Composto e impresso na
TIPOGRAFIA MATEMÁTICA, LDA.
R. General Sinel de Cordes, 11-A
TELEFONE 77 19 43 — LISBOA-1.

PREFÁCIO

Este livro está planeado para servir os estudantes dos dois primeiros anos das nossas Universidades. As matérias nele contidas limitam-se quase exclusivamente àqueles assuntos que não se encontram tratados nas obras do Prof. Vicente Gonçalves. E dizemos «quase exclusivamente», porque, numa pequena parte do livro, há pontos de contacto com o tratado daquele eminente Professor. Mesmo então, devemos acentuar, os nossos pontos de vista são diferentes; só assim, de resto, se poderá compreender que deles nos tenhamos ocupado.

Encontram-se no livro as ideias essenciais da Aritmética, da Álgebra e da Geometria. Esse facto permite-nos julgar que ele poderá ser também útil àqueles que se interessam por uma construção satisfatória daquelas disciplinas. Nesse sentido, não esquecemos os que têm uma parte da sua actividade ligada à Pedagogia das Matemáticas. Salvo o Capítulo IV, dedicado à Teoria dos Grupos com Operadores, tudo quanto se escreveu é de leitura extremamente simples.

O livro, que contém bastantes exemplos, não propõe exercícios. O nosso amigo e 1.º assistente, Doutor Tiago de Oliveira, que tem sido, de há muito tempo a esta parte, o nosso principal colaborador, preencherá, dentro de pouco tempo, essa lacuna.

Depara-se-nos a oportunidade, que não desejamos perder, de fazer algumas considerações de outra ordem, não menos importantes, porque podem evitar a inutilidade de muitos e bons esforços. Fora dos Centros de Estudos que temos dirigido, tanto no Porto como em Lisboa, a não ser por influência de anterior colaboração prestada nesses Centros, pode dizer-se que, tudo quanto no nosso País se tem escrito sobre a quase totalidade das matérias aqui tratadas, mal merece ser considerado. Havendo hoje, entre nós, como nos temos apercebido, um real interesse por essas matérias, importa ter em conta que é essencial não nos embrenharmos em especulações de Fundamentos, com prejuízo das ideias direc-

trizes gerais. O nosso livro, repitamo-lo mais uma vez, pretende impedir a perda dos esforços generosos de todos aqueles que, com temperamento semelhante ao nosso, encontram como principal recompensa desses esforços a alegria que lhes é proporcionada ao analisarem com justa medida os modelos de pensamento oferecidos por grande número de homens eminentes do nosso tempo.

Antes de acabar, seja-nos permitido dizer que, embora tenhamos encontrado já alguns êrros e lapsos, não damos uma nota dos mesmos, por os encontrarmos de fácil correcção. Limitamo-nos a dois, de entre os que reconhecemos como mais importantes: 1.º) Na página 65, linha 6, a contar do fim, deve dizer se: $\mathfrak{H}$ é bem determinado e contém uma parte $\mathfrak{T}$ que aplica classes distintas em classes distintas. $\mathfrak{T}$ é também bem determinado e forma um subgrupo de $\mathfrak{H}$, como vamos ver. 2.º) A págs. 72, o teorema do alto deve começar assim: Se $\mathfrak{H} \sim \mathfrak{H}'$ é um homomorfismo Ω entre dois grupos-Ω ....

Lisboa, 16 de Outubro de 1958.

A. Almeida Costa

ELEMENTOS

DE

ALGEBRA LINEAR E DE GEOMETRIA LINEAR

CAPITULO I

Conjuntos

§ 1. Generalidades da teoria dos conjuntos

1) **Notações e definições** — É costume exprimir que um *conjunto* $\mathfrak{C}$, ou colecção ou agregado de certos *elementos* $a, b, \cdots, x, \cdots$, se compõe exactamente dos referidos elementos, escrevendo $\mathfrak{C} = \{a, b, \cdots, x, y, \cdots\}$. Diz-se, então, que o elemento x, por exemplo, pertence a $\mathfrak{C}$ e representa-se esse facto simbòlicamente por $x \in \mathfrak{C}$. Por vezes, os elementos de $\mathfrak{C}$ são caracterizados por uma certa propriedade π; escreve-se, nesse caso, $\mathfrak{C} = \{x \mid \pi\}$, podendo, até, usar-se uma simbólica que põe em evidência a propriedade exigida aos elementos $x \in \mathfrak{C}$.

Para significarmos que A é uma parte de $\mathfrak{C}$, utilizaremos a notação $A \subseteq \mathfrak{C}$. Ainda mesmo que A seja parte duma parte B, de $\mathfrak{C}$, escrevemos $A \subseteq B$. Pode acontecer que A seja parte *imprópria* de B, isto é, que se tenha $A = B$. Com $A \subseteq B$, não se exclui a hipótese $A = B$; se ela se não dá, A é parte *própria* de B, o que se exprime, se isso precisar de ser posto em evidência, por $A \subset B$. Uma parte de $\mathfrak{C}$ diz-se também um *subconjunto* de $\mathfrak{C}$. Considera-se ainda o conjunto *vazio*, ou seja o conjunto que não contém qualquer elemento, como uma parte de qualquer conjunto. O símbolo $\emptyset$, que deve ler-se «zero», representará o conjunto vazio.

A expressão $B \supseteq A$ tem o mesmo significado que $A \subseteq B$. Diz-se, então, que B contém A. Também $B \supset A$ se interpreta como $A \subset B$.

A *intersecção* D, de duas partes A e B, de $\mathfrak{C}$, define-se como o conjunto dos elementos de $\mathfrak{C}$ que pertencem simultâneamente a A e a B. Escrever-se-á $D = A \cap B$, tendo-se $D = \{x \mid x \in A, x \in B\}$. A propriedade π é aqui expressa por: $x \in A, x \in B$. Devemos preservar-nos, porém, de supôr que a letra D virá a ser usada com o significado de intersecção.

A *união* ou *conjunto unido* de duas partes A e B, de $\mathfrak{C}$, define-se como o conjunto dos elementos de $\mathfrak{C}$ que pertencem, pelo menos, a uma daquelas partes. Escrever-se-á $U = A \cup B$, mas devemos preservar-nos de supor que a letra U virá a ser utilizada num tal sentido.

A e B dizem-se subconjuntos *disjuntos*, se a sua intersecção é o conjunto vazio. Não há, então, elementos comuns. Duma maneira geral, dois conjuntos dizem-se disjuntos se não tiverem elementos comuns.

A e B dizem-se *complementares*, em $\mathfrak{C}$, se B contiver exactamente os elementos de $\mathfrak{C}$ que não pertencem a A.

A *diferença* $A - B$ é entendida como o conjunto dos elementos de A que não pertencem a B. Quando A e B são complementares em $\mathfrak{C}$, tem-se $B = \mathfrak{C} - A = \{x \mid x \in \mathfrak{C}, x$ não pertencente a $A\}$.

Àcerca de notações é útil fixar ainda esta

Convenção: Um sinal cortado por um traço oblíquo significará «negação» daquilo que o sinal representa. Assim, $\notin$ significa «não pertence» ou «não pertencente»; $\not\subseteq$ significa «não contido», etc.

2) **Sobre certas relações entre subconjuntos** — Tendo em conta as definições e os sinais indicados no número anterior, estabelecem-se fàcilmente as igualdades e inclusões que vamos escrever:

I) $A \subseteq A$;
II) se $A \subseteq B$ e $B \subseteq A$, então $A = B$;
III) se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$;
IV) se $A \subseteq B$, tem-se $A \cap B = A, A \cup B = B, \mathfrak{C} - A \supseteq \mathfrak{C} - B$, sendo qualquer das três últimas relações equivalente à primeira;
V) em particular, de $A \subseteq A$, tira-se $A \cap A = A, A \cup A = A$;
VI) é sempre $A \cap (\mathfrak{C} - A) = \emptyset$ e $A \cup (\mathfrak{C} - A) = \mathfrak{C}$;
VII) supondo $A \cap B = \emptyset$, conclui-se $A \subseteq \mathfrak{C} - B$, e reciprocamente;
VIII) supondo $A \cup B = \mathfrak{C}$, conclui-se $A \supseteq \mathfrak{C} - B$, e reciprocamente.

Muitas outras igualdades e inclusões poderiam indicar-se. Limitamo-nos a dar mais as seguintes:

IX) $A \cap B = B \cap A$ e $A \cup B = B \cup A$;
X) $(A \cup B) \cup C = A \cup (B \cup C)$ e $(A \cap B) \cap C = A \cap (B \cap C)$;
XI) $\mathfrak{C} - (A \cup B) = (\mathfrak{C} - A) \cap (\mathfrak{C} - B)$;
XII) $\mathfrak{C} - (A \cap B) = (\mathfrak{C} - A) \cup (\mathfrak{C} - B)$;
XIII) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
XIV) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Todas as afirmações, de I) a XIV), se provam por um processo comum: se se trata duma igualdade, mostra-se que um elemento do primeiro membro pertence ao segundo, assim como a recíproca; se se trata duma inclusão do tipo $A \subseteq B$, mostra-se que todo o elemento de A pertence a B.

