá

$$\Theta_\nu(z) = \frac{\chi_\nu(z)}{n_\nu u} .$$

Sabemos que a correspondência $z \longrightarrow \Theta_\nu(z)$ é uma representação do 1º grau (irredutível) de $\mathcal{Z}$, e, portanto, um homomorfismo de $\mathcal{Z}$ em Ω. Por outro lado, estudando todas as representações irredutíveis do sistema $\mathcal{H}$, obtêm-se todas as representa-

ções irredutíveis (do 1º grau) de $\mathcal{Z}$. Tem lugar o seguinte

Teorema 2:- Se $\mathcal{G}$ é um sistema hiper-complexo sem radical sobre um corpo algèbricamente fechado Ω, os homomorfismos $\mathcal{Z} \sim \Omega$ do centro $\mathcal{Z}$ (operatórios relativamente a Ω) exprimem-se nos caracteres.

O homomorfismo $z \longrightarrow \chi_\nu(z)$ verifica, naturalmente, as relações

$$\frac{\chi_\nu(z+z')}{n_\nu u} = \frac{\chi_\nu(z)}{n_\nu u} + \frac{\chi_\nu(z')}{n_\nu u} \; ; \; \frac{\chi_\nu(z\,z')}{n_\nu u} = \frac{\chi_\nu(z)}{n_\nu u}\cdot\frac{\chi_\nu(z')}{n_\nu u} \; ; \; \frac{\chi_\nu(z\lambda)}{n_\nu u} = \frac{\chi_\nu(z)}{n_\nu u}\cdot\lambda$$

No que vai agora dizer-se, a fim de serem evitadas dificuldades que se prendem com a noção de característica dum corpo, supor-se-á nula a característica de $\mathcal{P}$. Não se poderá dar o caso de essa característica ser divisor dum inteiro.

Teorema 3:- O traço duma representação completamente redutível de $\mathcal{G}$, sobre $\mathcal{P}$, em $\Delta \supseteq \mathcal{P}$, define uma classe de representações. A representação completamente redutível ficará definida, logo que se conheça o número de vezes, q_ν, que figura em escada diagonal cada representação irredutível, que designaremos por D_ν. Seja e_ν o elemento um da parcela α_ν (simples) da decomposição de $\mathcal{G}_\Delta / \mathcal{R}$, à qual corresponde D_ν. Tem-se $T(e_\nu) = q_\nu n_\nu u$, (n_ν = grau de D_ν), igualdade que dá q_ν, visto que $T(e_\nu)$ é conhecido por hipótese. O teorema está demonstrado.

No caso dum grupo finito, os traços de cada elemento da Álgebra do grupo ficam conhecidos, uma vez conhecidos os traços dos elementos do grupo. Portanto:

Teorema 4:- Os traços dos elementos dum grupo, numa representação completamente redutível deste, se a representação tiver lugar num corpo de característica nula, definem uma classe de representações.

Numa representação qualquer de $\mathcal{G}$, sobre $\mathcal{P}$, em $\Delta \supseteq \mathcal{P}$, os traços são sempre somas de traços de representações irredutíveis, e correspondem, dessa maneira, a uma representação completamente redutível. Se a base de $\mathcal{G}$ for $(e_1, \ldots, e_n)$, o conhecimento dos traços dos e_i determina o de todos os elementos de $\mathcal{G}$.

Supondo Δ de característica nula, o conhecimento dos traços dos e_i é suficiente para a construção, pondo de parte equivalências, das representações irredutíveis que comparecem em diagonal, quando se procede à redução da representação. Se for q_ν o número de vezes que comparece D_ν, ter-se-á:

$$T(e_i) = \sum_{\nu=1}^{s} q_\nu T_\nu(e_i) \; ,$$

onde s significa o número de representações irredutíveis de $\mathcal{G}$ (em Δ). O sistema anterior de equações, com coeficientes conhecidos $T_\nu(e_i) \in \Delta$, dá as incógnitas q_ν, como se precisa.

Teorema 5:- O traço duma representação completamente redutível dum grupo infinito num corpo Δ, de característica nula, define uma classe de representações. Consideremos, com efeito, duas representações completamente redutíveis, de grau finito, do grupo, que tenham o mesmo traço. As duas representações, colocadas em diagonal, uma a seguir à outra, definem uma representação completamente redutível, cujas matrizes, afectadas de coeficientes do corpo de representação e combinadas por via de soma e de produto, geram um anel, que é um absoluto, ou seja um sistema hiper-complexo sem radical. Ora duas representações completamente redutíveis (componentes) dum sistema hiper-complexo que tenham o mesmo traço pertencem à mesma classe.

7) Descriminantes - Neste §, por simplicidade, empregaremos os símbolos T_p e T_r para designarem, respectivamente, traço principal e traço reduzido.

Seja $\mathcal{G}$ um sistema hiper-complexo qualquer. Se $e_1, \ldots, e_n$ constituem uma base, diz-se matriz descriminante (relativa à citada base) a matriz

$$D = \begin{pmatrix} T_p(e_1 e_1) & \ldots & T_p(e_1 e_n) \\ \cdots & \cdots & \cdots \\ T_p(e_n e_1) & \ldots & T_p(e_n e_n) \end{pmatrix} .$$

Passando de $\mathcal{G}$ a $\mathcal{G}_\Omega$ (Ω algèbricamente fechado), define-se a matriz descriminante reduzida pela igualdade

van der Waerden, Moderne Algebra, II Teil, pgs. 189.

$$\Delta = \begin{pmatrix} T_r(e_1e_1) & \cdots & T_r(e_1e_n) \\ - - - - - - - - - - - - \\ T_r(e_ne_1) & \cdots & T_r(e_ne_n) \end{pmatrix} .$$

Ω é aqui o corpo de representação. O determinante $|D|$ chama-se <u>descriminante</u> e o determinante $|\Delta|$ <u>descriminante reduzido</u>.

A matriz descriminante não muda pelo facto de se ampliar o corpo fundamental, visto que o traço principal se não altera.

Uma questão que se levanta é a de indagar como se modifica o descriminante quando se muda a base de $\mathcal{E}_f$. Se se supõe

$$(e_1, \ldots, e_n) = (u_1, \ldots, u_n).M, \qquad (6)$$

onde $M = (m_{lk})$ é uma matriz com inverso, as relações

$$\begin{aligned} e_1 &= u_1m_{11} + \cdots + u_nm_{n1} \\ &- - - - - - - - - - \\ e_n &= u_1m_{1n} + \cdots + u_nm_{nn} \end{aligned} \qquad (7)$$

dão

$$\begin{aligned} e_le_1 &= e_lu_1m_{11} + \cdots + e_lu_nm_{n1} \\ &- - - - - - - - - - - - - \\ e_le_n &= e_lu_1m_{1n} + \cdots + e_lu_nm_{nn}, \end{aligned}$$

ou seja, sob forma de matrizes,

$$(e_le_1, \ldots, e_le_n) = (e_lu_1, \ldots, e_lu_n).M .$$

A passagem aos traços dá

$$\begin{aligned} T_p(e_le_1) &= T_p(e_lu_1)\, m_{11} + \cdots + T_p(e_lu_n)\, m_{n1} \\ &- \\ T_p(e_le_n) &= T_p(e_lu_1)\, m_{1n} + \cdots + T_p(e_lu_n)\, m_{nn}, \end{aligned}$$

e, portanto, tem-se a seguinte igualdade entre matrizes:

$$\Big(T_p(e_le_k)\Big) = \Big(T_p(e_lu_k)\Big).M . \qquad (8)$$

Com a simbólica das matrizes, (6) e (7) tomam o aspecto

$$\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = M'. \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}, \qquad (M' = \text{matriz transposta de } M).$$

O mesmo tratamento que anteriormente leva a

$$\begin{pmatrix} e_1\, u_l \\ \vdots \\ e_n\, u_l \end{pmatrix} = M'. \begin{pmatrix} u_1\, u_l \\ \vdots \\ u_n\, u_l \end{pmatrix}, \quad \Big(T_p(e_lu_k)\Big) = M'.\Big(T_p(u_lu_k)\Big).$$

Por comparação de (8) com a última igualdade, tira-se

$$\Big(T_p(e_le_k)\Big) = M'.\Big(T_p(u_lu_k)\Big).M .$$

Daqui se conclui o seguinte

<u>Teorema 1</u>:-<u>O descriminante na base dos u_l é o produto do descriminante na base dos e_l pelo quadrado do determinante da transformação</u>.

Uma propriedade do descriminante que é invariante em face das mudanças de base é a de se anular ou não anular. Pode também dizer-se que o descriminante, aparte um factor que é um <u>quadrado</u> dum elemento do corpo fundamental, é bem determinado.

Teorema 2:-Um sistema com radical tem um descriminante nulo. Tomemos uma base de $\mathcal{Z}$ da forma $(w_1,\dots, w_r; e_{r+1},\dots,e_n)$ onde $(w_1,\dots, w_r)$ constitui uma base de $\mathcal{R}$. Como,em qualquer representação no corpo fundamental,os traços dos elementos de $\mathcal{R}$ são nulos,tem-se

$$T_p(w_l w_k) = T_p(w_l e_k) = T_p(e_k w_l) = 0 ,$$

e,portanto,

$$|D| = \begin{vmatrix} T_p(w_l w_k) & T_p(w_l e_k) \\ T_p(e_t w_k) & T_p(e_t e_s) \end{vmatrix} = 0 .$$

Quando $\mathcal{Z}$, sobre $\mathcal{P}$, se amplia para $\mathcal{Z}_\Omega$ ($\Omega \supseteq \mathcal{P}$), pode a ampliação ter radical, embora $\mathcal{Z}$ seja semi-simples. Tanto basta para que seja nulo o descriminante de $\mathcal{Z}$. O teorema supra não tem,pois,inverso. O teorema 4 mostrar-nos-á que,no caso dum corpo fundamental algèbricamente fechado,de característica nula,é válido o teorema inverso do actual.

Teorema 3:- Se $\mathcal{Z}$ é uma soma directa de álgebras simples $\mathfrak{a}_i$, o produto dos descriminantes destas álgebras é igual ao descriminante de $\mathcal{Z}$, pressuposto que a base de $\mathcal{Z}$ é formada pelo conjunto das bases dos $\mathfrak{a}_i$. Procuremos a matriz descriminante de $\mathcal{Z}$. Se $a_i \in \mathfrak{a}_i$, o traço principal de a_i é o mesmo, quer se considere $a_i \in \mathfrak{a}_i$ quer $a_i \in \mathcal{Z}$. Se $(e_l, e_l', e_l'',\dots)$ é uma base de $\mathfrak{a}_l$, tem-se $e_l^{(m)} e_k^{(p)} = 0$, $T_p(e_l^{(m)} e_k^{(p)}) = 0$, de sorte que vem

$$D = \begin{pmatrix} T_p(e_1e_1) & T_p(e_1e_1') \dots & & 0 \\ T_p(e_1'e_1) & T_p(e_1'e_1') \dots & & \\ \dots\dots\dots & & & \\ & & T_p(e_2e_2) & T_p(e_2e_2')\dots \\ 0 & & T_p(e_2'e_2) & T_p(e_2'e_2')\dots \\ & & \dots\dots\dots & \end{pmatrix} ,$$

ou seja $|D| = |D_1| \cdot |D_2| \dots |D_t|$, onde $|D_j|$ se supõe o descriminante de $\mathfrak{a}_j$.

Teorema 4:- É condição necessária e suficiente,para que uma álgebra $\mathcal{Z}$ (sobre $\mathcal{P}$) tenha um descriminante diferente de zero,que $\mathcal{Z}$ seja separável ($\mathcal{P}$ supõe-se de característica nula). Se $D \neq 0$, $\mathcal{Z}_\Omega$ não tem radical,pois,se o tivesse,o seu descriminante seria nulo. Ora esse descriminante é $|D|$. Vamos ver que a condição é suficiente. Se $\mathcal{Z}_\Omega$ é semi-simples,o seu descriminante é o produto dos descriminantes das álgebras simples em que se decompõe,nos termos do teorema anterior. Pelo facto de Ω ser algèbricamente fechado,uma álgebra simples sobre Ω é do tipo Ω_n. Por isso,há interesse em procurar,efectivamente,o descriminante duma álgebra $\mathcal{P}_n$, sobre $\mathcal{P}$. Designando por e_{lk} os n^2 elementos base da álgebra $\mathcal{P}_n$, tenhamos em conta a tabela da multiplicação dos mesmos elementos: $e_{lk} e_{jp} = \delta_{kj} e_{lp}$. É,então, depois duma conveniente troca de colunas,

$$|D'| = \begin{vmatrix} T_p(e_{11}) \dots T_p(e_{1n}) & & 0 \\ \dots\dots\dots & & \\ T_p(e_{n1}) \dots T(e_{nn}) & & \\ & T_p(e_{11}) \dots T_p(e_{1n}) & \\ 0 & \dots\dots\dots & \\ & T_p(e_{n1}) \dots T_p(e_{nn}) & \end{vmatrix} = \rho^n ,$$

onde ρ é o valor do determinante que figura em diagonal. Para se encontrar o valor de ρ, notemos que $T_p(e_{lk})$, com $i \neq k$, é nulo,e que $T_p(e_{ll}) = nu$. Assim,tem-se

$$|D'| = (n^n u)^n = n^{n^2} u .$$

Regressando à álgebra semi-simples $\mathcal{Z}_\Omega$, o valor do seu descriminante $|D_1|$ será

$$|D_1| = n_1^{n_1^2} \dots n_t^{n_t^2} u ,$$

onde $n_1,\dots, n_t$ designam os graus das matrizes que constituem

as álgebras simples da decomposição de $\mathcal{G}_\Omega$. Se se supõe que a característica de $\mathcal{P}$ é nula (mais geralmente, se a característica não divide qualquer n_l), tem-se $|D_1| \neq 0$, pelo que será também diferente de zero o descriminante de $\mathcal{G}$.

Relativamente ao descriminante reduzido, podem fazer-se considerações análogas.

Teorema 2':- Um sistema com radical tem um descriminante reduzido nulo. A demonstração faz-se como no teorema 2, correspondente. Não esqueçamos, com efeito, que os elementos do radical dum sistema hiper-complexo têm, numa representação qualquer, um traço igual a zero.

Também podemos dizer:

Teorema 3':- Nas condições do teorema 3, o descriminante reduzido de $\mathcal{G}$ é o produto dos descriminantes reduzidos dos $\mathcal{G}_l$.

Como no teorema 4, somos levados a procurar o descriminante reduzido duma álgebra $\mathcal{P}_n$, composta de elementos da forma $\alpha = \sum e_{lk}\alpha_{lk}$, onde $\alpha_{lk} \in \mathcal{P}$. Obtém-se, por troca de colunas,

$$|\Delta'| = \begin{vmatrix} T_r(e_{11}) & \dots & T_r(e_{1n}) \\ \dots & \dots & \dots \\ T_r(e_{n1}) & \dots & T_r(e_{nn}) \end{vmatrix}^n .$$

Mas, sendo $T_r(e_{lk}) = 0$, se $i \neq k$, e $T_r(e_{ll}) = u$, vem $|\Delta'| = u$, ou seja $|\Delta'| \neq 0$, independentemente do valor da característica de $\mathcal{P}$.

Qualquer que seja a característica de $\mathcal{P}$, consideremos uma álgebra $\mathcal{G}$, sobre $\mathcal{P}$, para a qual o descriminante reduzido seja $\Delta \neq 0$. A referida álgebra não tem radical (teorema 2'). Inversamente, seja $\mathcal{G}$ uma álgebra sem radical, e suponhamos que $\mathcal{G}_\Omega$ (Ω algèbricamente fechado) também não tem radical. O descriminante reduzido de $\mathcal{G}_\Omega$ é $|\Delta_1| \neq 0$, pois é $|\Delta_1| = u$, como vimos. Tem lugar, assim, o

Teorema 4':- Uma álgebra com descriminante reduzido diferente de zero não tem radical. A inversa é válida, se o corpo fundamental for algèbricamente fechado.

8) Aplicações aos grupos finitos - No Capítulo anterior, § 14, reduzimos a representação dum grupo finito $\mathcal{G}$ à da sua álgebra. Seja h o número de elementos de $\mathcal{G}$. Vamos demonstrar o seguinte

Teorema de Maschke :- Toda a representação dum grupo finito $\mathcal{G}$, num corpo cuja característica não divide h, é irredutível ou completamente redutível. Sabemos que toda a representação dum sistema hiper-complexo sem radical é irredutível ou completamente redutível. O teorema ficará provado, se se mostrar que a álgebra do grupo é semi-simples. É o que faremos, verificando que o respectivo descriminante é diferente de zero. Sejam $a_1, \dots, a_h$ os elementos de $\mathcal{G}$, entre os quais o elemento um, $a_1 = \varepsilon$. Na representação regular da álgebra $\mathcal{G}$ do grupo, o elemento a_1 é representado pela matriz unidade, tendo-se $T_p(a_1) = T_p(\varepsilon) = hu$. Relativamente aos produtos $a_l a_k$, em que não são ambos os elementos iguais a ε ($a_l \neq \varepsilon$, por ex.), tem-se, com a_l fixo, $a_l a_1 = a_l, \dots, a_l a_k = a_{\rho_k}$, $(\rho_j \neq j)$, de sorte que a matriz correspondente a a_l é uma matriz cujos elementos diagonais são nulos. Isto significa $T_p(a_l) = 0$, $(a_l \neq \varepsilon)$. Tomemos, então, as duas bases (ordenadas) seguintes de $\mathcal{G}$: $a_1 = \varepsilon$, $a_2, \dots, a_h$; $a_1^{-1} = \varepsilon$, $a_2^{-1}, \dots, a_h^{-1}$. Tem-se

$$|D| = |T_p(a_l a_k)| = |M| \cdot |T_p(a_l a_k^{-1})| ,$$

onde $a_1 = a_1^{-1}$, $a_2 = a_{\lambda_2}^{-1}, \dots$ e

$$M = \begin{pmatrix} u & o & o & \dots & o & \dots & o & \dots & o \\ o & o & o & \dots & u & \dots & o & \dots & o \\ o & o & o & \dots & o & \dots & u & \dots & o \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix} .$$

Como se vê (Cfr. com o começo do § anterior), a matriz quadrada M, de grau h, tem o elemento u uma só vez em cada linha e em cada coluna, pelo que se conclui $M = u$, pondo de parte o sinal. No tocante à matriz $J = (T_p(a_i a_k^{-1}))$, podemos pôr

$$J = \begin{pmatrix} T_p(a_1) & T_p(a_2^{-1}) & \dots & T_p(a_h^{-1}) \\ T_p(a_2) & T_p(a_2 a_2^{-1}) & \dots & T_p(a_2 a_h^{-1}) \\ \dots & \dots & \dots & \dots \\ T_p(a_h) & T_p(a_h a_2^{-1}) & \dots & T_p(a_h a_h^{-1}) \end{pmatrix} = \begin{pmatrix} hu & & o \\ & \ddots & \\ o & & hu \end{pmatrix},$$

de modo que se conclui $|D| = h^h u \neq 0$, visto não ser h um múltiplo da característica do corpo fundamental.

No Cap. VI, § 11, viu-se que a característica do centro da álgebra dum grupo é igual ao número de classes conjugadas equivalentes em que pode decompor-se o mesmo grupo. E como a álgebra do grupo tem tantas representações irredutíveis quantas as do seu centro, e este, no caso dum corpo fundamental algèbricamente fechado, tem tantas quantas ainda a sua característica, é válido o seguinte

Teorema:- O número de representações irredutíveis dum grupo num corpo algèbricamente fechado é igual ao número de classes de elementos conjugados do referido grupo. Podemos afirmar, de resto, que os graus $n_1, \dots, n_t$ dessas representações satisfazem à igualdade $\sum_{i=1}^{t} n_i^2 = h$.

Vamos dar do teorema de Maschke uma demonstração directa,(1) a qual uma vez feita, leva aos dois resultados seguintes, já conhecidos: 1º-Toda a representação da álgebra dum grupo é irredutível ou completamente redutível; 2º- a álgebra dum grupo é um sistema sem radical. Este segundo resultado conclui-se, notando que a representação regular é completamente redutível, e que, portanto, o módulo de representação, ou seja a própria álgebra, é completamente redutível.

(1) Cfr. van der Waerden, Moderne Algebra, II Teil, pgs. 193.

Passemos à demonstração anunciada. Seja $\mathfrak{M}$ um módulo de representação de $\mathfrak{G}$, em $\mathfrak{P}$. Se $\mathfrak{M}$ é irredutível, o teorema está provado. Se $\mathfrak{M}$ é redutível, designemos por $\mathfrak{M}_1$ um sub-módulo irredutível e façamos a decomposição de $\mathfrak{M}$ numa soma directa, tendo apenas em conta o facto de ser $\mathfrak{M}$ um módulo finito relativamente a um corpo: $\mathfrak{M} = \mathfrak{M}_1 + \mathfrak{M}'$. É possível, a partir de $\mathfrak{M}'$, construir um sub-módulo $\mathfrak{M}''$ de representação, tal que $\mathfrak{M} = \mathfrak{M}_1 + \mathfrak{M}''$. É claro que a construção de $\mathfrak{M}''$ demonstra o teorema, pois, se $\mathfrak{M}''$ não é irredutível, é possível repetir o raciocínio sobre $\mathfrak{M}''$ e continuar o processo até obter apenas sub-módulos irredutíveis, o que chega a suceder, por ser $\mathfrak{M}$ um módulo finito relativamente ao corpo de representação.

Seja $a \in \mathfrak{G}$. Se $m \in \mathfrak{M}$, a partir de $m = m_1 + m'$, $(m_1 \in \mathfrak{M}_1, m' \in \mathfrak{M}')$, pode construir-se $am' = n_1 + n'$, $(n_1 \in \mathfrak{M}_1, n' \in \mathfrak{M}')$. A correspondência $m' \longrightarrow n'$ é um endomorfismo operatório de $\mathfrak{M}'$, definido pelo elemento a. Representando-o por A', a correspondência $a \longrightarrow A'$ dá uma representação do grupo $\mathfrak{G}$, pois, se $b \longrightarrow B'$ tem-se, utilizando notações evidentes,

$$ba.m' = b.am' = b(n_1 + n') = bn_1 + bn' = bn_1 + b.A'm' = N_1 + (N_1' + M') =$$

$$= N_1'' + B'A'm'.$$

O modo de obter esta representação não nos diz, todavia, que $\mathfrak{M}'$ seja um sub-módulo de representação do grupo $\mathfrak{G}$, visto que am' não pertence a $\mathfrak{M}'$. Construamos o operador Θ definido por

$$\Theta = \frac{1}{hu} \sum_a a^{-1} A' ,$$

onde u é o elemento um de $\mathfrak{P}$. Por meio de Θ, passa-se de $\mathfrak{M}'$ a um sub-espaço $\Theta\mathfrak{M}' = \mathfrak{M}''$, que vamos ver estar nas condições exigidas. Tem-se

$$\Theta m' = \frac{1}{hu} \sum_a a^{-1} n' = \frac{1}{hu} \left(\sum_a p_1 + \sum_a p' \right) = M_1 + M' = m'' ,$$

$$(p_1 , M_1 \in \mathfrak{M}_1 ; \; p', M' \in \mathfrak{M}' ; \; m'' \in \mathfrak{M}'') .$$

Podemos também escrever

$$\ominus m' = \frac{1}{hu}\sum_a a^{-1}A'm' = \frac{1}{hu}\sum_a a^{-1}(am' - n_1) =$$

$$= \frac{1}{hu}\sum_a a^{-1}am' - \frac{1}{hu}\sum_a a^{-1}n_1 = \frac{1}{hu}\sum m' - N_1 ,$$

onde $N_1 \in \mathfrak{M}_1$. Em virtude de ser igual a m' a primeira parcela do último membro, vem $\ominus m' = m' - N_1$. Comparando esta igualdade com $m = m_1 + m'$, vê-se que

$$m = m_1 + \ominus m' + N_1 = \mu_1 + \ominus m' = \mu_1 + m'', \qquad (\mu_1 \in \mathfrak{M}_1) .$$

Deste modo, cada elemento $m \in \mathfrak{M}$ é uma soma dum elemento bem determinado $m'' \in \mathfrak{M}'' = \ominus\mathfrak{M}$ e dum elemento $\mu_1 \in \mathfrak{M}_1$. Conclui-se, portanto, a relação $\mathfrak{M} = (\mathfrak{M}_1, \mathfrak{M}'')$. Veremos, em seguida, que $\mathfrak{M}''$ é invariante em face de $\mathcal{G}$[1]. Desse modo, ter-se-á $[\mathfrak{M}_1, \mathfrak{M}'']=(0)$, visto que $\mathfrak{M}'' = \mathfrak{M}_1$ daria $\mathfrak{M} = \mathfrak{M}_1$. E, por consequência, como se quer, é $\mathfrak{M} = \mathfrak{M}_1 + \mathfrak{M}''$. A invariância referida demonstra-se como segue. Tem-se

$$bm'' = \frac{1}{hu}\sum_a ba^{-1}A'm' = \frac{1}{hu}\sum_a (ab^{-1})^{-1}(A'B'^{-1})B'm' =$$

$$= \frac{1}{hu}\sum_a c^{-1}C'.B'm' = \ominus.B'm' \in \mathfrak{M}'' .$$

A demonstração do teorema de Maschke exigiu que se fizesse a hipótese de h não ser múltiplo da característica do corpo de representação. Pode provar-se o seguinte

Teorema recíproco:- Se as representações dum grupo finito, num corpo comutativo $\mathcal{P}$, são todas irredutíveis ou completamente redutíveis, a característica do corpo não divide o número h de elementos do grupo. Consideremos o elemento S, da álgebra $\mathcal{G}$ do grupo, que é soma de todos os elementos do grupo: $S = a+b+\ldots+1$, (h parcelas). O ideal esquerdo $\mathcal{H}$, gerado por este ele-

(1) A invariância em face de $\mathcal{P}$ é imediata.

mento, é o conjunto de elementos

$$rS = (a\lambda+\ldots+1\tau)\,S = (a\lambda+\ldots+1\tau)(a+\ldots+1) = S\lambda+\ldots+$$

$$+ S\tau = S\Lambda ,$$

onde $r \in \mathcal{G}$, e $\lambda, \ldots, \tau, \Lambda \in \mathcal{P}$. O produto de dois elementos de $\mathcal{H}$ é da forma

$$rS.r'S = S\Lambda.S\Lambda' = S^2\Lambda\Lambda' = S.\Lambda\Lambda'h ,$$

pois que $S^2 = S\,S = S\,h\,u$. Admitindo que h é múltiplo da característica do corpo, vê-se que $S^2 = 0$, e que, portanto, $\mathcal{H}$ é um ideal nilpotente. O sistema $\mathcal{G}$ é um sistema com radical. Por outro lado, admite-se que a representação regular é completamente redutível, e, consequentemente, $\mathcal{G}$ não tem radical. Este absurdo prova o teorema. No caso de h não ser múltiplo da característica, o ideal $\mathcal{H}$ tem o elemento idempotente S/hu, pois

$$\frac{S}{hu}\cdot\frac{S}{hu} = \frac{S^2}{h^2u} = \frac{S.hu}{hu} = \frac{S}{hu} .$$

Trata-se, de resto, dum ideal esquerdo simples, visto que, dado $a \neq 0$ da forma $S\Lambda$, o ideal gerado por a contém $\Lambda^{-1}u.S\Lambda = S$, pelo que será idêntico a $\mathcal{H}$.

Capítulo X

Representações dos grupos

1) Espaço linear - Seja o conjunto

$$\mathfrak{M} = \{ \mathfrak{a}, \mathfrak{b}, \dots, \mathfrak{r}, \dots, \mathfrak{x}, \dots \mathfrak{z}, \dots \},$$

no qual os elementos se chamam vectores. Diz-se que se tem um espaço linear, se forem verificados os dois sistemas seguinte de postulados.

1º sistema (Postulados de adição): α) Dos dois elementos $\mathfrak{a}$ e $\mathfrak{b}$ deduz-se um elemento único $\mathfrak{z} = \mathfrak{a} + \mathfrak{b} \in \mathfrak{M}$, que se diz soma dos dois elementos; β) tres elementos $\mathfrak{a}, \mathfrak{b}, \mathfrak{z}$ verificam a propriedade associativa $(\mathfrak{a} + \mathfrak{b}) + \mathfrak{z} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{z})$; γ) dados dois elementos $\mathfrak{a}$ e $\mathfrak{b}$, existe um elemento $\mathfrak{x}$ tal que $\mathfrak{a} + \mathfrak{x} = \mathfrak{b}$; δ) tem lugar a propriedade comutativa $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$.

Este 1º sistema caracteriza $\mathfrak{M}$ como grupo abeliano aditivo ou módulo.

2º sistema (Postulados de multiplicação): α') se λ é um número complexo, existe uma multiplicação $\lambda\,\mathfrak{a}$ que leva a um elemento determinado de $\mathfrak{M}$; β') tem lugar a propriedade distributiva $\lambda(\mathfrak{a} + \mathfrak{b}) = \lambda\mathfrak{a} + \lambda\mathfrak{b}$; γ') vale a lei distributiva $(\lambda + \mu)\,\mathfrak{a} = \lambda\mathfrak{a} + \mu\mathfrak{a}$, onde μ é um número complexo; δ') vale a lei associativa $\lambda\mu \cdot \mathfrak{a} = \lambda \cdot \mu\,\mathfrak{a}$; ε') o número 1 é operador unitário: $1\mathfrak{a} = \mathfrak{a}$.(1)

Este 2º sistema caracteriza $\mathfrak{M}$ como um módulo relativo ao conjunto (corpo) dos números complexos para o qual 1 é operador unitário. Designaremos com $\mathcal{O}$ o corpo em questão.

O espaço linear diz-se um espaço finito com n dimensões,(2) se for um módulo finito com n dimensões relativamente a $\mathcal{O}$. Isto significa que podemos tomar n elementos $e_1, \dots, e_n \in \mathfrak{M}$, tais que, para cada $\mathfrak{x} \in \mathfrak{M}$, se tem, duma maneira única,

$$\mathfrak{x} = e_1 a_1 + \dots + e_n a_n , \qquad (a_i \in \mathcal{O}).$$

(1) H. Weyl, "Temps, espace, matière", Paris, 1922.

(2) ou de ordem n.

Introduziu-se, então, o postulado dimensional. Os elemtos e_i, para os quais a igualdade $\sum e_i \lambda_i = 0$ dá $\lambda_i = 0$, dizem-se linearmente independentes.(1)

Dados m vectores não nulos $\mathfrak{a}_1, \dots, \mathfrak{a}_m$, suponhamos que eles são linearmente dependentes, isto é, que é possível a relação $\mathfrak{a}_1\lambda_1 + \dots + \mathfrak{a}_m\lambda_m = 0$, sem que sejam nulos todos os λ_i. De entre os $\mathfrak{a}_i$ há r que são linearmente independentes $(m > r \geqslant 1)$, pois, se for por ex. $\mathfrak{a}_1\lambda_1 = 0$, com $\lambda_1 \neq 0$, será também $\mathfrak{a}_1\lambda_1/\lambda_1 = \mathfrak{a}_1 1 = \mathfrak{a}_1 = 0$. Imaginando, assim, que $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ são linearmente independentes, tem-se, supondo $j = r + 1, \dots, m$,

$$\mathfrak{a}_1\lambda_{1j} + \dots + \mathfrak{a}_r\lambda_{rj} - \mathfrak{a}_j\mu_j = 0,$$

sem que sejam simultâneamente nulos os λ_{ij} e o $-\mu_j$. Duma maneira mais precisa, μ_j é diferente de zero e os λ_{ij} não são todos nulos. Da igualdade anterior, tira-se

$$\mathfrak{a}_j = \mathfrak{a}_1\frac{\lambda_{1j}}{\mu_j} + \dots + \mathfrak{a}_r\frac{\lambda_{rj}}{\mu_j},$$

podendo enunciar-se o seguinte

Teorema:- No espaço linear (ou vectorial) de ordem n, m elementos não nulos, linearmente dependentes, exprimem-se por meio de $r < m$ dos mesmos elementos, linearmente independentes.

Uma segunda proposição importante é a seguinte:

Teorema:- Se no espaço vectorial de ordem n tomarmos n+1 elementos, há, necessàriamente, entre eles, uma dependência linear.

Sejam $\mathfrak{a}_1, \dots, \mathfrak{a}_{n+1}$ os vectores dados. Se algum deles for nulo ou se houver dois vectores iguais, o teorema é trivial. Por outro lado, o teorema é válido para a ordem 1. Se $\mathfrak{y}$ for a base, dados $\mathfrak{a}_1$ e $\mathfrak{a}_2$, diferentes entre si e diferentes de zero, tem-se

(1) De futuro, colocaremos os coeficientes λ à direita dos vectores.

$$\mathfrak{a}_1 = \mathfrak{y}\, a_1 , \qquad \mathfrak{a}_2 = \mathfrak{y}\, a_2 ,$$

$$\mathfrak{a}_1 \frac{1}{a_1} - \mathfrak{a}_2 \frac{1}{a_2} = 0, \qquad \left(\frac{1}{a_1}, \frac{1}{a_2} \neq 0\right).$$

Admitamos, assim, que o teorema é válido para o espaço vectorial de ordem $n-1$. Vamos demonstrar que vale para n dimensões. Quando os vectores $\mathfrak{a}_1, \ldots, \mathfrak{a}_{n+1}$ se exprimem nos $n-1$ primeiros elementos base, o teorema é verdadeiro. Seja então, contràriamente a isso,

$$\mathfrak{a}_j = \sum_{k=1}^{n} e_k\, a_{kj} , \qquad (j = 1, \ldots, n+1),$$

onde um, pelo menos, dos a_{nj} é diferente de zero. Suponhamos, por ex., $a_{n,\,n+1} \neq 0$. Podemos escrever

$$\mathfrak{a}_{n+1} \frac{1}{a_{n,n+1}} = e_n + \sum_{k=1}^{n-1} e_k \frac{a_{k,n+1}}{a_{n,n+1}} ,$$

e, consequentemente,

$$\mathfrak{a}_j = \sum_{k=1}^{n-1} e_k\, a_{kj} + \left(\mathfrak{a}_{n+1} \frac{1}{a_{n,n+1}} - \sum_{k=1}^{n-1} e_k \frac{a_{k,n+1}}{a_{n,n+1}} \right) a_{nj} ,$$

ou seja ainda

$$\sum_{k=1}^{n-1} e_k \left(a_{kj} - \frac{a_{k,n+1}}{a_{n,n+1}}\, a_{nj} \right) = \mathfrak{a}_j - \mathfrak{a}_{n+1} \frac{a_{nj}}{a_{n,n+1}} , \quad (j = 1, \ldots, n)$$

É neste momento que se aplica a hipótese feita quanto à validade do teorema no espaço a $n-1$ dimensões. Entre os n elementos de $\mathfrak{M}$ que figuram nos primeiros membros das n igualdades anteriores, existe, por hipótese, uma relação linear com coeficientes não todos nulos. Assim, existe uma relação

$$\mathfrak{a}_1 c_1 + \ldots + \mathfrak{a}_n c_n - \sum_{j=1}^{n} \mathfrak{a}_{n+1} \frac{a_{nj}}{a_{n,n+1}}\, c_j = 0 ,$$

onde os coeficientes c não são todos nulos. O teorema está demonstrado.

Corolário:- No espaço vectorial de ordem n, qualquer sistema de n elementos linearmente independentes constitui uma base. Se $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ forem os elementos em questão, para qualquer elemento $\mathfrak{x}$ vale uma relação

$$\mathfrak{x}\,\lambda = \mathfrak{b}_1 b_1 + \ldots + \mathfrak{b}_n b_n ,$$

sem que λ possa ser nulo. Daqui tira-se a expressão de $\mathfrak{x}$.

Estamos agora em condições de mostrar que a ordem n do espaço vectorial é um número bem determinado, o que justificará o enunciado do postulado dimensional sob a forma seguinte: um sistema de n vectores linearmente independentes constitui uma base de $\mathfrak{M}$.

Imaginemos que era possível representar o espaço vectorial por meio de m elementos. Se estes fossem linearmente independentes, ter-se-ia $m = n$, visto que não poderia ser $m > n$ nem tão pouco $m < n$. Mas, se os m elementos são dependentes, há $r < m$ desses elementos que são linearmente independentes, pelo que será $r = n$.(1)

Os sub-grupos admissíveis do espaço linear que acabamos de construir dizem-se sub-espaços.

Seja $\mathfrak{M}_m$ um sub-espaço no qual há m e só m vectores linearmente independentes $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$. Como estes vectores não podem constituir uma base para $\mathfrak{M}$, existe um vector $\mathfrak{a}_{m+1}$ não exprimível em $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$. Em seguida o raciocínio repete-se sobre $\mathfrak{a}_1, \ldots, \mathfrak{a}_{m+1}$, para se provar a existência de $\mathfrak{a}_{m+2}$, e assim sucessivamente, até $\mathfrak{a}_n$.

Imaginemos agora que se conhece uma base $\mathfrak{x}_1, \ldots, \mathfrak{x}_n$ de $\mathfrak{M}$ e suponhamos $\mathfrak{M}'(\mathfrak{z}_1, \ldots, \mathfrak{z}_r)$, com $r < n$, um sub-espaço de $\mathfrak{M}$. Visto que os $\mathfrak{x}_t$ se não exprimem totalmente nos $\mathfrak{z}_j$, con-

(1) Nas demonstrações anteriores, seguimos A. Adrian Albert, "Modern Higher Algebra". Para o estudo de módulos com respeito a corpos, pode ver-se Almeida Costa, "Grupos abelianos e Anéis e Ideais não comutativos", Porto, 1942, Cap. II.

sideremos um primeiro dos ε_i, por ex., ε_{r+1}, nessas condições; em seguida o sistema dos z_j e do ε_{r+1} não basta para exprimir os restantes ε_i; se for $r+1<n$. Considerando ε_{r+2} como não exprimível, juntaremos este último ao sistema dos z_j e do ε_{r+1}. E, proseguindo desta maneira, vê-se que se chega a formar uma base de n elementos, que será constituida pelos r elementos z_j e mais $n-r$ dos ε_i.

Sejam $\mathfrak{M}_k$ e $\mathfrak{M}_{n-k}$ dois sub-espaços, de ordens k e $n-k$, respectivamente. Se não têm vector comum, salvo o vector nulo, é $\mathfrak{M} = \mathfrak{M}_k + \mathfrak{M}_{n-k}$. Inversamente, se $\mathfrak{M}_k$ e $\mathfrak{M}_{k'}$ são sub-espaços de ordens k e k', sem vector comum, e tais que todo o vector de $\mathfrak{M}$ se pode exprimir como soma dum vector do 1º e dum vector do 2º, é $k+k'=n$, $\mathfrak{M} = \mathfrak{M}_k + \mathfrak{M}_{k'}$.

Um espaço simples (ou sem sub-espaços) exprime-se numa base dum único elemento e inversamente.

Cada elemento base e_i gera um sub-espaço simples (ou cíclico) e o espaço $\mathfrak{M}$ é a soma directa de n espaços simples.

Dado o sub-espaço $\mathfrak{M}_k$ $(k<n)$, o grupo factor $\mathfrak{M}/\mathfrak{M}_k$ é, como vamos ver, um espaço vectorial de ordem $n-k$. Em primeiro lugar, o grupo $\mathfrak{M}$ é completamente redutível, e, consequentemente, pode escrever-se $\mathfrak{M} = \mathfrak{M}_k + \mathfrak{M}_{n-k}$. Em segundo lugar, o primeiro teorema da isomorfia dá

$$\mathfrak{M}/\mathfrak{M}_k \cong \mathfrak{M}_{n-k},$$

o que mostra ser o grupo factor (ou diferença) $\mathfrak{M}/\mathfrak{M}_k$ de ordem $n-k$, como se deseja. O grupo (ou multiplicidade) $\mathfrak{M}_{n-k}$ diz-se projecção de $\mathfrak{M}$ paralelamente a $\mathfrak{M}_k$.

Sob uma forma mais elementar, designemos com $\varepsilon_1,\dots,\varepsilon_n$ uma base de $\mathfrak{M}$ e com $z_1,\dots,z_k$ uma base de $\mathfrak{M}_k$. Visto que é possível, como se viu, completar a base de $\mathfrak{M}_k$ por meio de vectores ε_i por forma a constituir uma base para $\mathfrak{M}$, podemos supor que os z_j são os k últimos vectores ε_i. Tomando, então, um vector $\sum \varepsilon_i a_i \in \mathfrak{M}$, o complexo associado correspondente é

$$\sum_{i=1}^{n} \varepsilon_i a_i + \mathfrak{M}_k = \sum_{i=1}^{n-k} \varepsilon_i a_i + \sum_{j=n-k+1}^{n} \varepsilon_j \lambda_j \quad , \qquad (1)$$

onde os λ_j são números quaisquer. Podemos dar a (1) a forma

$$\sum_{i=1}^{n-k} \varepsilon_i a_i + \sum_{j=n}^{n} \varepsilon_j \mu_{k+1} \quad ,$$

onde os μ_j são números quaisquer. Vê-se agora que, tomando os elementos

$$\varepsilon_1 + \mathfrak{M}_k, \dots, \varepsilon_{n-k} + \mathfrak{M}_k \quad ,$$

do grupo factor, se obtém uma base para esse grupo. A projecção do vector $\sum_1^n \varepsilon_i a_i$ é o vector $\sum_1^{n-k} \varepsilon_i a_i$. Dois vectores cuja diferença pertença a $\mathfrak{M}_k$ têm a mesma projecção. Designando esses vectores com α e β, escreve-se

$$\alpha \equiv \beta (\mathrm{mod}\ \mathfrak{M}_k) \qquad \text{ou} \qquad \alpha \equiv \beta (\ \mathfrak{M}_k)$$

e diz-se que α e β são congruentes módulo $\mathfrak{M}_k$ (1).

2) Transformações lineares - Sejam $\mathfrak{M}_n(e_1,\dots,e_n)$ e $\mathfrak{M}_m(v_1,\dots,v_m)$ dois espaços vectoriais, de ordens n e m, respectivamente. Um homomorfismo operatório $\mathfrak{M}_n \sim \mathfrak{M}_m$ (ou uma homomorfia) fica definido conhecidos os elementos $U_j \in \mathfrak{M}_m$, correspondentes dos e_j. Poremos

$$U_j = \sum_{k=1}^{m} v_k a_{kj} \quad , \qquad (j=1,2,\dots,n). \qquad (2)$$

(1) H. Weyl, "The Theory of Groups and Quantum Mechanics", Londres, 1931.

Dado o elemento $\sum e_j a_j \in \mathcal{M}_n$, o seu correspondente em $\mathcal{M}_m$ é

$$\sum_{j=1}^{n} U_j\, a_j = \sum_{j,k} v_k a_{kj}\, a_j = \sum_{k=1}^{m} v_k\, b_k ,$$

com

$$b_k = \sum_{j=1}^{n} a_{kj}\, a_j .$$

Vê-se que o homomorfismo também pode considerar-se definido pela matriz rectangular $A = (a_{kj})$ de m linhas e n colunas. Se considerarmos um 2º homomorfismo $\mathcal{M}_m \sim \mathcal{M}_q(w_1,\ldots,w_q)$, definido pelas igualdades

$$v_k \longrightarrow W_k = \sum_{s=1}^{q} w_s b_{sk} , \qquad (k = 1,\ldots,m),$$

levanta-se a questão de procurar definir por uma matriz o homomorfismo $\mathcal{M}_n \sim \mathcal{M}_q$. Obtém-se sucessivamente

$$e_j \longrightarrow U_j \longrightarrow \sum_{k=1}^{m} W_k\, a_{kj} = \sum_{k=1}^{m} \sum_{s=1}^{q} w_s b_{sk} a_{kj} = \sum_{s} w_s \sum_{k} b_{sk}\, a_{kj} =$$

$$= \sum_{s} w_s c_{sj} , \qquad c_{sj} = \sum_{k} b_{sk}\, a_{kj} .$$

A matriz $C = B\,A = (c_{sj})$, produto das matrizes B e A, é a matriz procurada.

Em correlação com o emprego de matrizes, vamos tratar algumas questões importantes.

Suponhamos $\mathcal{M}_m$ $(m \leqslant n)$ um sub-espaço de $\mathcal{M}_n$. O homomorfismo torna-se num endomorfismo operatório Θ, de $\mathcal{M}_n$, segundo o qual se tem a correspondência

$$e_j \longrightarrow \Theta\, e_j = U_j = \sum_{k=1}^{n} e_k\, a_{kj} , \qquad (j = 1, 2,\ldots,n). \qquad (3)$$

A matriz $A = (a_{kj})$ é agora quadrada. Levanta-se a questão de saber em que condições o endomorfismo é um automorfismo. Como, mediante (3), a $\sum e_j a_j$ corresponde $\sum U_j a_j$, o automorfismo exige que sob esta segunda forma se possam exprimir todos os elementos de $\mathcal{M}_n$, e, em seguida, que essa expressão seja única. Assim, devemos procurar condições necessárias e suficientes para que os U_j constituam uma base independente. Se os U_j são, de facto, independentes, a relação $\sum U_j b_j = 0$ dá $b_j = 0$. Mas, sendo

$$\sum U_j b_j = \sum_{j,k} e_k\, a_{kj}\, b_j , \qquad (k,j = 1,\ldots,n),$$

vê-se que as igualdades $\sum a_{kj}\, b_j = 0$ dão $b_j = 0$. Este resultado diz que o produto de matrizes

$$A \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

só pode levar à matriz nula de uma coluna, se todos os b_j forem nulos. E conclui-se igualmente que o produto $A\,B = 0$, no qual B é uma matriz quadrada, leva a $B = 0$. Inversamente, esta condição garante que os U_j são independentes. Resta ver como se exprime a condição de os U_j constituirem uma base. Deverá ser, em particular,

$$e_k = \sum_{j=1}^{n} U_j b_{jk} ,$$

e, portanto,

$$e_k = \sum_{j,s} e_s a_{sj} b_{jk}$$

o que leva a

$$\sum_{j} a_{sj}\, b_{jk} = \delta_{sk} = \begin{cases} 0, & \text{se } s \neq k, \\ 1, & \text{se } s = k . \end{cases}$$

to significa que $\underline{A}$ é uma matriz com inverso direito, isto tal que $AB = U_n$ = matriz unidade. Esta condição garante, versamente, que os U_j constituem uma base. O carácter de ciprocidade em que se encontram $\underline{A}$ e $\underline{B}$ mostra que é tam- m $BA = AB = U$. Podemos enunciar o seguinte

Teorema:- É necessário e basta, para que as fórmulas (3) finam uma nova base independente, que a matriz $\underline{A}$ seja in- rtível. De facto, a condição é necessária. Ela é suficiente, virtude de a relação $AS = 0$ dar $BAS = U\,S = S = 0$.

O conjunto das matrizes quadradas com inverso forma gru- : o grupo linear; o conjunto das matrizes quadradas é um el.

A segunda questão que vamos tratar consiste em procurar matriz que define o homomorfismo (2) quando se praticam em $\mathfrak{V}_n$ e $\mathfrak{M}_m$ mudanças de base. Sejam as mudanças de base expres- s pelas seguintes relações entre matrizes:

$$(E_1 \dots E_n) = (e_1 \dots e_n).P, \qquad (P^{-1} = \text{inverso de } P \text{ existe}),$$

$$(V_1 \dots V_m) = (v_1 \dots v_m).Q, \qquad (Q^{-1} \text{ existe}).$$

nosso objectivo é exprimir os correspondentes E'_j, dos E_j, s novos elementos base, V_l, de $\mathfrak{M}_m$. Tem-se, sucessivamente,

$$(E'_1 \dots E'_n) = (U_1 \dots U_n).P = (v_1 \dots v_m).AP =$$

$$= (V_1 \dots V_m).Q^{-1}AP.$$

matriz $\underline{A}$ é substituida por $T = Q^{-1}AP$.

Seja agora, em último lugar, definir um automorfismo (3) ma nova base $(E_1 \dots E_n) = (e_1 \dots e_n).P$. A matriz $\underline{A}$ é subs- tuida pela matriz $A' = P^{-1}AP$, pois que o raciocínio anterior aplicável com $Q = P$. Directamente chega-se ao mesmo resulta- , exprimindo os transformados V_j, dos E_j, nos próprios E_j:

$(\dots V_n) = (U_1 \dots U_n).P = (e_1 \dots e_n).AP = (E_1 \dots E_n).P^{-1}AP.$

Neste § vamos introduzir ainda a noção importante de sub-espaço invariante duma transformação linear. Consideremos um endomorfismo de $\mathfrak{M}_n$:

$$\mathfrak{e} \longrightarrow \mathfrak{e}' = A\,\mathfrak{e}, \qquad x'_k = \sum_l a_{kl}\, x_l \,. \qquad (4)$$

Supõe-se aqui que o vector $\mathfrak{e} = \Sigma\, e_l x_l$ tem o correspondente $\mathfrak{e}' = \sum e_k x'_k \in \mathfrak{M}_n$. Um sub-espaço $\mathfrak{M}_k$, de $\mathfrak{M}_n$, diz-se invariante para a transformação $\underline{A}$, se um vector qualquer de $\mathfrak{M}_k$ se transforma, por meio de (4), num vector igualmente pertencente a $\mathfrak{M}_k$. A matriz $\underline{A}$, relativa ao sistema fundamental $(e_1, \dots, e_n)$, tem um aspecto particular, se supomos os k primeiros e_l vectores linearmente independentes de $\mathfrak{M}_k$. Nesse caso é, com efeito,

$$Ae_l = \sum_{\nu=1}^{k} e_\nu a_{\nu l}\,, \qquad (i = 1, \dots, k),$$

$$Ae_j = \sum_{\nu=1}^{k} e_\nu a_{\nu j} + \sum_{\mu=k+1}^{n} e_\mu a_{\mu j}, \qquad (j = k+1, \dots, n),$$

e a matriz $\underline{A}$ oferece o aspecto

$$A = \begin{pmatrix} \mathcal{A} & \mathcal{B} \\ 0 & \mathcal{A}' \end{pmatrix}, \qquad (5)$$

onde $\mathcal{A}$ e $\mathcal{A}'$ são matrizes quadradas e $\mathcal{B}$ e 0 (zero) são matrizes rectangulares. A matriz $\mathcal{A}$, por si só, define um endomorfismo no espaço $\mathfrak{M}_k$. A matriz $\mathcal{A}'$ pode ter uma interpretação análoga. Tomemos o grupo factor $\mathfrak{M}_n/\mathfrak{M}_k \cong \mathfrak{M}_{n-k}$. Cada elemento do grupo factor pode considerar-se determinado pelo elemento correspondente de $\mathfrak{M}_{n-k}$. A este elemento de $\mathfrak{M}_{n-k}$ a transformação faz corresponder um vector de $\mathfrak{M}_n$, que é soma de dois vectores, um de $\mathfrak{M}_k$, outro de $\mathfrak{M}_{n-k}$. A transformação faz, assim, corresponder a um elemento do grupo factor outro elemento do grupo factor. A matriz $\mathcal{A}'$ é, precisamente, a matriz dessa correspondência. Desenvolvamos o cálculo. Tem-se,

Isto significa que $\underline{A}$ é uma matriz com inverso direito, isto é, tal que $AB = U_n$ = matriz unidade. Esta condição garante, inversamente, que os U_j constituem uma base. O carácter de reciprocidade em que se encontram $\underline{A}$ e $\underline{B}$ mostra que é também $BA = AB = U$. Podemos enunciar o seguinte

Teorema:- É necessário e basta, para que as fórmulas (3) definam uma nova base independente, que a matriz $\underline{A}$ seja invertível. De facto, a condição é necessária. Ela é suficiente, em virtude de a relação $AS = 0$ dar $BAS = U\,S = S = 0$.

O conjunto das matrizes quadradas com inverso forma grupo: o grupo linear; o conjunto das matrizes quadradas é um anel.

A segunda questão que vamos tratar consiste em procurar a matriz que define o homomorfismo (2) quando se praticam em $\mathfrak{M}_n$ e $\mathfrak{M}_m$ mudanças de base. Sejam as mudanças de base expressas pelas seguintes relações entre matrizes:

$$(E_1 \dots E_n) = (e_1 \dots e_n).P, \qquad (P^{-1} = \text{inverso de P existe}),$$

$$(V_1 \dots V_m) = (v_1 \dots v_m).Q, \qquad (Q^{-1} \text{ existe}).$$

O nosso objectivo é exprimir os correspondentes E'_j, dos E_j, nos novos elementos base, V_l, de $\mathfrak{M}_m$. Tem-se, sucessivamente,

$$(E'_1 \dots E'_n) = (U_1 \dots U_n).P = (v_1 \dots v_m).AP =$$

$$= (V_1 \dots V_m).Q^{-1}AP.$$

A matriz $\underline{A}$ é substituida por $T = Q^{-1}AP$.

Seja agora, em último lugar, definir um automorfismo (3) numa nova base $(E_1 \dots E_n) = (e_1 \dots e_n).P$. A matriz $\underline{A}$ é substituida pela matriz $A' = P^{-1}AP$, pois que o raciocínio anterior é aplicável com $Q = P$. Directamente chega-se ao mesmo resultado, exprimindo os transformados V_j, dos E_j, nos próprios E_j:

$$(V_1 \dots V_n) = (U_1 \dots U_n).P = (e_1 \dots e_n).AP = (E_1 \dots E_n).P^{-1}AP.$$

Neste § vamos introduzir ainda a noção importante de sub-espaço invariante duma transformação linear. Consideremos um endomorfismo de $\mathfrak{M}_n$:

$$\mathfrak{e} \longrightarrow \mathfrak{e}' = A\,\mathfrak{e}, \qquad x'_k = \sum_l a_{kl}\,x_l \,. \qquad (4)$$

Supõe-se aqui que o vector $\mathfrak{e} = \Sigma\, e_l x_l$ tem o correspondente $\mathfrak{e}' = \sum e_k x'_k \in \mathfrak{M}_n$. Um sub-espaço $\mathfrak{M}_k$, de $\mathfrak{M}_n$, diz-se invariante para a transformação $\underline{A}$, se um vector qualquer de $\mathfrak{M}_k$ se transforma, por meio de (4), num vector igualmente pertencente a $\mathfrak{M}_k$. A matriz $\underline{A}$, relativa ao sistema fundamental $(e_1, \dots, e_n)$, tem um aspecto particular, se supomos os k primeiros e_l vectores linearmente independentes de $\mathfrak{M}_k$. Nesse caso é, com efeito,

$$Ae_l = \sum_{\nu=1}^{k} e_\nu a_{\nu l}\,, \qquad (i = 1, \dots, k),$$

$$Ae_j = \sum_{\nu=1}^{k} e_\nu a_{\nu j} + \sum_{\mu=k+1}^{n} e_\mu a_{\mu j}, \qquad (j = k+1, \dots, n),$$

e a matriz $\underline{A}$ oferece o aspecto

$$A = \begin{pmatrix} \mathcal{A} & \mathcal{L} \\ 0 & \mathcal{A}' \end{pmatrix}, \qquad (5)$$

onde $\mathcal{A}$ e $\mathcal{A}'$ são matrizes quadradas e $\mathcal{L}$ e 0 (zero) são matrizes rectangulares. A matriz $\mathcal{A}$, por si só, define um endomorfismo no espaço $\mathfrak{M}_k$. A matriz $\mathcal{A}'$ pode ter uma interpretação análoga. Tomemos o grupo factor $\mathfrak{M}_n / \mathfrak{M}_k \equiv \mathfrak{M}_{n-k}$. Cada elemento do grupo factor pode considerar-se determinado pelo elemento correspondente de $\mathfrak{M}_{n-k}$. A este elemento de $\mathfrak{M}_{n-k}$ a transformação faz corresponder um vector de $\mathfrak{M}_n$, que é soma de dois vectores, um de $\mathfrak{M}_k$, outro de $\mathfrak{M}_{n-k}$. A transformação faz, assim, corresponder a um elemento do grupo factor outro elemento do grupo factor. A matriz $\mathcal{A}'$ é, precisamente, a matriz dessa correspondência. Desenvolvamos o cálculo. Tem-se,

dado $\varepsilon = \sum_{j=k+1}^{n} e_j x_j$,

$$\varepsilon' = A\varepsilon = \sum_{j=k+1}^{n} Ae_j . x_j = \sum_{j=k+1} \left(\sum_{\nu=1}^{k} e_\nu a_{\nu j} + \sum_{\mu=k+1}^{n} e_\mu a_{\mu j} \right) x_j =$$

$$= e_1 \sum_{j=k+1}^{n} a_{1j} x_j + \cdots + e_k \sum_{j=k+1}^{n} a_{kj} x_j + e_{k+1} \sum_{j=k+1}^{n} a_{k+1,j} x_j +$$

$$+ \cdots + e_n \sum_{j=k+1}^{n} a_{nj} x_j \ .$$

Ao elemento do grupo factor determinado por ε corresponde o elemento do grupo factor determinado por

$$e_{k+1} \sum_{j=k+1}^{n} a_{k+1,j} x_j + \cdots + e_n \sum_{j=k+1}^{n} a_{nj} x_j \ .$$

Em particular, aos elementos base do grupo factor, representados por

$$e_{k+1} , \cdots , e_n ,$$

correspondem os elementos do grupo factor representados por

$$\sum_{r=1}^{n-k} e_{k+r} a_{k+r,\,k+1} , \cdots , \sum_{r=1}^{n-k} e_{k+r} a_{k+r,\,n} \ .$$

A matriz da correspondência é, pois, a matriz $\mathcal{A}'$.

É claro que, se os primeiros k vectores do sistema fundamental escolhido forem quaisquer, a matriz A não tem a forma (5). Uma mudança de sistema fundamental dará a A a forma $P^{-1}AP$, podendo, pois, enunciar-se o seguinte

Teorema:- É necessário e basta, para que a matriz A seja equivalente a uma matriz da forma (5), que o endomorfismo definido por A possua sub-espaço invariante.

Sempre que à matriz quadrada A se pode dar a forma (5), diz-se que A é uma matriz redutível. No caso contrário, diz-se irredutível. Se for possível escolher uma base na qual A tome o aspecto

$$\begin{pmatrix} \mathcal{A} & 0 \\ 0 & \mathcal{A}' \end{pmatrix} , \qquad (5')$$

diz-se que A é decomponível. Nesse caso o espaço $\mathcal{M}_{n-k}$ é também um sub-espaço invariante da transformação linear definida por A. O raciocínio generaliza-se e pode supor-se que A tome o aspecto

$$A = \begin{pmatrix} \mathcal{A}_1 & 0 & \cdots & 0 \\ 0 & \mathcal{A}_2 & \cdots & 0 \\ \hline 0 & 0 & & \mathcal{A}_r \end{pmatrix} ,$$

onde $\mathcal{A}_1 , \cdots , \mathcal{A}_r$ são matrizes quadradas irredutíveis. Haverá, então, r sub-espaços invariantes sem elemento comum, em cada um dos quais se define uma transformação linear pela matriz $\mathcal{A}_t$ correspondente. A matriz A diz-se completamente redutível.

3) Espaço unitário - Diz-se forma de Hermúte uma expressão $G(\varepsilon)$, função do vector ε, definida como segue:

$$G(\varepsilon) = \sum_{t,k} g_{tk} \overline{x}_t x_k , \qquad (g_{tk} = \overline{g}_{kt}) ,$$

onde $\overline{x}_t$ significa complexo conjugado de x_t. Uma forma de Hermite toma sempre valores reais.

Diz-se que se introduz uma métrica no espaço linear $\mathfrak{M}_n$, quando se dá uma forma hermiteana definida positiva, $(\mathfrak{x},\mathfrak{x}) = G(\mathfrak{x})$, que apenas toma valores positivos, salvo se todos os x_i forem nulos, pois que então é $G(0) = 0$. O valor $G(\mathfrak{x})$ diz-se norma do vector $\mathfrak{x}$. A coerência da definição exige que uma forma hermiteana se conserve hermiteana, quando se faz uma mudança de base. Ora, tomando uma nova base $E_1, \dots, E_n$, definida pela igualdade

$$(E_1 \dots E_n) = (e_1 \dots e_n).P, \qquad (P \text{ invertível}),$$

o vector $\mathfrak{x} = \sum e_i x_i$ aparece sob a forma $\mathfrak{x} = \sum E_i x'_i$, com

$$x_k = \sum_i p_{ki} x'_i .$$

Vem, sucessivamente,

$$G(\mathfrak{x}) = \sum_{i,k,l,m} g_{ik} \overline{p}_{il} \overline{x}'_l p_{km} x'_m = \sum_{l,m} G_{lm} \overline{x}'_l x'_m ,$$

com

$$G_{lm} = \sum_{i,k} \pi_{li} g_{ik} p_{km} , \qquad (\pi_{li}) = \Pi = (\overline{p}_{il}) = P^* ,$$

onde P^* indica a matriz conjugada transposta de P. A matriz $G = (g_{ik})$ é substituida por P^*GP. Vê-se, então, que é

$$\overline{G}_{ml} = \sum_{i,k} \overline{\pi}_{mi} \overline{g}_{ik} \overline{p}_{kl} = \sum_{i,k} p_{im} g_{ki} \pi_{ik} = \sum_{i,k} \pi_{li} g_{ik} p_{km} = G_{lm} .$$

Dizem-se transformações métricas ou unitárias as transformações isomorfas do espaço $\mathfrak{M}_n$ que fazem corresponder ao vector $\mathfrak{x}$ o vector $\mathfrak{x}'$ tal que $G(\mathfrak{x}) = G(\mathfrak{x}')$. As transformações métricas formam um sub-grupo do grupo linear, como se verifica imediatamente.

A igualdade

$$G(\mathfrak{x}+\mathfrak{z}) = \sum_{i,k} g_{ik} (\overline{x}_i + \overline{z}_i)(x_k + z_k) = G(\mathfrak{x}) + Q(\mathfrak{x},\mathfrak{z}) + Q(\mathfrak{z},\mathfrak{x}) + G(\mathfrak{z}),$$

na qual se pôs $Q(\mathfrak{x},\mathfrak{z}) = \sum_{i,k} g_{ik} \overline{x}_i z_k$, pode ainda escrever-se

$$(\mathfrak{x}+\mathfrak{z}, \mathfrak{x}+\mathfrak{z}) = (\mathfrak{x},\mathfrak{x}) + (\mathfrak{x},\mathfrak{z}) + (\mathfrak{z},\mathfrak{x}) + (\mathfrak{z},\mathfrak{z}),$$

introduzindo a notação $Q(\mathfrak{x},\mathfrak{z}) = (\mathfrak{x},\mathfrak{z})$. A expressão

$$P(\mathfrak{x},\mathfrak{z}) = \frac{1}{2}\left[Q(\mathfrak{x},\mathfrak{z}) + Q(\mathfrak{z},\mathfrak{x})\right]$$

diz-se forma polar de $G(\mathfrak{x})$. É uma forma bilinear simétrica de $\mathfrak{x}$ e $\mathfrak{z}$. Da forma polar passa-se à forma de Hermite pela relação $G(\mathfrak{x}) = Q(\mathfrak{x},\mathfrak{x}) = P(\mathfrak{x},\mathfrak{x})$.

A expressão $Q(\mathfrak{x},\mathfrak{z}) = (\mathfrak{x},\mathfrak{z})$ diz-se produto escalar dos dois vectores $\mathfrak{x}$ e $\mathfrak{z}$.

Consideremos as transformações isomorfas do espaço que conservam os produtos escalares: $Q(\mathfrak{x},\mathfrak{z}) = Q(\mathfrak{x}',\mathfrak{z}')$. Essas transformações constituem um sub-grupo do grupo linear, que é precisamente o grupo das transformações métricas. Na verdade, de $(\mathfrak{x},\mathfrak{z}) = (\mathfrak{x}',\mathfrak{z}')$, tira-se $(\mathfrak{x},\mathfrak{x}) = (\mathfrak{x}',\mathfrak{x}')$. Inversamente, uma transformação para a qual $(\mathfrak{x},\mathfrak{x}) = (\mathfrak{x}',\mathfrak{x}')$ dá

$$(\mathfrak{x}+\mathfrak{z}i, \mathfrak{x}+\mathfrak{z}i) = (\mathfrak{x},\mathfrak{x}) + (\mathfrak{x},\mathfrak{z})i - (\mathfrak{z},\mathfrak{x})i + (\mathfrak{z},\mathfrak{z}) =$$

$$= (\mathfrak{x}'+\mathfrak{z}'i, \mathfrak{x}'+\mathfrak{z}'i) = (\mathfrak{x}',\mathfrak{x}') + (\mathfrak{x}',\mathfrak{z}')i - (\mathfrak{z}',\mathfrak{x}')i + (\mathfrak{z}',\mathfrak{z}')$$

e, anàlogamente,

$$(\mathfrak{x}+\mathfrak{z}, \mathfrak{x}+\mathfrak{z}) = (\mathfrak{x},\mathfrak{x}) + (\mathfrak{x},\mathfrak{z}) + (\mathfrak{z},\mathfrak{x}) + (\mathfrak{z},\mathfrak{z}) =$$

$$\Rightarrow (\mathfrak{x}'+\mathfrak{z}', \mathfrak{x}'+\mathfrak{z}') = (\mathfrak{x}', \mathfrak{x}') + (\mathfrak{x}', \mathfrak{z}')+(\mathfrak{z}', \mathfrak{x}')+(\mathfrak{z}', \mathfrak{z}').$$

Logo, sendo

$$(\mathfrak{x}, \mathfrak{z}) - (\mathfrak{z}, \mathfrak{x}) = (\mathfrak{x}', \mathfrak{z}') - (\mathfrak{z}', \mathfrak{x}') ,$$

$$(\mathfrak{x}, \mathfrak{z}) + (\mathfrak{z}, \mathfrak{x}) = (\mathfrak{x}', \mathfrak{z}') + (\mathfrak{z}', \mathfrak{x}') ,$$

deduz-se $(\mathfrak{x}, \mathfrak{z}) = (\mathfrak{x}', \mathfrak{z}')$, q. e. d.

Dois vectores para os quais o produto escalar é nulo dizem-se ortogonais. Um vector de norma igual à unidade diz-se normalizado. Um espaço linear de métrica hermiteana diz-se unitário. Empregaremos às vezes o símbolo $\mathcal{R}_n$ para o representar.

Dada uma base $(e_1, \ldots, e_n)$, de $\mathcal{R}_n$, é sempre possível escolher os e_l de modo que sejam ortogonais e normalizados (sistema base ortonormalizado). Ponhamos primeiramente

$$E_1 = \frac{e_1}{\sqrt{G(e_1)}} ,$$

o que dará $(E_1, E_1) = 1$. Em seguida ponhamos

$$E_2' = E_1\alpha + e_2\beta .$$

O 2º membro não pode ser nulo, a não ser que seja $\alpha = \beta = 0$, visto que, doutra forma haveria uma relação linear entre e_1 e e_2. Determinando α e β pela condição

$$(E_1, E_2') = (E_1, E_1)\alpha + (E_1, e_2)\beta = 0 ,$$

vê-se que pode sempre supor-se $\beta = 1$, $\alpha = -(E_1, e_2)$. Vem, então,

$$E_2' = e_2 - E_1(E_1, e_2) ,$$

e, em seguida, por normalização,

$$E_2 = \frac{E_2'}{\sqrt{G(E_2')}} .$$

Anàlogamente, por-se-á

$$E_3' = E_1\alpha + E_2\beta + e_3\gamma ,$$

com as condições

$$(E_1, E_3') = \alpha + (E_1, e_3)\gamma = 0,$$

$$(E_2, E_3') = \beta + (E_2, e_3)\gamma = 0,$$

às quais podemos satisfazer pondo

$$\gamma = 1, \qquad \alpha = -(E_1, e_3) , \qquad \beta = -(E_2, e_3),$$

o que leva a

$$E_3' = e_3 - E_1\cdot(E_1, e_3) - E_2\cdot(E_2, e_3), \qquad E_3 = \frac{E_3'}{\sqrt{G(E_3')}} .$$

Prossegue-se deste modo até

$$E_n' = e_n - \sum_{l=1}^{n-1} E_l\cdot(E_l, e_n), \qquad E_n = \frac{E_n'}{\sqrt{G(E_n')}} .$$

O sistema $(E_1, \ldots, E_n)$ é o sistema orto-normalizado que se desejava. A matriz que faz passar à nova base é do tipo

$$\begin{pmatrix} a & b & d & \cdots \\ o & c & e & \cdots \\ o & o & f & \cdots \\ \vdots & \vdots & \vdots & \cdots \\ o & o & o & \cdots \end{pmatrix} ,$$

na qual são diferentes de zero todos os elementos diagonais. Tal resultado mostra que o determinante da matriz é diferente de zero.

Com uma base orto-normalizada, a forma hermiteana que define a métrica é do tipo

$$G(\mathcal{C}) = \overline{x}_1 x_1 + \cdots + \overline{x}_n x_n .$$

Construamos em $\mathcal{R}_n$ um sub-espaço de ordem k, $\mathcal{R}_k$. Os vectores base de $\mathcal{R}_k$ podem supor-se orto-normalizados. Se $E_1, \ldots, E_k$ forem esses vectores, podemos completar a base de $\mathcal{R}_n$ procedendo do modo seguinte: tomamos um primeiro vector normalizado E_{k+1}, ortogonal aos anteriores, vector que sabemos existir; depois um vector análogo, E_{k+2}, ortogonal aos $k+1$ anteriores; e assim sucessivamente, até E_n.

Os vectores $E_{k+1}, \ldots, E_n$ definem um sub-espaço $\mathcal{R}_{n-k}$ cujos vectores são todos ortogonais aos vectores de $\mathcal{R}_k$. Assim, diz-se que $\mathcal{R}_{n-k}$ é o <u>espaço totalmente ortogonal a</u> $\mathcal{R}_k$. Qualquer sub-espaço de k dimensões tem, pois, um espaço totalmente ortogonal de $n-k$ dimensões. Podemos observar, de resto, que vectores ortogonais são sempre linearmente independentes.

Diz-se <u>desigualdade de Schwarz</u> a importante relação

$$|(\mathcal{C}, \mathcal{Z})|^2 \leqq (\mathcal{C}, \mathcal{C}) \cdot (\mathcal{Z}, \mathcal{Z}),$$

que vamos demonstrar. Consideremos a desigualdade

$$\sum_l (x_l \beta + z_l)(\overline{x}_l \beta + \overline{z}_l) \geqq 0 ,$$

onde β é real. Tira-se

$$\beta^2 \sum_l \overline{x}_l x_l + \beta \left(\sum_l \overline{x}_l z_l + \sum_l \overline{z}_l x_l \right) + \sum_l \overline{z}_l z_l \geqq 0 ,$$

e, por consequência,

$$\left(\sum_l \overline{x}_l z_l + \sum_l \overline{z}_l x_l \right)^2 - 4 \sum_l \overline{x}_l x_l \cdot \sum_l \overline{z}_l z_l \leqq 0 .$$

Se pusermos $(\mathcal{C}, \mathcal{Z}) = a + ib$, vem

$$(2a)^2 - 4 (\mathcal{C}, \mathcal{C}) \cdot (\mathcal{Z}, \mathcal{Z}) \leqq 0, \quad \text{ou} \quad a^2 \leqq (\mathcal{C}, \mathcal{C}) \cdot (\mathcal{Z}, \mathcal{Z}).$$

Posto isto, substituamos $\mathcal{C}$ por $\mathcal{C} e^{i\varphi}$. Então, passa-se de

$$\mathcal{C} \longrightarrow \mathcal{C} e^{i\varphi}, \quad (\mathcal{Z}, \mathcal{C}) \longrightarrow (\mathcal{Z}, \mathcal{C}) e^{i\varphi},$$

$$(\mathcal{C}, \mathcal{Z}) \longrightarrow (\mathcal{C}, \mathcal{Z}) e^{i\varphi}, \quad (\mathcal{C}, \mathcal{C}) \longrightarrow (\mathcal{C}, \mathcal{C}),$$

$$(\mathcal{Z}, \mathcal{Z}) \longrightarrow (\mathcal{Z}, \mathcal{Z}), \quad 2a \longrightarrow 2a \cos\varphi + 2b \operatorname{sen}\varphi ,$$

pelo que se terá

$$(a \cos\varphi + b \operatorname{sen}\varphi)^2 \leqq (\mathcal{C}, \mathcal{C}) \cdot (\mathcal{Z}, \mathcal{Z}).$$

Como esta desigualdade subsiste qualquer que seja φ, tem-se, em particular, para o valor de φ dado por $\operatorname{tg}\varphi = \frac{b}{a}$,

$$a^2 + b^2 \leqq (\mathcal{C}, \mathcal{C}) \cdot (\mathcal{Z}, \mathcal{Z}),$$

que é precisamente a desigualdade de <u>Schwarz</u>.(1)

Diz-se <u>desigualdade de Bessel</u> a relação

$$\sum_{l=1}^{m} \overline{x}_l x_l \leqq (\mathcal{C}, \mathcal{C}), \quad \text{quando } m = n,$$

que é imediata.

(1) A demonstração foi extraída de <u>L. de Broglie, "Quantification dans la nouvelle Mécanique"</u>, Paris, 1932.

4) Transformações unitárias - Se A é uma matriz duma transformação métrica ou uma matriz unitária, o transformado $\mathcal{C}'$, de $\mathcal{C}$, definido pelas suas componentes $x'_l = \sum_k a_{lk} x_k$, tem a mesma norma. Então deverá ser

$$\sum_{l,k} g_{lk} \overline{x}_l x_k = \sum_{l,k} g_{lk} \overline{x}'_l x'_k .$$

Ora tem-se

$$\sum_{l,k} g_{lk} \overline{x}'_l x'_k = \sum_{l,k,l,m} g_{lk} \overline{a}_{ll} \overline{x}_l a_{km} x_m = \sum_{l,m} \left(\sum_{l,k} \alpha_{ll} g_{lk} a_{km} \right) \overline{x}_l x_m ,$$

onde $\alpha_{ll} = \overline{a}_{ll}$ é o elemento geral de A^*. Conclui-se o

Teorema:- É necessário e suficiente, para que A seja unitária, que tenha lugar a relação $A^* G A = G$. (6)

No caso de se ter uma base ortogonal, a relação anterior é substituida pela seguinte: $A^* A = U_n$, ou $A^* = A^{-1}$.

O determinante $|G|$ é diferente de zero, pois, como se sabe, por passagem a uma base orto-normalizada, obtém-se $P^* G P = U_n$. Nestas condições é $|A| \neq 0$, sempre que A é unitária. Uma tal matriz tem inverso, o que aqui se pode demonstrar do modo seguinte: se A é unitária, há um sistema no qual a sua transformada A' verifica a equação $A'^* A' = U_n$. E como se tem $A' = P^{-1} A P$, será $P A' P^{-1} = A$. O 1º membro tem inverso, pelo que o terá o segundo.(1) É por isso que na definição de transformação métrica se pode excluir a exigência de isomorfismo, pois este tem necessàriamente lugar.

Ao lado das matrizes unitárias, introduziremos ainda as matrizes hermiteanas ou auto-adjuntas, que são matrizes A satisfazendo à relação $(A\mathcal{C}, \mathcal{Z}) = (\mathcal{C}, A\mathcal{Z})$. A condição para que A seja hermiteana é dada pela igualdade

(1) Verifica-se também recorrendo à matriz auto-adjunta. Veja-se Almeida Costa, "Grupos abelianos e Anéis ...", pgs. 43.

$$\sum_{l,k,l} g_{lk} \overline{a}_{ll} \overline{x}_l z_k = \sum_{l,k,l} g_{lk} \overline{x}_l a_{kl} z_l ,$$

da qual se tira

$$\sum_l g_{lk} \overline{a}_{ll} = \sum_l g_{ll} a_{lk} , \quad \text{ou seja} \quad A^* G = G A .$$

Numa base ortogonal, tem-se simplesmente $A^* = A$, $(\overline{a}_{lk} = a_{kl})$.

Tanto as transformações unitárias como as auto-adjuntas gozam duma propriedade importante, que se exprime no seguinte

Teorema:- Existe um sistema de n vectores próprios ortogonais da transformação. Isto significa que é possível determinar n vectores ortogonais $\mathcal{C}_1, \ldots, \mathcal{C}_n$, para os quais

$$A \mathcal{C}_l = \mathcal{C}'_l = \mathcal{C}_l \lambda_l , \qquad (i = 1, \ldots, n).$$

Comecemos por observar que os dois tipos de transformação, se deixam invariante um sub-espaço $\mathcal{R}_k$, deixam igualmente invariante o sub-espaço totalmente ortogonal $\mathcal{R}_{n-k}$. E isto porque, se for $e_1, \ldots, e_k$ uma base de $\mathcal{R}_k$, e $\mathcal{Z}$ um vector de $\mathcal{R}_{n-k}$, temos, no caso de matrizes auto-adjuntas, $(Ae_l, \mathcal{Z}) = (e_l, A\mathcal{Z}) = 0$, enquanto que, tratando-se de matrizes unitárias, resulta o facto da sua própria definição e da invertibilidade da matriz A.