Seja, como exemplo, justificar a igualdade XI), a qual, juntamente com a igualdade XII), constitui o par de relações conhecidas sob o nome de relações de De Morgan.

Para isso, tomemos $a \in \mathfrak{C} - (A \cup B)$, ou seja $a \in \mathfrak{C}, a \notin A \cup B$, e, portanto, $a \notin A, a \notin B$. Será $a \in \mathfrak{C} - A, a \in \mathfrak{C} - B$, consequentemente, $a \in (\mathfrak{C} - A) \cap (\mathfrak{C} - B)$. Recíprocamente, se $a \in (\mathfrak{C} - A) \cap (\mathfrak{C} - B)$, tem-se $a \in \mathfrak{C} - A, a \in \mathfrak{C} - B$, isto é, $a \notin A, a \notin B$, consequentemente, $a \notin A \cup B, a \in \mathfrak{C} - (A \cup B)$, como se deseja.

3) **Aplicações** — Dados dois conjuntos $\mathfrak{C} = \{a, b, c, \cdots\}$ e $\mathfrak{C}' = \{a', b', c', \cdots\}$, suponhamos que, por um certo processo, se faz corresponder a cada elemento $a \in \mathfrak{C}$, duma maneira *unívoca*, um elemento $a' \in \mathfrak{C}'$. Diz-se que, pelo referido processo, se definiu uma *aplicação* φ, de $\mathfrak{C}$ em $\mathfrak{C}'$. O elemento a' diz-se *imagem* de a, sendo habitual escrever $a' = \varphi(a)$. Pode haver elementos de $\mathfrak{C}'$ que não sejam obtidos como imagens de elementos de $\mathfrak{C}$. Quando todos os elementos de $\mathfrak{C}'$ forem imagens, diz-se que φ é uma aplicação de $\mathfrak{C}$ *sobre* $\mathfrak{C}'$.

Se tomarmos $A \subseteq \mathfrak{C}$, escreve-se $A' = \varphi(A) \subseteq \mathfrak{C}'$ para significar o subconjunto de $\mathfrak{C}'$ constituído por todas as imagens dos elementos de A. Em particular, a imagem do subconjunto vazio de $\mathfrak{C}$ é o subconjunto vazio de $\mathfrak{C}'$.

É muito importante o caso duma aplicação *biunívoca* de $\mathfrak{C}$ sobre $\mathfrak{C}'$. Significa-se com isto, não apenas que todos os elementos de $\mathfrak{C}'$

são obtidos como imagem, mas ainda que cada a' é imagem dum único elemento a. Esta última afirmação também se traduz dizendo que, suposto $a \neq b$, é $a' \neq b' = \varphi(b)$, ou que $a' = b'$ arrasta $a = b$. Uma aplicação biunívoca de $\mathfrak{C}$ sobre $\mathfrak{C}'$ recebe, por vezes, o nome de *bijecção*.

Uma aplicação biunívoca dum conjunto sobre si será chamada uma *permutação* ou *transformação* da conjunto. Entre as transformações distinguiremos a *transformação identidade*, que aplica cada elemento em si mesmo.

Sempre que dois conjuntos se podem aplicar um sobre o outro de modo biunívoco, diz-se que os conjuntos têm a mesma *potência* (são equivalentes) ou que têm o mesmo *número cardinal* (são equicardinais).

Regressemos a $a' = \varphi(a)$. Podemos dizer que a é um *objecto, original* de a'. O símbolo $\varphi^{-1}(A')$ representará, duma maneira geral, a totalidade dos elementos originais dos elementos de A'. Recebe o nome de *imagem completa inversa* de A'. A este respeito, convém observar que φ^{-1} não é uma aplicação de $\mathfrak{C}'$ em $\mathfrak{C}$, pois pode haver elementos de $\mathfrak{C}'$ sem original em $\mathfrak{C}$, assim como pode a' ter vários originais.

Se, porém, φ é uma aplicação biunívoca de $\mathfrak{C}$ sobre $\mathfrak{C}'$, φ^{-1} é igualmente uma aplicação biunívoca de $\mathfrak{C}'$ sobre $\mathfrak{C}$. Neste caso, diz-se que φ^{-1} é a *aplicação inversa* de φ.

Igualdades e inclusões fáceis de demonstrar, nas quais intervêm φ e φ^{-1}, são as seguintes:

$$\begin{aligned} &\varphi(A \cup B) = \varphi(A) \cup \varphi(B), && \varphi^{-1}(A' \cup B') = \varphi^{-1}(A') \cup \varphi^{-1}(B'), \\ &\varphi(A \cap B) \subseteq \varphi(A) \cap \varphi(B), && \varphi^{-1}(A' \cap B') = \varphi^{-1}(A') \cap \varphi^{-1}(B'), \\ &\varphi(\mathfrak{C} - A) \supseteq \mathfrak{C}' - \varphi(A), && \varphi^{-1}(\mathfrak{C}' - A') = \mathfrak{C} - \varphi^{-1}(A'). \end{aligned}$$

A inclusão $\varphi(\mathfrak{C} - A) \supseteq \mathfrak{C}' - \varphi(A)$ implica que se trate duma aplicação sobre $\mathfrak{C}'$. Com essa hipótese, também se tem $\varphi(\varphi^{-1}(A')) = A'$, enquanto que é sempre $\varphi^{-1}(\varphi(A)) \supseteq A$.

Vamos referir-nos ainda a outro simbolismo que é usado com grande frequência. A aplicação φ, de $\mathfrak{C}$ em $\mathfrak{C}'$, será muitas vezes representada por letras maiúsculas Q, S, T, V, etc., ou, mesmo, A, B, C, escrevendo-se

$$a \to a\,T = a', \qquad [a\,T = \varphi(a)].$$

No caso de T significar uma transformação, poremos também

$$a' \to a'\,T^{-1} = a, \qquad [a'\,T^{-1} = \varphi^{-1}(a')].$$

Digamos ainda que as letras maiúsculas em questão podem encontrar-se afectadas de índices, tanto superiores como inferiores. Claramente que, em todos os casos, uma igualdade do tipo $a\,T = a\,S$, válida para todos os elementos $a \in \mathfrak{C}$, se interpreta escrevendo $T = S$.

Se $\mathfrak{C}'' = \{a'', b'', c'', \cdots\}$ é um terceiro conjunto e S uma aplicação de $\mathfrak{C}'$ em $\mathfrak{C}''$, definiremos um *produto* TS de duas aplicações que leva de $\mathfrak{C}$ a $\mathfrak{C}''$, segundo o esquema: $a \to a\,T = a' \to a'\,S = a'' = (a\,T)\,S = a(TS)$, podendo escrever-se, muito simplesmente, $a'' = a\,T\,S$.

Como caso particular, tomemos $\mathfrak{C} = \mathfrak{C}' = \mathfrak{C}''$. Fica definido o produto de aplicações dum conjunto em si Assim, por exemplo, se T for uma transformação, tem-se

$$a\,T\,T^{-1} = a\,T^{-1}\,T = a = a\,I,$$

onde I é a transformação identidade. É igualmente de interesse fixar desde já a igualdade seguinte, relativa a transformações:

$$(S\,T)^{-1} = T^{-1}\,S^{-1}.$$

OBSERVAÇÃO: Se φ é uma aplicação de $\mathfrak{C}$ em $\mathfrak{C}'$, diz-se, muitas vezes, que $\varphi(A)$ é a *restrição* a A da aplicação φ. Utilizando um *argumento* ξ, de tal modo que, escrevendo $\varphi(\xi)$, em vez de φ, se significa que o referido argumento percorre o *domínio* $\mathfrak{C}$, então, em lugar de $\varphi(A)$, pode designar-se por $\varphi_A(\xi)$ a restrição em causa. Por sua vez, $\varphi(\xi)$ diz-se *extensão* de $\varphi_A(\xi)$.

4) **Relações**—Tomemos o conjunto $\mathfrak{C} = \{a, b, c, \cdots, t, v, \cdots, x, y, z, \cdots\}$ e formemos, seguidamente, um conjunto de pares da forma

$$\mathfrak{D} = \{(a, b); (a, t); \cdots; (x, y); (t, z); \cdots\}. \tag{1}$$

Diz-se, então, que se introduziu em $\mathfrak{C}$ uma *relação*. O elemento a, por exemplo, está em relação com b e com t; o elemento x está em relação com y, etc. Em $\mathfrak{D}$, considera-se $(a, b) \neq (b, a)$, se, porven-

tura, $(b,a)\in\mathfrak{D}$. Representando por α a relação definida em (1), escrever-se-á $x\alpha y$ para significar que x e y estão na relação α, isto é, que $(x,y)\in\mathfrak{D}$.

Diz-se que α gosa da propriedade *reflexiva*, se, para cada $x\in\mathfrak{C}$, valer $x\alpha x$. A relação α será *simétrica*, se, sempre que $x\alpha y$, também se tem $y\alpha x$. Finalmente, α diz-se *transitiva*, se as hipóteses $x\alpha y$, $y\alpha z$ arrastarem $x\alpha z$.