Posto isto, escrevamos desenvolvidamente as condições que determinam $\mathcal{C}_i(\xi_1, \ldots, \xi_n)$:

$$\begin{aligned} a_{11} \xi_1 + \cdots + a_{1n} \xi_n &= \xi_1 \lambda_1 , \\ \text{- - - - - - - - - - - - - -} & \\ a_{n1} \xi_1 + \cdots + a_{nn} \xi_n &= \xi_n \lambda_1 . \end{aligned}$$

A existência de solução não nula para estas equações é expressa pela igualdade

$$\begin{vmatrix} a_{11} - \lambda & \cdots & a_{1n} \\ \text{- - - - - - -} & & \\ a_{n1} & \cdots & a_{nn} - \lambda \end{vmatrix} = 0 ,$$

chamada equação secular. Determinando λ_1 por meio desta equação, façamos-lhe corresponder $\mathcal{C}_1 \neq 0$. O espaço $\mathcal{R}_{n-1}$, totalmente ortogonal a $\mathcal{C}_1$, é conservado pela transformação. Sendo assim, a nossa matriz define em $\mathcal{R}_{n-1}$ uma transformação da mesma espécie, para a qual, pelo processo supra, podemos encontrar um vector próprio $\mathcal{C}_2$, ortogonal a $\mathcal{C}_1$. E o raciocínio prossegue até $\mathcal{C}_n$, e só até $\mathcal{C}_n$. Depois de se encontrar $\mathcal{C}_1$, pode tomar-se uma base $(\mathcal{C}_1, v_2, \ldots, v_n)$ onde $v_l \in \mathcal{R}_{n-1}$. A matriz $\underline{A}$ torna-se numa matriz $\underline{A}'$ sendo

$$A' \mathcal{C}_1 = \mathcal{C}_1 \lambda_1, \qquad A' v_l = \sum_{k=2}^{n} v_k \, a'_{kl} . \tag{7}$$

O significado dos $\lambda\lambda$ é independente da base. Na nova base, se $\underline{P}$ for a matriz da transformação, a nova equação secular tem as mesmas raizes que a anterior. Efectivamente, vê-se que é

$$\left|A' - \lambda U_n\right| = \left|P^{-1}AP - \lambda P^{-1}U_n P\right| = \left|P^{-1}\right|\left|A - \lambda U_n\right|\left|P\right| = \left|A - \lambda U_n\right| = 0.$$

As igualdades (7) que afectam os v_l são as que determinam a transformação no espaço $\mathcal{R}_{n-1}$. Determinando $\mathcal{C}_2 \in \mathcal{R}_{n-1}$ tal que $A' \mathcal{C}_2 = \mathcal{C}_2 \lambda_2$, obtém-se, sob forma desenvolvida,

$$A' \mathcal{C}_2 = A' \sum_{2}^{n} v_k \xi_k = \sum_{l=2}^{n} v_l \left(\sum_{k=2}^{n} a'_{lk} \xi_k \right),$$

$$a'_{22}\xi_2 + a'_{23}\xi_3 + \cdots + a'_{2n}\xi_n = \xi_2 \lambda_2,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$a'_{n2}\xi_2 + a'_{n3}\xi_3 + \cdots + a'_{nn}\xi_n = \xi_n \lambda_2 .$$

A equação que dá λ_2 é

$$\begin{vmatrix} a'_{22} - \lambda & \cdots & a'_{2n} \\ \cdots\cdots & & \\ a'_{n2} & \cdots & a'_{nn} - \lambda \end{vmatrix} = 0 ,$$

de modo que a equação a que satisfazem λ_1 e λ_2 é

$$\begin{vmatrix} \lambda_1 - \lambda & 0 & \cdots & 0 \\ 0 & a'_{22} - \lambda & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & a'_{n2} & \cdots & a'_{nn} - \lambda \end{vmatrix} = \begin{vmatrix} a_{11} - \lambda & \cdots & a_{1n} \\ \cdots\cdots & & \\ a_{n1} & \cdots & a_{nn} - \lambda \end{vmatrix} = 0 .$$

Ele é precisamente a equação secular tirada das equações (7). Significa isto que os λ_l constituem todas as raizes da equação secular, cada uma delas com o seu grau de multiplicidade.

Quando se tomam os $\mathcal{C}_l$ (que são linearmente independentes) como base de $\mathcal{R}_n$, tem-se

$$A \mathcal{C}_1 = \mathcal{C}_1 \lambda_1, \ldots, A \mathcal{C}_n = \mathcal{C}_n \lambda_n ,$$

e $\underline{A}$ tem a forma diagonal

$$A = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

Os números λ_l dizem-se valores próprios ou números característicos de $\underline{A}$ e os $\mathcal{C}_l$ são os vectores próprios correspondentes.

No caso de $\underline{A}$ ser hermiteana, os λ_l são números reais:

$$(A \mathcal{C}_1, \mathcal{C}_1) = (\mathcal{C}_1, A \mathcal{C}_1) = (\mathcal{C}_1, \mathcal{C}_1)\,\overline{\lambda}_1 = (\mathcal{C}_1, \mathcal{C}_1)\,\lambda_1 .$$

Mostrou-se atrás, incidentalmente, que a equação secular é invariante em face das mudanças de base. Os coeficientes respectivos são igualmente invariantes. Em particular, é invarian-

te o coeficiente de $(-\lambda)^{n-1}$, que constitui o traço, T(A), da matriz A :

$$T(A) = T(P^{-1} A P) \quad .$$

O termo conhecido da equação secular, que é o determinante $|A|$, é outro invariante a fixar.

Num espaço unitário de métrica $G(\mathcal{x})$, consideremos uma matriz hermiteana $A = (a_{lk})$. Tem-se

$$(A\,\mathcal{x}\,,\,\mathcal{x}\,) = (\,\mathcal{x}\,,\,A\,\mathcal{x}) = H(\mathcal{x}).$$

H é uma forma de Hermite, como vamos ver. Tem-se

$$H = \sum_{l,k,l} g_{lk}\overline{x}_l a_{kl} x_l = \sum_{l,l}\left(\sum_k g_{lk}\, a_{kl}\right)\overline{x}_l\, x_l = \sum_{l,l} h_{ll}\overline{x}_l\, x_l \ ,$$

$$h_{ll} = \sum_k g_{lk}\, a_{kl} = \sum_k \overline{a}_{kl}\, g_{kl} \ ,$$

$$\overline{h}_{ll} = \sum_k \overline{g}_{lk}\, \overline{a}_{kl} = \sum_k g_{kl}\, \overline{a}_{kl} = h_{ll} \ .$$

À forma $H(\mathcal{x})$ faremos corresponder a matriz $H = GA$. Inversamente, dada uma forma de Hermite $H(\mathcal{x})$, designemos com H a matriz correspondente e ponhamos $H = GA$. Esta igualdade dá $G^{-1}H = A$ e permite determinar uma matriz A tal que

$$G\,A = H, \quad (G\,A)^* = H^* = H = A^* G^* = A^* G,$$

o que mostra ser A uma matriz hermiteana.

Tomemos como nova base de $\mathcal{R}_n$ a base dos vectores próprios de A. As matrizes A e G ficam reduzidas à forma diagonal, assim como $H = G\,A$. Podemos enunciar o seguinte

Teorema:- Uma forma hermiteana definida positiva G e uma forma hermiteana qualquer H são redutíveis simultâneamente à forma

$$G = \sum_l \overline{x}_l x_l \ , \qquad H = \sum_l \lambda_l \overline{x}_l x_l \ .$$

E podemos acrescentar que os λ_l são raizes da equação

$$|A - \lambda U| = |G^{-1}H - \lambda U| = 0,$$

ou seja da equação

$$|G| \cdot |G^{-1}H - \lambda U| = |H - \lambda G| = 0 \ .$$

A correspondência que estudámos, entre a matriz hermiteana A e a forma de Hermite $H(\mathcal{x})$, é invariante em face das mudanças de base do espaço $\mathcal{R}_n$. Comecemos por verificar directamente que a matriz A se conserva hermiteana. Se a mudança de base é definida pela matriz invertível P, têm-se as correspondências

$$A \longrightarrow P^{-1} A P \ , \qquad G \longrightarrow P^* G P \ ,$$

e, por consequência,

$$A^* G \longrightarrow (P^{-1} A P)^* \cdot P^* G P = P^* A^* (P^{-1})^* P^* G P.$$

Ora, da relação $P P^{-1} = U_n$, tira-se

$$(P P^{-1})^* = (P^{-1})^* P^* = U_n, \qquad P^{*-1} = P^{-1*},$$

de sorte que é

$$A^* G \longrightarrow P^* A^* G P = P^* G A P \ ,$$

$$G A \longrightarrow P^* G P P^{-1} A P = P^* G A P \ .$$

Nestas condições, tem-se

$$H \longrightarrow P^{*}HP = P^{*}GAP = P^{*}GP.P^{-1}AP,$$

como se deseja.

Concluiremos este § tratando o importante problema da diagonalização dum sistema de matrizes unitárias ou auto-adjuntas. É válido o seguinte

Teorema:- É condição necessária e suficiente, para que duas matrizes unitárias (ou auto-adjuntas) sejam simultâneamente redutíveis à forma diagonal, que sejam comutáveis.

Se A e B são simultâneamente redutíveis à forma diagonal, elas comutam sob esta forma. Ora a comutabilidade é independente da mudança de base. Para se ver que a condição é suficiente, façamos a redução de A à forma diagonal e suponhamos que o vectores próprios correspondentes são

$$\mathcal{e}_1, \ldots, \mathcal{e}_h \; ; \; \mathcal{z}_1, \ldots, \mathcal{z}_k ; \ldots ;$$

com os valores próprios λ_1, para os primeiros h vectores; λ_2, para os k seguintes, etc. Em virtude de se ter

$$AB\mathcal{e}_l = BA\mathcal{e}_l = B\mathcal{e}_l\lambda_1 = B\mathcal{e}_l \cdot \lambda_1,$$

vê-se que os vectores $B\mathcal{e}_l$, $B\mathcal{z}_j, \ldots$ são vectores próprios de A, correspondentes aos valores próprios $\lambda_1, \lambda_2, \ldots$. Posto isto, consideremos os sub-espaços $\mathcal{R}_h$, $\mathcal{R}_k$, etc., definidos, respectivamente, pelos $\mathcal{e}_l$, $\mathcal{z}_j$, etc. Eles conservam-se invariantes em face da transformação definida pela matriz B; o que significa que, depois de A estar sob a forma diagonal, B se apresenta como matriz em escada

$$B = \begin{pmatrix} B_1 & 0 & \ldots & 0 \\ 0 & B_2 & \ldots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \ldots & B_s \end{pmatrix},$$

onde $B_1, \ldots, B_s$ são matrizes quadradas de graus h, k, etc. Efectuando em $\mathcal{R}_h$ a transformação que dá a B_1 a forma diagonal, em $\mathcal{R}_k$ a transformação que diagonaliza B_2, etc., a matriz B fica reduzida à forma diagonal. Basta observar que, se for, por ex.,

$$P_1^{-1}B_1P_1 = B_1', \ldots, P_s^{-1}B_sP_s = B_s',$$

com $B_1', \ldots, B_s'$ sob forma diagonal, pondo

$$P = \begin{pmatrix} P_1 & \ldots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \ldots & P_s \end{pmatrix}, \qquad P^{-1} = \begin{pmatrix} P_1^{-1} & \ldots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \ldots & P_s^{-1} \end{pmatrix},$$

vem

$$B' = P^{-1}BP = \begin{pmatrix} P_1^{-1}B_1P_1 & \ldots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \ldots & P_s^{-1}B_sP_s \end{pmatrix} = \begin{pmatrix} B_1' & \ldots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \ldots & B_s' \end{pmatrix},$$

sob a forma diagonal. Ora A continua diagonal.

Trataremos, então, com sistemas de matrizes unitárias (ou auto-adjuntas) comutáveis. Vale o

Teorema:- É possível tornar simultâneamente diagonais todas as matrizes dum sistema de matrizes comutáveis unitárias (ou auto-adjuntas). Comecemos por fazer a nota de que uma matriz múltipla da matriz unidade conserva o mesmo aspecto em todas as bases de referência. Nessas condições, tomemos no sistema dado das matrizes uma matriz A que não seja múltipla da matriz unidade (se tal matriz não existir o teorema está demonstrado) e reduzamo-la à forma diagonal. As matrizes B do sistema originam sistemas de matrizes unitárias (ou auto-adjuntas), como B_1, B_2, ..., em espaços de menor número de dimensões do que $\mathcal{R}_n$. Se o teorema for válido em espaços com menos do que n dimensões, é válido em $\mathcal{R}_h$, $\mathcal{R}_k$, ... e o teorema está demonstrado. Ora o teorema é válido nos espaços com uma dimensão.

Para se não ser induzido em erro, convém fazer uma observação. Imaginemos um sistema de matrizes quaisquer comutáveis, entre as quais uma matriz $\underline{A}$ redutível à forma diagonal e não múltipla da matriz unidade. Poderão reduzir-se simultâneamente à forma diagonal as matrizes de tal sistema ? O processo anterior de demonstração não é aplicável, porque a matriz determinada por $\underline{A}$ em cada um dos sub-espaços $\mathcal{R}_n$, $\mathcal{R}_R$, etc. é precisamente múltipla da matriz unidade, não permitindo a indução.

5) Representação dum grupo por transformações lineares - Consideremos um espaço $\mathfrak{M}_n$ e um grupo $\mathcal{G}$. Se a cada $g_1 \in \mathcal{G}$ se puder fazer corresponder uma matriz $\underline{A}_1$, de tal forma que ao produto $g_1 g_2$ corresponda o produto $\underline{A}_1 \underline{A}_2$, o homomorfismo $\mathcal{G} \sim \mathcal{L}$, onde $\mathcal{L}$ é o conjunto das matrizes $\underline{A}$, define uma representação $\mathcal{D}$, de $\mathcal{G}$, por meio de transformações lineares. O grau das matrizes é o grau da representação. Esta diz-se fiel, se o homomorfismo é um isomorfismo. Quando uma representação de $\mathcal{G}$ não é fiel, um teorema conhecido garante-nos que existe um grupo factor de $\mathcal{G}$ do qual a referida representação é representação fiel.

Se $(e_1, \ldots, e_n)$ for uma base de $\mathfrak{M}_n$, dada uma representação $\mathcal{D}$, escreveremos $g \cdot \sum e_i x_i = \underline{A} \sum e_i x_i$, onde $\underline{A}$ corresponde a g. As representações que estarão em causa são aquelas para as quais ao elemento um de $\mathcal{G}$ corresponde a matriz unidade. Isto significa que uma matriz $\underline{A}$ não pode ser singular.

Duas representações de $\mathcal{G}$ dizem-se equivalentes, se existir uma matriz fixa invertível $\underline{P}$, tal que as matrizes $\underline{A}$ e $\underline{A}'$, correspondentes de $g \in \mathcal{G}$ nas duas representações, estejam ligadas pela relação $\underline{A}' = \underline{P}^{-1} \underline{A} \underline{P}$.

Se, no espaço $\mathfrak{M}_n$ de representação, existe um sub-espaço invariante para todas as transformações de $\mathcal{D}$, as matrizes reduzem-se todas à forma (5) do § 2. $\mathcal{D}$ diz-se redutível e o espaço $\mathfrak{M}_n$ (que admite os elementos de $\mathcal{G}$ como operadores) diz-se igualmente redutível relativamente ao grupo.

As definições de representações irredutíveis ou de representações completamente redutíveis (cfr. 5', do § 2) resultam também do que de análogo se disse para uma matriz. No caso de decomponibilidade, tem-se

$$\mathfrak{M}_n = \mathfrak{M}_R + \mathfrak{M}_{n-R},$$

e escreve-se, para $\mathcal{D}$,

$$\mathcal{D} = \mathcal{D}_1 + \mathcal{D}_2 ,$$

onde $\mathcal{D}_1$ é a representação de $\mathcal{G}$ pertencente a $\mathfrak{M}_R$ e $\mathcal{D}_2$ a que pertence a $\mathfrak{M}_{n-R}$. Duma maneira geral, à decomposição de $\mathfrak{M}_n$ em sub-espaços invariantes indecomponíveis,

$$\mathfrak{M}_n = \mathfrak{M}' + \mathfrak{M}'' + \ldots + \mathfrak{M}^{(k)},$$

faz-se corresponder a decomposição completamente redutível

$$\mathcal{D} = \mathcal{D}' + \mathcal{D}'' + \ldots + \mathcal{D}^{(k)},$$

onde $\mathcal{D}^{(i)}$ é a representação irredutível do grupo pertencente a $\mathfrak{M}^{(i)}$, ou induzida pelo grupo no referido espaço.

No caso duma representação redutível, existe, por hipótese, uma base $(e_1, \ldots, e_n)$ de $\mathfrak{M}_n$, tal que

$$g e_i = A e_i = \sum_{\nu=1}^{R} e_\nu \, a_{\nu i} , \qquad (i = 1, \ldots, k) ,$$

$$g e_j = \sum_{\nu=1}^{R} e_\nu \, a_{\nu j} + \sum_{\mu=R+1} e_\mu \, a_{\mu j} , \qquad (j = k+1, \ldots, n) ,$$

qualquer que seja $g \in \mathcal{G}$. Os raciocínios feitos no § 2, a propósito de sub-espaços invariantes, mostram que, pondo

$$A = \begin{pmatrix} \mathcal{U}' & \mathcal{L} \\ 0 & \mathcal{U}'' \end{pmatrix} ,$$

as matrizes $\mathcal{U}'$ constituem uma representação $\mathcal{D}'$ pertencente a $\mathfrak{M}_R$ e as matrizes $\mathcal{U}''$ uma representação pertencente a $\mathfrak{M}_n / \mathfrak{M}_R \cong \mathfrak{M}_{n-R}$.

6) Representações unitárias - Diz-se representação unitária dum grupo $\mathcal{G}$ toda a representação por meio de matrizes unitárias. A definição exige, pois, que se introduza uma métrica em $\mathcal{M}_n$, de modo a definir $\mathcal{R}_n$. Pode enunciar-se o seguinte

Teorema:- Toda a representação unitária dum grupo é irredutível ou completamente redutível. De facto, se em $\mathcal{R}_n$ não há um sub-espaço invariante, a representação é irredutível. Se um sub-espaço $\mathcal{M}_R$ é invariante, o espaço totalmente ortogonal $\mathcal{M}_{n-R}$ é também invariante e a representação é decomponível. A decomposição pode continuar-se, se algum dos sub-espaços $\mathcal{M}_R$ ou $\mathcal{M}_{n-R}$ não é irredutível, e o raciocínio prossegue-se até obtermos espaços todos irredutíveis.

No caso de grupos finitos, a proposição anterior pode precisar-se e demonstrar-se o

Teorema:- Toda a representação dum grupo finito é irredutível ou completamente redutível. Dado o grupo $\mathcal{G}$ de N elementos, seja uma representação $\mathcal{G}$ pertencente a um espaço $\mathcal{M}_n$. Vamos ver que é possível introduzir uma métrica, para a qual todas as matrizes da representação são unitárias. Consideremos a forma hermiteana definida positiva $H = \sum_{l=1}^{n} \overline{x}_l x_l$ e efectuemos a transformação $\mathcal{C} \longrightarrow \mathcal{C}' = A_1 \mathcal{C}$, onde A_1 é a matriz correspondente de $g_1 \in \mathcal{G}$. Cada A_1 é uma matriz com inverso, de sorte que, da relação

$$\begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} = A_1 \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad \text{tira-se} \quad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = A^{-1} \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix}.$$

Por meio desta última igualdade, passa-se de H, de matriz unidade, a

$$H_1 = \sum_{kl} \left(\sum_l \overline{a}_{lk}^{-1} a_{ll}^{-1} \right) \overline{x}'_k x'_l = \sum_{kl} \left(\sum_l \overline{b}_{lk} b_{ll} \right) \overline{x}'_k x'_l ,$$

$$\left[A_1^{-1} = B = (a_{lk}^{-1}) = (b_{lk}) \right].$$

Ora $\sum_l \overline{a}_{lk}^{-1} a_{ll}^{-1} = \sum_l \overline{b}_{lk} b_{ll} = \sum_l \rho_{kl} \, b_{ll}$, com $\rho_{kl} = \overline{b}_{lk}$. A matriz definida em H_1 é, assim, $B^*B = A_1^{-1*} A_1^{-1} = A_1^{*-1} A_1^{-1}$. Feito isto, operemos com outra matriz A_2 da representação, tal como se fez com A_1. Finalmente, consideremos a forma

$$G = \sum_{j=1}^{N} H_j, \quad \text{que define a matriz} \quad \sum_{j=1}^{N} A_j^{-1*} A_j^{-1} = G.$$

Se tomarmos em $\mathcal{M}_n$ a métrica definida por G, cada transformação A_R (ou A_R^{-1}) é unitária, como vamos ver. Tem-se

$$A_R^{-1*} G A_R^{-1} = \sum_{j=1}^{N} (A_j^{-1} A_R^{-1})^* (A_j^{-1} A_R^{-1}) =$$

$$= \sum_{j=1}^{N} (A_R A_j)^{-1*} (A_R A_j)^{-1} = \sum_{l=1}^{N} A_l^{-1*} A_l^{-1} = G ,$$

pelo que o teorema se encontra demonstrado. Seria preferível utilizar os elementos do grupo $\mathcal{G}$, em vez das matrizes, para indicar as transformações. Assim se justifica que os somatórios vão de 1 a N.

Para o que toca à redução efectiva duma representação, têm lugar os raciocínios que vão seguir-se. Dada uma representação $\mathcal{G}$ dum grupo $\mathcal{G}$, seja $\mathcal{M}_n(e_1, \ldots, e_n)$ o espaço de representação. Quando fizermos uma mudança de base, poremos

$$(E_1 \ldots E_n) = (e_1 \ldots e_n) . P ,$$

mas, quando $A \in \mathcal{G}$ se interpretar como definindo uma transformação linear de $\mathcal{M}_n$, poremos

$$(e'_1 \ldots e'_n) = (e_1 \ldots e_n) \, A .$$

Neste caso, ao vector $\mathcal{C}(x_l)$ corresponde o vector $\mathcal{C}'(x'_l)$, com

$$\begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} .$$

Dada uma forma linear

$$\mathcal{L} = \sum_l a_l x_l = (a_1 \dots a_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} ,$$

efectuemos sobre os x_l a transformação anterior. Virá

$$\mathcal{L} = \sum_l a_l x_l = \sum_l a'_l x'_l .$$

A variância dos a_l é definida pelas relações

$$(a'_1 \dots a'_n) \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} = (a_1 \dots a_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (a'_1 \dots a'_n) A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} ,$$

o que dá

$$(a_1 \dots a_n) = (a'_1 \dots a'_n).A .$$

Diz-se que $\mathcal{L}$ é uma <u>forma invariante em face de</u> A quando $a'_l = a_l$. É claro que esta definição é independente da base de $\mathfrak{M}_n$. Quando se muda de base, pondo

$$\mathcal{L} = \sum_l a_l x_l = \sum_l \alpha_l \xi_l , \qquad \text{com} \qquad x_l = \sum_k p_{lk} \xi_k ,$$

vem

$$(\alpha_1 \dots \alpha_n) = (a_1 \dots a_n).P .$$

Por consequência, a hipótese de invariância relativa à antiga base,

$$(a_1 \dots a_n) = (a_1 \dots a_n) A ,$$

dá, na nova base,

$$(\alpha_1 \dots \alpha_n) = (a_1 \dots a_n).P = (a_1 \dots a_n) A P = (\alpha_1 \dots \alpha_n) P^{-1} A P .$$

Ao fazer-se a redução completa duma representação $\mathfrak{H}$, pode a representação idêntica, que faz corresponder a matriz unidade (do 1º grau) a cada elemento do grupo, comparecer em diagonal um certo número de vezes. A esse respeito enuncia-se o seguinte

<u>Teorema:- É condição necessária e suficiente, para que a representação idêntica dum grupo $\mathcal{G}$ (finito) seja uma parte irredutível duma representação $\mathfrak{H}$, que haja uma forma linear invariante para as transformações da representação.</u>

<u>A condição é necessária</u>. Existindo a representação idêntica, existe uma base para o espaço de representação, tal que uma transformação $A \in \mathfrak{H}$ determina a correspondência

$$E'_1 = A E_1 = E_1 , \qquad E'_2 = A E_2 = \sum_2^n E_k a_{k2} , \dots .$$

A forma linear $\mathcal{L}_1 = \lambda \xi_1$, do vector $\varepsilon(\xi_1, \dots, \xi_n)$ é invariante:

$$(\lambda\ 0 \dots 0) = (a'_1 \dots a'_n) \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & a_{22} & \dots & a_{2n} \\ - & - & - & - \\ 0 & a_{n2} & \dots & a_{nn} \end{pmatrix} ,$$

tendo em conta que o determinante $|A|$ é diferente de zero, dá imediatamente $a'_1 = \lambda$, $a'_2 = \dots = a'_n = 0$. Directamente, resulta o facto de ser $\xi'_1 = \xi_1$.

<u>A condição é suficiente</u>. Se $\mathcal{L}_1 = a_1 x_1 + \dots + a_n x_n$, com $a_1 \neq 0$, é uma forma invariante, juntemos-lhe mais $n-1$ formas lineares distintas $\mathcal{L}_l$, nas variáveis $x_2, \dots, x_n$, e efectuemos em $\mathfrak{M}_n$ a mudança de base definida pela matriz P, inversa da matriz Q que figura nessas formas. Facilmente se

verificam as relações

$$\begin{pmatrix} \mathfrak{L}_1 \\ \mathfrak{L}_2 \\ \vdots \\ \mathfrak{L}_n \end{pmatrix} = Q \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = Q\,P \begin{pmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{pmatrix} = U \begin{pmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{pmatrix} = \begin{pmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{pmatrix} ,$$

nas quais se subentendeu

$$a_1 = q_{11}, \ldots, a_n = q_{1n} .$$

Por meio das transformações de $\mathfrak{G}$, que agora são do tipo $A' = P^{-1}A\,P = Q\,A\,Q^{-1}$, as formas $\xi_1, \ldots, \xi_n$ tornam-se em formas em $\xi'_1, \xi'_2, \ldots, \xi'_n$, com

$$\begin{pmatrix} \xi'_1 \\ \vdots \\ \xi'_n \end{pmatrix} = A' \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} .$$

Em particular é $\xi'_1 = \xi_1$, o que dá

$$a'_{11} = 1, \quad a'_{12} = a'_{13} = \ldots = a'_{1n} = 0 .$$

De resto, tem-se, por hipótese,

$$(q_{11} \ldots q_{1n}) = (q_{11} \ldots q_{1n})A .$$

Pelo que toca aos elementos $a'_{21}, \ldots, a'_{n1}$ da matriz $\underline{A}'$, tem-se

$$a'_{21} = \ldots = a'_{n1} = 0 ,$$

pois

$$a'_{j1} = \sum_R (Q\,A)_{jR}\, p_{R1} = 0 , \qquad (j = 2, \ldots, n) ,$$

visto ser $p_{21} = \ldots = p_{n1} = 0$. Estes resultados mostram que é

$$A'E_1 = E'_1 = \sum_R E_R\, a'_{R1} = E_1 ,$$

$$A'E_2 = E'_2 = \sum_R E_R\, a'_{R2} = \sum_{R=2}^{n} E_R\, a'_{R2} , \quad \text{etc.} ,$$

pelo que o teorema se encontra demonstrado.

Corolário:- É condição necessária e suficiente, para que a representação idêntica figure exactamente r vezes na representação $\mathfrak{G}$, que haja exactamente r formas lineares invariantes distintas para as transformações da representação.

Posto isto, vamos indicar um processo para a construção de todas as formas lineares invariantes. Seja $\mathfrak{L}_0 = \sum a_l\, x_l$ uma forma inicial qualquer:

$$\mathfrak{L}_0 = (a_1 \ldots a_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} .$$

Uma transformação $A_1 \in \mathfrak{G}$ dá

$$\mathfrak{L}_0 = (a_1 \ldots a_n)\, A_1^{-1} \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} .$$

Tomaremos a forma nos x x:

$$\mathfrak{L}_1 = (a'_1 \ldots a'_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (a_1 \ldots a_n)\, A_1^{-1} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} .$$

Em seguida, formaremos, anàlogamente,

$$\mathfrak{L}_2 = (a''_1 \ldots a''_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (a_1 \ldots a_n)\, A_2^{-1} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} ,$$

e, finalmente,

$$\mathcal{L} = (a_1 \dots a_n) \cdot \left(\sum_{l=1}^{N} A_l^{-1} \right) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} .$$

Para se ver que $\mathcal{L}$ é invariante em face das transformações de $\mathcal{G}$, tomemos uma dessas transformações, $\underline{A}$. Vem

$$\mathcal{L} = (a_1 \dots a_n) \cdot (\sum A_l^{-1}) \cdot A^{-1} \cdot \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} =$$

$$= (a_1 \dots a_n) \cdot \sum_l (A\, A_l)^{-1} \cdot \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} = (a_1 \dots a_n) \cdot \sum_j A_j^{-1} \cdot \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix},$$

o que demonstra a afirmação.

No que vai seguir-se, poremos (sempre sob a hipótese de os somatórios irem de 1 a $\underline{N}$)

$$\sum_l A_l^{-1} = \sum_l A_l = M .$$

Apliquemos o processo de construção duma forma invariante às formas lineares

$$\mathcal{L}'_0 = x_1 , \quad \mathcal{L}''_0 = x_2 , \dots , \quad \mathcal{L}^{(n)}_0 = x_n .$$

Obtem-se

$$\mathcal{L}' = (1 \dots 0) \cdot M \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = m_{11} x_1 + \dots + m_{1n} x_n ,$$

$$\mathcal{L}^{(n)} = (0 \dots 1) \cdot M \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = m_{n1} x_1 + \dots + m_{nn} x_n .$$

Nestas condições, a forma invariante deduzida de

$$\mathcal{L}_0 = a_1 x_1 + \dots + a_n x_n \qquad \text{é} \qquad \mathcal{L} = a_1 \mathcal{L}' + \dots + a_n \mathcal{L}^{(n)} . \tag{8}$$

De resto, tem-se

$$(a_1 \dots a_n) \cdot M = a_1 (1 \dots 0) \cdot M + \dots + a_n (0 \dots 1) \cdot M .$$

No geral, $\mathcal{L}'$, $\mathcal{L}''$, ... não são independentes.

Teorema:- Se a representação $\mathcal{G}$ não contém a representação idêntica, $\underline{M}$ é a matriz nula. Não havendo, com efeito, forma invariante, deverá ser $\mathcal{L}' = \mathcal{L}'' = \dots = 0$.

Sob a expressão de $\mathcal{L}$, em (8), encontram-se todas as formas invariantes. Se, na verdade, $\mathcal{L}_0 = b_1 x_1 + \dots + b_n x_n$ for invariante, a aplicação do processo leva a $N \mathcal{L}_0$ (É claro que poderia a representação em causa considerar-se como representação fiel dum certo grupo factor e os somatórios poderiam reduzir-se ao número $\underline{g}$ de matrizes distintas = número de elementos daquele grupo factor). Basta ver que se tem

$$(b_1 \dots b_n) \cdot M = (b_1 \dots b_n)\, A_1 + \dots + (b_1 \dots b_n)\, A_N =$$

$$= (b_1 \dots b_n) + \dots + (b_1 \dots b_n) = N(b_1 \dots b_n) .$$

Por outro lado, deve aplicar-se o resultado (8), de sorte que vem

$$N \mathcal{L}_0 = N b_1 x_1 + \dots + N b_n x_n = b_1 \mathcal{L}' + \dots + b_n \mathcal{L}^{(n)} ,$$

donde se tira, como se deseja,

$$\mathcal{L}_0 = \frac{b_1}{N} \mathcal{L}' + \dots + \frac{b_n}{N} \mathcal{L}^{(n)} .$$

Deste modo, o número de formas lineares invariantes distintas é o número de formas distintas entre os $\mathcal{L}'$, ..., $\mathcal{L}^{(n)}$. E este nú-

mero, por outro lado, é dado pelo número de linhas independentes da matriz M. Chamando característica duma matriz a ordem do determinante de mais alta ordem não nulo tirado da mesma, pode enunciar-se o seguinte

Teorema:- A característica da matriz M dá o número de vezes que a representação idêntica figura na representação $\mathcal{G}$.

Diz-se traço duma representação o conjunto dos traços das suas matrizes. É claro que esta definição é independente da base a que está referido o espaço de representação. Se $\mathcal{G}$ é irredutível, o traço diz-se caracter. Tem lugar o

Teorema:- A soma dos caracteres das matrizes duma representação irredutível é igual a zero. Se a representação $\mathcal{G}$ é redutível (completamente redutível), a soma dos traços é rN, em que r representa o número de vezes que a representação idêntica figura em $\mathcal{G}$ e N é o número de elementos de $\mathcal{G}$. A demonstração é imediata.(1)

Dada uma representação $\mathcal{G}$, consideremos o conjunto das matrizes inversas das suas transpostas:

$$U,\ \tilde{A}_1^{-1},\ \ldots,\ \tilde{A}_{N-1}^{-1}\ .$$

Obtém-se aqui uma nova representação do grupo dado $\mathcal{G}$, mediante a correspondência $g \longrightarrow \tilde{A}_i^{-1}$. De facto, será

$$g \longrightarrow \tilde{A}_1^{-1}, \qquad g' \longrightarrow \tilde{A}_2^{-1},$$

$$gg' \longrightarrow (\tilde{A_1 A_2})^{-1} = (\tilde{A}_2 \tilde{A}_1)^{-1} = \tilde{A}_1^{-1} \tilde{A}_2^{-1}.$$

Esta representação diz-se adjunta de $\mathcal{G}$ e designa-se com $\mathcal{G}_a$.

(1) Seguimos A. Speiser, "Die Theorie der Gruppen von endlicher Ordnung", Berlin, 1927, pgs. 160 e seguintes.

Teorema:- Os traços das matrizes de $\mathcal{G}_a$ são imaginários conjugados dos traços das matrizes correspondentes de $\mathcal{G}$. Tomemos uma matriz $A_i \in \mathcal{G}$. Como é unitária (para uma certa métrica), pode reduzir-se à forma diagonal, o que não altera o seu traço. Supondo assim,

$$A_i = \begin{pmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \ldots & \lambda_n \end{pmatrix},$$

o facto de ser $A_i^N = U$ mostra que os λ_l são raizes da unidade. E, como é,

$$\tilde{A}_i^{-1} = \begin{pmatrix} \frac{1}{\lambda_1} & 0 & \ldots & 0 \\ 0 & \frac{1}{\lambda_2} & \ldots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \ldots & \frac{1}{\lambda_n} \end{pmatrix},$$

o facto de se ter $\frac{1}{\lambda_l} = \overline{\lambda}_l$ demonstra o teorema.

7) Exemplos de representações unitárias(1) - Se $\mathcal{G}$ é um grupo abeliano, aos elementos a e b, de $\mathcal{G}$, correspondem matrizes A e B que comutam. E, como um sistema de matrizes unitárias comutáveis é redutível, em globo, à forma diagonal, pode enunciar-se o

Teorema:- As representações unitárias irredutíveis dum grupo abeliano são todas do 1º grau.

Grupo cíclico de ordem n - Tomemos, como 1º ex., as representações irredutíveis do grupo cíclico de ordem n:

(1) A redacção dum certo número de §§ que vão seguir-se é extraida do livro de B. L. van der Waerden, "Die Gruppentheoretische Methode in der Quantenmechanik", Berlin, 1932.

$$\mathcal{G} = \left\{ \varepsilon, a, \ldots, a^{n-1} \right\}.$$

O elemento a é representado pela matriz de uma linha e de uma coluna $A = (a_{11})$. A matriz representante de a^k é $A^k = (a_{11}^k)$, pelo que deverá ter-se $a_{11}^n = 1$. Isto significa que os valores possíveis para a_{11} são os seguintes: $a_{11} = \cos \frac{2k\pi}{n} + i \operatorname{sen} \frac{2k\pi}{n}$, $(k = 0, 1, \ldots, n-1)$. Aqui ficam conhecidas n representações irredutíveis de $\mathcal{G}$, que são as únicas possíveis.

Grupo das rotações à volta dum eixo - Em 2º lugar, estudemos as representações unitárias irredutíveis do grupo abeliano constituido pelas rotações à volta dum eixo. Sejam R_θ, $R_{\theta'}$ dois elementos do grupo $\mathcal{G}$, correspondentes, respectivamente, às rotações de ângulos θ e θ'. Tem-se $R_\theta . R_{\theta'} = R_{\theta'} . R_\theta = R_{\theta+\theta'}$. Nas representações do 1º grau em estudo, faz-se corresponder a R_θ um número $\varphi(\theta)$ tal que

$$\varphi(\theta) \, . \, \varphi(\theta') = \varphi(\theta + \theta').$$

Para se encontrarem as soluções desta equação funcional, pode proceder-se do modo seguinte. Tem-se, sucessivamente,

$$\varphi(\theta) . \varphi(d\theta) = \varphi(\theta + d\theta) = \varphi(\theta) + \frac{\partial \varphi}{\partial \theta} d\theta,$$

$$\varphi(\theta) \left[\varphi(d\theta) - 1 \right] = \frac{\partial \varphi}{\partial \theta} d\theta, \qquad \varphi(d\theta) = \varphi(0) + \left(\frac{\partial \varphi}{\partial \theta} \right)_0 d\theta .$$

Se $\varphi(\theta)$ é uma função finita com derivada finita, $\varphi(d\theta) - 1$ é infinitamente pequeno. Assim, será $\varphi(0) = 1$, e, portanto,

$$\varphi(\theta) \left(\frac{\partial \varphi}{\partial \theta} \right)_0 d\theta = \frac{\partial \varphi}{\partial \theta} d\theta , \qquad \frac{d\varphi}{\varphi} = \left(\frac{\partial \varphi}{\partial \theta} \right)_0 d\theta ,$$

$$\log \frac{\varphi}{C} = \left(\frac{\partial \varphi}{\partial \theta} \right)_0 \theta , \qquad \varphi = e^{\alpha\theta}, \qquad \alpha = \left(\frac{d\varphi}{d\theta} \right)_0 .$$

Se supomos agora que a representação em causa é unívoca, deverá ter-se $\varphi(2\pi) = \varphi(0) = 1$, e, consequentemente,

$$e^{2\pi\alpha} = 1 , \qquad \alpha = ik , \qquad (k = 0, \pm 1, \pm 2, \ldots).$$

As representações procuradas são, pois,

$$R_\theta \longrightarrow A = (e^{ik\theta}) , \qquad (k = 0, \pm 1, \pm 2, \ldots) .$$

Há aqui uma infinidade de representações irredutíveis, o que joga com o facto de não ser finito o grupo considerado. Verifica-se imediatamente *a posteriori* que todas as representações encontradas são unitárias.

Grupo das rotações e das reflexões - Como último exemplo deste §, vamos tratar as representações unitárias irredutíveis do grupo das rotações à volta dum eixo e das reflexões em planos passando por esse eixo. As operações do grupo podem gerar-se por uma reflexão S num plano determinado passando pelo eixo e pelas rotações R_θ à volta do eixo. Verifica-se imediatamente que têm lugar as seguintes leis de composição

$$R_\psi . R_\varphi = R_\varphi . R_\psi = R_{\varphi+\psi} ; \qquad S R_\varphi = R_{-\varphi} S .$$

O grupo não é abeliano, pelo que pode haver representações irredutíveis que não sejam do 1º grau. Para se encontrarem as partes irredutíveis duma representação, comecemos por fazer a redução do sub-grupo das rotações. Os vectores base e_j ficarão a satisfazer às relações $R_\theta e_j = A e_j = e_j e^{ik\theta}$. Distinguiremos entre os e_j para os quais $j = k$ é positivo ou negativo, empregando, respectivamente, as notações e_k, e_{-k}. Para um vector do tipo e_k (ou de caracter positivo k), tem-se

$$R_{-\varphi}(S\, e_k) = S(R_\varphi e_k) = S\, e_k . e^{ik\varphi},$$

ou, mudando φ em $-\varphi$,

$$R_\varphi(S\, e_k) = S\, e_k \cdot e^{-ik\varphi}.$$

Isto significa que Se_k é um vector do tipo e_{-k}, o conjunto dos dois vectores e_k, $Se_k = e_{-k}$ constitui um sub-espaço invariante para a representação, pois

$$R_\varphi e_k = e_k e^{ik\varphi}, \qquad R_\varphi e_{-k} = e_{-k}\, e^{-ik\varphi},$$

$$Se_k = e_{-k}, \qquad Se_{-k} = e_k = (S^2 e_k).$$

As matrizes correspondentes da representação do 2º grau são

$$R_\varphi \longrightarrow \begin{pmatrix} e^{ik\varphi} & 0 \\ 0 & e^{-ik\varphi} \end{pmatrix}, \quad S \longrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Designar-se-á com $\mathcal{U}_k$ uma tal representação. Ela é irredutível, porque, se pudesse ter-se

$$R_\varphi(e_k a + e_{-k} b) = (e_k a + e_{-k} b)c = e_k a\, e^{ik\varphi} + e_{-k} b\, e^{-ik\varphi},$$

concluia-se, tendo em vista que $\underline{a}$ e $\underline{b}$ seriam diferentes de zero,

$$c = e^{ik\varphi} = e^{-ik\varphi}, \qquad k = 0.$$

Isto quer dizer que uma representação irredutível do 1º grau só pode ter lugar num espaço de 1ª ordem cuja base seja um vector de caracter zero. Duma maneira precisa, suponhamos que há um único vector deste tipo. Devendo, então, ser

$$\begin{cases} R_\varphi e_0 = e_0, \\ R_\varphi(Se_0) = Se_0 = e_0 \alpha, \end{cases} \qquad \begin{cases} S^2 e_0 = Se_0 \cdot \alpha = e_0 \alpha^2 = e_0, \\ \alpha = \pm 1, \end{cases}$$

verifica-se que há uma representação irredutível de uma das formas

$$\begin{cases} R_\varphi e_0 = e_0, \\ S\, e_0 = e_0, \end{cases} \qquad \begin{cases} R_\varphi e_0 = e_0, \\ S\, e_0 = -e_0. \end{cases}$$

Estas duas representações distinguem-se pelo "caracter" da reflexão S. Se esse caracter é 1, tem-se a representação idêntica $\mathcal{U}_0^+$; se esse caracter é -1, tem-se a representação $\mathcal{U}_0^-$, na qual S é representada pela matriz (-1). Se há mais do que um vector do tipo $\underline{e_0}$, ao lado da circunstância anterior, pode ter-se

$$R_\varphi e_0 = e_0, \qquad R_\varphi(Se_0) = Se_0 \neq e_0 \alpha.$$

Vem, então, imediatamente

$$\begin{cases} R_\varphi(e_0 + Se_0) = e_0 + Se_0, \\ S\,(e_0 + Se_0) = e_0 + Se_0, \end{cases} \qquad \begin{cases} R_\varphi(e_0 - Se_0) = e_0 - Se_0, \\ S\,(e_0 - Se_0) = -(e_0 - Se_0), \end{cases}$$

pelo que se obtêm ainda as duas representações do 1º grau já referidas.

Todas as representações encontradas são unitárias, como se verifica fàcilmente. Há aqui, pois, uma infinidade de representações unitárias irredutíveis $\mathcal{U}_0^+, \mathcal{U}_0^-, \mathcal{U}_1, \mathcal{U}_2, \ldots$ e não há outras.

8) A representação produto de Kronecker - Sejam $\mathcal{M}(u_1, \ldots, u_m)$ e $\mathcal{N}(v_1, \ldots, v_n)$ dois espaços e $\underline{A}$ e $\underline{B}$ dois endomorfismos de $\mathcal{M}$ e $\mathcal{N}$, respectivamente. Pôr-se-á

$$u'_l = Au_l = \sum_j u_j a_{jl}, \qquad v'_k = Bv_k = \sum_l v_l b_{lk}.$$

Os $\underline{mn}$ produtos $u_l v_k$ podem tomar-se como base dum novo espaço $\underline{mn}$ - dimensional $\mathcal{R}$. Se se sujeitam à transformação

$$(A \times B)u_l v_k = u'_l v'_k = \sum_j u_j a_{jl} \cdot \sum_l v_l b_{lk} = \sum_{j,l} u_j v_l a_{jl} b_{lk}, \qquad (8')$$

tem-se um endomorfismo de $\mathcal{R}$. A matriz correspondente representa-se por $A \times B = P$ e diz-se transformação linear produto a transformação de $\mathcal{R}$ assim obtida. Na definição não se distinguirá entre um produto $u_l v_k$ e o produto $v_k u_l$. Será ainda

$$(B \times A) v_k u_l = \sum_l v_l b_{lk} \cdot \sum_j u_j a_{jl} = \sum_{l,j} v_l u_j b_{lk} a_{jl} .$$

Dispondo convenientemente da ordem dos vectores base, resulta

$$A \times B = B \times A .$$

Teorema:- O traço de P é o produto dos traços de A e de B. De facto, tem-se

$$T(P) = \sum_{j,l} a_{jj} b_{ll} = \sum_j a_{jj} \cdot \sum_l b_{ll} = T(A) \cdot T(B) .$$

Se um conjunto de matrizes A, B, ... constitui uma representação $\mathcal{D}$ dum grupo $\mathcal{G}$, e um conjunto de matrizes A', B', ... constitui uma segunda representação $\mathcal{D}'$ do mesmo grupo, o conjunto das matrizes $P = A \times A'$, $Q = B \times B'$, ... define ainda uma representação $\Delta = \mathcal{D} \times \mathcal{D}'$ do grupo. A demonstração repousa sobre a igualdade

$$AB \times A'B' = (A \times A') \cdot (B \times B') ,$$

que vamos verificar. Tem-se

$$(AB \times A'B') u_l v_k = \sum_{j,l} u_j v_l \left(\sum_m a_{jm} b_{ml}\right) \left(\sum_n a'_{ln} b'_{nk}\right) = \sum_{j,l,m,n} u_j v_l a_{jm} b_{ml} a'_{ln} b'_{nk} ,$$

$$(A \times A') \cdot (B \times B') u_l v_k = (A \times A') \sum_{m,n} u_m v_n b_{ml} b'_{nk} = \sum_{m,n,j,l} u_j v_l a_{jm} a'_{ln} b_{ml} b'_{nk} ,$$

donde se conclui o que se deseja. A representação produto de Kronecker é a representação Δ. São válidas as igualdades seguintes

$$\mathcal{D}_1 \times \mathcal{D}_2 = \mathcal{D}_2 \times \mathcal{D}_1 , \qquad (\mathcal{D}_1 \times \mathcal{D}_2) \times \mathcal{D}_3 = \mathcal{D}_1 \times (\mathcal{D}_2 \times \mathcal{D}_3) .$$

A primeira foi já assinalada. A segunda verifica-se directamente aplicando $(A \times A') \times A''$ e $A \times (A' \times A'')$ ao vector $u_l v_k w_m$, composto à custa dos vectores fundamentais dos tres espaços em que se construiram $\mathcal{D}_1$, $\mathcal{D}_2$ e $\mathcal{D}_3$.

Uma questão importante que se levanta é a seguinte: dadas duas representações irredutíveis $\mathcal{D}_1$ e $\mathcal{D}_2$, dum grupo $\mathcal{G}$, procurar em que condições figura a representação idêntica no produto $\mathcal{D}_1 \times \mathcal{D}_2$. É necessário e basta, como se sabe, que no espaço $\mathcal{R}$ haja um sub-espaço invariante de 1ª ordem.(1) Se $V = \sum u_l v_k p_{kl} = \sum u_l \sum v_k p_{kl} = \sum u_l V_l$, com $V_l = \sum_k v_k p_{kl}$, é um vector invariante, tem-se, para cada elemento $g \in \mathcal{G}$,

$$g V = \sum_l (g u_l)(g V_l) = \sum_l u_l V_l ,$$

ou seja

$$\sum_{l,j} u_j a_{jl} \cdot g V_l = \sum_j u_j \sum_l a_{jl} g V_l = \sum_j u_j V_j ,$$

donde se conclui

$$\sum_{l=1}^{m} a_{jl} \cdot g V_l = V_j , \qquad (j = 1, 2, \ldots, m) .$$

Introduzindo aqui a matriz $\tilde{A} = (\tilde{a}_{jl} = a_{lj})$, podemos escrever

$$\sum_{l=1}^{m} g V_l \cdot \tilde{a}_{lj} = V_j ,$$

ou, sob forma de matrizes,

$$(g V_1 \ldots g V_m) \cdot \tilde{A} = (V_1 \ldots V_m) ,$$

que pode ainda escrever-se

$$(g V_1 \ldots g V_m) = (V_1 \ldots V_m) \cdot \tilde{A}^{-1} . \qquad (9)$$

Conclui-se daqui que o espaço $\mathcal{V} = (V_1, \ldots, V_m)$ é invariante em face das transformações de $\mathcal{D}_2$. Como se dá o facto de ser

(1) melhor: haja vector invariante.

$\mathcal{V} \neq (0)$, tem-se $\mathcal{V} = \mathcal{V}(v_1, \ldots, v_n)$, de sorte que é $n \leqslant m$. Invertendo os papéis de $\mathcal{M}$ e de $\mathcal{N}$, conclui-se também $m \leqslant n$. Será, assim, $m = n$, e os vectores V_l são independentes. As relações (9) mostram agora que, na base dos V_l, a representação ϑ_1 se torna na adjunta de ϑ_1. Pode enunciar-se o seguinte

Teorema:- É condição necessária e suficiente, para que o produto $\vartheta_1 \times \vartheta_2$ de duas representações irredutíveis contenha a representação idêntica, que elas sejam do mesmo grau e que a representação ϑ_2 seja equivalente à adjunta de ϑ_1.

Sejam $x_1, \ldots, x_m$ as componentes dum vector $\mathcal{X} \in \mathcal{M}$, $y_1, \ldots y_n$ as dum vector $Y \in \mathcal{N}$, e $z_1, \ldots, z_{mn}$ as dum vector $\mathcal{Z}$ do espaço produto $\mathcal{R}$. Pode pôr-se, por ex.:

$$
\begin{aligned}
z_1 &= \text{componente segundo o eixo } u_1 v_1 , \\
&\text{- - - - - - - - - - - - - - - - - - -} \\
z_m &= \quad " \quad " \quad " \quad " \quad u_m v_1 , \\
z_{m+1} &= \quad " \quad " \quad " \quad " \quad u_1 v_2 , \\
&\text{- - - - - - - - - - - - - - - - - - -} \\
z_{2m} &= \quad " \quad " \quad " \quad " \quad u_m v_{a_2} , \\
&\text{- - - - - - - - - - - - - - - - - - -} \\
z_{km+j} &= \quad " \quad " \quad " \quad " \quad u_j v_{k+1} , \\
&\text{- - - - - - - - - - - - - - - - - - -} .
\end{aligned}
$$

A variância de z_{km+j}, que corresponde à matriz $A \times A'$, é definida raciocinando como segue:

$$\sum_{j,k} u_j v_{k+1} z_{km+j} \longrightarrow \sum_{j,k} (Au_j . A' v_{k+1}) z_{km+j} =$$

$$= \sum_{r,s} u_r v_s \left(\sum_{j,k} a_{rj} a'_{s,k+1} z_{km+j} \right) ,$$

$$z'_{(s-1)m+r} = \sum_{j,k} a_{rj} a'_{sk} z_{km+j} , \qquad \begin{cases} j = 1, 2, \ldots, m , \\ k = 0, 1, \ldots, n-1 . \end{cases}$$

Mudando aqui k em $k + 1$, vem

$$z'_{(s-1)m+r} = \sum_{j,k} a_{rj} a'_{sk} z_{(k-1)m+j} , \qquad \begin{cases} j = 1, 2, \ldots, m , \\ k = 1, 2, \ldots, n . \end{cases}$$

Consideremos, por outro lado, a variância do produto $x_r y_s$ quando x_r e y_s variam separàdamente. Tem-se

$$x'_r = \sum_j a_{rj} x_j , \qquad y'_s = \sum_k a'_{sk} y_k ,$$

$$x'_r y'_s = \sum_{j,k} a_{rj} a'_{sk} x_r y_s .$$

Assim, a variância de $z'_{(s-1)m+r}$ é a mesma que a de $x'_r y'_s$. Tendo em vista a proposição anterior, podemos dizer:

Teorema:- Se ϑ_1 e ϑ_2 são representações irredutíveis de $\mathcal{G}$ e se ϑ_2 não é equivalente a ϑ_{1a}, não há forma bilinear das variáveis $x_1, \ldots, x_m ; y_1, \ldots, y_n$ que fique invariante, quando as duas séries de variáveis se sujeitam à variância que lhes corresponde em ϑ_1 e ϑ_2, respectivamente.

É claro que, sendo a representação irredutível ϑ_2 equivalente à adjunta da representação irredutível ϑ_1, inversamente, esta última é equivalente à adjunta de ϑ_2. As representações ϑ_1 e ϑ_2 dizem-se, então, contragradiantes uma da outra. Numa base determinada, o vector $\Sigma u_l v_l$ é invariante para a representação produto. Em termos de formas lineares, podemos enunciar o seguinte

Teorema:- A representação irredutível ϑ e a sua adjunta ϑ_a deixam invariante a forma bilinear $\Sigma x_l y_l = F$. Sujeitando, com efeito, os x_l à variância imposta por A e os y_l à variância imposta por $A^{-1} = A'$, tem-se

$$\sum_l x_l y_l \longrightarrow \sum_l \left(\sum_k a_{lk}^{-1} x_k\right)\left(\sum_j a'^{-1}_{lj} y_j\right) = \sum_{j,k}\left(\sum_l a_{lk}^{-1}\tilde{a}_{lj}\right)x_k y_j =$$

$$= \sum_{j,k}\left(\sum_l a_{jl}\, a_{lk}^{-1}\right) x_k y_j = \sum_{j,k} \delta_{jk} x_k y_j = \sum_k x_k y_k \,.$$

Podemos precisar, mostrando que não há outra forma bilinear invariante. Seja $G = \sum g_{lk} x_l y_k$ uma tal forma. Mediante A e A', a matriz (g_{lk}), de G, torna-se na matriz correspondente à forma

$$G_1 = \sum_{l,k,r,s} g_{lk} a_{lr}^{-1} x_r a'^{-1}_{ks} y_s = \sum_{r,s}\left(\sum_{l,k} \tilde{a}_{rl}^{-1} g_{lk} \tilde{a}_{ks}\right) x_r y_s \,.$$

Utilizando a mesma notação para matrizes e formas bilineares, é $G_1 = \tilde{A}^{-1} G \tilde{A}$. A invariância fica traduzida pela relação $\tilde{A}^{-1} G \tilde{A} = G$, ou $\tilde{A}\, G = G\, \tilde{A}$. No § seguinte demonstrar-se-á que uma matriz comutável com todas as matrizes duma representação irredutível, se não é a matriz nula, é múltipla da matriz unidade. Portanto, vale o

Teorema:- As formas bilineares $C \sum_l x_l y_l$ são as únicas que se conservam invariantes em face das transformações das representações irredutíveis $\mathfrak{g}$ e $\mathfrak{g}_a$.

Voltemos às representações irredutíveis do grau n, $\mathfrak{g}_1$ e $\mathfrak{g}_2$. Se $\mathfrak{g}_2$ não é equivalente a $\mathfrak{g}_{1a}$, a matriz M da representação produto $\mathfrak{g}_1 \times \mathfrak{g}_2$ é a matriz nula. Então têm lugar as relações

$$\sum_{A\times A'} a_{jl} a'_{lk} = \sum_A a_{jl} a'_{lk} = \sum_l a_{jl} a'_{lk} = 0,$$

como se conclui imediatamente de (8'). Se $\mathfrak{g}_2$ é igual a $\mathfrak{g}_{1a}$, sabemos que as únicas formas bilineares invariantes são

$$C(x_1 y_1 + \cdots + x_n y_n) \,.$$

Vamos procurar estas formas pelo processo geral. A partir de $x_r y_s$ (ou de $z_{(s-1)m+r}$), pela aplicação de $A \in \mathfrak{g}_1$ e de $A' \in \mathfrak{g}_2$, obtém-se

$$x_r y_s \longrightarrow \sum_{l,j} a_{rl}^{-1} a'^{-1}_{sj} x_l y_j \,,$$

de sorte que a forma invariante a ter em conta é

$$\sum_{l,j}\left(\sum_A a_{rl}^{-1}\, a'^{-1}_{sj}\right) x_l y_j \,.$$

Pondo $A^{-1} = \mathcal{A} = (\alpha_{lj})$, $A'^{-1} = \mathcal{A}' = (\alpha'_{lj})$, a forma anterior escreve-se

$$\sum_{l,j}\left(\sum_{\alpha} \alpha_{rl}\alpha'_{sj}\right) x_l y_j = \sum_{l,j}\left(\sum_A a_{rl} a'_{sj}\right) x_l y_j \,.$$

Tendo em vista resultados já estabelecidos, concluem-se as relações

$$\sum_A a_{rl} a'_{sj} = 0 \,, \qquad \text{se} \quad i \neq j \,. \tag{9'}$$

Quando $i = j$, deverá ter-se

$$\sum_A a_{rl} a'_{sl} = D \,,$$

onde a constante D é independente de i. Esta constante pode ser nula.
Vamos ver que assim sucede, se $r \neq s$, de modo que as únicas formas invariantes serão construidas a partir dos $x_r y_r$, todas elas estando incluidas na expressão

$$C(x_1 y_1 + \cdots + x_n y_n) \,.$$

Tem-se, de facto, atendendo a (9'),

$$\sum_A a_{rl} a'_{sl} = \sum_A a_{rl}^{-1}\, a'^{-1}_{sl} = \sum_A a_{rl}^{-1}\, \tilde{a}_{sl} = \sum_A a_{rl}^{-1}\, a_{ls} = \sum_A a'_{lr}\, a_{ls} = 0.$$

Por consequência, apenas $\sum a_{rl} a'_{rl}$ é $\neq 0$. Como a representação produto só tem uma vez a representação idêntica, a soma dos traços das matrizes é N (= nº de elementos de $\mathfrak{g}$). Ora essa soma é, por outro lado, igual a

$$\sum_A \Big(\sum_{j,\ell} a_{jj}\, a'_{\ell\ell} \Big) = \sum_{j,\ell} \Big(\sum_A a_{jj}\, a'_{\ell\ell} \Big) = \sum_j D = n\,D,$$

pelo que se tem $D = \frac{N}{n}$. Resumindo os resultados obtidos, pode enunciar-se o

Teorema:- Se $A, \ldots ; A', \ldots$ forem as matrizes de duas representações irredutíveis de grau n, tem-se

$$\sum_A a_{ij}\, a'_{k\ell} = 0 \ , \quad \text{se } \vartheta_2 \text{ não é equivalente a } \vartheta_1 ;$$

$$\sum_A a_{ij}\, a'_{k\ell} = \begin{cases} 0, & \text{se } (ij) \neq (k\ell) \text{ e } \vartheta_2 = \vartheta_1 ; \\ \frac{N}{n}, & \text{se } (ij) = (k\ell) \text{ e } \vartheta_2 = \vartheta_1 ; \end{cases}$$

onde N é o número de matrizes A, distintas ou não.

A noção de produto de representação subsiste inteiramente, mesmo que se trate de grupos infinitos. Demonstraremos o seguinte

Teorema:- O produto de duas representações unitárias é uma representação unitária. Sejam ϑ_1 e ϑ_2 as duas representações e $\mathcal{M}(u_1, \ldots, u_m)$, $\mathcal{N}(v_1, \ldots, v_n)$ os espaços de representação. Uma transformação $A \in \vartheta_1$ transforma as coordenadas dum vector do modo seguinte:

$$x_\lambda \to x'_\lambda = \sum_{j=1}^{m} a_{\lambda j} x_j \ , \qquad \overline{x'_\lambda} = \sum_j \overline{a}_{\lambda j}\, \overline{x}_j \ .$$

Para uma transformação $A' \in \vartheta_2$ é, anàlogamente,

$$y'_\lambda = \sum_1^n a'_{\lambda j}\, y_j \ , \qquad \overline{y'_\lambda} = \sum_j \overline{a}'_{\lambda j}\, \overline{y}_j \ .$$

No espaço $\mathcal{R}(u_\lambda v_\mu)$ as coordenadas dum vector são $c_{\lambda\mu}$. Dado o vector $V = \sum_{\lambda,\mu} u_\lambda v_\mu c_{\lambda\mu}$, tem-se, com $P = A \times A'$,

$$P\,V = \sum_{\lambda,\mu} (Au_\lambda)(A'v_\mu) c_{\lambda\mu} = \sum_{\lambda,\mu} \sum_{j,k} u_j v_k a_{j\lambda}\, a'_{k\mu}\, c_{\lambda\mu} =$$

$$= \sum_{j,k} u_j v_k \sum_{\lambda,\mu} a_{j\lambda}\, a'_{k\mu}\, c_{\lambda\mu} \ .$$

As fórmulas de transformação para as coordenadas dum vector são, assim,

$$c'_{jk} = \sum_{\lambda,\mu} a_{j\lambda}\, a'_{k\mu}\, c_{\lambda\mu} \ .$$

Ponhamos como métrica no espaço a forma de Hermite $\sum_{j,k} \overline{c}_{jk} c_{jk}$. Tem-se

$$\sum_{j,k} \overline{c}'_{jk} c'_{jk} = \sum_{j,k} \sum_{\lambda,\mu} \sum_{\rho,\sigma} \overline{a}_{j\lambda}\, \overline{a}'_{k\mu}\, \overline{c}_{\lambda\mu}\, a_{j\rho}\, a'_{k\sigma}\, c_{\rho\sigma} =$$

$$= \sum_{\lambda,\mu} \sum_{\rho,\sigma} \overline{c}_{\lambda\mu} c_{\rho\sigma} \sum_{j,k} \overline{a}_{j\lambda} a_{j\rho}\, \overline{a}'_{k\mu}\, a'_{k\sigma} = \sum_{\lambda,\mu} \sum_{\rho,\sigma} \overline{c}_{\lambda\mu} c_{\rho\sigma}\, \delta_{\lambda\rho}\, \delta_{\mu\sigma} =$$

$$= \sum_{\lambda,\mu} \overline{c}_{\lambda\mu} c_{\lambda\mu} \ ,$$

pois que ϑ_1 e ϑ_2 são unitárias. O teorema está demonstrado.

9) Homomorfismos de módulos simples - Sabe-se, da Teoria dos Grupos com operadores, que os endomorfismos dum módulo constituem um anel.(1) No que vai seguir-se, os módulos poderão ter um ou dois domínios operatórios. Se há dois, os operadores dum domínio (no geral elementos dum grupo $\mathcal{G}$) operarão à esquerda, os do outro operarão à direita.

Seja $\mathcal{M}$ um módulo simples. Vamos demonstrar o seguinte

Teorema:- O anel endomórfico dum módulo simples $\mathcal{M}$ constitui um corpo. Um endomorfismo operatório faz corresponder a $\mathcal{M}$ um seu sub-módulo $\mathcal{M}'$. Como deverá ter-se $\mathcal{M}' = (0)$ ou $\mathcal{M}' = \mathcal{M}$, o endomorfismo ou é o endomorfismo nulo, no qual a cada elemento de $\mathcal{M}$ corresponde o elemento nulo de $\mathcal{M}$, ou é um automorfismo. Neste último caso há, porém, um automorfismo inverso. Como existe um automorfismo idêntico, que faz corresponder a cada elemento

(1) Almeida Costa , "Elementos da Teoria dos Grupos", Porto, 1942, pgs. 130 e 131.

de $\mathfrak{M}$ o próprio elemento, segue-se que o anel endomórfico constitui um grupo, em face do preceito de produto (excluído que seja o elemento nulo). Ora um tal anel diz-se um corpo (ex.: o corpo dos números reais, o dos números complexos, etc.)

Consideremos, então, um espaço irredutível $\mathfrak{M}$, em face dum grupo $\mathcal{G}$. Os elementos de $\mathcal{G}$ introduzem transformações lineares em $\mathfrak{M}$. Designemos com $\underline{P}$ um endomorfismo operatório de $\mathfrak{M}$, por meio do qual, se $\mathfrak{x}'$ é correspondente de $\mathfrak{x}$, $g\mathfrak{x}'$ é correspondente de $g\mathfrak{x}$, se $g \in \mathcal{G}$. Assim, tem-se

$$\mathfrak{x}' = P\mathfrak{x}\ , \qquad g\mathfrak{x}' = P.g\mathfrak{x}\ ,$$

ou, pondo $g\mathfrak{x} = A\mathfrak{x}$,

$$A\mathfrak{x}' = A\,P\mathfrak{x} = P\,A\mathfrak{x}\ .$$

Este resultado mostra que o endomorfismo $\underline{P}$ comuta com todas as matrizes $\underline{A}$. Vale o

Teorema:- A matriz $\underline{P}$ do endomorfismo operatório é uma matriz diagonal de elementos iguais. De facto, é

$$A(P - \lambda U)\,\mathfrak{x} = (P - \lambda U)A\mathfrak{x}\ ,$$

onde λ é um número. Se a matriz $\underline{P}$ não é a matriz nula, determina um automorfismo de $\mathfrak{M}$. Mas pode calcular-se λ por forma que $P - \lambda U$ faça corresponder o vector nulo a um vector não nulo. Em primeiro lugar $Q = P - \lambda U$ determina um endomorfismo operatório de $\mathfrak{M}$, porque, pondo $\mathfrak{x}' = Q\mathfrak{x}$, tem-se $Q.A\mathfrak{x} = AQ\mathfrak{x} = A\mathfrak{x}'$, o que mostra valer a correspondência

$$\mathfrak{x} \longrightarrow \mathfrak{x}' = Q\mathfrak{x}\ , \qquad g\mathfrak{x} \longrightarrow QA\mathfrak{x} = g\mathfrak{x}'\ .$$

Em seguida, as igualdades

$$\begin{aligned} x_1' &= (p_{11} - \lambda)x_1 + \ldots + p_{1n}x_n = 0\ , \\ &\text{- - - - - - - - - - - - - -} \\ x_n' &= p_{n1}x_1 + \ldots + (p_{nn} - \lambda)x_n = 0, \end{aligned}$$

onde os $\underline{x_i'}$ são as componentes de $\mathfrak{x}'$, os $\underline{x_i}$ as de $\mathfrak{x}$ e os $\underline{p_{ij}}$ os elementos de $\underline{P}$, poderão ter soluções $x_i \neq 0$, determinando λ pela equação secular

$$\begin{vmatrix} p_{11} - \lambda & \cdots & p_{1n} \\ \text{- - - - - - -} & & \\ p_{n1} & \cdots & p_{nn} - \lambda \end{vmatrix} = 0\ .$$

Nestas condições, a matriz $P - \lambda U$ determina a correspondência $\mathfrak{M} \sim (0)$, pelo que será a matriz nula. E, de $P - \lambda U = 0$, tira-se $P = \lambda U$, q. e. d.

Imaginemos agora que $\mathfrak{M}_1$ e $\mathfrak{M}_2$ são dois espaços irredutíveis com o mesmo domínio operatório $\mathcal{G}$. Se $\underline{P}$ determina um homomorfismo operatório de $\mathfrak{M}_1$ sobre $\mathfrak{M}_2$, os correspondentes $\underline{E_i}$, dos elementos base $e_i^{(1)}$, de $\mathfrak{M}_1$, exprimem-se nos elementos base $e_j^{(2)}$, de $\mathfrak{M}_2$, do modo seguinte:

$$\begin{aligned} E_1 &= e_1^{(2)}p_{11} + \ldots + e_m^{(2)}p_{m1}\ , \\ &\text{- - - - - - - - - - - -} \\ E_n &= e_1^{(2)}p_{1n} + \ldots + e_m^{(2)}p_{mn}\ , \end{aligned}$$

supondo $\underline{n}$ o número de dimensões de $\mathfrak{M}_1$ e $\underline{m}$ o de $\mathfrak{M}_2$. Se o homomorfismo $\underline{P}$ não é o homomorfismo nulo, trata-se necessàriamente dum isomorfismo. Então, os vectores E_k constituem uma base independente de $\mathfrak{M}_2$, tendo-se $m = n$. Designemos com $\mathfrak{x}_2 \in \mathfrak{M}_2$ o correspondente de $\mathfrak{x}_1 \in \mathfrak{M}_1$, por meio de $\underline{P}$. Se $g \in \mathcal{G}$, tem-se

$$\mathfrak{x}_1 \longrightarrow \mathfrak{x}_2\ , \qquad g\mathfrak{x}_1 \longrightarrow g\mathfrak{x}_2\ .$$

Representando com $\underline{A_1}$ e $\underline{A_2}$ as matrizes representativas de $\underline{g}$ nos dois espaços, é $P.g\mathfrak{x}_1 = PA_1\mathfrak{x}_1 = g\mathfrak{x}_2 = A_2\mathfrak{x}_2 = A_2P\mathfrak{x}_1$. Não pode dizer-se aqui que $PA_1 = A_2P$ traduza a comutabilidade de $\underline{P}$ com as matrizes $\underline{A_1}$ ou $\underline{A_2}$. Todavia, efectuemos em $\mathfrak{M}_2$ a transformação de base indicada por $P = (p_{ij})$, ou seja, passemos de $e_j^{(2)}$ para os E_j. A matriz $\underline{A_2}$ tomará a forma $A_2' = P^{-1}A_2P =$

Assim, tomando nos espaços equivalentes $\mathfrak{M}_1$ e $\mathfrak{M}_2$ duas bases que se correspondam na isomorfia, as matrizes representativas dos operadores são iguais, como, aliás, já era sabido. Supondo realizada essa condição, imaginemos agora um isomorfismo operatório $\underline{T}$ dos dois espaços. A matriz $\underline{T}$ é ainda uma matriz diagonal de elementos iguais, pois verifica a condição $TA_1 = A_1T$, tal como no caso dum endomorfismo.

10) Caracteres dos grupos. Representação regular - Seja $\mathcal{G}$ um grupo qualquer. Já dissemos que uma representação de $\mathcal{G}$, não fiel, é representação fiel dum certo grupo factor $\mathcal{G}/\mathcal{J}$. Quase no final do § 8, foi enunciado um teorema que contém somatórios estendidos aos elementos de $\mathcal{G}$ ou às matrizes não distintas da representação. É evidente que poderia fazer-se uma ligeira modificação, de modo a estender os somatórios aos elementos de $\mathcal{G}/\mathcal{J}$ ou às matrizes distintas da referida representação. Por comodidade, poremos agora

$$\mathcal{G} = \{u, a, b, \ldots, s, t, \ldots\}$$

e designaremos as matrizes das representações irredutíveis $\mathcal{D}_1$ e $\mathcal{D}_2$ respectivamente com

$$A(u),\ A(a), \ldots,\ A(s), \ldots ;$$

$$A'(u), A'(a), \ldots, A'(s), \ldots .$$

As relações finais do § 8 escrevem-se

$$\sum_s a_{ij}(s)\, a'_{k\ell}(s) = 0, \text{ se } \mathcal{D}_2 \text{ não é equivalente a } \mathcal{D}_{1a} ;$$

$$\sum_s a_{ij}(s)\, a'_{k\ell}(s) = \begin{cases} 0, & \text{se } (ij) \neq (k\ell) \text{ e } \mathcal{D}_2 = \mathcal{D}_{1a} ; \\ \frac{N}{n}, & \text{se } (ij) = (k\ell) \text{ e } \mathcal{D}_2 = \mathcal{D}_{1a} . \end{cases}$$

Representemos com $a_{ij}(s)$ os elementos da matriz correspondente a s na representação $\mathcal{D}_{1a}$ e tenhamos em conta que é $a_{ij}(s^{-1}) = \overline{a'_{ij}}(s)$. Pode escrever-se, então

$$\sum_s a_{ij}(s)a'_{k\ell}(s) = \sum_s a^{-1}_{ij}(s^{-1})a'_{k\ell}(s) = \sum_s \alpha_{ji}(s^{-1})a'_{k\ell}(s) .$$

Sejam Δ_1 e Δ_2 duas representações irredutíveis e $A(s)$, $A'(s)$ as matrizes correspondentes. As relações finais do § 8 podem tomar a forma

$$\left.\begin{aligned} &\sum_s a_{ij}(s)a'_{k\ell}(s^{-1}) = 0, \quad \text{se } \Delta_1 \text{ e } \Delta_2 \text{ não são equivalentes;} \\ &\sum_s a_{ij}(s)a'_{k\ell}(s^{-1}) = \begin{cases} 0, & \text{se } (ji) \neq (k\ell) \text{ e } \Delta_2 = \Delta_1 ; \\ \frac{N}{n}, & \text{se } (ji) = (k\ell) \text{ e } \Delta_2 = \Delta_1 . \end{cases} \end{aligned}\right\} (10)$$

Tomemos um espaço de métrica $\sum \overline{x}_i x_i$, no qual as matrizes de Δ_2 sejam unitárias. Nesse caso é $A'^{-1}(s) = A'^{*}(s)$, ou ainda $A'(s^{-1}) = A'^{*}(s)$. As relações (10) escrevem-se ainda

$$\left.\begin{aligned} &\sum_s a_{ij}(s)\overline{a}'_{\ell k}(s) = 0, \quad \text{se } \Delta_1 \text{ e } \Delta_2 \text{ não são equivalentes ;} \\ &\sum_s a_{ij}(s)\overline{a}'_{\ell k}(s) = \begin{cases} 0, & \text{se } (ij) \neq (\ell k) \text{ e } \Delta_2 = \Delta_1 ; \\ \frac{N}{n}, & \text{se } (ij) = (\ell k) \text{ e } \Delta_2 = \Delta_1 . \end{cases} \end{aligned}\right\} (11)$$

Teorema:- Se Δ_1 e Δ_2 são duas representações irredutíveis dum grupo $\mathcal{G}$, têm lugar as seguintes relações de ortogonalidade dos caracteres

$$\sum_s x_1(s)\,\overline{x}_2(s) = \begin{cases} 0, & \text{se } \Delta_1 \text{ e } \Delta_2 \text{ não são equivalentes} ; \\ N, & \text{se } \Delta_1 \text{ e } \Delta_2 \text{ são equivalentes.} \end{cases} \quad (12)$$

Como as relações entre os caracteres são independentes das bases de referência, utilizaremos as igualdades (11). A primeira dá

(1) O símbolo $x_1(s)$ representa o traço ou caracter da matriz de Δ_1 que corresponde a s.

$$\sum_{i,k}\left(\sum_s a_{ii}(s)\overline{a}^{1}_{kk}(s)\right) = \sum_s\left(\sum_i a_{ii}(s)\cdot\sum_k \overline{a}^{1}_{kk}(s)\right) = \sum_s \chi_1(s)\,\overline{\chi}_2(s) = 0.$$

As outras igualdades dão, nas mesmas condições,

$$\sum_{i,j}\sum_s a_{ii}(s)\overline{a}^{1}_{jj}(s) = \sum_s\left(\sum_i a_{ii}(s)\cdot\sum_j \overline{a}^{1}_{jj}(s)\right) = \sum_s \chi_1(s)\,\overline{\chi}_2(s) =$$

$$= \sum_{i,j}\sum_s a_{ii}(s)\,\overline{a}^{1}_{jj}(s) = \sum_i\sum_s a_{ii}(s)\,\overline{a}^{1}_{ii}(s) = \sum_i \frac{N}{n} = N\ ,\ \text{q. e. d.}$$

Corolário 1º:- É condição necessária e suficiente, para que duas representações irredutíveis Δ_1 e Δ_2 sejam equivalentes, que tenham os mesmos caracteres. Se são equivalentes, têm os mesmos caracteres. Se têm os mesmos caracteres, como Δ_2 é equivalente de si mesmo, pode escrever-se

$$\sum_s \chi_2(s)\,\overline{\chi}_2(s) = N = \sum_s \chi_1(s)\,\overline{\chi}_2(s),$$

o que, em face do teorema, mostra ser Δ_1 equivalente de Δ_2.

Corolário 2º:- Pondo de parte equivalências, uma representação qualquer $\mathcal{D}$ (completamente redutível), dum grupo finito $\mathcal{G}$, fica determinada pelos traços das suas matrizes. Façamos uma redução de $\mathcal{D}$ e designemos com $\chi_1, \ldots, \chi_\rho$ os caracteres das representações irredutíveis $\mathcal{D}_i$ $(i = 1, \ldots, \rho)$ que nela figuram. Se for a_i o número de vezes que comparece a representação $\mathcal{D}_i$, tem-se

$$T(s) = a_1\chi_1(s) + \ldots + a_\rho\chi_\rho(s),$$

onde se representa com T(s) o traço da matriz correspondente a s. Daqui deduz-se

$$\sum_s T(s)\,\overline{\chi}_i(s) = \sum_s\sum_j a_j\chi_j(s)\overline{\chi}_i(s) = \sum_j a_j\sum_s \chi_j(s)\,\overline{\chi}_i(s) = a_i N\ .$$

Admitindo conhecidos os caracteres das representações irredutíveis, que são bem determinados, as igualdades anteriores definem os números a_i, e o corolário fica demonstrado. Importa, porém,

introduzir o seguinte

Complemento ao corolário 2º:- As representações irredutíveis que figuram numa representação dum grupo finito $\mathcal{G}$, pondo de parte a ordem e equivalência, são bem determinadas. A demonstração faz-se imediatamente, admitindo duas reduções diferentes da representação em causa.

A questão do número de representações irredutíveis distintas do grupo $\mathcal{G}$ levanta-se imediatamente. Para começarmos a sua resolução, vamos definir o que se entende pela representação regular de $\mathcal{G}$. Tomemos o espaço $\mathcal{M}_N$, em que os elementos base são os N elementos u, a, ..., s, ..., t, de $\mathcal{G}$, e para o qual $\mathcal{G}$ é domínio operatório conforme a regra

$$s(u\,\epsilon_1 + a\,\alpha_2 + \ldots + t\,\alpha_N) = s\,\alpha_1 + (sa)\alpha_2 + \ldots + (st)\alpha_N\ ,$$

onde, é claro, os α_i são números complexos. Fàcilmente se vê ser

$$T(u) = N\ ,\qquad T(s) = 0\ ,\qquad (\text{se } s \neq u)\ .$$

Tem lugar o seguinte importante

Teorema:- A representação regular D, de $\mathcal{G}$, contém todas as representações irredutíveis e cada uma delas tantas vezes quantas o seu respectivo grau. Façamos, com efeito, a redução completa de D conforme a igualdade

$$D = a_1\mathcal{D}_1 + \ldots + a_q\mathcal{D}_q\ ,$$

na qual $\mathcal{D}_i$ é símbolo de representação irredutível e a_i dá o número de vezes que $\mathcal{D}_i$ comparece em D. Tem-se

$$T(s) = a_1\chi_1(s) + \ldots + a_q\chi_q(s) = \begin{cases} N, & \text{se } s = u, \\ 0, & \text{se } s \neq u, \end{cases}$$

e também

$$\sum_s T(s)\,\overline{\chi_1}(s) = N\,\overline{\chi_1}(u) = Nn_1 = a_1 N\ ,$$

onde n_1 é o grau da representação $\mathfrak{D}_1$. Vê-se que é $a_1 = n_1$. A conclusão é a mesma para qualquer $\mathfrak{D}_l$. Se uma representação irredutível $\mathfrak{D}_j$ não figurasse em D, chegava-se a um absurdo. O teorema está demonstrado e o número dos $\mathfrak{D}_l$ é bem determinado.

Posto isto, decomponhamos $\mathcal{G}$ em classes de elementos conjugados. Aos elementos da mesma classe correspondem, em qualquer representação, matrizes com o mesmo traço:

$$T(s) = T(asa^{-1}),\quad \text{pois}\quad |A(asa^{-1})| = |A(a)|\cdot|A(s)|\cdot|A(a^{-1})| = |A(s)|$$

Os traços dos elementos de $\mathcal{G}$ podem considerar-se, assim, como "funções de classe", de modo que, se forem $C_1, C_2, \ldots, C_r$, essas classes, e se for q o número de representações irredutíveis, a totalidade dos caracteres fica definida pelo quadro matricial seguinte:

$$\left\|\begin{matrix} \chi_1(C_1) & \chi_1(C_2) & \ldots & \chi_1(C_r) \\ \chi_2(C_1) & \chi_2(C_2) & \ldots & \chi_2(C_r) \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots\cdots \\ \chi_q(C_1) & \chi_q(C_2) & \ldots & \chi_q(C_r) \end{matrix}\right\| . \qquad (13)$$

Suponhamos $q > r$. Se da matriz rectangular anterior se puder extrair um determinante de ordem r não nulo, existem soluções bem determinadas para um sistema de equações como, por ex., o seguinte:

$$\begin{aligned} \chi_q(C_1) &= \beta_1\chi_1(C_1) + \beta_2\chi_2(C_1) + \ldots + \beta_r\chi_r(C_1)\ , \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \chi_q(C_r) &= \beta_1\chi_1(C_r) + \beta_2\chi_2(C_r) + \ldots + \beta_r\chi_r(C_r)\ . \end{aligned}$$

Neste caso existem relações lineares entre os caracteres da forma

$$\sum_{\rho=1}^{q} \lambda_\rho \chi_\rho(C_l) = 0, \qquad (14)$$

sem que sejam nulos todos os λ_ρ. Ora uma tal relação é impossível, como vamos verificar. Representando com h_ρ o número de elementos da classe C_ρ, as relações (12) podem escrever-se

$$\sum_s \chi_i(s)\overline{\chi}_2(s) = h_1\chi_1(C_1)\overline{\chi}_2(C_1) + \ldots + h_r\chi_i(C_r)\overline{\chi}_2(C_r) = \begin{cases} 0\ , \\ N\ , \end{cases}$$

conforme Δ_1 e Δ_2 não são ou são equivalentes. De (14) deduz-se em seguida

$$\sum_{l=1}^{r} h_l\,\overline{\chi}_j(C_l)\cdot\sum_{\rho=1}^{q}\lambda_\rho\chi_\rho(C_l) = \sum_\rho \lambda_\rho \sum_l h_l\,\chi_\rho(C_l)\,\overline{\chi}_j(C_l) = \lambda_j N = 0\ ,$$

contra o facto de haver coeficientes λ_j diferentes de zero. Se, porventura, todos os determinantes não nulos tirados de (13) forem de ordem inferior a r, a conclusão é a mesma. Será, assim $q \geq r$. Posto isto, os raciocínios que vão seguir-se levar-nos-ão ao resultado expresso na proposição seguinte:

Teorema:- O número de representações irredutíveis não equivalentes dum grupo finito é igual ao número de classes de elementos conjugados em que o grupo pode ser decomposto. Designemos com $s_1^{(l)}, \ldots, s_{h_l}^{(l)}$ os elementos da classe C_l, e, dada uma representação qualquer de $\mathcal{G}$, formemos a matriz

$$\mathcal{C}_l = A(C_l) = A(s_1^{(l)}) + \ldots + A(s_{h_l}^{(l)}). \qquad (15)$$

O produto

$$\mathcal{C}_l\,\mathcal{C}_j = \sum_{k=1}^{h_l}\sum_{\ell=1}^{h_j} A(s_k^{(l)})\,A(s_\ell^{(j)})$$

pode escrever-se sob a forma

$$\mathcal{C}_l\mathcal{C}_j = \sum_{m=1}^{r} \alpha_{ljm}\,A(C_m), \qquad (16)$$

pelos motivos a seguir. Consideremos duas classes de elementos conjugados de $\mathcal{G}$:

$$a,\ b,\ldots,\ s\ ; \qquad \alpha\ ,\ \beta,\ldots,\sigma\ ;$$

e o conjunto dos produtos dos elementos duma pelos da outra. Se t for um elemento qualquer de $\mathcal{G}$, aquelas classes podem escrever-se

$$t\,a\,t^{-1},\ldots,\ t\,s\,t^{-1};\qquad t\alpha t^{-1},\ldots,\ t\sigma t^{-1}\ ;$$

e o produto dos elementos duma pelos da outra é constituido por elementos da forma

$$t\,s\,t^{-1}.\ t\sigma t^{-1} = t\,s\sigma t^{-1}\ .$$

Conclui-se, assim, que o conjunto produto se não modifica quando os seus elementos, P, se transformam em tPt^{-1}. Ora o produto contém, com cada elemento, os seus conjugados, de modo que, extraindo dele todas as classes completas possíveis (com, ou sem repetição) o conjunto que ainda fica tem de continuar a ser invariante em face da transformação $P \longrightarrow tPt^{-1}$. Só pode ser o conjunto vazio, visto já não conter qualquer classe. A fórmula (16) está justificada. O coeficiente α_{ijm} indica o número de vezes que se repete $A(C_m)$.

Os resultados do § anterior permitem dar uma propriedade importante da matriz $A(C_i)$, no caso de se tratar duma representação irredutível. Dados dois elementos conjugados $a, b \in \mathcal{G}$, tais que $b = x\,a\,x^{-1}$, é

$$tb = t.xax^{-1} = tx.a.(tx)^{-1}.t\ .$$

Nessas condições, multiplicando à esquerda ou à direita uma classe de elementos conjugados por um elemento t, obtém-se o mesmo conjunto de elementos. Assim, é

$$A(t).A(C_i) = A(C_i).A(t),$$

e, por consequência, $\mathcal{O}_i$ é múltipla da matriz unidade:

$$\mathcal{O}_i = A(C_i) = \lambda_i U\ .$$

Lema 1º:- Os caracteres das representações irredutíveis dum grupo finito $\mathcal{G}$ verificam as relações

$$\sum_{i=1}^{q} \chi_i(u)\,\chi_i(C_k) = \begin{cases} 0, & \text{se } C_k \neq \{u\}\ , \\ N, & \text{se } C_k = \{u\}\ . \end{cases}$$

Escrevendo a representação regular D sob a forma

$$D = n_1\vartheta_1 + \cdots + n_q\vartheta_q\ ,$$

a igualdade entre os traços dos dois membros dá

$$T(u) = n_1\chi_1(u) + \cdots + n_q\chi_q(u) = \sum_{i=1}^{q} \chi_i(u)\,\chi_i(u) = N,$$

$$T(s) = \chi_1(u)\,\chi_1(C_k) + \cdots + \chi_q(u)\,\chi_q(C_k) = 0\ , \qquad (s \in C_k)\ ,$$

como se deseja. Neste lema está incluido o importante resultado seguinte: os graus $n_1,\ldots,\ n_q$ das representações irredutídum grupo finito $\mathcal{G}$ verificam a igualdade

$$\sum_{i=1}^{q} n_i^2 = N\ .$$

Dada uma classe C_j, designemos com $C_{j'}$ a classe cujos elementos são os inversos dos elementos daquela. Tem lugar o seguinte

Lema 2º:- Os caracteres das representações irredutíveis dum grupo $\mathcal{G}$ verificam as seguintes relações:

$$\sum_{i=1}^{q} \chi_i(C_j)\,\chi_i(C_k) = \begin{cases} 0, & \text{se } k \neq j', \\ \dfrac{N}{h_j}, & \text{se } k = j'. \end{cases}$$

Tomemos uma representação irredutível qualquer ϑ_i, de grau n_i. Para a classe $C_1 = \{u\}$, tem-se $\chi_i(C_1) = \chi_i(u) = n_i$. Como é, nessa representação,

$$A(C_j) = \lambda_j U\ , \qquad A(C_R) = \lambda_R U\ ,$$

$$A(C_j).A(C_R) = \lambda_j \lambda_R U = \sum_{m=1}^{r} \alpha_{jRm} A(C_m) = \sum_{m=1}^{r} \alpha_{jRm} \lambda_m U = U . \sum_{m=1}^{r} \alpha_{jRm}\ \lambda_m ,$$

têm-se as relações, análogas a (16),

$$\lambda_j\ \lambda_R = \sum_{m=1}^{r} \alpha_{jRm} \lambda_m .$$

Por outro lado é $\chi_l(\mathcal{C}_j) = \lambda_j n_l$, de modo que a igualdade anterior dá

$$\chi_l(\mathcal{C}_j) . \chi_l(\mathcal{C}_R) = n_l \sum_{m=1}^{r} \alpha_{jRm} \chi_l(\mathcal{C}_m) .$$

Tem-se agora sucessivamente

$$\chi_l(\mathcal{C}_j) = h_j\ \chi_l(C_j) ,$$

$$h_j h_R \chi_l(C_j)\ \chi_l(C_R) = n_l \sum_{m=1}^{r} \alpha_{jRm}\ h_m \chi_l(C_m) ,$$

$$\sum_{l=1}^{q} \chi_l(C_j)\ \chi_l(C_R) = \frac{1}{h_j h_R} \sum_{l=1}^{q} n_l \sum_{m=1}^{r} \alpha_{jRm} h_m \chi_l(C_m) = \frac{1}{h_j h_R} \sum_{m=1}^{r} h_m \alpha_{jRm} .$$

$$. \sum_{l=1}^{q} \chi_l(u)\ \chi_l(C_m) ,$$

e, portanto, atendendo ao lema anterior,

$$\sum_{l=1}^{q} \chi_l(C_j)\ \chi_l(C_R) = \frac{1}{h_j h_R} \alpha_{jR1} . N .$$

É fácil encontrar os coeficientes α_{jR1}. No produto $\mathcal{C}_j . \mathcal{C}_R$ o aparecimento de $A(u) = U$ exige que haja dois elementos $s_\alpha^{(j)}, s_\beta^{(R)}$ que sejam inversos. Essa circunstância leva a $\mathcal{C}_R = \mathcal{C}_{j'}$, ou $k = j'$. Quando for $k \neq j'$, é $\sum_{l=1}^{q} \chi_l(C_j)\ \chi_l(C_R) = 0$. Tendo-se $k = j'$, cada elemento da classe C_R é inverso dum elemento da classe C_j, as duas classes têm o mesmo número de elementos h_j e o produto $\mathcal{C}_j \mathcal{C}_R$ contém h_j vezes a matriz $A(u) = U$. Então é $\alpha_{jR1} = h_j$,

e, portanto,

$$\sum_{l=1}^{q} \chi_l(C_j)\ \chi_l(C_R) = \frac{N}{h_j} .$$

Demonstrados os lemas, o teorema que enunciámos resulta imediatamente. No quadro matricial (13) não pode haver uma relação linear entre as colunas, visto que, pondo

$$\sum_{R=1}^{r} \alpha_R \chi_i(C_R) = 0, \qquad (i = 1, 2, \ldots, q) ,$$

virá também

$$\sum_{l} \chi_l(C_j) \sum_{R=1}^{r} \alpha_R \chi_l(C_R) = \sum_{R} \alpha_R \sum_{l} \chi_l(C_j)\ \chi_l(C_R) = \alpha_{j'} \frac{N}{h_j} = 0, \quad \alpha_{j'} = 0 .$$

O número r das colunas não pode ser maior que q, e as duas desigualdades $r \geq q$, $q \geq r$ dão $q = r$.

11) Aplicações e exemplos - A representação $\mathcal{G}_a$, adjunta duma representação qualquer $\mathcal{G}$, diz-se também contragradiante de $\mathcal{G}$, tal como no caso em que $\mathcal{G}$ é irredutível. O vector $\Sigma u_l v_l$ é invariante para o produto $\mathcal{G} \times \mathcal{G}_a$:

$$P. \sum_{l} u_l v_l = \sum_{l} Au_l . A' v_l = \sum_{l, j, R} u_j a_{jl}\ v_R a'_{Rl} = \sum_{j, R} u_j\ v_R \left(\sum_{l} a_{jl}\ a'_{Rl}\right) =$$

$$= \sum_{j, R} u_j v_R \left(\sum_{l} a_{jl}\ a_{iR}^{-1}\right) = \sum_{j, R} u_j v_R \delta_{jR} = \sum_{j} u_j v_j .$$

Quando $\mathcal{G}$ é completamente redutível, $\mathcal{G}_a$ é também completamente redutível, como vamos ver. Seja

$$A = \begin{pmatrix} \mathcal{A} & \mathcal{B} \\ 0 & \mathcal{C} \end{pmatrix}, \qquad A^{-1} = \begin{pmatrix} \mathcal{A}' & \mathcal{B}' \\ \mathcal{F}' & \mathcal{L}' \end{pmatrix} .$$

A igualdade

$$A^{-1} A = \begin{pmatrix} \mathcal{A}'\mathcal{A} & \mathcal{A}'\mathcal{B} + \mathcal{B}'\mathcal{C} \\ \mathcal{F}'\mathcal{A} & \mathcal{F}'\mathcal{B} + \mathcal{L}'\mathcal{C} \end{pmatrix} = U$$

mostra que $\mathcal{U}'$ é inversa de $\mathcal{U}$. Por outro lado, tendo-se

$$\mathcal{F}'\,\mathcal{U} = 0\ , \qquad \mathcal{F}'\,\mathcal{U}\,\mathcal{U}' = \mathcal{F}' = 0\ ,$$

a conclusão é imediata.

Se $\mathcal{G}$ é unitária, a relação $A\,A^* = U$ dá $\bar{A}\bar{A}^* = U = \bar{A}^*\bar{A}$, de sorte que a inversa de $\bar{A}$ é $\bar{A}^*$. Esta última resulta de $\underline{A}$ por passagem aos complexos conjugados. Neste caso, por consequência, dá imediatamente a adjunta.

O produto de representações goza da propriedade distributiva, no sentido seguinte: se $\mathcal{G}$ é completamente redutível e da forma $\mathcal{G} = \mathcal{G}_2 + \mathcal{G}_3$, tem-se $\mathcal{G}_1 \times \mathcal{G} = \mathcal{G}_1 \times (\mathcal{G}_2 + \mathcal{G}_3) = \mathcal{G}_1 \times \mathcal{G}_2 + \mathcal{G}_1 \times \mathcal{G}_3$. A verificação é imediata. Servindo-nos deste resultado, podemos demonstrar o seguinte

Teorema:- É condição necessária e suficiente, para que o produto $\mathcal{G} \times \mathcal{G}'$, onde $\mathcal{G}$ é completamente redutível, contenha a representação idêntica, que na decomposição de $\mathcal{G}$ figure uma representação equivalente a $\mathcal{G}_a'$. De facto, pondo $\mathcal{G} = \mathcal{G}_1 + \cdots + \mathcal{G}_h$, tem-se

$$\mathcal{G} \times \mathcal{G}' = \mathcal{G}_1 \times \mathcal{G}' + \cdots + \mathcal{G}_h \times \mathcal{G}'\ .$$

Se a representação idêntica figura no 1º membro, figura numa das parcelas do 2º membro e há uma representação $\mathcal{G}_i$ equivalente a $\mathcal{G}_a'$. E a inversa é também imediata.

Visto que o produto de duas representações unitárias é unitária e que toda a representação unitária é completamente redutível, vamos resolver o seguinte

Problema:- Reduzir os produtos $\mathcal{U}_R \times \mathcal{U}$ das representações unitárias do final do § 7. Comecemos por $\mathcal{U}_0^- \times \mathcal{U}_0^-$. Como o produto é uma representação do 1º grau, só pode tratar-se de $\mathcal{U}_0^+$ ou de $\mathcal{U}_0^-$. A dúvida levanta-se procurando o "carácter" da reflexão S. Se as bases das representações dadas são $\underline{u}_0$ e $\underline{v}_0$, tem-se

$$S(u_0 v_0) = (S\,u_0).(S\,v_0) = (-u_0).(-v_0) = u_0 v_0\ .$$

Será, pois,

$$\mathcal{U}_0^- \times \mathcal{U}_0^- = \mathcal{U}_0^+\ .$$

Tratemos, em seguida, o produto $\mathcal{U}_R \times \mathcal{U}_0^+$. Se for $k = 0$, tem-se imediatamente

$$\mathcal{U}_0^+\ \mathcal{U}_0^+ = \mathcal{U}_0^+\ , \qquad \mathcal{U}_0^- \times \mathcal{U}_0^+ = \mathcal{U}_0^-\ .$$

Supondo $k > 0$, vem

$$S(u_R v_0) = (S u_R).(S v_0) = u_R v_0\ ,$$

$$S(u_{-R} v_0) = (S u_{-R}).(S v_0) = u_R v_0\ ,$$

$$R_\varphi(u_R v_0) = (R_\varphi u_R).(R_\varphi v_0) = u_R v_0\, e^{iR\varphi}$$

$$R_\varphi(u_{-R} v_0) = (R_\varphi u_{-R}).(R_\varphi v_0) = u_{-R} v_0\, e^{-iR\varphi}\ .$$

Na representação produto têm lugar as correspondências

$$S \to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad R_\varphi \to \begin{pmatrix} e^{iR\varphi} & 0 \\ 0 & e^{-iR\varphi} \end{pmatrix},$$

de sorte que é

$$\mathcal{U}_R \times \mathcal{U}_0^+ = \mathcal{U}_R\ .$$

Vê-se anàlogamente que se tem

$$\mathcal{U}_R \times \mathcal{U}_0^- = \mathcal{U}_R\ ,$$

para o que basta tomar a base $(u_R v_0^-\ ,\ -u_{-R} v_0^-)$.

Finalmente, suponhamos $k, j > 0$. Os vectores fundamentais do espaço produto são $u_R v_j$, $u_R v_{-j}$, $u_{-R} v_j$, $u_{-R} v_{-j}$, tendo-se

$$\begin{cases} S(u_k v_j) = u_{-k} v_{-j}, \\ S(u_k v_{-j}) = u_{-k} v_j, \end{cases} \qquad \begin{cases} S(u_{-k} v_j) = u_k v_{-j}, \\ S(u_{-k} v_{-j}) = u_k v_j. \end{cases}$$

Os vectores $u_k v_j$, $u_{-k} v_{-j}$ constituem um sub-espaço invariante:

$$\begin{cases} S(u_k v_j) = u_{-k} v_{-j}, \\ S(u_{-k} v_{-j}) = u_k v_j, \end{cases} \qquad \begin{cases} R_\varphi(u_k v_j) = u_k v_j e^{i(k+j)\varphi}, \\ R_\varphi(u_{-k} v_{-j}) = u_{-k} v_{-j} e^{-i(k+j)\varphi}. \end{cases}$$

A este sub-espaço corresponde a representação $\mathcal{U}_{k+j}$. Quanto aos vectores $u_k v_{-j}$, $u_{-k} v_j$, tem-se

$$\begin{cases} S(u_k v_{-j}) = u_{-k} v_j, \\ S(u_{-k} v_j) = u_k v_{-j}, \end{cases} \qquad \begin{cases} R_\varphi(u_k v_{-j}) = u_k v_{-j} e^{i(k-j)\varphi}, \\ R_\varphi(u_{-k} v_j) = u_{-k} v_j e^{-i(k-j)\varphi}. \end{cases}$$

Se for $k \neq j$, pode, pois, escrever-se (se $k > j$)

$$\mathcal{U}_k \times \mathcal{U}_j = \mathcal{U}_{k+j} + \mathcal{U}_{k-j}.$$

Mas, sendo $k = j$, os vectores $u_k v_{-k}$, $u_{-k} v_k$ ficam invariantes em face de R_φ, havendo mais do que um vector do tipo e_0. Os vectores $e_0 + Se_0$, $e_0 - Se_0$ são aqui

$$e_0 + Se_0 = u_k v_{-k} + u_{-k} v_k,$$

$$e_0 - Se_0 = u_k v_{-k} - u_{-k} v_k,$$

e levam a $\mathcal{U}_0^+$ e $\mathcal{U}_0^-$. É, pois,

$$\mathcal{U}_k \times \mathcal{U}_k = \mathcal{U}_{2k} + \mathcal{U}_0^+ + \mathcal{U}_0^-.$$

Resolvido o problema, passemos a outras indicações e exemplos.

Entre as representações figura sempre a representação idêntica, que se decompõe em representações idênticas do 1º grau irredutíveis. Se o grupo finito $\mathcal{G}$ é abeliano, as representações irredutíveis são do 1º grau. Se não é abeliano, pode haver representações irredutíveis do 1º grau ou de grau superior. As do 1º grau não são fiéis, pois que dois elementos diferentes $\underline{ab}$ e $\underline{ba}$, produtos de $\underline{a}$ e de $\underline{b}$, pertencentes a $\mathcal{G}$, têm a mesma matriz representante. O comutador $C = ab(ba)^{-1}$, de $\underline{a}$ e $\underline{b}$, que é diferente do elemento um, tem a unidade como representante, o mesmo sucedendo a qualquer elemento do grupo comutador. A representação do 1º grau, em causa, será uma representação fiel dum grupo factor abeliano $\mathcal{G}/\mathcal{H}$, onde $\mathcal{H}$ é um divisor normal que contém o grupo comutador e é composto de todos os elementos de $\mathcal{G}$ aos quais corresponde a unidade. $\mathcal{H}$ é, de resto, um divisor normal autêntico, dado que a representação é diferente da representação idêntica.

Tomemos o grupo simétrico $\mathcal{S}_n$. Em toda a representação do 1º grau, o grupo alterno é representado pela unidade, pois é gerado pelos ciclos de tres elementos e tais ciclos podem sempre considerar-se como comutadores:

$$(abc) = (ab)(abc)(ab)^{-1}(abc)^{-1}.$$

Como entre $\mathcal{S}_n$ e o grupo alterno $\mathcal{A}_n$ não há divisor normal, o divisor normal $\mathcal{H}$ a que acima se aludiu ou é igual a $\mathcal{A}_n$ ou a $\mathcal{S}_n$. Se se tem $\mathcal{H} = \mathcal{A}_n$, a representação do 1º grau faz corresponder a unidade a todos os elementos de $\mathcal{A}_n$, e um mesmo elemento, -1, a todas as permutações ímpares. É uma representação <u>anti-simétrica</u> de $\mathcal{S}_n$. Se, pelo contrário, se tem $\mathcal{H} = \mathcal{S}_n$, a representação é a representação idêntica ou <u>simétrica</u> de $\mathcal{S}_n$.

Estudemos agora as representações irredutíveis do grupo alterno $\mathcal{A}_4$. Como há 4 classes de elementos conjugados, de representantes (1), (123), (132), (12).(34), há 4 representações irredutíveis. Os graus satisfazem à relação

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 = 12.$$

Uma representação do grupo abeliano de 3 elementos, $\mathcal{U}' = \mathcal{U}_4/\mathcal{H}_4$,

onde $\mathfrak{V}_4$ é o grupo de 4 elementos de Kleín, é uma representação de $\mathcal{A}_4$. Ora $\mathcal{A}'$ tem 3 representações irredutíveis do 1º grau, pelo que deverá ser

$$n_1 = n_2 = n_3 = 1, \qquad n_4 = 3 .$$

Daqui o

Teorema:- O grupo alterno $\mathcal{A}_4$ tem 3 representações irredutíveis do 1º grau e uma do 3º.

Passemos ao estudo das representações do grupo simétrico $\mathcal{S}_4$. Há 5 classes de elementos conjugados, de representantes (1), (12), (123), (12).(34), (1234), e, portanto, 5 representações irredutíveis. Os graus satisfazem a

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = 24 .$$

O grupo $\mathcal{S}_4/\mathcal{A}_4$ é um grupo cíclico de 2ª ordem, pelo que podemos supor $n_1 = n_2 = 1$. O grupo de Kleín é divisor normal de $\mathcal{S}_4$, tendo-se, aliás, $\mathcal{S}_3 \cong \mathcal{S}_4/\mathfrak{V}_4$. Entre as representações de $\mathcal{S}_4$ figuram, pois, as de $\mathcal{S}_3$. Como este último tem 3 classes de elementos conjugados, de representantes (1), (12), (123), e como tem duas representações do 1º grau, a igualdade $1 + 1 + x^2 = 6$, dá $x = 2$. Podemos supor, assim, $n_3 = 2$, vindo

$$n_4^2 + n_5^2 = 18 ,$$

o que dá $n_4 = n_5 = 3$. Daqui se conclui o

Teorema:- O grupo $\mathcal{S}_4$ tem duas representações irredutíveis do 1º grau, uma do 2º grau e duas do 3º grau.

Para encontrar as últimas, pode proceder-se do modo que vai ver-se. Seja um espaço a 4 dimensões, de base (e_1, e_2, e_3, e_4). Façamos corresponder a cada elemento de $\mathcal{S}_4$ a matriz determinada pela permutação dos e_i, definida por esse elemento. Por-se-á, por ex.,

$$(12)e_1 = e_2 , \quad (13)e_1 = e_3 , \ldots$$

$$(123)e_1 = e_2 , \quad (123)e_2 = e_3 , \ldots$$

$$(12)(34)e_1 = e_2 , \quad (12)(34)e_3 = e_4 , \text{ etc.} .$$

O espaço em questão pode representar-se na base

$$e_1 - e_2 , \; e_2 - e_3 , \; e_3 - e_4 , \; e_4 ,$$

pois tem-se

$$e_1 = (e_1 - e_2) + (e_2 - e_3) + (e_3 - e_4) + e_4 ,$$

$$e_2 = (e_2 - e_3) + (e_3 - e_4) + e_4 ,$$

$$e_3 = (e_3 - e_4) + e_4 ,$$

$$e_4 = e_4 .$$

Ora é fácil de verificar que o sub-espaço $\mathcal{R}'$ definido pelos vectores $e_1 - e_2$, $e_2 - e_3$, $e_3 - e_4$ é invariante. Por ex.:

$$(123)(e_1 - e_2) = e_2 - e_3 ,$$

$$(123)(e_2 - e_3) = e_3 - e_1 = -(e_1 - e_2) - (e_2 - e_3) ,$$

$$(123)(e_3 - e_4) = e_1 - e_4 = (e_1 - e_2) + (e_2 - e_3) + (e_3 - e_4) .$$

Pode igualmente ver-se que $\mathcal{R}'$ não tem sub-espaço invariante. Isto significa que não há dois vectores

$$v_1 = \alpha(e_1 - e_2) + \beta(e_2 - e_3) + \gamma(e_3 - e_4) ,$$

$$v_2 = \alpha'(e_1 - e_2) + \beta'(e_2 - e_3) + \gamma'(e_3 - e_4) ,$$

tais que a aplicação de todos os elementos de $\mathcal{S}_4$ aos mesmos vectores leve a vectores exprimíveis neles. A esta conclusão se

chega notando que a representação definida pelo espaço $\mathcal{K}'$ é fiel. Se a representação de 3ª ordem se decompuzesse numa de 1ª e noutra de 2ª ordem, por ex., as matrizes diferentes só poderiam ser 12 e não 24.

Tomando em $\mathcal{K}'$ os vectores fundamentais

$$E_1 = 3\tau(e_1 - e_2) + 2\tau(e_2 - e_3) + \tau(e_3 - e_4) ,$$

$$E_2 = -\tau(e_1 - e_2) + 2\tau(e_2 - e_3) + \tau(e_3 - e_4) ,$$

$$E_3 = -\tau(e_1 - e_2) - 2\tau(e_2 - e_3) + \tau(e_3 - e_4) ,$$

onde $\tau \neq 0$, as matrizes transformam-se segundo a lei seguinte, escrita para as representantes de (12) e (14):

$$\begin{pmatrix} \frac{1}{4\tau} & 0 & \frac{1}{4\tau} \\ -\frac{1}{4\tau} & \frac{1}{4\tau} & \frac{1}{4\tau} \\ 0 & -\frac{1}{4\tau} & \frac{1}{2\tau} \end{pmatrix} \cdot \begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3\tau & -\tau & -\tau \\ 2\tau & 2\tau & -2\tau \\ \tau & \tau & \tau \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix};$$

$$\begin{pmatrix} \frac{1}{4\tau} & 0 & \frac{1}{4\tau} \\ -\frac{1}{4\tau} & \frac{1}{4\tau} & \frac{1}{4\tau} \\ 0 & -\frac{1}{4\tau} & \frac{1}{2\tau} \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & -1 \\ -1 & 1 & -1 \\ -1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3\tau & -\tau & -\tau \\ 2\tau & 2\tau & -2\tau \\ \tau & \tau & \tau \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}.$$

Pode verificar-se que as novas matrizes obtidas podiam determinar-se raciocinando como vai seguir-se: tomam-se um espaço (E_1, E_2, E_3) e um quarto vector $E_4 = -E_1 - E_2 - E_3$ deste espaço e constroem-se as matrizes correspondentes a cada elemento de $\mathcal{G}_4$ operando sobre os vectores E_1, E_2, E_3 como indica o próprio elemento, tendo o cuidado de substituir, no resultado, E_4 por $-E_1 - E_2 - E_3$. Por ex.:

$$(14)\ E_1 = -E_1 - E_2 - E_3, \quad (14)\ E_2 = E_2, \quad (14)\ E_3 = E_3 ,$$

$$(123)\ E_1 = E_2 , \quad (123)\ E_2 = E_3 , \quad (123)\ E_3 = E_1 .$$

Se, na representação irredutível do 3º grau que acabamos de estudar, trocarmos o sinal a todos os elementos das matrizes que são representantes das permutações ímpares e mantivermos as matrizes correspondentes às permutações pares, obtém-se um novo grupo de matrizes que é a outra representação fiel irredutível do 3º grau de $\mathcal{G}_4$.

Para completarmos o nosso objectivo, apenas resta encontrar a representação irredutível do 2º grau de $\mathcal{G}_3$. Consideremos o espaço $\mathcal{K}_3(e_1, e_2, e_3)$, no qual, como anteriormente, os elementos de $\mathcal{G}_3$ induzem as transformações lineares que eles próprios indicam. O vector $\varepsilon = e_1 + e_2 + e_3$ define, é claro, um sub-espaço invariante. Se tomarmos o sub-espaço $\mathcal{K}'_2(e_1 - e_2, e_2 - e_3)$, este é igualmente invariante. Em $\mathcal{K}'_2$ não há sub-espaço invariante, como se mostra ainda com o facto de ser fiel a representação pertencente a $\mathcal{K}'_2$. Na verdade, tem-se a seguinte correspondência, que dá a representação desejada:

$$(1) \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (12) \to \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad (13) \to \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix},$$

$$(23) \to \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \quad (123) \to \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \quad (132) \to \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}.$$

12) Sobre as representações irredutíveis dos grupos abelianos finitos - Como exemplo interessante, vemos tratar ainda o das representações do 1º grau dos grupos abelianos finitos. Dado um tal grupo $\mathcal{G}$, de N elementos, sabemos que existe uma base composta de s elementos $a_1, \ldots, a_s$, tais que cada elemento

$b \in \mathcal{G}$ é da forma[1]

$$b = a_1^{\rho_1} \dots a_s^{\rho_s} \quad , \qquad (1 \leqslant \rho_i \leqslant N_i), \qquad N_1 \dots N_s = N \ .$$

O elemento a_i gera um grupo cíclico de ordem N_i. Numa representação irredutível de $\mathcal{G}$, tem-se uma correspondência homomorfa $b \rightarrow \chi(b)$, segundo a qual a cada elemento corresponde um número. Essa correspondência verifica as relações

$$\chi(bc) = \chi(b).\ \chi(c), \qquad \chi(u) = 1 \ ,$$
$$\left(\chi(a_1)\right)^{N_1} = \dots = \left(\chi(a_s)\right)^{N_s} = 1 \ ,$$
$$\chi(b) = \left(\chi(a_1)\right)^{\rho_1} \dots \left(\chi(a_s)\right)^{\rho_s} .$$

Duma maneira precisa, pôr-se-á

$$\chi(a_j) = e^{\frac{2i\pi k}{N_j}} \quad , \qquad \begin{cases} k = 0, 1, \dots, N_j - 1 \ , \\ j = 1, 2, \dots, s \ . \end{cases}$$

A função $\chi(b)$ é aqui um caracter de $\mathcal{G}$, o que justifica o uso da letra χ.

Teorema:- Os caracteres de $\mathcal{G}$ constituem um grupo $\mathcal{G}$. Os caracteres são em número de N, tantos quantas as classes de elementos conjugados de $\mathcal{G}$ ou os elementos de $\mathcal{G}$. O produto de 2 caracteres $\chi_1(b)$, $\chi_2(b)$ define, de facto, uma correspondência

$$b \rightarrow \chi_1 \chi_2(b) = \chi_1(b).\ \chi_2(b) = \chi(b) \ ,$$

pois

$$bc \rightarrow \chi_1(bc).\ \chi_2(bc) = \chi_1(b)\ \chi_2(b).\ \chi_1(c)\ \chi_2(c) = \chi_1\chi_2(b).\ \chi_1\chi_2(c).$$

(1) Elementos da Teoria dos Grupos, pgs.88 e seguintes.

O inverso dum caracter é um caracter, visto que

$$b \rightarrow \frac{1}{\chi(b)} = \chi^{-1}(b) \ , \quad bc \rightarrow \frac{1}{\chi(bc)} = \frac{1}{\chi(b)} \cdot \frac{1}{\chi(c)} = \chi^{-1}(b)\chi^{-1}(c).$$

É costume pôr $\chi^{-1}(b) = \overline{\chi}(b)$, pelo facto de ser $\chi^{-1}(b)$ complexo conjugado de $\chi(b)$. O grupo $\mathcal{G}$ dos caracteres é abeliano.

Posto isto, seja η_j uma raiz primitiva de ordem N_j da unidade. Um caracter χ é, por ex., o seguinte:

$$a_j \rightarrow \chi_j(a_j) = \eta_j \ , \qquad a_k \rightarrow \chi_j(a_k) = 1 \ , \qquad \text{se } k \neq j \ .$$

χ_j gera no grupo dos caracteres um sub-grupo cíclico de ordem N_j, $\mathcal{G}_j$. O grupo $\mathcal{G}$ é o produto directo

$$\mathcal{G} = \mathcal{G}_1 \times \dots \times \mathcal{G}_s ,$$

pelo que tem lugar o seguinte

Teorema:- O grupo dos caracteres é isomorfo do grupo dado.

Como exemplo dum elemento do produto $\mathcal{G}_1 \times \mathcal{G}_2$, podemos dar o caracter que determina as seguintes correspondências:

$$a_1 \rightarrow \eta_1^{\rho_1} \ , \qquad a_2 \rightarrow \eta_2^{\rho_2} \ , \qquad a_i \rightarrow 1 \ , \qquad \text{se } i \neq 1, 2.$$

Voltemos agora a considerar as igualdades

$$\chi_1\chi_2(b) = \chi_1(b).\ \chi_2(b) \ ,$$
$$\chi(bc) = \chi(b).\ \chi(c) \ ,$$

na primeira das quais figuram um elemento de $\mathcal{G}$, dois elementos de $\mathcal{G}$ e o produto destes, enquanto que na segunda figuram um elemento de $\mathcal{G}$, dois elementos de $\mathcal{G}$ e o produto destes. As duas igualdades têm carácter de reciprocidade, no sentido seguinte: se, em $\chi(b)$, χ é fixo e b varia, obtém-se uma certa função

de $\underline{b}$; se $\underline{b}$ é fixo e $\underline{x}$ varia, obtém-se uma função de x, para a qual se tem

$$x_1 x_2(b) = x_1(b) \cdot x_2(b) .$$

Isto mostra que $\underline{b}$ define uma homomorfia de $\mathcal{G}$ sobre o corpo dos números complexos, ou seja uma representação de $\mathcal{G}$. Dois elementos diferentes de $\mathcal{G}$ definem homomorfismos diferentes, pois que, supondo

$$b = a_1^{\lambda_1} \cdots a_s^{\lambda_s}, \qquad c = a_1^{\mu_1} \cdots a_s^{\mu_s}, \quad \text{com } \lambda_t \neq \mu_t ,$$

vem imediatamente

$$x_t(b) = \eta_t^{\lambda_t}, \qquad x_t(c) = \eta_t^{\mu_t}, \qquad x_t(b) \neq x_t(c) .$$

Podemos enunciar o

Teorema:- O grupo dos caracteres de $\mathcal{G}$ é o grupo $\mathcal{G}$.

Passemos às relações de ortogonalidade dos caracteres. Comecemos por formar a expressão $\sum_b x(b)$. Tem-se

$$x(b) = x(a_1)^{\rho_1} \cdots x(a_s)^{\rho_s} = e^{\rho_1 \cdot \frac{2i\pi k_1}{N_1}} \cdots e^{\rho_s \cdot \frac{2i\pi k_s}{N_s}} ,$$

$$\sum_b x(b) = \sum_{\rho_1, \cdots, \rho_s} e^{\rho_1 \cdot \frac{2i\pi k_1}{N_1}} \cdots e^{\rho_s \frac{2i\pi k_s}{N_s}} = \left(\sum_{\rho_1} e^{\rho_1 \cdot \frac{2i\pi k_1}{N_1}} \right) \cdots \left(\sum_{\rho_s} e^{\rho_s \cdot \frac{2i\pi k_s}{N_s}} \right) =$$

$$= \begin{cases} N_1 \cdots N_s = N, \text{ se todos os } k_j \text{ são iguais aos } N_j; \\ 0 , \text{ se um } k_j \text{ é diferente de } N_j; \end{cases}$$

visto que, por ex., supondo $k_1 \neq N_1$, é

$$e^{\frac{2i\pi k_1}{N_1}} + e^{\frac{2i\pi k_1 \cdot 2}{N_1}} + \cdots + e^{\frac{2i\pi k_1 \cdot N_1}{N_1}} = \frac{e^{2i\pi k_1} \cdot e^{\frac{2i\pi k_1}{N_1}} - e^{\frac{2i\pi k_1}{N_1}}}{e^{\frac{2i\pi k_1}{N_1}} - 1} = 0 .$$

Em resumo é

$$\sum_b x(b) = \begin{cases} N , \text{ quando } x = x_0, \text{ onde } x_0 \text{ é o } \underline{\text{caracter principal}}, \text{ correspondente à representação idêntica;} \\ 0 , \text{ quando } x \neq x_0 . \end{cases}$$

O comportamento recíproco de $\mathcal{G}$ e de $\mathcal{G}$ permite que se escreva

$$\sum_x x(b) = \begin{cases} N , \text{ se } b = u = \text{elemento um de } \mathcal{G} ; \\ 0 , \text{ se } b \neq u . \end{cases}$$

Substituindo aqui $\underline{b}$ por um produto $\underline{cd}$, vem

$$\sum_x x(c)\, x(d) = \begin{cases} N , \text{ se } d = c^{-1} , \\ 0 , \text{ se } d \neq c^{-1} , \end{cases}$$

e, por consequência,

$$\sum_b x_1(b)\, x_2(b) = \begin{cases} N , \text{ se } x_2 = \overline{x}_1 , \\ 0 , \text{ se } x_2 \neq \overline{x}_1 . \end{cases} \qquad (16')$$

Tendo em conta que é $x(b^{-1}) = \overline{x}(b)$, pode escrever-se

$$\sum_x x(c)\, \overline{x}(d^{-1}) = \begin{cases} N , \text{ se } d = c^{-1} (\text{ou } d^{-1} = c), \\ 0 , \text{ se } d^{-1} \neq c , \end{cases}$$

ou ainda

$$\sum_x x(c)\, \overline{x}(d) = \begin{cases} N, \text{ se } d = c , \\ 0 , \text{ se } d \neq c . \end{cases} \qquad (17)$$

Anàlogamente, tem-se, a partir de (16'),

$$\sum_b \chi_1(b)\,\overline{\chi}_2(b^{-1}) = \begin{cases} N\,, & \text{se } \chi_2 = \overline{\chi}_1 \ (\text{ou } \overline{\chi}_2 = \chi_1)\,, \\ 0\,, & \text{se } \overline{\chi}_2 \neq \chi_1\,, \end{cases}$$

$$\sum_b \chi_1(b)\ \chi_2(b^{-1}) = \begin{cases} N\,, & \text{se } \chi_2 = \chi_1\,, \\ 0\,, & \text{se } \chi_2 \neq \chi_1\,, \end{cases}$$

ou, finalmente,

$$\sum_b \chi_1(b)\,\overline{\chi}_2(b) = \begin{cases} N\,, & \text{se } \chi_2 = \chi_1\,, \\ 0\,, & \text{se } \chi_2 \neq \chi_1\,. \end{cases} \tag{18}$$

As relações (17) e (18) são as relações de ortogonalidade que tínhamos em vista.(1) As últimas poderiam escrever-se imediatamente a partir de (12).

Consideremos as matrizes quadradas de grau N

$$A = \begin{pmatrix} \chi_1(u) & \chi_1(a) & \chi_1(b) & \cdots \\ \chi_2(u) & \chi_2(a) & \chi_2(b) & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix}, \quad B = \begin{pmatrix} \overline{\chi}_1(u) & \overline{\chi}_1(a) & \overline{\chi}_1(b) & \cdots \\ \overline{\chi}_2(u) & \overline{\chi}_2(a) & \overline{\chi}_2(b) & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix}$$

e as suas transpostas

$$\tilde{A} = \begin{pmatrix} \chi_1(u) & \chi_2(u) & \cdots \\ \chi_1(a) & \chi_2(a) & \cdots \\ \chi_1(b) & \chi_2(b) & \cdots \\ \cdots & \cdots & \cdots \end{pmatrix}, \qquad \tilde{B} = \begin{pmatrix} \overline{\chi}_1(u) & \overline{\chi}_2(u) & \cdots \\ \overline{\chi}_1(a) & \overline{\chi}_2(a) & \cdots \\ \overline{\chi}_1(b) & \overline{\chi}_2(b) & \cdots \\ \cdots & \cdots & \cdots \end{pmatrix}.$$

As igualdades (17) e (18) mostram que é

$$\tilde{A}B = A\tilde{B} = U.N = \text{matriz unidade} \times N.$$

(1) Deduzidas conforme B.L. van der Waerden, "Moderne Algebra" II Teil, Berlin, 1931, pgs. 189 a 192.

13) O grupo das rotações do espaço ordinário e o grupo unitário especial. Seja o espaço $(\overset{1}{u}, \overset{2}{u})$ a duas dimensões. Diz-se grupo linear especial, L_2, o grupo das transformações lineares

$$\begin{cases} \overset{1}{u}' = \overset{1}{u}\,\alpha + \overset{2}{u}\,\tau\,, \\ \overset{2}{u}' = \overset{1}{u}\,\beta + \overset{2}{u}\,\delta\,, \end{cases} \qquad \text{com} \quad \alpha\delta - \beta\tau = 1\,. \tag{18'}$$

Os coeficientes $\alpha, \tau, \beta, \delta$ são números complexos. Um vector $u = \overset{1}{u}\,\xi_1 + \overset{2}{u}\,\xi_2$ transforma-se num vector $u' = \overset{1}{u}'\xi_1 + \overset{2}{u}'\xi_2 = \overset{1}{u}\,\xi_1' + \overset{2}{u}\,\xi_2'$, com

$$\begin{cases} \xi_1' = \alpha\,\xi_1 + \beta\,\xi_2\,, \\ \xi_2' = \tau\,\xi_1 + \delta\,\xi_2\,. \end{cases} \tag{19}$$

Neste § interessam especialmente as transformações lineares da forma

$$\begin{cases} \overset{1}{u}' = \overset{1}{u}\,\alpha - \overset{2}{u}\,\overline{\beta}\,, \\ \overset{2}{u}' = \overset{1}{u}\,\beta + \overset{2}{u}\,\overline{\alpha}\,, \end{cases} \qquad \alpha\overline{\alpha} + \beta\overline{\beta} = 1\,, \tag{20}$$

que constituem um sub-grupo de L_2, chamado o grupo unitário especial U_2. De facto, pondo

$$\begin{cases} \overset{1}{u}'' = \overset{1}{u}'a - \overset{2}{u}'\overline{b}\,, \\ \overset{2}{u}'' = \overset{1}{u}'b + \overset{2}{u}'\overline{a}\,, \end{cases} \qquad a\overline{a} + b\overline{b} = 1\,,$$

tem-se fàcilmente

$$\begin{cases} \overset{1}{u}'' = \overset{1}{u}(\alpha a - \beta\overline{b}) - \overset{2}{u}\,(\overline{\beta}\,a + \overline{\alpha}\,\overline{b})\,, \\ \overset{2}{u}'' = \overset{1}{u}(\alpha b + \beta\overline{a}) + \overset{2}{u}\,(-\overline{\beta}\,b + \overline{\alpha}\,\overline{a})\,. \end{cases}$$

O determinante desta transformação é a unidade e a disposição dos coeficientes obedece à regra indicada em (20). Introduzindo no espaço a métrica hermiteana

$$G(u) = \bar{\xi}_1 \xi_1 + \bar{\xi}_2 \xi_2 ,$$

as transformações (20) são transformações métricas (unitárias). Procurando, de resto, as transformações de L_2 que conservam o produto escalar, chega-se a (20), como vamos ver. Deverá ser

$$\bar{\xi}'_1 \eta'_1 + \bar{\xi}'_2 \eta'_2 = (\bar{\alpha} \bar{\xi}_1 + \bar{\beta} \bar{\xi}_2)(\alpha \eta_1 + \beta \eta_2) + (\bar{\gamma} \bar{\xi}_1 + \bar{\delta} \bar{\xi}_2)(\gamma \eta_1 + \delta \eta_2) =$$

$$= \bar{\xi}_1 \eta_1 + \bar{\xi}_2 \eta_2 ,$$

o que leva a

$$\bar{\alpha}\alpha + \bar{\gamma}\gamma = 1 , \qquad \bar{\alpha}\beta + \bar{\gamma}\delta = 0 ,$$

$$\bar{\beta}\alpha + \bar{\delta}\gamma = 0 , \qquad \bar{\beta}\beta + \bar{\delta}\delta = 1 ,$$

ou seja a

$$\begin{pmatrix} \bar{\alpha} & \bar{\gamma} \\ \bar{\beta} & \bar{\delta} \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} .$$

Ora, tendo-se

$$\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} ,$$

concluem-se, como se deseja, as igualdades

$$\gamma = -\bar{\beta} , \qquad \delta = \bar{\alpha} .$$

A transformação dos $\xi\xi$ relativa a (20) é

$$\begin{cases} \xi'_1 = \alpha \xi_1 + \beta \xi_2 , \\ \xi'_2 = -\bar{\beta} \xi_1 + \bar{\alpha} \xi_2 . \end{cases}$$

Consideremos agora um vector V_0 do espaço ordinário com as componentes

$$a = \frac{\xi_1^2 - \xi_2^2}{2} , \quad b = i \frac{\xi_1^2 + \xi_2^2}{2} , \quad c = -\xi_1 \xi_2 . \tag{21}$$

É um vector isótropo, pois $V_0^2 = a^2 + b^2 + c^2 = 0$. Inversamente, as relações (21) permitem passar dum vector isótropo arbitrário aos valores ξ_1, ξ_2. Elas definem, porém, dois sistemas de valores, visto que é

$$\xi_1^2 = a - bi , \qquad \xi_2^2 = -a - bi .$$

Escolhido, por meio destas igualdades, um sistema ξ_1, ξ_2 que verifique a relação $\xi_1 \xi_2 = -c$, um segundo sistema obtém-se do anterior por troca de sinal.

Efectuemos uma rotação do espaço ordinário, à volta da origem, por meio da qual o sistema de referência inicial Oxyz se torna no sistema Ox'y'z'. O vector V_0 passa a ter as componentes

$$\begin{aligned} a' &= \alpha_{11} a + \alpha_{12} b + \alpha_{13} c , \\ b' &= \alpha_{21} a + \alpha_{22} b + \alpha_{23} c , \\ c' &= \alpha_{31} a + \alpha_{32} b + \alpha_{33} c . \end{aligned} \tag{21'}$$

Aos números a', b', c' estão ligados os números ξ'_1, ξ'_2 pelas relações

$$\xi_1'^2 = a' - b'i , \quad \xi_2'^2 = -a' - b'i , \quad \xi'_1 \xi'_2 = -c'$$

tendo-se, sucessivamente,

$$\xi_1'^2 = (\alpha_{11} - i\alpha_{21}) a + (\alpha_{12} - i\alpha_{22}) b + (\alpha_{13} - i\alpha_{23}) c =$$

$$= (\alpha_{11} - i\alpha_{21})\frac{\xi_1^2 - \xi_2^2}{2} + (\alpha_{12} - i\alpha_{22})i\frac{\xi_1^2 + \xi_2^2}{2} - (\alpha_{13} - i\alpha_{23})\xi_1\xi_2 =$$

$$= \frac{1}{2}\left[(\alpha_{11} - i\alpha_{21} + \alpha_{12}i + \alpha_{22})\xi_1^2 + (-\alpha_{11} + i\alpha_{21} + i\alpha_{12} + \alpha_{22})\xi_2^2 - \right.$$

$$\left. - (\alpha_{13} - i\alpha_{23})\xi_1\xi_2\right].$$

A forma quadrática em ξ_1, ξ_2 que figura no último membro tem o descriminante

$$(\alpha_{13} - i\alpha_{23})^2 - \left[(\alpha_{11} - i\alpha_{21}) + (\alpha_{12} - i\alpha_{22})i\right]\left[(\alpha_{12} - i\alpha_{22})i - \right.$$

$$\left. - (\alpha_{11} - i\alpha_{21})\right] = (\alpha_{13} - i\alpha_{23})^2 + \left((\alpha_{12} - i\alpha_{22})^2 + (\alpha_{11} - i\alpha_{21})^2\right) = 0.$$

Isto significa que $\xi_1'^2$ é um quadrado perfeito, o mesmo se dizendo de ξ_2'. Pondo, deste modo,

$$\begin{cases} \xi_1' = \alpha\xi_1 + \beta\xi_2 , \\ \xi_2' = \gamma\xi_1 + \delta\xi_2 , \end{cases} \qquad (22)$$

poder-se-iam escrever também as mesmas igualdades trocando o sinal a todos os coeficientes. Por meio de (22) calculam-se $\xi_1'^2$, $\xi_2'^2$, $\xi_1'\xi_2'$ expressos em ξ_1^2, ξ_2^2, $\xi_1\xi_2$ e determina-se o jacobiano

$$\Delta = \frac{D(\xi_1'^2, \xi_2'^2, \xi_1'\xi_2')}{D(\xi_1^2, \xi_2^2, \xi_1\xi_2)} = (\alpha\delta - \beta\gamma)^3.$$

Sendo, por outro lado,

$$\Delta = \frac{D(\xi_1'^2, \xi_2'^2, \xi_1'\xi_2')}{D(a', b', c')} \cdot \frac{D(a', b', c')}{D(a, b, c)} \cdot \frac{D(a, b, c)}{D(\xi_1^2, \xi_2^2, \xi_1\xi_2)} = 1 ,$$

conclui-se a relação $\alpha\delta - \beta\gamma = \sqrt[3]{1}$. Fazendo variar $Ox'y'z'$ de modo contínuo, a partir de $Oxyz$, $\alpha\delta - \beta\gamma$ conserva o valor

inicial, o qual é relativo à transformação

$$a' = a , \qquad b' = b , \qquad c' = c ,$$

$$\xi_1' = \pm\,\xi_1 , \qquad \xi_2' = \pm\,\xi_2 , \text{ (com correspondência dos sinais).}$$

Será, pois, $\alpha\delta - \beta\gamma = 1$. A transformação (22) é unitária, como vamos ver. Tem-se

$$\bar{a}a + \bar{b}b + \bar{c}c = \frac{\bar{\xi}_1^2 - \bar{\xi}_2^2}{2}\cdot\frac{\xi_1^2 - \xi_2^2}{2} - i\frac{\bar{\xi}_1^2 + \bar{\xi}_2^2}{2}\cdot i\frac{\xi_1^2 + \xi_2^2}{2} + \bar{\xi}_1\bar{\xi}_2\xi_1\xi_2 =$$

$$= \frac{1}{2}(\bar{\xi}_1\xi_1 + \bar{\xi}_2\xi_2)^2 ,$$

ou seja

$$\bar{\xi}_1\xi_1 + \bar{\xi}_2\xi_2 = \sqrt{2(\bar{a}a + \bar{b}b + \bar{c}c)} .$$

Mas, se pusermos

$$V_0 = (A + iA_1)I + (B + iB_1)J + (C + iC_1)K ,$$

onde I, J, K são os vectores base do espaço ordinário, vê-se que é

$$A^2 + B^2 + C^2 = A_1^2 + B_1^2 + C_1^2 ,$$

$$AA_1 + BB_1 + CC_1 = 0 ,$$

$$\bar{a}a + \bar{b}b + \bar{c}c = A^2 + B^2 + C^2 + A_1^2 + B_1^2 + C_1^2 = 2(A^2 + B^2 + C^2).$$

A expressão $\bar{a}a + \bar{b}b + \bar{c}c$ é invariante em face das rotações à volta da origem, tendo-se, como se quer,

$$\bar{\xi}_1\xi_1 + \bar{\xi}_2\xi_2 = \bar{\xi}_1'\xi_1' + \bar{\xi}_2'\xi_2' .$$

Os raciocínios feitos mostram que tem lugar o seguinte

Teorema:- A cada rotação (21'), à volta da origem, no espaço ordinário, correspondem duas transformações (22) do grupo unitário especial U_2, a saber:

$$\begin{cases} \xi_1' = \alpha\,\xi_1 + \beta\,\xi_2\,, \\ \xi_2' = -\bar\beta\,\xi_1 + \bar\alpha\,\xi_2\,, \end{cases} \qquad \begin{cases} \xi_1' = -\alpha\,\xi_1 - \beta\,\xi_2\,, \\ \xi_2' = \bar\beta\,\xi_1 - \bar\alpha\,\xi_2\,. \end{cases} \tag{23}$$

Representaremos com R o grupo das rotações à volta da origem. Suponhamos uma dessas rotações definida pelos ângulos de Euler, θ, φ, ψ. É fácil encontrar os coeficientes (23). Basta, para isso, considerar um vector isótropo particular, por ex.: $V_0 = I' + iJ'$. É, então, $a' = 1$, $b' = i$, $c' = 0$,

$$a = (\cos\psi\cos\varphi - \operatorname{sen}\psi\operatorname{sen}\varphi\cos\theta) + i(-\cos\psi\operatorname{sen}\varphi - \operatorname{sen}\psi\cos\varphi\cdot$$

$$\cdot\cos\theta) = (\cos\psi - i\cos\theta\operatorname{sen}\psi)e^{-i\varphi},$$

$$b = (\operatorname{sen}\psi + i\cos\theta\cos\psi)e^{-i\varphi}, \qquad c = i\operatorname{sen}\theta\, e^{-i\varphi},$$

$$\xi_1' = \sqrt{a' - b'i} = \pm\sqrt{2}\,, \qquad \xi_2' = 0\,,$$

$$\xi_1 = \sqrt{a - bi} = \pm\sqrt{2}\cos\frac{\theta}{2}\,e^{-i\frac{\varphi+\psi}{2}}, \quad \xi_2 = \sqrt{-a - bi} = \mp i\sqrt{2}\operatorname{sen}\frac{\theta}{2}e^{-i\frac{\varphi-\psi}{2}},$$

e, portanto,

$$\xi_1' = \cos\frac{\theta}{2}\,e^{i\frac{\varphi+\psi}{2}}\cdot\xi_1 + i\operatorname{sen}\frac{\theta}{2}\,e^{i\frac{\varphi-\psi}{2}}\cdot\xi_2,$$

$$\xi_2' = i\operatorname{sen}\frac{\theta}{2}\,e^{-i\frac{\varphi-\psi}{2}}\cdot\xi_1 + \cos\frac{\theta}{2}\,e^{-i\frac{\varphi+\psi}{2}}\cdot\xi_2,$$

donde se conclui

$$\alpha = \cos\frac{\theta}{2}\,e^{i\frac{\varphi+\psi}{2}}\,, \qquad \beta = i\operatorname{sen}\frac{\theta}{2}\,e^{i\frac{\varphi-\psi}{2}}\,. \tag{24}$$

Para se ver que, numa transformação unitária de U_2, α e β têm sempre o aspecto anterior, notemos que a relação

$$\alpha\bar\alpha + \beta\bar\beta = 1$$

mostra serem $|\alpha|\,,\ |\beta| \leqslant 1$, e que, portanto, se pode escrever

$$\alpha = \cos\frac{\theta}{2}\cdot e^{i\sigma}, \qquad (0 \leqslant \theta \leqslant \pi)\,,$$

o que dá

$$\beta\bar\beta = 1 - \cos^2\frac{\theta}{2} = \operatorname{sen}^2\frac{\theta}{2}\,, \qquad |\beta| = \operatorname{sen}\frac{\theta}{2}\,.$$

Daqui se conclui valerem relações como as seguintes:

$$\alpha = \cos\frac{\theta}{2}\,e^{i\sigma}\,, \qquad \beta = i\operatorname{sen}\frac{\theta}{2}\,e^{i\tau}\,.$$

Fazendo, depois;

$$\begin{cases} \varphi = \sigma + \tau\,, \\ \psi = \sigma - \tau\,, \end{cases} \quad \text{ou} \quad \begin{cases} \sigma = \dfrac{\varphi+\psi}{2}\,, \\ \tau = \dfrac{\varphi-\psi}{2}\,, \end{cases}$$

obtém-se a forma desejada. O teorema anterior tem o seguinte

Complemento:- Na correspondência que leva de R a elementos de U_2, reencontram-se todos os elementos de U_2.

Escrevendo, ao lado de (24), as relações

$$-\alpha = \cos\frac{\theta}{2}\,e^{i\frac{(\varphi+2\pi)+\psi}{2}} = \cos\frac{\theta}{2}\,e^{i\frac{\varphi+(\psi+2\pi)}{2}},$$

$$-\beta = i\operatorname{sen}\frac{\theta}{2}\,e^{i\frac{(\varphi+2\pi)-\psi}{2}} = i\operatorname{sen}\frac{\theta}{2}\,e^{i\frac{\varphi-(\psi+2\pi)}{2}},$$

vê-se quais as duas transformações (23) correspondentes a ângulos de Euler dados.

Teorema:- O grupo R dá uma representação uniforme do grupo U_2, e, inversamente, U_2 dá uma representação biforme de R. A demonstração é consequência de se provar que os ângulos de Euler, Θ, Φ, Ψ, correspondentes à transformação de U_2 resultante do produto de duas transformações de U_2, são os ângulos de Euler relativos à rotação do espaço ordinário que é o produto das duas rotações correspondentes àquelas duas transformações de U_2. Ponhamos

$$\begin{cases} \xi_1' = \alpha\,\xi_1 + \beta\,\xi_2, \\ \xi_2' = -\bar{\beta}\,\xi_1 + \bar{\alpha}\,\xi_2, \end{cases} \qquad \begin{cases} \xi_1'' = \alpha_1\,\xi_1' + \beta_1\,\xi_2', \\ \xi_2'' = -\bar{\beta}_1\,\xi_1' + \bar{\alpha}_1\,\xi_2' \end{cases}$$

$$\begin{cases} \xi_1'' = (\alpha_1\alpha - \beta_1\bar{\beta})\,\xi_1 + (\alpha_1\beta + \beta_1\bar{\alpha})\,\xi_2, \\ \xi_2'' = (-\bar{\beta}_1\alpha - \bar{\alpha}_1\bar{\beta})\,\xi_1 + (-\bar{\beta}_1\beta + \bar{\alpha}_1\bar{\alpha})\,\xi_2, \end{cases}$$

$$\alpha_1\alpha - \beta_1\bar{\beta} = \cos\frac{\Theta_1}{2}e^{i\frac{\varphi_1+\psi_1}{2}}\cdot\cos\frac{\Theta}{2}e^{i\frac{\varphi+\psi}{2}} - i\,\operatorname{sen}\frac{\Theta_1}{2}e^{i\frac{\varphi_1-\psi_1}{2}}\left(-i\,\operatorname{sen}\frac{\Theta}{2}\right)e^{-i\frac{\varphi-\psi}{2}} =$$

$$= \cos\frac{\Omega}{2}e^{i\frac{\Phi+\Psi}{2}}, \qquad (25)$$

$$\alpha_1\beta + \beta_1\bar{\alpha} = \cos\frac{\Theta_1}{2}e^{i\frac{\varphi_1+\psi_1}{2}}\cdot i\,\operatorname{sen}\frac{\Theta}{2}e^{i\frac{\varphi-\psi}{2}} + i\,\operatorname{sen}\frac{\Theta_1}{2}e^{i\frac{\varphi_1-\psi_1}{2}}\cos\frac{\Theta}{2}e^{-i\frac{\varphi+\psi}{2}} =$$

$$= i\,\operatorname{sen}\frac{\Omega}{2}e^{i\frac{\Phi-\Psi}{2}}. \qquad (26)$$

De (25) tira-se

$$\cos\frac{\Theta_1}{2}\cos\frac{\Theta}{2}\left[\cos\frac{\varphi_1+\psi_1}{2} + i\,\operatorname{sen}\frac{\varphi_1+\psi_1}{2}\right]\left[\cos\frac{\varphi+\psi}{2} + i\,\operatorname{sen}\frac{\varphi+\psi}{2}\right] -$$

$$- \operatorname{sen}\frac{\Theta_1}{2}\operatorname{sen}\frac{\Theta}{2}\left[\cos\frac{\varphi_1-\psi_1}{2} + i\,\operatorname{sen}\frac{\varphi_1-\psi_1}{2}\right]\left[\cos\frac{\varphi-\psi}{2} - i\,\operatorname{sen}\frac{\varphi-\psi}{2}\right] =$$

$$= \cos\frac{\Theta_1}{2}\cos\frac{\Theta}{2}\cos\left(\frac{\varphi_1+\varphi}{2} + \frac{\psi_1+\psi}{2}\right) - \operatorname{sen}\frac{\Theta_1}{2}\operatorname{sen}\frac{\Theta}{2}\cos\left(\frac{\varphi_1-\varphi}{2} - \frac{\psi_1-\psi}{2}\right) +$$

$$+ i\left[\cos\frac{\Theta_1}{2}\cos\frac{\Theta}{2}\operatorname{sen}\left(\frac{\varphi_1+\varphi}{2} + \frac{\psi_1+\psi}{2}\right) - \operatorname{sen}\frac{\Theta_1}{2}\operatorname{sen}\frac{\Theta}{2}\operatorname{sen}\left(\frac{\varphi_1-\varphi}{2} - \frac{\psi_1-\psi}{2}\right)\right] =$$

$$= \cos\frac{\Omega}{2}\cos\frac{\Phi+\Psi}{2} + i\cos\frac{\Omega}{2}\operatorname{sen}\frac{\Phi+\Psi}{2},$$

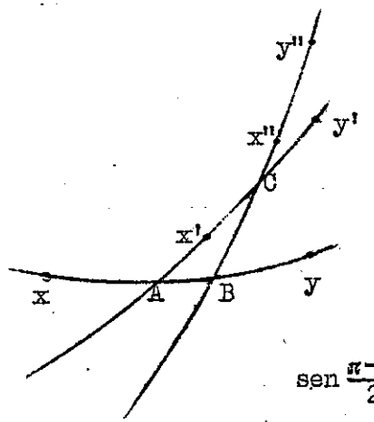
e, portanto,

$$\begin{cases} \cos\frac{\Omega}{2}\cos\frac{\Phi+\Psi}{2} = \cos\frac{\Theta_1}{2}\cos\frac{\Theta}{2}\cos\left(\frac{\varphi_1+\varphi}{2} + \frac{\psi_1+\psi}{2}\right) - \operatorname{sen}\frac{\Theta_1}{2}\operatorname{sen}\frac{\Theta}{2}\cdot \\ \qquad\qquad \cdot\cos\left(\frac{\varphi_1-\varphi}{2} - \frac{\psi_1-\psi}{2}\right), \\ \cos\frac{\Omega}{2}\operatorname{sen}\frac{\Phi+\Psi}{2} = \cos\frac{\Theta_1}{2}\cos\frac{\Theta}{2}\operatorname{sen}\left(\frac{\varphi_1+\varphi}{2} + \frac{\psi_1+\psi}{2}\right) - \operatorname{sen}\frac{\Theta_1}{2}\operatorname{sen}\frac{\Theta}{2}\cdot \\ \qquad\qquad \cdot\operatorname{sen}\left(\frac{\varphi_1-\varphi}{2} - \frac{\psi_1-\psi}{2}\right). \end{cases} \qquad (27)$$

De (26) concluem-se anàlogamente as igualdades

$$\begin{cases} \operatorname{sen}\frac{\Omega}{2}\cos\frac{\Phi-\Psi}{2} = \cos\frac{\Theta_1}{2}\operatorname{sen}\frac{\Theta}{2}\cos\left(\frac{\varphi_1+\varphi}{2} + \frac{\psi_1-\psi}{2}\right) + \operatorname{sen}\frac{\Theta_1}{2}\cos\frac{\Theta}{2}\cdot \\ \qquad\qquad \cdot\cos\left(\frac{\varphi_1-\varphi}{2} - \frac{\psi_1+\psi}{2}\right), \\ \operatorname{sen}\frac{\Omega}{2}\operatorname{sen}\frac{\Phi-\Psi}{2} = \cos\frac{\Theta_1}{2}\operatorname{sen}\frac{\Theta}{2}\operatorname{sen}\left(\frac{\varphi_1+\varphi}{2} + \frac{\psi_1-\psi}{2}\right) + \operatorname{sen}\frac{\Theta_1}{2}\cos\frac{\Theta}{2}\cdot \\ \qquad\qquad \cdot\operatorname{sen}\left(\frac{\varphi_1-\varphi}{2} - \frac{\psi_1+\psi}{2}\right). \end{cases} \qquad (28)$$

As relações (27) e (28) determinam completamente Θ, φ, Ψ. Ora, na figura junta, deve tomar-se:



$\theta = y\hat{A}y'$, $\psi = \widehat{xA}$, $\varphi = \widehat{Ax'}$,

$\theta_1 = y'\hat{C}y''$, $\psi_1 = \widehat{x'C}$, $\varphi_1 = \widehat{Cx''}$,

$\sim = y\hat{B}y''$, $\Psi = \widehat{xB}$, $\Phi = \widehat{Bx''}$.

As analogias de Delambre aplicadas ao triângulo esférico ABC são as seguintes:

$$\operatorname{sen}\frac{\pi-\sim}{2}\operatorname{sen}\frac{\Psi-\psi+\Phi-\varphi_1}{2} = \operatorname{sen}\frac{\varphi+\psi_1}{2}\cos\frac{\theta_1-\theta}{2},$$

$$\operatorname{sen}\frac{\pi-\sim}{2}\cos\frac{\Psi-\psi+\Phi-\varphi_1}{2} = \cos\frac{\varphi+\psi_1}{2}\cos\frac{\theta_1+\theta}{2},$$

$$\cos\frac{\pi-\sim}{2}\operatorname{sen}\frac{\Psi-\psi-\Phi+\varphi_1}{2} = \operatorname{sen}\frac{\varphi+\psi_1}{2}\operatorname{sen}\frac{\theta_1-\theta}{2},$$

$$\cos\frac{\pi-\sim}{2}\cos\frac{\Psi-\psi-\Phi+\varphi_1}{2} = \cos\frac{\varphi+\psi_1}{2}\operatorname{sen}\frac{\theta_1+\theta}{2}.$$

As duas primeiras, por ex., dão

$$\cos\frac{\sim}{2}\operatorname{sen}\frac{\Phi+\Psi}{2}\cos\frac{\psi+\varphi_1}{2} - \cos\frac{\sim}{2}\cos\frac{\Phi+\Psi}{2}\operatorname{sen}\frac{\psi+\varphi_1}{2} = \operatorname{sen}\frac{\varphi+\psi_1}{2}\cos\frac{\theta_1-\theta}{2},$$

$$\cos\frac{\sim}{2}\operatorname{sen}\frac{\Phi+\Psi}{2}\operatorname{sen}\frac{\psi+\varphi_1}{2} + \cos\frac{\sim}{2}\cos\frac{\Phi+\Psi}{2}\cos\frac{\psi+\varphi_1}{2} = \cos\frac{\varphi+\psi_1}{2}\cos\frac{\theta_1+\theta}{2}.$$

Multiplicando as relações anteriores respectivamente por $\cos\frac{\psi+\varphi_1}{2}$ e $\operatorname{sen}\frac{\psi+\varphi_1}{2}$ e somando, vem a 2ª igualdade (27); multiplicando respectivamente por $\operatorname{sen}\frac{\psi+\varphi_1}{2}$ e $\cos\frac{\psi+\varphi_1}{2}$ e subtraindo a 1ª da 2ª, vem a outra relação (27).

As duas últimas fórmulas de Delambre levariam anàlogamente a (28).

Definido o homomorfismo $U_2 \sim R$, a circunstância de haver duas transformações de U_2 que levam ao mesmo elemento de R reencontra-se por considerações da teoria geral dos grupos.

É, com efeito, $R \cong U_2/\mathcal{N}$, onde $\mathcal{N}$ é o conjunto das transformações de U_2 que levam à rotação identidade (rotação nula). Ora, para $N \in \mathcal{N}$, deverá ter-se $\varphi = \psi = \theta = 0$, ou $\varphi = 2\pi$, $\psi = \theta = 0$, ou $\psi = 2\pi$, $\varphi = \theta = 0$, o que leva às duas transformações de U_2:

$$\alpha = 1, \quad \beta = 0; \qquad \alpha = -1, \quad \beta = 0.$$

Os dois elementos de U_2 são

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

As matrizes de U_2 correspondentes à rotação (θ, φ, ψ) são, pois,

$$\begin{pmatrix} \cos\frac{\theta}{2}\, e^{i\frac{\varphi+\psi}{2}} & i\operatorname{sen}\frac{\theta}{2}\, e^{i\frac{\varphi-\psi}{2}} \\ i\operatorname{sen}\frac{\theta}{2}\, e^{-i\frac{\varphi-\psi}{2}} & \cos\frac{\theta}{2}\, e^{-i\frac{\varphi+\psi}{2}} \end{pmatrix}, \quad \begin{pmatrix} -\cos\frac{\theta}{2}\, e^{i\frac{\varphi+\psi}{2}} & -i\operatorname{sen}\frac{\theta}{2}\, e^{i\frac{\varphi-\psi}{2}} \\ -i\operatorname{sen}\frac{\theta}{2}\, e^{-i\frac{\varphi-\psi}{2}} & -\cos\frac{\theta}{2}\, e^{-i\frac{\varphi+\psi}{2}} \end{pmatrix} \quad (29)$$

Se fizermos no espaço $(\overset{1}{u}, \overset{2}{u})$ a mudança de base

$$\overset{1}{V} = \overset{2}{u}, \qquad \overset{2}{V} = i\,\overset{1}{u},$$

a primeira das matrizes anteriores, A, é substituida por

$$P^{-1}AP = \begin{pmatrix} \cos\frac{\theta}{2}\, e^{-i\frac{\varphi+\psi}{2}} & -\operatorname{sen}\frac{\theta}{2}\, e^{-i\frac{\varphi-\psi}{2}} \\ \operatorname{sen}\frac{\theta}{2}\, e^{i\frac{\varphi-\psi}{2}} & \cos\frac{\theta}{2}\, e^{i\frac{\varphi+\psi}{2}} \end{pmatrix} \quad (1),$$

(1) É a matriz que escreve van der Waerden a pgs.60 do livro "Die Gruppentheoretische Methode in der Quantenmechanik". As matrizes (29) são dadas em H.A.Kramers, "Theorie des Aufbaues der Materie", Leipzig, 1938, pgs.261.

visto que se tem

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -i & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} .$$

Vamos referir-nos agora às representações do grupo R conhecidas em Espectroscopia pela designação de representações $\mathcal{D}_J$. Consideremos um espaço linear S a $\rho+1$ dimensões, cujos vectores fundamentais representaremos com

$$(\overset{1}{u})^{\rho}, \ (\overset{1}{u})^{\rho-1}\overset{2}{u}, \ldots, \ (\overset{1}{u})^{\rho-r}(\overset{2}{u})^{r}, \ldots, \ (\overset{2}{u})^{\rho} .$$

Dado um vector

$$\mathfrak{x} = \sum_{r=0}^{\rho} (\overset{1}{u})^{\rho-r}(\overset{2}{u})^{r}\xi_r ,$$

tomemos como norma a expressão

$$G(\mathfrak{x}) = \sum_{r=0}^{\rho} r!\ (\rho-r)!\ \bar{\xi}_r\xi_r .^{(1)} \qquad (30)$$

Se a cada transformação $\underline{A}$, de U_2, como (20), fizermos corresponder a transformação seguinte de S:

$$A.(\overset{1}{u})^{\rho-r}(\overset{2}{u})^{r} = (\overset{1}{u}')^{\rho-r}(\overset{2}{u}')^{r} = (\overset{1}{u}\alpha - \overset{2}{u}\,\bar{\beta})^{\rho-r}(\overset{1}{u}\beta + \overset{2}{u}\,\bar{\alpha})^{r} =$$

$$= \sum_{t=0}^{\rho} (\overset{1}{u})^{\rho-t}(\overset{2}{u})^{t}\, a_{tr} , \qquad (31)$$

(1) A $G(\mathfrak{x})$ pode dar-se a forma $\sum \bar{\xi}_r\xi_r$ tomando os vectores fundamentais

$$v_r = \frac{(\overset{1}{u})^{\rho-r}(\overset{2}{u})^{r}}{\sqrt{r!\ (\rho-r)!}}, \quad (r = 0, 1, \ldots, \rho) .$$

fàcilmente se vê que esta transformação é unitária. Tomemos, de facto, o vector que pode escrever-se simbòlicamente

$$\mathfrak{x}_0 = (\overset{1}{u}x_1 + \overset{2}{u}x_2)^{\rho} = \sum_{r=0}^{\rho} (\overset{1}{u})^{\rho-r}(\overset{2}{u})^{r}\binom{\rho}{r} x_1^{\rho-r}x_2^{r} = \sum_{r=0}^{\rho} (\overset{1}{u})^{\rho-r}(\overset{2}{u})^{r}\xi_r .$$

Por meio de $\underline{A}$, obtém-se

$$\mathfrak{x}_0' = A\mathfrak{x}_0 = (\overset{1}{u}'x_1 + \overset{2}{u}'x_2)^{\rho} = (\overset{1}{u}x_1' + \overset{2}{u}x_2')^{\rho} = \sum_{t=0}^{\rho} (\overset{1}{u})^{\rho-t}(\overset{2}{u})^{t}\binom{\rho}{t} x_1'^{\rho-t}x_2'^{t} =$$

$$= \sum_{t=0}^{\rho} (\overset{1}{u})^{\rho-t}(\overset{2}{u})^{t}\,\xi' ,$$

com

$$x_1' = \alpha x_1 + \beta x_2 ,$$

$$x' = -\bar{\beta}x_1 + \bar{\alpha}x_2 .$$

A variância dos ξ_r é a mesma que de $\binom{\rho}{r} x_1^{\rho-r}x_2^{r}$. Ora $G(\mathfrak{x}_0)$ toma, quando $\mathfrak{x}_0$ se substitui por $A\,\mathfrak{x}_0 = \mathfrak{x}_0'$, o mesmo valor que

$$\sum_{r=0}^{\rho} r!\,(\rho-r)!\binom{\rho}{r}(\bar{x}_1)^{\rho-r}(\bar{x}_2)^{r}\binom{\rho}{r} x_1^{\rho-r}x_2^{r} = \rho! \sum_{r=0}^{\rho}\binom{\rho}{r}(\bar{x}_1)^{\rho-r}\cdot$$

$$\cdot\, x_1^{\rho-r}(\bar{x}_2)^{r}x_2^{r} = \rho!\ (\bar{x}_1x_1 + \bar{x}_2x_2)^{\rho} , \qquad (32)$$

quando se substitui aqui x_1 por x_1', $\bar{x}_1$ por $\bar{x}_1'$, x_2 por x_2', $\bar{x}_2$ por $\bar{x}_2'$. Como (32) fica, então, invariante, o mesmo se diz de $G(\mathfrak{x})$:

$$G(\mathfrak{x}') = G(\mathfrak{x}) , \qquad \text{se} \quad \mathfrak{x}' = A\mathfrak{x} .$$

As transformações de S definidas por (31), como transformações unitárias, são de determinante $\neq 0$. Se ao produto de dois elementos $A, B \in U_2$ corresponder o produto das transformações correspondentes de S, tem-se uma representação de U_2. Ora é

$$B.(\overset{1}{u})^{\rho-r}(\overset{2}{u})^{r} = (B\overset{1}{u})^{\rho-r}(B\overset{2}{u})^{r} ,$$

$$AB.(\overset{1}{u})^{\rho-r}(\overset{2}{u})^{r} = (AB\overset{1}{u})^{\rho-r}(AB\overset{2}{u})^{r} = (A.B\overset{1}{u})^{\rho-r}(A.B\overset{2}{u})^{r} =$$

$$= A.(B\overset{1}{u})^{\rho-r}(B\overset{2}{u})^{r} = A.\left(B.(\overset{1}{u})^{\rho-r}(\overset{2}{u})^{r}\right),$$

donde se conclui o que se deseja.