Uma relação que seja simultâneamente reflexiva, simétrica e transitiva diz-se uma *relação de equivalência*. E os elementos em relação dizem-se *equivalentes*. É válido este

TEOREMA: *Se, num conjunto* $\mathfrak{C}$, *tivermos uma relação de equivalência, podemos dividir o conjunto em classes de elementos equivalentes, verificando as seguintes propriedades:* I') *um elemento do conjunto pertence a uma das classes;* II') *duas classes são sempre disjuntas.* Seja ρ a relação em causa. Visto que $a\rho a$, o elemento a figura numa classe C_a, de elementos equivalentes a a. Dada uma segunda classe C_b, que contém o elemento b, se for $a\in C_b$ (isto é $b\rho a$), vamos ver que $C_a=C_b$. Em primeiro lugar, tendo-se $b\rho a$ é $a\rho b$ e $b\in C_a$. Dado outro elemento $d\in C_b$, por ser $a\rho b$, $b\rho d$, é também $a\rho d$, ou seja $d\in C_a$. A classe C_b estará contida em C_a e esta estará contida naquela. O teorema está provado, precisamente por não poderem existir classes só em parte coincidentes.

O conjunto $\mathfrak{C}'=\{C_a,C_b,\cdots\}$, das classes, diz-se *conjunto cociente* de $\mathfrak{C}$ segundo a relação de equivalência ρ. É um conjunto de partes de $\mathfrak{C}$. Do conjunto $\mathfrak{C}$, passa-se para o conjunto cociente pela aplicação $a\to C_a$, que faz corresponder a cada $a\in\mathfrak{C}$ a classe $C_a\in\mathfrak{C}'$ que contém a. É costume escrever ainda $\mathfrak{C}'=\mathfrak{C}/\rho$.

Inversamente, de toda a aplicação $a\to aT=a'$, dum conjunto $\mathfrak{C}$ num conjunto $\mathfrak{C}'$, deduz-se uma relação de equivalência τ, pondo

$$a\tau b, \text{ se e só se } aT=bT.$$

As classes $C_a,\cdots$ dizem-se *classes de equivalência*; e, escrevendo C_a para representar a classe que contém a, diz-se que a é *representante* da classe. Qualquer elemento da classe pode ser tomado como seu representante.

Para quaisquer relações α e β, introduzidas em $\mathfrak{C}$, definiremos a *intersecção* $\alpha\wedge\beta$, do modo seguinte: $x(\alpha\wedge\beta)y$, se e só se $x\alpha y$ e $x\beta y$. Daqui resulta logo a igualdade $\alpha\wedge\beta=\beta\wedge\alpha$.

A *união* $\alpha\vee\beta$ de duas relações é entendida assim: $x(\alpha\vee\beta)y$, se e só se $x\alpha y$ ou $x\beta y$. Daqui resulta $\alpha\vee\beta=\beta\vee\alpha$.

Ainda se define um *produto* $\alpha\beta$ de duas relações, escrevendo $x(\alpha\beta)y$, se e só se existe z tal que $x\alpha z$, $z\beta y$.

Ver na pág. 39 o que é preciso pôr mais aqui sobre relações.

5) **Conjuntos ordenados** — Um conjunto $\mathfrak{C}=\mathfrak{M}$ diz-se *parcialmente ordenado*, quando para ele estiver singularizada uma relação ρ com as propriedades seguintes: I) para cada $a\in\mathfrak{M}$, é $a\rho a$; II) se for $a\rho b$ e $b\rho a$, tem-se $b=a$ (ou, então, se os elementos dum conjunto se consideram distintos: nunca pode ter-se $a\rho b$ e $b\rho a$); III) se for $a\rho b$ e $b\rho c$, é também $a\rho c$. Em geral, tratando-se de conjuntos parcialmente ordenados, é costume escrever-se $a\leqq b$, em vez de $a\rho b$. E diz-se, então, que a «precede» b e que b «segue» a.

Um conjunto $\mathfrak{C}=\mathfrak{O}\neq\emptyset$ diz-se *ordenado, totalmente ordenado* ou *cadeia*, quando para ele estiver singularizada uma relação ρ com as propriedades seguintes: I') dados $a,b\in\mathfrak{O}$, tem-se sempre uma e uma só das hipóteses $a\rho b$ ou $b\rho a$; II') se $a\rho b$ e $b\rho c$, então $a\rho c$. Em geral, tratando-se de conjuntos ordenados, escreveremos $a<b$, em vez de $a\rho b$.

Um conjunto ordenado $\mathfrak{O}=\mathfrak{B}$ diz-se *bem ordenado*, se cada subconjunto não vazio $A\subseteq\mathfrak{B}$ contiver um *primeiro elemento*, ou seja um elemento a_0 que «precede» todos os elementos do subconjunto ($a_0<a$, para cada $a\in A$, tal que $a\neq a_0$). Um conjunto bem ordenado também se chama um *ordinal*.

Há interesse em fixarmos aqui um certo número de vocábulos e de locuções, que, por vezes, permitirão exprimir-nos de modo simples. Seja $\mathfrak{M}$ um conjunto parcialmente ordenado e tomemos $a,b\in\mathfrak{M}$. Se for $a\leqq b$, com $a\neq b$, também poderemos escrever $a<b$. Dada uma parte $\mathfrak{M}_0\subseteq\mathfrak{M}$, diz-se que $v\in\mathfrak{M}$ é um *majorante* de $\mathfrak{M}_0$, se, para cada $a_0\in\mathfrak{M}_0$, for válido $a_0\leqq v$. O elemento $t\in\mathfrak{M}$ é um *minorante* de $\mathfrak{M}_0$, se, para cada $a_0\in\mathfrak{M}_0$, for $t\leqq a_0$. Claramente que $\mathfrak{M}_0$ é um conjunto parcialmente ordenado para a mesma relação $\leqq$. Um elemento $m\in\mathfrak{M}$ chama-se *máximo*, quando não existe $x\in\mathfrak{M}$ tal que $m<x$. Um elemento $m_0\in\mathfrak{M}$ é *mínimo*, se não existe $x\in\mathfrak{M}$ tal que $x<m_0$.

Se, entre os majorantes de $\mathfrak{M}_0$, existir um majorante v_0 tal que qualquer outro majorante v verifique a condição $v_0<v$, chama-se a v_0 *limite superior* ou *supremo* de $\mathfrak{M}_0$. O *limite inferior* ou *ínfimo* de

$\mathfrak{M}_0$, se existe, é um minorante $t_0 \in \mathfrak{M}$ tal que, para qualquer outro minorante t, se tem $t < t_0$. Os limites superior e inferior de $\mathfrak{M}_0$ podem pertencer ou não a $\mathfrak{M}_0$.

As noções anteriores também se dão para um conjunto ordenado $\mathfrak{O}$. Assim, por exemplo, tomado $\mathfrak{O}_0 \subseteq \mathfrak{O}$, será $v \in \mathfrak{O}$ majorante de $\mathfrak{O}_0$, se, para cada $a_0 \in \mathfrak{O}_0$ tal que $a_0 \neq v$, se tenha $a_0 < v$; e um majorante v_0, de $\mathfrak{O}_0$, será o limite superior de $\mathfrak{O}_0$, se, para cada majorante $v \neq v_0$, for $v_0 < v$.

Imaginemos o conjunto das relações possíveis num conjunto $\mathfrak{C}$. Poremos $\alpha \leqq \beta$, se $x \alpha y$ implicar $x \beta y$. Então, o conjunto das relações em questão constitui um conjunto parcialmente ordenado, verificando-se fàcilmente que $\alpha \vee \beta$ é o limite superior das relações α e β e que $\alpha \wedge \beta$ é o seu ínfimo.

Se introduzirmos a *relação vazia*, ou seja a relação para a qual nenhum elemento está em relação com outro, assim como a *relação um* ou *relação universal*, para a qual todos os elementos estão em relação, verifica-se que a relação vazia precede todas as relações, dizendo-se, por isso, *elemento zero* do conjunto parcialmente ordenado das relações, e que a relação um é precedida por todas as relações, dizendo-se, por isso, *elemento um* do mesmo conjunto. A relação vazia permite se possa dar sempre sentido ao produto $\alpha\beta$ de duas relações.

6) **Produto de conjuntos** — Limitemo-nos aos casos mais simples. Dados dois conjuntos $\mathfrak{C} = \{a, b, c, \cdots\}$ e $\mathfrak{C}' = \{a', b', c', \cdots\}$, que podem ou não ser distintos, diz-se *produto* ou *produto cartesiano* dos dois conjuntos o conjunto dos pares ordenados (a, a'); (b, b'); etc. Escreve-se

$$\mathfrak{C} \times \mathfrak{C}' = \{(a, a'); (a, b'); (b, a'); (b, b'); \cdots\}.$$

Se for $A \subseteq \mathfrak{C}$ e $A' \subseteq \mathfrak{C}'$, é imediato que $A \times A' \subseteq \mathfrak{C} \times \mathfrak{C}'$. Recìprocamente, esta inclusão implica $A \subseteq \mathfrak{C}$, $A' \subseteq \mathfrak{C}'$. E, no caso particular de ser $\mathfrak{C} = \phi$ ou $\mathfrak{C}' = \phi$, é $\mathfrak{C} \times \mathfrak{C}' = \phi$. Recìprocamente, esta última igualdade implica que um dos factores seja o conjunto vazio.