A representação de U_2 definida em (31) representa-se com $\mathcal{D}_{\frac{1}{2}\rho} = \mathcal{D}_J$, onde $J = \frac{1}{2}\rho$. O espaço duma representação $\mathcal{D}_J$ tem, assim, $2J + 1$ dimensões. Se supomos $J = \rho = 0$, o espaço S tem o único vector base $(\overset{1}{u})^0(\overset{2}{u})^0$, e é

$$A(\overset{1}{u})^0(\overset{2}{u})^0 = (\overset{1}{u'})^0(\overset{2}{u'})^0 = (\overset{1}{u})^0(\overset{2}{u})^0 .$$

A representação $\mathcal{D}_0$ é, pois, a representação idêntica. Se é $\rho = 1$, $J = \frac{1}{2}$, tem-se $2J + 1 = 2$, e obtém-se a representação de U_2 por si mesmo.

Consideremos o grupo R das rotações. Como U_2 dá uma representação biforme de R, podemos enunciar o seguinte

Teorema:- As representações $\mathcal{D}_J$ são representações biformes (quando muito) do grupo R. A representação $\mathcal{D}_0$, por ex., é uniforme e a representação $\mathcal{D}_{\frac{1}{2}}$ é biforme. A representação $\mathcal{D}_1$ volta a ser uniforme, pois que, tomando os vectores fundamentais de S, $(\overset{1}{u})^2$, $\overset{1}{u}\overset{2}{u}$, $(\overset{2}{u})^2$, tem-se

$$A.(\overset{1}{u})^2 = (\overset{1}{u}\alpha - \overset{2}{u}\,\overline{\beta})^2 ,$$

$$A.\overset{1}{u}\overset{2}{u} = (\overset{1}{u}\alpha - \overset{2}{u}\,\overline{\beta})(\overset{1}{u}\beta + \overset{2}{u}\,\overline{\alpha}),$$

$$A.(\overset{2}{u})^2 = (\overset{1}{u}\beta + \overset{2}{u}\,\overline{\alpha})^2 ,$$

e é

$$-A.(\overset{1}{u})^2 = A(\overset{1}{u})^2, \quad -A.\overset{1}{u}\,\overset{2}{u} = A.\overset{1}{u}\,\overset{2}{u} , \quad -A.(\overset{2}{u})^2 = A.(\overset{2}{u})^2 .$$

Dum modo geral, as representações $\mathcal{D}_J$, de R, são uniformes ou biformes, conforme J é inteiro ou semi-inteiro.

14) O grupo de Lorentz e o grupo linear especial - Voltemos ao espaço $(\overset{1}{u}, \overset{2}{u})$ e ao grupo linear especial L_2 das transformações (18'). Consideremos, de novo, o vector isótropo V_0 (a, b, c) do espaço ordinário e as relações (21) que definem ξ_1, ξ_2, aparte o sinal. Se fazemos uma transformação (21'), deixando aos coeficientes a liberdade de serem reais ou imaginários, mas satisfazendo sempre às condições de ortogonalidade (rotações complexas), obtêm-se ainda as fórmulas (22), com $\alpha\delta - \beta\gamma = 1$. Ao escrever-se, porém,

$$V_0 = (A + iA_1)I + (B + iB_1)J + (C + iC_1)K ,$$

não podemos dizer que a variância de (A, B, C) e de (A_1, B_1, C_1) tem lugar segundo a lei (21'), pois tal resultado exigiria que fossem reais os coeficientes α_{ij}. A expressão $\overline{\xi}_1\xi_1 + \overline{\xi}_2\xi_2$ não é, pois, invariante, em face de (19). No entanto, tem lugar o seguinte

Teorema:- A cada rotação complexa (21'), à volta da origem, no espaço ordinário, correspondem duas transformações (22) do grupo linear especial L_2, a saber:

$$\begin{cases} \xi_1' = \alpha\xi_1 + \beta\xi_2 , \\ \xi_2' = \gamma\xi_1 + \delta\xi_2 , \end{cases} \qquad \begin{cases} \xi_1' = -\alpha\xi_1 - \beta\xi_2 , \\ \xi_2' = -\gamma\xi_1 - \delta\xi_2 . \end{cases} \tag{32'}$$

Inversamente, dada a 1ª das transformações anteriores, tem-se

$$\begin{cases} \xi_1'^2 = \alpha^2\xi_1^2 + \beta^2\xi_2^2 + 2\alpha\beta\xi_1\xi_2 , \\ \xi_2'^2 = \gamma^2\xi_1^2 + \delta^2\xi_2^2 + 2\gamma\delta\xi_1\xi_2 , \\ \xi_1'\xi_2' = \alpha\gamma\xi_1^2 + \beta\delta\xi_2^2 + (\alpha\delta + \beta\gamma)\xi_1\xi_2 , \end{cases}$$

$$\begin{cases} a' = \dfrac{\xi_1'^2 - \xi_2'^2}{2} = \dfrac{\alpha^2 - \gamma^2}{2}\xi_1^2 + \dfrac{\beta^2 - \delta^2}{2}\xi_2^2 + (\alpha\beta - \gamma\delta)\xi_1\xi_2 , \\[2ex] b' = i\,\dfrac{\xi_1'^2 + \xi_2'^2}{2} = i\,\dfrac{\alpha^2 + \gamma^2}{2}\xi_1^2 + i\,\dfrac{\beta^2 + \delta^2}{2}\xi_2^2 + i(\alpha\beta + \gamma\delta)\xi_1\xi_2 , \\[2ex] c' = -\xi_1'\xi_2' = -\alpha\gamma\xi_1^2 - \beta\delta\xi_2^2 - (\alpha\delta + \beta\gamma)\xi_1\xi_2 , \end{cases}$$

$$\begin{cases} a' = \dfrac{\alpha^2 - \gamma^2}{2}(a - bi) + \dfrac{\beta^2 - \delta^2}{2}(-a - bi) - (\alpha\beta - \gamma\delta)c , \\[2ex] b' = i\,\dfrac{\alpha^2 + \gamma^2}{2}(a - bi) + i\,\dfrac{\beta^2 + \delta^2}{2}(-a - bi) - i(\alpha\beta + \gamma\delta)c , \\[2ex] c' = -\alpha\gamma(a - bi) - \beta\delta(-a - bi) + (\alpha\delta + \beta\gamma)c . \end{cases}$$

Estas últimas igualdades escrevem-se ainda

$$\begin{cases} a' = \dfrac{\alpha^2 + \delta^2 - \beta^2 - \gamma^2}{2}a + i\,\dfrac{\gamma^2 + \delta^2 - \alpha^2 - \beta^2}{2}b - (\alpha\beta - \gamma\delta)c , \\[2ex] b' = i\,\dfrac{\alpha^2 + \gamma^2 - \beta^2 - \delta^2}{2}a + \dfrac{\alpha^2 + \gamma^2 + \beta^2 + \delta^2}{2}b - i(\alpha\beta + \gamma\delta)c , \qquad (32'') \\[2ex] c' = -(\alpha\gamma - \beta\delta)a + i(\alpha\gamma + \beta\delta)b + (\alpha\delta + \beta\gamma)c . \end{cases}$$

Têm-se aqui fórmulas que definem uma rotação complexa no espaço ordinário, como fàcilmente se verifica. Se utilizássemos a 2ª transformação (32'), ainda se obteria (32''). O teorema anterior tem o seguinte

<u>Complemento</u>:- <u>Na correspondência que leva do grupo das rotações complexas, R_c, ao grupo L_2, reencontram-se todos os elementos de L_2.</u>

E pode ainda enunciar-se o

<u>Teorema</u>:- <u>O grupo R_c dá uma representação uniforme do grupo L_2, e, inversamente, L_2 dá uma representação biforme de R_c.</u>

O processo de cálculo que acaba de ser indicado leva, de facto, dum elemento de L_2 a um elemento bem determinado de R_c. Basta ver que leva do produto ao produto. Ora, pondo

$$\begin{cases} \xi_1'' = \alpha_1\xi_1' + \beta_1\xi_2' = (\alpha_1\alpha + \beta_1\gamma)\xi_1 + (\alpha_1\beta + \beta_1\delta)\xi_2 , \\ \xi_2'' = \gamma_1\xi_1' + \delta_1\xi_2' = (\gamma_1\alpha + \delta_1\gamma)\xi_1 + (\gamma_1\beta + \delta_1\delta)\xi_2 , \end{cases}$$

$$\begin{cases} a'' = \dfrac{\alpha_1^2 + \delta_1^2 - \beta_1^2 - \gamma_1^2}{2}a' + i\,\dfrac{\gamma_1^2 + \delta_1^2 - \alpha_1^2 - \beta_1^2}{2}b' - (\alpha_1\beta_1 - \gamma_1\delta_1)c' , \\ \text{- -} , \end{cases}$$

chega-se a

$$\begin{cases} a'' = \dfrac{\alpha_1^2 + \delta_1^2 - \beta_1^2 - \gamma_1^2}{2}\left[\dfrac{\alpha^2 + \delta^2 - \beta^2 - \gamma^2}{2}a + i\,\dfrac{\gamma^2 + \delta^2 - \alpha^2 - \beta^2}{2}b - (\alpha\beta - \gamma\delta)c\right] + \\[2ex] \quad + i\,\dfrac{\gamma_1^2 + \delta_1^2 - \alpha_1^2 - \beta_1^2}{2}\left[i\,\dfrac{\alpha^2 + \gamma^2 - \beta^2 - \delta^2}{2}a + \dfrac{\alpha^2 + \gamma^2 + \beta^2 + \delta^2}{2}b - i(\alpha\beta + \gamma\delta)c\right] - \\[2ex] \quad - (\alpha_1\beta_1 - \gamma_1\delta_1)\left[-(\alpha\gamma - \beta\delta)a + i(\alpha\gamma + \beta\delta)b + (\alpha\delta + \beta\gamma)c\right] , \\ \text{- -} . \end{cases}$$

São fáceis de demonstrar igualdades como a seguinte, que provam a afirmação:

$$\frac{(\alpha_1\alpha + \beta_1\gamma)^2 + (\gamma_1\beta + \delta_1\delta)^2 - (\alpha_1\beta + \beta_1\delta)^2 - (\gamma_1\alpha + \delta_1\gamma)^2}{2} =$$

$$= \frac{(\alpha_1^2 + \delta_1^2 - \beta_1^2 - \gamma_1^2)(\alpha^2 + \delta^2 - \beta^2 - \gamma^2)}{4} - \frac{(\gamma_1^2 + \delta_1^2 - \alpha_1^2 - \beta_1^2)(\alpha^2 + \gamma^2 - \beta^2 - \delta^2)}{4} +$$

$$+ (\alpha_1\beta_1 - \gamma_1\delta_1)(\alpha\gamma - \beta\delta) .$$

Definido o homomorfismo $L_2 \sim R_c$, a circunstância de haver duas transformações de L_2 que levam ao mesmo elemento de R_c reencontra-se por considerações da teoria geral dos grupos. É, com efeito, $R_c \cong L_2/\mathfrak{N}$, onde $\mathfrak{N}$ é o conjunto de transformações de L_2 que levam à rotação identidade (rotação nula). Das relações

$$a' = a \,, \quad b' = b \,, \quad c' = c \,,$$

tira-se sucessivamente, tendo em conta (32''),

$$\alpha\gamma - \beta\delta = \alpha\gamma + \beta\delta = \alpha\beta + \gamma\delta = \alpha\beta - \gamma\delta = 0 \,, \quad \alpha\delta + \beta\gamma = 1,$$

$$\beta\delta = \gamma\delta = \alpha\gamma = \alpha\beta = 0, \quad \alpha\delta + \beta\gamma = 1.$$

Tendo ainda em conta a relação $\alpha\delta - \beta\gamma = 1$, vê-se que deve tomar-se $\beta\gamma = 0$, de sorte que vem

$$\beta = 0, \quad \gamma = 0, \quad \alpha\delta = 1, \quad \text{a que se pode juntar} \quad \alpha^2 + \delta^2 = 2.$$

Finalmente, encontra-se

$$\alpha = \pm 1, \quad \delta = \pm 1, \quad \beta = 0, \quad \gamma = 0,$$

sem outras possibilidades (e com correspondência dos sinais). Há duas transformações de L_2 que têm a rotação identidade como correspondente:

$$\begin{cases} \xi_1' = \xi_1 \,, \\ \xi_2' = \xi_2 \,, \end{cases} \qquad \begin{cases} \xi_1' = -\xi_1 \,, \\ \xi_2' = -\xi_2 \,. \end{cases}$$

As matrizes respectivas são

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \,, \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} .$$

Os resultados a que se chegou estão de acordo com o facto de dependerem do mesmo número de parâmetros tanto os elementos de R_c como os de L_2 (3 complexos ou 6 reais).

Posto isto, consideremos as transformações lineares com **coeficientes** reais

$$\begin{aligned} x' &= a_{11}x + a_{12}y + a_{13}z + a_{14}\cdot ct \,, \\ y' &= a_{21}x + a_{22}y + a_{23}z + a_{24}\cdot ct \,, \\ z' &= a_{31}x + a_{32}y + a_{33}z + a_{34}\cdot ct \,, \\ ct' &= a_{41}x + a_{42}y + a_{43}z + a_{44}\cdot ct \,, \end{aligned} \quad \text{ou} \quad \begin{pmatrix} x' \\ y' \\ z' \\ ct' \end{pmatrix} = A \begin{pmatrix} x \\ y \\ z \\ ct \end{pmatrix}, \quad (33)$$

(nas quais c é uma constante numérica) que conservam invariante a forma quadrática $x^2 + y^2 + z^2 - c^2t^2$. Na 2ª forma escrita, A representa a matriz (a_{ik}). Para simplicidade de escrita, ponhamos $x = y_1$, $y = y_2$, $z = y_3$, $ct = y_4$. Da relação

$$\left(\sum_{j=1}^{4} a_{1i} y_i \cdot \sum_j a_{1j} y_j\right) + \left(\sum_i a_{2i} y_i \cdot \sum_j a_{2j} y_j\right) + \left(\sum_i a_{3i} y_i \cdot \sum_j a_{3j} y_j\right) - \left(\sum_i a_{4i} y_i \cdot \sum_j a_{4j} y_j\right) = y_1^2 + y_2^2 + y_3^2 - y_4^2 \,,$$

concluem-se as 10 igualdades seguintes:

$$\begin{cases} \sum_{k=1}^{3} a_{ki}^2 - a_{4i}^2 = 1 \,, & (i = 1, 2, 3) \\ \sum_{k=1}^{3} a_{k4}^2 - a_{44}^2 = -1 \,, \\ \sum_k a_{ki} a_{kj} - a_{4i} a_{4j} = 0 \,, & (i \neq j). \end{cases} \quad (34)$$

Nas igualdades (33) há, deste modo, apenas 6 parâmetros independentes. Elas podem ser resolvidas em ordem a y_1, y_2, y_3, y_4, tendo em conta (34). Vem, efectivamente,

$$a_{11} y_1' + a_{21} y_2' + a_{31} y_3' - a_{41} y_4' = y_1 \,,$$
$$- - - - - - - - - - - - - - - - \,,$$
$$a_{14} y_1' + a_{24} y_2' + a_{34} y_3' - a_{44} y_4' = -y_4 .$$

As fórmulas inversas de (33) são, pois,

$$\begin{aligned} x &= a_{11}x' + a_{21}y' + a_{31}z' - a_{41}\cdot ct', \\ y &= a_{12}x' + a_{22}y' + a_{32}z' - a_{42}\cdot ct', \\ z &= a_{13}x' + a_{23}y' + a_{33}z' - a_{43}\cdot ct', \\ ct &= -a_{14}x' - a_{24}y' - a_{34}z' - a_{44}\cdot ct', \end{aligned} \quad \text{ou} \quad \begin{pmatrix} x \\ y \\ z \\ ct \end{pmatrix} = A^{-1}\begin{pmatrix} x' \\ y' \\ z' \\ ct' \end{pmatrix} .$$

Ao lado de (34), encontram-se agora as relações seguintes, consequência delas:

$$\begin{cases} \sum_{k=1}^{3} a_{ik}^2 - a_{i4}^2 = 1 , & (i = 1, 2, 3) , \\ \sum_{k=1}^{3} a_{4k}^2 - a_{44}^2 = -1 , & \\ \sum_{k=1}^{3} a_{ik}a_{jk} - a_{i4}a_{j4} = 0 , & (i \neq j) . \end{cases} \tag{34'}$$

O determinante Δ da transformação (33) verifica a igualdade

$$\Delta\Delta^{(-1)} = \begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{vmatrix} \cdot \begin{vmatrix} a_{11} & a_{21} & a_{31} & -a_{41} \\ a_{12} & a_{22} & a_{32} & -a_{42} \\ a_{13} & a_{23} & a_{33} & -a_{43} \\ -a_{14} & -a_{24} & -a_{34} & +a_{44} \end{vmatrix} = \Delta^2 = 1 .$$

Diz-se <u>grupo próprio de Lorentz</u>, $\mathcal{L}$, o conjunto das transformações (33) para as quais $\Delta = +1$.

Vamos procurar uma correspondência entre o grupo $\mathcal{L}$ e o grupo R_c das rotações complexas do espaço ordinário definidas em (21'). É claro que estas últimas são caracterizadas pela invariância da forma quadrática $a^2 + b^2 + c^2$ (o determinante da transformação é +1).

Suponhamos y_1, y_2, y_3, y_4 componentes dum vector do <u>espaço da relatividade</u>, para o qual a métrica é definida pela

forma quadrática $y_1^2 + y_2^2 + y_3^2 - y_4^2$. O grupo $\mathcal{L}$ é um sub-grupo do grupo das transformações métricas reais. Dados dois vectores (x_l), (y_k) as 16 quantidades $x_l y_k$ têm uma variância, em face das transformações métricas, que se diz a variância dum <u>tensor de 2ª ordem</u>. 16 números T_{lk} (reais) com essa variância definem o tensor. Este diz-se <u>hemi-simétrico</u>, se for $T_{lk} = -T_{kl}$, e <u>simétrico</u>, quando $T_{lk} = T_{kl}$.

A definição de simetria e de hemi-simetria é independente das transformações métricas. Assim, se $T_{lk} = -T_{kl}$, tem-se

$$T'_{lk} = \sum_{m,n} a_{lm}a_{kn}T_{mn} ,$$

$$-T'_{kl} = -\sum_{m,n} a_{km}a_{ln}T_{mn} = -\sum_{m,n} a_{kn}a_{lm}T_{nm} = \sum_{m,n} a_{lm}a_{kn}T_{mn} = T'_{lk} .$$

Um tensor hemi-simétrico fica conhecido a partir das 6 componentes $T_{12}, T_{23}, T_{31}, T_{14}, T_{24}, T_{34}$, visto ser $T_{ll} = 0$. Na correspondência $\mathcal{L} \sim R_c$ a estudar, a variância das 6 componentes que acabamos de referir vai servir-nos para definir a variância das 3 componentes reais e das 3 componentes imaginárias dum vector, de harmonia com (21'). As relações (21'), sob forma desenvolvida, deverão escrever-se

$$\left.\begin{aligned} A' + iA'_1 &= (\alpha_{11} + i\beta_{11})(A + iA_1) + (\alpha_{12} + i\beta_{12})(B + iB_1) + \\ &\quad + (\alpha_{13} + i\beta_{13})(C + iC_1) \\ B' + iB'_1 &= (\alpha_{21} + i\beta_{21})(A + iA_1) + \cdots \\ C' + iC'_1 &= (\alpha_{31} + i\beta_{31})(A + iA_1) + \cdots \end{aligned}\right\} . \tag{35}$$

Vê-se, por ex., que nas expressões de A', B', C' figuram não sòmente A, B, C, mas ainda A_1, B_1, C_1. Demonstraremos, a seguir, que uma transformação do grupo próprio de <u>Lorentz</u> se pode escrever sempre como produto de transformações do espaço ordinário (obtidas de (33) pondo $a_{14} = a_{24} = a_{34} = 0$ e $ct' = ct$) e duma <u>transformação especial de Lorentz</u> da forma

$$x' = x\ ,\quad y' = y\ ,\quad z' = \frac{z - vt}{\sqrt{1 - \frac{v^2}{c^2}}}\ ,\quad ct' = \frac{ct - \frac{v}{c}z}{\sqrt{1 - \frac{v^2}{c^2}}}\ . \qquad (36)$$

Deste modo, limitar-nos-emos a procurar as transformações (35) correspondentes aos elementos de $\mathscr{L}$ da forma (36) ou da forma

$$y_1' = a_{11}y_1 + a_{12}y_2 + a_{13}y_3\ ,$$
$$y_2' = a_{21}y_1 + a_{22}y_2 + a_{23}y_3\ , \qquad (37)$$
$$y_3' = a_{31}y_1 + a_{32}y_2 + a_{33}y_3\ ,$$
$$y_4' = y_4\ .$$

Relativamente a (37), obtém-se

$$T'_{12} = (a_{11}a_{22} - a_{12}a_{21})T_{12} + (a_{13}a_{21} - a_{11}a_{23})T_{31} + (a_{12}a_{23} - a_{22}a_{13})T_{23}\ ,$$
$T'_{23} =$ -

- .

Tendo em vista as propriedades conhecidas dos coeficientes de (37), as fórmulas anteriores podem escrever-se

$$T'_{12} = a_{33}T_{12} + a_{32}T_{31} + a_{31}T_{23}\ ,$$
$$T'_{31} = a_{23}T_{12} + a_{22}T_{31} + a_{21}T_{23}\ ,$$
$$T'_{23} = a_{13}T_{12} + a_{12}T_{31} + a_{11}T_{23}\ ,$$
$$T'_{14} = a_{11}T_{14} + a_{12}T_{24} + a_{13}T_{34}\ ,$$
$$T'_{24} = a_{21}T_{14} + a_{22}T_{24} + a_{23}T_{34}\ ,$$
$$T'_{34} = a_{31}T_{14} + a_{32}T_{24} + a_{33}T_{34}\ .$$

Daqui tiram-se as relações

$$T'_{14} - iT'_{23} = a_{11}(T_{14} - iT_{23}) + a_{12}(T_{24} - iT_{31}) + a_{13}(T_{34} - iT_{12})\ ,$$
$$T'_{24} - iT'_{31} = a_{21}(T_{14} - iT_{23}) + a_{22}(T_{24} - iT_{31}) + a_{23}(T_{34} - iT_{12})\ , \qquad (38)$$
$$T'_{34} - iT'_{12} = a_{31}(T_{14} - iT_{23}) + a_{32}(T_{24} - iT_{31}) + a_{33}(T_{34} - iT_{12})\ .$$

Dada, portanto, uma transformação de $\mathscr{L}$ que seja um elemento de R (melhor seria dizer: que se possa interpretar como tal), os números $T_{14} - iT_{23}$, $T_{24} - iT_{31}$, $T_{34} - iT_{12}$ (T_{ik} = tensor hemi-simétrico) variam conforme (38), que é uma transformação do grupo R_c, precisamente o elemento considerado de R.

Passemos agora às transformações especiais de Lorentz.

Tem-se

$$T'_{12} = T_{12}\ ,\quad T'_{31} = \frac{T_{31} + \beta T_{14}}{\sqrt{1-\beta^2}}\ ,\quad T'_{23} = \frac{T_{23} - \beta T_{24}}{\sqrt{1-\beta^2}}\ ,\qquad \left(\beta = \frac{v}{c}\right)\ ,$$

$$T'_{14} = \frac{T_{14} + \beta T_{31}}{\sqrt{1-\beta^2}}\ ,\quad T'_{24} = \frac{T_{24} - \beta T_{23}}{\sqrt{1-\beta^2}}\ ,\qquad T'_{34} = T_{34}\ ,$$

e, portanto,

$$T'_{14} - iT'_{23} = \frac{1}{\sqrt{1-\beta^2}}(T_{14} - iT_{23}) + \frac{i\beta}{\sqrt{1-\beta^2}}(T_{24} - iT_{31})\ ,$$

$$T'_{24} - iT'_{31} = \frac{-i\beta}{\sqrt{1-\beta^2}}(T_{14} - iT_{23}) + \frac{1}{\sqrt{1-\beta^2}}(T_{24} - iT_{31})\ ,$$

$$T'_{34} - iT'_{12} = T_{34} - iT_{12}\ .$$

A transformação (35) é, deste modo, a seguinte:

$$a' = \frac{a}{\sqrt{1-\beta^2}} + \frac{i\beta b}{\sqrt{1-\beta^2}}\ ,$$
$$b' = \frac{-i\beta a}{\sqrt{1-\beta^2}} + \frac{b}{\sqrt{1-\beta^2}}\ , \qquad |\Delta| = 1\ , \qquad (39)$$
$$c' = c\ ,$$

pois que, efectivamente, se tem $a'^2 + b'^2 + c'^2 = a^2 + b^2 + c^2$. É evidente que ao produto duma transformação (36) por uma transformação (37) corresponde o produto das transformações correspondentes de R_c.

A cada transformação do grupo próprio de Lorentz faz-se corresponder, pois, uma rotação complexa do espaço ordinário. Vamos procurar inverter esta afirmação. Em vez de tratarmos o problema directamente, procederemos do modo seguinte: [1] α) mostraremos que a toda a transformação de L_2 (grupo linear especial) corresponde uma transformação de $\mathcal{L}$ (grupo próprio de Lorentz; β) que uma transformação de $\mathcal{L}$ corresponde a duas transformações de L_2 (definidas por duas matrizes iguais e de sinais contrários); γ) que, portanto, dada uma transformação de R_c (grupo das rotações complexas) há uma transformação de $\mathcal{L}$ que lhe corresponde e reciprocamente; δ) e, finalmente, que, nesta correspondência $R_c \rightleftarrows \mathcal{L}$, as rotações reais de R_c levam a transformações (37) e as rotações (39) levam a (36). Feito isto, ficarão provadas as duas proposições a seguir (A e B):

Teorema A:- O grupo próprio de Lorentz dá uma representação uniforme do grupo linear especial, e, inversamente, este dá uma representação biforme daquele.

Teorema B:- O grupo das rotações complexas dá uma representação fiel do grupo próprio de Lorentz.

α)) - Consideremos o espaço unitário $(\overset{1}{u}, \overset{2}{u})$ e as transformações do grupo L_2:

$$\begin{cases} \overset{1}{u}' = \overset{1}{u}\,\alpha + \overset{2}{u}\,\gamma , \\ \overset{2}{u}' = \overset{1}{u}\,\beta + \overset{2}{u}\,\delta , \end{cases} \tag{40}$$

às quais associaremos as transformações

(1) B. L. van der Waerden, "Die Gruppentheoretische Methode in der Quantenmechanik", pgs. 78 e seguintes.

$$\begin{cases} \overset{\dot{1}}{u}' = \overset{\dot{1}}{u}\,\overline{\alpha} + \overset{\dot{2}}{u}\,\overline{\gamma} , \\ \overset{\dot{2}}{u}' = \overset{\dot{1}}{u}\,\overline{\beta} + \overset{\dot{2}}{u}\,\overline{\delta} , \end{cases} \qquad (\overline{\alpha}\,\overline{\delta} - \overline{\beta}\,\overline{\gamma}) = 1 . \tag{41}$$

Em seguida, consideremos o espaço a 4 dimensões $(\overset{1}{u}\,\overset{\dot{1}}{u},\ \overset{1}{u}\,\overset{\dot{2}}{u},\ \overset{2}{u}\,\overset{\dot{1}}{u},\ \overset{2}{u}\,\overset{\dot{2}}{u})$ e as transformações lineares deste espaço formalmente definidas por (40) e (41). A um vector

$$\xi = \overset{1}{u}\,\overset{\dot{1}}{u}\,x_{1\dot{1}} + \overset{1}{u}\,\overset{\dot{2}}{u}\,x_{1\dot{2}} + \overset{2}{u}\,\overset{\dot{1}}{u}\,x_{2\dot{1}} + \overset{2}{u}\,\overset{\dot{2}}{u}\,x_{2\dot{2}} \tag{42}$$

far-se-á corresponder um vector

$$\begin{aligned} \xi' = A\xi &= \overset{1}{u}'\,\overset{\dot{1}}{u}'x_{1\dot{1}} + \cdots + \overset{2}{u}'\overset{\dot{2}}{u}'x_{2\dot{2}} = \\ &= \overset{1}{u}\,\overset{\dot{1}}{u}\,x'_{1\dot{1}} + \overset{1}{u}\,\overset{\dot{2}}{u}\,x'_{1\dot{2}} + \overset{2}{u}\,\overset{\dot{1}}{u}\,x'_{2\dot{1}} + \overset{2}{u}\,\overset{\dot{2}}{u}\,x'_{2\dot{2}} . \end{aligned} \tag{43}$$

As operações a efectuar para se passar de (42) a (43) são formalmente as seguintes: é dada a forma bilinear de duas séries de variáveis (42) e praticam-se nas variáveis as transformações (40) e (41). A substituição leva imediatamente à igualdade

$$x'_{2\dot{1}}\,x'_{1\dot{2}} - x'_{1\dot{1}}\,x'_{2\dot{2}} = x_{2\dot{1}}\,x_{1\dot{2}} - x_{1\dot{1}}\,x_{2\dot{2}} .$$

Deste modo, sendo

$$(x + iy)(x - iy) - (ct + z)(ct - z) = x^2 + y^2 + z^2 - c^2t^2,$$

vê-se que, pondo

$$x + iy = x_{2\dot{1}}, \quad x - iy = x_{1\dot{2}}, \quad ct + z = x_{1\dot{1}}, \quad ct - z = x_{2\dot{2}}, \tag{44}$$

a variância de x, y, z, ct definida através destas igualdades satisfaz à relação $x'^2 + y'^2 + z'^2 - c^2t'^2 = x^2 + y^2 + z^2 - c^2t^2$. A fim de que, em (44), se possam interpretar x, y, z, ct como quantidades reais, devemos supor $x_{2\dot{1}}$ imaginário conjugado de $x_{1\dot{2}}$, e supor reais $x_{1\dot{1}}$ e $x_{2\dot{2}}$. Esta hipótese é compatível com (40),

pois que, interpretando (42) como forma bilinear, na qual $\overset{1}{u}$, $\overset{2}{u}$ são variáveis conjugadas de $\overset{1}{u}$, $\overset{2}{u}$, (42) toma apenas valores reais. Então, em (43), o penúltimo membro é real, assim como o último, quaisquer que sejam $\overset{1}{u}$ e $\overset{2}{u}$. Portanto, x'_{11}, x'_{22} são reais e x'_{12}, x'_{21} são imaginários conjugados. As relações que ligam x', y', z', ct' a x, y, z, ct têm os coeficientes reais e são transformações do grupo próprio de Lorentz. Reconhece-se este último ponto, sem ser directamente, notando que o determinante Δ respectivo, quando a transformação varia continuamente, conserva o seu valor. Ora, para $\alpha = \delta = 1$, $\beta = \gamma = 0$, vem

$$x' = x\,, \quad y' = y\,, \quad z' = z\,, \quad ct' = ct\,, \quad \Delta = +1\,.$$

Posto isto, tomemos, em particular, as transformações de L_2 que constituem o grupo unitário U_2:

$$\begin{cases} \overset{1}{u}' = \overset{1}{u}.\cos\frac{\theta}{2}\, e^{i\frac{\varphi+\psi}{2}} + u.i\,\operatorname{sen}\frac{\theta}{2}\, e^{-i\frac{\varphi-\psi}{2}} = \overset{1}{u}\alpha - \overset{2}{u}\,\overline{\beta}\,, \\ \overset{2}{u}' = \overset{1}{u}.i\,\operatorname{sen}\frac{\theta}{2}\, e^{i\frac{\varphi-\psi}{2}} + \overset{2}{u}.\cos\frac{\theta}{2}\, e^{-i\frac{\varphi+\psi}{2}} = \overset{1}{u}.\beta + \overset{2}{u}\,\overline{\alpha}\,. \end{cases}$$

Tem-se

$$x' = \frac{x'_{21} + x'_{12}}{2} = -\frac{1}{2}(\alpha\beta + \overline{\beta}\,\overline{\alpha})(ct + z) + \frac{1}{2}(\alpha\alpha - \overline{\beta}\,\overline{\beta})(x - iy) +$$

$$+ \frac{1}{2}(-\beta\beta + \overline{\alpha}\,\overline{\alpha})(x + iy) + \frac{1}{2}(\beta\alpha + \overline{\alpha}\,\overline{\beta})(ct - z)\,.$$

O coeficiente de ct desaparece e fica

$$x' = \frac{1}{2}(\alpha\alpha + \overline{\alpha}\,\overline{\alpha} - \beta\beta - \overline{\beta}\,\overline{\beta})x - \frac{i}{2}(\alpha\alpha - \overline{\alpha}\,\overline{\alpha} + \beta\beta - \overline{\beta}\,\overline{\beta})y - (\alpha\beta + \overline{\alpha}\,\overline{\beta})z,$$

ou seja ainda

$$x' = (\cos\psi\cos\varphi - \operatorname{sen}\psi\operatorname{sen}\varphi\cos\theta).x +$$

$$+ (\operatorname{sen}\psi\cos\varphi + \cos\psi\operatorname{sen}\varphi\cos\theta).y + \operatorname{sen}\varphi\operatorname{sen}\theta.z\,. \qquad (45)$$

Anàlogamente, encontra-se

$$y' = -i\frac{x'_{21} - x'_{12}}{2} = -\frac{i}{2}(-\overline{\beta}\,\overline{\alpha} + \alpha\beta)(ct + z) - \frac{i}{2}(-\overline{\beta}\,\overline{\beta} - \alpha\alpha).$$

$$.(x - iy) - \frac{i}{2}(\overline{\alpha}\,\overline{\alpha} + \beta\beta)(x + iy) - \frac{i}{2}(\overline{\alpha}\,\overline{\beta} - \beta\alpha)(ct - z),$$

e, em seguida,

$$y' = (-\cos\psi\operatorname{sen}\varphi - \operatorname{sen}\psi\cos\varphi\cos\theta).x +$$

$$+ (-\operatorname{sen}\psi\operatorname{sen}\varphi + \cos\psi\cos\varphi\cos\theta).y - \cos\varphi\operatorname{sen}\theta.z\,. \qquad (46)$$

Finalmente

$$z' = \frac{x'_{11} - x'_{22}}{2} = \frac{1}{2}(\alpha\overline{\alpha} - \overline{\beta}\,\beta)(ct + z) + \frac{1}{2}(\alpha\overline{\beta} + \overline{\beta}\,\alpha)(x - iy) +$$

$$+ \frac{1}{2}(\beta\,\overline{\alpha} + \overline{\alpha}\,\beta)(x + iy) + \frac{1}{2}(\beta\overline{\beta} - \alpha\overline{\alpha})(ct - z) =$$

$$= \operatorname{sen}\psi\operatorname{sen}\theta.x - \cos\psi\operatorname{sen}\theta.y + \cos\theta.z\,, \qquad (47)$$

$$ct' = \frac{x'_{11} + x'_{22}}{2} = \frac{x_{11} + x_{22}}{2} = ct. \qquad (48)$$

Na correspondência que leva de L_2 a $\mathcal{L}$, o grupo U_2 é representado pelas transformações de Lorentz (37) (que são as rotações do espaço ordinário), pois que os coeficientes das igualdades (45), (46), (47) mostram tratar-se duma rotação à qual correspondem os ângulos de Euler θ, φ, ψ.

β.)) - Na correspondência $L_2 \to \mathcal{L}$, estudada em α)), reencontram-se todos os elementos de $\mathcal{L}$, pois vamos ver que é possível reencontrar uma transformação especial qualquer (36). Façamos

$$\tau = \pm\sqrt[4]{\frac{1-\beta}{1+\beta}}\,, \qquad \left(\beta = \frac{v}{c}\,,\ \tau \text{ real}\right).$$

Tem-se, sucessivamente,

$$\tau^2 = \sqrt{\frac{1-\beta}{1+\beta}}, \quad \tau^2+\tau^{-2} = \frac{2}{\sqrt{1-\beta^2}}, \quad \tau^2-\tau^{-2} = -\frac{2\beta}{\sqrt{1-\beta^2}},$$

de sorte que (36) pode tomar o aspecto

$$\begin{aligned} x' &= x, \\ y' &= y, \\ z' &= \frac{1}{2}(\tau^2+\tau^{-2}).z + \frac{1}{2}(\tau^2-\tau^{-2}).ct \\ ct' &= \frac{1}{2}(\tau^2-\tau^{-2}).z + \frac{1}{2}(\tau^2+\tau^{-2}).ct . \end{aligned} \qquad (49)$$

Se considerarmos a transformação de L_2

$$\overset{1}{u}' = \overset{1}{u}\tau, \qquad \overset{2}{u}' = \overset{2}{u}\tau^{-1}, \qquad (49')$$

vem imediatamente

$$x'_{1\dot{1}} = \tau^2 x_{1\dot{1}}, \quad x'_{1\dot{2}} = x_{1\dot{2}}, \quad x'_{2\dot{1}} = x_{2\dot{1}}, \quad x'_{2\dot{2}} = \tau^{-2} x_{2\dot{2}},$$

e, portanto,

$$x' = x, \qquad y' = y,$$

$$z' = \frac{\tau^2 x_{1\dot{1}} - \tau^{-2} x_{2\dot{2}}}{2} = \frac{1}{2}(\tau^2+\tau^{-2}).z + \frac{1}{2}(\tau^2-\tau^{-2}).ct,$$

$$ct' = \frac{\tau^2 x_{1\dot{1}} + \tau^{-2} x_{2\dot{2}}}{2} = \frac{1}{2}(\tau^2-\tau^{-2}).z + \frac{1}{2}(\tau^2+\tau^{-2}).ct .$$

Chega-se a (49), como se desejava. O processo utilizado em α)) e β)) mostra que duas matrizes de L_2, iguais e de sinais contrários, levam à mesma transformação de Lorentz. O estudo completo do homomorfismo $L_2 \sim \mathcal{L}$ resulta procurando os elementos de L_2 que levam à identidade em $\mathcal{L}$. De $x' = x$, $y' = y$, $z' = z$, $ct' = ct$ conclui-se

$$x'_{2\dot{1}} = x_{2\dot{1}}, \quad x'_{1\dot{2}} = x_{1\dot{2}}, \quad x'_{1\dot{1}} = x_{1\dot{1}}, \quad x'_{2\dot{2}} = x_{2\dot{2}}.$$

Deve ser então, formalmente,

$$\begin{aligned} \overset{1}{u}'\overset{\dot{1}}{u}' &= (\overset{1}{u}\alpha + \overset{2}{u}\gamma)(\overset{\dot{1}}{u}\overline{\alpha} + \overset{\dot{2}}{u}\overline{\gamma}) = \overset{1}{u}\overset{\dot{1}}{u}, \\ \overset{1}{u}'\overset{\dot{2}}{u}' &= (\overset{1}{u}\alpha + \overset{2}{u}\gamma)(\overset{\dot{1}}{u}\overline{\beta} + \overset{\dot{2}}{u}\overline{\delta}) = \overset{1}{u}\overset{\dot{2}}{u}, \\ \overset{2}{u}'\overset{\dot{1}}{u}' &= (\overset{1}{u}\beta + \overset{2}{u}\delta)(\overset{\dot{1}}{u}\overline{\alpha} + \overset{\dot{2}}{u}\overline{\gamma}) = \overset{2}{u}\overset{\dot{1}}{u}, \\ \overset{2}{u}'\overset{\dot{2}}{u}' &= (\overset{1}{u}\beta + \overset{2}{u}\delta)(\overset{\dot{1}}{u}\overline{\beta} + \overset{\dot{2}}{u}\overline{\delta}) = \overset{2}{u}\overset{\dot{2}}{u}, \end{aligned} \qquad (50)$$

ou seja, atendendo à primeira e à última das relações anteriores,

$$\alpha\overline{\alpha} = 1, \quad \gamma\overline{\gamma} = 0, \quad \beta\overline{\beta} = 0, \quad \delta\overline{\delta} = 1, \qquad (\text{com } \alpha\delta = 1),$$

donde se tira

$$\alpha = \overline{\delta} = e^{i\varphi}.$$

Servindo-nos das relações intermediárias (50), vem

$$\alpha\overline{\delta} = \delta\overline{\alpha} = 1, \qquad \text{ou} \qquad \alpha^2 = \delta^2 = 1,$$

e, finalmente,

$$\alpha = \pm 1, \quad \delta = \pm 1, \quad \text{com correspondência dos sinais.}$$

Cada transformação de Lorentz corresponde a duas matrizes de L_2, iguais e de sinais contrários.

γ)) - Como uma rotação complexa leva a duas matrizes de L_2, iguais e de sinais contrários, passa-se duma rotação complexa, por intermédio de L_2, a uma transformação de Lorentz. Inversamente, duma transformação de Lorentz, passa-se a duas matrizes de L_2, iguais e de sinais contrários, e, portanto a uma rotação complexa.

§)) - Tomemos, em $\mathcal{L}$, a transformação (37). As 3 primeiras igualdades definem uma rotação real do espaço ordinário de ângulos θ, φ, ψ. Em L_2 encontram-se dois elementos de U_2 que, em seguida, na representação $U_2 \sim R$, fazem passar à mesma rotação do espaço ordinário. Se tomarmos, em $\mathcal{L}$, uma transformação (36), com a forma (49), passa-se, em L_2, às fórmulas (49'). Depois, em $L_2 \to R_c$, passa-se a (32''), que aqui é

$$a' = \frac{\tau^2+\tau^{-2}}{2}\,a + i\,\frac{\tau^{-2}-\tau^2}{2}\,b = \frac{a}{\sqrt{1-\beta^2}} + \frac{i\beta b}{\sqrt{1-\beta^2}},$$

$$b' = i\,\frac{\tau^2-\tau^{-2}}{2}\,a + \frac{\tau^2+\tau^{-2}}{2}\,b = -\frac{i\beta a}{\sqrt{1-\beta^2}} + \frac{b}{\sqrt{1-\beta^2}},$$

$$c' = c,$$

ou seja precisamente (39).

Para acabarmos o §, resta demonstrar que uma transformação G do grupo próprio de Lorentz se pode escrever sob a forma

$$G = R' E S',^{(1)} \qquad (51)$$

onde E é uma transformação especial (36) e R' e S' são do tipo (37). Se (51) é possível, é igualmente possível a relação

$$E = R'^{-1} G\, S'^{-1} = RGS, \qquad (R = R'^{-1}, \quad S = S'^{-1}),$$

e reciprocamente. Vamos provar esta última. Utilizaremos as seguintes notações:

$$G = (a_{lR}), \qquad E = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e_{33} & e_{34} \\ 0 & 0 & e_{43} & e_{44} \end{pmatrix} = (e_{lR}),$$

(1) Cfr. R. Luís Gomes, "A teoria da relatividade", Lisboa, 1938, pgs. 50 e 51.

$$R = (r_{lR}) = \begin{pmatrix} r_{11} & r_{12} & r_{13} & 0 \\ r_{21} & r_{22} & r_{23} & 0 \\ r_{31} & r_{32} & r_{33} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad S = (s_{lR}) = \begin{pmatrix} s_{11} & s_{12} & s_{13} & 0 \\ s_{21} & s_{22} & s_{23} & 0 \\ s_{31} & s_{32} & s_{33} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

e, dum modo geral,

$$G = \begin{pmatrix} G_{11} & G_{12} \\ G_{21} & G_{22} \end{pmatrix}, \qquad G_{11} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix},$$

$$G = \begin{pmatrix} a_{14} \\ a_{24} \\ a_{34} \end{pmatrix}, \qquad G_{21} = (a_{41}\ a_{42}\ a_{43}), \qquad G_{22} = (a_{44}).$$

Tem-se, assim,

$$RGS = \begin{pmatrix} R_{11} G_{11} S_{11} & R_{11} G_{12} \\ G_{21} S_{11} & G_{22} \end{pmatrix}.$$

O número dos r_{lR} independentes é de 3, assim como o dos s_{lR}. Determinaremos essas 6 quantidades independentes pelas condições seguintes: pondo $RGS = \mathfrak{S} = (\theta_{jm})$, far-se-á:

$$\theta_{12} = \theta_{13} = \theta_{14} = 0, \qquad \theta_{21} = \theta_{23} = \theta_{24} = 0.$$

Vamos verificar directamente que RGS aparece então, precisamente, sob a forma $\mathfrak{S} = E$. Em primeiro lugar, $\mathfrak{S} = (\theta_{ij})$ é uma matriz do grupo próprio de Lorentz, de modo que são válidas as igualdades (34), que aqui se escreverão

$$\begin{cases} \Theta_{11}^2 + \Theta_{31}^2 - \Theta_{41}^2 = 1, \\ \Theta_{22}^2 + \Theta_{32}^2 - \Theta_{42}^2 = 1, \\ \Theta_{33}^2 - \Theta_{43}^2 = 1, \\ \Theta_{34}^2 - \Theta_{44}^2 = -1, \end{cases} \qquad \begin{cases} \Theta_{31}\Theta_{32} - \Theta_{41}\Theta_{42} = 0, \\ \Theta_{31}\Theta_{33} - \Theta_{41}\Theta_{43} = 0, \\ \Theta_{31}\Theta_{34} - \Theta_{41}\Theta_{44} = 0, \\ \Theta_{32}\Theta_{33} - \Theta_{42}\Theta_{43} = 0, \\ \Theta_{32}\Theta_{34} - \Theta_{42}\Theta_{44} = 0, \\ \Theta_{33}\Theta_{34} - \Theta_{43}\Theta_{44} = 0. \end{cases} \tag{52}$$

Podemos juntar a relação que exprime ser igual à unidade o determinante $|\Theta| = \Delta$:

$$\Delta = \Theta_{11}\Theta_{22}(\Theta_{33}\Theta_{44} - \Theta_{43}\Theta_{34}) = 1. \tag{53}$$

Como é $\Theta_{44} = a_{44}$, vamos exprimir os Θ_{ij} em Θ_{44}. Vem

$$\Theta_{44} = \Theta_{44}, \qquad \Theta_{34} = \pm\sqrt{\Theta_{44}^2 - 1}.$$

A última relação (52) da direita e a penúltima da esquerda dão

$$\Theta_{33} = \pm\Theta_{44}, \qquad \Theta_{43} = \pm\sqrt{\Theta_{44}^2 - 1}.$$

A penúltima e ante-penúltima das relações da direita em (52) mostram que deve ter-se, atendendo a (53),

$$\Theta_{32} = \Theta_{42} = 0.$$

Anàlogamente, será

$$\Theta_{31} = \Theta_{41} = 0.$$

Por consequência, valem as relações

$$\Theta_{11}^2 = 1, \quad \Theta_{22}^2 = 1.$$

A igualdade (53) mostra agora que deve tomar-se

$$\Theta_{33} = \pm\Theta_{44}, \qquad \Theta_{34} = \pm\Theta_{43},$$

com correspondência dos sinais. É evidente que podemos escolher R e S de modo que seja $\Theta_{11} = \Theta_{22} = 1$. Nessas condições, (53) leva a concluir

$$\Theta_{33}\Theta_{44} - \Theta_{43}\Theta_{34} = 1, \qquad \Theta_{33} = \Theta_{44}, \qquad \Theta_{43} = \Theta_{34}.$$

A matriz Θ, como se deseja, é a matriz E. Supondo $\Theta_{44} = \frac{1}{\sqrt{1-\beta^2}}$, vem

$$\Theta_{33} = \frac{1}{\sqrt{1-\beta^2}}, \qquad \Theta_{43} = \Theta_{34} = \pm\sqrt{\frac{1}{1-\beta^2} - 1} = \pm\frac{\beta}{\sqrt{1-\beta^2}}.$$

15) <u>O grupo completo de Lorentz</u> - Diz-se <u>grupo completo de Lorentz</u>, $\mathcal{G}$, o grupo gerado pelo grupo próprio $\mathcal{L}$ e pela "reflexão"

$$x' = -x, \quad y' = -y, \quad z' = -z, \quad t' = t,$$

que designaremos com S. É claro que $\mathcal{G}$ também deixa invariante a forma quadrática $x^2 + y^2 + z^2 - c^2t^2$, e é precisamente caracterizado por esse facto.

Uma representação de $\mathcal{G}$ obtém-se como vai ver-se. Consideremos as seguintes transformações

$$\begin{cases} \overset{1}{u}' = \overset{1}{u}\alpha + \overset{2}{u}\gamma, & (\alpha\delta - \beta\gamma = \bar{\alpha}\bar{\delta} - \bar{\beta}\bar{\gamma} = 1) \\ \overset{2}{u}' = \overset{1}{u}\beta + \overset{2}{u}\delta, \\ \overset{1}{v}' = \overset{1}{v}\bar{\delta} - \overset{2}{v}\bar{\beta}, \\ \overset{2}{v}' = -\overset{1}{v}\bar{\gamma} + \overset{2}{v}\bar{\alpha}. \end{cases} \tag{54}$$

Para as escrever, tomam-se o grupo especial L_2, as transformações (40) e (41), e, em seguida, põe-se

$$\overset{1}{Y} = -\overset{2}{u}\,, \qquad \overset{2}{Y} = \overset{1}{u}\,.$$

Feito isto, consideremos o espaço a 4 dimensões ($\overset{1}{u}\overset{1}{Y}$, $\overset{1}{u}\overset{2}{Y}$, $\overset{2}{u}\overset{1}{Y}$, $\overset{2}{u}\overset{2}{Y}$) e as transformações lineares deste espaço formalmente definidas por (54). A um vector

$$\mathscr{C} = \overset{1}{u}\overset{2}{Y}x_{1\dot{1}} - \overset{1}{u}\overset{1}{Y}x_{1\dot{2}} + \overset{2}{u}\overset{2}{Y}x_{2\dot{1}} - \overset{2}{u}\overset{1}{Y}x_{2\dot{2}}$$

far-se-á corresponder um vector

$$\mathscr{C}' = A\mathscr{C} = \overset{1}{u}'\overset{1}{Y}'x_{1\dot{1}} - \cdots = \overset{1}{u}\overset{1}{Y}x'_{1\dot{1}} - \overset{1}{u}\overset{1}{Y}x'_{1\dot{2}} + \overset{2}{u}\overset{1}{Y}x'_{2\dot{1}} - \overset{2}{u}\overset{1}{Y}x'_{2\dot{2}}.$$

As relações que ligam os x'_{lR} aos x_{lR} podem encontrar-se também considerando um vector (42)

$$\mathscr{Z} = \overset{1}{u}\overset{\dot{1}}{u}x_{1\dot{1}} + \overset{1}{u}\overset{\dot{2}}{u}x_{1\dot{2}} + \overset{2}{u}\overset{\dot{1}}{u}x_{2\dot{1}} + \overset{2}{u}\overset{\dot{2}}{u}x_{2\dot{2}}$$

e praticando (40) e (41). Este facto prova que, se pusermos

$$x = \frac{x_{2\dot{1}} + x_{1\dot{2}}}{2}\,, \qquad y = -\,i\,\frac{x_{2\dot{1}} - x_{1\dot{2}}}{2}\,,$$

$$z = \frac{x_{1\dot{1}} - x_{2\dot{2}}}{2}\,, \qquad ct = \frac{x_{1\dot{1}} + x_{2\dot{2}}}{2}\,,$$

fazemos corresponder a cada matriz de 4ª ordem definida em (54) uma transformação do grupo próprio de Lorentz. O grupo de matrizes de (54) é isomorfo do grupo L_2, de modo que se recai na representação biforme já estudada $\mathscr{L} \sim L_2$.

Relativamente à reflexão S, vamos fazer-lhe corresponder a matriz de 4ª ordem, S, definida pelas igualdades

$$S\,\overset{1}{u} = i\,\overset{1}{Y}\,, \quad S\,\overset{2}{u} = i\,\overset{2}{Y}\,, \quad S\,\overset{1}{Y} = i\,\overset{1}{u}\,, \quad S\,\overset{2}{Y} = i\,\overset{2}{u}\,. \qquad (55)$$

Virá, então,

$$S\mathscr{C} = \mathscr{C}' = -\,\overset{2}{u}\overset{1}{Y}x_{1\dot{1}} + \overset{1}{u}\overset{1}{Y}x_{1\dot{2}} - \overset{2}{u}\overset{2}{Y}x_{2\dot{1}} + \overset{1}{u}\overset{2}{Y}x_{2\dot{2}}\,,$$

e, por consequência,

$$x'_{1\dot{1}} = x_{2\dot{2}}\,, \quad x'_{1\dot{2}} = -\,x_{1\dot{2}}\,, \quad x'_{2\dot{1}} = -\,x_{2\dot{1}}\,, \quad x'_{2\dot{2}} = x_{1\dot{1}}\,,$$

$$x' = \frac{x'_{2\dot{1}} + x'_{1\dot{2}}}{2} = -\,\frac{x_{2\dot{1}} + x_{1\dot{2}}}{2} = -\,x\,,$$

$$y' = -\,y\,, \qquad z' = -\,z\,, \qquad ct' = \frac{x'_{1\dot{1}} + x'_{2\dot{2}}}{2} = \frac{x_{2\dot{2}} + x_{1\dot{1}}}{2} = ct.$$

A matriz que figura em (55) é aceitável como representante de S. Uma representação de $\mathscr{L}$ é, assim, a seguinte: a cada transformação do grupo próprio de Lorentz (à qual no § anterior se fazia corresponder a matriz de 2ª ordem de (40)) faz-se corresponder uma das matrizes de 4ª ordem

$$\begin{pmatrix} \alpha & \beta & 0 & 0 \\ \gamma & \delta & 0 & 0 \\ 0 & 0 & \bar{\delta} & -\bar{\gamma} \\ 0 & 0 & -\bar{\beta} & \bar{\alpha} \end{pmatrix}, \qquad \begin{pmatrix} -\alpha & -\beta & 0 & 0 \\ -\gamma & -\delta & 0 & 0 \\ 0 & 0 & -\bar{\delta} & \bar{\gamma} \\ 0 & 0 & \bar{\beta} & -\bar{\alpha} \end{pmatrix},$$

e à "reflexão" S uma das matrizes

$$S \rightarrow \begin{pmatrix} 0 & 0 & i & 0 \\ 0 & 0 & 0 & i \\ i & 0 & 0 & 0 \\ 0 & i & 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 & -i & 0 \\ 0 & 0 & 0 & -i \\ -i & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \end{pmatrix}.$$

Na representação biforme assim obtida tem lugar a relação

$$S^2 = -\,U_4 = -\,(\text{matriz unidade de 4ª ordem}).$$

Obtém-se uma representação de $\mathscr{L}$, na qual $S^2 = U_4$, mantendo na

representação anterior a correspondência relativa ao grupo próprio e multiplicando por -i as matrizes correspondentes à reflexão:

$$S \to \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

16) Espinores - Voltemos ao espaço $(\overset{1}{u},\overset{2}{u})$ e às transformações

$$\begin{cases} \overset{1}{u}' = \overset{1}{u}\alpha + \overset{2}{u}\gamma, \\ \overset{2}{u}' = \overset{1}{u}\beta + \overset{2}{u}, \end{cases} \qquad \alpha\delta - \beta\gamma = 1. \tag{56}$$

Um vector $\mathcal{C} = \overset{1}{u}x_1 + \overset{2}{u}x_2$ transforma-se no vector $\mathcal{C}'$ de componentes

$$\begin{cases} x_1' = \alpha x_1 + \beta x_2, \\ x_2' = \gamma x_1 + \delta x_2. \end{cases} \tag{57}$$

O vector $\mathcal{C}$, ou o sistema de números (x_1,x_2) sujeitos à variância (57), diz-se um espinor de 1ª ordem. Se considerarmos o espaço conjugado $(\overset{1}{\bar{u}},\overset{2}{\bar{u}})$ e as transformações conjugadas de (56):

$$\begin{cases} \overset{1}{\bar{u}}' = \overset{1}{\bar{u}}\,\bar{\alpha} + \overset{2}{\bar{u}}\,\bar{\gamma}, \\ \overset{2}{\bar{u}}' = \overset{1}{\bar{u}}\,\bar{\beta} + \overset{2}{\bar{u}}\,\bar{\delta}, \end{cases} \qquad \bar{\alpha}\,\bar{\delta} - \bar{\beta}\,\bar{\gamma} = 1,$$

um vector $\bar{\mathcal{C}} = \overset{1}{\bar{u}}\,x_1 + \overset{2}{\bar{u}}\,x_2$ é ainda um espinor de 1ª ordem, conjugado do anterior. É costume tomar-se antes o sistema $(x_{\dot{1}},x_{\dot{2}})$, cuja variância é definida pelas igualdades

$$\begin{cases} x_{\dot{1}}' = \bar{\alpha}\,x_{\dot{1}} + \bar{\beta}\,x_{\dot{2}}, \\ x_{\dot{2}}' = \bar{\gamma}\,x_{\dot{1}} + \bar{\delta}\,x_{\dot{2}}. \end{cases} \tag{58}$$

Ponhamos agora

$$\underset{1}{v} = -\overset{\dot{2}}{\bar{u}}, \qquad \underset{2}{v} = \overset{\dot{1}}{\bar{u}},$$
$$\bar{\mathcal{C}} = \overset{\dot{1}}{\bar{u}}\,x_{\dot{1}} + \overset{\dot{2}}{\bar{u}}\,x_{\dot{2}} = \underset{1}{v}\,x^{\dot{1}} + \underset{2}{v}\,x^{\dot{2}}.$$

Tem-se imediatamente

$$x^{\dot{1}} = -x_{\dot{2}}, \qquad x^{\dot{2}} = x_{\dot{1}},$$

com a variância

$$\begin{cases} x^{\dot{1}'} = \bar{\delta}\,x^{\dot{1}} - \bar{\gamma}\,x^{\dot{2}}, \\ x^{\dot{2}'} = -\bar{\beta}\,x^{\dot{1}} + \bar{\alpha}\,x^{\dot{2}}. \end{cases} \tag{58'}$$

Diz-se que os números $(x^{\dot{1}},x^{\dot{2}})$ dão uma representação contravariante do espinor de representação covariante $(x_{\dot{1}},x_{\dot{2}})$. A expressão $x_{\dot{1}}x^{\dot{1}} + x_{\dot{2}}x^{\dot{2}}$ é invariante. É claro que as relações

$$\underset{1}{v} = -\overset{2}{\bar{u}}, \qquad \underset{2}{v} = \overset{1}{\bar{u}},$$

levam também da representação covariante do espinor (x_1,x_2) à sua representação contravariante pelo sistema (x^1, x^2), com

$$x^{1'} = \delta x^1 - \gamma x^2,$$
$$x^{2'} = -\beta x^1 + \alpha x^2.$$

Passa-se, em seguida, aos espinores de 2ª ordem (com 4 componentes), considerando espaços a 4 dimensões de qualquer das bases:

$$(\overset{1}{u}\,\overset{1}{u},\ \overset{1}{u}\,\overset{2}{u},\ \overset{2}{u}\,\overset{1}{u},\ \overset{2}{u}\,\overset{2}{u});\quad (\overset{1}{u}\,\overset{\dot{1}}{u},\ \overset{1}{u}\,\overset{\dot{2}}{u},\ \overset{2}{u}\,\overset{\dot{1}}{u},\ \overset{2}{u}\,\overset{\dot{2}}{u});$$

$$(\overset{\dot{1}}{u}\,\overset{1}{u},\ \overset{\dot{1}}{u}\,\overset{2}{u},\ \overset{\dot{2}}{u}\,\overset{1}{u},\ \overset{\dot{2}}{u}\,\overset{2}{u});\quad (\overset{\dot{1}}{u}\,\overset{\dot{1}}{u},\ \overset{\dot{1}}{u}\,\overset{\dot{2}}{u},\ \overset{\dot{2}}{u}\,\overset{\dot{1}}{u},\ \overset{\dot{2}}{u}\,\overset{\dot{2}}{u}).$$

No primeiro espaço tem-se um vector

$$\mathcal{C} = \overset{1}{u}\,\overset{1}{u}\,x_{11} + \overset{1}{u}\,\overset{2}{u}\,x_{12} + \overset{2}{u}\,\overset{1}{u}\,x_{21} + \overset{2}{u}\,\overset{2}{u}\,x_{22}.$$

As componentes $x_{\lambda\mu}$ definem um espinor de 2ª ordem. Não há inconsequência, se o espinor se considerar simétrico: $x_{12} = x_{21}$. Pode também considerar-se como tendo apenas 3 componentes, imaginando o espaço a 3 dimensões $(\overset{1}{u}\,\overset{1}{u},\ \overset{1}{u}\,\overset{2}{u},\ \overset{2}{u}\,\overset{2}{u})$ e estudando a variância dos coeficientes x_{lR} da expressão

$$\overset{1}{u}\,\overset{1}{u}\,x_{11} + \overset{1}{u}\,\overset{2}{u}\,x_{12} + \overset{2}{u}\,\overset{2}{u}\,x_{22},$$

quando $\overset{1}{u}$ e $\overset{2}{u}$ se sujeitam à variância (56). Os coeficientes x_1y_2, $x_1y_2 + x_2y_1$, x_2y_2, da expressão $(\overset{1}{u}\,x_1 + \overset{2}{u}\,x_2)(\overset{1}{u}\,y_1 + \overset{2}{u}\,y_2)$ têm a variância de x_{11}, x_{12}, x_{22}. O mesmo se diz dum espinor simétrico $x_{\lambda\mu}$, que se considera igualmente com 3 componentes.

Tomemos agora um espinor de 2ª ordem de componentes $x_{\lambda\dot{\mu}}$. Foi estudado no § 14, onde se viu que a sua variância era a mesma que a das quantidades

$$ct + z,\qquad x - iy,\qquad x + iy,\qquad ct - z.$$

em face das transformações de Lorentz correspondentes de (56). Um exemplo de espinor $x_{\lambda\dot{\mu}}$ é dado pelo produto de dois espinores (x_λ), $(y_{\dot{\mu}})$, produto que terá as componentes $x_1y_{\dot{1}}$, $x_1y_{\dot{2}}$, $x_2y_{\dot{1}}$, $x_2y_{\dot{2}}$. Não se distingue entre um espinor $x_{\lambda\dot{\mu}}$ e um espinor $x_{\dot{\lambda}\mu} = (x_{\dot{1}1}, x_{\dot{2}1}, x_{\dot{1}2}, x_{\dot{2}2})$, pelo simples facto de as fórmulas de transformação serem as mesmas.

Existem outras importantes regras de composição dos espinores, além da da soma de espinores do mesmo tipo e da do produto que acaba de referir-se. Consideremos, por ex., uma expressão da forma

$$\sum_{\dot{\mu}} x_{\lambda\dot{\mu}}\, y^{\dot{\mu}},$$

e estudemos a sua variância em face de (56) [maneira abreviada de falar de (57), (58) e (58')]. Basta estudar a variância de

$$\sum_{\dot{\mu}} x_\lambda\, z_{\dot{\mu}}\, y^{\dot{\mu}} = x_\lambda \sum_{\dot{\mu}} z_{\dot{\mu}}\, y^{\dot{\mu}}.$$

Como o último somatório é invariante, podemos escrever

$$\eta_\lambda = \sum_{\dot{\mu}} x_{\lambda\dot{\mu}} y^{\dot{\mu}}, \tag{59}$$

definindo, pois, um espinor (η_1, η_2). Sob a forma de igualdade de matrizes, podemos pôr

$$\begin{pmatrix}\eta_1\\ \eta_2\end{pmatrix} = \begin{pmatrix}x_{1\dot{1}} & x_{1\dot{2}}\\ x_{2\dot{1}} & x_{2\dot{2}}\end{pmatrix}\begin{pmatrix}y^{\dot{1}}\\ y^{\dot{2}}\end{pmatrix}.$$

Tira-se daqui

$$\begin{pmatrix}y^{\dot{1}}\\ y^{\dot{2}}\end{pmatrix} = \frac{1}{\Delta}\begin{pmatrix}x_{2\dot{2}} & -x_{1\dot{2}}\\ -x_{2\dot{1}} & x_{1\dot{1}}\end{pmatrix}\begin{pmatrix}\eta_1\\ \eta_2\end{pmatrix},$$

onde Δ é o determinante da matriz

$$\mathcal{U} = \begin{pmatrix}x_{1\dot{1}} & x_{1\dot{2}}\\ x_{2\dot{1}} & x_{2\dot{2}}\end{pmatrix}.$$

Ponhamos

$$\mathcal{U}' = \frac{1}{\Delta}\begin{pmatrix}x_{2\dot{2}} & -x_{1\dot{2}}\\ -x_{2\dot{1}} & x_{1\dot{1}}\end{pmatrix},\quad \begin{pmatrix}y^{\dot{1}}\\ y^{\dot{2}}\end{pmatrix} = \mathcal{U}'\begin{pmatrix}\eta_1\\ \eta_2\end{pmatrix};$$

como Δ é um invariante em face de (57) e de (58), vê-se que as igualdades

$$\xi^{\dot\mu} = \sum_{\lambda} \chi^{\dot\mu\lambda}\, x_{\lambda}\,, \qquad (60)$$

nas quais

$$\chi^{\dot1\dot1} = x_{2\dot2}\,, \quad \chi^{\dot1\dot2} = -x_{1\dot2}, \quad \chi^{\dot2\dot1} = -x_{2\dot1}, \quad \chi^{\dot2\dot2} = x_{1\dot1},$$

estão em correspondência com (59), permitindo definir um espinor $(\xi^{\dot1}, \xi^{\dot2})$. A interpretação dos $\chi^{\dot\lambda\dot\mu}$ como correspondentes dum espinor resulta simplesmente. Escrevendo

$$\underset{1}{v}\,\underset{1}{v}\,\chi^{\dot1\dot1} + \underset{1}{v}\,\underset{2}{v}\,\chi^{\dot1\dot2} + \underset{2}{v}\,\underset{1}{v}\,\chi^{\dot2\dot1} + \underset{2}{v}\,\underset{2}{v}\,\chi^{\dot2\dot2},$$

a variância dos coeficientes é a mesma que a dos coeficientes do produto

$$(\underset{1}{v}\,x^{\dot1} + \underset{2}{v}\,x^{\dot2})\;(\underset{1}{v}\,x^{1} + \underset{2}{v}\,x^{2}),$$

e, portanto, que a dos números

$$x_{\dot2}x_{2}\,, \quad -x_{\dot2}x_{1}, \quad -x_{\dot1}x_{2}\,, \quad x_{\dot1}x_{1}\,,$$

donde se conclui o que se deseja.

Consideremos agora as igualdades

$$\mathcal{U} = \begin{pmatrix} x_{1\dot1}\, x_{1\dot2} \\ x_{2\dot1}\, x_{2\dot2} \end{pmatrix} = \begin{pmatrix} ct+z & x-iy \\ x+iy & ct-z \end{pmatrix} = x\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + y\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + z\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + ct\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\mathcal{V} = \begin{pmatrix} \chi^{\dot1\dot1} & \chi^{\dot1\dot2} \\ \chi^{\dot2\dot1} & \chi^{\dot2\dot2} \end{pmatrix} = \begin{pmatrix} x_{2\dot2} & -x_{1\dot2} \\ -x_{2\dot1} & x_{1\dot1} \end{pmatrix} = \begin{pmatrix} ct-z & -x+iy \\ -x-iy & ct+z \end{pmatrix} = x\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} +$$

$$+ y\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} + z\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} + ct\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

e utilizemos as matrizes de Pauli

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad (61)$$

que permitem pôr

$$\mathcal{U} = x\,\sigma_x + y\,\sigma_y + z\,\sigma_z + ct\,\sigma_0\,,$$

$$\mathcal{V} = -x\sigma_x - y\,\sigma_y - z\sigma_z + ct\,\sigma_0\,.$$

Na teoria dos espinores, os elementos $\sigma_{x\lambda\dot\mu}$, $\sigma_{y\lambda\dot\mu}$, $\sigma_{z\lambda\dot\mu}$, $\sigma_{0\lambda\dot\mu}$ são números determinados, fixados em (61) como elementos de matrizes (linha λ, coluna $\dot\mu$). Pondo

$$-\sigma_x = \sigma'_x\,, \quad -\sigma_y = \sigma'_y\,, \quad -\sigma_z = \sigma'_z\,, \quad \sigma_0 = \sigma'_0\,,$$

os elementos $\sigma_x'^{\dot\lambda\dot\mu}$, $\sigma_y'^{\dot\lambda\dot\mu}$, $\sigma_z'^{\dot\lambda\dot\mu}$, $\sigma_0'^{\dot\lambda\dot\mu}$ são igualmente números bem determinados. E tem-se, com $x = Y^1$, $y = Y^2$, $z = Y^3$, $ct = Y^0$,

$$x_{\lambda\dot\mu} = \sum_{k} Y^k \sigma_{k\lambda\dot\mu}\,, \qquad x^{\dot\lambda\dot\mu} = \sum_{k} Y^k \sigma_k'^{\dot\lambda\dot\mu}\,, \qquad (k = 0, 1, 2, 3),$$

de sorte que (59) e (60) podem escrever-se

$$\eta_{\lambda} = \sum_{\dot\mu}\sum_{k} Y^k \sigma_{k\lambda\dot\mu} y^{\dot\mu}, \qquad \xi^{\dot\mu} = \sum_{\lambda}\sum_{k} Y^k\, \sigma_k'^{\dot\mu\lambda}\, x_{\lambda}\,. \qquad (62)$$

Este resultado permite enunciar o seguinte

Teorema:- Dadas as relações (62), nas quais os $\sigma_{k\lambda\dot\mu}$ e os $\sigma_k'^{\dot\mu\lambda}$ são números determinados (conhecidos), se os Y^k se su-

jeitam à variância prescrita por uma transformação do grupo próprio de Lorentz e os η_λ, $y^{\dot\mu}$, $\xi^{\dot\mu}$, x_λ à variância correspondente, prescrita por uma das transformações do grupo linear representante daquela transformação na representação estudada no § 14, as referidas relações ficam individualmente invariantes.

Passemos, por fim, ao grupo completo de Lorentz e à sua representação estudada no § anterior. Efectuemos em (62) tanto sobre os Y^R como sobre os η_λ, $y^{\dot\mu}$, $\xi^{\dot\mu}$, x_λ a transformação prescrita pela "reflexão" S.0 efeito de S sobre $\xi^{\dot\mu}$,... resulta do modo seguinte: é, por ex.,

$$S(\sum_1 x^{\dot i} + \sum_2 x^{\dot i}) = \overset{1}{u}\, x^{\dot i} + \overset{2}{u}\, x^{\dot i} = \overset{1}{u}\, x_1 + \overset{2}{u}\, x_2,$$

de sorte que

$$S\,\xi^{\dot i} = \eta_1, \quad S\,\xi^{\dot 2} = \eta_2; \quad S\,x_1 = y^{\dot i}, \quad S\,x_2 = y^{\dot 2}.$$

Deste modo, tomemos

$$\eta_1 = \sum_{\dot\mu}\sum_R Y^R \sigma_{R1\dot\mu}\, y^{\dot\mu} = Y^1\sigma_{11\dot i}\, y^{\dot i} + Y^1\sigma_{11\dot 2}\, y^{\dot 2} + Y^2\sigma_{21\dot i}\, y^{\dot i} +$$

$$+ Y^2\sigma_{21\dot 2} y^{\dot 2} + Y^3\sigma_{31\dot i}\, y^{\dot i} + Y^3\sigma_{31\dot 2} y^{\dot 2} + Y^0\sigma_{01\dot i}\, y^{\dot i} + Y^0\sigma_{01\dot 2} y^{\dot 2},$$

e apliquemos S a ambos os membros. Vem

$$\xi^{\dot i} = - Y^1\sigma_1^{\prime\dot i 1}\, x_1 - Y^1\sigma_1^{\prime\dot i 1}\, x_2 - Y^2\sigma_2^{\prime\dot i 1}\, x_1 - Y^2\sigma_2^{\prime\dot 2 1}\, x_2 - Y^3\sigma_3^{\prime\dot i 1}\, x_1 -$$

$$- Y^3\sigma_3^{\prime\dot 2 1}\, x_2 + Y^0\sigma_0^{\prime\dot i 1}\, x_1 + Y^0\sigma_0^{\prime\dot 2 1}\, x_2 .$$

Os dois membros são efectivamente iguais, por ser

$$\xi^{\dot i} = \eta_1, \qquad x_1 = y^{\dot i}, \quad x_2 = y^{\dot 2},$$

$$\sigma_1^{\prime\dot i 1} = -\sigma_{11\dot i} = 0; \quad \sigma_1^{\prime\dot i 2} = -\sigma_{11\dot 2} = -1; \quad \sigma_2^{\prime\dot i 1} = -\sigma_{21\dot i} = 0;$$

$$\sigma_2^{\prime\dot i 2} = -\sigma_{21\dot 2} = 1; \quad \sigma_3^{\prime\dot i 1} = -\sigma_{31\dot i} = -1; \quad \sigma_3^{\prime\dot i 2} = -\sigma_{31\dot 2} = 0;$$

$$\sigma_0^{\prime\dot i 1} = \sigma_{01\dot i} = 1; \qquad \sigma_0^{\prime\dot i 2} = \sigma_{01\dot 2} = 0 .$$

Deste modo, mediante uma condição evidente para os números $\sigma_{R\lambda\dot\mu}$, $\sigma_R^{\dot\lambda\mu}$ (precisamente $\sigma_{R\lambda\dot\mu}$ transforma-se em $\sigma_R^{\prime\dot\lambda\mu}$), pode enunciar-se o

Teorema:- As relações (62) ficam globalmente invariantes para o grupo completo de Lorentz.