Tomado um novo conjunto $\mathfrak{C}'' = \{a'', b'', c'', \cdots\}$, há lugar para se considerar um produto

$$(\mathfrak{C} \times \mathfrak{C}') \times \mathfrak{C}'' = \{((a, a'), a''); \cdots; ((b, a'), c''); \cdots\}.$$

Como existe uma correspondência biunívoca completa entre os sistemas $(a, b'), c'')$, e os sistemas $(a, (b', c''))$ e entre qualquer destes sistemas

e o sistema (a, b', c''), o produto anterior considera-se *associativo*, e escreve-se

$$(\mathfrak{C} \times \mathfrak{C}') \times \mathfrak{C}'' = \mathfrak{C} \times (\mathfrak{C}' \times \mathfrak{C}'') = \mathfrak{C} \times \mathfrak{C}' \times \mathfrak{C}''.$$

No mesmo sentido daquele em que acabamos de estabelecer a associatividade, pode admitir-se que o *produto é comutativo*: $\mathfrak{C} \times \mathfrak{C}' = \mathfrak{C}' \times \mathfrak{C}$.

Imaginemos definida uma relação α num conjunto $\mathfrak{C}$. Se $a \alpha b$, isto é, se a e b estão na relação α, podemos simbolizar também esse facto, como dissemos em (I, 1, 4), por meio da representação (a, b). Neste sentido, dar uma relação em $\mathfrak{C}$, é dar um subconjunto do produto $\mathfrak{C} \times \mathfrak{C}$.

Designando, duma maneira geral, pelo símbolo $P(\mathfrak{C})$, o conjunto formado pela totalidade dos subconjuntos de $\mathfrak{C}$, podemos usar a linguagem seguinte: dar uma relação α, em $\mathfrak{C}$, é dar um elemento $A_\alpha \in P(\mathfrak{C} \times \mathfrak{C})$. Com esta notação, torna-se fácil verificar que

$$A_{\alpha \wedge \beta} = A_\alpha \cap A_\beta, \quad A_{\alpha \vee \beta} = A_\alpha \cup A_\beta,$$

onde, bem entendido, o elemento $A_{\alpha \wedge \beta} \in P(\mathfrak{C} \times \mathfrak{C})$, por exemplo, é aquele elemento que se compõe dos elementos da intersecção dos dois subconjuntos de $\mathfrak{C}$ que constituem, respectivamente, A_α e A_β.

§ 2. Os números naturais

1) **Postulados e operações** — Um conjunto $\mathfrak{C} = \mathfrak{N}$ diz-se um conjunto de *números naturais*, se nele forem realizados os axiomas de PEANO: I) existe um número natural chamado *um* e representado por 1; II) cada número natural a tem um *sucessor* a', que é um número natural; III) o número 1 não é sucessor de qualquer número natural; IV) os sucessores a' e b', suposto $a \neq b$, são números naturais distintos; V) é válido o *princípio da indução completa*, assim enunciado: se um conjunto $\mathfrak{N}_0 \subseteq \mathfrak{N}$ contém 1, e com cada $a \in \mathfrak{N}_0$, contém a', então é $\mathfrak{N}_0 = \mathfrak{N}$.

O princípio da indução completa prova imediatamente que todo o número natural $\neq 1$ é sucessor dum elemento. Basta, com efeito, considerar o subconjunto $\mathfrak{N}_0$ formado por 1 e pelos números naturais que são sucessores dum número natural. Vê-se que $\mathfrak{N}_0 = \mathfrak{N}$.

Introduzir uma *operação* num conjunto é dar um processo pelo qual, dum par ordenado (a, b) de elementos de $\mathfrak{C}$, se deduz, de modo unívoco, um elemento $c \in \mathfrak{C}$. É frequente designar-se a operação por *soma*, escrevendo-se, então, $a+b=c$, ou por *produto*, escrevendo-se, então, $a \cdot b = c$, ou, mais simplesmente ainda, $ab = c$.

No conjunto $\mathfrak{N}$ dos números naturais, definiremos uma soma pelas duas igualdades seguintes:

$$a + 1 = a', \quad a + b' = (a + b)'.$$

A soma fica, efectivamente, bem definida, por sabermos somar um elemento qualquer com outro elemento qualquer. Ela gosa das propriedades seguintes:

I') é *associativa*: $(a+b)+c = a+(b+c)$;
II') é *comutativa*: $a + b = b + a$;
III') de $a + b = a + c$, deduz-se $b = c$ (lei de *corte*).

Demonstremos, por exemplo, a propriedade comutativa, admitindo ter-se já provado a propriedade associativa (o que se faria tendo em conta o princípio da indução completa, que aqui vamos também utilizar).

Comecemos por supor $a = 1$. Então

$$1+1=1+1=1'; \text{ e, se } 1+b=b+1=b',$$

é também

$$1+b'=1+(b+1)=(1+b)+1=b'+1.$$

Admitindo agora que se tem $a + b = b + a$, vamos mostrar que é $a' + b = b + a'$. Ora

$$a'+b=(1+a)+b=1+(a+b)=1+(b+a)=(1+b)+a= \\ =(b+1)+a=b+(1+a)=b+a'.$$

De modo análogo se define um produto em $\mathfrak{N}$, por meio das igualdades

$$a \cdot 1 = a, \quad a \cdot b' = ab + a.$$

O produto gosa das propriedades seguintes: Deverá ser:

I'') é *associativo*: $ab \cdot c = a \cdot bc$; — I'') é distributivo à direita $(a+b)c = ac+bc$;
II'') é *comutativo*: $ab = ba$; — II'') é comutativo: $ab = ba$;
III'') é *distributivo*: $a \cdot (b + c) = ab + ac$; — III'') $ab \cdot c = a \cdot bc$;
IV'') de $ac = bc$, deduz-se $a = b$, (lei de *corte*). — IV'') de $ac = bc$, deduz-se $a = b$.

Demonstremos, por exemplo, a propriedade distributiva. Pondo $a = 1$, tem-se

$$1 \cdot (b + c) = (b + c) \cdot 1 = b + c = b \cdot 1 + c \cdot 1 = 1 \cdot b + 1 \cdot c,$$

pois que a comutatividade do produto se supõe estabelecida. Em seguida, supondo $a \cdot (b + c) = ab + ac$, vem

$$a' \cdot (b+c) = (b+c)a' = (b+c)a + (b+c) = (ba+ca) + (b+c) = \\ = (ba+b) + (ca+c) = ba' + ca' = a'b + a'c.$$

2) **Ordenação dos números naturais** — A operação de soma vai permitir-nos introduzir em $\mathfrak{N}$ uma ordenação, por forma que os números naturais constituam uma cadeia. Para isso, poremos $a < b$, sempre que exista c por forma que se tenha $b = a + c$. Desta definição resulta logo não poder ter-se simultâneamente $a < b$ e $b < a$. De facto, se fosse $b = a + c$, $a = b + d$, seria também $b = b + (d + c) = b + k$, se $d + c = k$. Então, $b + 1 = (b + k) + 1 = b + (k + 1)$, o que implicaria $1 = k + 1$, que não pode ter lugar. Resta ver que, dados dois números naturais a e b, ou é $a < b$ ou $b < a$. Na verdade, tomemos a e consideremos o conjunto $\mathfrak{N}_0$ de números naturais nas seguintes condições: pertencem a $\mathfrak{N}_0$ o número a, os números que precedem a (também designados *menores* que a) e os números que são precedidos por a (também designados *maiores* que a ou que «seguem» a). O número 1 pertence a $\mathfrak{N}_0$, visto que, ou é $a = 1$, ou de, contrário, é $a = (a_0)' = a_0 + 1 = 1 + a_0$, o que implica $1 < a$. E, se um número b pertence a $\mathfrak{N}_0$, o mesmo se diz de b', pelo seguinte: se é $b = a$, então $b' = a + 1$, $a < b'$; sendo $b \neq a$, é, por exemplo, $b < a$, ou seja $a = b + b_0$; nesse caso, ou $b_0 = 1$ e $b' = a$, ou $b_0 = k + 1$ e $a = b + (k + 1) = (b + 1) + k$, isto é $b' < a$. A hipótese $a < b$ tratar-se-ia anàlogamente. Vê-se assim que é $\mathfrak{N}_0 = \mathfrak{N}$, pelo que $\mathfrak{N}$ é um conjunto ordenado, pois que a transitividade do sinal $<$ é imediata. Na ordenação em causa o número 1 precede qualquer número natural.

O sinal $<$ também gosa das propriedades que passamos a indicar:

I''') de $a < b$, conclui-se $a + c < b + c$;
II''') de $a < b$, conclui-se $ac < bc$;
III''') não pode ter-se $a < b < a + 1$.

A validade de III''') permite dar à noção abstracta de «sucessor», atrás introduzida, o sentido usual: não existe $b \in \mathfrak{N}$ tal que $a<b<a'$, ou seja não existe número natural «entre» a e b. Tendo em conta o princípio da indução completa, podemos afirmar que é

(I) $$\mathfrak{N} = \{1, 1', (1')', ((1')')', \cdots\}.$$

É importante a afirmação seguinte:

TEOREMA DE BOA ORDENAÇÃO: *Todo o conjunto não vazio de números naturais tem primeiro elemento.* Seja $\mathfrak{N}_0$ o conjunto em questão. Se $1 \in \mathfrak{N}_0$, será 1 o primeiro elemento de $\mathfrak{N}_0$. Supondo $1 \notin \mathfrak{N}_0$, vamos considerar o conjunto B daqueles números naturais que precedem todos os números de $\mathfrak{N}_0$. O conjunto B não é vazio, pois que $1 \in B$; e também não é igual a $\mathfrak{N}$, porque os elementos de $\mathfrak{N}_0$ não pertencem a B. Existe, deste modo, um número $t \in B$ tal que é $t' \notin B$. Por consequência, existe $v_0 \in \mathfrak{N}_0$ tal que $t < v_0$, sem que se tenha $t' < v_0$. Ou é, pois, $t' = v_0$, ou é $t' = v_0 + k$. Esta última hipótese não pode realizar-se, como se conclui de não poder ter-se $t < v_0 < t'$. Assim, é $v_0 = t + 1$. Para qualquer $v \in \mathfrak{N}_0$, é agora $v = t + n$. Ou se tem $n=1$, $v=v_0$, ou é $n=x+1$, o que dá $v=(t+1)+x=v_0+x$, $v_0 < v$. O teorema está completamente demonstrado.

O princípio da indução completa pode substituir-se, para efeito das suas utilizações, pelo enunciado seguinte: um conjunto $\mathfrak{N}_0$ de números naturais que, contendo os números naturais que precedem n, também contém n, é igual ao conjunto de todos os números naturais. De facto, $\mathfrak{N}_0$ não é vazio, porque, estando o conjunto vazio contido em qualquer conjunto, $\mathfrak{N}_0$ contém o conjunto dos números naturais que precedem 1, pelo que será $1 \in \mathfrak{N}_0$. Em seguida, designemos por $\mathfrak{N}_1$, o conjunto dos números naturais que não pertencem a $\mathfrak{N}_0$. Se esse conjunto for vazio, a afirmação está provada. Se o não fosse, teria, pelo teorema da boa ordenação, um elemento «mínimo» n_1. Todos os números naturais que precedessem n_1 pertenceriam a $\mathfrak{N}_0$. Então, seria $n_1 \in \mathfrak{N}_0$, o que é uma contradição. Logo, o conjunto $\mathfrak{N}_1$ é vazio, tendo-se $\mathfrak{N}_0 = \mathfrak{N}$. O enunciado referido costuma designar-se por *segundo princípio de indução completa.*

Em vez da representação dos números naturais indicada em (I), utilizaremos esta outra:

(II) $$\mathfrak{N} = \{1, 2, 3, 4, \cdots, n, \cdots\}.$$

O segundo princípio de indução completa justifica um modo importante de *definir* ou *realizar* (ou *construir*) uma aplicação ψ do conjunto dos números naturais $\mathfrak{N}$ noutro conjunto. Suponhamos que é dado um sistema de *relações de recorrência*, nas condições seguintes: o sistema de relações liga $\psi(b)$ aos $\psi(a)$, para os quais $a < b$; então, determina unìvocamente $\psi(b)$, sempre que se supõe que os $\psi(a)$ já foram escolhidos compatìvelmente por via das referidas relações, isto é, são tais que, tomado $\psi(b_0)$, com $b_0 < b$, $\psi(b_0)$ é o mesmo que o que seria determinado pelas relações, por via dos $\psi(a)$ conhecidos, para os quais $a < b_0$. Desta maneira, o sistema de relações de recorrência que, em particular, determina unìvocamente $\psi(1)$, [em geral uma das relações consiste em dar $\psi(1)$], define a aplicação ψ. É o que resulta imediatamente, com efeito, do segundo princípio de indução completa.

3) **Sobre os números cardinais** — No conjunto (II) do número anterior, chamaremos *secção* de $\mathfrak{N}$ uma parte de $\mathfrak{N}$ que se componha exactamente dum número n e de todos os números que precedem n. Representaremos por S_n essa secção. Um conjunto diz-se *finito* e de cardinalidade n, se for equipotente de S_n. Para os conjuntos finitos é válido o seguinte

TEOREMA FUNDAMENTAL: *Um conjunto finito* $\mathfrak{C}$ *não pode ser equipotente de uma sua parte própria.* Suponhamos que o conjunto $\mathfrak{F} = \mathfrak{F}_1 = \{f_1\}$ é parte própria dum conjunto $\mathfrak{C} = \{f_1, f_2, \cdots, f_i\}$. Neste caso, não pode ter-se $\varphi(\mathfrak{F}) = \varphi(\mathfrak{F}_1) = \mathfrak{C}$, visto que $\varphi(f_1)$, pelo facto de φ ser uma aplicação, não pode ser igual a vários elementos. Assim, o teorema é válido para as partes próprias com um só elemento. Vamos admiti-lo para as partes próprias $\mathfrak{G} = \mathfrak{G}_n = \{g_1, \cdots, g_n\}$, com n elementos, e demonstrá-lo para as partes próprias $\mathfrak{H} = \mathfrak{H}_{n+1} = \{h_1, \cdots, h_n, h_{n+1}\}$, com $n+1$ elementos. Se pudesse ter-se

$$\psi(\mathfrak{H}) = \{h_1, h_2, \cdots, h_{n+1}, h_{n+2}, \cdots, h_i\},$$

seria, por exemplo, $\psi(h_{n+1}) = h_{n+2}$. Então, por meio de ψ, obter-se-ia $\psi(\{h_1, \cdots, h_n\}) = \{h_1, h_2, \cdots, h_n, h_{n+1}, \cdots\}$, o que não tem lugar, por hipótese. Se fosse, porém, $\psi(h_{n+1}) = h \neq h_{n+2}$, suponhamos $\psi(h_i) = h_{n+2}$, com i igual a um dos números $1, 2, \cdots, n$. Poderíamos definir uma aplicação θ, de $\mathfrak{H}_{n+1}$ em $\theta(\mathfrak{H}_{n+1}) = \psi(\mathfrak{H}_{n+1})$, que coincidiria com ψ em todos os h_j, salvo que daria $\theta(h_{n+1}) = h_{n+2}, \theta(h_i) = h$. Para esta

aplicação θ, a contradição anteriormente encontrada voltaria a repetir-se. O teorema está, portanto, demonstrado.

Consideremos, de novo, o conjunto $\mathfrak{N}$ dos números naturais. Uma aplicação biunívoca completa de $\mathfrak{N}$ em $\mathfrak{N}_0 = \{2, 3, 4, \cdots\}$ é por exemplo, a seguinte: $\varphi(n) = n'$. Por isso, $\mathfrak{N}$ não é um conjunto finito. Chamaremos conjunto *infinito*, todo aquele que não for finito. $\mathfrak{N}$ é, pois, um conjunto infinito.

Os conjuntos que têm a mesma potência ou cardinalidade de $\mathfrak{N}$, ou de uma secção, S_n, de $\mathfrak{N}$, dizem-se *numeráveis*. É costume utilizar o símbolo $\aleph_0$ para significar o cardinal de $\mathfrak{N}$.

É imediato que o conceito de igualdade de potências é transitivo. Resulta daí que um conjunto infinito nunca pode ter a cardinalidade dum conjunto finito.

Dados dois conjuntos finitos quaisquer, $\mathfrak{C}$ e $\mathfrak{D}$, se eles tiverem, respectivamente, as potências de S_m e de S_n, diremos que a cardinalidade de $\mathfrak{C}$ é *inferior* à de $\mathfrak{D}$, e a deste superior à de $\mathfrak{C}$, se for $m < n$. Para dois conjuntos finitos $\mathfrak{C}$ e $\mathfrak{D}$, o problema da *tricotomia* resolve-se pela positiva: 1) ou a cardinalidade de $\mathfrak{C}$ é inferior à de $\mathfrak{D}$; 2) ou $\mathfrak{C}$ e $\mathfrak{D}$ têm a mesma cardinalidade; 3) ou a cardinalidade de $\mathfrak{C}$ é superior à de $\mathfrak{D}$.

O problema da tricotomia também se põe para conjuntos quaisquer, resolvendo-se igualmente pela positiva. Dessa solução e de muitas outras questões da teoria dos conjuntos nos ocuparemos noutro lugar.