Damos aqui por terminadas as nossas considerações elementares sobre a teoria dos espinores. Para estudos mais completos, há a literatura especializada.(1)

(1) Por ex. E.Cartan, "La theorie des spineurs", Paris, 1938, em dois tomos.

Capítulo XI

Corpos de decomposição das álgebras. Teoria de Galois[1]

1) Definições gerais - Dada uma álgebra $\mathcal{A}$, sobre $\mathcal{P}$, definimos, no Cap.IX, § 3, uma representação absolutamente irredutível da álgebra, como uma representação irredutível de $\mathcal{A}$, em $\mathcal{P}$, tal que é ainda irredutível a representação de $\mathcal{A}_\Omega$ no corpo algèbricamente fechado $\Omega \supseteq \mathcal{P}$, que a partir dela se define. Uma representação irredutível de $\mathcal{A}$, em $\Delta \supseteq \mathcal{P}$, prolonga-se para uma representação irredutível de $\mathcal{A}_\Delta$, em Δ, e, por isso, tem lugar a definição geral seguinte: uma representação de $\mathcal{A}$, sobre $\mathcal{P}$, em $\Delta \supseteq \mathcal{P}$, diz-se absolutamente irredutível, se for absolutamente irredutível a representação de $\mathcal{A}_\Delta$, em Δ.

Uma representação absolutamente irredutível de $\mathcal{A}$, sobre $\mathcal{P}$, em $\Delta \supseteq \mathcal{P}$, não pode tornar-se redutível, ainda mesmo que se façam ampliações transcendentes do corpo algèbricamente fechado $\Theta \supseteq \Delta$. Basta notar, com efeito, que, sendo

$$\mathcal{A}_\Theta / \mathcal{R} = \Theta_1 + \cdots + \Theta_n, \qquad (\mathcal{R} = \text{radical de } \mathcal{A}_\Theta),$$

onde Θ_t representa um anel completo de matrizes com elementos de Θ, ao passar-se a $\Theta' \supseteq \Theta$, vem

$$\mathcal{A}_{\Theta'} / \mathcal{R}_{\Theta'} = \Theta'_1 + \cdots + \Theta'_n ,$$

onde os Θ'_t são anéis completos de matrizes com elementos de Θ'. O anel cociente do 1º membro é semi-simples e $\mathcal{R}_{\Theta'}$ é o seu radical. As representações irredutíveis de $\mathcal{A}$ em Θ' são ainda

(1) Neste Capítulo regressamos a E.Noether, "Nichtkommutative Algebra". Os resultados expostos sobre corpos de decomposição devem comparar-se com Albert, pgs.56 a 62. Veja-se igualmente, tanto para este Capítulo como para os Capítulos IX e XII, o livro seguinte de van der Waerden: "Gruppen von linearen Transformationen", "Ergebnisse der Mathematik ...", IV Band, 1935, Cap.II.

em número de n, precisamente dos mesmos graus que as representações de $\mathcal{A}$ em Θ e precisamente as mesmas que estas últimas, como se vê recorrendo à decomposição de cada Θ_t em ideais esquerdos simples $\mathfrak{N}_t$ e observando que $(\mathfrak{N}_t)_{\Theta'}$ é ideal esquerdo simples de Θ'_t.

No § 8 do Cap.VII, definimos corpo de decomposição duma álgebra $\mathcal{A}$, sobre $\mathcal{P}$, como um corpo $\Delta \supseteq \mathcal{P}$, tal que $\mathcal{A}_\Delta$ é soma de anéis completos de matrizes com elementos de Δ[1]. Esta definição abrange apenas as álgebras separáveis. Duma maneira geral, diremos: dada uma álgebra $\mathcal{A}$, sobre $\mathcal{P}$, diz-se corpo de decomposição de $\mathcal{A}$ um corpo comutativo $\Delta \supseteq \mathcal{P}$ tal que todas as representações irredutíveis de $\mathcal{A}$ em Δ são absolutamente irredutíveis. Se $\mathcal{A}$ for separável, esta definição coincide com a anterior. Com efeito, se Δ satisfaz à actual definição, pondo

$$\mathcal{A}_\Delta = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n, \qquad (\mathfrak{a}_t = \text{álgebra simples sobre } \Delta),$$

e decompondo $\mathfrak{a}_t$ em ideais esquerdos simples $\mathfrak{N}_t$, ao passar-se ao corpo algèbricamente fechado $\Theta \supseteq \Delta$, o ideal $(\mathfrak{N}_t)_\Theta$ permanece simples. Cada $(\mathfrak{a}_t)_\Theta$ é álgebra simples, e, portanto, anel completo de matrizes do grau r_t com elementos de Θ. O anel $\mathfrak{a}_t$ é também anel completo de matrizes do grau r_t. Como a representação de $\mathcal{A}$, em Δ, pertencente a $\mathfrak{N}_t$, é do grau r_t, o corpo dos endomorfismos de $\mathfrak{N}_t^{(2)}$ não pode deixar de ser isomorfo de Δ. Assim, Δ é corpo de decomposição no antigo sentido. Inversamente, se $\mathcal{A}_\Delta$ é uma soma de anéis completos de matrizes com elementos de Δ, ao passar-se a $\mathcal{A}_\Theta$, conserva-se o número de ideais esquerdos simples da decomposição de $\mathcal{A}_\Delta$, pois se conserva o de cada álgebra simples parcela.

Se $\mathcal{A} = \mathfrak{A}$ é uma álgebra normal simples sobre $\mathcal{P}$, a álgebra $\mathfrak{A}_\Delta$ é normal simples sobre Δ, qualquer que seja a ampliação comutativa Δ, de $\mathcal{P}$. $\mathfrak{A}$ é, pois, álgebra separável, de sorte que um corpo de decomposição duma álgebra normal simples $\mathfrak{A}$, sobre $\mathcal{P}$,

(1) Aqui, como já na linguagem de considerações anteriores, melhor seria dizer: "anéis com a estrutura de anéis completos de matrizes com elementos de corpos isomorfos de Δ".

(2) Cap.VIII, § 16.

isomorfo de $\sum$ relativamente a $\mathcal{P}$. A inversa é ainda verdadeira.

O sub-corpo mínimo de decomposição é corpo de decomposição, se for ampliação de Galois de $\mathcal{P}$, e apenas nesse caso.

Podemos observar, por último, que uma ampliação algèbricamente fechada Ω, de $\mathcal{P}$, contém apenas um corpo de decomposição mínimo de $\sum$, pelas razões a seguir. Seja $\sum_1 \cong \sum$, relativamente a $\mathcal{P}$, um corpo contido em Ω. Pondo $\sum_1 = \mathcal{P}(\alpha_1, \ldots, \alpha_r)$, a ampliação de Galois mínima de $\mathcal{P}$, contendo $\sum_1$ e contida em Ω, é uma ampliação Γ, obtida por adjunção a $\mathcal{P}$ das raizes da equação $\varphi(x) = 0$, com

$$\varphi(x) = \prod_{l=1}^{r} f_l(x), \quad [f_l(x) = 0 \text{ equação irredutível em } \mathcal{P} \text{ a que satisfaz } \alpha_l].$$

Se existisse em Ω outro corpo $\sum_1' = \mathcal{P}(\alpha_1', \ldots, \alpha_r') \cong \sum$, relativamente a $\mathcal{P}$, a ampliação de Galois mínima de $\mathcal{P}$, contendo $\sum_1'$ e contida em Ω, seria uma ampliação Γ' obtida por adjunção a $\mathcal{P}$ das raizes da equação $\varphi'(x) = 0$, com

$$\varphi'(x) = \prod_{l=1}^{r} f_l(x) = \varphi(x).$$

Seria, pois, $\Gamma' = \Gamma$, como se afirmou.

Dos sistemas comutativos (ampliações algébricas comutativas finitas de $\mathcal{P}$) elevar-nos-emos aos sistemas não comutativos que sejam álgebras normais de divisão sobre $\mathcal{P}$. Seja $\mathcal{A}$ uma tal álgebra. Um corpo de decomposição Δ, de $\mathcal{A}$, é também corpo de decomposição do anel de matrizes $\mathcal{A}_m$ (álgebra normal simples sobre $\mathcal{P}$), visto que, supondo $\mathcal{A}_\Delta = \Delta_\varphi$ é também

$$(\mathcal{A}_m)_\Delta = (\mathcal{A} \times \mathcal{P}_m)_\Delta = \mathcal{A}_\Delta \times \Delta_m = \Delta_q \times \Delta_m = \Delta_{qm}.$$

Inversamente, supondo

$$(\mathcal{A}_m)_\Delta = \Delta_\rho = \mathcal{A}_\Delta \times \Delta_m,$$

sabemos que $\mathcal{A}_\Delta$ é álgebra normal simples sobre Δ (pg.164), e, além disso, comutador de Δ_m, em Δ_ρ. Esse comutador (Cap.IX, § 4, corolário 5) é uma álgebra Δ_q.

Teorema 3:- É condição necessária e suficiente, para que a ampliação comutativa finita Δ, de $\mathcal{P}$, seja corpo de decomposição da álgebra normal simples $\mathcal{A} = \mathcal{A}_m$, que a representação directa irredutível única, de grau r, de Δ, em $\mathcal{A}$, seja um corpo Δ^*, sub-corpo comutativo máximo de $\mathcal{A}_r$.

Recordemos, antes da demonstração, um facto muito utilizado no Cap.IX, § 4, 4ª aplicação. Sempre que alí se falou de corpos anti-isomorfos $\mathcal{A}$ e $\mathcal{L}$, com o centro comum $\mathcal{P}$, supoz-se que o anti-isomorfismo deixava invariantes os elementos de $\mathcal{P}$. Só assim se compreende que, dada uma representação recíproca $\mathcal{L}_s$, dum sistema hiper-complexo $\mathcal{H}$, sobre $\mathcal{P}$, no corpo $\mathcal{L}$, se passa, por anti-isomorfismo, para o anel de matrizes $\mathcal{A}_s$, que dará uma representação directa do mesmo sistema $\mathcal{H}$ no corpo $\mathcal{A}$. Posto isto, passemos ao teorema

Δ é sistema hiper-complexo comutativo sobre $\mathcal{P}$. Se $\mathcal{L}$ é anti-isomorfo de $\mathcal{A}$, $\Delta_\mathcal{L} = \Delta \times \mathcal{L} = \mathcal{L} \times \Delta = \mathcal{L}_\Delta$ é álgebra normal simples sobre Δ. A representação irredutível única de Δ em $\mathcal{L}$ (que é também directa por ser Δ comutativo) serve para definir, como se recordou, a representação directa irredutível única de Δ em $\mathcal{A}$. Suporemos, assim, $\Delta \cong \Delta^* \subseteq \mathcal{A}_r$. Admitamos, agora, que Δ é corpo de decomposição de $\mathcal{A}$. Será $\mathcal{A}_\Delta = \Delta_q$. Procuremos o comutador $\bar{\Delta}^*$, de Δ^*, em $\mathcal{A}_r$. Será um corpo

$$\bar{\Delta}^* = \bar{\mathcal{G}}, \text{ com } \bar{\mathcal{G}} \neq \mathcal{F}, \quad \Delta^*_\mathcal{G} = \mathcal{F}_t.$$

Ora $\Delta^*_\mathcal{G}$ é anti-isomorfo de $\Delta_\mathcal{A} = \mathcal{A}_\Delta = \Delta_q$. Portanto, ter-se-á

$$\mathcal{A}_\Delta = \Delta_q \neq \mathcal{F}_t, \qquad \Delta_q \cong \bar{\mathcal{G}}_t = \bar{\Delta}^*_t.$$

Daqui se conclui $t = q$, $\bar{\Delta}^* \cong \Delta$, e, assim, $\bar{\Delta}^* \cong \Delta^*$. O anti-isomorfismo $\Delta_\mathcal{G} \neq \Delta^*_\mathcal{G}$ tem lugar relativamente a $\mathcal{P}$, o mesmo se dizendo, por isso, do isomorfismo $\bar{\Delta}^* \cong \Delta^*$. Como $\Delta^* \subseteq \bar{\Delta}^*$, é válida a igualdade $\bar{\Delta}^* = \Delta^*$, das duas álgebras sobre $\mathcal{P}$. Não pode haver corpo comutativo contido em $\mathcal{A}_r$ que contenha Δ^* visto que um tal corpo estaria contido em $\bar{\Delta}^*$. Inversamente, suponhamos que $\Delta \supseteq \mathcal{P}$ é um corpo comutativo, finito sobre $\mathcal{P}$, tal que a sua representação $\Delta^* \subseteq \mathcal{A}_r$ é corpo comutativo máximo de $\mathcal{A}_r$. O comutador de Δ^*, em $\mathcal{A}_r$, é o próprio Δ^*. Portanto, $\mathcal{A}_\Delta \cong \Delta^*_t \cong \Delta_t$, e, consequentemente, pode supor-se $\mathcal{A}_\Delta = \Delta_t$.

Do Cap.VII,§ 8, sabemos sempre da existência dum corpo Δ como o do teorema que acaba de demonstrar-se. Vê-se agora que um sub-corpo comutativo máximo de $\mathfrak{A}$, contendo $\mathfrak{P}$, está nas condições de Δ. Duma maneira geral, os corpos de decomposição, de grau finito, de $\mathfrak{A} = \mathfrak{A}_m$, são os sub-corpos comutativos máximos das álgebras $\mathfrak{A}_s$, qualquer que seja s [ou corpos isomorfos desses sub-corpos]. Podemos reconhece-lo do modo seguinte: seja $\Delta \cong \mathfrak{A}_s$ um sub-corpo comutativo máximo de $\mathfrak{A}_s$. Se Δ não está mergulhado de modo irredutível, há uma representação irredutível de Δ em $\mathfrak{A}$ que leva a $\Delta \cong \Delta^* \cong \mathfrak{A}_r$. Então, ou Δ^* é sub-corpo comutativo máximo de $\mathfrak{A}_r$, e, portanto, Δ é corpo de decomposição de $\mathfrak{A}$ (e de $\mathfrak{A}_m$), ou existe corpo comutativo Ψ nas condições seguintes: $\Delta^* \cong \Psi \cong \mathfrak{A}_r$. Por ser r divisor de s, podemos mergulhar $\mathfrak{A}_r$ em $\mathfrak{A}_s$ e supor $\Delta \cong \Psi \cong \mathfrak{A}_s$, o que levará a $\Delta = \Psi$. O corpo Δ^* é sempre sub-corpo comutativo máximo de $\mathfrak{A}_r$, como se deseja.

Se construirmos o corpo algèbricamente fechado Ω, sobre $\mathfrak{P}$, que contém Δ, é possível reconhecer, em geral, a existência, em Ω, duma infinidade de corpos não isomorfos, os quais são corpos de decomposição de grau mínimo de $\mathfrak{A}$, contràriamente ao que sucede no caso comutativo. Efectivamente, um sub-corpo comutativo máximo Ψ contido em $\mathfrak{A}_s$ (e contendo $\mathfrak{P}$) tem um correspondente isomorfo (relativamente a $\mathfrak{P}$) em Ω. Qualquer sub-corpo de Ω contendo Ψ é corpo de decomposição de $\mathfrak{A}$, mas um sub-corpo próprio de Ψ não está nessas condições.

Outra observação é esta: seja $\Delta \subset \mathfrak{S} \subset \Omega$, e $\mathfrak{S}$ ampliação finita de Δ; se $\mathfrak{S}^*$ é um corpo, representação irredutível única da ampliação finita $\mathfrak{S}$, de $\mathfrak{P}$, em $\mathfrak{A}$, o grau dessa representação é necessàriamente $\rho \equiv r$. Não pode ter-se $\rho = r$, pois que, de contrário, o corpo isomorfo de Δ, contido em $\mathfrak{S}^*$, não seria sub-corpo máximo de $\mathfrak{A}_r$.

Finalmente, notemos que, dado um corpo comutativo máximo $\Delta^* \cong \mathfrak{A}_r$, que contenha $\mathfrak{P}$, mergulhado de modo irredutível em $\mathfrak{A}_r$, não há sub-anel comutativo de $\mathfrak{A}_r$ que contenha, de modo próprio, o corpo Δ^*, de sorte que este último é também sub-anel comutativo máximo. Reconhece-se este facto, observando que Δ^* contém todas as matrizes comutáveis com os seus elementos.

Tratado o caso das álgebras normais simples, deveríamos passar às álgebras simples, depois a álgebras semi-simples (ou álgebras quaisquer, como veremos). Deixaremos para um § adiante algumas considerações relativas ao problema das álgebras simples, limitando aqui o nosso objectivo a reduzir o problema geral ao de tais álgebras.

Teorema 4:- Um corpo de decomposição (ou de sub-decomposição) duma álgebra qualquer $\mathfrak{F}$, sobre $\mathfrak{P}$, é sempre um corpo de decomposição (ou de sub-decomposição) da álgebra semi-simples $\mathfrak{F}/\mathfrak{R}$, sobre $\mathfrak{P}$. Numa representação irredutível de $\mathfrak{F}$, em $\Delta \cong \mathfrak{P}$, o radical $\mathfrak{R}$, de $\mathfrak{F}$, é representado por matrizes nulas, visto que a referida representação é uma parte da representação irredutível de $\mathfrak{F}_\Delta$, em Δ, e nesta o radical $\mathfrak{R}'$, de $\mathfrak{F}_\Delta$, é representado por matrizes nulas. Ora é $\mathfrak{R} \cong \mathfrak{R}_\Delta \cong \mathfrak{R}'$. Assim, a representação irredutível de $\mathfrak{F}$, em Δ, é representação irredutível de $\mathfrak{F}/\mathfrak{R}$, em Δ. A inversa é também verdadeira.

Teorema 5:- É condição necessária e suficiente, para que $\Delta \cong \mathfrak{P}$ seja corpo de decomposição duma álgebra semi-simples $\mathfrak{F}$, sobre $\mathfrak{P}$, que $\mathfrak{F}_\Delta/\mathfrak{R}'$ ($\mathfrak{R}'$ = radical de $\mathfrak{F}_\Delta$) seja uma soma de anéis completos de matrizes com elementos de Δ. Efectuemos a decomposição

$$\mathfrak{F}_\Delta/\mathfrak{R}' = \mathfrak{a}_1' + \cdots + \mathfrak{a}_s' = (\mathfrak{N}_1 + \mathfrak{N}_1' + \cdots) + (\mathfrak{N}_2 + \mathfrak{N}_2' + \cdots) + \cdots ,$$

onde os $\mathfrak{a}_i'$ são simples e os $\mathfrak{N}_i$ são ideais esquerdos simples dos $\mathfrak{a}_i'$. Se, por hipótese, Δ é corpo de decomposição de $\mathfrak{F}$, a representação irredutível de $\mathfrak{F}$, em Δ, pertencente a $\mathfrak{N}_1$, por ex., permanece irredutível se se considera representação de $\mathfrak{F}$ no corpo algèbricamente fechado $\Omega \cong \Delta$. Portanto, $(\mathfrak{N}_1)_\Omega$ continua ideal esquerdo simples de $(\mathfrak{a}_1')_\Omega$. Os ideais $(\mathfrak{N}_1)_\Omega, (\mathfrak{N}_1')_\Omega, \ldots$ são isomorfos, de modo que $(\mathfrak{a}_1')_\Omega$ é álgebra simples sobre Ω. Tem-se $(\mathfrak{a}_1')_\Omega = \Omega_\rho$, $\mathfrak{a}_1' = \mathfrak{D}_\rho = \mathfrak{D} \times \Delta_\rho$, onde $\mathfrak{D}$ é álgebra de divisão sobre Δ. Em virtude de ser também $(\mathfrak{a}_1')_\Omega = \mathfrak{D}_\Omega \times \Omega_\rho = \Omega_\rho$, vê-se que $\mathfrak{D}_\Omega$ é de 1ª ordem sobre Ω. $\mathfrak{D}$ será de 1ª ordem sobre Δ, isto é, será $\mathfrak{a}_1' = \Delta_\rho$, como se quer. Inversamente, supondo

$$\mathfrak{F}_\Delta/\mathfrak{R}' = \Delta_1 + \cdots + \Delta_s ,$$

onde os Δ_i são anéis completos de matrizes com elementos de Δ, este último é corpo de decomposição de $\mathcal{G}$, pois é corpo de decomposição da álgebra separável $\mathcal{G}_\Delta/\mathcal{R}'$.

Se observarmos que, na demonstração acabada de fazer, não se fez intervir o facto de $\mathcal{G}$ ser semi-simples, podemos dar o seguinte enunciado:

Teorema 5':- É condição necessária e suficiente, para que $\Delta \supseteq \mathcal{P}$ seja corpo de decomposição duma álgebra qualquer $\mathcal{G}$, sobre $\mathcal{P}$, que $\mathcal{G}_\Delta/\mathcal{R}'$ seja uma soma de anéis completos de matrizes com elementos de Δ, ou que esta mesma propriedade tenha lugar para a álgebra $(\mathcal{G}/\mathcal{R})_\Delta/\mathcal{R}''$ [$\mathcal{R}''$ = radical de $(\mathcal{G}/\mathcal{R})_\Delta$].

Continuemos a supor $\mathcal{G}$, de radical $\mathcal{R}$, uma álgebra qualquer sobre $\mathcal{P}$. Escrevamos, como habitualmente,

$$\mathcal{G}/\mathcal{R} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_s = \mathfrak{N}_1 + \cdots + \mathfrak{N}_n .$$

Uma representação irredutível de $\mathcal{G}$ (em $\mathcal{P}$) pertence, por ex., ao ideal esquerdo $\mathfrak{N}_1 \subseteq \mathfrak{a}_1$. Trata-se, assim, duma representação irredutível de $\mathfrak{a}_1$. Se Δ_1 é um corpo de decomposição de $\mathfrak{a}_1$, tem-se

$$(\mathfrak{a}_1)_{\Delta_1}/\mathcal{R}_1 = \Delta_1' + \Delta_1'' + \cdots ,$$

onde os $\Delta\,\Delta$ são anéis completos de matrizes com elementos de Δ_1. Supondo $\Psi \supseteq \Delta_1$, vem

$$\left((\mathfrak{a}_1)_{\Delta_1}/\mathcal{R}_1\right)_\Psi = \mathfrak{P}_1' + \mathfrak{P}_1'' + \cdots = (\mathfrak{a}_1)_\Psi/(\mathcal{R}_1)_\Psi ,$$

onde $(\mathcal{R}_1)_\Psi$ é o radical de $(\mathfrak{a}_1)_\Psi$ e $\mathfrak{P}_1', \ldots$ são anéis completos de matrizes com elementos de Ψ. Vê-se que Ψ é igualmente corpo de decomposição de $\mathfrak{a}_1$. Assim, se Δ_2 for o corpo de decomposição de $\mathfrak{a}_2$, Δ_3 de $\mathfrak{a}_3$, etc., um corpo Δ, que contenha os diferentes Δ_i, é corpo de decomposição de todos os $\mathfrak{a}_i$. Vamos reconhecer que é também corpo de decomposição de $\mathcal{G}/\mathcal{R}$, ou de $\mathcal{G}$. Tem-se, pondo $\mathfrak{a}_i = \mathfrak{a}$,

$$\mathfrak{a}_\Delta/\mathcal{R}_i' = \Delta' + \Delta'' + \cdots , \qquad (i = 1, 2, \ldots, s),$$

onde $\mathcal{R}_i'$ é radical e $\Delta', \ldots$ são anéis completos de matrizes com elementos de Δ. Deste modo, é

$$(\mathcal{G}/\mathcal{R})_\Delta/\mathcal{R}'' = \sum\Delta' + \sum\Delta'' + \cdots ,$$

pois que o radical $\mathcal{R}''$, de $\mathcal{G}_\Delta$, é a soma dos radicais $\mathcal{R}_i'$, dos $(\mathfrak{a}_i)_\Delta$. Podemos enunciar o

Teorema 6:- Um corpo de decomposição duma álgebra $\mathcal{G}$, sobre $\mathcal{P}$, é sempre um corpo de decomposição da álgebra semi-simples $\mathcal{G}/\mathcal{R}$ (teorema 4). Como tal, é corpo de decomposição das álgebras simples em que se decompõe $\mathcal{G}/\mathcal{R}$. Inversamente é sempre possível obter um corpo de decomposição de $\mathcal{G}$ por ampliações sucessivas de corpos de decomposição de álgebras simples. De modo análogo: um corpo de sub-decomposição dum $\mathfrak{a}_i$ (da decomposição de $\mathcal{G}/\mathcal{R}$) é corpo de sub-decomposição de $\mathcal{G}/\mathcal{R}$, e, portanto, de $\mathcal{G}$; e, reciprocamente, um corpo de sub-decomposição de $\mathcal{G}/\mathcal{R}$ é também corpo de sub-decomposição dum $\mathfrak{a}_i$.

Vejamos a última parte do enunciado. Se $\mathcal{G}/\mathcal{R}$ tem o sub-corpo de decomposição Φ, ponhamos

$$\mathcal{G}/\mathcal{R} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_s , \qquad (\mathcal{G}/\mathcal{R})_\Phi = (\mathfrak{a}_1)_\Phi + \cdots + (\mathfrak{a}_s)_\Phi .$$

Representando por $\mathcal{R}'$ o radical de $(\mathcal{G}/\mathcal{R})_\Phi$ e por $\mathcal{R}_i$ o radical de $(\mathfrak{a}_i)_\Phi$, será $\mathcal{R}' = \mathcal{R}_1 + \cdots + \mathcal{R}_s$ e

$$(\mathcal{G}/\mathcal{R})_\Phi/\mathcal{R}' = (\mathfrak{a}_1)_\Phi/\mathcal{R}_1 + \cdots + (\mathfrak{a}_s)_\Phi/\mathcal{R}_s .$$

Como, por hipótese, existe uma representação absolutamente irredutível do 1º membro no corpo Φ, a mesma afirmação tem lugar para uma das parcelas do 2º membro, por ex. $(\mathfrak{a}_1)_\Phi/\mathcal{R}_1$. Daqui se conclui a existência de representação absolutamente irredutível, em Φ, de $(\mathfrak{a}_1)_\Phi$, e, portanto, de $\mathfrak{a}_1$.

3) As classes de álgebras semelhantes. - Regressemos às álgebras normais simples sobre $\mathcal{P}$. Se $\mathcal{A}$, $\mathcal{L}$, $\mathcal{M}$, ... são álgebras normais de divisão equivalentes, sobre $\mathcal{P}$, diremos que as álgebras de matrizes (sobre $\mathcal{P}$) representadas por $\mathcal{A}_r$, $\mathcal{L}_s$, $\mathcal{M}_t$, ... constituem uma classe de álgebras semelhantes sobre $\mathcal{P}$.

Outra classe será constituida por elementos $\mathfrak{A}_r', \mathfrak{L}_s', \ldots$

Teorema 1:- As classes de álgebras semelhantes constituem um grupo abeliano multiplicativo. A operação do grupo é definida do modo que vai ver-se. Ponhamos $\mathfrak{A}_r \times \mathfrak{L}_s' = \mathfrak{A} \times \mathfrak{P}_r \times \mathfrak{L}' \times \mathfrak{P}_s = (\mathfrak{A} \times \mathfrak{L}') \times \mathfrak{P}_{rs}$. Como $\mathfrak{A} \times \mathfrak{L}'$ é uma álgebra normal simples sobre $\mathfrak{P}$, ponhamos $\mathfrak{A} \times \mathfrak{L}' = \mathfrak{M}_t''$. Virá, então, $\mathfrak{A}_r \times \mathfrak{L}_s' = \mathfrak{M}_{rst}''$. Visto que a álgebra de divisão $\mathfrak{M}''$ é independente dos índices r e s e é determinada a menos dum isomorfismo relativo a $\mathfrak{P}$, a operação de multiplicação das álgebras pode considerar-se operação de multiplicação do grupo. A referida operação é comutativa e associativa. De futuro, utilizaremos os símbolos $(\mathfrak{A})$, $(\mathfrak{A}')$, ... para as diferentes classes. Demonstrámos no Cap.VI, § 12 (álgebras normais), que o produto duma álgebra normal de divisão $\mathfrak{D}$, sobre $\mathfrak{P}$, pela sua álgebra recíproca $\mathfrak{D}^{-1}$ é uma álgebra completa de matrizes com elementos de $\mathfrak{P}$[1]. Será, assim, $(\mathfrak{A})(\mathfrak{A}^{-1}) = (\mathfrak{P})$. Ora a classe um (elemento um do grupo) é precisamente a classe $(\mathfrak{P})$. Os postulados dos grupos são, pois, verificados.

Pode demonstrar-se a igualdade $\mathfrak{A} \times \mathfrak{A}^{-1} = \mathfrak{P}_t$ deste outro modo: $\mathfrak{A}$ está mergulhado em si mesmo de modo irredutível. O conjunto $\bar{\mathfrak{A}} = \mathfrak{P}$ dos elementos de $\mathfrak{A}$ que comutam com $\mathfrak{A}$ é, como sabemos, um corpo $\mathfrak{L} \neq \mathfrak{F}$, com $\mathfrak{A}_{\mathfrak{L}} = \mathfrak{A} \times \mathfrak{L} = \mathfrak{A} \times \mathfrak{A}^{-1} = \mathfrak{F}_t$. Visto ser aqui $\bar{\mathfrak{L}} = \mathfrak{P}$ comutativo, será também $\mathfrak{A} \times \mathfrak{A}^{-1} = \mathfrak{P}_t$, como se quer.

Seja Φ uma ampliação comutativa finita de $\mathfrak{P}$. A álgebra $\mathfrak{A}_\Phi$, sobre Φ, pode escrever-se $\mathfrak{A}_\Phi = \mathfrak{A} \times \Phi = \Phi \times \mathfrak{A} = \Phi_{\mathfrak{L}}$. Vê-se que se trata duma álgebra normal sobre Φ. Representaremos por $(\mathfrak{A})_\Phi$ a classe ampliada de álgebras semelhantes sobre Φ, obtida a partir de $(\mathfrak{A})$. Será, por ex.,

$$\mathfrak{A}_{r\Phi} = (\mathfrak{A} \times \mathfrak{P}_r)_\Phi = \mathfrak{A}_\Phi \times \Phi_r = \mathfrak{L} \times \Phi_s \times \Phi_r = \mathfrak{L} \times \Phi_{sr} = \mathfrak{L}_{sr} \in (\mathfrak{A})_\Phi ,$$

onde a álgebra de divisão $\mathfrak{L}$, sobre Φ, é independente do índice r.

(1) Este teorema encontra-se já a pgs.103 da memória de R.Brauer, citada no Cap.IX, "Über Systeme hyperkomplexer Zahlen".

Para se indagar da álgebra de divisão $\mathfrak{L}$ acabada de referir ($\mathfrak{A}_\Phi = \mathfrak{L} \times \Phi_s = \mathfrak{L}_s$), consideremos a representação irredutível da álgebra Φ (sobre $\mathfrak{P}$), em $\mathfrak{A}$, que é um corpo $\Phi^* \cong \mathfrak{A}_r$. O conjunto dos elementos de $\mathfrak{A}_r$ que comutam com Φ^* constitui um corpo $\bar{\Phi}^* \cong \mathfrak{L} \neq \mathfrak{F}$, com $\Phi^*_{\mathfrak{L}} = \mathfrak{F}_t$, onde $\mathfrak{L} \neq \mathfrak{A}$. Por consequência, em virtude de ser $\Phi^*_{\mathfrak{L}} \neq \Phi_{\mathfrak{L}} = \mathfrak{A}_\Phi$, ter-se-á $\mathfrak{A}_\Phi = \mathfrak{L}_s \neq \mathfrak{F}_t$, ou seja ainda $\mathfrak{A}_\Phi = \mathfrak{L}_s \cong \Phi^*_s$. Daqui se tira o seguinte

Teorema 2:- Da classe $(\mathfrak{A})$ de álgebras semelhantes sobre $\mathfrak{P}$, passa-se à classe ampliada $(\mathfrak{A})_\Phi = (\bar{\Phi}^*)$, de álgebras semelhantes sobre Φ, considerando o corpo $\bar{\Phi}^*$ composto dos elementos de $\mathfrak{A}_r$ que comutam com o corpo Φ^*, que é representação irredutível de Φ (de grau r, bem determinado) em $\mathfrak{A}$.

Do que se disse sobre corpos de decomposição de álgebras normais simples, resulta que um corpo de decomposição de $\mathfrak{A}$ é corpo de decomposição da classe $(\mathfrak{A})$. No teorema acabado de enunciar, quando $\bar{\Phi}^* \supseteq \Phi$ coincidir com $\Phi^* \cong \Phi$, chega-se simplesmente a $(\mathfrak{A})_\Phi = (\Phi)$. Φ é corpo de decomposição da classe $(\mathfrak{A})$.

4) O índice de Schur - No Cap.VII, § 6, mostrámos que uma álgebra normal de divisão $\mathfrak{A}$, sobre $\mathfrak{P}$, tem uma ordem que é um quadrado perfeito. E, tendo posto $(\mathfrak{A}/\mathfrak{P}) = m^2$, dissemos que m se chama índice da álgebra. É o índice de Schur. Seja $\Phi \supseteq \mathfrak{P}$ uma ampliação comutativa finita, máxima, de $\mathfrak{P}$, contida em $\mathfrak{A}$. Φ é a sua própria representação irredutível em $\mathfrak{A}$, de sorte que $(\Phi/\mathfrak{P})^2 = (\mathfrak{A}/\mathfrak{P}) = m^2$. Reconhece-se aqui, de novo, por consequência, que a ordem duma álgebra normal de divisão é um quadrado perfeito. Pode enunciar-se o

Teorema 1:- O índice de Schur duma álgebra normal de divisão $\mathfrak{A}$, sobre $\mathfrak{P}$, é o grau comum de todos os corpos comutativos máximos de $\mathfrak{A}$ que contêm $\mathfrak{P}$.

Consideremos, em seguida, um corpo de decomposição qualquer Δ, de $\mathfrak{A}$, que seja ampliação finita de $\mathfrak{P}$. Se a representação irredutível única de Δ, em $\mathfrak{A}$, é $\Delta^* \cong \mathfrak{A}_r$, como se tem

$$(\Delta^*/\mathfrak{P})^2 = (\Delta/\mathfrak{P})^2 = r^2 : (\mathfrak{A}/\mathfrak{P}) = r^2 m^2, \quad (\Delta/\mathfrak{P}) = r\,m,$$

tem lugar este

Teorema 2:- O grau $(\Delta/\mathcal{P})$ dum corpo de decomposição duma álgebra normal de divisão $\mathcal{A}$, sobre $\mathcal{P}$ [ou duma álgebra normal simples da classe $(\mathcal{A})$], é divisível pelo índice de $\mathcal{A}$.(1)

Duma maneira geral, seja Γ uma ampliação comutativa finita de $\mathcal{P}$. Se Γ^* é a representação irredutível única de Γ, em $\mathcal{A}$, tem-se $\Gamma^* \cong \mathcal{A}_\Gamma$, e o comutador $\overline{\Gamma}^* = \mathcal{Y}$, de Γ^*, em $\mathcal{A}_\Gamma$, como se viu no § anterior, é tal que $\mathcal{A}_\Gamma \in (\mathcal{Y})$. Ponhamos $(\mathcal{Y}/\Gamma) = d^2$. Tem-se

$$(\Gamma^*/\mathcal{P})(\mathcal{Y}/\mathcal{P}) = (\Gamma/\mathcal{P})(\mathcal{Y}/\mathcal{P}) = (\Gamma/\mathcal{P})^2 d^2 = r^2(\mathcal{A}/\mathcal{P}) = r^2 m^2,$$

e, portanto, $(\Gamma/\mathcal{P}).d = r\,m$. Ao passo que, quando Γ é corpo de decomposição, se tem $d = 1$, aqui é $d \neq 1$. Vale o

Teorema 3:- O grau $(\Gamma/\mathcal{P})$, duma ampliação finita do corpo fundamental $\mathcal{P}$ duma álgebra normal de divisão $\mathcal{A}$, é tal que, supondo $\mathcal{A}_\Gamma \in (\mathcal{Y})$ e $(\mathcal{Y}/\Gamma) = d^2$, é verificada a igualdade $(\Gamma/\mathcal{P}) \cdot d = r\,m$, em que m é o índice de Schur de $\mathcal{A}$.

Enquanto que m é o índice de Schur da classe $(\mathcal{A})$ de álgebras sobre $\mathcal{P}$, o número d é o índice de Schur da classe $(\mathcal{Y})$, a que pertence $\mathcal{A}_\Gamma$, de álgebras sobre Γ. Γ é ampliação finita comutativa de $\mathcal{P}$. Se supusermos $\mathcal{A}_\Gamma = \mathcal{Y}_\rho$, ρ é o número de ideais esquerdos simples em que pode decompor-se $\mathcal{A}_\Gamma = \Gamma_\mathcal{A}$. Ter-se-á $(\Gamma_\mathcal{A}/\mathcal{A}) = (\Gamma/\mathcal{P}) = r\rho$, e, portanto, $r\rho\, d = r\, m$, ou $m = \rho d$. O índice d divide o índice m e o cociente ρ é um divisor do grau $(\Gamma/\mathcal{P})$. O número ρ diz-se factor de redução do índice de $\mathcal{A}$ relativamente a Γ.(2) Tem lugar o seguinte

Teorema 4:- Nas condições do teorema 3, o índice de Schur d divide o índice de Schur m, e o cociente ρ, chamado factor de redução do índice de $\mathcal{A}$ relativamente a Γ, é um divisor do grau $(\Gamma/\mathcal{P})$.

(1) Albert, pgs. 60.
(2) Albert, pag. 59.

Corolário 1:- Dada a álgebra normal simples $\mathcal{A}_n$, sobre $\mathcal{P}$, se o índice de $(\mathcal{A})$ é primo com o grau $(\Gamma/\mathcal{P})$ duma ampliação comutativa finita Γ, de $\mathcal{P}$, o índice de $\mathcal{A}_\Gamma \in (\mathcal{Y})$ é o mesmo que o índice de $\mathcal{A}$. $\mathcal{A}_\Gamma$ é álgebra de divisão sobre Γ.

Com efeito, visto ser ρ divisor de m e do grau $(\Gamma/\mathcal{P})$, ter-se-á $\rho = 1$, $m = d$. Por outro lado, $\mathcal{A}_\Gamma = \mathcal{Y}_\rho = \mathcal{Y}$ é álgebra de divisão sobre Γ.

Observações:- Seja $\mathcal{B} = \mathcal{A}_n$ uma álgebra normal simples sobre $\mathcal{P}$. Qualquer que seja a ampliação comutativa Φ, de $\mathcal{P}$, $\mathcal{B}_\Phi$ é álgebra normal simples sobre Φ. Suponhamos Δ um corpo de decomposição de $\mathcal{B}$ (ou de $\mathcal{A}$). Em princípio, Δ é ampliação finita de $\mathcal{P}$. Vimos que Δ existe. A afirmação anterior, relativa a $\mathcal{B}_\Phi$, resulta também desse facto. Se Ψ é uma ampliação qualquer de $\mathcal{P}$ (algébrica ou transcendente, mas comutativa), para um corpo Θ, contendo Ψ e Δ(1), é $\mathcal{B}_\Theta = \Theta_q$, se $\mathcal{B}_\Delta = \Delta_q$. Assim, $\mathcal{B}_\Psi$ não tem radical. Como o seu centro é Ψ, estamos em presença duma álgebra normal semi-simples, portanto duma álgebra normal simples. Pondo, em particular, $\mathcal{A}_\Delta = \Delta_m$, em virtude de se ter $(\mathcal{A}_\Delta/\Delta) = (\mathcal{A}/\mathcal{P}) = m^2$, m é o índice de Schur. De resto, notando que o índice de $\mathcal{A}_\Delta$ é $d = 1$, tem-se $m = \rho$, com $\mathcal{A}_\Delta = \Delta_\rho$. O índice de $\mathcal{A}$ (sobre $\mathcal{P}$) significa, assim, o número máximo de ideais esquerdos simples em que pode decompor-se uma ampliação $\mathcal{A}_\Gamma$, $(\Gamma \supseteq \mathcal{P})$.

Depois de demonstrada a existência de corpos de decomposição duma álgebra normal simples, e, na verdade, corpos que são ampliações finitas do corpo fundamental da mesma álgebra, provaremos, de modo mais preciso, a existência de corpos de decomposição que são ampliações separáveis finitas do referido corpo fundamental. Embora o pudéssemos fazer sem as considerações do § a seguir, não hesitamos em expor o conteúdo desse §, que nos parece susceptível de aplicações interessantes na teoria geral.

(1) Acerca da noção de Kompositum de corpos que contêm um corpo $\mathcal{P}$, vejam-se, por ex., N. Jacobson, "The Theory of rings", pgs. 97, ou Albert, "Modern Higher Algebra", pgs. 161. Vejam-se também pgs. 115 a 126 do livro de H. Hasse, "Höhere Algebra", citado no § 8. No Cap. XII, parte final, consagraremos um § a essa noção.

5) Derivações duma álgebra[1] - Dadas uma álgebra $\mathcal{A}$, sobre $\mathcal{P}$, e uma sua sub-álgebra $\mathcal{U}$, uma derivação de $\mathcal{U}$ no interior de $\mathcal{A}$ é uma aplicação D, de $\mathcal{U}$, sobre uma parte de $\mathcal{A}$, nas condições seguintes: se a, a_1, $a_2 \in \mathcal{U}$, e $\lambda \in \mathcal{P}$,

$$Da \in \mathcal{A}, \quad D(a_1 + a_2) = Da_1 + Da_2 , \qquad D(\lambda a) = \lambda . Da ,$$

$$D(a_1 a_2) = Da_1 . a_2 + a_1 . Da_2 .$$

Utilizam-se, como se vê, as regras habituais da derivação duma soma e dum produto, assim como a do produto duma constante por uma função. Um exemplo simples de D é fornecido pela operação

$$[x,d] = xd - dx ,$$ com d fixo em $\mathcal{A}$ e x qualquer em $\mathcal{U}$.

Efectivamente, tem-se, por ex.,

$$[a_1 a_2, d] = a_1 a_2 d - d a_1 a_2 = [a_1, d]\, a_2 + a_1 [a_2, d] .$$

As derivações deste tipo dizem-se internas. O símbolo Da significa $D(Da)$. Do mesmo modo se interpretam os símbolos $D^R a$. Quando o domínio de aplicação de D é toda a álgebra $\mathcal{A}$, fala-se duma derivação de $\mathcal{A}$. Para significar derivada de a pode utilizar-se a'. Em seguida põe-se $(a')' = a''$, ..., $(a^{(R-1)})' = a^{(R)}$.

Teorema 1:- Se $p \neq 0$ é a característica de $\mathcal{P}$, é válida a igualdade $[a, d^p] = a^{(p)}$, subentendendo no 2º membro resultado de derivações internas definidas por d.

Com efeito, tendo-se $[a,d] = ad - da$, é também $ad = da + [a,d]$. Analogamente, $ad^2 = ad.d = d.ad + [ad,d] = d(da + [a,d]) + [da,d] + [[a,d],d] = d^2 a + d[a,d] + d[a,d] + a''$, ou seja $ad^2 = d^2 a + 2da' + a''$. Por indução, prova-se a igualdade

$$ad^R = d^R a + \binom{k}{1} d^{R-1} a' + \cdots + a^{(R)},$$

(1) Seguimos aqui N.Jacobson, "The Theory of rings", pgs.101 a 103. Nos §§ 6 e 7, subsidiamo-nos do mesmo livro, pgs.106 e 107.

da qual se tira

$$ad^R - d^R a = \binom{k}{1} d^{(R-1)} a' + \cdots + a^{(R)} = [a, d^R] .$$

Quando $k = p$, desaparecem os termos que contêm p como factor, ficando apenas $[a, d^p] = a^{(p)}$.

Teorema 2:- Se $a \in \mathcal{A}$ for um elemento tal que $[a,d] = d$, tem-se, supondo ainda $p \neq 0$, $[a^p, d] = d$. Observem-se, na verdade, as relações seguintes:

$$[a,d] = ad - da = d,$$

$$[a,[a,d]] = a(ad - da) - (ad - da)a = a^2 d - 2ada + da^2 = d,$$

$$[a,[a,[a,d]]] = a^3 d - 3a^2 da + 3ada^2 - da^3 = d.$$

Dum modo geral, prova-se, por indução, a igualdade

$$[a,[a,\ldots,[a,d]\ldots]] = a^R d - \binom{k}{1} a^{R-1} da + \binom{k}{2} a^{R-2} da^2 - \cdots \pm da^R,$$

conforme k for par ou ímpar. Pondo $k = p$, vem, então,

$$[a^p, d] = a^p d - da^p = [a,[a,\ldots,[a,d]\ldots]] = d,$$

como se enunciou.

Se D_1 e D_2 são dois símbolos de derivação duma álgebra, poremos, por definição: $(D_1 + D_2)a = D_1 a + D_2 a$; $(D_1 D_2)a = D_1(D_2 a)$; $(\lambda D)a = \lambda (Da)$. Verifica-se que, destes novos símbolos, apenas não define uma derivação o produto $D_1 D_2$. O comutador $[D_1, D_2] = D_1 D_2 - D_2 D_1$ é, porém, já uma derivação.

Teorema 3:- Se $p \neq 0$, o símbolo D^p é uma derivação. De facto, uma indução em ordem a n leva à igualdade

$$D^n(a_1 a_2) = a_1 (D^n a_2) + \binom{n}{1} (Da_1).(D^{n-1} a_2) + \cdots + (D^n a_1) a_2 .$$

Por consequência, tem-se

$$D^p(a_1 a_2) = a_1 (D^p a_2) + (D^p a_1) a_2 .$$

As restantes propriedades características duma derivação são imediatas.

Teorema 4:- Se $\mathcal{L}$ é uma álgebra normal normal simples[1] dada uma sub-álgebra semi-simples $\mathcal{U}$, com o mesmo elemento um que $\mathcal{L}$, uma derivação qualquer de $\mathcal{U}$ no interior de $\mathcal{L}$ pode ampliar-se para uma derivação de $\mathcal{L}$, e, de facto, para uma derivação interna. Jacobson (loc.cit.) dá a demonstração que se segue. Consideremos o conjunto de matrizes do 2º grau, com elementos de $\mathcal{L}$, da forma

$$\begin{pmatrix} a & Da \\ o & a \end{pmatrix}, \qquad (a \in \mathcal{U}) , \qquad (2)$$

e observemos as igualdades

$$\begin{pmatrix} a & Da \\ o & a \end{pmatrix} + \begin{pmatrix} b & Db \\ o & b \end{pmatrix} = \begin{pmatrix} a+b & D(a+b) \\ o & a+b \end{pmatrix},$$

$$\begin{pmatrix} a & Da \\ o & a \end{pmatrix}\begin{pmatrix} b & Db \\ o & b \end{pmatrix} = \begin{pmatrix} ab & D(ab) \\ o & ab \end{pmatrix}, \quad \begin{pmatrix} \lambda a & D(\lambda a) \\ o & \lambda a \end{pmatrix} = \lambda \begin{pmatrix} a & Da \\ o & a \end{pmatrix}.$$

O conjunto em questão dá uma álgebra equivalente a $\mathcal{U}$, portanto uma representação de $\mathcal{U}$ em $\mathcal{L}$. Se $\mathfrak{M}(u_1, u_2)$ for o módulo de representação, tem-se

$$au_1 = u_1 a ,$$

$$au_2 = u_1(Da) + u_2 a .$$

Podemos considerar $\mathfrak{M}$ como módulo direito relativamente a $\mathcal{U}_{\mathcal{L}}^{1}$,

(1) No livro de Jacobson, pgs.98, por sugestão de Albert, utiliza-se a designação de "álgebra central simples", em vez de "álgebra normal simples".

se $\mathcal{U}'$ é uma álgebra anti-isomorfa de $\mathcal{U}$. Ponhamos $\mathcal{U}_{\mathcal{L}} = \mathcal{U} \times \mathcal{L} = (\mathcal{U}_1' + \cdots + \mathcal{U}_s') \times \mathcal{L} = \mathcal{U}_1' \times \mathcal{L} + \cdots$, onde os $\mathcal{U}_i'$ se supõem álgebras simples. Por virtude de se ter, por ex.,

$$\mathcal{U}_1' \times \mathcal{L} \cong \mathcal{L}_r \times \mathfrak{N} \times \mathcal{P}_{rt} = \mathcal{L} \times \mathfrak{N} \times \mathcal{P}_{rt} = \mathcal{L}_\rho \times \mathcal{P}_{rt} = \mathcal{L}_{\rho r t} ,$$

onde $\mathcal{L}$ é álgebra de divisão sobre $\mathcal{P}$, $\mathfrak{N}$ álgebra normal de divisão sobre o mesmo corpo e $\mathcal{L}$ ainda álgebra de divisão sobre $\mathcal{P}$, vê-se que $\mathcal{U}_{\mathcal{L}}'$ é álgebra semi-simples sobre $\mathcal{P}$. O módulo $\mathfrak{M}$ será completamente redutível em face de $\mathcal{U}_{\mathcal{L}}'$. Cada sub-módulo simples é, depois, módulo simples relativamente a $\mathcal{U}$ (à esquerda) e a $\mathcal{L}$ (à direita). Nessas condições, visto que o sub-espaço $u_1\mathcal{L}$, de $\mathfrak{M}$, é invariante em face de $\mathcal{U}$, existe um sub-espaço invariante em face de $\mathcal{U}$ e $\mathcal{L}$, da forma $v\mathcal{L}$, tal que $\mathfrak{M} = u_1\mathcal{L} + u_2\mathcal{L} = u_1\mathcal{L} + v\mathcal{L}$. Ponhamos

$$v = u_1 h_1 + u_2 h_2 , \qquad u_2 = u_1 f_1 + v f_2 , \qquad (h_i, f_i \in \mathcal{L}).$$

Das relações

$$v = u_1 h_1 + u_2 h_2 = u_1 h_1 + (u_1 f_1 + v f_2) h_2 = u_1(h_1 + f_1 h_2) + v f_2 h_2 ,$$

conclui-se que f_2 e h_2 são elementos inversos em $\mathcal{L}$. Como base de $v\mathcal{L}$ pode tomar-se $vf_2 = V$, de sorte que $u_2 = u_1 f_1 + V$. A passagem da base (u_1, u_2) à base (u_1, V), do módulo $\mathfrak{M}$, tem lugar, assim, pela transformação

$$u_1 = u_1 , \qquad V = -u_1 f_1 + u_2 .$$

Para encontrarmos as matrizes que substituem (2), na representação que se obtém utilizando a nova base, calculemos aV. Tem-se

$$aV = -a(u_1 f_1) + au_2 = u_1(-af_1) + u_1(Da) + u_2 a =$$

$$= u_1(-af_1 + Da) + (u_1 f_1 + V)a = u_1(-af_1 + f_1 a + Da) + Va .$$

Será, portanto,

$$au_1 = u_1 a ,$$

$$aV = u_1([f_1, a] + Da) + Va .$$

Como $V\mathcal{G}$ é invariante em face de $\mathfrak{A}$, valerá $[f_1, a] + Da = 0$, ou seja $Da = [a, f_1]$. A derivação D reduz-se, logo que se estenda à álgebra $\mathcal{G}$, à derivação interna definida por f_1. O teorema está provado.

Corolário:- Toda a derivação duma álgebra normal simples é interna.

6) Sobre as álgebras - p - A álgebra $\mathcal{G}$, sobre $\mathcal{P}$, diz-se uma álgebra - p, quando a característica de $\mathcal{P}$ é p e $\mathcal{G}$ é normal simples com um grau igual a uma potência de p. O nosso objectivo neste § é muito limitado,(1) reduzindo-se à verificação de álgumas propriedades muito simples das álgebras - p mais elementares: das álgebras normais de divisão de grau p.

Se o polinómio principal da álgebra normal de divisão $\mathcal{D}$ é de grau p, tomemos $a \in \mathcal{D}$ tal que $a \notin \mathcal{P}$. O polinómio principal de a é uma potência do seu polinómio mínimo (pgs.153). Portanto, este último será também do grau p. A ordem de $\mathcal{D}$ é p^2, pelas razões que vão ver-se. Seja Φ um corpo de decomposição de $\mathcal{D}$. Por ser $\mathcal{D}_\Phi = \Phi_\rho$, a ordem de $\mathcal{D}$ será ρ^2. O grau da álgebra quadrada sobre Φ, $\mathcal{D}_\Phi$, é ρ (pgs.152); e como esse grau é o grau de $\mathcal{D}$(2), ter-se-á $\rho = p$, $(\mathcal{D}/\mathcal{P}) = (\mathcal{D}_\Phi/\Phi) = p^2$. Tira-se daqui o seguinte

Teorema 1:- Numa álgebra normal de divisão de grau p, todo o elemento da álgebra que não pertença ao corpo fundamental gera um sub-corpo comutativo máximo de $\mathcal{D}$. Efectivamente, p é o índice da álgebra.

Posto isto, a existência de corpos de decomposição separáveis para a álgebra $\mathcal{D}$ em questão resulta simplesmente, provando a existência dum elemento separável de $\mathcal{D}$ não contido em $\mathcal{P}$. Demonstraremos o

Teorema 2:- Se $\mathcal{D}$ é uma álgebra normal de divisão de grau p, cujo corpo fundamental é de característica $p \neq 0$, a existência dum elemento inseparável de $\mathcal{D}$, não pertencente a $\mathcal{P}$, arrasta a existência dum elemento separável nas mesmas condições.

(1) Veja-se Albert, pgs.104 e seguintes, para um estudo sério das álgebras-p. (2) O polinómio principal de $\mathcal{D}$ e $\mathcal{D}_\Phi$ é o mesmo (pgs.114, corolário 1º).

Seja a um elemento de $\mathcal{D}$ inseparável relativamente a $\mathcal{P}$. É claro que $a^p \in \mathcal{P}$. Como $\mathcal{P}(a)$ é um corpo máximo contido em $\mathcal{D}$, coincide com o seu próprio comutador. Se se considera uma derivação interna definida por a, a condição necessária e suficiente, para que um elemento tenha a derivada nula, é que pertença a $\mathcal{P}(a)$. Posto isto, tomemos um elemento $\alpha \in \mathcal{D}$ que não pertença a $\mathcal{P}(a)$. Será $[\alpha, a] \neq 0$, $[\alpha, a^p] = \alpha^{(p)} = 0$. Existe um número $k \geq 1$ tal que $\alpha^{(k)} \neq 0$, $\alpha^{(k+1)} = 0$. O elemento $b = \alpha^{(k-1)}(\alpha^{(k)})^{-1}$ tem a derivada

$$b' = \alpha^{(k)}(\alpha^{(k)})^{-1} + \alpha^{(k-1)}\left[(\alpha^{(k)})^{-1}\right]'.$$

Ora valem as relações

$$(\alpha^{(k)})^{-1}\alpha^{(k)} = u, \qquad \left[(\alpha^{(k)})^{-1}\right]'\alpha^{(k)} + (\alpha^{(k)})^{-1}\alpha^{(k+1)} = 0,$$

de modo que

$$\left[(\alpha^{(k)})^{-1}\right]' = 0, \qquad b' = u.$$

O elemento $c = ab$ tem a derivada $c' = a$. O teorema 2 do § 5 dá, então, $[c^p, a] = a$, $[c^p - c, a] = 0$, $c^p - c = \tau \in \mathcal{P}(a)$. O facto de c não pertencer a $\mathcal{P}(a)$ permite-nos afirmar que uma sub-álgebra de $\mathcal{D}$ que contenha c e a é igual a $\mathcal{D}$, pois a ordem duma tal sub-álgebra é, por um lado, múltipla da ordem de $\mathcal{P}(a)$, e, por outro, sub-múltipla da ordem de $\mathcal{D}$. O elemento τ comuta com c e com a, e, portanto, comuta com todos os elementos de $\mathcal{D}$. Será $\tau \in \mathcal{P}$, pois $\mathcal{D}$ é normal. A equação $x^p - x - \tau = 0$, com coeficientes em $\mathcal{P}$, é irredutível e separável, visto que, se fosse inseparável, teria a forma $\Pi(x - \beta_i)^{p^t} = 0$. Mais pròpriamente, ter-se-ia $t = 1$, $\beta_i = \beta_1$, e a forma da equação seria $x^p - \beta_1^p = 0$, o que é absurdo. O elemento c é o elemento separável aludido no teorema.

7) Sobre a existência de corpos de decomposição separáveis

Sabemos que o problema dos corpos de decomposição duma álgebra normal simples se reduz ao caso do das álgebras normais de divisão. Se a característica de $\mathcal{P}$ é nula, qualquer ampliação de $\mathcal{P}$ é separável. Uma ampliação máxima de $\mathcal{P}$, contida em $\mathcal{D}$, é um corpo de decomposição separável de $\mathcal{D}$. O teorema enuncia-se, em geral, do modo seguinte:

Teorema:- Toda a álgebra normal de divisão contém uma ampliação separável máxima do corpo fundamental. Suponhamos, então, $p \neq 0$. Pode dar-se o caso de $\mathcal{P}$ ser já um corpo sem ampliação separável contida em $\mathcal{D}$. Se assim não for, tomemos um elemento $\alpha_1 \in \mathcal{D}$ tal que $(\mathcal{P}(\alpha_1)/\mathcal{P}) > 1$, com α_1 separável. Em seguida, consideremos o comutador $\overline{\mathcal{P}(\alpha_1)} = \mathcal{Q}$, de $\mathcal{P}(\alpha_1)$, em $\mathcal{D}$. Sabemos que $\mathcal{P}(\alpha_1)$ é o centro de $\mathcal{Q}$. Se $\alpha_2 \in \mathcal{Q}$ for separável relativamente a $\mathcal{P}(\alpha_1)$ e tal que $(\mathcal{P}(\alpha_1, \alpha_2)/\mathcal{P}(\alpha_1)) > 1$, obtém-se um corpo $\mathcal{P}(\alpha_1, \alpha_2)$, contido em $\mathcal{D}$, que é ainda ampliação separável de $\mathcal{P}$. Volta a considerar-se o comutador de $\mathcal{P}(\alpha_1, \alpha_2)$, que é sub-corpo próprio de $\mathcal{Q}$, como se reconhece tendo em conta a relação

$$(\mathcal{P}(\alpha_1, \alpha_2)/\mathcal{P})(\overline{\mathcal{P}(\alpha_1, \alpha_2)}/\mathcal{P}) = (\mathcal{D}/\mathcal{P}) .$$

O raciocínio prossegue até nos encontrarmos em qualquer das duas situações seguintes: ou se obtém uma ampliação separável máxima Φ (isto é, para a qual não há corpo comutativo, ampliação de $\mathcal{P}$, contido em $\mathcal{D}$, que admita aquela ampliação como sub-corpo próprio), caso em que $\overline{\Phi} = \Phi$, ou, então, Φ é tal que o seu comutador $\overline{\Phi}$ constitui uma álgebra normal de divisão sobre Φ contendo apenas elementos que satisfazem a equações irredutíveis inseparáveis com coeficientes em Φ. Há apenas esta segunda situação a ser tratada, a fim de se verificar que ela não pode ter lugar. O teorema ficará, então, provado. Designemos por Ψ uma ampliação máxima de Φ contida em $\overline{\Phi}$ e ponhamos $\Psi = \Phi(\alpha, \beta, \ldots, \lambda, \mu)$. Admitindo que $\mu \notin \Phi(\alpha, \beta, \ldots, \lambda)$, consideremos o corpo $\Psi_1 = \Phi(\alpha, \beta, \ldots, \lambda, \mu^p)$. Não pode ter-se $\Psi_1 = \Psi$, pois isso implicaria μ = elemento separável relativamente a $\Phi(\alpha, \beta, \ldots, \lambda)$, o que não pode ter lugar por ser Ψ ampliação pura de Φ, e, portanto, ampliação pura de qualquer corpo intermédio entre Φ e Ψ (vidé pgs.170 e 178). A equação $x^p - \mu^p = 0$ é irredutível em Ψ_1, e, por isso, tem-se $(\Psi/\Psi_1) = p$, $\Psi = \Psi_1(\mu)$. O comutador $\overline{\Psi}_1$, de Ψ_1, em $\overline{\Phi}$, é uma álgebra sobre Φ, para a qual

$$(\overline{\Psi}_1/\Phi)(\Psi_1/\Phi) = (\overline{\Phi}/\Phi) = (\Psi/\Phi)^2 = (\Psi/\Psi_1)^2(\Psi_1/\Phi)^2 = p^2(\Psi_1/\Phi)^2 .$$

Como se tem também

$$(\overline{\Psi}_1/\Phi) = (\overline{\Psi}_1/\Psi_1)(\Psi_1/\Phi) ,$$

conclui-se $(\overline{\Psi}_1/\Psi_1) = p^2$. Assim, $\overline{\Psi}_1$ é uma álgebra normal de divisão do grau p, sobre Ψ_1. Como μ não pertence a Ψ_1, existe um elemento separável $c \in \overline{\Psi}_1$ que satisfaz a uma equação $c^p - c - \tau = 0$, com $\tau \in \Psi_1$. Por ser c separável relativamente a Ψ_1, é $\Psi_1(c) = \Psi_1(c^{p^\rho}) \supset \Psi_1$, qualquer que seja ρ. Se ρ é suficientemente grande para que $c^{p^\rho} \in \Phi$, não pode ter-se $\Psi_1(c^{p^\rho}) \supset \Psi_1$. É absurdo admitir a emistência de $\overline{\Phi}$ nas condições indicadas.

8) A teoria de Galois dos corpos comutativos - O teorema 27 de pgs.181 põe em evidência o facto seguinte: se $\mathcal{O}$ é uma ampliação normal, separável, finita, de grau n, de $\mathcal{P}$, e se $\mathcal{G} = \{S_1, \ldots, S_n\}$ é o grupo dos isomorfismos de $\mathcal{O}$ relativamente a $\mathcal{P}$ (grupo de Galois), a cada corpo intermédio entre $\mathcal{P}$ e $\mathcal{O}$, pode fazer-se corresponder, duma maneira unívoca, um sub-grupo de $\mathcal{G}$, sub-grupo cujos elementos deixam individualmente invariantes os elementos do corpo intermédio, e apenas esses elementos. Costuma dizer-se que o corpo intermédio é sub-corpo invariante completo do sub-grupo em questão.

O teorema fundamental da teoria de Galois dos corpos comutativos pode enunciar-se assim:

Teorema:- Seja $\mathcal{O}$ uma ampliação normal, separável, finita, do grau n, de $\mathcal{P}$, e $\mathcal{G}$ o seu grupo de Galois. Existe uma correspondência biunívoca completa entre os corpos intermédios $\mathcal{L}$, entre $\mathcal{P}$ e $\mathcal{O}$, e os sub-grupos $\mathcal{L}_\mathcal{G}$, de $\mathcal{G}$, nas condições seguintes: 1) $\mathcal{L}$ é sub-corpo invariante completo de $\mathcal{L}_\mathcal{G}$; 2) $\mathcal{L}_\mathcal{G}$ é sub-grupo invariante completo de $\mathcal{L}$; 3) a ordem m, de $\mathcal{L}_\mathcal{G}$, é igual ao grau

$(\mathcal{A}/\mathcal{L})$ e o índice r, de $\mathcal{L}$, em $\mathcal{G}$, é igual ao grau $(\mathcal{L}/\mathcal{P})$.[1] A demonstração que vamos dar assenta sobre considerações inteiramente diferentes das utilizadas nas obras referidas em nota. Na ordem de ideias deste livro, começaremos por provar dois lemas. O processo é devido a Deuring.

Consideremos a ampliação $\mathcal{A}$ aludida no teorema. Qualquer que seja o corpo Ψ, ampliação de $\mathcal{P}$, sabemos que $\mathcal{A}_\Psi$ não tem radical. As ampliações finitas separáveis de $\mathcal{P}$ realizam o exemplo mais simples de álgebras separáveis. Um corpo Δ que contenha um sub-corpo isomorfo de $\mathcal{A}$ é corpo de decomposição de $\mathcal{A}$ (§ 1). Em particular, será corpo de decomposição todo o corpo isomorfo de $\mathcal{A}$. Se $\Delta \supseteq \mathcal{P}$ é corpo de decomposição, todas as representações de $\mathcal{A}$ em Δ são do 1º grau. Os ideais em que se decompõe $\mathcal{A}_\Delta$ são todos de 1ª ordem relativamente a Δ:

$$\mathcal{A}_\Delta = e_1\Delta + \cdots + e_n\Delta \ . \qquad (3)$$

Os e_i são idempotentes ortogonais. Aos módulos de representação $e_i\Delta$ pertencem também representações de $\mathcal{A}_\Delta$. Designemos

(1) Há, em português, os livros seguintes, que desenvolvem a teoria de Galois no caso de corpos de números: Mira Fernandes, "Grupo de substituições e resolubilidade algébrica", II, Lisboa, 1931; Madureira e Sousa, "Resolução algébrica das equações", Porto, 1932; Vicente Gonçalves, "Álgebra Superior", Cap. XII, Coimbra, 1933. Para o caso de corpos quaisquer (teoria posterior a E. Steinitz) podem ver-se: van der Waerden, "Moderne Algebra", I Teil, Cap. VII, pgs. 148 e seguintes; H. Hasse "Höhere Algebra", II, Berlin, 1937, pgs. 100 e seguintes; A. A. Albert, "Modern Higher Algebra", Cap. VIII, pgs. 172 e seguintes; assim como E. Artin e A. Milgram, "Galois Theory", Michigan, 1944. O ponto de vista em que aqui nos colocamos é devido a M. Deuring, "Galoissche Theorie und Darstellungstheorie", Mathematische Annalen, Band 107, 1933, pgs. 140 a 144.

por $(a_1, \ldots, a_n)$ uma base de $\mathcal{A}$ relativamente a $\mathcal{P}$ e suponhamos

$$a_j e_i = e_i \alpha_j \ , \qquad (\alpha_j \in \Delta).$$

Será, para cada $\sum a_j \delta_j$, $(\delta_j \in \Delta)$, $(\sum a_j \delta_j)e_i = e_i(\sum \alpha_j \delta_j)$. Os elementos S_i do grupo de Galois $\mathcal{G}$, de $\mathcal{A}$, podem considerar-se operadores sobre $\mathcal{A}$. Estendem-se a operadores sobre $\mathcal{A}_\Delta$, pondo $S(a_j \delta_j) = Sa_j \cdot \delta_j$. Esta operação define um automorfismo de $\mathcal{A}_\Delta$, pois que $S(\sum a_j \delta_j) = \sum (Sa_j)\delta_j = 0$ implica $\delta_j = 0$, por virtude de os Sa_j (como os a_j) constituírem uma base de $\mathcal{A}$. Estudemos, em particular, a aplicação de S_i aos e_j que figuram em (3). Por ser

$$\mathcal{A}_\Delta = Se_1 \cdot \Delta + \cdots + Se_n \cdot \Delta, \qquad (S = S_R), \qquad (4)$$

e ser também

$$Se_i \cdot Se_j = 0, \qquad Se_i \cdot Se_i = Se_i \ ,$$

cada ideal $Se_i \cdot \Delta$ é um ideal $e_j\Delta$. Será $S_R e_i = e_j \cdot \mathcal{A}_\Delta$ aparece-nos como um módulo finito relativamente a Δ, que admite $\mathcal{G}$ como domínio operatório e tal que $S(v\delta) = Sv \cdot \delta$, $(v \in \mathcal{A}_\Delta)$. Se for $(S_i S_R)v = S_i(S_R v)$, trata-se dum módulo de representação de $\mathcal{G}$ em Δ. Ora

$$(S_i S_R)v = (S_i S_R)(a_1\delta_1 + \cdots + a_n\delta_n) = (S_i S_R)a_1 \cdot \delta_1 + \cdots + (S_i S_R)a_n \cdot \delta_n =$$

$$= S_i(S_R a_1) \cdot \delta_1 + \cdots + S_i(S_R a_n) \cdot \delta_n = S_i(S_R a_1 \cdot \delta_1 + \cdots + S_R a_n \cdot \delta_n) =$$

$$= S_i(S_R v).$$

Acerca das matrizes da representação, pode observar-se que, no quadro

$$\begin{array}{llll} S_1 e_1 = e_{i_1}, & \ldots, & S_n e_1 = e_{i_1}, \\ \cdots\cdots\cdots\cdots\cdots\cdots & & & \qquad (5) \\ S_1 e_n = e_{i_n}, & \ldots, & S_n e_n = e_{i_n}, \end{array}$$

tanto em cada linha horizontal como em cada linha vertical dos 2ºs membros comparecem todos os e_i $(i = 1, 2, \ldots, n)$. Para as

linhas verticais já foi feita a demonstração. Quanto às horizontais, vamos ver que

$$Se = Te\ , \qquad (S,\ T \in \mathcal{G}\ ;\quad e = \text{um dos } e_\iota)\ ,$$

implica $S = T$. Na verdade, se $a \in \mathcal{O}$, a representação de $\mathcal{O}$ em Δ, definida por e, dá $ae = e\alpha$, $\alpha \in \Delta$. E como $S(ae) = Sa.Se = S(e\alpha) = Se.\alpha$, vê-se que Se define uma representação de $\mathcal{O}$, em Δ, que faz corresponder a Sa o elemento α. Será

$$Sa.Se = Se.\alpha\ , \qquad Ta.Te = Te.\alpha = Ta.Se = Se.\alpha\ .$$

Como se trata duma representação isomorfa, conclui-se $Sa = Ta$, qualquer que seja $a \in \mathcal{O}$, e, portanto, $S = T$. Posto isto, consideremos a álgebra $\mathcal{G}_\Delta = S_1\Delta + \cdots + S_n\Delta$, do grupo $\mathcal{G}$, e estabeleçamos a correspondência seguinte entre $\mathcal{G}_\Delta$ e $\mathcal{O}_\Delta$:

$$\sum_\iota S_\iota \delta_\iota \longrightarrow \sum_\iota (S_\iota\ e)\,\delta_\iota\ .$$

Imaginada como correspondência operatória de módulos relativamente a Δ e $\mathcal{G}$, trata-se dum isomorfismo operatório. Tem lugar o seguinte

Lema 1:- Se $\mathcal{O}$ é uma ampliação finita, normal, separável, de $\mathcal{P}$, e se $\mathcal{G}$ é o grupo de Galois de $\mathcal{O}$, a álgebra $\mathcal{G}_\mathcal{P}$, do grupo $\mathcal{G}$, considerada apenas como módulo relativamente a $\mathcal{G}$ e a $\mathcal{P}$, é isomorfa, no sentido operatório, do módulo $\mathcal{O}$. A aplicação dum elemento $S \in \mathcal{G}$ a um elemento $a \in \mathcal{O}$ supõe-se levar ao elemento $Sa \in \mathcal{O}$, obtido pelo automorfismo S, de $\mathcal{O}$ (relativamente a $\mathcal{P}$).(1)

A demonstração assenta neste

Lema preliminar:- Sejam $\mathfrak{M} = u_1\mathcal{P} + \cdots + u_m\mathcal{P}$ e $\mathfrak{N} = v_1\mathcal{P} + \cdots + v_n\mathcal{P}$ dois módulos relativamente a $\mathcal{P}$ que admitem um certo domínio operatório comum $\mathcal{G}$. Se Δ é uma ampliação finita de $\mathcal{P}$,

(1) O lema é devido a E.Noether, "Normalbasis bei Körpern ohne höhere Verzweigung", Journal für die reine und angewandte Mathematik", Band 167, 1931, pgs.147 a 152.

de grau r, e se os módulos ampliados $\mathfrak{M}_\Delta = u_1\Delta + \cdots + u_m\Delta$, $\mathfrak{N}_\Delta = v_1\Delta + \cdots + v_n\Delta$ são operatòriamente isomorfos relativamente a $\mathcal{G}$ e a Δ, então $\mathfrak{M}$ e $\mathfrak{N}$ são operatòriamente isomorfos relativamente a $\mathcal{G}$ e a $\mathcal{P}$. No enunciado supõe-se que $g \in \mathcal{G}$ se aplica aos diferentes módulos segundo leis como as seguintes: $g(u_i\,\delta) = gu_i.\,\delta$, $g(v_i p) = gv_i.p$, onde $\delta \in \Delta$, $p \in \mathcal{P}$. Para provarmos esta proposição de Noether, ponhamos $\Delta = w_1\mathcal{P} + \cdots + w_r\mathcal{P}$, de modo a podermos considerar $\mathfrak{M}_\Delta$ como módulo relativamente a $\mathcal{G}$ e a $\mathcal{P}$, escrevendo

$$\mathfrak{M}_\Delta = \sum_i u_i(w_1\mathcal{P} + \cdots + w_r\mathcal{P}) = \sum_{i,j} u_i\mathcal{P}w_j = \sum_j \mathfrak{M}\,w_j\ .$$

Cada sub-módulo $\mathfrak{M}\,w_j$ é admissível em face de $\mathcal{G}$ e $\mathcal{P}$. E vê-se que $\mathfrak{M} \cong \mathfrak{M}\,w_j$. Desde que $\mathfrak{M}$ e $\mathfrak{M}_\Delta$ se podem considerar módulos finitos relativamente a $\mathcal{G}_\mathcal{P}$ ($\mathcal{P}$ é comutativo), e este é um sistema hiper-complexo semi-simples, então, se quisermos limitar a demonstração ao caso em que a característica de $\mathcal{P}$ não divide o número n de elementos de $\mathcal{G}$, podemos afirmar imediatamente que $\mathfrak{M}$ e $\mathfrak{M}_\Delta$ são somas directas de sub-módulos admissíveis simples. Não há, porém, necessidade de restrições, em virtude do que se segue. Chamemos grupo indecomponível aquele que não pode escrever-se sob a forma de produto directo (aqui, soma directa) de grupos diferentes do grupo unidade. A teoria dos grupos com operadores (devida a Krull, para o caso comutativo,(1) e a Schmidt, para o caso geral(2)) ensina que um grupo com condição de máximo e mínimo, pondo de parte a ordem dos factores (ou parcelas) e isomorfismos, é um produto (ou soma) de factores (ou parcelas) indecomponíveis bem determinados. Ora $\mathfrak{M}$ e $\mathfrak{M}_\Delta$ satisfazem à dupla condição referida (ou, também, condição dupla de cadeia(3)). Nessas circunstâncias, se forem s e t, respectivamente, os números de sub-módulos indecomponíveis em que se decompõem $\mathfrak{M}$ e $\mathfrak{N}$, tem-se, em virtude do isomorfismo $\mathfrak{M}_\Delta \cong \mathfrak{N}_\Delta$ (o qual, valendo, por

(1) W.Krull, "Über verallgemeinerte endliche Abelsche Gruppen", Mathematische Zeitschrift, Band 23, 1925, pgs.161 a 196.

(2) O.Schmidt, "Über unendliche Gruppen mit endlicher Kette", Mathematische Zeitschrift, Band 29, 1928, pgs.34 a 41.

(3) Veja-se, para as diferentes afirmações, N.Jacobson, "The Theory of rings", pgs.10 a 13.

hipótese, relativamente a $\mathcal{Y}$ e a Δ, vale igualmente com respeito a $\mathcal{Y}$ e a $\mathcal{P}$) rs = rt, e, portanto, s = t. Assim, $\mathfrak{M}$ e $\mathfrak{N}$ decompõem-se no mesmo número de sub-módulos indecomponíveis, havendo em cada decomposição um sub-módulo isomorfo dum correspondente na outra. O lema preliminar está provado.

Passemos agora ao lema 1. Já vimos que se tem $\mathcal{Y}_\Delta \cong \mathcal{O}_\Delta$, relativamente a $\mathcal{Y}$ e a Δ. Mas pode escrever-se

$$\mathcal{Y}_\Delta = S_1\Delta + \cdots + S_n\Delta\,, \qquad \mathcal{O}_\Delta = a_1\Delta + \cdots + a_n\Delta\,,$$

onde $(a_1, \ldots, a_n)$ constitui também uma base de $\mathcal{O}$ relativamente a $\mathcal{P}$. O lema acabado de provar diz-nos que

$$\mathcal{Y}_\mathcal{P} = S_1\mathcal{P} + \cdots + S_n\mathcal{P}\,, \qquad \mathcal{O}_\mathcal{P} = \mathcal{O} = a_1\mathcal{P} + \cdots + a_n\mathcal{P}\,,$$

são igualmente isomorfos relativamente a $\mathcal{Y}$ e a $\mathcal{P}$. É o que se deseja.