Neste momento, limitamo-nos a fazer a seguinte anotação: o conjunto das partes dum conjunto $\mathfrak{C}$, já representado por $P(\mathfrak{C})$, tem uma cardinalidade superior à de $\mathfrak{C}$. Isto significa que é possível definir uma correspondência biunívoca entre $\mathfrak{C}$ e um subconjunto próprio de $P(\mathfrak{C})$, sem que haja a possibilidade da inversa: de definir uma correspondência biunívoca entre $P(\mathfrak{C})$ e uma parte (própria ou imprópria) de $\mathfrak{C}$.

BIBLIOGRAFIA

N. Bourbaki, *Théorie des ensembles* (fascicule de résultats), Paris, 1951.

———, *Théorie des ensembles*, chapitres I et II, Paris, 1954.

H. Hermes, *Einführung in die Verbandstheorie*, Berlin, 1955.

B. van der Waerden, *Moderne Algebra*, erster Teil, Berlin, 1930.

A. Fraenkel, *Einleitung in die Mengenlehre*, New York, 1946.

P. Dubreil, *Algèbre*, Paris, 1954.

CAPÍTULO II

Grupoides e semi-grupos. Primeiros teoremas sobre grupos

§ 1. Grupoides e semi-grupos

1) **Definição de grupoides** — Se $\mathfrak{C}$ é um conjunto não vazio, consideremos o produto $\mathfrak{C} \times \mathfrak{C}$ e uma aplicação deste produto no próprio conjunto $\mathfrak{C}$. A cada par ordenado $(a, b) \in \mathfrak{C} \times \mathfrak{C}$ faz-se corresponder, de modo unívoco, um elemento $c \in \mathfrak{C}$. Escreveremos $a \cdot b = c$, para significar a aplicação em causa, e diremos, como já referimos em (I, 2, 1), que, sobre o *suporte* $\mathfrak{C}$, se definiu uma *operação binária* ou um *produto* de cada par ordenado de elementos. O conjunto $\mathfrak{C}$, dotado desta operação, passa a constituir um *espaço algébrico*, que designaremos por *grupoide*. Com o simbolismo $\mathfrak{S} = (\mathfrak{C}/\cdot)$, significaremos «grupoide $\mathfrak{S}$, sobre o suporte $\mathfrak{C}$, dotado da operação $\cdot$». De modo análogo se interpretarão igualdades como as seguintes: $\mathfrak{S} = (\mathfrak{D}/\circ)$, $\mathfrak{T} = (\mathfrak{H}/\times)$, etc. Pode, na verdade, haver conveniência em representar por outros sinais a operação introduzida para «algebrizar» conjuntos $\mathfrak{C}, \mathfrak{D}$, etc., de modo a formar diferentes grupoides. E pode até acontecer que o grupoide seja indicado, sem referência ao sinal da operação.

Tomemos $\mathfrak{S} = (\mathfrak{C}/\cdot)$. Diremos que $e \in \mathfrak{S}$ será *unidade esquerda*, quando $e \cdot a = a$, qualquer que seja $a \in \mathfrak{S}$. Uma *unidade direita*,

excepcionalmente representada pela letra grega ε, satisfaz a $a \cdot \varepsilon = a$, para cada a. Uma *unidade bilateral* u verifica as condições $u \cdot a = a \cdot u = a$. Sempre que haja e e ε, do facto de se ter $e \cdot \varepsilon = \varepsilon = e$ resulta a igualdade das duas unidades. Então, $e = \varepsilon$ é unidade bilateral. Uma unidade bilateral também se chama *identidade*.

Fixemos $a \in \mathfrak{S}$ e seja x um elemento qualquer de $\mathfrak{S}$. O facto de ser $x \cdot a$ (ou, mais simplesmente, xa) um elemento variável, bem determinado para cada x, mostra que, pondo $y = xa$, se define, por via de a, uma aplicação $A_a^{(d)}$, de $\mathfrak{C}$ em $\mathfrak{C}$, segundo o esquema

$$x \to x a = y = x A_a^{(d)}.$$

A notação $A_a^{(d)}$, utilizada para, de harmonia com (I, 1, 3), representar a aplicação em causa, lembra: 1) por intermédio da letra A, que se trata de uma aplicação; 2) por intermédio da letra a, que tal aplicação é definida pelo elemento a; 3) por intermédio da letra d, que o elemento a é «multiplicador», à direita, dos elementos de $\mathfrak{S}$.

De modo análogo se tem uma aplicação

$$x \to a x = y = x A_a^{(e)},$$

onde agora o índice superior e, em $A_a^{(e)}$, lembra que a é «multiplicador», à esquerda.

Se $A_a^{(d)}$ é uma transformação ou permutação de $\mathfrak{C}$, no sentido referido em (I, 1, 3), diz-se que a é um elemento *não singular à direita*; se $A_a^{(e)}$ é uma transformação de $\mathfrak{C}$, diz-se que a é *não singular à esquerda*. Um elemento diz-se *não singular*, se for não singular à direita e à esquerda. Por exemplo: uma unidade esquerda é não singular à esquerda; a transformação que ela define é a transformação identidade.

EXEMPLO DE GRUPOIDE: Como exemplo de grupoide, lembremos o conjunto das aplicações dum conjunto em si, segundo a regra de produto indicada em (I, 1, 3). Uma parte das aplicações é constituída pelas transformações. Entre estas últimas, a transformação identidade é unidade bilateral do grupoide.

As aplicações dum conjunto em si gosam da propriedade expressa na igualdade seguinte: $(x P)(Q R) = [x(P Q)] R$. De facto, ambos os membros são iguais a $((x P) Q) R$. Por isso se escreve $P(QR) = (P Q) R = P Q R$, o que se exprime dizendo que é válida a *propriedade associativa* para o produto $P Q$. Mais geralmente: o produto de aplicações sucessivas de conjuntos noutros conjuntos é associativo.

O grupoide $\mathfrak{S}$ diz-se *comutativo*, se se tiver $a \cdot b = b \cdot a$ ou $a A_b^{(d)} = a A_b^{(e)}$. A comutatividade caracteriza-se, assim, pela igualdade $A_x^{(d)} = A_x^{(e)}$, para cada $x \in \mathfrak{S}$.

Os números naturais, estudados em (I, 2), dão um exemplo importante de grupoide (associativo e comutativo), tanto relativamente à soma como relativamente ao produto.

2) **Grupoides associativos** — Encontrámos no número anterior grupoides associativos. Dado o grupoide $\mathfrak{S} = (\mathfrak{C}/\cdot)$, diremos precisamente que $\mathfrak{S}$ é um *semi-grupo*, se tiver lugar a propriedade associativa: $a(bc) = (ab)c$.

São muito importantes algumas relações que vamos demonstrar, tendo apenas em conta a propriedade associativa. Do facto de ser $a(bc) = (ab)c$, resulta podermos escrever simplesmente abc, para representarmos o valor comum dos dois membros da igualdade, o que, de resto, assinalámos já no número anterior, no caso particular de semi-grupo aí considerado.

Duma maneira geral, vamos ver que tem sentido escrever $a_1 a_2 \cdots a_n$ como produto de n elementos, pela razão de que todas as possíveis interpretações do símbolo $a_1 a_2 \cdots a_n$ levam ao mesmo resultado. Já vimos que assim é com o símbolo $a_1 a_2 a_3$. Imaginemos, em seguida, que interpretamos o símbolo em estudo pela seguinte lei de indução:

$$a_1 a_2 \cdots a_{n-1} a_n = (a_1 a_2 \cdots a_{n-1}) a_n .$$

Vamos provar que, se supusermos,

$$A = a_1 \cdots a_n , \qquad B = a_{n+1} \cdots a_p , \qquad (p \leqslant n+1),$$

é, de facto,

$$A B = a_1 a_2 \cdots a_p . \tag{1}$$

Para $p = n+1$, ou seja $B = a_{n+1}$, tem-se $A B = (a_1 \cdots a_n) a_{n+1} = a_1 \cdots a_{n+1} = a_1 \cdots a_p$. Admitamos que a igualdade (1) está provada para $p = n+k-1$, $k \geqslant 2$; demonstrá-la-emos para $p = n+k$. Ponhamos $B' = a_{n+1} \cdots a_{n+k-1}$. Tem-se $A B' = a_1 \cdots a_{n+k-1}$, por hipótese. Escrevamos, depois, $A B' \cdot a_{n+k} = A \cdot B' a_{n+k}$, onde o uso do ponto

dispensa o uso do parêntesis. Como $B' a_{n+k} = a_{n+1} \cdots a_{n+k-1} \cdot a_{n+k} = a_{n+1} \cdots a_{n+k} = B$, vê-se que $A B' \cdot a_{n+k} = A B$. Por outro lado, $A B' \cdot a_{n+k} = a_1 \cdots a_{n+k-1} \cdot a_{n+k} = a_1 \cdots a_{n+k}$. Assim, como se deseja, $A B = a_1 a_2 \cdots a_{n+k}$.