Pode fazer-se a seguinte observação. As igualdades (5) dão uma representação de $\mathcal{Y}$ em Δ (ou de $\mathcal{Y}_\Delta$), que é também uma representação de $\mathcal{Y}$ em $\mathcal{P}$ (ou de $\mathcal{Y}_\mathcal{P}$). O módulo de representação é $\mathcal{O}_\Delta$. Obtem-se uma representação de $\mathcal{Y}$ em Δ, equivalente à anterior, utilizando $a_1, \ldots, a_n$ como base de $\mathcal{O}_\Delta$. As matrizes então obtidas para os elementos de $\mathcal{Y}_\mathcal{P}$ só contêm (como na representação referida de $\mathcal{Y}_\mathcal{P}$) elementos pertencentes a $\mathcal{P}$. As duas representações equivalentes em Δ são ainda equivalentes (quanto a $\mathcal{Y}_\mathcal{P}$) em $\mathcal{P}$, porque, tendo os mesmos traços, pertencem à mesma classe [A legitimidade desta conclusão só tem lugar com certas restrições, como se viu no Cap. IX, § 6].

É claro que o isomorfismo operatório $\mathcal{Y}_\mathcal{P} \cong \mathcal{O}$ não é único. Se considerarmos, com efeito, um automorfismo de $\mathcal{Y}_\mathcal{P}$, obtem-se, de modo evidente, um novo isomorfismo. Analisemos o automorfismo em questão (sempre relativo a $\mathcal{Y}$ e a $\mathcal{P}$). Aos elementos $S_1, \ldots, S_n$ corresponderão elementos $\sigma_1, \ldots, \sigma_n \in \mathcal{Y}_\mathcal{P}$, sendo ainda

$$S_1^{-1}S_1 = u \longrightarrow S_1^{-1}\sigma_1\,, \qquad Su \longrightarrow S\,S_1^{-1}\sigma_1\,, \qquad up = p \longrightarrow S_1^{-1}\sigma_1 \cdot p,$$

$$S_1p_1 + \cdots + S_np_n \longrightarrow (S_1 \cdot S_1^{-1}\sigma_1)p_1 + \cdots + (S_n \cdot S_1^{-1}\sigma_1)p_n = (S_1p_1 + \cdots + S_np_n)S_1^{-1}\sigma_1\,.$$

O automorfismo é definido pela multiplicação (à direita) pelo elemento $S_1^{-1}\sigma_1$. Este elemento tem necessàriamente inverso, visto que o automorfismo inverso, definido por Θ, satisfará à condição

$$S_1^{-1}\sigma_1 \longrightarrow S_1^{-1}\sigma_1 \cdot \Theta = u.$$

Nestes termos, é válido este

Aditamento ao lema 1:- No isomorfismo $\mathcal{Y}_\mathcal{P} \cong \mathcal{O}$, as imagens dos ideais direitos de $\mathcal{Y}_\mathcal{P}$ são invariantes, em face dos isomorfismos possíveis. Com efeito, se $\mathfrak{k}$ é um ideal direito de $\mathcal{Y}_\mathcal{P}$, e se Θ determina um automorfismo deste último módulo, $\mathfrak{k}$ transforma-se em $\mathfrak{k}\Theta \subseteq \mathfrak{k}$. Como Θ tem inverso, será também $\mathfrak{k}\Theta^{-1} \subseteq \mathfrak{k}$, e, portanto, $\mathfrak{k} \subseteq \mathfrak{k}\Theta$, ou seja $\mathfrak{k} = \mathfrak{k}\Theta$. A imagem global de $\mathfrak{k}$, em $\mathcal{O}$, é sempre a mesma.

Lema 2:- Se $\mathcal{G}_\mathcal{Y}$ é um sub-grupo do grupo de Galois $\mathcal{Y}$ e $\mathcal{L}$ é o corpo formado por todos os elementos de $\mathcal{O}$ que ficam invariantes em face das operações de $\mathcal{G}_\mathcal{Y}$, a imagem $\mathfrak{k}$, de $\mathcal{L}$, no isomorfismo $\mathcal{O} \cong \mathcal{Y}_\mathcal{P}$, é um ideal direito deste último. Pode considerar-se $\mathfrak{k}$ como módulo de representação recíproca de $\mathcal{Y}$ em $\mathcal{P}$, ou como módulo de representação directa de $\mathcal{G}_\mathcal{Y}$ em $\mathcal{P}$. Nesta última, $\mathcal{G}_\mathcal{Y}$ é representado pela matriz unidade. Além disso, $\mathfrak{k}$ é determinado por $\mathcal{G}_\mathcal{Y}$, independentemente do isomorfismo $\mathcal{O} \cong \mathcal{Y}_\mathcal{P}$ que for utilizado. $\mathcal{L}$ diz-se aqui um módulo de Galois. Adiante precisaremos esta noção. Fixemos desde já que, uma vez provado constituirem os elementos de $\mathfrak{k}$ um ideal direito, este fica determinado por $\mathcal{G}_\mathcal{Y}$, em consequência do aditamento ao lema 1. Demonstremos, pois, que $\mathfrak{k}$ é ideal. Se $f \in \mathcal{L}$, tem-se, para cada $T \in \mathcal{G}_\mathcal{Y}$, $Tf = f$. O correspondente de f, no isomorfismo, será da forma

$$g = \sum_S Sp_S\,, \qquad (S \in \mathcal{Y}\,,\ p_S \in \mathcal{P}). \tag{6}$$

Como o isomorfismo é operatório relativamente a $\mathcal{Y}$, ter-se-á

$$Tg = g = \sum_S T\,S \cdot p_S = \sum_S S \cdot p_{T^{-1}S} = \sum_S Sp_S\,,$$

o que implica

$$p_{T^{-1}s} = p_s \ , \qquad (T \in \mathcal{G} \ , \ S \in \mathcal{Y}). \qquad (7)$$

Obtém-se, em (7), uma condição necessária e suficiente, para que um elemento da forma (6) seja correspondente dum elemento $f \in \mathcal{L}$, isto é, pertença a $\mathfrak{K}$ [repare-se, entretanto, em que a correspondência $\mathcal{L} \leftrightarrow \mathfrak{K}$, que estamos estudando, não é uma correspondência entre dois sub-módulos admissíveis]. Em virtude de (7), cada elemento $g \in \mathfrak{K}$ pode escrever-se (e apenas os elementos de $\mathfrak{K}$ se podem assim escrever)

$$g = \sum_T (TS_1)p_1 + \cdots + \sum_T (TS_r)p_r \ , \qquad (p_i \in \mathcal{P}), \qquad (8)$$

se supusermos que r é o índice de $\mathcal{G}$, em $\mathcal{Y}$, e que $S_1, \ldots, S_r$ são representantes das r classes direitas distintas em que se decompõe $\mathcal{Y}$, por via da relação de equivalência introduzida por $\mathcal{G}$, em $\mathcal{Y}$. Para se ver que os elementos (8) constituem um ideal direito, basta observar as igualdades seguintes:

$$\left[\sum_T (TS_i)p_i\right] S = \sum_T (T \cdot S_i S)p_i = \sum_T (TS_j)p_i \ ,$$

com $S_i S = S_j$. Então, na verdade, quando se multiplica, à direita, um elemento (8) por $S \in \mathcal{Y}$, ou por $p \in \mathcal{P}$, ou ainda por $\Sigma S_i p_i \in \mathcal{Y}$, obtém-se de novo, um elemento (8). Dum modo mais preciso, a multiplicação por S leva a permutar entre si as somas ΣTS_i. O conjunto $\mathfrak{K}$ é, como se deseja, um ideal direito, módulo duma representação recíproca de $\mathcal{Y}$ em $\mathcal{P}$. O lema 2 está demonstrado.

Estamos agora em condições de provar o teorema fundamental. Dado um corpo $\mathcal{L}$, intermédio entre $\mathcal{P}$ e $\mathcal{O}$, sabemos que há um sub-grupo $\mathcal{G}$, de $\mathcal{Y}$, tal que $\mathcal{L}$ é sub-corpo invariante completo de $\mathcal{G}$, e este último, por definição, é sub-grupo invariante completo de $\mathcal{L}$. A ordem de $\mathcal{G}$ é, de resto, igual ao grau $(\mathcal{O}/\mathcal{L})$, e, por consequência, o índice de $\mathcal{G}$ será igual ao grau $(\mathcal{L}/\mathcal{P})$. Inversamente, dado $\mathcal{G}$, construamos o sub-corpo $\mathcal{L}$, composto de todos os elementos de $\mathcal{O}$ que ficam invariantes em face das operações de $\mathcal{G}$, nos termos do lema 2. Se determinarmos o sub-grupo $\mathcal{G}' \cong \mathcal{G}$, de $\mathcal{Y}$, conforme com o raciocínio directo anterior, sabemos ser ordem de $\mathcal{G}' = (\mathcal{O}/\mathcal{L})$. O lema 2 faz corresponder a $\mathcal{L}$ um ideal direito $\mathfrak{K}$, de ordem r = índice de $\mathcal{G}$, em $\mathcal{Y} = (\mathcal{L}/\mathcal{P})$.

Será, portanto,

$$n = \text{ordem de } \mathcal{G} \times r = (\mathcal{O}/\mathcal{L})\,(\mathcal{L}/\mathcal{P}) = (\mathcal{O}/\mathcal{L}).r,$$

$$\text{ordem de } \mathcal{G} = (\mathcal{O}/\mathcal{L}) \ , \qquad \mathcal{G} = \mathcal{G}' \ .$$

O teorema fundamental está completamente demonstrado.

Observações:- 1) Precisemos a noção de módulo de Galois. Dá-se essa designação às imagens, em $\mathcal{O}$, dos ideais direitos de $\mathcal{Y}_p$. Os módulos de Galois são, por isso, bem determinados, independentes do isomorfismo $\mathcal{Y}_p \cong \mathcal{O}$. Exemplos dos mesmos são dados pelos sub-corpos $\mathcal{L}$, intermédios entre $\mathcal{P}$ e $\mathcal{O}$. Cada módulo de Galois determina uma representação recíproca de $\mathcal{Y}$, em $\mathcal{P}$, a saber: a representação que pertence ao ideal direito de que o módulo é imagem. - 2) Dado um corpo $\mathcal{P}$, tanto importa que o referido corpo seja um campo de Galois (isto é, tenha um número finito de elementos) como um corpo com uma infinidade de elementos, sabe-se que o número de isomorfismos relativos a $\mathcal{P}$, duma ampliação $\mathcal{K}$, de $\mathcal{P}$, é igual ao grau $(\mathcal{K}/\mathcal{P})$, se $\mathcal{K}$ for separável, e apenas nesse caso. Nessas condições, o lema 1, demonstrado por Noether sob a hipótese de $\mathcal{P}$ ser infinito, admite a demonstração geral que foi dada, devido a Deuring. Ela utiliza, com efeito, apenas a circunstância de ser igual a n o número de isomorfismos de $\mathcal{O}$ relativamente a $\mathcal{P}$. - 3) Também pode demonstrar-se aqui, sem excepção, que, tanto $\mathcal{O}$ como qualquer corpo intermédio entre $\mathcal{P}$ e $\mathcal{O}$, são ampliações simples de $\mathcal{P}$.(1) Provemos o seguinte

Teorema:- Qualquer que seja $\mathcal{L}$, sob a condição $\mathcal{P} \subseteq \mathcal{L} \subseteq \mathcal{O}$, há sempre elementos $f \in \mathcal{L}$ tais que os seus conjugados, em número igual ao grau $(\mathcal{L}/\mathcal{P})$, são linearmente independentes relativamente a $\mathcal{P}$. Como consequência, resulta, então, que é $\mathcal{L} = \mathcal{P}(f)$, nos termos da observação 3).

Dado $\mathcal{L}$, procuremos $\mathcal{G}$, depois $\mathfrak{K}$. O índice de $\mathcal{G}$, em $\mathcal{Y}$, é $r = (\mathcal{L}/\mathcal{P})$. Seja $\delta \in \mathfrak{K}$. Por via de $T \in \mathcal{G}$, tem-se $T\delta = \delta$. Consideremos $S_1\delta, \ldots, S_r\delta$. Poderá encontrar-se δ de modo que estes elementos sejam independentes relativamente a $\mathcal{P}$? Basta pôr $\delta = \Sigma T$, pois que uma relação

$$(S_1 \cdot \Sigma T)p_1 + \cdots + (S_r \cdot \Sigma T)p_r = 0,$$

(1) Veja-se Almeida Costa, "Elementos da Teoria dos Anéis", pgs. 245 e 246.

dá $p_1 = \ldots = p_r = 0$. Pode dizer-se, assim, que o ideal esquerdo gerado por $\underline{\delta}$ tem a ordem $\underline{r}$. Procurando em $\mathcal{L}$ o elemento f, correspondente de $\underline{\delta}$, sabemos que $S_1 f, \ldots, S_r f$ são independentes (relativamente a $\mathcal{P}$). Ora, se supomos $\varphi(x) = 0$ a equação irredutível, com coeficientes de $\mathcal{P}$, a que satisfaz $\underline{f}$, tem-se $S_i \varphi(f) = \varphi(S_i f) = 0$, $(i = 1, \ldots, r)$. Por isso os $S_i f$ são conjugados de $\underline{f}$, o que prova o teorema.

Para terminarmos as considerações deste §, tomemos ainda $\mathcal{L} = \mathcal{N}$. Independentemente dos raciocínios que acabamos de fazer, sabemos que $\mathcal{N}$ é módulo da representação regular de $\mathcal{G}$ em, $\mathcal{P}$, representação que é equivalente à pertencente a $\mathcal{G}_p$. É possível, assim, escolher em $\mathcal{N}$ elementos base $b_1, \ldots, b_n$ tais que as matrizes da representação sejam as mesmas que resultam de (5). Os elementos Sb_i, $(i = 1, 2, \ldots, n)$, quando S varia, dão uma permutação dos elementos $\underline{b_i}$. Eles constituem os conjugados de $\underline{b_i}$. Este elemento satisfaz a uma equação do grau $\underline{n}$, tendo-se

$$\mathcal{N} = \mathcal{P}(b_i) , \qquad (i = 1, 2, \ldots, n).$$

Diz-se que os $\underline{b_i}$ constituem uma <u>base normal</u> de $\mathcal{N}$.

9) <u>A teoria de Galois dos corpos não comutativos</u> - Deve-se a <u>Noether</u> a teoria que vai expor-se neste §[1] e que pode adaptar-se ao caso anterior dos corpos comutativos[2]

Seja $\mathcal{K}$ um corpo não comutativo, de centro $\mathcal{P}$, finito sobre $\mathcal{P}$. Os automorfismos de $\mathcal{K}$ que deixam invariantes os elementos de $\mathcal{P}$ são sempre automorfismos internos (Cap. IX, § 4, 4ª aplicação, corolário 2). Seja, assim, $\mathcal{G}$ o grupo dos automorfismos de $\mathcal{K}$ relativamente a $\mathcal{P}$. Se designarmos por $\mathcal{K}^*$ os elementos regulares de $\mathcal{K}$ (elementos com inverso ou elementos diferentes de zero), tem lugar o isomorfismo grupal

$$\mathcal{G} \simeq \mathcal{K}^* / \mathcal{H} , \qquad (9)$$

onde $\mathcal{H}$ é o conjunto dos elementos de $\mathcal{K}^*$ que definem o automorfismo idêntico de $\mathcal{K}$. Se $\Theta \in \mathcal{H}$, ter-se-á

$$\Theta k \Theta^{-1} = k , \qquad \Theta k = k \Theta , \qquad (k \in \mathcal{K}).$$

(1) <u>Nichtkommutative Algebra</u>, pgs. 530 a 532.
(2) <u>Nichtkommutative Algebra</u>, pgs. 536 a 539

Será, pois, $\Theta \in \mathcal{P}$, e, portanto, $\mathcal{H} = \mathcal{P}^*$ = conjunto dos elementos regulares de $\mathcal{P}$. A todo o sub-grupo $\mathcal{G}_\mathcal{Y}$, de $\mathcal{G}$, corresponde, por via de (9), um sub-grupo $\mathcal{Z}_\mathcal{Y}$, de $\mathcal{K}^*/\mathcal{P}^*$, e, consequentemente, um sub-grupo $\mathcal{G}_\mathcal{Y}^* \supseteq \mathcal{P}^*$, de $\mathcal{K}^*$, de modo que $\mathcal{Z}_\mathcal{Y} = \mathcal{G}_\mathcal{Y}^* / \mathcal{P}^*$. O sub-grupo $\mathcal{G}_\mathcal{Y}$ diz-se <u>fechado</u> se o sub-anel $\mathcal{Y}$, de $\mathcal{K}$, gerado por $\mathcal{G}_\mathcal{Y}^*$, for simples, e, além disso, o conjunto dos elementos regulares de $\mathcal{Y}$ for precisamente $\mathcal{G}_\mathcal{Y}^*$. Vamos traduzir de modo mais simples estas condições, aliás utilizadas, de novo, no § seguinte. Em primeiro lugar, $\mathcal{Y}$, como sub-módulo de $\mathcal{K}$, admissível em face de $\mathcal{P}$, será um sistema hiper-complexo sobre $\mathcal{P}$, portanto um corpo (sub-corpo de $\mathcal{K}$). Em segundo lugar, os elementos regulares de $\mathcal{Y}$ serão todos os seus elementos não nulos. Pode, pois, dizer-se: $\mathcal{G}_\mathcal{Y}$ é fechado, se o conjunto $\{\mathcal{G}_\mathcal{Y}^*, 0\} = \mathcal{Y}$ constituir um corpo. À semelhança do que se fez no § anterior, demonstraremos aqui o seguinte

<u>Teorema fundamental:- Seja $\mathcal{K}$ um corpo não comutativo, de centro $\mathcal{P}$, finito sobre $\mathcal{P}$, e $\mathcal{G}$ o grupo dos seus automorfismos que deixam invariantes os elementos de $\mathcal{P}$ (automorfismos internos). Existe uma correspondência biunívoca completa entre os corpos intermédios Ψ, entre $\mathcal{P}$ e $\mathcal{K}$, e os sub-grupos fechados de $\mathcal{G}$, nas condições seguintes: 1) Ψ é sub-corpo invariante completo de $\mathcal{G}_\mathcal{Y}$; 2) $\mathcal{G}_\mathcal{Y}$ é sub-grupo invariante completo de Ψ.</u> A demonstração assenta sobre dois lemas que vão ser tratados.

Para deixarmos aos lemas toda a possível generalidade, tomemos um corpo $\mathcal{M}$, não comutativo, finito sobre $\mathcal{P}$, mas não tendo o centro necessàriamente igual a $\mathcal{P}$. Suponhamos $\mathcal{L}$ um corpo não comutativo, de centro $\mathcal{P}$, e admitamos que existe uma representação recíproca (anti-representação) do 1º grau (irredutível) de $\mathcal{M}$, em $\mathcal{L}$. O anel $\mathcal{M}_\mathcal{L}$ é simples, de sorte que tem lugar a decomposição seguinte, em ideais esquerdos simples:

$$\mathcal{M}_\mathcal{L} = \mathcal{M}_\mathcal{L} e_1 + \ldots + \mathcal{M}_\mathcal{L} e_n .$$

Visto que a representação anti-isomorfa em causa pertence a um dos ideais e que estes são todos isomorfos, ter-se-á

$$\mathcal{M}_\mathcal{L} = \mathcal{L} e_1 + \ldots + \mathcal{L} e_n ,$$

e a referida representação será definida, por ex., pela igualdade

$$m\, e_i = \lambda\, e_i \ , \qquad (m \in \mathfrak{M} \ , \ \lambda \in \mathfrak{L}) ,$$

pondo de parte uma equivalência.

Lema 1:- Não obstante equivalentes, são diferentes as anti-representações de $\mathfrak{M}$ definidas por $e_1, \ldots, e_n$. Imaginemos que pudesse ter-se, por ex.,

$$m\, e_1 = \lambda e_1 \ , \qquad m\, e_2 = \lambda e_2 \ .$$

Pelo facto de ser $\mathfrak{M}_{\mathfrak{L}}\, e_1 = \mathfrak{L}\, e_1$, pode definir-se a amplicação de $\mathfrak{M}_{\mathfrak{L}}$ a e_1, sem se sair do módulo $\mathfrak{L}\, e_1$. Esta aplicação define uma imagem homomorfa de $\mathfrak{M}_{\mathfrak{L}}$, no sentido operatório relativamente a $\mathfrak{L}$: se $\lambda_t, \mu_t \in \mathfrak{L}$, $m_t \in \mathfrak{M}$, é

$$(\sum \mu_t m_t) e_1 = \sum \mu_t (m_t e_1) = \sum \mu_t (\lambda_t e_1) = (\sum \mu_t \lambda_t) e_1 .$$

o mesmo raciocínio se faz sobre $\mathfrak{L}\, e_2$. E verifica-se que os dois homomorfismos operatórios de $\mathfrak{M}_{\mathfrak{L}}$ serão idênticos, se forem idênticas as anti-representações de $\mathfrak{M}$ definidas por e_1 e e_2. Mas, sendo $e_1 e_1 = e_1$, $e_1 e_2 = 0$, esta última identidade (das representações) não pode ter lugar. O lema é válido.

Lema 2:- Se Ψ é um corpo intermédio entre $\mathfrak{P}$ e $\mathfrak{M}$, e s é a ordem de $\mathfrak{M}$ relativamente a Ψ, cada anti-isomorfismo de Ψ, em $\mathfrak{L}$, admite, pelo menos, s prolongamentos para anti-isomorfismos de $\mathfrak{M}$, em $\mathfrak{L}$. Estamos seguros da existência duma anti-representação do 1º grau, de Ψ, em $\mathfrak{L}$, por existir uma tal anti-representação de $\mathfrak{M}$. Como $\Psi_{\mathfrak{L}}$ é um anel simples, segue-se que todas as representações recíprocas irredutíveis de Ψ, em $\mathfrak{L}$, são do 1º grau e que se tem

$$\Psi_{\mathfrak{L}} = \Psi_{\mathfrak{L}} E_1 + \cdots + \Psi_{\mathfrak{L}} E_h = \mathfrak{L} E_1 + \cdots + \mathfrak{L} E_h \ .$$

O número h representa a ordem de $\Psi_{\mathfrak{L}}$ relativamente a $\mathfrak{L}$, que é também a ordem do módulo Ψ relativamente a $\mathfrak{P}$. A partir dos idempotentes ortogonais E_t, pode também escrever-se

$$\mathfrak{M}_{\mathfrak{L}} = \mathfrak{M}_{\mathfrak{L}} E_1 + \cdots + \mathfrak{M}_{\mathfrak{L}} E_h .$$

De resto, sendo

$$\mathfrak{M} \Psi_{\mathfrak{L}} = \mathfrak{M}_{\mathfrak{L}} = \mathfrak{M} \mathfrak{L} E_1 + \cdots + \mathfrak{M} \mathfrak{L} E_h = \mathfrak{M}_{\mathfrak{L}} E_1 + \cdots + \mathfrak{M}_{\mathfrak{L}} E_h \ , \qquad (10)$$

a conclusão é a mesma. É claro que os E_t não são idempotentes primitivos e que uma decomposição de $\mathfrak{M}_{\mathfrak{L}}$ em ideais esquerdos simples se obtém decompondo os E_t em idempotentes primitivos ortogonais. Estudemos $\mathfrak{M}_{\mathfrak{L}} E_t$. Ponhamos

$$\mathfrak{M} = u_1 \Psi + \cdots + u_s \Psi \ , \quad \mathfrak{L}\, \mathfrak{M} = \mathfrak{M}_{\mathfrak{L}} = \mathfrak{L}\, u_1 \Psi + \cdots + \mathfrak{L}\, u_s \Psi \ .$$

Tendo em vista que os elementos de $\mathfrak{M}$ e de $\mathfrak{L}$ são comutáveis, é também

$$\mathfrak{M}_{\mathfrak{L}} = u_1 \mathfrak{L} \Psi + \cdots + u_s \mathfrak{L} \Psi = u_1 \Psi_{\mathfrak{L}} + \cdots + u_s \Psi_{\mathfrak{L}} .$$

As somas escritas são sempre directas. De facto, supondo $\mathfrak{M}_{\mathfrak{L}}$ de ordem n relativamente a $\mathfrak{L}$, ou seja $\mathfrak{M}$ de ordem n relativamente a $\mathfrak{P}$, tem-se $n = sh$. A ordem de cada $u_j \Psi_{\mathfrak{L}}$ relativamente a $\mathfrak{L}$ é h, e a soma $\Sigma u_t \Psi_{\mathfrak{L}}$ é directa. Mas tem-se agora

$$\mathfrak{M}_{\mathfrak{L}} E_t = u_1 \Psi_{\mathfrak{L}} E_t + \cdots + u_s \Psi_{\mathfrak{L}} E_t = u_1 \mathfrak{L} E_t + \cdots + u_s \mathfrak{L} E_t =$$

$$= \mathfrak{L}\, u_1 E_t + \cdots + \mathfrak{L}\, u_s E_t .$$

Esta soma não pode deixar de ser directa, visto que ela, tendo em conta (10), mostra que a ordem de $\mathfrak{M}_{\mathfrak{L}}$, relativamente a $\mathfrak{L}$, é hs, quando muito. Ora já sabemos que é precisamente hs. Ponhamos

$$\mathfrak{M}_{\mathfrak{L}} E_t = \mathfrak{M}_{\mathfrak{L}} e_{t1} + \cdots + \mathfrak{M}_{\mathfrak{L}} e_{ts} = \mathfrak{L}\, e_{t1} + \cdots + \mathfrak{L}\, e_{ts} \ ,$$

onde os e_{tj} são idempotentes primitivos ortogonais. Vamos ver que as s representações recíprocas diferentes de $\mathfrak{M}$, em $\mathfrak{L}$, pertencentes aos e_{tj}, são todas prolongamentos duma mesma representação recíproca de Ψ, em $\mathfrak{L}$: a representação definida por E_t. De facto, supondo

$$\psi E_t = \lambda E_t \ , \qquad (\psi \in \Psi, \ \lambda \in \mathfrak{L}) \ ,$$

vem, sucessivamente,

$$\psi E_l = \psi e_{l1} + \cdots + \psi e_{ls} = \lambda E_l = \lambda e_{l1} + \cdots + \lambda e_{ls}\,, \quad \psi e_{lj} = \lambda e_{lj}\,,$$

como se afirmou. Para completar a demonstração do lema, resta apenas provar que toda a representação do 1º grau de Ψ, em $\mathcal{L}$, é sempre definida por um idempotente. Se fosse definida por μE_l, $(\mu \in \mathcal{L})$, ter-se-ia

$$\psi(\mu E_l) = \lambda(\mu E_l)\,,$$

$$\psi(\mu E_l \mu^{-1}) = \psi(\mu E_l).\mu^{-1} = \lambda(\mu E_l).\mu^{-1} = \lambda(\mu E_l \mu^{-1})\,.$$

A representação em causa seria definida pelo idempotente $\mu E_l \mu^{-1}$, que pode fazer-se figurar na decomposição

$$\Psi_{\mathcal{L}} = \mathcal{L}.\mu E_1 \mu^{-1} + \cdots + \mathcal{L}.\mu E_h \mu^{-1}.$$

Passemos ao teorema fundamental. Consideremos a sucessão de corpos $\mathfrak{K} \supseteq \Psi \supseteq \mathcal{P}$. Embora $\mathfrak{K}$ tenha o centro $\mathcal{P}$, no geral o corpo não comutativo Ψ não está nessas condições. No corpo $\mathcal{L}$, anti-isomorfo de $\mathfrak{K}$, admite este último uma anti-representação irredutível do 1º grau. Na totalidade das representações do 1º grau de $\mathfrak{K}$, em $\mathcal{L}$, vamos definir uma relação de equivalência, considerando cada classe de equivalentes C_Ψ constituida por aquelas representações que levam à mesma representação de Ψ. Se, na nova sucessão de corpos $\mathfrak{K} \supseteq \Phi \supseteq \Psi \supseteq \mathcal{P}$, for ρ a ordem de Φ relativamente a Ψ, sabemos que toda a representação do 1º grau de Ψ, em $\mathcal{L}$, se pode prolongar, pelo menos de ρ maneiras, para representações de Φ, em $\mathcal{L}$. Uma classe C_Ψ decompõe-se, portanto, em ρ classes C_Φ, pelo menos. Posto isto, regressemos à sucessão $\mathfrak{K} \supseteq \Psi \supseteq \mathcal{P}$. Se $\mathfrak{K}_1, \mathfrak{K}_1', \mathfrak{K}_1'', \ldots$ forem as diferentes representações (em causa) de $\mathfrak{K}$, em $\mathcal{L}$, podemos supor

$$i_1 \mathfrak{K} = \mathfrak{K}_1\,, \qquad i_1' \mathfrak{K} = \mathfrak{K}_1'\,, \qquad i_1'' \mathfrak{K} = \mathfrak{K}_1''\,, \ldots$$

desde que representemos pelos símbolos $i_1, i_1', i_1'', \ldots$ operadores correspondentes, de significado evidente. Neste sentido, os símbolos

$$i_1^{-1} i_1\,, \quad i_1^{-1} i_1'\,, \quad i_1^{-1} i_1''\,, \ldots \qquad (11)$$

representam os automorfismos internos de $\mathfrak{K}$, ou seja os elementos de $\mathcal{G}$. Se um certo conjunto $i_1, i_1', i_1'', \ldots$ determina uma classe C_Γ, os elementos correspondentes de (11) determinam a totalidade $\mathcal{G}_\Psi$ dos automorfismos de $\mathcal{G}$ que conservam Ψ. Do sub-grupo $\mathcal{G}_\Psi$ elevamo-nos sucessivamente a $\bar{\mathcal{G}}_\Psi$, $\mathcal{G}_\Psi^*$, $\mathcal{T}$. Verifica-se que $\mathcal{G}_\Psi$ é fechado. O corpo $\mathcal{T}$ compõe-se dos elementos de $\mathfrak{K}$ que comutam com Ψ e apenas desses elementos. Em particular é $\mathcal{P} \subseteq \mathcal{T}$. Vê-se, do raciocínio feito até agora, que $\mathcal{G}_\Psi$ é sub-grupo invariante completo do corpo Ψ. O lema 2 permite-nos provar que, em sentido recíproco, Ψ é sub-corpo invariante completo do grupo $\mathcal{G}_\Psi$. Procuremos, com efeito, o conjunto dos elementos de $\mathfrak{K}$ que comutam com $\mathcal{T}$. Será um corpo $\Gamma \supseteq \Psi$. Se pudesse ter-se $\mathfrak{K} \supseteq \Gamma \supset \Psi \supseteq \mathcal{P}$, o sub-grupo invariante completo de Γ seria $\mathcal{G}_\Psi' \subset \mathcal{G}_\Psi$, consequentemente viria $\mathcal{G}_\Psi'^* \subset \mathcal{G}_\Psi^*$; $\mathcal{T}' \subset \mathcal{T}$. Desde que $\mathcal{T}'$ representa o conjunto dos elementos de $\mathfrak{K}$ que comutam com Γ, tal conjunto não pode ser sub-conjunto próprio de $\mathcal{T}$. É absurdo supor $\Gamma \supset \Psi$, valendo $\Gamma = \Psi$. É claro que, se, em vez de partirmos de Ψ, partirmos de $\mathcal{G}_\Psi$ (fechado), construimos Γ, depois o corpo Ψ composto dos elementos comutáveis com os elementos de $\mathcal{T}$. O teorema fundamental está provado.

10) A teoria de Galois dos sistemas simples - Seja $\mathfrak{K}_m$ uma álgebra normal simples sobre $\mathcal{P}$. Os automorfismos de $\mathfrak{K}_m$ que deixam fixos os elementos de $\mathcal{P}$ são automorfismos internos (Cap. IX, § 4, 4ª aplicação, corolário 2). Se designarmos por $\mathfrak{K}_m^*$ o conjunto dos elementos regulares de $\mathfrak{K}_m$, tem lugar o isomorfismo grupal

$$\mathcal{G} \cong \mathfrak{K}_m^* / \mathcal{P}^*, \qquad (12)$$

entre o grupo $\mathcal{G}$ dos automorfismos citados e o grupo factor do 2º membro. $\mathcal{P}^*$ é o conjunto dos elementos de $\mathcal{P}$ diferentes de zero (ou conjunto dos elementos de $\mathfrak{K}_m$ cada um dos quais define o automorfismo idêntico desta álgebra). Como no § anterior, dado um sub-grupo $\mathcal{G}_\Psi$, de $\mathcal{G}$, passa-se, por via de (12), a $\mathcal{G}_\Psi \cong \bar{\mathcal{G}}_\Psi = \mathcal{G}_\Psi^* / \mathcal{P}^*$. Diz-se que $\mathcal{G}_\Psi$ é fechado, se $\mathcal{G}_\Psi^* \subset \mathfrak{K}_m$ gerar um sub-anel simples cujos elementos regulares sejam precisamente os elementos de $\mathcal{G}_\Psi^*$ e apenas esses. Tem lugar a seguinte proposição de E. Noether:

Teorema fundamental:- Seja $\mathfrak{A}_m$ uma álgebra normal simples, de centro $\mathfrak{P}$, e $\mathcal{G}$ o grupo dos seus automorfismos que deixam invariantes os elementos de $\mathfrak{P}$ (automorfismos internos). Existe uma correspondência biunívoca completa entre os sistemas hiper-complexos simples $\mathfrak{T}$, intermédios entre $\mathfrak{P}$ e $\mathfrak{A}_m$, e os sub-grupos fechados de $\mathcal{G}$, nas condições seguintes: 1) $\mathfrak{T}$ é sub-domínio invariante completo de $\mathfrak{H}$; 2) $\mathfrak{H}$ é sub-grupo invariante completo de $\mathfrak{T}$. A demonstração assenta no lema que vamos enunciar e que provaremos a seguir ao teorema.

Lema:- Um sistema hiper-complexo simples $\mathfrak{A}$, sobre $\mathfrak{P}$, é gerado pelos seus elementos regulares.(1)

Dado este enunciado, tenhamos também em conta o teorema 3 do Cap.IX, § 4, 4ª aplicação. Então, consideremos a sucessão $\mathfrak{A}_m \supseteq \mathfrak{T} \supseteq \mathfrak{P}$ e o sub-grupo $\mathfrak{H}$, de $\mathcal{G}$, formado pelos automorfismos Θ, de $\mathfrak{A}_m$, que deixam invariantes os elementos $S \in \mathfrak{T}$. Sendo

$$\Theta S = \alpha S \alpha^{-1} = S , \quad \text{ou} \quad \alpha S = S\alpha , \qquad (\alpha \in \mathfrak{A}_m) ,$$

vê-se que a cada Θ se pode fazer corresponder, pelo menos, um elemento regular α do comutador $\overline{\mathfrak{T}}$, de $\mathfrak{T}$. A recíproca é válida. Será, por consequência,

$$\mathfrak{H} \cong \overline{\mathfrak{T}}^* / \mathfrak{P}^* .$$

O sub-grupo $\mathfrak{H}$ é fechado, porque, tendo-se $\mathfrak{H}^* = \overline{\mathfrak{T}}^*$, este último conjunto, em face do lema, gera $\mathfrak{T}$, que é simples. Sem dúvida que $\mathfrak{H}$ é sub-grupo invariante completo de $\mathfrak{T}$. Para se ver que $\mathfrak{T}$ é domínio invariante completo de $\mathfrak{H}$, tomemos um elemento $\beta \in \mathfrak{A}_m$, tal que, qualquer que seja $\Theta \in \mathfrak{H}$, seja $\Theta\beta = \beta$. Então virá $\alpha\beta\alpha^{-1} = \beta$, $\alpha\beta = \beta\alpha$, e β será um elemento comutável com qualquer $\tau \in \overline{\mathfrak{T}}$. Será, assim, $\beta \in \mathfrak{T}$, precisamente pelo teorema 3, do Cap.IX, acima

(1) Este lema, com toda a generalidade, é devido a K.Shoda, "Über die Galoissche Theorie der halbeinfachen hyperkomplexen Systeme", Mathematische Annalen, Band 107, 1933, pgs.252 a 258.

citado. Em resumo: partindo de $\mathfrak{T}$, obtém-se $\mathfrak{H}$; inversamente, dado $\mathfrak{H}$, suposto fechado, passa-se a $\mathfrak{H}^*$, depois a uma álgebra simples $\widetilde{\mathfrak{T}}$ contendo $\mathfrak{P}$ e gerada por $\mathfrak{H}^*$, finalmente a $\mathfrak{T}$. O teorema fundamental está provado. Ele contém o teorema fundamental do § anterior como caso particular.

Resta o lema. Suponhamos, como habitualmente, $\mathfrak{P} \subseteq \mathfrak{A}$. O elemento $u \in \mathfrak{P}$ é regular. Se $r \in \mathfrak{A}$ for um elemento nilpotente, sabemos que $u + r$ (Cap.I, pgs.7) é um elemento regular. Pondo $u + r = v$, ou seja $r = v - u$, vê-se que todo o elemento nilpotente pertence ao sub-anel $\mathfrak{T}$, gerado pelos elementos regulares de $\mathfrak{A}$. Se for

$$\mathfrak{A} = \sum_{i,j} e_{ij} \mathfrak{L} , \qquad (\mathfrak{P} \subseteq \mathfrak{L}) ,$$

como cada $e_{ij}\tau$, $(i \neq j, \tau \in \mathfrak{L})$, é nilpotente, conclui-se $e_{ij}\mathfrak{L} = \mathfrak{T}$. Por outro lado, tem-se $E = (e_{21} + \cdots + e_{n1})(e_{12} + e_{13} + \cdots + e_{1n}) = (e_{22} + e_{23} + \cdots + e_{2n}) + (e_{32} + e_{33} + \cdots + e_{3n}) + \cdots + (e_{n2} + e_{n3} + \cdots + e_{nn}) = (u - e_{11})$ + elementos nilpotentes. Ora tem-se $E \in \mathfrak{T}$, por ser o produto de dois elementos pertencentes a $\mathfrak{T}$. Da relação anterior, tira-se $u - e_{11} \in \mathfrak{T}$. Será, assim, $e_{11} = u - (u - e_{11}) \in \mathfrak{T}$, e, portanto, $e_{11}\mathfrak{L} \subseteq \mathfrak{T}$. Do mesmo modo se prova $e_{ii}\mathfrak{L} \subseteq \mathfrak{T}$, o que leva a $\mathfrak{T} = \mathfrak{A}$, q. e. d.

11) Sobre os corpos de sub-decomposição e de decomposição das álgebras simples - Depois de termos reduzido, no § 2, o problema dos corpos de sub-decomposição e decomposição duma álgebra ao problema correspondente das álgebras simples, vamos dar alguns detalhes sobre esta última questão.

Seja $\mathfrak{A}$ uma álgebra simples sobre $\mathfrak{P}$. Se for uma álgebra normal, o caso fica ilucidado pelo teorema 3 do referido § 2. Suponhamos agora que $\mathfrak{A}$ não é normal, mas limitemo-nos a supor que o centro $\mathfrak{Z}$, de $\mathfrak{A}$, é ampliação separável de $\mathfrak{P}$. O teorema 10, do § 5, do Cap.VII, garante-nos que $\mathfrak{A}_\Delta$, qualquer que seja o corpo comutativo $\Delta \supseteq \mathfrak{P}$, é semi-simples. $\mathfrak{A}$ é uma álgebra separável. Se Ψ for um corpo de sub-decomposição de $\mathfrak{A}$, há, em Ψ, uma representação absolutamente irredutível de $\mathfrak{A}$, a qual se prolonga para uma representação absolutamente irredutível, bem determinada, de $\mathfrak{A}_\Psi$, em Ψ. O centro $\mathfrak{Z}_\Psi$, de $\mathfrak{A}_\Psi$, e bem assim o centro $\mathfrak{Z}$, de $\mathfrak{A}$, são representados por matrizes múltiplas da matriz unida-

de (Cap.IX, § 5, teorema 5). Há, portanto, em Ψ, um sub-corpo $\mathfrak{z}_1$, isomorfo de $\mathfrak{z}$ relativamente a $\mathfrak{P}$, sub-corpo que dá uma representação absolutamente irredutível (do 1º grau) de $\mathfrak{z}$, em Ψ. Vamos ver que, inversamente, o conhecimento desta última representação do 1º grau identifica a representação absolutamente irredutível de $\mathcal{U}$, em Ψ. De facto, ela prolonga-se para uma representação absolutamente irredutível (do 1º grau), bem determinada, de $\mathfrak{z}_\Psi$, em Ψ, o que identifica uma representação irredutível de $\mathcal{U}_\Psi$, em Ψ, e, portanto, uma representação irredutível de $\mathcal{U}$, em Ψ. Esta última não pode deixar de ser aquela de que se partiu.

Em virtude de Ψ conter o corpo $\mathfrak{z}_1 \cong \mathfrak{z}$ relativamente a $\mathfrak{P}$, podemos supor $\Psi \supseteq \mathfrak{z}$. Por outro lado, limitar-nos-emos ao caso de Ψ ser uma ampliação finita de $\mathfrak{P}$. Vemos, então, que a representação de $\mathcal{U}$ (sobre $\mathfrak{P}$), em Ψ, se pode imaginar operatória homomorfa relativamente a $\mathfrak{z}$, pelo que se trata duma representação absolutamente irredutível da álgebra normal simples $\mathcal{U} = \mathfrak{A}_\rho$ (sobre $\mathfrak{z}$) no corpo $\Psi \supseteq \mathfrak{z}$. A representação irredutível única, do grau r, no corpo $\mathfrak{A}$, de Ψ (sobre $\mathfrak{z}$), é um sub-corpo comutativo máximo $\Psi^* \subseteq \mathfrak{A}_r$, sub-corpo que contém um corpo $\mathfrak{z}^* \cong \mathfrak{z}$. Podemos enunciar o seguinte

Teorema 1:- É condição necessária e suficiente, para que uma ampliação finita Ψ, de $\mathfrak{P}$, seja corpo de sub-decomposição da álgebra simples $\mathcal{U} = \mathfrak{A}_\rho$, sobre $\mathfrak{P}$, de centro separável $\mathfrak{z} \cong \mathfrak{P}$ (admitindo ser $\Psi \supseteq \mathfrak{z}$), que a representação irredutível única, de grau r, de Ψ (sobre $\mathfrak{z}$), em $\mathfrak{A}$, seja um sub-corpo comutativo máximo de $\mathfrak{A}_r$ (contendo um corpo isomorfo de $\mathfrak{z}$). Já demonstrámos que a condição é necessária. Inversamente, dada a álgebra simples $\mathcal{U} = \mathfrak{A}_\rho$, sobre $\mathfrak{P}$, de centro separável $\mathfrak{z} \cong \mathfrak{P}$, consideremos um corpo comutativo finito Ψ, sobre $\mathfrak{z}$, tal que a representação irredutível única, de grau r, de Ψ, em $\mathfrak{A}$, operatório relativamente a $\mathfrak{z}$, seja um sub-corpo comutativo máximo Ψ^*, de $\mathfrak{A}_r$, contendo $\mathfrak{z}^* \cong \mathfrak{z}$. Vamos ver que Ψ é corpo de sub-decomposição de $\mathcal{U}$, sobre $\mathfrak{P}$. Efectivamente, a representação irredutível única de $\mathcal{U}$, em Ψ, operatória relativamente a $\mathfrak{z}$, é absolutamente irredutível. Considerada como representação de $\mathcal{U}$, sobre $\mathfrak{P}$, em Ψ, do mesmo grau σ, se for $\sigma = 1$, trata-se duma representação absolutamente irredutível neste último sentido. Supondo $\sigma > 1$, a representação continua a ser absolutamente irredutível, pois que,

se o não fosse, tomando o corpo algèbricamente fechado $\Omega \supseteq \Psi$, chegaríamos a obter uma representação absolutamente irredutível de $\mathcal{U}$, sobre $\mathfrak{P}$, em Ω, de grau $\sigma' < \sigma$. Estaríamos também em presença duma representação absolutamente irredutível da álgebra $\mathcal{U}$, sobre $\mathfrak{z}$, o que seria absurdo, pelo facto de se ter $\sigma' < \sigma$.

Imaginemos, em seguida, que Ψ é corpo de decomposição de $\mathcal{U}$, sobre $\mathfrak{P}$. Pondo $\mathcal{U}_\Psi = \mathcal{U}_\Psi e_1 + \cdots + \mathcal{U}_\Psi e_n$, o número de álgebras simples, sobre Ψ, em que se decompõe $\mathcal{U}_\Psi$, é igual à característica $(\mathfrak{z}/\mathfrak{P}) = n$ do centro de $\mathcal{U}$ (Cap.IX, § 5, teorema 7'). No corpo Ψ há n representações do 1º grau de $\mathfrak{z}$, que são dadas por corpos isomorfos de $\mathfrak{z}$: $\mathfrak{z}_1, \mathfrak{z}_2, \ldots, \mathfrak{z}_n$. Significa isto que Ψ possui um corpo isomorfo da ampliação de Galois mínima de $\mathfrak{P}$ que contém $\mathfrak{z}$. É claro que se tem $\mathfrak{z}_\Psi = \Psi e_1 + \cdots + \Psi e_n$. Uma realização de Ψ, ampliação finita de $\mathfrak{P}$, obtém-se como segue. Tomemos um corpo $\Theta \supseteq \mathfrak{z}$, ampliação finita de $\mathfrak{P}$, que seja corpo de decomposição de $\mathfrak{z}$: $\mathfrak{z}_\Theta = \Theta e_1 + \cdots + \Theta e_n$. Pondo $\mathcal{U}_\Theta = \mathcal{U}_\Theta e_1 + \cdots + \mathcal{U}_\Theta e_n$, cada álgebra $\mathcal{U}_\Theta e_\ell$, sobre Θ, é álgebra simples de centro Θe_ℓ. Se Ω é um corpo de sub-decomposição de $\mathcal{U}$ contendo Θ e ampliação finita deste, é fácil de ver que, na decomposição

$$\mathcal{U}_\Omega = \mathcal{U}_\Omega e_1 + \cdots + \mathcal{U}_\Omega e_n ,$$

cada parcela $\mathcal{U}_\Omega e_\ell$ é anel completo de matrizes com elementos dum corpo isomorfo de Ω. Basta ver que a uma representação absolutamente irredutível de $\mathcal{U}$, em Ω, ou de $\mathcal{U}_\Omega$, em Ω, correspondem representações absolutamente irredutíveis dos $\mathcal{U}_\Omega e_\ell$, nos Ωe_ℓ respectivos e que os $\mathcal{U}_\Omega e_\ell$ são álgebras normais sobre os Ωe_ℓ. Podemos afirmar, por consequência, que Ω é corpo de decomposição de $\mathcal{U}$. Tem lugar o

Teorema 2:- É condição necessária e suficiente, para que uma ampliação finita Ω, de $\mathfrak{P}$, seja corpo de decomposição da álgebra simples $\mathcal{U} = \mathfrak{A}_\rho$, de centro separável $\mathfrak{z} \cong \mathfrak{P}$, que contenha um corpo de sub-decomposição de $\mathcal{U}$ e um corpo de decomposição de $\mathfrak{z}$. É evidente que, se for $\mathfrak{z}$ ampliação de Galois de $\mathfrak{P}$, um corpo de sub-decomposição de $\mathcal{U}$ é já seu corpo de decomposição. Nesse caso os corpos mínimos de sub-decomposição são também corpos mínimos de decomposição. Esta circunstância pode ainda ter lugar, mesmo que $\mathfrak{z}$ não seja de Galois, contanto que o sub-

-corpo de decomposição mínimo de $\mathcal{A}$ contenha logo uma ampliação de $\mathcal{P}$ isomorfa da ampliação de Galois mínima de $\mathcal{P}$ que contém $\mathcal{Z}$.

Capítulo XII

Produtos cruzados

1) Definição e construção de produtos cruzados (1) - Representemos por $\mathcal{K}$ uma ampliação finita, normal e separável, do grau n, do corpo comutativo $\mathcal{P}$. Se for $\mathcal{G}$ o grupo dos automorfismos de $\mathcal{K}$ relativamente a $\mathcal{P}$, poremos $\mathcal{G}=\{\rho, \sigma, \ldots, \tau\}$. Consideremos, em seguida, os n símbolos $u_\rho, u_\sigma, \ldots, u_\tau$ e o módulo de ordem n relativamente a $\mathcal{K}$ da forma $\mathcal{K}u_\rho + \mathcal{K}u_\sigma + \ldots + \mathcal{K}u_\tau$. O elemento $u \in \mathcal{K}$ supõe-se operador unitário do módulo. Vamos introduzir agora uma multiplicação, pondo

$$\sum_\rho \alpha_\rho u_\rho \cdot \sum_\sigma \beta_\sigma u_\sigma = \sum_{\rho,\sigma} \alpha_\rho \beta_\sigma^\rho a_{\rho,\sigma} u_{\rho\sigma} \cdot \qquad (1)$$

Nesta igualdade, nos somatórios, figuram os elementos de $\mathcal{G}$ como índices de soma. Os elementos α_ρ, β_σ, $a_{\rho,\sigma}$ pertencem a $\mathcal{K}$. O símbolo $\rho\sigma$ representa o produto de dois automorfismos de $\mathcal{K}$ relativamente a $\mathcal{P}$, supondo-se, todavia, que σ se efectua em primeiro lugar. Finalmente, um símbolo da forma τ^ρ, onde $\tau \in \mathcal{K}$, significa o transformado de τ por via de ρ [Quando se escrever $\rho = 1$, tem-se o automorfismo idêntico de $\mathcal{K}$].

A multiplicação definida em (1) dá, em particular,

$$u_\rho u_\sigma = a_{\rho,\sigma} u_{\rho\sigma} \cdot \qquad (2)$$

A fim de que o módulo, já fechado com respeito ao produto, se torne num anel $\mathcal{A}$, necessitamos fazer verificar as leis distributivas e a lei associativa da multiplicação. As leis distributivas são válidas, em virtude da própria igualdade (1), se admitirmos que nos somatórios não há repetição de parcelas contendo um dado u_ρ. De contrário, notando que é

$$(\alpha u_\rho + \beta u_\rho) \cdot \tau u_\sigma = (\alpha + \beta) u_\rho \cdot \tau u_\sigma = (\alpha + \beta) \tau^\rho a_{\rho,\sigma} u_{\rho\sigma} =$$

$$= \alpha \tau^\rho a_{\rho,\sigma} u_{\rho\sigma} + \beta \tau^\rho a_{\rho,\sigma} u_{\rho\sigma} = \alpha u_\rho \cdot \tau u_\sigma + \beta u_\rho \cdot \tau u_\sigma ,$$

fica provada a lei distributiva direita. A lei distributiva esquerda tem demonstração análoga. Quanto à lei associativa, escrevamos

$$\alpha u_\rho \cdot (\beta u_\sigma \cdot \tau u_\tau) = (\alpha u_\rho \cdot \beta u_\sigma) \cdot \tau u_\tau \cdot$$

Deduz-se, sucessivamente:

$$\alpha u_\rho \cdot \beta \tau^\rho a_{\sigma,\tau} u_{\sigma\tau} = \alpha \beta^\rho a_{\rho,\sigma} u_{\rho\sigma} \cdot \tau u_\tau ,$$

$$\alpha \beta^\rho \tau^{\rho\sigma} a_{\sigma,\tau}^\rho a_{\rho,\sigma\tau} u_{\rho\sigma\tau} = \alpha \beta^\rho a_{\rho,\sigma} \tau^{\rho\sigma} a_{\rho\sigma,\tau} u_{\rho\sigma\tau} ;$$

de sorte que a lei associativa impõe aos $a_{\rho,\sigma}$ as propriedades seguintes (também suficientes):

$$a_{\sigma,\tau}^\rho a_{\rho,\sigma\tau} = a_{\rho,\sigma} a_{\rho\sigma,\tau} \cdot \qquad (3)$$

O anel $\mathcal{A}$, acabado de construir, diz-se um produto cruzado. Um produto cruzado fica definido, pois, dando os corpos $\mathcal{K}$ e $\mathcal{P}$, assim como um sistema de elementos $a_{\rho,\sigma} \in \mathcal{K}$, satisfazendo a (3). Este sistema diz-se um sistema de factores. Escreveremos $\mathcal{A} = (\mathcal{K}/\mathcal{P}, a_{\rho,\sigma})$.

(1) A teoria dos produtos cruzados encontra-se tratada nos livros de texto já citados por várias vezes: "Algebren", de Deuring; "Structure of algebras", de Albert; "The Theory of rings", de Jacobson. O livro que seguimos mais de perto é, porém, o seguinte: "Rings with minimum condition", de E. Artin, C.J. Nesbitt, e R.M. Thrall, Michigan, 1944. A parte final do Capítulo (§ 7 e seguintes) será consagrada a uma extensão da teoria, conforme O. Teichmüller.

Como casos particulares das relações (3), podemos observar as igualdades

$$a^{i}_{i,\sigma}a_{i,\sigma} = a_{i,i}a_{i,\sigma} \; ; \qquad a^{\sigma}_{i,i}a_{\sigma,i} = a_{\sigma,i}a_{\sigma,i} \; , \qquad (4)$$

das quais se deduz $a_{i,\sigma} = a_{i,i}$, $a^{\sigma}_{i,i} = a_{\sigma,i}$.

O anel $\mathcal{A}$, que é módulo de ordem n relativamente a $\mathcal{K}$, pode considerar-se um módulo de ordem n^2 relativamente a $\mathcal{P}$, por ser $(\mathcal{K}/\mathcal{P}) = n$. Neste sentido, vamos demonstrar a importante proposição:

Teorema 1:- Um produto cruzado $\mathcal{A} = (\mathcal{K}/\mathcal{P}, a_{\rho,\sigma})$ é uma álgebra central simples[1] sobre $\mathcal{P}$, de ordem n^2, que contém "mergulhado", de modo irredutível, o corpo $\mathcal{K}$ (de ordem n relativamente a $\mathcal{P}$), o qual é seu corpo de decomposição. Aceitemos que $\mathcal{A}$ é uma álgebra sobre $\mathcal{P}$. Vamos ver que o elemento $U = a^{-1}_{i,i}u^{(2)}_{i}$ é elemento um da álgebra. De facto,

$$a^{-1}_{i,i}u_i \cdot \alpha u_\rho = a^{-1}_{i,i}\alpha a_{i,\rho}u_\rho = \alpha u_\rho \; ,$$

como se vê tendo em conta (2) e (4). Do mesmo modo,

$$\alpha u_\rho \cdot a^{-1}_{i,i}u_i = \alpha\,(a^{\rho}_{i,i})^{-1}a_{\rho,i}u_\rho = \alpha u_\rho \; .$$

Nestas condições, podemos supor $\mathcal{K}U$ identificado com $\mathcal{K}$. De resto, mesmo em face das notações utilizadas, tem-se

$$\alpha \cdot \beta u_\sigma = \alpha\beta u_\sigma \; , \qquad \alpha U \cdot \beta u_\sigma = \alpha\beta u_\sigma \; .$$

Passa agora a ter significado uma expressão $\alpha u_\rho \cdot \beta$. É

$$\alpha u_\rho \cdot \beta = \alpha u_\rho \cdot \beta a^{-1}_{i,i}u_i = \alpha\,\beta^{\rho}(a^{\rho}_{i,i})^{-1}a_{\rho,i}u_\rho = \alpha\,\beta^{\rho}u_\rho \; .$$

---

(1) Utilizaremos, de futuro, a designação de álgebra central simples, já referida no Cap. anterior, pelo facto de começarmos a ver que o mesmo fazem outros autores.

(2) Um símbolo α^{-1} significa inverso de α .

Como caso particular, vale

$$u_\rho\beta = \beta^{\rho}u_\rho \; . \qquad (5)$$

Não é indiferente, portanto, escrever os elementos $\mathcal{K}$ à esquerda ou à direita dos elementos u_ρ. Para os elementos de $\mathcal{P}$, porém, o facto de se ter, quando $\beta \in \mathcal{P}$, $\beta^{\rho} = \beta$, a relação (5) dá $u_\rho\beta = \beta u_\rho$. $\mathcal{A}$ é álgebra sobre $\mathcal{P}$, como se disse.

Posto isto, procuremos os elementos do centro de $\mathcal{A}$. Comecemos por procurar os elementos de $\mathcal{A}$ que comutam com todos os elementos de $\mathcal{K}$. Se $w = \sum \alpha_\sigma u_\sigma$ é um tal elemento, tem-se

$$w\beta = \beta w, \qquad \sum_{\sigma} \alpha_\sigma \beta^{\sigma} u_\sigma = \sum \beta\alpha_\sigma u_\sigma \; ,$$

qualquer que seja $\beta \in \mathcal{K}$. Por consequência, valerá $\beta^{\sigma} = \beta$, para qualquer β, o que exige $\sigma = 1$. O elemento w será da forma $\alpha u_1 = \tau U = \tau \in \mathcal{K}$. Nestas condições, se z pertence ao centro de $\mathcal{A}$, deverá pertencer a $\mathcal{K}$. Das relações

$$z\,u_\sigma = u_\sigma z = z^{\sigma}u_\sigma \; ,$$

conclui-se $z^{\sigma} = z$, qualquer que seja σ, o que mostra ser $z \in \mathcal{P}$. O centro de $\mathcal{A}$ é o corpo $\mathcal{P}$.

Provemos, em seguida, que $\mathcal{A}$ é simples. Seja $\mathfrak{a}$ um ideal bilateral $\neq (0)$ e $a = \alpha_\rho u_\rho + \alpha_\sigma u_\sigma + \cdots + \alpha_\tau u_\tau$ um elemento não nulo pertencente a $\mathfrak{a}$. Também pertence a $\mathfrak{a}$ o elemento

$$b = (\beta^{\rho})^{-1}a\beta = (\beta^{\rho})^{-1}\beta^{\rho}\alpha_\rho u_\rho + (\beta^{\rho})^{-1}\beta^{\sigma}\alpha_\sigma u_\sigma + \cdots =$$

$$= \alpha_\rho u_\rho + (\beta^{\rho})^{-1}\beta^{\sigma}\alpha_\sigma u_\sigma + \cdots \; .$$

O elemento $b - a$ pertence a $\mathfrak{a}$, sendo, aliás,

$$b - a = \tau_\sigma u_\sigma + \cdots + \tau_\tau u_\tau \; .$$

Nesta diferença figura uma parcela menos do que em a, pois supomos $\alpha_\rho \neq 0$. Se, em a, há mais do que uma parcela, se é, por ex., $\alpha_\sigma \neq 0$, imaginaremos β escolhido por tal forma que $\beta^{\sigma} \neq \beta^{\rho}$. Então, será $\tau_\sigma \neq 0$. O raciocínio pode prosseguir-se, de modo a estabelecer que o ideal $\mathfrak{a}$ contém um elemento da forma $c = \alpha u_\tau$,

em que há, apenas, uma parcela. Um tal elemento tem inverso, como vamos ver. É

$$\alpha u_\tau . u_{\tau-1} \xi = \alpha u_\tau . \xi^{\tau-1} u_{\tau-1} = \alpha \xi a_{\tau,\tau-1} u_1 .$$

Para que se tenha, no último membro, o elemento U, basta por

$$\xi = \alpha^{-1} a_{\tau,\tau-1}^{-1} a_{1,1}^{-1} .$$

O elemento αu_τ tem, pois, um inverso direito da forma $\beta u_{\tau-1}$. Este último terá, por consequência, um inverso esquerdo e um inverso direito, precisamente αu_τ. O ideal $\mathfrak{a}$ conterá $U \in \mathcal{U}$, pelo que será $\mathfrak{a} = \mathcal{U}$, como se queria mostrar.

Finalmente, observemos que $\mathcal{K}$ é uma sub-álgebra de $\mathcal{U}$, com o mesmo elemento um que esta última. Como o comutador de $\mathcal{K}$, em $\mathcal{U}$, é $\overline{\mathcal{K}} = \mathcal{K}$, segue-se que $\mathcal{K}$ está mergulhado em $\mathcal{U}$ de modo irredutível (Cap.IX, § 4, 4ª aplicação, teoremas 2 e 3) e que $\mathcal{K}$ é sub-corpo máximo de $\mathcal{U}$ contendo $\mathcal{K}$. Este último é corpo de decomposição de $\mathcal{U}$ (Cap.XI, § 2, teorema 3). O teorema enunciado está completamente demonstrado.

Construida a álgebra $\mathcal{U}$, observemos que as relações (5) dão

$$u_\rho \beta u_\rho^{-1} = \beta^\rho . \qquad (6)$$

Cada elemento u_ρ define, portanto, um automorfismo interno da álgebra $\mathcal{U}$, o qual prolonga o automorfismo $\rho \in \mathcal{G}$ da sub-álgebra $\mathcal{K}$. O elemento u_ρ, de (6), não é, porém, único. Seja $v_\rho \in \mathcal{U}$ um novo elemento tal que $v_\rho \beta v_\rho^{-1} = \beta^\rho$. Das relações

$$u_\rho \beta = \beta^\rho u_\rho , \qquad v_\rho \beta = \beta^\rho v_\rho ,$$

deduzimos

$$v_\rho u_\rho^{-1} \beta^\rho u_\rho = \beta^\rho v_\rho , \qquad \text{ou} \qquad v_\rho u_\rho^{-1} . \beta^\rho = \beta^\rho . v_\rho u_\rho^{-1} .$$

Como $\beta \in \mathcal{K}$ é qualquer, $\beta^\rho \in \mathcal{K}$ é qualquer. O elemento $v_\rho u_\rho^{-1} \in \mathcal{U}$ pertence ao comutador de $\mathcal{K}$, de sorte que se tem $v_\rho u_\rho^{-1} = \alpha \in \mathcal{K}$, ou seja $v_\rho = \alpha u_\rho$. Vê-se, inversamente, que qualquer elemento desta forma define o mesmo automorfismo que u_ρ. Escrevendo

$$\mathcal{K} u_\rho + \ldots + \mathcal{K} u_\tau = \mathcal{K} v_\rho + \ldots + \mathcal{K} v_\tau ,$$

o sistema de factores $b_{\rho,\sigma}$, correspondente aos v_ρ, é diferente do sistema $a_{\rho,\sigma}$. Efectivamente, tem-se, pondo $v_\sigma = \beta_\sigma u_\sigma$,

$$v_\rho v_\sigma = \beta_\rho u_\rho . \beta_\sigma u_\sigma = \beta_\rho \beta_\sigma^\rho a_{\rho,\sigma} u_{\rho\sigma} = \frac{\beta_\rho \beta_\sigma^\rho}{\beta_{\rho\sigma}} a_{\rho,\sigma} v_{\rho\sigma} ,$$

pelo que é

$$b_{\rho,\sigma} = \frac{\beta_\rho \beta_\sigma^\rho}{\beta_{\rho\sigma}} a_{\rho,\sigma} . \qquad (7)$$

Os elementos $b_{\rho,\sigma}$ verificam necessàriamente as relações (3). Dois sistemas de factores, $a_{\rho,\sigma}$ e $b_{\rho,\sigma}$, relacionados como se indica em (7), dizem-se <u>associados</u>. É válido o seguinte

<u>Teorema 2</u>:- <u>Se $(\mathcal{K}/\mathcal{P}, a_{\rho,\sigma})$ é um produto cruzado, os elementos $b_{\rho,\sigma}$, dados por (7), são tais que $(\mathcal{K}/\mathcal{P}, a_{\rho,\sigma}) \cong (\mathcal{K}/\mathcal{P}, b_{\rho,\sigma})$</u>. Nós podemos, com efeito, encontrar no produto cruzado correspondente aos $a_{\rho,\sigma}$ elementos v_ρ tais que $(\mathcal{K}/\mathcal{P}, a_{\rho,\sigma}) = (\mathcal{K}/\mathcal{P}, b_{\rho,\sigma})$, como acabámos de ver. Então, construindo o produto cruzado $(\mathcal{K}/\mathcal{P}, b_{\rho,\sigma})$, dado inicialmente à custa de elementos w_ρ, podemos estabelecer uma equivalência entre os dois produtos cruzados, pondo

$$v_\rho \longleftrightarrow w_\rho , \qquad \mathcal{K} \longleftrightarrow \mathcal{K} ,$$

subentendendo que os elementos de $\mathcal{K}$ se conservam.

O teorema 2 admite este recíproco:

<u>Teorema 3</u>:- <u>A equivalência $(\mathcal{K}/\mathcal{P}, a_{\rho,\sigma}) \cong (\mathcal{K}/\mathcal{P}, b_{\rho,\sigma})$, de dois produtos cruzados, arrasta a existência de elementos $\beta_\rho \in \mathcal{K}$, em correspondência com os automorfismos ρ, de tal modo que as relações (7) são válidas.</u>

Procuremos, no 2º produto cruzado, os elementos u_{ρ_1}, que correspondem, no isomorfismo, aos elementos u_ρ do primeiro. O mesmo isomorfismo leva do corpo $\mathcal{K}$ a um corpo $\mathcal{K}_1$ (apenas com conservação dos elementos de $\mathcal{P}$). Tem-se, respectivamente, nos dois produtos cruzados:

$$u_\rho u_\sigma = a_{\rho,\sigma} u_{\rho\sigma} , \qquad u_{\rho_1} u_{\sigma_1} = a_{\rho_1,\sigma_1} u_{\rho_1\sigma_1} ,$$

onde $a_{\rho_1,\sigma_1} \in \mathfrak{K}_1$ é o correspondente de $a_{\rho,\sigma}$, por via do isomorfismo. É claro que $\rho_1, \sigma_1, \ldots$ representam aqui os automorfismos de $\mathfrak{K}_1$ relativamente a $\mathcal{P}$, definidos do modo seguinte: o isomorfismo $\mathfrak{K} \cong \mathfrak{K}_1$ determina as correspondências

$$\alpha \longrightarrow \alpha_1 , \qquad x^\rho \longrightarrow X_1 \in \mathfrak{K}_1 ;$$

então, por-se-á $X_1 = x_1^{\rho_1}$. É assim que se terá

$$u_\rho \alpha = \alpha^\rho u_\rho , \qquad u_{\rho_1} \alpha_1 = \alpha_1^{\rho_1} u_{\rho_1} . \qquad (8)$$

Também é evidente a igualdade

$$(\mathfrak{K}/\mathcal{P},\ b_{\rho,\sigma}) = (\mathfrak{K}_1/\mathcal{P},\ a_{\rho_1,\sigma_1}) .$$

Dentro deste produto, as duas sub-álgebras $\mathfrak{K}$ e $\mathfrak{K}_1$ são equivalentes e têm o mesmo elemento um que o produto. Tal equivalência pode ser estendida a todo o produto cruzado (Cap. IX, § 4, 4ª apl., teor. 1). Virá, nessas condições:

$$u_{\rho_1} \longrightarrow w_\rho , \qquad a_{\rho_1,\sigma_1} \longrightarrow a_{\rho,\sigma} , \qquad w_\rho w_\sigma = a_{\rho,\sigma} w_{\rho\sigma} ,$$

$$(\mathfrak{K}/\mathcal{P},\ b_{\rho,\sigma} ;\ v_\rho, v_\sigma, \ldots) = (\mathfrak{K}/\mathcal{P}, a_{\rho,\sigma} ;\ w_\rho,\ w_\sigma, \ldots),$$

admitindo que $v_\rho, v_\sigma, \ldots$ são os símbolos iniciais utilizados na definição de $(\mathfrak{K}/\mathcal{P},\ b_{\rho,\sigma})$. Ora, dado $\alpha \in \mathfrak{K}$, tem-se:

$$v_\rho \alpha = \alpha^\rho v_\rho , \qquad w_\rho \alpha = \alpha^\rho w_\rho ,$$

como se conclui tendo em vista a segunda relação (8). Os elementos v_ρ serão necessàriamente da forma $v_\rho = \beta_\rho w_\rho$, o que demonstra o teorema.

2) Aplicação às álgebras centrais simples - Percebe-se imediatamente a importância da noção de produto cruzado em face dos teoremas que a seguir provaremos.

Seja $\mathcal{A} = A_q$ uma álgebra central simples sobre $\mathcal{P}$. Na álgebra de divisão A existe uma ampliação separável máxima $\Phi =$

$= \mathcal{P}(\mu)$, de $\mathcal{P}$, que é corpo de decomposição de $\mathcal{A}$. Se $\varphi(x) = 0$ for a equação irredutível em $\mathcal{P}$ a que satisfaz μ, o corpo de decomposição $\mathfrak{K} = \mathcal{P}(\Theta)$, do polinómio $\varphi(x)$, é uma ampliação normal separável de $\mathcal{P}$, e também um corpo de decomposição de $\mathcal{A}$. Consideremos a representação irredutível única, de grau r, de $\mathfrak{K}$, em A. Obter-se-á um corpo $\mathfrak{K}^* \cong A_r = \mathcal{B}$. A álgebra $\mathcal{B}$ é semelhante à álgebra $\mathcal{A}$. Como $\mathfrak{K}^*$ é isomorfo de $\mathfrak{K}$, existe uma álgebra $\mathcal{L}$, isomorfa de $\mathcal{B}$, obtida substituindo $\mathfrak{K}^*$ por $\mathfrak{K}$. Será $\mathcal{L} = C_r$, com $C \cong A$. Portanto:

Teorema 1:- Uma álgebra central simples $\mathcal{A}$, sobre $\mathcal{P}$, é sempre semelhante a uma álgebra central simples $\mathcal{L}$, sobre $\mathcal{P}$, que contém um corpo de decomposição $\mathfrak{K}$, de $\mathcal{A}$, o qual é ampliação normal, separável e finita de $\mathcal{P}$.

Sabemos, mesmo, que $\mathfrak{K}$ é sub-corpo máximo de $\mathcal{L}$, contendo $\mathcal{P}$, e que o comutador de $\mathfrak{K}$, em $\mathcal{L}$, é igual a $\mathfrak{K}$. Assim

$$(\mathfrak{K}/\mathcal{P})^2 = n^2 = (\mathcal{L}/\mathcal{P}) .$$

Consideremos o grupo $\mathcal{G} = \{\rho, \sigma, \ldots, \tau\}$ dos automorfismos de $\mathfrak{K}$, relativamente a $\mathcal{P}$. Como tais automorfismos podem ser estendidos a automorfismos de $\mathcal{L}$, designemos por $u_\rho, u_\sigma, \ldots, u_\tau$ elementos de $\mathcal{L}$ definindo os últimos automorfismos. Tem lugar este

Teorema 2:- Os elementos $u_\rho, u_\sigma, \ldots, u_\tau$ são independentes, em face de $\mathfrak{K}$. Com efeito, suponhamos que era possível uma relação

$$\alpha_\rho u_\rho + \alpha_\sigma u_\sigma + \cdots + \alpha_\tau u_\tau = 0, \qquad (\alpha_\rho, \ldots \in \mathfrak{K}), \qquad (9)$$

sem que fossem nulos todos os $\alpha\alpha$. Visto que é, por hipótese, para cada $\alpha \in \mathfrak{K}$,

$$u_\rho \alpha u_\rho^{-1} = \alpha^\rho , \quad \text{ou} \quad u_\rho \alpha = \alpha^\rho u_\rho ,$$

poderíamos tirar, de (9), supondo $\tau \in \mathfrak{K}$,

$$(\tau^\rho)^{-1} \alpha_\rho u_\rho \tau + (\tau^\rho)^{-1} \alpha_\sigma u_\sigma \tau + \cdots = 0 ,$$

$$\alpha_\sigma\left[u - \frac{\tau^\sigma}{\tau^\rho}\right]u_\sigma + \cdots + \alpha_\tau\left[u - \frac{\tau^\tau}{\tau^\rho}\right]u_\tau = 0 \ ,$$

que escreveremos

$$\beta_\sigma u_\sigma + \cdots + \beta_\tau u_\tau = 0.$$

Seria possível, portanto, chegar a estabelecer uma relação do tipo $\tau_\tau u_\tau = 0$, com $\tau_\tau \neq 0$, que é absurda, pelo facto de u_τ ter inverso.

A álgebra $\mathcal{L}$, considerada como módulo esquerdo relativamente a $\mathcal{A}$, é de ordem n, e os elementos u_ρ constituem uma base para o módulo. Dentro da álgebra $\mathcal{L}$, tem-se $u_\rho u_\tau \alpha = u_\rho \alpha^\tau u_\tau = \alpha^{\rho\tau} u_\rho u_\tau$; $u_\rho u_\tau \alpha = \alpha^{\rho\tau} u_{\rho\tau}$. Daqui se tira $(u_\rho u_\tau . u_{\rho\tau}^{-1})\alpha^{\rho\tau} = \alpha^{\rho\tau}(u_\rho u_\tau . u_{\rho\tau}^{-1})$. O elemento $u_\rho u_\tau . u_{\rho\tau}^{-1}$ comuta com todos os elementos de $\mathcal{A}$, pelo que pertence a $\mathcal{A}$. Pode escrever-se

$$u_\rho u_\tau . u_{\rho\tau}^{-1} = a_{\rho,\tau} \ , \quad \text{ou} \quad u_\rho u_\tau = a_{\rho,\tau} u_{\rho\tau}.$$

As relações (3) são aqui necessàriamente verificadas, e, por isso, pode enunciar-se este

Teorema 3:- Toda a álgebra central simples $\mathcal{U}$, sobre $\mathcal{P}$, é semelhante a um produto cruzado $(\mathcal{A}/\mathcal{P}, a_{\rho,\sigma}) = \mathcal{L}$.

Outro teorema importante é o seguinte:

Teorema 4:- É condição necessária e suficiente, para que $(\mathcal{A}/\mathcal{P}, a_{\rho,\sigma})$ seja isomorfo dum anel completo de matrizes com elementos de $\mathcal{P}$, que existam elementos $\beta_\rho \in \mathcal{A}$ tais que $a_{\rho,\sigma} = \beta_\rho \beta_\sigma^\rho (\beta_{\rho\sigma})^{-1}$. Se os elementos β_ρ existem, ponhamos $\beta_\rho^{-1} = \tau_\rho$. Então, tem-se $u = \tau_\rho \tau_\sigma^\rho (\tau_{\rho\sigma})^{-1} . a_{\rho,\sigma}$, visto que $(\beta_\sigma^\rho)^{-1} = (\beta_\sigma^{-1})^\rho = \tau_\sigma^\rho$. Vê-se que o sistema $b_{\rho,\sigma}$ definido pelas relações $b_{\rho,\sigma} = u$ (quaisquer que sejam ρ e σ), é um sistema associado dos $a_{\rho,\sigma}$. Trata-se de ver agora que, sempre que todos os elementos $b_{\rho,\sigma}$ dum sistema de factores são iguais a u, o produto cruzado é isomorfo duma álgebra $\mathcal{P}_n$. As considerações a fazer são um tanto indirectas.

Suponhamos $\mathcal{A} = K_1\mathcal{P} + \cdots + K_n\mathcal{P}$, $(K_i \in \mathcal{A})$. Conforme se viu no Cap. VIII, §§ 6 e 9, é

$$\mathcal{U}_\mathcal{P}' \cong \mathcal{P}_n, \quad \mathcal{L}_1' \cong \mathcal{U}_\mathcal{B}, \quad \mathcal{L}_1' = \mathcal{U}_\mathcal{A}' = \mathcal{U}_\mathcal{L}' \ .$$

Ora $\mathcal{U}_\mathcal{A}' \subseteq \mathcal{U}_\mathcal{P}'$, de modo que $\mathcal{U}_\mathcal{P}'$ contém $\mathcal{L}_1'$. Em $\mathcal{U}_\mathcal{P}'$ existem também os automorfismos $\rho, \sigma, \ldots, \tau$, e, por isso, pode definir-se em $\mathcal{U}_\mathcal{P}'$ o sub-anel gerado por $\mathcal{L}_1'$ e pelos elementos $\rho, \sigma, \ldots, \tau$. Nesse sub-anel existe o módulo

$$\mathcal{L}_1'\rho + \mathcal{L}_1'\sigma + \cdots + \mathcal{L}_1'\tau \subseteq \mathcal{U}_\mathcal{P}' \ . \tag{10}$$

A demonstração da suficiência da condição expressa no teorema ultima-se do modo seguinte. Prova-se que, em (10), é válido o sinal = . Depois, verifica-se que $\mathcal{L}_1'\rho + \cdots + \mathcal{L}_1'\tau$ é um produto cruzado $(\mathcal{L}_1'/\mathcal{P}_1', u')$, para o qual o sistema de factores é composto de elementos todos iguais ao elemento um, $u' \in \mathcal{L}_1'$. Então, virá $(\mathcal{L}_1'/\mathcal{P}_1', u') \cong \mathcal{P}_n$. Por fim, mostra-se que um produto cruzado $(\mathcal{A}/\mathcal{P}, u)$ é sempre isomorfo dum produto $(\mathcal{L}_1'/\mathcal{P}_1', u')$, com $\mathcal{L}_1' \cong \mathcal{A}$, $\mathcal{P}_1' \cong \mathcal{P}$.