Suponhamos, em seguida, que os *factores* do produto $a_1 a_2 \cdots a_n$ são todos iguais entre si e iguais a a. Poremos $a_1 \cdots a_n = a^n$. Desta definição resultam fàcilmente as igualdades

$$a^m \cdot a^n = a^{m+n}, \qquad (a^m)^n = a^{mn}, \qquad \text{[illegible]}$$

que se provam por indução. Tratemos a última, suposta provada a anterior. Se fôr $n=1$, temos $(a^m)^1 = a^m = a^{m \cdot 1}$ e a afirmação é verdadeira. Admitamos agora a igualdade para n e demonstremo-la para $n+1$. É

$$(a^m)^{n+1} = (a^m)^n \cdot (a^m)^1 = a^{mn} \cdot a^m = a^{mn+m} = a^{m(n+1)}.$$

3) **Grupoides de elementos não singulares** — Se o grupoide $(\mathfrak{Q} / \cdot)$ se compõe apenas de elementos não singulares, as aplicações $A_a^{(d)}$ e $A_a^{(e)}$ serão transformações e representar-se-ão por $T_a^{(d)}$ e $T_a^{(e)}$, respectivamente. Um tal grupoide diz-se um *quase-grupo*. Fixemos, pois:

1.º SISTEMA DE POSTULADOS PARA QUASE-GRUPOS: Q_1) a cada elemento $a \in \mathfrak{Q}$ estão associadas duas transformações $T_a^{(d)}$ e $T_a^{(e)}$; Q_2) tem lugar a igualdade $x T_a^{(d)} = a T_x^{(e)}$, na qual o valor comum dos dois membros é o produto $x a$.

Outras definições de quase-grupos estão contidas nos dois sistemas seguintes de postulados.

2.º SISTEMA DE POSTULADOS: Q'_1) há, em $\mathfrak{Q}$, um produto $a \cdot b$ de cada par ordenado de elementos; Q'_2) as equações $x \cdot a = b$, $a \cdot y = b$ são solúveis e têm uma única solução.

3.º SISTEMA DE POSTULADOS: Q''_1) trata-se dum conjunto $\mathfrak{Q}$ para o qual, posta a igualdade $a \cdot b = c$, é possível determinar, duma maneira única, um dos elementos, conhecidos os outros dois.

As transformações $T_a^{(d)}$ e $T_a^{(e)}$ têm aqui uma particularidade que convém assinalar: se se tiver $x T_a^{(d)} = x T_b^{(d)}$, para único elemento x, [illegible]

já se tem $a = b$. De facto, a hipótese leva a $a T_x^{(e)} = b T_x^{(e)}$; então, $a = b$, dado que $T_x^{(e)}$ leva de elementos diferentes a elementos diferentes.

Um quase-grupo com identidade diz-se um *loop*.

4) **Regularidade** — Tomemos um semi-grupo com identidade u. Nesse caso, a noção de elementos não singulares, aludida em (II, 1, 1), presta-se a uma interpretação a que vamos referir-nos. Suponhamos a e a' elementos dum semi-grupo com identidade e tais que $a a' = u$. Diremos, então, que a é *regular à direita* e que a' é o seu *inverso direito*; e também diremos que a' é *regular à esquerda*, sendo a o seu *inverso esquerdo*. Um elemento que seja regular à direita e à esquerda é chamado *regular*. Supondo a regular, tem-se, por exemplo, $a a' = u$, $a'' a = u$. Da primeira igualdade tira-se $a'' \cdot (a a') = a'' = (a'' a) \cdot a' = u a' = a'$. Assim, quando um elemento é regular, o seu inverso direito é igual ao seu inverso esquerdo. Diz-se, nesse caso, que o elemento a tem *inverso* e representa-se este por a^{-1}.

Quando um elemento a é regular à direita, a equação $a y = b$ é solúvel, tendo, pelo menos, a solução $a' b$ (se a' é o inverso direito de a). Não podemos afirmar que a solução seja única. Relativamente à equação $x a = b$, a situação é inversa: *se for solúvel*, a solução é única, pois que, de $xa = x'a$, se deduz $(xa) \cdot a' = x(aa') = x = (x'a)a' = x'$.

Posto isto, passemos às relações entre regularidade e não singularidade. Se a é não singular à esquerda, $A_a^{(e)} = T_a^{(e)}$ é uma transformação e $(T_a^{(e)})^{-1}$ existe. A equação $ay = b$ tem a solução $y = b(T_a^{(e)})^{-1}$, qualquer que seja b. Em particular, $a y = u$ dá $y = u(T_a^{(e)})^{-1} = a'$, sendo $a a' = u$. *Um elemento não singular à esquerda é regular à direita.* Vamos ver que também é regular à esquerda. Tem-se, efectivamente, $(a' a) T_a^{(e)} = a(a' a) = (a a') a = a$, donde se tira $a' a = a(T_a^{(e)})^{-1} = (a u)(T_a^{(e)})^{-1} = u$. É válido o

TEOREMA 1: *Num semi-grupo com identidade, todo o elemento não singular à esquerda é regular.*

Inversamente, seja a regular, de inverso a^{-1}. Ambas as equações $x a = b$ e $a y = b$ são solúveis e têm uma única solução. A solução da primeira é $b a^{-1}$, a da segunda é $a^{-1} b$. Como b é qualquer, vê-se

que $T_a^{(d)}$ e $T_a^{(e)}$ são transformações, de sorte que a, além de não singular à esquerda, é elemento não singular. Assim:

TEOREMA 2: *Num semi-grupo com identidade, todo o elemento não singular à esquerda (ou à direita) é elemento não singular. Os elementos não singulares são elementos regulares, e recìprocamente.*

Verifica-se que o produto de dois elementos não singulares é um elemento não singular. E, por ser u não singular, podemos afirmar que o conjunto dos elementos regulares dum semi-grupo com identidade é um semi-grupo com identidade (*sub-semi-grupo* daquele, por ser semi-grupo contido nele). Convém observar, de resto, que tem lugar a igualdade $(ab)^{-1} = b^{-1}a^{-1}$, quando a e b são regulares. Por vezes os elementos regulares dum semi-grupo recebem a designação de *unidades*, mas isso não implica que o termo «unidade» seja utilizado nesse único sentido.

5) **Semi-grupos regulares** — Um semi-grupo para o qual todos os elementos sejam regulares diz-se um *semi-grupo regular* ou um *grupo*. Dada a importância desta noção, vamos pôr de diferentes maneiras os postulados dos grupos e mostrar a sua equivalência. À face da definição, um conjunto $\mathfrak{C}$ é um grupo se valer o seguinte

1.º SISTEMA DE POSTULADOS PARA GRUPOS: G_1) existe em $\mathfrak{C}$ uma operação binária, de sorte que $\mathfrak{C}$ é um grupoide $(\mathfrak{G}/\cdot)$; G_2) a operação binária é associativa, de sorte que $\mathfrak{G}$ é um semi-grupo; G_3) existe em $\mathfrak{G}$ uma identidade ou elemento $um = u$; G_4) todos os elementos de $\mathfrak{G}$, que é semi-grupo com identidade, são regulares, pelo que $\mathfrak{G}$ é semi-grupo regular.

Dos raciocínios anteriormente feitos, sabemos que o sistema anterior é equivalente a este

2.º SISTEMA DE POSTULADOS: G'_1) $\mathfrak{G}$ é um conjunto a cada elemento a, ou x, do qual estão associadas duas aplicações de $\mathfrak{G}$ em $\mathfrak{G}$, de tal modo que é $aA_x^{(d)} = xA_a^{(e)}$; G'_2) as aplicações satisfazem às igualdades $A_a^{(e)}A_x^{(d)} = A_x^{(d)}A_a^{(e)}$; G'_3) existe em $\mathfrak{G}$ uma identidade u, ou seja um elemento para o qual $A_u^{(d)} = A_u^{(e)} = \mathrm{I}$; G'_4) cada aplicação $A_a^{(e)}$ é não singular.

Convém observar que G'_2) equivale à propriedade associativa, visto que se tem $bA_a^{(e)}A_x^{(d)} = bA_x^{(d)}A_a^{(e)}$, ou seja, precisamente, $(ab)x = a(bx)$. De resto, poderão pôr-se outras relações equivalentes a G'_2). De facto, G'_2) é equivalente a $A_a^{(d)}A_x^{(d)} = A_{aA_x^{(d)}}^{(d)}$ ou a $A_{xA_a^{(e)}}^{(e)} = A_x^{(e)}A_a^{(e)}$.