Representemos por $\lambda', \mu', \ldots, \nu'$ elementos de $\mathcal{L}_1'$. Não é possível uma relação

$$\lambda'\rho + \mu'\sigma + \cdots + \nu'\tau = 0, \tag{10'}$$

sem que se tenha $\lambda' = \mu' = \cdots = \nu' = 0$. Na verdade

$$\lambda'\rho . \alpha = \lambda' . \rho\alpha = \lambda' . \alpha^\rho \ ,$$

$$\lambda'\rho . \alpha\beta = \lambda' . \alpha^\rho \beta^\rho = \alpha^\rho . \lambda' \beta^\rho \ , \qquad (\alpha, \beta \in \mathcal{A}),$$

pois que os endomorfismos $\lambda', \ldots, \nu'$ são operatórios relativamente a $\mathcal{A}$. Se $\tau \in \mathcal{A}$, e se a relação (10') é válida, tem-se

$$\begin{aligned} (\lambda'\rho + \mu'\sigma + \cdots + \nu'\tau)\alpha &= 0 \ , \\ (\lambda'\rho + \mu'\sigma + \cdots + \nu'\tau)\tau\alpha &= 0 \ . \end{aligned} \tag{11}$$

Esta última relação pode escrever-se

$$\tau^\rho(\lambda'\rho . \alpha) + \tau^\sigma(\mu'\sigma . \alpha) + \cdots + \tau^\tau(\nu'\tau . \alpha) = 0 \ .$$

Multiplicando esta igualdade por $(\tau^\rho)^{-1}$ e tendo em conta a pri-

meira das relações (11), conclui-se

$$(u - \tfrac{\tau^\sigma}{\tau^\rho})\ (\mu'\sigma\,.\,\alpha) + \ldots + (u - \tfrac{\tau^\tau}{\tau^\rho})\ (\nu^\tau\,\tau\,.\,\alpha) = 0,$$

que pode ainda escrever-se

$$\mu'\left[(u - \tfrac{\tau^\sigma}{\tau^\rho})\,.\,\sigma\alpha\right] + \ldots + \nu'\left[(u - \tfrac{\tau^\tau}{\tau^\rho})\,.\,\tau\alpha\right] = 0\ .$$

Admitindo ser $\mu' \neq 0$, escolhamos τ de tal modo que se tenha $\tau^\sigma \neq \tau^\rho$, e, tendo em conta que $u - \tau^\sigma/\tau^\rho$ xultiplica $\sigma\alpha$ à esquerda, ponhamos

$$u - \frac{\tau^\sigma}{\tau^\rho} = \mu'' \in \mathcal{L}_1'\ .$$

Obtém-se, em vez de (10'), uma relação com o aspecto

$$\mu'\,\mu''\sigma + \ldots + \nu'\,\nu''\tau = 0, \qquad (\mu'\,\mu'' \neq 0).$$

Continuando o processo, chega-se a uma igualdade

$$\nu^{(\varkappa)}\,.\,\tau\alpha = 0, \quad \text{que dá} \quad \nu^{(\varkappa)}\tau = 0,$$

com $\nu^{(\varkappa)} \neq 0$. Um tal resultado é absurdo, pois τ tem inverso em $\mathcal{U}_\mathcal{P}'$.

Fica assim estabelecido que o primeiro membro de (10) é de ordem n relativamente a $\mathcal{L}_1'$, e, portanto, de ordem n^2 relativamente ao corpo $\mathcal{P}_1' \cong \mathcal{P}$, que corresponde a $\mathcal{P}$ no isomorfismo $\mathcal{A} \cong \mathcal{L}_1'$. Ora, na correspondência $\mathcal{P}_n \cong \mathcal{U}_\mathcal{P}'$, às matrizes diagonais de elementos iguais pertencentes a $\mathcal{P}$, vão corresponder precisamente os elementos do corpo $\mathcal{P}_1'$, de sorte que a ordem de $\mathcal{U}_\mathcal{P}'$ relativamente a $\mathcal{P}_1'$ é também n^2. Assim, pode escrever-se

$$\mathcal{U}_\mathcal{P}' = \mathcal{L}_1'\,\rho + \ldots + \mathcal{L}_1'\,\tau\ .$$

Além disso, tem-se

$$\rho\,.\,\sigma = u'\,.\,\rho\sigma = \rho\sigma\ ; \qquad \rho\,.\,\lambda' = \lambda'^\rho\rho\ ,$$

onde $u' \in \mathcal{L}_1'$ é o seu elemento um. Para se interpretar a última igualdade, raciocina-se como segue. Supondo $\alpha \in \mathcal{A}$ e admitindo que λ' é definido por multiplicação à esquerda pelo elemento $\varkappa \in \mathcal{A}$, é

$$\rho\lambda'\,.\,\alpha = \rho\,.\,(\lambda'\,\alpha) = \rho\,.\varkappa\,\alpha = \varkappa^\rho\ \alpha^\rho = \varkappa^\rho\,.\,\rho\alpha.$$

Os automorfismos de $\mathcal{L}_1'$ relativamente a $\mathcal{P}_1'$ podem representar-se pelas mesmas letras que os automorfismos correspondentes de $\mathcal{A}$ relativamente a $\mathcal{P}$. Nesse caso, se $\varkappa \longrightarrow \lambda'$, tem-se $\varkappa^\rho \longrightarrow \lambda'^\rho$, e, portanto,

$$\rho\lambda'\,.\,\alpha = \varkappa^\rho\,.\,\rho\alpha = \lambda'^\rho\,.\,\rho\alpha = \lambda'^\rho\rho\,.\,\alpha\ .$$

É agora evidente que

$$\mathcal{P}_n \cong \mathcal{U}_\mathcal{P}' = \mathcal{L}_1'\,\rho + \ldots + \mathcal{L}_1'\,\tau = (\mathcal{L}_1'/\mathcal{P}_1',\ u') \cong (\mathcal{A}/\mathcal{P},\ u)\ .$$

Inversamente, vê-se que $(\mathcal{A}/\mathcal{P},\ u)$ é isomorfo dum anel de matrizes com elementos de $\mathcal{P}$.

Finalmente, a condição expressa no teorema é necessária, porque, se $(\mathcal{A}/\mathcal{P},\ a_{\rho,\sigma})$ é isomorfo dum anel de matrizes com elementos de $\mathcal{P}$, é isomorfo dum produto cruzado $(\mathcal{A}/\mathcal{P},\ u)$ [No § 9 daremos outra demonstração deste teorema 4].

3) <u>O teorema da multiplicação</u>[1] Dados $\mathcal{P}$ e $\mathcal{A}$, como nos dois §§ anteriores, consideremos o conjunto dos diferentes sistemas de factores possíveis. Define-se uma relação de equivalência nesse conjunto, tomando como classes de equivalentes as que são constituidas por sistemas de factores associados. De facto, neste sentido, tem-se:

I) o sistema $a_{\rho,\sigma}$ é associado de si mesmo;

II) de $b_{\rho,\sigma} = \beta_\rho\,\beta_\sigma^\rho\,a_{\rho,\sigma}/\beta_{\rho\sigma}$, tira-se $a_{\rho,\sigma} = \tau_\rho\,\tau_\sigma^\rho\,b_{\rho,\sigma}/\tau_{\rho\sigma}$, desde que se ponha $\beta_\rho^{-1} = \tau_\rho$;

III) de $b_{\rho,\sigma} = \beta_\rho\,\beta_\sigma^\rho a_{\rho,\sigma}/\beta_{\rho\sigma}$ e $c_{\rho,\sigma} = \tau_\rho\,\tau_\sigma^\rho\,b_{\rho,\sigma}/\tau_{\rho\sigma}$, tira-se

$$c_{\rho,\sigma} = \frac{(\tau_\rho\beta_\rho)\ (\tau_\sigma^\rho\beta_\sigma^\rho)}{\tau_{\rho\sigma}\,\beta_{\rho\sigma}}\,.\,a_{\rho,\sigma} = \frac{\delta_\rho\,\delta_\sigma^\rho}{\delta_{\rho\sigma}}\,.\,a_{\rho,\sigma}\ ,$$

(1) Cfr. Deuring, "Algebren", pgs. 56 a 58.

desde que se ponha $\gamma_\rho\,\beta_\rho = \delta_\rho$, e, portanto, $(\gamma_\rho\,\beta_\rho)^\sigma = \delta_\rho^\sigma = \gamma_\rho^\sigma\,\beta_\rho^\sigma$.

As classes de equivalente acabadas de construir podem algebrizar-se, definindo um produto consoante a regra $c_{\rho,\sigma} = a_{\rho,\sigma}\,b_{\rho,\sigma}$. Vê-se imediatamente, com efeito, que os $c_{\rho,\sigma}$ constituem um sistema de factores, pois verificam as relações (3). Forma-se, deste modo, um grupo multiplicativo, no qual o elemento um é definido pondo $a_{\rho,\sigma} = u$, para quaisquer ρ e σ. A classe inversa da que é representada por $b_{\rho,\sigma}$ é $b_{\rho,\sigma}^{-1}$.

O teorema da multiplicação que temos em vista neste § pode enunciar-se como segue:

Teorema:- Existe um isomorfismo entre o grupo das classes de álgebras centrais simples semelhantes (sobre $\mathcal{P}$), que admitem $\mathcal{K}$ como corpo de decomposição, e o grupo das classes de equivalentes constituidas pelos sistemas de factores associados.

A correspondência biunívoca entre os elementos dos dois grupos é fácil de provar. Seja $\mathcal{K}$ normal, separável, finito, sobre $\mathcal{P}$. O produto cruzado $(\mathcal{K}/\mathcal{P}, a_{\rho,\sigma}) = C_r$ define uma classe de álgebras centrais simples sobre $\mathcal{P}$. Se o sistema de factores $b_{\rho,\sigma}$ não for associado de $a_{\rho,\sigma}$, o produto cruzado $(\mathcal{K}/\mathcal{P}, b_{\rho,\sigma}) = D_r$, não pode pertencer à classe (C). Com efeito, se fosse $D \cong C$, seria $r' = r$, e as duas álgebras centrais C_r e D_r seriam equivalentes. Então, os $b_{\rho,\sigma}$ seriam associados dos $a_{\rho,\sigma}$, contra a hipótese. Inversamente, seja (C) uma classe de álgebras centrais sobre $\mathcal{P}$ que admite $\mathcal{K}$ como corpo de decomposição. A representação irredutível única, de grau r, de $\mathcal{K}$, em C, é $\mathcal{K}^* \subseteq C_r$. Os automorfismos de $\mathcal{K}^*$ relativamente a $\mathcal{P}$ podem ser estendidos a automorfismos de C_r. C_r é um produto cruzado da forma $(\mathcal{K}^*/\mathcal{P}, a^*_{\rho,\sigma})$. Substituindo $\mathcal{K}^*$ por $\mathcal{K}$ obtém-se um produto cruzado $(\mathcal{K}/\mathcal{P}, a_{\rho,\sigma})$. O processo de passagem de (C) a este último produto cruzado leva a uma classe de sistemas de factores bem determinada. A correspondência biunívoca em causa está provada.

A demonstração completa do teorema reduz-se agora a provar o seguinte: supondo $c_{\rho,\sigma} = a_{\rho,\sigma}\,b_{\rho,\sigma}$, o produto cruzado $(\mathcal{K}/\mathcal{P}, c_{\rho,\sigma})$ pertence à mesma classe de álgebras centrais sobre $\mathcal{P}$ que o produto directo $(\mathcal{K}/\mathcal{P}, a_{\rho,\sigma}) \times (\mathcal{K}/\mathcal{P}, b_{\rho,\sigma})$.

Representemos por $\mathcal{K}'$ e $\mathcal{K}''$ os dois corpos isomorfos de $\mathcal{K}$, respectivamente contidos em $\mathcal{A} = (\mathcal{K}/\mathcal{P}, a_{\rho,\sigma})$ e $\mathcal{B} = (\mathcal{K}/\mathcal{P}, b_{\rho,\sigma})$. Há aqui conveniência em não os identificar com $\mathcal{K}$.

No produto directo $\mathcal{A} \times \mathcal{B} = \mathcal{L}$ figura o produto directo $\mathcal{K}' \times \mathcal{K}''$. As considerações a fazer podem resumir-se deste modo:(1) encontra-se em $\mathcal{K}' \times \mathcal{K}''$ um idempotente e e constroi-se a álgebra central simples sobre $\mathcal{P}$, e $\mathcal{L}$; mostra-se, depois, que $e\mathcal{L}e$ é isomorfa do produto cruzado $(\mathcal{K}/\mathcal{P}, c_{\rho,\sigma})$; finalmente, prova-se que $\mathcal{L}$ e $e\mathcal{L}e$ são álgebras centrais simples sobre $\mathcal{P}$ pertencentes à mesma classe.

A última parte é imediata. Com efeito, se $\mathcal{L}$ é simples, e $\mathcal{L}e$ é igualmente simples (pgs.17). Supondo e' um idempotente primitivo em $e\mathcal{L}e$ (portanto em $\mathcal{L}$), os dois anéis $e'.e\mathcal{L}e.e'$, $e'\mathcal{L}e'$ são corpos (pgs.18 e 55). Mas, como e é o elemento um de $e\mathcal{L}e$, tem-se $e'.e\mathcal{L}e.e' = e'\mathcal{L}e'$. Assim, $\mathcal{L}$ é um anel completo de matrizes com elementos dum corpo isomorfo de $e'\mathcal{L}e'$, o mesmo se dizendo de $e\mathcal{L}e$. As duas álgebras $\mathcal{L}$ e $e\mathcal{L}e$ são semelhantes.(2)

Passemos à construção de e. Supondo $\mathcal{K} = \mathcal{P}(\alpha)$, suporemos também $\mathcal{K}' = \mathcal{P}(\alpha')$, $\mathcal{K}'' = \mathcal{P}(\alpha'')$.(3) Por meio das correspondências

$$\mathcal{P} \longleftrightarrow \mathcal{P}\,, \quad \alpha' \longleftrightarrow \alpha''\,, \qquad (\mathcal{P} \text{ invariante})\,,$$

define-se o isomorfismo $\mathcal{K}' \cong \mathcal{K}''$, que se obteria por intermédio de $\mathcal{K}$. Admitiremos que é $\alpha'^\sigma \longleftrightarrow \alpha''^\sigma$, isto é, admitiremos que, no isomorfismo $\mathcal{K}' \cong \mathcal{K}''$, se α' e α'' estão em correspondência, também o estão os elementos α'^σ e α''^σ, os quais são correspondentes de α^σ nos isomorfismos $\mathcal{K} \cong \mathcal{K}'$, $\mathcal{K} \cong \mathcal{K}''$. Neste sentido, o grupo $\mathcal{G} = \{\rho, \sigma, \ldots \tau\}$, dos automorfismos de $\mathcal{K}$ relativamente a $\mathcal{P}$, é também o grupo dos automorfismos de $\mathcal{K}'$ (ou de $\mathcal{K}''$) relativamente a $\mathcal{P}$. Seja $\varphi(x) = 0$ a equação irredutível em $\mathcal{P}$ a que satisfaz α (e, portanto, α' e α''). O elemento $\underline{e}$ será

$$e = \Phi(\alpha', \alpha'') = \frac{\prod_{\rho \neq 1} (\alpha' - \alpha''^\rho)}{\varphi'(\alpha')}\,,$$

como vamos ver. Em primeiro lugar, no produto $\mathcal{K}' \times \mathcal{K}''$ (como, semelhantemente, no produto $\mathcal{A} \times \mathcal{P}$), um elemento formado à custa de

(1) São tiradas de Artin-Nesbitt-Thrall, loc.cit.

(2) Das considerações a fazer resultará que $e\mathcal{L}e$ tem o centro $\mathcal{P}$.

(3) $\mathcal{P}$ pertencerá, portanto, a $\mathcal{K}'$ e a $\mathcal{K}''$.

elementos independentes de $\mathcal{K}'$, com coeficientes pertencentes a $\mathcal{K}''$, só é nulo, se os coeficientes forem nulos. No numerador da expressão anterior de e, o coeficiente de α'^{n-1} é o elemento um de $\mathcal{K}''$, de sorte que $e \neq 0$. Todavia, é

$$e(\alpha' - \alpha'') = \frac{\Pi(\alpha' - \alpha''^{\rho})}{\varphi'(\alpha')} = 0, \qquad (\rho \text{ qualquer}),$$

pois que $\varphi(x) = \Pi(x - \alpha''^{\rho})$ é um polinómio com coeficientes de $\mathcal{P}$, que se anula pondo $x = \alpha'$. Concluem-se, assim, as igualdades

$$e\,\alpha' = e\,\alpha'', \quad e\,\alpha'^2 = e\,\alpha''\alpha' = e\,\alpha'\alpha'' = e\,\alpha''^2, \ldots, e\,\alpha'^n = e\,\alpha''^n;$$

e, consequentemente,

$$ek' = ek'', \qquad (k' \in \mathcal{K}', \quad k'' \in \mathcal{K}''), \qquad (12)$$

onde k' e k'' se correspondem no isomorfismo $\mathcal{K}' \cong \mathcal{K}''$, que acima se definiu. Pondo

$$e' = \Phi(\alpha'^{\sigma}, \alpha''^{\sigma}) = \frac{\Pi(\alpha'^{\sigma} - \alpha''^{\rho\sigma})}{\varphi'(\alpha'^{\sigma})},$$

fàcilmente se vê que se tem $ee' = e = e'$, e, portanto, $e^2 = ee' = e$. De facto, é

$$ee' = e\,\Phi(\alpha'^{\sigma}, \alpha''^{\sigma}) = e\,\Phi(\alpha'^{\sigma}, \alpha'^{\sigma});$$

e, como

$$\varphi'(x) = \frac{\varphi(x)}{x - \alpha'^{\rho}} + \frac{\varphi(x)}{x - \alpha'^{\sigma}} + \cdots,$$

vem

$$\varphi'(\alpha'^{\sigma}) = \left(\frac{\varphi(x)}{x - \alpha'^{\sigma}}\right)_{x=\alpha'^{\sigma}} = \left(\prod_{\rho \neq 1}(x - \alpha'^{\rho\sigma})\right)_{x=\alpha'^{\sigma}} = \prod_{\rho \neq 1}(\alpha'^{\sigma} - \alpha'^{\rho\sigma}).$$

Portanto, tem-se

$$ee' = e\,\Phi(\alpha'^{\sigma}, \alpha'^{\sigma}) = e\,\frac{\varphi'(\alpha'^{\sigma})}{\varphi'(\alpha'^{\sigma})} = e, \qquad (\sigma \text{ qualquer}),$$

A igualdade $ee' = e'$ resulta deste outro modo. É

$$(\alpha'^{\sigma} - \alpha''^{\sigma})e' = \frac{\Pi(\alpha'^{\sigma} - \alpha''^{\rho\sigma})}{\varphi'(\alpha'^{\sigma})} = 0,$$

de sorte que $k'e' = k''e'$, como em (12). Assim, tem-se

$$ee' = \Phi(\alpha', \alpha'')e' = \Phi(\alpha', \alpha')e' = \frac{\varphi'(\alpha')}{\varphi'(\alpha')}e' = e'.$$

Posto isto, passemos ao estudo da álgebra $e\mathcal{L}e$. Se

$$\mathcal{A} = \mathcal{K}'u'_{\rho} + \cdots + \mathcal{K}'u'_{\tau}, \qquad \mathcal{B} = \mathcal{K}''u''_{\rho} + \cdots + \mathcal{K}''u''_{\tau},$$

$$\mathcal{L} = \mathcal{K}'\mathcal{K}''u'_{\rho}u''_{\rho} + \mathcal{K}'\mathcal{K}''u'_{\rho}u''_{\sigma} + \cdots,$$

vemos que o elemento geral de $e\mathcal{L}e$ tem a forma

$$\sum ek'e.ek''e.e\,u'_{\rho}u''_{\sigma}e, \qquad (13)$$

pois que e pertence ao produto comutativo $\mathcal{K}' \times \mathcal{K}''$. A relação (12) mostra agora que podemos escrever (13) com o aspecto

$$\sum ek'e.e\,u'_{\rho}u''_{\sigma}e. \qquad (14)$$

Deixemos, para dentro dum momento, a determinação das relações

$$e\,u'_{\rho}u''_{\sigma}e = 0, \quad \text{se } \rho \neq \sigma; \qquad e\,u'_{\rho}u''_{\rho}e = e\,u'_{\rho}u''_{\rho}. \qquad (14')$$

Por meio delas, o elemento geral (14) toma a expressão

$$\sum_{\sigma} ek'e.e\,u'_{\sigma}u''_{\sigma}e, \qquad (15)$$

que tem o aspecto do elemento geral dum produto cruzado ($e\mathcal{K}'e/e\mathcal{P}e$, $\alpha_{\rho,\sigma}$). Ponhamos, abreviadamente,

$$e\mathcal{K}'e = \mathcal{K}^*, \qquad e\mathcal{P}e = \mathcal{P}, \qquad e\,u'_{\sigma}u''_{\sigma}e = u^*_{\sigma},$$

sem inconveniente na substituição de e $\mathcal{P}$ e por $\mathcal{P}$. Importa verificar que os elementos u^*_σ são independentes em face de $\mathcal{K}^*$. A demonstração faz-se como para a questão análoga tratada no § 2. Por um lado, tem-se, se $\alpha^* \in \mathcal{K}^*$,

$$u^*_\sigma \alpha^* = e\, u'_\sigma\, u''_\sigma\, e.ek'e = e\, u'_\sigma\, u''_\sigma .k'e = e\, u'_\sigma\, k'.u''_\sigma\, e =$$

$$= ek'^\sigma u'_\sigma\, u''_\sigma\, e = ek'^\sigma e.e\, u'_\sigma\, u''_\sigma\, e = \alpha^{*\sigma} u^*_\sigma ,$$

visto que o automorfismo σ, de e$\mathcal{K}'$e, se definirá pondo $(ek'e)^\sigma = ek'^\sigma e$. Por outro lado, u^*_σ tem inverso, precisamente

$$e\, u'_{\sigma^{-1}}\, \xi' .\, u''_{\sigma^{-1}}\, \xi'' ,$$

onde $u'_{\sigma^{-1}}\, \xi'$, $u''_{\sigma^{-1}}\, \xi''$ são os inversos, em $\mathcal{U}$ e $\mathcal{L}$, respectivamente, de u'_σ e u''_σ. É claro que o produto de elementos (15) é necessàriamente associativo e distributivo. Procuremos os $\alpha_{\rho,\sigma}$. Tem-se, em virtude de (14'),

$$u^*_\rho u^*_\sigma = e\, u'_\rho\, u''_\rho\, u'_\sigma\, u''_\sigma\, e = e\, u'_\rho\, u'_\sigma\, u''_\rho\, u''_\sigma\, e = e\, a'_{\rho,\sigma} u'_{\rho\sigma} b''_{\rho,\sigma} u''_{\rho\sigma}\, e,$$

onde $a'_{\rho,\sigma} \in \mathcal{K}'$, $b''_{\rho,\sigma} \in \mathcal{K}''$ são os correspondentes de $a_{\rho,\sigma}$ e $b_{\rho,\sigma}$, respectivamente, nos isomorfismos $\mathcal{K} \cong \mathcal{K}'$, $\mathcal{K} \cong \mathcal{K}''$. É, assim,

$$u^*_\rho u^*_\sigma = ea'_{\rho,\sigma} e.eb''_{\rho,\sigma} e.e\, u'_{\rho\sigma} u''_{\rho\sigma} e = ea'_{\rho,\sigma} b'_{\rho,\sigma} e.eu'_{\rho\sigma} u''_{\rho\sigma} e = c^*_{\rho,\sigma} u^*_{\rho\sigma},$$

com $c^*_{\rho,\sigma} = e\, c'_{\rho,\sigma} e$, $c'_{\rho,\sigma} = a'_{\rho,\sigma} . b'_{\rho,\sigma}$. Deste modo fica provado que

$$e\, \mathcal{L}\, e = (\mathcal{K}^*/\mathcal{P},\ c^*_{\rho,\sigma}) \cong (\mathcal{K}/\mathcal{P},\ c_{\rho,\sigma}) .$$

Só resta demonstrar as relações (14'). Tem-se

$$eu'_\rho\, u''_\sigma\, e = eu'_\rho\, u''_\sigma \Phi(\alpha', \alpha'') = eu'_\rho\, \Phi(\alpha', \alpha''^\sigma) u''_\sigma = e\, \Phi(\alpha'^\rho, \alpha''^\sigma) u'_\rho\, u''_\sigma,$$

pois que é $u'_\rho \alpha' = \alpha'^\rho u'_\rho$, $u''_\sigma \alpha'' = \alpha''^\sigma u''_\sigma$, e os elementos de $\mathcal{U}$ e $\mathcal{L}$ são comutáveis. Mas

$$e\, \Phi(\alpha'^\rho, \alpha''^\sigma) = 0, \quad \text{se } \rho \neq \sigma\ ; \quad \Phi(\alpha'^\rho, \alpha''^\rho) = e' = e ,$$

de modo que

$$e\, u'_\rho\, u''_\sigma\, e = 0, \quad \text{se } \rho \neq \sigma\ ; \quad e\, u'_\rho\, u''_\rho\, e = e\, u'_\rho\, u''_\rho .$$

O teorema da multiplicação fica estabelecido.

4) Teorema da ampliação do corpo fundamental[1] - O teorema que temos em vista exige um certo número de considerações preliminares.

Seja Ω um corpo no qual se supõem existir os diferentes corpos que vão ser considerados e são ampliações dum corpo $\mathcal{P}$. $\mathcal{K}$ será uma ampliação normal, separável e finita de $\mathcal{P}$; $\mathcal{Y}$ uma segunda ampliação de $\mathcal{P}$, que apenas se supõe algébrica. Pondo $\mathcal{K} = \mathcal{P}(\alpha)$, onde α satisfaz a uma equação $g(x) = 0$, irredutível em $\mathcal{P}$, o corpo $\mathcal{K}(\mathcal{Y})$, obtido por adjunção de $\mathcal{Y}$ a $\mathcal{K}$, pode escrever-se sob qualquer das formas

$$\mathcal{K}(\mathcal{Y}) = \mathcal{Y}(\alpha) = \mathcal{K}\mathcal{Y} .$$

Efectivamente, $\mathcal{Y}(\alpha)$ contém $\mathcal{K}$, e, portanto, $\mathcal{K}(\mathcal{Y})$. Inversamente, êste último contém $\mathcal{Y}$ e α. Por outro lado, $\mathcal{K}\mathcal{Y}$ está contido em $\mathcal{K}(\mathcal{Y}) = \mathcal{Y}(\alpha)$, e como os elementos de $\mathcal{Y}(\alpha)$ são polinómios em α com coeficientes pertencentes a $\mathcal{Y}$, segue-se que $\mathcal{Y}(\alpha)$ está contido em $\mathcal{K}\mathcal{Y}$.

α é algébrico relativamente a $\mathcal{Y}$, satisfazendo a uma equação irredutível em $\mathcal{Y}$ da forma $g_1(x) = 0$, sendo, aliás, $g(x) = g_1(x).h(x)$. Como todas as raizes de $g_1(x)$ estão contidas em $\mathcal{K}$, segue-se que os coeficientes de $g_1(x)$ pertencem simultâneamente a $\mathcal{K}$ e a $\mathcal{Y}$, isto é, estão contidos em $\mathcal{K} \cap \mathcal{Y}$. Nessas condições, tem-se $(\mathcal{K}/\mathcal{K} \cap \mathcal{Y}) = (\mathcal{K}\mathcal{Y}/\mathcal{Y})$. Posto isto, consideremos o grupo de Galois, $\mathcal{G} = \{\rho, \ldots, \sigma, \ldots, \tau\}$, de $\mathcal{K}$ relativamente a $\mathcal{P}$. O sub-grupo $\mathcal{G}' = \{\sigma', \ldots, \tau'\}$, de $\mathcal{G}$, que deixa fixos os elementos de $\mathcal{K} \cap \mathcal{Y} \equiv \mathcal{P}$, pode identificar-se com o grupo de Galois de $\mathcal{K}\mathcal{Y}$ relativamente a $\mathcal{Y}$, pelas duas razões seguintes:

1) o sub-grupo e o grupo têm a mesma ordem, que é precisamente o

(1) Artin - Nesbitt - Thrall, loc.cit., pgs.89 e seguintes. Voltaremos ao teorema no § final deste Capítulo.

grau de $g_1(x) = 0$; 2) dado um automorfismo de $\mathfrak{K}\mathfrak{P}$ relativamente a $\mathfrak{P}$, tal automorfismo muda α numa outra raiz de $g_1(x) = 0$ e conserva também os elementos de $\mathfrak{K}\cap\mathfrak{P}$; isto é: é um prolongamento dum automorfismo de $\mathfrak{K}$ relativamente a $\mathfrak{K}\cap\mathfrak{P}$. Inversamente, considerado um automorfismo σ', há um automorfismo de $\mathfrak{K}\mathfrak{P}$ relativamente a $\mathfrak{P}$, bem determinado, prolongamento daquele. Podemos enunciar o seguinte

Lema 1:- Se $\mathfrak{K}$ é uma ampliação normal, separável e finita de $\mathfrak{P}$, e se $\mathfrak{P}$ é uma ampliação algébrica de $\mathfrak{p}$, o sub-grupo $\mathcal{G}'$, do grupo de Galois de $\mathfrak{K}$ relativamente a $\mathfrak{p}$, que deixa fixos os elementos de $\mathfrak{K}\cap\mathfrak{P}$, pode identificar-se com o grupo de Galois de $\mathfrak{K}\mathfrak{P}$ relativamente a $\mathfrak{P}$.

Sejam $\mathcal{R} = \mathfrak{K}_m$ uma álgebra central simples sobre $\mathfrak{p}$ e $\mathcal{T}$ uma sub-álgebra simples de $\mathfrak{K}_m$, com o mesmo elemento um da álgebra. Sabemos que $(\mathcal{T}/\mathfrak{p})(\overline{\mathcal{T}}/\mathfrak{p}) = (\mathcal{R}/\mathfrak{p})$, onde $\overline{\mathcal{T}}$ é o comutador de $\mathcal{T}$, em $\mathcal{R}$. Escreveremos $\mathcal{R}^{\mathcal{T}} = \overline{\mathcal{T}}$, utilizando uma notação seguida por muitos autores. Consideremos, em seguida, a álgebra $\mathfrak{P}_n$ e procuremos o comutador de $\mathcal{T}$ em $\mathcal{R}\times\mathfrak{P}_n$. É claro que $\mathcal{R}\times\mathfrak{P}_n$ é uma álgebra central simples sobre $\mathfrak{p}$, na qual se pode supor o elemento um também elemento um de $\mathcal{R}$, de $\mathfrak{P}_n$, e de $\mathcal{T}^{\mathcal{T}}$. Tem-se, evidentemente,

$$(\mathcal{R}\times\mathfrak{P}_n)^{\mathcal{T}} \supseteq \mathcal{R}^{\mathcal{T}}\times\mathfrak{P}_n. \qquad (16)$$

Designemos por N a ordem (relativamente a $\mathfrak{p}$) do 1º membro. Sabemos que $N.(\overline{\mathcal{T}}/\mathfrak{p}) = n^2.(\mathcal{R}/\mathfrak{p})$. A ordem do 2º membro é $n^2.(\mathcal{R}^{\mathcal{T}}/\mathfrak{p})$. Ora é

$$n^2.(\mathcal{R}^{\mathcal{T}}/\mathfrak{p}).(\mathcal{T}/\mathfrak{p}) = n^2.(\mathcal{R}/\mathfrak{p}) = N.(\mathcal{T}/\mathfrak{p}).$$

Daqui se conclui que a ordem dos dois membros de (16) é a mesma, o que nos permite dar este

Lema 2:- Se $\mathcal{R}$ é uma álgebra central simples sobre $\mathfrak{p}$ e $\mathcal{T}$ uma sub-álgebra simples com o mesmo elemento um que a álgebra, o comutador $\mathcal{R}^{\mathcal{T}}$, de $\mathcal{T}$, em $\mathcal{R}$, verifica a relação $(\mathcal{R}\times\mathfrak{P}_n)^{\mathcal{T}} = \mathcal{R}^{\mathcal{T}}\times\mathfrak{P}_n$.

Tomemos ainda a álgebra $\mathfrak{P}_n$. Se $\mathcal{A}$ é uma álgebra de ordem n, sobre $\mathfrak{p}$, com elemento um, escrevendo $\mathcal{A} = e_1\mathfrak{p} + \cdots + e_n\mathfrak{p}$ e considerando $\mathcal{A}$ como um módulo duplo relativamente a $\mathcal{A}$ (à esquerda) e a $\mathfrak{p}$ (à direita), tem-se $\mathcal{A} \cong \mathcal{A}'_1 \subseteq \mathcal{A}'_{\mathfrak{p}} \cong \mathfrak{P}_n$. Por isso, é válido o

Lema 3:- Uma álgebra de ordem n, sobre $\mathfrak{p}$, com elemento um, tem, em $\mathfrak{P}_n$, uma sub-álgebra isomorfa. [Este resultado já foi demonstrado a propósito da representação regular duma álgebra, pgs. 133 e seguintes].

Imaginemos agora que $\mathcal{A}$, além de satisfazer às condições anteriores, é simples, e, nas condições do lema 2, é sub-álgebra de $\mathcal{R}$ com o mesmo elemento um que $\mathcal{R}$. Se $\mathcal{A}_1$ é a sub-álgebra isomorfa de $\mathcal{A}$ contida em $\mathfrak{P}_n$, vale a relação

$$(\mathfrak{P}_n\times\mathcal{R})^{\mathcal{A}_1} \cong \mathfrak{P}_n^{\mathcal{A}_1}\times\mathcal{R}. \qquad (17)$$

A ordem do comutador $\mathfrak{P}_n^{\mathcal{A}_1}$ é também n. Se N é a ordem do 1º membro de (17), tem-se $N.(\mathcal{A}_1/\mathfrak{p}) = n^2.(\mathcal{R}/\mathfrak{P})$, ou $N = n.(\mathcal{R}/\mathfrak{P})$. Em (17) é válido o sinal = . A álgebra $\mathfrak{P}_n\times\mathcal{R}$ contém as duas sub-álgebras isomorfas $\mathcal{A}$ (contida em $\mathcal{R}$) e $\mathcal{A}_1$ (contida em $\mathfrak{P}_n$), as quais têm o mesmo elemento um que a álgebra. O isomorfismo pode ser estendido para um automorfismo de $\mathfrak{P}_n\times\mathcal{R}$, no qual os comutadores de $\mathcal{A}$ e $\mathcal{A}_1$ são correspondentes. Assim, tem-se, por comparação de (16) e (17) [onde o sinal = tem lugar],

$$(\mathcal{R}\times\mathfrak{P}_n)^{\mathcal{A}} \cong (\mathfrak{P}_n\times\mathcal{R})^{\mathcal{A}_1}, \quad \text{ou} \quad \mathcal{R}^{\mathcal{A}}\times\mathfrak{P}_n \cong \mathfrak{P}_n^{\mathcal{A}_1}\times\mathcal{R},$$

o que nos leva ao

Lema 4:- Se $\mathcal{A}$ é uma sub-álgebra simples, de ordem n, da álgebra central simples $\mathcal{R}$, sobre $\mathfrak{p}$, com o mesmo elemento um que a álgebra, e se $\mathcal{A}_1$ é uma sub-álgebra de $\mathfrak{P}_n$, com o mesmo elemento um que esta última e isomorfa de $\mathcal{A}$, tem lugar a seguinte relação: $\mathcal{R}^{\mathcal{A}}\times\mathfrak{P}_n \cong \mathcal{R}\times\mathfrak{P}_n^{\mathcal{A}_1}$.

Lema 5:- Dada a álgebra $\mathcal{L}_\Gamma$, sobre $\mathfrak{p}$, se se tiver $\Omega \supseteq \mathfrak{K} \supseteq \mathfrak{p}$, a álgebra $\mathcal{L}_{\Gamma\Omega}$, sobre Ω, é isomorfa da álgebra sobre Ω obtida

pela expressão $(\mathcal{A}_{\mathfrak{A}})_{\Omega}$, na qual $\mathcal{A}_{\mathfrak{A}}$ é uma álgebra sobre $\mathfrak{A}$. Este lema resulta imediatamente da definição de álgebra ampliada duma álgebra dada. Podemos, mesmo, supor $\mathcal{A}_{\Omega} = (\mathcal{A}_{\mathfrak{A}})_{\Omega}$.

Aditamento ao lema 5:- Se Ω e $\mathfrak{A}$ são ampliações finitas de $\mathfrak{P}$, a álgebra $\mathcal{A}_{\mathfrak{A}} = \mathcal{A}_{\mathfrak{N}} \times \Omega$ (sobre $\mathfrak{P}$) é ainda isomorfa da álgebra sobre $\mathfrak{P}$ obtida pela expressão $\mathcal{A}_{\mathfrak{A}} \times \Omega$, na qual os dois factores $\mathcal{A}_{\mathfrak{A}}$ ($= \mathcal{A}_{\mathfrak{N}} \times \mathfrak{A}$) e Ω se consideram álgebras sobre $\mathfrak{A}$. Embora a demonstração fosse dispensável, vamos fazer uma verificação. Note-se, em primeiro lugar, que é

$$(\mathcal{A}/\mathfrak{P}).(\Omega/\mathfrak{P}) = (\mathcal{A} \times \mathfrak{A}/\mathfrak{A}).(\Omega/\mathfrak{A}).(\mathfrak{A}/\mathfrak{P}),$$

de sorte que as ordens das duas álgebras consideradas são iguais Em seguida, um elemento de $\mathcal{A} \times \Omega$ é da forma seguinte:

$$\alpha = \sum_{\lambda} u_{\lambda} \Omega_{\lambda} = \sum_{\lambda} u_{\lambda} \left(\sum_{\nu} \omega_{\nu} K_{\lambda\nu} \right) =$$

$$= \sum_{\lambda} u_{\lambda} \left(\sum_{\nu} \omega_{\nu} \left(\sum_{\mu} \varkappa_{\mu} p_{\mu\lambda\nu} \right) \right) = \sum_{\lambda,\mu,\nu} u_{\lambda} \omega_{\nu} \varkappa_{\mu} p_{\mu\lambda\nu} ,$$

onde os u_{λ} constituem uma base de $\mathcal{A}$ (sobre $\mathfrak{P}$), os $\Omega_{\lambda} \in \Omega$, os ω_{ν} são uma base de Ω (sobre $\mathfrak{A}$), os $K_{\lambda\nu} \in \mathfrak{A}$, os $\varkappa_{\mu}$ formam uma base de $\mathfrak{A}$ (sobre $\mathfrak{P}$) e os $p_{\mu\lambda\nu} \in \mathfrak{P}$. Quando for $\alpha = 0$, é $\Omega_{\lambda} = 0$, por consequência $K_{\lambda\nu} = 0$ e $p_{\mu\lambda\nu} = 0$. Inversamente, se $p_{\mu\lambda\nu} = 0$, tem-se $\alpha = 0$. Estudemos, por fim, os elementos de $(\mathcal{A} \times \mathfrak{A}) \times \Omega$. Se β é um tal elemento, tem-se

$$\beta = \sum_{\lambda,\nu} u_{\lambda} \omega_{\nu} K_{\lambda\nu} = \sum_{\lambda,\nu} u_{\lambda} \omega_{\nu} \left(\sum_{\mu} \varkappa_{\mu} p_{\mu\lambda\nu} \right) = \sum_{\lambda,\nu,\mu} u_{\lambda} \omega_{\nu} \varkappa_{\mu} p_{\mu\lambda\nu} .$$

Como anteriormente, se $\beta = 0$, tem-se $K_{\lambda\nu} = 0$, $p_{\mu\lambda\nu} = 0$. Inversamente, se $p_{\mu\lambda\nu} = 0$, é $\beta = 0$. O aditamento está provado.

As considerações desenvolvidas vão permitir-nos demonstrar o teorema seguinte, objecto deste §.

Teorema:- Se $\mathfrak{A}$, $\mathfrak{N}$, $\mathfrak{P}$ são os corpos referidos no lema 1, o produto cruzado $Q = (\mathfrak{A}\mathfrak{N}/\mathfrak{N}, a_{\sigma,\tau})$, considerado como álgebra central sobre $\mathfrak{N}$, é semelhante à álgebra sobre $\mathfrak{N}$, $(\mathfrak{A}/\mathfrak{P}, a_{\sigma,\tau})_{\mathfrak{N}}$.

A existência do produto cruzado Q resulta imediatamente das considerações feitas a propósito do lema 1. Para se provar o teorema, trataremos primeiramente dois casos limites, nos quais se baseia depois a demonstração do caso geral. Esses casos limites são os que correspondem às duas hipóteses seguintes: $\mathfrak{A} \cap \mathfrak{N} = \mathfrak{N}$, $\mathfrak{A} \cap \mathfrak{N} = \mathfrak{P}$. No primeiro, tem-se $\mathfrak{N} \subseteq \mathfrak{A}$, $\mathfrak{A}\mathfrak{N} = \mathfrak{A}$. Se for n a ordem de $\mathfrak{N}$ relativamente a $\mathfrak{P}$, tendo em conta que é $\mathfrak{N} \subseteq P = (\mathfrak{A}/\mathfrak{P}, a_{\sigma,\tau})$, podemos escrever (lema 4)

$$P^{\mathfrak{N}} \times \mathfrak{P}_n \cong \mathfrak{P}_n^{\mathfrak{N}_1} \times P , \qquad (\mathfrak{N} \cong \mathfrak{N}_1 \subseteq \mathfrak{P}_n) .$$

Ora o comutador de $\mathfrak{N}_1$ em $\mathfrak{P}_n$ é precisamente $\mathfrak{N}_1$. Assim, tem-se

$$P^{\mathfrak{N}} \times \mathfrak{P}_n \cong \mathfrak{N}_1 \times P \cong \mathfrak{N} \times P . \tag{18}$$

Sabemos que $P^{\mathfrak{N}}$ é uma sub-álgebra simples de P, com o mesmo elemento um que a álgebra e tendo o centro igual a $\mathfrak{N}$. Significa isto que $P^{\mathfrak{N}}$ é álgebra central sobre $\mathfrak{N}$, da forma $P^{\mathfrak{N}} = \mathcal{D}_r$, onde $\mathcal{D}$ é álgebra central de divisão sobre $\mathfrak{N}$. Mas, então, considerando os produtos directos sucessivos de álgebras sobre $\mathfrak{P}$, $P^{\mathfrak{N}} \times \mathfrak{P}_n = \mathcal{D}_r \times \mathfrak{P}_n = \mathcal{D} \times \mathfrak{P}_r \times \mathfrak{P}_n = \mathcal{D}_{rn}$, vê-se que o produto indicado em 1º lugar é uma álgebra central sobre $\mathfrak{N}$, o que também se conclui a partir de (18). Na correspondência entre o 1º membro e o último membro de (18), como resulta dos raciocínios a propósito do lema 4, os elementos de $\mathfrak{N}$ conservam-se invariantes. A álgebra $P_{\mathfrak{N}}$, sobre $\mathfrak{N}$, é precisamente $P \times \mathfrak{N}$, de sorte que o caso em questão do teorema, por ser $P^{\mathfrak{N}} \approx P_{\mathfrak{N}}$, reduz-se a mostrar a semelhança $Q \approx P^{\mathfrak{N}}$. Estudemos esta última. A condição necessária e suficiente para que $\alpha = \Sigma a_{\sigma} u_{\sigma} \in P$ comute com $\varkappa \in \mathfrak{N}$ é dada por $\Sigma \varkappa a_{\sigma} u_{\sigma} = \Sigma a_{\sigma} \varkappa^{\sigma} u_{\sigma}$, ou $\varkappa a_{\sigma} = a_{\sigma} \varkappa^{\sigma}$. Visto ser $\varkappa$ qualquer, a relação $\varkappa = \varkappa^{\sigma}$ mostra que, na expressão de α, apenas podem figurar os automorfismos $\sigma \in \mathcal{G}$ que deixam invariantes os elementos de $\mathfrak{N} = \mathfrak{A} \cap \mathfrak{N}$, isto é, mostra que deverá ter-se $\sigma = \sigma', \ldots, \tau'$. Assim

$$\alpha = \sum_{\sigma \in \mathcal{G}} a_{\sigma} u_{\sigma} .$$

O conjunto dos $a a_{\sigma}$ constitui um sistema isomorfo de Q, tendo-se, como se deseja, $P^{\mathfrak{N}} \approx Q$. Podemos, mesmo, supor $P^{\mathfrak{N}} = Q$.

No segundo caso limite, o corpo $\mathfrak{A}\mathfrak{N}$ pode escrever-se sob a forma $\mathfrak{A}\mathfrak{N}$, pois que a ordem de $\mathfrak{A}\mathfrak{N}$ relativamente a $\mathfrak{N}$ é dada pelas igualdades

$$(\mathfrak{K}\mathfrak{o}/\mathfrak{o}) = (\mathfrak{K}/\mathfrak{K}\cap\mathfrak{o}) = (\mathfrak{K}/\mathfrak{Z}) = (\mathfrak{K}_{\mathfrak{o}}/\mathfrak{o}).$$

A álgebra $P_{\mathfrak{o}}$ (sobre $\mathfrak{o}$) contém, assim, $\mathfrak{K}\mathfrak{o}$. Dentro dela pode definir-se o produto cruzado $(\mathfrak{K}\mathfrak{o}/\mathfrak{o}, a_{\sigma,\tau})$. A ordem deste produto, considerado como álgebra sobre $\mathfrak{o}$, é a ordem de P (sobre $\mathfrak{Z}$) ou de $P_{\mathfrak{o}}$ (sobre $\mathfrak{o}$). Quer dizer que se tem $P_{\mathfrak{o}} = (\mathfrak{K}\mathfrak{o}/\mathfrak{o}, a_{\sigma,\tau})$, como se afirma no teorema.

Passemos, finalmente, ao caso geral. É aqui que se aplica o lema 5. Ponhamos $\mathfrak{M}=\mathfrak{K}\cap\mathfrak{o}$, de sorte que $\mathfrak{o}\supseteq\mathfrak{M}\supseteq\mathfrak{Z}$. O lema 5 dá

$$P_{\mathfrak{o}} \cong (P_{\mathfrak{M}})\times\mathfrak{o} = (P\times\mathfrak{M})_{\mathfrak{o}}, \qquad (19)$$

onde o 2º membro se deve considerar uma álgebra sobre $\mathfrak{o}$, ampliação da álgebra sobre $\mathfrak{M}$, $P\times\mathfrak{M} = P_{\mathfrak{M}}$. Consideremos o produto directo $P\times\mathfrak{M}$, nas condições seguintes, que são relativas ao 1º caso limite (envolvendo aqui álgebras sobre $\mathfrak{M}$):

$$\mathfrak{K}\supseteq\mathfrak{M}, \quad \mathfrak{K}\cap\mathfrak{M}=\mathfrak{M}, \quad (\mathfrak{K}\mathfrak{M}/\mathfrak{M}, a_{\sigma',\tau'}) = (\mathfrak{K}/\mathfrak{M}, a_{\sigma',\tau'}),$$

$$Q' = (\mathfrak{K}/\mathfrak{M}, a_{\sigma',\tau'}) = P' = P^{\mathfrak{M}} \approx P\times\mathfrak{M} = P_{\mathfrak{M}},$$

depois, formemos a álgebra $P'_{\mathfrak{o}}$, nestas outras condições, relativas ao segundo caso limite (onde se consideram álgebras sobre $\mathfrak{o}$):

$$\mathfrak{o}\supseteq\mathfrak{M}, \quad \mathfrak{K}\cap\mathfrak{o}=\mathfrak{M}, \quad (\mathfrak{K}\mathfrak{o}/\mathfrak{o}, a_{\sigma',\tau'}) = P'_{\mathfrak{o}}.$$

Visto que P' e $P\times\mathfrak{M}$ são duas álgebras centrais semelhantes, sobre $\mathfrak{M}$, as duas álgebras, sobre $\mathfrak{o}$,

$$(P\times\mathfrak{M})_{\mathfrak{o}}, \qquad P'_{\mathfrak{o}} = (\mathfrak{K}\mathfrak{o}/\mathfrak{o}, a_{\sigma',\tau'}),$$

são também semelhantes. A relação (19) dá, em seguida,

$$P_{\mathfrak{o}} \approx (\mathfrak{K}\mathfrak{o}/\mathfrak{o}, a_{\sigma',\tau'}),$$

como afirma o teorema.

5) Álgebras cíclicas[1] - Os raciocínios do § 1 revestem-se dum aspecto muito simples, quando a ampliação separável $\mathfrak{K}$, de $\mathfrak{Z}$, é cíclica. Significa isto que o grupo de Galois, $\mathfrak{G}$, dos automorfismos de $\mathfrak{K}$ relativamente a $\mathfrak{Z}$, é cíclico. Poremos

$$\mathfrak{G} = \{\rho, \rho^2, \ldots, \rho^n\}, \qquad (\rho^n = 1). \qquad (20)$$

Um sistema de factores $a_{\rho,\sigma}$, sempre tendo em conta as relações (3), vai ser determinado pelas considerações a seguir. Imaginemos construido o produto cruzado. Por via de (5), tem-se

$$u_\rho\beta = \beta^{\rho^\nu} u_\rho .$$

Mas, numa prova por indução, tem-se

$$u_\rho\beta = \beta^\rho u_\rho, \qquad u_\rho^{\nu-1}\beta = \beta^{\rho^{\nu-1}} u_\rho^{\nu-1},$$

$$u_\rho^\nu\beta = u_\rho(u_\rho^{\nu-1}\beta) = u_\rho\left(\beta^{\rho^{\nu-1}} u_\rho^{\nu-1}\right) = \beta^{\rho^\nu} u_\rho^\nu .$$

Vê-se que os elementos u_ρ^ν e u_{ρ^ν} definem automorfismos internos do produto cruzado, os quais prolongam o mesmo automorfismo de $\mathfrak{K}$. Os símbolos necessários à construção do produto podem ser, por isso, os elementos u_ρ^ν. Se observarmos que se tem $u_\rho^n\beta = \beta^{\rho^n} u_\rho^n = \beta u_\rho^n$, concluimos que u_ρ^n comuta com todos os elementos de $\mathfrak{K}$. Como comuta igualmente com todos os símbolos base u_ρ^ν, segue-se que u_ρ^n pertence ao centro do produto cruzado. Pondo $u_\rho^n = a\in\mathfrak{Z}$, as regras (2) são aqui as seguintes:

$$\begin{aligned} &u_\rho^\lambda u_\rho^\mu = u_\rho^{\lambda+\mu}, \quad \text{se} \quad \lambda+\mu < n; \\ &u_\rho^\lambda u_\rho^\mu = a\, u_\rho^{\lambda+\mu-n}, \quad \text{se} \quad \lambda+\mu \geq n. \end{aligned} \qquad (21)$$

Verifiquemos directamente as igualdades (3) que garantem a associatividade do produto definido por (1). Bastará verificar a relação

(1) Cfr. Deuring, Algebren, pgs. 64 e seguintes; e Albert, pgs. 74 e 75.

$$u_\rho^\lambda\,(u_\rho^\mu \cdot u_\rho^\nu) = (u_\rho^\lambda \cdot u_\rho^\mu)\,u_\rho^\nu \,. \qquad (22)$$

Imaginemos, por ex., $\mu+\nu<n$, $\lambda+\mu<n$, $\lambda+\mu+\nu<n$. Os dois membros de (22) são iguais a $u_\rho^{\lambda+\mu+\nu}$. Como 2º exemplo, tomemos $\mu+\nu<n$, $\lambda+\mu<n$, e $\lambda+\mu+\nu>n$. Então, o primeiro membro, como o segundo, será $a u_\rho^{\lambda+\mu+\nu-n}$. A hipótese $\lambda+\mu<n$, $\mu+\nu>n$ dá, no 1º membro,

$$u_\rho^\lambda\,(a\,u_\rho^{\mu+\nu-n}) = a\,u_\rho^{\lambda+\mu+\nu-n}\,, \qquad (\lambda+\mu+\nu<2n),$$

pois que $a\in\mathfrak{P}$. No 2º membro encontra-se também

$$u_\rho^{\lambda+\mu}\cdot u_\rho^\nu = a\,u_\rho^{\lambda+\mu+\nu-n}\,.$$

Do mesmo modo se tratam as restantes hipóteses que se imaginem. O significado deste raciocínio é imediato: por um lado, se o produto cruzado em que $\mathfrak{K}$ é cíclico se pode construir, as relações (22) são necessàriamente válidas; por outro, os símbolos u_ρ^λ, com as regras de produto indicadas em (21), permitem estabelecer as igualdades (22). Assim, é válido o

Teorema 1:- À custa dum elemento $a\in\mathfrak{P}$ e dum corpo cíclico $\mathfrak{K}$, de ordem n relativamente a $\mathfrak{P}$, constroi-se um produto cruzado $(\mathfrak{K}/\mathfrak{P}, a)$, pondo (21) como regras de multiplicação dos elementos base. O referido produto cruzado contém um corpo cíclico de decomposição (o corpo $\mathfrak{K}$). Reciprocamente: se uma álgebra central simples sobre $\mathfrak{P}$, de ordem n, contém um corpo cíclico $\mathfrak{K}$ de decomposição, de ordem n, a referida álgebra é um produto cruzado $(\mathfrak{K}/\mathfrak{P}, a)$, onde $a\in\mathfrak{P}$.

Dizem-se álgebras cíclicas as álgebras centrais simples de ordem n^2 sobre $\mathfrak{P}$, que contêm um corpo cíclico de decomposição de ordem n.

Tratemos a questão dos sistemas de factores associados. Por simplicidade de escrita, poremos $\rho=\rho$, $\rho^2=\sigma$, ..., $\rho^n=\tau$. Se, na álgebra cíclica $(\mathfrak{K}/\mathfrak{P}, a)$, substituirmos os elementos $u_\rho = u_\rho$, $u_\sigma = u_\rho^2$, ..., $u_\tau = u_\rho^n$, por elementos $v_\rho, v_\sigma, \ldots, v_\tau$, sabemos que é possível imaginar

$$v_\rho = v_\rho\,, \quad v_\sigma = v_\rho^2\,, \ldots, v_\tau = v_\rho^n\,.$$

Pondo, então $v_\rho^n = b$, tem-se

$$(\mathfrak{K}/\mathfrak{P}, a) = (\mathfrak{K}/\mathfrak{P}, b), \qquad v_\rho = \alpha u_\rho\,.$$

Em virtude de ser

$$b = v_\rho^n = \alpha u_\rho \cdot \alpha u_\rho \ldots \alpha u_\rho = \alpha\alpha^\rho\,\alpha^{\rho^2}\ldots\alpha^{\rho^{n-1}}\,u_\rho^n = \Big(\prod_{\sigma\in v_\rho^1}\alpha^\sigma\Big)\cdot a\,,$$

podemos enunciar o seguinte

Teorema 2:- É condição necessária e suficiente, para que duas álgebras cíclicas $(\mathfrak{K}/\mathfrak{P}, a)$ e $(\mathfrak{K}/\mathfrak{P}, b)$ sejam isomorfas, que exista um elemento $\alpha\in\mathfrak{K}$ tal que

$$b = a\cdot\prod_{\sigma\in v_\rho^1}\alpha^\sigma\,, \qquad (\sigma=\rho, \rho^2, \ldots, \rho^n). \qquad (23)$$

A quantidade $\prod_{\sigma\in v_\rho^1}\alpha^\sigma$, que pode representar-se ainda pelo símbolo $N(\alpha) = N_{\mathfrak{K}/\mathfrak{P}}(\alpha)$, diz-se norma do elemento $\alpha\in\mathfrak{K}$.

Teorema 3:- É condição necessária e suficiente, para que uma álgebra cíclica, de ordem n^2, $(\mathfrak{K}/\mathfrak{P}, b)$, seja uma álgebra $\mathfrak{P}_n$, que b seja norma dum elemento de $\mathfrak{K}$. Os factores $a_{\rho,\sigma}$ deverão poder reduzir-se, exclusivamente, a $a_{\rho,\sigma} = u$. Mas, então, supondo $a = u$ na relação (23), tem-se $b =$ norma de α.

Teorema 4:- O produto directo de duas álgebras cíclicas geradas à custa do mesmo corpo cíclico $\mathfrak{K}$ pode tomar a forma

$$(\mathfrak{K}/\mathfrak{P}, a)\times(\mathfrak{K}/\mathfrak{P}, b) = (\mathfrak{K}/\mathfrak{P}, u)\times(\mathfrak{K}/\mathfrak{P}, ab)\,.$$

O teorema da multiplicação mostra que o primeiro membro é uma álgebra central simples sobre $\mathfrak{P}$ semelhante a $(\mathfrak{K}/\mathfrak{P}, ab) = \mathcal{L}_t$. O 1º membro é, assim, da forma $\mathcal{L}_\rho = \mathcal{L}\times\mathfrak{P}_\rho$. O 2º membro é da forma $\mathfrak{P}_n\times\mathcal{L}_t = \mathfrak{P}_{n_t}\times\mathcal{L}$. Devendo ter-se $nt = \rho$, podemos supor iguais os dois membros.

Teorema 5:- A potência n duma álgebra cíclica de ordem n^2 é uma álgebra $\mathcal{P}_t$. De facto, tem-se

$$(\mathcal{A}/\mathcal{P}, a)^n \approx (\mathcal{A}/\mathcal{P}, a^n) .$$

Ora a^n pode escrever-se sob a forma de norma dum elemento de $\mathcal{A}$:

$$a^n = N(a) = \prod_{\sigma \in \mathcal{G}} a^\sigma , \qquad (a^\sigma = a, \text{ qualquer que seja } \sigma \in \mathcal{G}).$$

Teorema 6:- É condição necessária e suficiente, para que a potência $\mathcal{D}^r$ duma álgebra cíclica de divisão de ordem p^2, com p primo, seja uma álgebra $\mathcal{P}_m$, que se tenha $r = pq$. Ponhamos

$$\mathcal{D} = (\mathcal{A}/\mathcal{P}, a) , \qquad \mathcal{P}_m = \mathcal{D}^r \approx (\mathcal{A}/\mathcal{P}, a^r) .$$

Sabemos que é $a^r = N(\alpha)$, com $\alpha \in \mathcal{A}$. Se p não dividisse r, existiriam dois inteiros λ, μ tais que $\lambda p + \mu r = 1$. E, então, seria

$$a = a^{\lambda p + \mu r} = (a^\lambda)^p . (a^r)^\mu = (a^\lambda)^p . \left[N(\alpha)\right]^\mu .$$

Como a norma dum produto é o produto das normas dos factores, pode pôr-se ainda

$$a = (a^\lambda)^p . N(\alpha^\mu) = N(a^\lambda \alpha^\mu) .$$

Este resultado prova que $\mathcal{D}$ seria uma álgebra $\mathcal{P}_t$, o que é absurdo. Inversamente, se p divide r, tem-se

$$\mathcal{D}^r \approx (\mathcal{A}/\mathcal{P}, a^r) = (\mathcal{A}/\mathcal{P}, a^{pq}), \qquad a^{pq} = N(a^q).$$

O teorema está demonstrado.

Voltemos ao teorema 2. Os elementos $a, b \in \mathcal{P}$ são equivalentes, por via da seguinte relação de equivalência, definida no grupo multiplicativo $\mathcal{P}^*$, dos elementos não nulos do corpo $\mathcal{P}$: considera-se, em $\mathcal{P}^*$, o sub-grupo $\mathcal{N}^*$ daqueles elementos que são normas de elementos de $\mathcal{A}$; depois, consideram-se as classes $\mathcal{P}^*/\mathcal{N}^*$ de equivalentes. $\mathcal{P}^*/\mathcal{N}^*$ diz-se, então, o grupo factor das

normas, e os seus elementos dizem-se classes de normas. Da combinação dos teoremas 2 e 4 resulta, em seguida, esta proposição:

Teorema 7:- As classes de álgebras cíclicas semelhantes formam um grupo isomorfo do grupo factor das normas.

Aplicação:- Há uma só álgebra central de divisão sobre o corpo $\mathcal{P}$ dos números reais: é a álgebra $\mathcal{D}$ dos quaterniões (pgs.131).(1)

Vimos no Capítulo anterior, § 7, que toda a álgebra central de divisão contém uma ampliação separável máxima do seu corpo fundamental. Essa ampliação só pode ser o corpo algèbricamente fechado, Ω, dos números complexos. Nessas condições, ter-se-á $(\mathcal{D}/\mathcal{P}) = (\Omega/\mathcal{P})^2$, de sorte que a álgebra $\mathcal{D}$ é necessàriamente de 4ª ordem. Ω é um corpo cíclico do 2º grau (relativamente a $\mathcal{P}$). As únicas álgebras cíclicas $(\Omega/\mathcal{P}, a)$, não semelhantes, são as duas álgebras $(\Omega/\mathcal{P}, 1)$ e $(\Omega/\mathcal{P}, -1)$, ambas de 4ª ordem, visto que os números positivos, e apenas esses, são normas de elementos de Ω. A primeiras das duas álgebras não é álgebra de divisão. A álgebra $\mathcal{D}$ será, portanto, $\mathcal{D} = (\Omega/\mathcal{P}, -1)$. Se u_ρ e u_ρ^2 forem os elementos de $\mathcal{D}$ que definem os automorfismos de Ω, podemos supor

$$\mathcal{D} = \mathcal{P}u_\rho + \mathcal{P}i\, u_\rho + \mathcal{P}u_\rho^2 + \mathcal{P}i\, u_\rho^2 , \qquad (i = \sqrt{-1} , \quad u_\rho^2 = -1).$$

As regras de multiplicação dos elementos base são as regras de pgs.131, se substituirmos u_ρ^2 por $-u_\rho^2$. Então tem-se, com efeito,

$$-u_\rho^2 (-u_\rho^2) = 1 = -u_\rho^2 , \qquad u_\rho(-u_\rho^2) = u_\rho ,$$

$$-u_\rho^2 (u_\rho) = -(-u_\rho) = u_\rho , \qquad u_\rho u_\rho = -(-u_\rho^2) ,$$

(1) Para outra forma de concluir, veja-se Deuring, Algebren, pgs. 50, assim como van der Waerden, Moderne Algebra, II Teil, pgs.211.

$$-u_\rho^2\,(i\,u_\rho) = -\,i\,u_\rho^3 = i\,u_\rho\ , \qquad u_\rho(i\,u_\rho) = -\,i\,u_\rho^2\ ,$$

$$-u_\rho^2\,(-i\,u_\rho^2) = i\,u_\rho^4 = i = -i\,u_\rho^2\ , \qquad u_\rho(-i\,u_\rho^2) = i\,u_\rho^3 = -i\,u_\rho ,$$

etc. Estamos em presença da álgebra dos quaterniões, como se afirmou.

6) O expoente duma álgebra central simples[1] - Tomemos uma classe $(\mathcal{G})$ de álgebras centrais simples sobre $\mathcal{P}$. Se for $\mathcal{A}\in(\mathcal{G})$, tem-se $\mathcal{A} = \mathcal{G}\times\mathcal{P}_\lambda$, e, portanto,

$$\mathcal{A}^f = \mathcal{G}^f \times \mathcal{P}_{\lambda^f}\ .$$

Se for $\mathcal{A}^f\in(\mathcal{P})$, é também $\mathcal{G}^f\in(\mathcal{P})$, e reciprocamente. Diz-se expoente da álgebra $\mathcal{A}$, ou, mais precisamente, expoente da classe $(\mathcal{G})$, o mais pequeno inteiro ρ, tal que $\mathcal{G}^\rho\in(\mathcal{P})$. O expoente duma classe representa, pois, a ordem dessa classe, considerada como elemento do grupo abeliano multiplicativo constituido pelas classes.

Um dos teoremas a demonstrar sobre o expoente assenta sobre algumas propriedades dos grupos finitos, propriedades que vamos tratar imediatamente.

Seja p um número primo. Num grupo de ordem p não há outro sub-grupo próprio além do sub-grupo unidade. Qualquer elemento do grupo diferente do elemento um tem a ordem igual a p. É válido o seguinte

Lema 1 (Cauchy):- Se um número primo p divide a ordem N dum grupo finito $\mathcal{G}$, há, em $\mathcal{G}$, um elemento de ordem p. O lema é válido para os grupos cuja ordem, decomposta em números primos (distintos ou não), leva ao único número primo p. Admitamos que é igualmente válido para os grupos cuja ordem N se decompõe em $n-1$ factores primos. Vamos mostrar que é válido para o caso de N se decompor em n factores primos (entre os quais p). Se o grupo $\mathcal{G}$ contém um sub-grupo $\mathcal{G}'$, de ordem N' e índice $I \neq 1$ que não admite p como factor, a relação $N = I\times N'$ mostra que o lema tem lugar, por hipótese, em $\mathcal{G}'$, e, portanto, em $\mathcal{G}$. Finalmente, admitamos que todos os sub-grupos de $\mathcal{G}$ têm índices divisíveis por p. Se $a\in\mathcal{G}$, os elementos de $\mathcal{G}$ que comutam com a constituem um sub-grupo, chamado normalizador de a. O índice do normalizador é igual ao número de elementos conjugados de a. Fazendo a decomposição de $\mathcal{G}$ em classes de elementos conjugados, os números $C_1, C_2, \ldots, C_r$, de elementos das diferentes classes, representam, portanto, índices de sub-grupos de $\mathcal{G}$. Supondo $C_1 = \ldots = C_q = 1$, $C_{q+1} = p.D_{q+1}, \ldots, C_r = p.D_r$, tem-se

$$N = C_1 + \ldots + C_r = q + p(D_{q+1} + \ldots + D_r)\ .$$

Como p divide N, será q divisível por p. Ora q representa o número de elementos do centro $\mathcal{Z}$, de $\mathcal{G}$. Como grupo abeliano cuja ordem contém o factor p, $\mathcal{Z}$ é um produto directo de grupos cíclicos de ordens iguais a potências de números primos, entre os quais um grupo cíclico de ordem p^t, com $t > 0$. Neste último grupo cíclico há elementos de ordem p. O lema está provado.[1]

Lema 2 (Sylow):- Se p^s é a maior potência de p contida na ordem N dum grupo finito $\mathcal{G}$, há, em $\mathcal{G}$, sub-grupos de ordem p^r, qualquer que seja $0 \lesssim r \lesssim s$. Os sub-grupos de ordem p^s dizem-se os grupos de Sylow, de $\mathcal{G}$, relativos ao número primo p. Como o lema é válido no caso de ser $N = p$ a ordem de $\mathcal{G}$, podemos aplicar o mesmo processo de indução que foi utilizado no lema anterior. Assim, o lema tem lugar quando a ordem N é um produto de $n-1$ números primos, distintos ou não. Se há n números primos na decomposição de N, temos de considerar apenas a hipótese de serem divisíveis por p todos os índices dos sub-grupos de $\mathcal{G}$. Então, o centro $\mathcal{Z}$, de $\mathcal{G}$, contém um sub-grupo de ordem p. Esse sub-grupo é um divisor normal de $\mathcal{G}$, e o grupo factor correspondente contém, pela hipótese da indução, sub-grupos da ordem p^r com $0 \lesssim r \lesssim s-1$. Distinguindo os elementos de $\mathcal{G}$ que cons-

(1) Artin - Nesbitt - Thrall, loc.cit. pgs.93-95.

(1) Para as diferentes propriedades dos grupos finitos que foram invocadas, veja-se Almeida Costa, "Elementos da Teoria dos Grupos", pgs.65 e 66, assim como pgs.88 e seguintes.

tituem os diferentes elementos de cada um daqueles sub-grupos, obtêm-se sub-grupos de $\mathcal{G}$ cujas ordens são da forma $p.p^r$. O lema 2 está demonstrado.(1)

Depois disto, eis aqui a primeira afirmação sobre expoentes:

Teorema 1:- Se a ordem da álgebra central de divisão $\mathcal{D}$, sobre $\mathcal{P}$, for $(\mathcal{D}/\mathcal{P}) = n_1^2$ tem-se $\mathcal{D}^n \in (\mathcal{P})$. O número n é, assim, um múltiplo do expoente da classe $(\mathcal{D})$.

Seja Δ uma ampliação finita, normal e separável de $\mathcal{P}$, corpo de decomposição de $\mathcal{D}$. A representação irredutível única, de grau r, de Δ, em $\mathcal{D}$, é um corpo $\Delta^* \cong \mathcal{D}_r = \mathcal{D} \times \mathcal{P}_r$. Como $\Delta \cong \Delta^*$, tem-se

$$(\mathcal{D}_r/\mathcal{P}) = (\Delta/\mathcal{P})^2 = r_1^2(\mathcal{D}/\mathcal{P}) = r^2n^2, \quad (\Delta/\mathcal{P}) = rn .$$

Suponhamos Δ contido em $\mathcal{D}_r$. Os automorfismos de Δ relativamente a $\mathcal{P}$ prolongam-se, em $\mathcal{D}_r$, para automorfismos internos desta última álgebra, definidos por elementos $u_\rho, u_\sigma, \ldots, u_\tau$, independentes com respeito a Δ. O produto cruzado correspondente $(\Delta/\mathcal{P}, a_{\rho,\sigma}) \subseteq \mathcal{D}_r$ é necessàriamente igual a $\mathcal{D}_r$, visto que as ordens das duas álgebras sobre $\mathcal{P}$ são iguais. Pondo $\mathcal{D}_r = \sum \mathcal{W}_i$, $(i = 1, 2, \ldots, r)$, onde os $\mathcal{W}_i$ são ideais esquerdos simples, cada $\mathcal{W}_i$ é módulo esquerdo relativamente a Δ. Será $(\mathcal{W}_i/\Delta) = n$, pois $(\mathcal{D}_r/\Delta) = nr$. Tomemos, em $\mathcal{W}_i$, os n elementos $f_1, f_2, \ldots, f_n$, de modo a constituirem uma base independente sobre Δ. É claro que se tem

$$u_\rho f_k = \sum_{l=1}^{n} \delta_{kl}^{(\rho)} f_l , \quad (\delta_{kl}^{(\rho)} \in \Delta), \quad (k = 1, 2, \ldots, n) .$$

Sob forma matricial, podemos escrever

$$u_\rho \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = U_\rho \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}, \qquad U_\rho = (\delta_{kl}^{(\rho)}) , \quad (\rho = \rho, \sigma, \ldots, \tau) ,$$

(1) Um estudo pormenorizado dos grupos de Sylow e dos grupos-p (grupos cuja ordem é a potência dum número primo p) encontra-se nas obras seguintes:
- Theorie der Gruppen von endlicher Ordnung, de A. Speiser, pgs. 64 e seguintes; e Lehrbuch der Gruppentheorie, de H. Zassenhaus, Berlin, 1937, pgs. 99 e seguintes.

de sorte que os U_ρ constituem matrizes quadradas de n filas, com elementos de Δ. Mas tem-se, chamando F a matriz de uma coluna formada pelos f_i,

$$u_\rho u_\sigma F = u_\rho U_\sigma F = U_\sigma^\rho U_\rho F , \qquad u_\rho u_\sigma F = a_{\rho,\sigma} u_{\rho\sigma} F = a_{\rho,\sigma} U_{\rho\sigma} F ,$$

onde U_σ^ρ representa a matriz quadrada cujos elementos se obtêm dos elementos de U_σ por via do automorfismo ρ, de Δ. Das relações anteriores, conclui-se

$$U_\sigma^\rho \, U_\rho = a_{\rho,\sigma} U_{\rho\sigma} .$$

Pondo o determinante $|U_\rho| = \beta_\rho$, a igualdade anterior, tomando os determinantes dos dois membros, dá

$$\beta_\sigma^\rho \beta_\rho = a_{\rho,\sigma}^n \beta_{\rho\sigma} , \qquad \text{ou} \qquad a_{\rho,\sigma}^n = \frac{\beta_\rho \beta_\sigma^\rho}{\beta_{\rho\sigma}} .$$

O teorema 4 do § 2 diz-nos que o produto cruzado $(\Delta/\mathcal{P}, a_{\rho,\sigma}^n)$ é isomorfo dum anel completo de matrizes com elementos de $\mathcal{P}$. Este produto cruzado, conforme o teorema da multiplicação, pertence à mesma classe de álgebras semelhantes que a álgebra $(\Delta/\mathcal{P}, a_{\rho,\sigma})^n = \mathcal{D}_r^n$; e a relação

$$\mathcal{D}_r^n = \mathcal{D}^n \times \mathcal{P}_r^n \in (\mathcal{P})$$

mostra que $\mathcal{D}^n \in (\mathcal{P})$, como se afirmou.

Teorema 2:- O expoente da álgebra $\mathcal{D}$ do teorema 1 é divisível por todo o número primo p que divida n. Seja p divisor de n. O grupo de Galois $\mathcal{G} = \{\rho, \sigma, \ldots, \tau\}$, de Δ, relativamente a $\mathcal{P}$, referido no teorema anterior, é de ordem nr. Se p^t é a ordem dum grupo-p de Sylow, $\mathcal{G}'$, contido em $\mathcal{G}$, designemos por $\mathcal{P}'$ o sub-corpo invariante completo de $\mathcal{G}'$, intermédio entre $\mathcal{P}$ e Δ. Em virtude de se ter $(\Delta/\mathcal{P}) = (\Delta/\mathcal{P}').(\mathcal{P}'/\mathcal{P}) = p^t(\mathcal{P}'/\mathcal{P})$, vê-se que p não divide $(\mathcal{P}'/\mathcal{P})$. O grau $(\Delta/\mathcal{P}')$ verifica, de resto, uma outra relação. Ponhamos

$$\mathcal{D}_{\mathcal{P}'} = \mathcal{L} \times \mathcal{P}_\lambda' , \qquad (\mathcal{L} = \text{álgebra de divisão sobre } \mathcal{P}') ,$$

e notemos que Δ é corpo de decomposição de $\mathfrak{D}_{\mathfrak{p}'}$ e de $\mathcal{L}$. Se s for o grau da representação irredutível única de Δ, em $\mathcal{L}$, tem-se $(\Delta/\mathfrak{P}')^2 = s^2(\mathcal{L}/\mathfrak{P}')$, que é precisamente a relação em vista. O grau $(\mathcal{L}/\mathfrak{P}')$ será, assim, uma potência de p, e o seu expoente ρ' (como álgebra sobre $\mathfrak{P}'$), pelo facto de dividir $(\mathcal{L}/\mathfrak{P}')$, é igualmente uma potência de p. A igualdade

$$(\mathfrak{D}\times\mathfrak{D}\times\dots\times\mathfrak{D})_{\mathfrak{p}'} = \mathfrak{D}_{\mathfrak{p}'}\times\dots\times\mathfrak{D}_{\mathfrak{p}'}$$

mostra que

$$(\mathfrak{D}^\rho)_{\mathfrak{p}'} = (\mathfrak{D}_{\mathfrak{p}'})^\rho = (\mathfrak{P}_\mu)_{\mathfrak{p}'} = \mathfrak{P}'_\mu \ ,$$

de sorte que o expoente ρ é múltiplo do expoente ρ'. Conclui-se, como se afirmou, que p é divisor de ρ.

Os resultados anteriores vão ser ainda aplicados neste §.

Lema 3:- O produto de duas álgebras de divisão, $\mathcal{A}$ e $\mathcal{B}$, de ordens m^2 e n^2, primas entre si, é uma nova álgebra de divisão, $\mathcal{L}$.

Ponhamos

$$\mathcal{L} = \mathcal{A}\times\mathcal{B} = \mathfrak{M}_r\times\mathfrak{D} \ ,$$

onde $\mathfrak{D}$ é álgebra de divisão e $\mathfrak{M}_r$ uma álgebra completa de matrizes de grau r. Tem-se

$$\mathcal{L}\times\mathcal{A}^{-1} = (\mathcal{A}\times\mathcal{A}^{-1})\times\mathcal{B} = \mathfrak{M}_r\times(\mathcal{A}^{-1}\times\mathfrak{D}) = \mathfrak{M}_r\times(\mathfrak{M}_s\times\mathcal{F}) \ ,$$

onde $\mathcal{F}$ é álgebra de divisão. Tendo também em conta que é $\mathcal{A}\times\mathcal{A}^{-1} = \mathfrak{M}_t$, a igualdade $\mathfrak{M}_t\times\mathcal{B} = \mathfrak{M}_r\times\mathcal{F}$ mostra que $\mathfrak{M}_t \cong \mathfrak{M}_{rs}$. Pelo facto de se ter $t = m^2_s$ o número r divide m^2. Demonstrava-se, de modo análogo, que r divide n^2. Será $r = 1$ e $\mathcal{L} = \mathfrak{D}$ = álgebra de divisão, como se afirmou.

Teorema 3:- Se o índice n duma álgebra de divisão $\mathfrak{D}$ (sobre) se decompõe sob a forma $n = p_1^{f_1}\dots p_s^{f_s}$, onde os p_t são números primos distintos, pode escrever-se $\mathfrak{D} = \mathfrak{D}_1\times\mathfrak{D}_2\times\dots\times\mathfrak{D}_s$, onde as álgebras de divisão $\mathfrak{D}_t$ (sobre $\mathfrak{P}$) têm os índices $p_t^{f_t}$ e são

determinadas, a menos de equivalências.(1) Seja ρ o expoente de $\mathfrak{D}$. Pelo teorema 2, ρ é divisível pelos números primos p. Por outro lado (teorema 1), n é múltiplo de ρ. Será, pois,

$$\rho = p_1^{g_1}\dots p_s^{g_s} \ , \qquad (0 \leq g_t \leq f_t) \ , \qquad (i = 1, 2, \dots, s).$$

No grupo abeliano das classes de álgebras centrais simples semelhantes sobre $\mathfrak{P}$ (ou grupo de Brauer), tem-se $\mathfrak{D}^\rho \in (\mathfrak{P})$. A ordem da classe $(\mathfrak{D})$ é ρ. Da teoria dos grupos finitos,(2) sabe-se que o elemento $(\mathfrak{D})$ se pode escrever, duma maneira única, como produto de elementos de ordens $p_1^{g_1}, \dots, p_s^{g_s}$, primas entre si. Pondo $(\mathfrak{D}) = (\mathfrak{D}_1)\dots(\mathfrak{D}_s)$, as classes $(\mathfrak{D}_t)^{p^{g_t}}$, a que pertencem as álgebras de divisão $\mathfrak{D}_t$, levam a $\mathfrak{D}_1\times\mathfrak{D}_2\times\dots\times\mathfrak{D}_s \in (\mathfrak{D})$. Os expoentes dos $\mathfrak{D}_t$ são os números p^{g_t}. O teorema 2 e o lema 3 dizem-nos que o produto directo anterior é uma álgebra de divisão. Podemos supor, portanto, $\mathfrak{D} = \mathfrak{D}_1\times\mathfrak{D}_2\times\dots\times\mathfrak{D}_s$. Se os índices dos $\mathfrak{D}_t$ são os números n_t, tem-se $n = n_1 n_2 \dots n_s = p_1^{f_1}\dots p_s^{f_s}$, com $n_t = p_t^{f_t}$. Para concluir a demonstração, tomemos uma outra decomposição de $\mathfrak{D}$: $\mathfrak{D} = \mathfrak{D}'_1\times\dots\times\mathfrak{D}'_s$, onde os $\mathfrak{D}'_t$ se supõem álgebras de divisão de índices $p_t^{f_t}$. Será, por ex., $\mathfrak{D}'_1 \in (\mathfrak{D}_1), \dots, \mathfrak{D}'_s \in (\mathfrak{D}_s)$, e, por consequência, $\mathfrak{D}'_1 \cong \mathfrak{D}_1, \dots, \mathfrak{D}'_s \cong \mathfrak{D}_s$, q. e. d.

Corolário:- Toda a álgebra primária tem um índice que é uma potência dum número primo. Vimos no Cap. IX que uma álgebra primária sobre $\mathfrak{P}$ ou era uma álgebra completa de matrizes $\mathfrak{P}_p$, com p primo, ou era uma álgebra de divisão. No 1º caso, o corolário está provado. Para o segundo, o teorema 3 acaba de nos garantir não ser possível haver mais do que um factor $p_1^{f_1}$ na decomposição de n. O corolário é válido.

7) Anéis normais - É possível estender a noção de produto cruzado e definir produtos cruzados com anéis normais, nos ter-

(1) Albert, pgs. 77.

(2) Veja-se Almeida Costa, "Elementos da Teoria dos Grupos", pgs. 49 a 53.

mos que vão ser expostos.(1)

Seja $\mathcal{T}$ um sistema hiper-complexo comutativo e semi-simples sobre $\mathcal{P}$, com a seguinte decomposição em corpos comutativos: $\mathcal{T} = \mathcal{L}_1 + \ldots + \mathcal{L}_r$. Suponhamos dado um grupo finito $\mathcal{G}$, de endomorfismos de $\mathcal{T}$ relativamente a $\mathcal{P}$. Por hipótese, pondo $\mathcal{G} = \{1, \rho, \sigma, \ldots, \tau\}$, significaremos que 1 representa o automorfismo idêntico. Como se trata dum grupo, os endomorfismos são necessàriamente automorfismos. Com efeito, se se tem

$$s \longrightarrow s^\rho = s' \; ; \qquad t \longrightarrow t^\rho = t' \; ,$$

não pode ser $s \neq t$, se for $s' = t'$, pois que, considerando o endomorfismo ρ^{-1}, viria

$$s'^{\rho^{-1}} = t'^{\rho^{-1}} = (t^\rho)^{\rho^{-1}} = t^{\rho^{-1}\rho} = t^1 = t \; ,$$

$$s'^{\rho^{-1}} = (s^\rho)^{\rho^{-1}} = s = t.$$

Por outro lado, todos os elementos de $\mathcal{T}$ são utilizados como imagens, o que se vê raciocinando assim: dado $\rho \in \mathcal{G}$, há sempre $t \in \mathcal{T}$ tal que $t^\rho = s$, qualquer que seja $s \in \mathcal{T}$. Basta por $t = s'$, com $s^{\rho^{-1}} = s'$, visto que

$$s'^\rho = (s^{\rho^{-1}}) = s^{\rho\rho^{-1}} = s.$$

Por via da aplicação de cada $\rho \in \mathcal{G}$ ao sistema $\mathcal{T}$, cada ideal de $\mathcal{T}$ se transforma num ideal de $\mathcal{T}$. Em particular, $\mathcal{L}_i$ transforma-se num ideal $\mathcal{L}_i'$, o qual, como soma de ideais $\mathcal{L}_i$, será igual a um $\mathcal{L}_i$. Podemos dizer, por isso, que o grupo $\mathcal{G}$ é um grupo de permutações do conjunto dos $\mathcal{L}_i$.

Teichmüller designa $\mathcal{T}$ por anel normal, se se verificam as duas propriedades seguintes:

P_1: - só o elemento $\sigma = 1$, de $\mathcal{G}$, deixa individualmente invariantes os elementos dum $\mathcal{L}_i$;

P_2: - apenas os elementos de $\mathcal{P} \subseteq \mathcal{T}$ ficam invariantes para todos os $\sigma \in \mathcal{P}$.

(1) Os raciocínios são devidos a O.Teichmüller, "Verschränkte Produkte mit Normalringen", Deutsche Mathematik, I Heft, 1936, pgs.92 a 102.

Com estas duas hipóteses, é possível estabelecer os dois teoremas a seguir, cuja demonstração, feita por uma via indirecta, deixamos para o próximo § 9.

Teorema I:- Num anel normal $\mathcal{T}$ (relativo a $\mathcal{G}$ e a $\mathcal{P}$) o grupo $\mathcal{G}$ é transitivo sobre o conjunto dos corpos $\mathcal{L}_i$ em que $\mathcal{T}$ pode decompor-se, de modo que estes corpos são necessàriamente isomorfos (relativamente a $\mathcal{P}$).

Teorema II:- A ordem $(\mathcal{T}/\mathcal{P})$ dum anel normal $\mathcal{T}$ (relativo a $\mathcal{G}$ e a $\mathcal{P}$) é igual à ordem do grupo finito $\mathcal{G}$.

São igualmente válidas estas outras proposições, cuja demonstração é também diferida para o § 9:

Teorema III:- Dado um sistema hiper-complexo comutativo semi-simples $\mathcal{T}$, sobre $\mathcal{P}$, se a propriedade P_1 e o teorema II têm lugar para $\mathcal{T}$, este sistema é um anel normal.

Teorema IV:- Um anel normal $\mathcal{T}$ (relativo a $\mathcal{G}$ e a $\mathcal{P}$) é soma de corpos normais separáveis (finitos) sobre corpos isomorfos de $\mathcal{P}$.

Teorema V:- Se $\mathcal{T}$ é normal (relativamente a $\mathcal{G}$ e a $\mathcal{P}$), é também normal (relativamente a $\mathcal{G}$ e a Ω) o anel $\mathcal{T}_\Omega$, onde $\Omega \supseteq \mathcal{P}$ é uma ampliação qualquer de $\mathcal{P}$.

Teorema VI:- Se $\mathcal{T}$ é normal relativamente a $\mathcal{G}$ e a $\mathcal{P}$, e $\mathcal{T}_1$ é normal relativamente a $\mathcal{G}_1$ e a $\mathcal{P}$, o produto directo $\mathcal{T} \times \mathcal{T}_1$ é normal relativamente ao produto directo $\mathcal{G} \times \mathcal{G}_1$ e ao corpo $\mathcal{P}$.

8) Produtos cruzados com anéis normais - Retomemos as considerações do § 1 deste Capítulo, substituindo, porém, a ampliação finita, normal e separável $\mathcal{K}$, de $\mathcal{P}$, de grau n, pelo anel normal $\mathcal{T}$, de ordem n, sobre $\mathcal{P}$, definido no § anterior. Por N designamos a ordem do grupo dado $\mathcal{G}$, de automorfismos de $\mathcal{T}$ relativamente a $\mathcal{P}$. Aqui, o grupo $\mathcal{G}$ tem de ser prèviamente fixado, de modo um tanto

arbitrário, contràriamente ao que sucedia no referido § 1, no qual o grupo $\mathcal{G}$ era necessàriamente o grupo dos automorfismos de $\mathcal{A}$ (relativamente a $\mathcal{P}$). Por $u_1, u_\rho, \ldots, u_\tau$ designaremos ainda N símbolos base dum módulo esquerdo relativo a $\mathcal{Y}$, para o qual o elemento $u \in \mathcal{Y}$ é operador unitário. Poremos

$$\mathcal{U} = \sum_\sigma \mathcal{Y} u_\sigma , \qquad (\sigma \in \mathcal{G}) .$$

Introduzindo as relações (1) de definição dum produto em $\mathcal{U}$, suporemos, bem entendido, que os elementos $a_{\rho,\sigma} \in \mathcal{Y}$ são elementos regulares. As relações (2), (3) e (4) serão válidas. O módulo $\mathcal{U}$ torna-se num anel de ordem Nn relativamente a $\mathcal{P}$: $((\mathcal{U}/\mathcal{P}) = (\mathcal{U}/\mathcal{Y})(\mathcal{Y}/\mathcal{P}) = Nn$. Em $\mathcal{U}$ existe elemento um e as igualdades (5) têm lugar:

$$U = a_{1,1}^{-1} u_1 , \qquad u_\rho \beta = \beta^\rho u_\rho , \qquad (\beta \in \mathcal{Y}) .$$

O sistema $\mathcal{Y}$ está contido em $\mathcal{U}$, sendo $\mathcal{U} \supseteq \mathcal{Y} \supseteq \mathcal{P}$. $\mathcal{U}$ é álgebra sobre $\mathcal{P}$.

Procuremos agora o centro de $\mathcal{U}$. Se $w = \sum \alpha_\sigma u_\sigma$, $(\alpha_\sigma \in \mathcal{Y})$, pertence ao centro, deverá ter-se

$$w\,\beta = \beta w , \qquad \sum_\sigma \alpha_\sigma \beta^\sigma u_\sigma = \sum_\sigma \beta\, \alpha_\sigma u_\sigma ,$$

qualquer que seja $\beta \in \mathcal{Y}$. Valerá, por consequência, $\alpha_\sigma (\beta^\sigma - \beta) = 0$, para todo o $\beta \in \mathcal{Y}$. A fim de que, como no § 1, possamos concluir ser $\sigma = 1$, no caso de ser $\alpha_\sigma \neq 0$, precisamos introduzir precisamente a propriedade P_1. A este respeito, vamos demonstrar o seguinte

Teorema 1:- Se um grupo finito $\mathcal{G}$, de automorfismos do sistema hiper-complexo comutativo semi-simples $\mathcal{Y}$, sobre $\mathcal{P}$, verifica a propriedade P_1, tem lugar esta outra propriedade P_1': Dados $\alpha \in \mathcal{Y}$ fixo, e fixado também $\sigma \in \mathcal{G}$, a igualdade $\alpha(\beta^\sigma - \beta) = 0$, suposta válida para qualquer $\beta \in \mathcal{Y}$, implica $\sigma = 1$, salvo se for $\alpha = 0$. Inversamente, a propriedade P_1' arrasta P_1. Eis aqui a demonstração de Teichmüller. Suponhamos que à decomposição de $\mathcal{Y}$ nos corpos $\mathcal{L}_l$ corresponde a seguinte decomposição de $U = u \in \mathcal{P}$, $\mathcal{Y}$, $\mathcal{U}$ em idempotentes ortogonais: $u = e_1 + \cdots + e_r$. Se P_1 é válida, admitamos que se tem, com α e σ fixos e β qualquer,

$$\alpha(\beta^\sigma - \beta) = 0 , \qquad \alpha \neq 0 .$$

Será igualmente

$$e_l\, \alpha (\beta_l^\sigma - \beta_l) = 0 , \qquad (\beta_l \in \mathcal{L}_l) .$$

Visto que $\alpha \neq 0$, não podem ser nulos todos os $e_l \alpha$. Suponhamos, pois, $e_l \alpha \neq 0$, na igualdade anterior. Como $e_l \alpha \in \mathcal{L}_l$ e este é um corpo, será, necessàriamente, $\beta_l^\sigma = \beta_l$. Ora, pela propriedade P_1, isto significa $\sigma = 1$. Assim, P_1' é válida. Inversamente, se P_1' é válida, imaginemos que σ deixa invariantes os elementos de $\mathcal{L}_l$. Será, para qualquer $\beta \in \mathcal{Y}$, $e_l \beta \in \mathcal{L}_l$, e, portanto,

$$e_l \left((e_l \beta)^\sigma - e_l \beta \right) = e_l (\beta^\sigma - \beta) = 0 ,$$

pois que $e_l^\sigma = e_l$. Mas, então, pela propriedade P_1', ter-se-á $\sigma = 1$, visto que $e_l \neq 0$. Logo, P_1 é válida.

A propriedade P_1 encontra-se, deste modo, para garantir que o centro $\mathcal{Z}$, de $\mathcal{U}$, tal como no § 1, é composto de elementos $w = \alpha u_1 = \tau U \in \mathcal{Y}$. Vamos ver que a propriedade P_2 vai garantir que o referido centro se compõe dos elementos de $\mathcal{P}$ e apenas desses elementos. Devendo ter-se, para $z \in \mathcal{Z}$,

$$z\, u_\sigma = u_\sigma z = z^\sigma\, u_\sigma , \qquad (z \in \mathcal{Y}) ,$$

conclui-se $z^\sigma = z$, qualquer que seja σ. Se P_2 tem lugar, será $z \in \mathcal{P}$. Podemos provar este

Teorema 2:- Se $\mathcal{Y}$ é anel normal, a álgebra central $\mathcal{U} = (\mathcal{Y}/\mathcal{P}, \overline{\mathcal{G}}, a_{\rho,\sigma})$ é álgebra central simples. Basta demonstrar que $\mathcal{U}$ é álgebra semi-simples. Ora, tem lugar o seguinte

Lema:- Se $\mathcal{Y}$ é um sistema hiper-complexo comutativo semi-simples, sobre $\mathcal{P}$, gozando da propriedade P_1, a álgebra $\mathcal{U}$ (não necessàriamente central) é semi-simples. Vamos ver que, na verdade, $\mathcal{U}$ não tem ideal bilateral nilpotente. Se $\mathfrak{a} \neq (0)$ é um ideal bilateral de $\mathcal{U}$ e se $a = \Sigma \alpha_\sigma u_\sigma$ é um elemento não nulo de $\mathfrak{a}$, a intersecção $\mathfrak{a} \cap \mathcal{Y} = \mathfrak{a}'$ é um ideal não nulo de $\mathcal{Y}$, pelas razões a seguir. Em primeiro lugar

$$\mathfrak{a}'\,\mathfrak{T} = (\mathfrak{a}\cap\mathfrak{T})\,\mathfrak{T} \subseteq \mathfrak{a}\,\mathfrak{T}\cap\mathfrak{T}\mathfrak{T} = \mathfrak{a}\cap\mathfrak{T} = \mathfrak{a}'.$$

Em seguida, suponhamos que, na expressão de $a \neq 0$, se faz figurar o número mínimo de parcelas $\alpha_\sigma u_\sigma$, de modo que, por ex., $\alpha_\sigma \neq 0$. Tem-se

$$b = a\cdot u_{\sigma^{-1}} = \sum \alpha_\rho u_\rho \cdot u_{\sigma^{-1}} = \alpha_\sigma\, a_{\sigma,\sigma^{-1}}\, u_1 + \cdots = \beta u_1 + \cdots \in \mathfrak{a}.$$

Como é $\beta \neq 0$, o elemento

$$\xi b - b\xi = (\xi\beta - \beta\xi)u_1 + \cdots \in \mathfrak{a}, \qquad (\xi \in \mathfrak{T}),$$

é um elemento de $\mathfrak{a}$ com uma expressão em que figuram menos parcelas do que em a, visto se ter $\xi\beta - \beta\xi = 0$. Deverá ter-se também $\xi b - b\xi = 0$, qualquer que seja ξ. Isto significa $b \in \mathfrak{T}$, e, portanto, $b \in \mathfrak{a}'$. Como é $b \neq 0$, fica demonstrada a afirmação feita quanto ao ideal $\mathfrak{a}'$. Se, agora, existisse $\mathfrak{a} \neq (0)$, com $\mathfrak{a}^\lambda = (0)$, ter-se-ia igualmente $\mathfrak{a}' \neq (0)$, com $\mathfrak{a}'^\lambda = (0)$. Este resultado é absurdo, pois $\mathfrak{T}$ é semi-simples. O lema está provado. Com o lema, está provado o teorema.

A álgebra central simples $\mathcal{U}$, que acabamos de definir, diz-se <u>um produto cruzado com o anel normal $\mathfrak{T}$</u>.

9) <u>Os teoremas sobre anéis normais</u> - A demonstração do teorema I do § 7 exige algumas proposições preliminares, de resto utilizadas também no teorema III. Em seguida, no teorema IV, são utilizados os resultados expressos nos teoremas I e III. Comecemos pelo seguinte

<u>Lema 1:- Se $\mathfrak{T}$ é um sistema hiper-complexo comutativo semi-simples, sobre $\mathcal{P}$, com a propriedade P_1, há uma correspondência biunívoca completa entre os ideais bilaterais $\mathfrak{a}$, da álgebra semi-simples (não central) $\mathcal{U}$, e os ideais de $\mathfrak{T}$ que são globalmente conservados por todos os automorfismos $\sigma \in \mathcal{G}$.</u> Dado $\mathfrak{a}$, passemos a $\mathfrak{a}\cap\mathfrak{T} = \mathfrak{a}'$. Sabemos existir um idempotente $e \in \mathfrak{z} \subseteq \mathfrak{T}$, tal que $\mathfrak{a} = e\mathcal{U}$, e $\mathfrak{T} \subseteq \mathfrak{a}'$. Para tirar a igualdade desta última inclusão, tomemos $a' \in \mathfrak{a}'$ e escrevamos $a' = ea$, $(a \in \mathfrak{a})$. Ter-se-á $ea' = ea = a'$, pelo que $a' \in e\mathfrak{T}$. Assim, é, de facto, $\mathfrak{a}' = e\mathfrak{T}$.

Inversamente, tomemos um idempotente $e \in \mathfrak{T}$. Ele gera um ideal $e\mathfrak{T} = \mathfrak{a}'$ e um ideal direito $\mathfrak{K} = e\mathcal{U}$, de $\mathcal{U}$. A intersecção $\mathfrak{K}\cap\mathfrak{T}$ é igual a $\mathfrak{a}'$, como se vê imediatamente. Para verificar em que casos é $\mathfrak{K}$ um ideal bilateral, procede-se como vai indicar-se. Dado $\mathfrak{a}$, tem-se $\mathfrak{a} = u_\sigma\cdot u_\sigma^{-1}\mathfrak{a}\, u_\sigma\cdot u_\sigma^{-1} \subseteq u_\sigma\mathfrak{a}\, u_\sigma^{-1}$, e, portanto, $\mathfrak{a} = u_\sigma\mathfrak{a}\, u_\sigma^{-1}$; considerado $\mathfrak{T}$, pelo facto de ser, para $\beta \in \mathfrak{T}$, $u_\sigma\beta u_\sigma^{-1} = \beta^\sigma$, é $u_\sigma\mathfrak{T}u_\sigma^{-1} \subseteq \mathfrak{T}$; mas é também (pondo $u_\sigma^{-1} = \xi u_{\sigma^{-1}}$)

$$u_\sigma^{-1}\beta u_\sigma = \xi\, u_{\sigma^{-1}}\beta u_\sigma = \xi\,\beta^{\sigma^{-1}} a_{\sigma^{-1},\sigma}\, u_1 \in \mathfrak{T},$$

de sorte que $u_\sigma^{-1}\mathfrak{T}u_\sigma \subseteq \mathfrak{T}$, $\mathfrak{T} \subseteq u_\sigma\mathfrak{T}u_\sigma^{-1}$, $\mathfrak{T} = u_\sigma\mathfrak{T}u_\sigma^{-1}$. Em seguida, verificam-se as relações $u_\sigma\mathfrak{a}'u_\sigma^{-1} = u_\sigma\cdot\mathfrak{a}\cap\mathfrak{T}\cdot u_\sigma^{-1} = \mathfrak{a}'$, ou $\mathfrak{a}'^\sigma = \mathfrak{a}'$. Pode afirmar-se, pois, que os ideais bilaterais de $\mathcal{U}$ determinam univocamente ideais $\mathfrak{a}'$, de $\mathfrak{T}$, que ficam globalmente conservados pelos automorfismos $\sigma \in \mathcal{G}$. Inversamente, vamos mostrar que o ideal $\mathfrak{K}$, gerado pelo idempotente $e \in \mathfrak{a}' = \mathfrak{a}'^\sigma$ é um ideal bilateral $\mathfrak{a}$. De facto,

$$\mathfrak{K} = e\mathcal{U} = e\mathfrak{T}\mathcal{U} = \mathfrak{a}'\mathcal{U} = \mathfrak{a}'\cdot\sum_\sigma \mathfrak{T}\, u_\sigma = \sum_\sigma \mathfrak{a}'\, u_\sigma,$$

$$\mathcal{U}\mathfrak{K} = \sum_\sigma \mathcal{U}\mathfrak{a}'\, u_\sigma \subseteq \sum_\sigma \mathfrak{a}'\, u_\sigma = \mathfrak{K},$$

pois que um elemento de $\mathcal{U}\mathfrak{a}'\, u_\sigma$ é soma de elementos da forma

$$(\alpha_\rho u_\rho + \cdots)a' u_\sigma = \alpha_\rho\, a'^\rho\, a_{\rho,\sigma} u_{\rho\sigma} + \cdots = b'_\rho\, u_\rho + b'_\sigma\, u_\sigma + \cdots,$$

onde $b'_\rho, b'_\sigma, \ldots \in \mathfrak{a}'$, por virtude de ser $a'^\rho, \ldots \in \mathfrak{a}'$. Além do lema 1, tem lugar este outro

<u>Lema 2:- Se o sistema $\mathfrak{T}$, referido no lema 1, além de possuir a propriedade P_1, é tal que os corpos $\mathcal{L}_i$ da sua decomposição são todos isomorfos relativamente a $\mathcal{P}$ (isto é, se $\mathcal{G}$ é transitivo sobre o conjunto dos $\mathcal{L}_i$), então a álgebra semi-simples (não central) $\mathcal{U}$ é uma álgebra simples sobre $\mathcal{P}$.</u> Na verdade, admitamos apenas P_1. Pode sempre escrever-se

$$\mathfrak{T} = \mathcal{L}_1 + \cdots + \mathcal{L}_r = S_1 + \cdots + S_t, \qquad (t \leq r),$$

onde cada S_i representa a soma de todos os $\mathcal{L}_j$ que resultam dum dado $\mathcal{L}$ por meio de todos os automorfismos $\sigma \in \mathcal{G}$: se, por ex.,

$\mathcal{L}_2 = \mathcal{L}_1^{\rho}$, $\mathcal{L}_3 = \mathcal{L}_1^{\sigma}$, tem-se $\mathcal{L}_3 = (\mathcal{L}_2^{\rho^{-1}})^{\sigma} = \mathcal{L}_2^{\sigma\rho^{-1}} = \mathcal{L}_2^{\tau}$.

Dado um $\mathfrak{a}^1$ para o qual $\mathfrak{a}^{1\sigma} = \mathfrak{a}^1$, qualquer que seja σ, podemos afirmar que $\mathfrak{a}^1$ é soma directa dum certo número de SS. Os ideais bilaterais de $\mathcal{A}$ são necessàriamente da forma

$$\mathfrak{a} = \sum_{\sigma} S_k u_{\sigma} + \sum_{\sigma} S_l u_{\sigma} + \dots, \quad (k, l, \dots \text{ determinados}), \quad \dots \quad (24)$$

e uma expressão como a do 2º membro representa um ideal bilateral $\mathfrak{a}$. É claro, com efeito, que esse 2º membro é uma soma directa: se, por ex., se tivesse $\alpha_k u_{\sigma} + \alpha_{\rho} u_{\sigma} = 0$, com $\alpha_k \in S_k$, $\alpha_l \in S_l$, seria $\alpha_k + \alpha_l = 0$, e, portanto, $\alpha_k = \alpha_l = 0$, ou seja $\alpha_k u_{\sigma} + \alpha_l u_{\sigma} = 0$. Pondo

$$\mathfrak{a}_k = \sum_{\sigma} S_k u_{\sigma},$$

$\mathfrak{a}_k$ é um ideal bilateral de $\mathcal{A}$, e pode concluir-se que os ideais simples de $\mathcal{A}$ têm de ser da forma $\mathfrak{a}_k$. Inversamente, $\mathfrak{a}_k$ é simples, pois todo o ideal de $\mathcal{A}$ contém, pelo menos, uma parcela completa de (24).

O teorema I resulta agora imediatamente. O produto cruzado $\mathcal{A}$ é álgebra simples. Não pode $\mathcal{T}$ decompor-se numa soma de vários SS, visto que, de contrário, haveria em $\mathcal{A}$ ideais bilaterais simples, distintos e não nulos.

Passemos ao teorema II. Para isso, consideremos a álgebra central simples $\mathcal{A} = (\mathcal{T}/\mathcal{P}, \mathcal{G}, u)$, na qual os $a_{\rho,\sigma}$ são todos iguais ao elemento um de $\mathcal{T}$ (ou de $\mathcal{P}$). $\mathcal{A}$ é ainda, como no § 2, um anel completo de matrizes com elementos de $\mathcal{P}$. A demonstração pode conduzir-se do modo seguinte, aplicável aos produtos cruzados vulgares [Veja-se o teorema 4 do § 2]. Tomemos o elemento $w = u_1 + \dots + u_{\tau} \in \mathcal{A}$ e estudemos o conjunto $\mathcal{T}w \subseteq \mathcal{A}$. Em virtude de ser $u_{\sigma} w = w$, qualquer que seja σ, vê-se que $\mathcal{A}\mathcal{T}w \subseteq \mathcal{T}w$, de modo que $\mathcal{T}w$ é ideal esquerdo de $\mathcal{A}$. Vamos provar que é ideal mínimo. Estudemos o anel dos seus endomorfismos (relativos a $\mathcal{A}$). Se E é um endomorfismo, tem-se

$$w \longrightarrow Ew, \qquad u_{\sigma} w = w \longrightarrow E \cdot u_{\sigma} w = Ew = u_{\sigma} \cdot Ew,$$

pelo que, pondo $Ew = \alpha w$ $(\alpha \in \mathcal{T})$, se conclui

$$u_{\sigma} \cdot \alpha w = \alpha^{\sigma} u_{\sigma} w = \alpha^{\sigma} w = \alpha w, \qquad \alpha^{\sigma} = \alpha,$$

qualquer que seja σ. Será $\alpha \in \mathcal{P}$. Inversamente, a correspondência

$$w \longrightarrow \pi w, \qquad (\pi \in \mathcal{P}),$$

define um endomorfismo de $\mathcal{T}w$ relativo a $\mathcal{A}$:

$$aw \longrightarrow \pi \cdot aw = a \cdot \pi w, \qquad (a \in \mathcal{A}).$$

Elementos diferentes de $\mathcal{P}$ definem endomorfismos diferentes. Os endomorfismos são automorfismos e o anel correspondente é um corpo. Não pode o ideal $\mathcal{T}w$ ser uma soma de ideais esquerdos mínimos de $\mathcal{A}$, pois que, se assim fosse, o anel dos endomorfismos seria um anel completo de matrizes de grau superior ao primeiro (pgs. 229). Ora sabemos que $\mathcal{A}$ é um anel completo de matrizes com elementos dum corpo isomorfo do corpo dos endomorfismos de $\mathcal{T}w$, portanto: $\mathcal{A} \cong \mathcal{R}$. O número λ representa o número de ideais esquerdos mínimos em que se decompõe $\mathcal{A}$ ou a ordem de cada ideal esquerdo mínimo relativamento ao seu corpo de automorfismos. Essa ordem é aqui $(\mathcal{T}w/\mathcal{P}) = (\mathcal{T}/\mathcal{P}) = n$. Assim, como se afirmou,

$$(\mathcal{A}/\mathcal{P}) = \lambda^2 = n^2 = Nn, \qquad N = \text{ordem de } \mathcal{G} = n = (\mathcal{T}/\mathcal{P}).$$

A demonstração do teorema III é feita como segue por Teichmüller. Comecemos por decompor $\mathcal{T}$ nos $\mathcal{L}_j$ e destacar nestes todos os corpos que resultam dum dado $\mathcal{L}_l$ pela aplicação das operações $\sigma \in \mathcal{G}$. A soma directa desses corpos levará a $S \subseteq \mathcal{T}$. O sistema S verifica a propriedade P_1. A custa de S, construamos uma álgebra (não central, em princípio) $\mathcal{A}'$, como se sabe. O centro $\mathcal{Z}'$, de $\mathcal{A}'$, está contido em S. O lema 2 garante-nos que $\mathcal{A}'$ é uma álgebra simples sobre $\mathcal{P}$. Então, o centro $\mathcal{Z}'$ será um corpo $\subseteq$ S. Qualquer que seja $z' \in \mathcal{Z}'$, é $z'^{\sigma} = z'$, como resulta de se ter $z' u_{\sigma} = u_{\sigma} z' = z'^{\sigma} u_{\sigma}$. Considerando S como sistema hiper-complexo comutativo semi-simples sobre $\mathcal{Z}'$, S será anel normal relativamente a $\mathcal{G}$ e a $\mathcal{Z}'$. O teorema II será válido para $\mathcal{A}'$, como álgebra central simples sobre $\mathcal{Z}'$, podendo escrever-se

$$N = (S/\mathcal{Z}') \leqq (\mathcal{T}/\mathcal{Z}') \leqq (\mathcal{T}/\mathcal{P}) = n.$$

A igualdade N = n implicará, pois, $S = \mathcal{T}$, $\mathcal{Z}' = \mathcal{P}$, pelo que $\mathcal{T}$ é anel normal sobre $\mathcal{P}$.

Demonstremos o teorema IV. Já sabemos que $\mathcal{T}$ é uma soma de corpos isomorfos $\mathcal{L}_i$ (relativamente a $\mathcal{P}$). O corpo $\mathcal{L}_1$, por ex., é um sistema hiper-complexo sobre $\mathcal{P}$. Se considerarmos o sub-grupo $\mathcal{H}$, de $\mathcal{G}$, cujas permutações deixam globalmente fixo $\mathcal{L}_1$ ($\mathcal{L}_1^{\sigma} = \mathcal{L}_1$, se $\sigma \in \mathcal{H}$); vê-se que o sistema $\mathcal{L}_1$ verifica a propriedade P_1 relativamente a $\mathcal{H}$. A transitividade do grupo $\mathcal{G}$ sobre o conjunto dos $\mathcal{L}_i$ leva a estabelecer uma correspondência biunívoca entre os corpos $\mathcal{L}_i$ e as classes associadas de $\mathcal{G}$ com respeito a $\mathcal{H}$[1]. Será, pois,

$$\text{índice de } \mathcal{H} = r = \frac{N}{\text{ordem de } \mathcal{H}}, \quad \text{ordem de } \mathcal{H} = \frac{N}{r} = \frac{n}{r},$$

visto que $N = n$. Ora é também

$$(\mathcal{T}/\mathcal{P}) = n = r.(\mathcal{L}_1/\mathcal{P}), \qquad (\mathcal{L}_1/\mathcal{P}) = \frac{n}{r} = \text{ordem de } \mathcal{H}.$$

Daqui se conclui que $\mathcal{L}_1$ goza da propriedade expressa no teorema II. Assim, $\mathcal{L}_1$ é anel normal relativo a $\mathcal{H}$ e a $\mathcal{P}$. Mas, se a ordem do corpo $\mathcal{L}_1$ (sobre $\mathcal{P}e_1$) é igual a um certo número de automorfismos de $\mathcal{L}_1$ (relativamente a $\mathcal{P}e_1$), o corpo $\mathcal{L}_1$ é necessàriamente uma ampliação separável e normal (além de finita) de $\mathcal{P}e_1$. É a afirmação do teorema IV. Este resultado justifica a designação de anel normal dada ao sistema $\mathcal{T}$.

Quanto a V, comecemos por observar que um automorfismo $\sigma \in \mathcal{G}$ se pode estender para um automorfismo de $\mathcal{T}_\Omega$ (relativamente a Ω), pelo facto de se poder tomar para base de $\mathcal{T}_\Omega$ uma base de $\mathcal{T}$. Então, para $\mathcal{T}_\Omega$ é válido o teorema II, pois que $(\mathcal{T}_\Omega/\Omega) = (\mathcal{T}/\mathcal{P}) =$ = ordem de $\mathcal{G}$. Conforme a afirmação do teorema III, basta verificar a propriedade P_1 em $\mathcal{T}_\Omega$. Para isso, verificaremos a propriedade equivalente P_1'. Suponhamos

$$\alpha(\beta^{\sigma} - \beta) = 0, \qquad (\alpha, \beta \in \mathcal{T}_\Omega;\ \sigma \text{ fixo}), \tag{25}$$

(1) Veja-se Almeida Costa, "Elementos da Teoria dos Grupos", pgs. 121 e 122.

com β qualquer. Se $v_1, v_2, \ldots, v_n$ for uma base de $\mathcal{T}$ (sobre $\mathcal{P}$), escrevamos

$$\alpha = \omega_1 v_1 + \cdots + \omega_n v_n, \qquad \beta = x_1 v_1 + \cdots + x_n v_n, \qquad (\omega_i, x_j \in \Omega).$$

De (25), tira-se

$$\sum_i \omega_i v_i \Big[\sum_j x_j (v_j^{\sigma} - v_j)\Big] = \sum_{i,j} \omega_i x_j . v_i (v_j^{\sigma} - v_j) = 0 . \tag{26}$$

Se pusermos

$$v_i (v_j^{\sigma} - v_j) = \sum_\ell p_{ij\ell}^{(\sigma)} v_\ell , \qquad (p_{ij\ell}^{(\sigma)} \in \mathcal{P}),$$

a relação (26) dá

$$\sum_{i,j,\ell} \omega_i p_{ij\ell}^{(\sigma)} x_j v_\ell = \sum_\ell \Big(\sum_{i,j} p_{ij\ell}^{(\sigma)}\ \omega_i x_j\Big) v_\ell = 0 .$$

Por consequência, se (25) é válido, tem-se

$$\sum_{i,j} p_{ij\ell}^{(\sigma)}\ \omega_i x_j = \sum_j \Big(\sum_i p_{ij\ell}^{(\sigma)}\ \omega_i\Big) x_j = 0 , \qquad \sum_i p_{ij\ell}^{(\sigma)}\ \omega_i = 0.$$

Imaginemos $\sigma \neq 1$. O sistema

$$\sum_i p_{ij\ell}^{(\sigma)} z_i = 0 , \qquad (i = 1, 2, \ldots, n\ ;\ j = 1, 2, \ldots, n),$$

no qual ℓ e σ são fixos, tem coeficientes em $\mathcal{P}$. Como a propriedade P_1' é válida em $\mathcal{T}$, será $z_i = 0$. Considerando o sistema como tendo coeficientes em Ω (tomo I, pgs. 79), os ω_i serão nulos, e ter-se-á $\alpha = 0$. Assim, em (25), se $\alpha \neq 0$, deverá ter-se $\sigma = 1$. $\mathcal{T}_\Omega$ é um anel normal relativo a $\mathcal{G}$ e a Ω.

Finalmente, trataremos VI. Dado o produto directo $\mathcal{T} \times \mathcal{T}_1$, constroi-se o produto $\mathcal{G} \times \mathcal{G}_1$ de automorfismos (relativamente a $\mathcal{P}$), pondo, para cada elemento $\alpha\alpha_1$ ($\alpha \in \mathcal{T}, \alpha_1 \in \mathcal{T}_1$),

$$(\alpha\alpha_1)^{\sigma\sigma_1} = \alpha^{\sigma}\alpha_1^{\sigma_1} , \qquad (\sigma \in \mathcal{G},\ \sigma_1 \in \mathcal{G}_1).$$

Em particular, será

$$\alpha^{\sigma\sigma_1} = \alpha^{\sigma} , \qquad \alpha_1^{\sigma\sigma_1} = \alpha_1^{\sigma_1} .$$

Também aqui se tem

$$(\mathcal{T}\times\mathcal{T}_1/\mathcal{P}) = (\mathcal{T}/\mathcal{P})\cdot(\mathcal{T}_1/\mathcal{P}) = \text{ordem de } \mathcal{G}\times\mathcal{G}_1 .$$

Quanto à propriedade P_1', raciocinemos de modo análogo ao que se fez para o teorema anterior. Suponhamos

$$\xi(\eta^{\sigma\sigma_1} - \eta) = 0 , \qquad (\xi, \eta \in \mathcal{T}\times\mathcal{T}_1;\ \sigma \text{ e } \sigma_1 \text{ fixos}) , \qquad (27)$$

com η qualquer. No caso de se ter $\sigma = 1$, $\sigma_1 = 1$, a igualdade anterior é válida com $\xi \neq 0$. Não sendo assim, admitamos que é $\sigma \neq 1$. A relação (27), quando se toma $\eta \in \mathcal{T} = \mathcal{P}(v_1, \dots, v_n)$ e se põe

$$\eta = x_1 v_1 + \dots + x_n v_n , \qquad \xi = t_1 v_1 + \dots + t_n v_n ,$$

($x_i \in \mathcal{P}$; $t_l \in \mathcal{T}$), dá, sucessivamente:

$$\sum_l t_l v_l \Big[\sum_j x_j (v_j^{\sigma} - v_j)\Big] = \sum_{l,j} t_l x_j \cdot v_l (v_j^{\sigma} - v_j) =$$
$$= \sum_{l,j,\ell} t_l x_j p_{lj\ell}^{(\sigma)} \ v_\ell = \sum_\ell \Big(\sum_{l,j} p_{lj\ell}^{(\sigma)} \ x_j t_l\Big) v_\ell = 0 .$$

Por consequência, se (27) é válida, tem-se

$$\sum_{l,j} p_{lj\ell}^{(\sigma)} x_j t_l = \sum_l \Big(\sum_j p_{lj\ell}^{(\sigma)} x_j\Big) t_l = 0. \qquad (28)$$

Se fizermos

$$t_l = \sum_R \pi_{lR} w_R , \qquad (\pi_{lR} \in \mathcal{P};\ w_1, w_2, \dots = \text{base de } \mathcal{T}_1 \text{ sobre } \mathcal{P}),$$

(28) leva a

$$\sum_{l,R} \Big(\sum_j p_{lj\ell}^{(\sigma)} x_j\Big) \ \pi_{lR} w_R = \sum_R \Big(\sum_{l,j} p_{lj\ell}^{(\sigma)} \ \pi_{lR} x_j\Big) w_R = 0 ,$$

e, portanto, a

$$\sum_{l,j} p_{lj\ell}^{(\sigma)} \ \pi_{lR} x_j = \sum_j \Big(\sum_l p_{lj\ell}^{(\sigma)} \ \pi_{lR}\Big) x_j = 0.$$

A arbitrariedade dos x_j leva a

$$\sum_l p_{lj\ell}^{(\sigma)} \pi_{lR} = 0 , \qquad \begin{cases} j = 1, 2, \dots, n , \\ \ell \text{ e } k \text{ fixos} . \end{cases}$$

Viu-se já que estas últimas igualdades, se $\sigma \neq 1$, implicam $\pi_{lR} = 0$, ($i = 1, 2, \dots, n$; $k = 1, 2, \dots, n_1$), com n_1 = ordem de $\mathcal{T}_1$. Então os t_l serão nulos e $\xi = 0$, como se quer.

10) Alguns teoremas sobre produtos cruzados com anéis normais. No § anterior (teorema IV), vimos que existe um produto cruzado vulgar formado à custa da ampliação finita, normal e separável, $\mathcal{L}_1$, de $\mathcal{P}$ e e_i. Vamos demonstrar o seguinte

Teorema 1:- Dados o anel normal $\mathcal{T}$ e o produto cruzado correspondente $\mathcal{A} = (\mathcal{T}/\mathcal{P}, \mathcal{G}, a_{\rho,\sigma})$, o produto cruzado vulgar $P = (\mathcal{L}_1/\mathcal{P}e_1, \mathcal{G}_\mathcal{G}, e_1 a_{\rho,\sigma})$ é semelhante àquele. Neste enunciado deve pressupor-se, é claro, que, depois da construção do produto P, o corpo $\mathcal{P}e_1$ se substituiu pelo corpo isomorfo $\mathcal{P}$. Por outro lado, na construção de P, os automorfismos $\rho, \sigma, \dots$, a considerar, são apenas os que pertencem ao sub-grupo $\mathcal{G}_\mathcal{G} \subseteq \mathcal{G}$, que conserva $\mathcal{L}_1$. O idempotente e_1 pertence a $\mathcal{A}$, e a álgebra simples sobre $\mathcal{P}$, $e_1\mathcal{A}\,e_1$, é semelhante a $\mathcal{A}$ (§ 3). O teorema prova-se mostrando a semelhança $e_1\mathcal{A}\,e_1 \approx P$. Ora tem-se

$$e_1\mathcal{A}\,e_1 = \sum_\sigma e_1 \mathcal{T} u_\sigma e_1 = \sum_\sigma \mathcal{L}_1 u_\sigma e_1 .$$

Como é $u_\sigma e_1 u_\sigma^{-1} = e_1^\sigma$, podemos escrever $u_\sigma e_1 = e_1^\sigma u_\sigma$, e, portanto,

$$e_1\mathcal{A}\,e_1 = \sum_{\sigma\in\mathcal{G}_\mathcal{G}} \mathcal{L}_1 e_1^\sigma u_\sigma = \sum_{\sigma\in\mathcal{G}_\mathcal{G}} \mathcal{L}_1 e_1 u_\sigma , \qquad (29)$$

visto que, se $\sigma \in \mathcal{G}_\mathcal{G}$, vale $e_1^\sigma = e_1$, e, se $\sigma \notin \mathcal{G}_\mathcal{G}$, também $e_1^\sigma \notin \mathcal{L}_1$, e vale $\mathcal{L}_1 e_1^\sigma = 0$. Em (29), os elementos $e_1 u_\sigma$ são independentes em face de $\mathcal{L}_1$, e as regras de multiplicação, válidas em $e_1\mathcal{A}\,e_1$,

$$e_1 u_\rho \cdot e_1 u_\sigma = e_1 u_\rho e_1 \cdot u_\sigma = e_1 e_1^\rho \ u_\rho u_\sigma = e_1 a_{\rho,\sigma} u_{\rho\sigma} = e_1 a_{\rho,\sigma} \cdot e_1 u_{\rho\sigma} ,$$

($\rho, \sigma \in \mathcal{G}_\mathcal{G}$), mostram que a álgebra $e_1\mathcal{A}\,e_1$ se pode considerar precisamente igual ao produto cruzado P.

Teorema 2:- Se Ω é uma ampliação qualquer de $\mathcal{P}$, a álgebra central ampliada (sobre Ω), $\mathcal{A}_\Omega = (\mathcal{T}/\mathcal{P}, \mathcal{G}, a_{\rho,\sigma})_\Omega$, é isomorfa (relativamente a Ω) da álgebra $(\mathcal{T}_\Omega/\Omega, \mathcal{G}, a_{\rho,\sigma})$. Este último símbolo, visto que $\mathcal{T}_\Omega$ é anel normal (teorema V sobre anéis normais), representa um produto cruzado. Quanto a $\mathcal{A}_\Omega$, tem-se, supondo $S_1, \ldots, S_n$ uma base de $\mathcal{T}$ com respeito a $\mathcal{P}$:

$$\mathcal{A} = \sum_\sigma \mathcal{T} u_\sigma = \sum_\sigma \mathcal{P} S_1 u_\sigma + \ldots + \sum_\sigma \mathcal{P} S_n u_\sigma ,$$

$$\mathcal{A}_\Omega = \sum_\sigma \Omega S_1 u_\sigma + \ldots + \sum_\sigma \Omega S_n u_\sigma = \sum_\sigma (\Omega S_1 + \ldots + \Omega S_n) u_\sigma = \sum_\sigma \mathcal{T}_\Omega u_\sigma .$$

Em $\mathcal{A}_\Omega$ existem os elementos u_σ (que são regulares), bem como os elementos $a_{\rho,\sigma}$ (também regulares). As regras de construção dos produtos cruzados com anéis normais são verificadas, e é legítimo escrever, mesmo,

$$\mathcal{A}_\Omega = (\mathcal{T}_\Omega/\Omega, \mathcal{G}, a_{\rho,\sigma}) .$$

Teorema 3:- Se $\mathcal{T}$ e $\mathcal{T}_1$ são anéis normais relativos a $\mathcal{P}$ e aos grupos $\mathcal{G}$ e $\mathcal{G}_1$, respectivamente, é válido o seguinte isomorfismo:

$$(\mathcal{T}\times\mathcal{T}_1/\mathcal{P}, \mathcal{G}\times\mathcal{G}_1, a_{\rho,\sigma} b_{\rho_1,\sigma_1}) \cong (\mathcal{T}/\mathcal{P}, \mathcal{G}, a_{\rho,\sigma}) \times (\mathcal{T}_1/\mathcal{P}, \mathcal{G}_1, b_{\rho_1,\sigma_1}) .$$

No 1º membro figura um produto cruzado com um anel normal, como vamos ver. Em primeiro lugar, $\mathcal{T}\times\mathcal{T}_1$ é um anel normal relativo a $\mathcal{G}\times\mathcal{G}_1$ e a $\mathcal{P}$ (teorema VI sobre anéis normais). Depois, tomemos os símbolos $u_{\rho\rho_1}, u_{\rho\sigma_1}, \ldots, u_{\sigma\rho_1}, \ldots$ e ponhamos

$$u_{\rho\rho_1} \cdot u_{\sigma\sigma_1} = a_{\rho,\sigma} b_{\rho_1,\sigma_1} u_{(\rho\sigma)(\rho_1\sigma_1)} .$$

Os elementos $a_{\rho,\sigma} b_{\rho_1,\sigma_1}$ são regulares em $\mathcal{T}\times\mathcal{T}_1$ e as relações (3) são válidas. Quanto às relações (5), elas revestem-se aqui do aspecto

$$u_{\rho\rho_1\beta} = u_{\rho\rho_1}(ss_1) = (ss_1)^{\rho\rho_1} u_{\rho\rho_1} = s^\rho s_1^{\rho_1} u_{\rho\rho_1} ,$$

($\beta = ss_1$, $s \in \mathcal{T}$, $s_1 \in \mathcal{T}_1$). Feita, assim, a verificação anunciada, formemos o produto directo indicado no 2º membro da relação de isomorfismo afirmada no teorema. Tem-se (se $T_1, \ldots, T_{n_1}$ representa uma base de $\mathcal{T}_1$ sobre $\mathcal{P}$):

$$\mathcal{A} = (\mathcal{T}/\mathcal{P}, \mathcal{G}, a_{\rho,\sigma}) = \sum_{\sigma\in\mathcal{G}} \mathcal{T} u_\sigma = \sum_\sigma \mathcal{P} S_1 u_\sigma + \ldots + \sum_\sigma \mathcal{P} S_n u_\sigma ;$$

$$\mathcal{A}_1 = (\mathcal{T}_1/\mathcal{P}, \mathcal{G}_1, b_{\rho_1,\sigma_1}) = \sum_{\sigma_1\in\mathcal{G}_1} \mathcal{T}_1 u_{\sigma_1} = \sum_{\sigma_1} \mathcal{P} T_1 u_{\sigma_1} + \ldots + \sum_{\sigma_1} \mathcal{P} T_{n_1} u_{\sigma_1} ;$$

$$\mathcal{A}\times\mathcal{A}_1 = \sum_{\sigma,\sigma_1,t,k} \mathcal{P}(S_t u_\sigma \cdot T_k u_{\sigma_1}) = \sum_{\sigma,\sigma_1,t,k} \mathcal{P} S_t T_k u_\sigma u_{\sigma_1} = \sum_{\sigma,\sigma_1} (\mathcal{T}\times\mathcal{T}_1) u_\sigma u_{\sigma_1} ;$$

$$u_\rho u_{\rho_1} \cdot u_\sigma u_{\sigma_1} = u_\rho u_\sigma \cdot u_{\rho_1} u_{\sigma_1} = a_{\rho,\sigma} b_{\rho_1,\sigma_1} u_{\rho\sigma} u_{\rho_1\sigma_1} .$$

Basta identificar $u_\rho u_{\rho_1}$ com $u_{\rho\rho_1}$ para se reconhecer que o teorema tem lugar.

O último § deste Capítulo será dedicado, sempre com Teichmüller, a uma outra demonstração dos teoremas da multiplicação e da ampliação do corpo fundamental (relativos aos produtos cruzados vulgares), tratados nos §§ 3 e 4, respectivamente. Fá-lo-emos preceder dum outro § sobre a construção de Komposita de corpos, o que nos permitirá precisar certos raciocínios não inteiramente levados a cabo em Capítulos anteriores.(1)

11) Komposita de corpos - Dado o corpo comutativo Φ, se $\mathcal{K}$ e $\mathcal{L}$ são dois sub-corpos de Φ, diz-se Kompositum de $\mathcal{K}$ e $\mathcal{L}$, em Φ, e representa-se por $(\mathcal{K}, \mathcal{L}; \Phi)$, o sub-corpo $\mathcal{F}$, de Φ, obtido por intersecção de todos os sub-corpos de Φ que contêm $\mathcal{K}$ e $\mathcal{L}$. A definição estende-se ao caso de vários sub-corpos de Φ. O Kompositum é, neste sentido, um corpo bem determinado. Podemos escrever $\mathcal{F} = (\mathcal{K}, \mathcal{L}; \Phi) = \mathcal{K}(\mathcal{L}) = \mathcal{L}(\mathcal{K}) = \mathcal{K}\mathcal{L}$.

Tomemos, por ex., o corpo de decomposição $\Phi = \mathcal{P}(\Theta_1, \ldots, \Theta_r)$ dum polinómio $\varphi(x) = 0$, com coeficientes pertencentes a $\mathcal{P}$. O corpo Φ é Kompositum $\mathcal{F}$ dos sub-corpos $\mathcal{P}(\Theta_i) \subseteq \Phi$.

Ainda no caso de ampliações algébricas finitas, suponhamos Φ uma tal ampliação de $\mathcal{P}$, do grau n, e consideremos dois sub-

(1) Vejam-se as indicações bibliográficas referidas no § 4 do Cap. anterior.

-corpos $\mathcal{K}$ e $\mathcal{L}$, de Φ, respectivamente de graus μ e λ, relativamente a $\mathcal{P}$. O Kompositum de $\mathcal{K}$ e $\mathcal{L}$ tem um grau m, sobre $\mathcal{P}$, dado por

$$m = \left(\mathcal{K}(\mathcal{L})/\mathcal{P}\right) = \left(\mathcal{K}(\mathcal{L})/\mathcal{K}\right).(\mathcal{K}/\mathcal{P}) = \left(\mathcal{K}(\mathcal{L})/\mathcal{K}\right).\mu .$$

Se $v_1, \ldots, v_\lambda$ constituem elementos de $\mathcal{L}$ independentes em face de $\mathcal{P}$, os mesmos elementos não são, em geral, independentes em face de $\mathcal{K}$, tendo-se, por isso, $\left(\mathcal{K}(\mathcal{L})/\mathcal{K}\right) \geq (\mathcal{L}/\mathcal{P})$, e $\left(\mathcal{K}(\mathcal{L})/\mathcal{P}\right) \geq \lambda\mu$. No caso de valer aqui o sinal $=$, a álgebra $\mathcal{K}(\mathcal{L})$, sobre $\mathcal{P}$, é isomorfa (relativamente a $\mathcal{P}$) do produto directo $\mathcal{K}\times\mathcal{L}$, podendo escrever-se $\mathcal{K}(\mathcal{L}) = \mathcal{K}\times\mathcal{L}$. É válido o seguinte

Teorema 1:- Se $\mathcal{K}$ e $\mathcal{L}$ são duas ampliações algébricas finitas, de graus μ e λ, de $\mathcal{P}$, contidas em Φ, o Kompositum de $\mathcal{K}$ e $\mathcal{L}$, em Φ, tem um grau m, sobre $\mathcal{P}$, igual ou inferior ao produto $\lambda\mu$. No caso da igualdade, o referido Kompositum é o produto directo $\mathcal{K}\times\mathcal{L}$ (sobre $\mathcal{P}$).

Precisemos ainda. Se $u_1, \ldots, u_\mu$ constitui uma base de $\mathcal{K}$ (sobre $\mathcal{P}$), quando se tem $m = \lambda\mu$, as quantidades $u_i v_j$ são independentes em face de $\mathcal{P}$. Os elementos de $\mathcal{K}(\mathcal{L})$ são da forma $\sum \pi_{ij} u_i v_j$, com $\pi_{ij} \in \mathcal{P}$. São ainda da mesma forma os elementos da álgebra $\mathcal{K}\times\mathcal{L}$. Na correspondência biunívoca estabelecida, reconhece-se imediatamente o isomorfismo relativo a $\mathcal{P}$.

O grau m é múltiplo de μ e de λ. Se μ e λ são primos entre si, valerá necessàriamente $m = \lambda\mu$, de sorte que tem lugar este

Corolário 1:- O Kompositum de $\mathcal{K}$ e $\mathcal{L}$, em Φ, se $\mathcal{K}$ e $\mathcal{L}$ são ampliações algébricas finitas de $\mathcal{P}$, de graus primos entre si, é a álgebra $\mathcal{K}\times\mathcal{L}$.

Suponhamos agora que $\mathcal{K}$ e $\mathcal{L}$ não são sub-corpos dum corpo, mas são ampliações quaisquer dum corpo $\mathcal{P}$. Podemos definir ainda um Kompositum como vai ver-se. Seja $\mathcal{F}$ uma ampliação de $\mathcal{P}$ e admitamos que existem em $\mathcal{F}$ dois corpos $\mathcal{K}'$ e $\mathcal{L}'$ isomorfos de $\mathcal{K}$ e $\mathcal{L}$, com respeito a $\mathcal{P}$. $\mathcal{F}$ diz-se um Kompositum de $\mathcal{K}$ e $\mathcal{L}$ relativo a $\mathcal{P}$, quando se realiza a condição seguinte: não há, em $\mathcal{F}$, sub-corpo próprio que contenha $\mathcal{K}'$ e $\mathcal{L}'$. Como notação, seria

legítimo escrever agora $\mathcal{F} = (\mathcal{K}, \mathcal{L}; \mathcal{P}) = (\mathcal{K}', \mathcal{L}'; \mathcal{F})$. O último símbolo, precisamente o que foi dado no começo do §, faz perder o carácter de "relativo a $\mathcal{P}$". Mas $\mathcal{F}$ supõe-se, então, prèviamente definido. Por simplicidade, tendo sempre em vista que haverá um corpo fundamental $\mathcal{P}$, do qual os outros serão ampliações, poremos apenas $\mathcal{F} = \{\mathcal{K}, \mathcal{L}\}$, para símbolo de Kompositum.

Para se obter a totalidade dos Komposita de $\mathcal{K}$ e $\mathcal{L}$, relativos a $\mathcal{P}$, devemos considerar primeiramente um determinado corpo Φ, onde existam sub-corpos $\mathcal{K}'$ e $\mathcal{L}'$, isomorfos de $\mathcal{K}$ e $\mathcal{L}$, relativamente a $\mathcal{P}$, e determinar, em Φ, os Komposita dos possíveis $\mathcal{K}'$ e $\mathcal{L}'$; em seguida, devemos considerar todos os corpos Φ nas condições referidas.

Imaginemos realizadas as hipóteses seguintes: $\Phi \supset \mathcal{K}$, $\Phi \supset \mathcal{L}$ e $\mathcal{K} \cong \mathcal{L}$, relativamente a $\mathcal{P}$. Podemos definir, em Φ, os dois Komposita seguintes, de $\mathcal{K}$ e $\mathcal{L}$ relativos a $\mathcal{P}$: $\mathcal{F} = (\mathcal{K}, \mathcal{L}; \Phi)$, $(\mathcal{K}, \mathcal{K}; \Phi) = \mathcal{K}$. Se há em $\mathcal{L}$ elementos não pertencentes a $\mathcal{K}$, o Kompositum $\mathcal{F}$ contém $\mathcal{K}$ como sub-corpo próprio. Supondo Φ finito sobre $\mathcal{P}$, não pode haver uma equivalência entre $\mathcal{F}$ e $\mathcal{K}$, relativamente a $\mathcal{P}$. Dois Komposita

$$\{\mathcal{K}, \mathcal{L}\} = (\mathcal{K}', \mathcal{L}'; \mathcal{F}) = \mathcal{F}\,; \qquad \{\mathcal{K}, \mathcal{L}\} = (K', L'; F) = F\,,$$

relativos a $\mathcal{P}$, dizem-se equivalentes, se os isomorfismos simultâneos

$$\mathcal{K}' \cong K', \qquad \mathcal{L}' \cong L', \qquad \text{(relativos a } \mathcal{P}),$$

determinados por intermédio de $\mathcal{K}$ e de $\mathcal{L}$, puderem ampliar-se e levar a um isomorfismo $\mathcal{F} \cong F$ (relativo a $\mathcal{P}$).

Vamos estudar em detalhe o caso em que $\mathcal{K} = \mathcal{P}(\Theta)$ é uma ampliação finita simples de $\mathcal{P}$, podendo $\mathcal{L}$ ser uma ampliação qualquer do mesmo corpo. O corpo $\mathcal{L}(\Theta) = \mathcal{F}_0$ é um Kompositum $\{\mathcal{K}, \mathcal{L}\}$. Outro Kompositum $\mathcal{F}$ conterá um corpo $\mathcal{K}' = \mathcal{P}(\Theta')$, onde Θ' satisfaz à equação irredutível em $\mathcal{P}$, $\varphi(x) = 0$, a que também satisfaz Θ. Além disso, conterá $\mathcal{L}' \cong \mathcal{L}$ (relativamente a $\mathcal{P}$). Nós vamos admitir que $\mathcal{L}'$ se substitui por $\mathcal{L}$. Assim, todo o $\{\mathcal{K}, \mathcal{L}\}$ será da forma $\mathcal{L}(\Theta')$, pondo de parte equivalências, no sentido atrás indicado. Se $\varphi(x)$ admitir em $\mathcal{L}$ a decomposição $\varphi(x) = \varphi_1(x) \ldots \varphi_r(x)$, cada Kompositum é equivalente a um certo $\mathcal{L}(\Theta')$, onde Θ' satisfaz a uma determinada equação $\varphi_i(x) = 0$. Mas, a

φ_i φ_j diferentes, correspondem Komposita não equivalentes. A equivalência, com efeito, estaria aqui subordinada às seguintes correspondências: $\mathcal{L} \leftrightarrow \mathcal{L}$, $\Theta \leftrightarrow \Theta'$. Se Θ é zero de φ_i e Θ' é zero de φ_j, os dois polinómios φ_i e φ_j deveriam ter os mesmos coeficientes e coincidiriam. Importa, todavia, fazer a seguinte observação: dois Komposita podem ser isomorfos relativamente a $\mathcal{P}$ (ou relativamente a $\mathcal{L}$), sem que sejam equivalentes. Daremos o seguinte enunciado:

Teorema 2:- Os Komposita de $\mathcal{K}$ e $\mathcal{L}$, relativos a $\mathcal{P}$, se $\mathcal{K} = \mathcal{P}(\Theta)$ é ampliação algébrica simples de $\mathcal{P}$ e $\mathcal{L}$ é uma ampliação qualquer do mesmo corpo, são equivalentes aos corpos $\mathcal{L}(\Theta')$, onde Θ' é raiz da equação irredutível em $\mathcal{P}$, $\varphi(x) = 0$, a que satisfaz Θ, ou raiz da equação irredutível em $\mathcal{L}$, $\varphi_i(x) = 0$, suposto φ_i um factor da decomposição $\varphi(x) = \varphi_1(x) \cdots \varphi_r(x)$, que tem lugar em $\mathcal{L}$. O número de Komposita não equivalentes é igual ao número dos φ_i φ_j distintos.

Corolário 2:- Os Komposita de $\mathcal{K}$ e $\mathcal{L}$, referidos no teorema anterior, são todos equivalentes, se $\varphi(x)$ for uma potência dum polinómio irredutível em $\mathcal{L}$.

Incidentalmente, ficou demonstrada esta proposição:

Teorema 3:- Se $\mathcal{K} = \mathcal{P}(\Theta)$ é uma álgebra comutativa de divisão (sobre $\mathcal{P}$) e $\varphi(x) = 0$ é a equação irredutível em $\mathcal{P}$ a que satisfaz Θ; se, além disso, $\varphi(x)$ é irredutível na ampliação finita $\mathcal{L}$, de $\mathcal{P}$, a álgebra $\mathcal{K}_{\mathcal{L}}$ é uma álgebra de divisão (sobre $\mathcal{L}$). De facto, $\mathcal{K}_{\mathcal{L}} = \mathcal{K} \times \mathcal{L} = \mathcal{L}(\Theta)$, nos termos do teorema 1, reduz-se, essencialmente, ao único Komposítum de $\mathcal{K}$ e $\mathcal{L}$ relativamente a $\mathcal{P}$.

Passemos ao caso de $\mathcal{K}$ ser separável, além de finito. Então, é sempre $\mathcal{K} = \mathcal{P}(\Theta)$, e os teoremas anteriores são aplicáveis. Em particular: no teorema 2, o número dos Komposita não equivalentes é igual a $\underline{r}$; e, no teorema 3, tem-se uma afirmação que resulta imediatamente do teorema 1, de pgs. 199.

Se $\mathcal{K}$, além de finito e separável, é normal, podemos dizer:

Teorema 4:- Pondo de parte equivalências, os Komposita de $\mathcal{K}$ e $\mathcal{L}$ relativos a $\mathcal{P}$, se $\mathcal{K} = \mathcal{P}(\Theta)$ é normal e separável e $\mathcal{L}$ é uma ampliação qualquer de $\mathcal{P}$, são em número igual ao dos factores φ_i referidos no teorema 2. Além disso, os diferentes Komposita são isomorfos relativamente a $\mathcal{L}$, se este último corpo é sub-corpo dos Komposita. Neste caso, com efeito, $\mathcal{L}(\Theta')$ contém todas as raizes de $\varphi(x) = 0$ ou dos $\varphi_i(x) = 0$. Os diferentes $\mathcal{L}(\Theta')$ são idênticos. Como tais, são isomorfos relativamente a $\mathcal{L}$. O facto de os $\mathcal{L}(\Theta')$ serem todos do mesmo grau relativamente a $\mathcal{L}$ mostra-nos que os $\varphi_i(x)$ são também todos do mesmo grau. A equivalência falha, como se sabe. Logo que se quisesse, em $\mathcal{L}(\Theta)$, um isomorfismo de $\mathcal{K}$ relativamente a $\mathcal{P}$, teríamos de considerar uma correspondência $\Theta \leftrightarrow \Theta'$, que conservaria globalmente $\mathcal{K}$, mas que só poderia ser um isomorfismo $\mathcal{L}(\Theta) \cong \mathcal{L}(\Theta')$, com conservação individual dos elementos de $\mathcal{L}$, se Θ e Θ' fossem zeros do mesmo $\varphi_i(x)$.

Os resultados anteriores podem ligar-se a considerações doutra ordem. Sejam $\mathcal{K}$ uma ampliação finita de $\mathcal{P}$ e $\mathcal{L}$ uma ampliação qualquer do mesmo corpo. A álgebra $\mathcal{K}_{\mathcal{L}}$, se $\varkappa_1, \ldots, \varkappa_n$ for uma base de $\mathcal{K}$ (sobre $\mathcal{P}$), compõe-se de elementos da forma $\sum \iota_i \varkappa_i$, $(\iota_i \in \mathcal{L})$. No Komposítum $\mathcal{F}$ podem formar-se também os elementos $\sum \iota_i \varkappa_i$, desde que admitamos haver substituido $\mathcal{K}'$ e $\mathcal{L}'$, respectivamente por $\mathcal{K}$ e $\mathcal{L}$. Então, $\mathcal{F}$ é imagem anular homomorfa de $\mathcal{K}_{\mathcal{L}}$ [A fim de se compreender claramente a afirmação, raciocinemos como segue: Tomemos $\mathcal{K} = \mathcal{L}$; $\mathcal{K}_{\mathcal{L}}$ é de ordem $\underline{n}$ relativamente a $\mathcal{L}$ e de ordem $\underline{n}^2$ relativamente a $\mathcal{P}$, enquanto que $\mathcal{K}\mathcal{L} = \mathcal{K} = \mathcal{F}$ é de ordem $\underline{n}$ relativamente a $\mathcal{P}$. O elemento $-\varkappa_2\varkappa_1 + \varkappa_1\varkappa_2 \in \mathcal{K}_{\mathcal{L}}$, se $\varkappa_1$ e $\varkappa_2$ não forem simultâneamente nulos, é diferente de zero; mas o elemento com a mesma forma pertencente a $\mathcal{F}$ é igual a zero]. O homomorfismo $\mathcal{K}_{\mathcal{L}} \sim \mathcal{F}$ tem lugar relativamente a $\mathcal{L}$. Não pode falar-se de homomorfismo relativamente a $\mathcal{K}$, pois que $\mathcal{K}$ se não aplica a $\mathcal{K}_{\mathcal{L}}$. É válido o seguinte

Teorema 5:- O Komposítum $\mathcal{K}\mathcal{L} = \mathcal{F}$, de $\mathcal{K}$ e $\mathcal{L}$, se $\mathcal{K}$ é finito (sobre $\mathcal{P}$), é uma imagem anular homomorfa (relativamente a $\mathcal{L}$) da álgebra $\mathcal{K}_{\mathcal{L}}$ (sobre $\mathcal{L}$). Inversamente, é Komposítum de $\mathcal{K}$ e $\mathcal{L}$ toda a imagem homomorfa de $\mathcal{K}_{\mathcal{L}}$ (relativamente a $\mathcal{L}$) que seja corpo.

Passemos ao caso em que $\mathcal{K}$ é ampliação separável de $\mathcal{P}$. A álgebra $\mathcal{K}_\mathcal{L}$ é semi-simples, e, portanto, uma soma de corpos comutativos (não isomorfos relativamente a $\mathcal{K}_\mathcal{L}$). Pondo $\mathcal{K}_\mathcal{L} = \mathcal{F}_1 + \cdots + \mathcal{F}_r$, o teorema anterior mostra-nos que cada corpo $\mathcal{F}_i$ é um Kompositum de $\mathcal{K}$ e $\mathcal{L}$. Reciprocamente, um tal Kompositum $\mathcal{F}$, como imagem anular homomorfa de $\mathcal{K}_\mathcal{L}$, contém corpos isomorfos de $\mathcal{K}$ e de $\mathcal{L}$ (relativamente a $\mathcal{P}$). Por outro lado, $\mathcal{F}$ é isomorfo dum certo anel factor $\mathcal{K}_\mathcal{L}/\mathfrak{a}$, isomorfismo que tem lugar relativamente a $\mathcal{L}$. Como $\mathfrak{a}$ é soma de determinados $\mathcal{F}_j$, segue-se que $\mathcal{F}$ é isomorfo dum $\mathcal{F}_i$ fixo. A análise deste isomorfismo mostra que $\mathcal{F}$ e $\mathcal{F}_i$ são Komposita equivalentes. Tem lugar este outro

Teorema 6:- Se $\mathcal{K}$ é uma ampliação separável finita de $\mathcal{P}$, e $\mathcal{L}$ é uma ampliação qualquer do mesmo corpo $\mathcal{P}$, todo o Kompositum de $\mathcal{K}$ e $\mathcal{L}$, relativamente a $\mathcal{P}$, é equivalente a um Kompositum $\mathcal{F}_i$ da decomposição $\mathcal{K}_\mathcal{L} = \mathcal{F}_1 + \cdots + \mathcal{F}_r$. Os Komposita $\mathcal{F}_i$ não são equivalentes.

Precisemos ainda os raciocínios que antecederam este enunciado. Em primeiro lugar, não devemos esquecer que, em $\mathcal{F}$, se supõe feita a substituição de $\mathcal{L}'$ pelo corpo isomorfo $\mathcal{L}$. Quanto a $\mathcal{F}_i$, devemos observar, em seguida, que, decompondo $u \in \mathcal{K}_\mathcal{L}$ em idempotentes ortogonais pela igualdade $u = e_1 + \cdots + e_r$, $(e_i \in \mathcal{F}_i)$, e tendo em conta as relações

$$k = ke_1 + \cdots + ke_r, \quad \ell = \ell e_1 + \cdots + \ell e_r, \quad (k \in \mathcal{K}, \ell \in \mathcal{L}),$$

se conclui serem isomorfismos relativos a $\mathcal{P}$ as correspondências $\mathcal{K} \longleftrightarrow \mathcal{K}e_i$, $\mathcal{L} \longleftrightarrow \mathcal{L}e_i$.

Posto isto, vejamos, finalmente, que $\mathcal{F}_i$ e $\mathcal{F}_j$ não são equivalentes. (1) Se o pudessem ser, ter-se-ia

$$e_i = \sum_m \ell_{im} \varkappa_m \longrightarrow e_j = \sum_m \ell_{jm} \varkappa_m, \qquad (\ell_{Rq} \in \mathcal{L}, \varkappa_p \in \mathcal{K}),$$

$$e_i^2 = e_i = \sum_m (\ell_{im} e_i)(\varkappa_m e_i) \longrightarrow e_j = e_j^2 = \sum_m (\ell_{jm} e_j)(\varkappa_m e_j),$$

pois que uma expressão da forma $\ell \varkappa e_j$ se pode escrever

(1) Jacobson, loc. cit., pgs.97.

$$\ell \varkappa e_j = \ell(\varkappa e_j) = e_j(\ell \cdot \varkappa e_j) = \ell(e_j \cdot \varkappa e_j) = \ell e_j \cdot \varkappa e_j .$$

A referida equivalência seria uma ampliação da equivalência $\mathcal{L}e_i \longleftrightarrow \mathcal{L}e_j$, de sorte que se teria ainda

$$e_j = \sum_m (\ell_{im} e_j)(\varkappa_m e_j) = \sum_m \ell_{im} \varkappa_m \cdot e_j = e_i \cdot e_j = 0,$$

o que seria absurdo. A última parte do teorema fica provada.

Os teoremas 4 e 6 ficam em concordância, logo que, conforme o estabelecido no teorema 1 de pgs.199, se tenha em conta ser o número dos $\mathcal{F}_i$ precisamente igual ao número dos factores irredutíveis de $\varphi(x)$, em $\mathcal{L}[x]$.

Quando $\mathcal{K}$ é ampliação inseparável de $\mathcal{P}$, $\mathcal{K}_\mathcal{L}$ pode ter radical $\mathcal{R}$. Considerando a álgebra semi-simples (sobre $\mathcal{L}$) $\mathcal{K}_\mathcal{L}/\mathcal{R}$, obtêm-se as imagens anulares homomorfas de $\mathcal{K}_\mathcal{L}$, que são corpos, fazendo a decomposição em corpos daquela álgebra semi-simples.

12) Os teoremas da multiplicação e da ampliação do corpo fundamental - O Capítulo vai terminar pelas demonstrações referidas no final do § 10, relativas aos teoremas em epígrafe. Se $\mathcal{K}$ e $\mathcal{K}_1$ são duas ampliações finitas, normais e separáveis de $\mathcal{P}$, já sabemos que se tem

$$(\mathcal{K}/\mathcal{P}, \mathcal{G}, a_{\rho,\sigma}) \times (\mathcal{K}_1/\mathcal{P}, \mathcal{G}_1, b_{\rho_1,\sigma_1}) \cong (\mathcal{K} \times \mathcal{K}_1/\mathcal{P}, \mathcal{G} \times \mathcal{G}_1, a_{\rho,\sigma} b_{\rho_1,\sigma_1}).$$

Também sabemos que, numa interpretação conveniente, da decomposição

$$\mathcal{K}_{\mathcal{L}_1} = \mathcal{L}_1 + \cdots + \mathcal{L}_r , \tag{30}$$

se tira a seguinte relação de semelhança:

$$(\mathcal{K} \times \mathcal{K}_1/\mathcal{P}, \mathcal{G} \times \mathcal{G}_1, a_{\rho,\sigma} b_{\rho_1,\sigma_1}) \approx (\mathcal{L}_1/\mathcal{P}e_1, \mathcal{L}_\mathcal{G}, e_1 a_{\rho,\sigma} b_{\rho_1,\sigma_1}).$$

Fazendo $\mathcal{K}_1 = \mathcal{K}$, a decomposição (30) leva a tantas parcelas quantas o grau $(\mathcal{K}/\mathcal{P})$. Cada parcela, como $\mathcal{L}_1$, é, então, álgebra de 1ª ordem sobre $\mathcal{K}$, o que significa $\mathcal{K} \cong \mathcal{L}_1$, com correspondên-

cia $\mathcal{P} \longrightarrow \mathcal{P}e_1$. É, assim,

$$(\mathcal{K}/\mathcal{P}, \mathcal{G}, a_{\rho,\sigma}) \times (\mathcal{K}/\mathcal{P}, \mathcal{G}, b_{\rho_1,\sigma_1}) \approx (\mathcal{K}/\mathcal{P}, \mathcal{G}, a_{\rho,\sigma} b_{\rho_1,\sigma_1}) ,$$

como afirma o teorema da multiplicação do § 3.

Quanto ao teorema da ampliação, vamos utilizar, em parte, as notações do § 4. $\mathcal{K}$ é uma ampliação finita, normal e separável de $\mathcal{P}$, e $\mathcal{Q}$ uma ampliação qualquer do mesmo corpo. $\mathcal{K}\mathcal{Q}$ é um Kompositum de $\mathcal{K}$ e $\mathcal{Q}$ relativo a $\mathcal{P}$, no qual se supõe existirem $\mathcal{K}$ e $\mathcal{Q}$. Feita a decomposição $\mathcal{K}\mathcal{Q} = \mathcal{L}_1 + \cdots \mathcal{L}_r$, sabemos que os diferentes $\mathcal{L}_l$ são ampliações normais separáveis de corpos isomorfos de $\mathcal{Q}$, ampliações todas isomorfas relativamente a $\mathcal{Q}$. O Kompositum $\mathcal{K}\mathcal{Q}$ é equivalente a $\mathcal{L}_1$, por ex. Como

$$(\mathcal{K}/\mathcal{P}, \mathcal{G}, a_{\rho,\sigma})_{\mathcal{Q}} \cong (\mathcal{K}_{\mathcal{Q}}/\mathcal{Q}, \mathcal{G}, a_{\rho,\sigma}) \approx (\mathcal{L}_1/\mathcal{Q}e_1, \mathcal{G}, e_1 a_{\rho',\sigma'}) ,$$

bastará mostrar o isomorfismo

$$(\mathcal{K}\mathcal{Q}/\mathcal{Q}, \mathcal{G}', a_{\rho',\sigma'}) \cong (\mathcal{L}_1/\mathcal{Q}e_1, \mathcal{G}, e_1 a_{\rho',\sigma'}) ,$$

para se concluir o teorema. Isso é imediato, visto que $\mathcal{K}\mathcal{Q}$ e $\mathcal{L}_1$ são supostos equivalentes, e, portanto, são válidas as correspondências seguintes:

$$\mathcal{K} \longleftrightarrow \mathcal{K}e_1 , \quad \mathcal{Q} \longleftrightarrow \mathcal{Q}e_1 , \quad \mathcal{K}\mathcal{Q} \longleftrightarrow \mathcal{L}_1 ,$$

das quais a última é prolongamento das anteriores.

ÍNDICE

(de termos e de autores)

HIPER-COMPLEXOS

I

POR

A. ALMEIDA COSTA

CENTRO DE ESTUDOS MATEMÁTICOS

SISTEMAS HIPER-COMPLEXOS E REPRESENTAÇÕES

POR

A. ALMEIDA COSTA

FACULDADE DE CIÊNCIAS DO PORTO
1948