Imaginemos que, no 1.º sistema de postulados, apenas substituimos os postulados G_3) e G_4) pelos seguintes: G_3'') existe em $\mathfrak{G}$ uma unidade direita ε, ou seja um elemento tal que $a\varepsilon = a$, para todo o $a \in \mathfrak{G}$, (cf. II, 1, 1); G_4'') todos os elementos de $\mathfrak{G}$ têm uma regularidade direita *relativa* a ε, isto é, para cada $a \in \mathfrak{G}$, existe $a' \in \mathfrak{G}$ tal que $aa' = \varepsilon$. Claramente, então, que os postulados G_3'') e G_4'') são consequências de G_3) e de G_4). Vamos provar a inversa. Dado a, seja $aa' = \varepsilon$; se for $a' \cdot a'' = \varepsilon$, vê-se que $(a'a)\cdot(a'a'') = (a'a)\varepsilon = a'a$. Por outro lado, tendo em conta a propriedade associativa, é $(a'a)(a'a'') = a'(aa')\cdot a'' = a'a'' = \varepsilon$, de sorte que $a'a = \varepsilon$. Estabelecido este facto, provaremos que ε é unidade bilateral. Sendo $b\varepsilon = b$, pretende-se ver que é também $\varepsilon b = b$. Ora, supondo $bb' = \varepsilon$, pode escrever-se $(bb')(b\varepsilon) = \varepsilon(b\varepsilon) = \varepsilon b$; mas, como se tem ainda $(bb')(b\varepsilon) = b(b'b)\varepsilon = (b\varepsilon)\varepsilon = b$, conclui-se $\varepsilon b = b$, como se deseja. Assim:

3.º SISTEMA DE POSTULADOS: G_1'') existe em $\mathfrak{G}$ uma operação binária, de sorte que $\mathfrak{G}$ é um grupoide; G_2'') a operação binária é associativa, de sorte que $\mathfrak{G}$ é semi-grupo; G_3'') existe em $\mathfrak{G}$ uma unidade direita ε; G_4'') todos os elementos de $\mathfrak{G}$ são regulares à direita relativamente a ε.

Do 1.º sistema de postulados, também deduzimos que as equações $xa = b$ e $ay = b$ são solúveis, de soluções únicas, respectivamente iguais a ba^{-1} e $a^{-1}b$. Existe um novo sistema de postulados, a saber:

4.º SISTEMA DE POSTULADOS: G_1''') o mesmo que G_1); G_2''') o mesmo que G_2); G_3''') as equações $xa = b$ e $ay = b$ são solúveis em $\mathfrak{G}$.

Temos ùnicamente de deduzir deste sistema um dos sistemas anteriores. Para isso, consideremos a equação $ay = a$ e chamemos ε uma solução, a qual existe, por hipótese. Se, agora, $xa = c$ for uma equação cuja solução é x, temos $(xa)\varepsilon = c\varepsilon = x(a\varepsilon) = xa = c$. A relação $c\varepsilon = c$, por ser c arbitrário, mostra que ε é unidade direita. Quanto à existência de inverso direito relativamente a ε, tomemos a

equação $ay=\varepsilon$. A equação é solúvel e a é regular à direita relativamente a ε. Passámos, assim, do sistema 4.º ao sistema 3.º de postulados.

EXEMPLOS DE GRUPOS Em todo o semi-grupo com identidade, os elementos não singulares formam um sub-semi-grupo composto de elementos regulares, portanto um grupo. Em particular, no semi-grupo com identidade constituído pelas aplicações dum conjunto sobre si, as transformações formam grupo.

Ainda por sugestão do sistema 4.º de postulados, vão seguir-se alguns raciocínios. Imaginemos um semi grupo, no qual, em vez de G_3'''), se admite o postulado seguinte: S_4) as equações $xa=b$, $ay=b$, se forem solúveis, têm uma única solução. Os semi-grupos em causa, entre os quais se situam os grupos, possuem as propriedades que traduzimos nas duas proposições que vamos enunciar.

TEOREMA 1: *Se num semi-grupo tiver lugar o postulado* S_4), *é válida a lei de corte. A recíproca é também válida.* Significa isto, como em (I, 2, 1), que, por exemplo, duma equação $ay=ay'$, se deduz $y=y'$. Efectivamente, pondo $ay=b$, a equação em z, $az=b$, tem uma única solução. Será $y=y'$, quando $ay=ay'$. No que toca à recíproca, a demonstração é imediata.

TEOREMA 2: *Se num semi-grupo com um número finito de elementos tiver lugar o postulado* S_4), *o semi-grupo é um grupo.* Admitindo que a é um elemento fixo do semi-grupo e que x percorre o semi-grupo, os elementos xa pertencem ao semi-grupo e são todos distintos. O número de elementos xa é igual ao número de elementos x, pelo que a equação $xa=b$ é sempre solúvel. O mesmo se diz da equação $ay=b$. O axioma G_3''') é válido e o semi-grupo é um grupo.

Este resultado permite dar os postulados dos *grupos finitos*, isto é, que têm um número finito de elementos, sob uma forma diferente da do sistema 4.º.

SISTEMA DE POSTULADOS DOS GRUPOS FINITOS: $G_2^{(IV)}$) o mesmo que G_1'''); $G_2^{(IV)}$) o mesmo que G_2'''); $G_3^{(IV)}$) a lei do corte é válida à direita e à esquerda.

Então, com efeito, estamos em presença dum semi-grupo em que o postulado S_4) é válido. O teorema 2 afirma que se trata dum grupo.

§ 2. Teorema de Cayley. A tabela do grupo

1) **Sobre a noção de espaço algébrico** — Em (II, 1, 1), ao definirmos grupoide, falámos já de espaço algébrico. Na verdade, dado um conjunto $\mathfrak{C}$, pode acontecer que se definam várias operações binárias em $\mathfrak{C}$. A designação de espaço algébrico ou de *sistema algébrico* abrange a totalidade dos conjuntos «algebrizados» com uma ou mais operações, as quais podem estar subordinadas a certas leis ou postulados, como no caso dos semi-grupos ou dos grupos. Com o símbolo $\mathfrak{S}=(\mathfrak{C}/\Omega^*)$ significamos um espaço algébrico, de suporte $\mathfrak{C}$, em que se definiram operações binárias formando um conjunto $\Omega^*=\{\lambda^*,\mu^*,\nu^*,\cdots\}$. O símbolo $a\lambda^*b$ representa o resultado obtido pela operação λ^*, efectuada sobre o par ordenado (a,b).

Suponhamos, em seguida, um segundo sistema algébrico $\mathfrak{S}=(\mathfrak{C}'/\Omega^*)$, de suporte $\mathfrak{C}'=\{a',b',c',\cdots\}$, no qual, como a notação indica, se admite ser o mesmo o domínio das operações.

Uma correspondência que aplique $\mathfrak{S}$ em $\mathfrak{S}'$, de modo que se tenha

$$a\to a',\qquad b\to b',\qquad a\lambda^*b\to a'\lambda^*b',$$

diz-se uma *homomorfia*. Quando todos os elementos de $\mathfrak{S}'$ são utilizados como imagem, a homomorfia designa-se por *homomorfismo*. Se, na homomorfia, a correspondência for biunívoca, tem-se uma *isomorfia*. Se, no homomorfismo, a correspondência for biunívoca, tem-se um *isomorfismo*. A homomorfia, na hipótese de $\mathfrak{S}'$ ser o próprio $\mathfrak{S}$, diz-se um *endomorfismo*; com a mesma hipótese, a isomorfia chama-se *meromorfismo* e o isomorfismo diz-se *automorfismo*.

Uma parte $\mathfrak{S}_1$ dum sistema algébrico tal que, sendo $a_1,b_1\in\mathfrak{S}_1$, também se tem $a_1\lambda^*b_1\in\mathfrak{S}_1$, qualquer que seja $\lambda^*\in\Omega^*$, e que, além disso, verifica as mesmas leis impostas ao sistema, diz-se um *subsistema algébrico* (ou um *subespaço algébrico*).

2) **Grupos homomorfos e isomorfos. Teorema de Cayley. Antihomomorfismo** — Dado um grupo $\mathfrak{G}(\cdot)$, se $\mathfrak{G}'(\cdot)$ for um sistema algébrico para o qual se sabe apenas da existência duma operação binária, o simples facto de $\mathfrak{G}'$ ser imagem homomorfa de $\mathfrak{G}$, à face dessa operação, implica que $\mathfrak{G}'$ seja um grupo. Reconhece-se isso de modo

simples, observando que, em $\mathfrak{G}'$, são válidos, por exemplo, os postulados do 3.º sistema de (II, 1, 5).

É muito importante o teorema a seguir, designado por teorema de CAYLEY:

TEOREMA 1: *Qualquer grupo é isomorfo dum grupo de transformações* (também chamadas *permutações*). Dado o grupo $\mathfrak{G}$, tomemos $a \in \mathfrak{G}$ fixo e $x \in \mathfrak{G}$ arbitrário. A correspondência $x \to x\,a = x\,A_a^{(d)}$ é uma permutação de $\mathfrak{G}$. Vamos fixar a nossa atenção na correspondência $a \to A_a^{(d)}$. Se for $a \neq b$, é $A_a^{(d)} \neq A_b^{(d)}$, como se verifica pondo $x = u$: $u\,a = a = u\,A_a^{(d)}$, $u\,b = b = u\,A_b^{(d)} \neq u\,A_a^{(d)}$. O produto $a\,b$ define a permutação

$$x \to x\,(a\,b) = (x\,a)\,b = (x\,A_a^{(d)})\,A_b^{(d)} = x\,A_a^{(d)}\,A_b^{(d)}.$$

Vê-se que ao produto $a\,b$ corresponde o produto das transformações correspondentes. O teorema está demonstrado.

Há aqui uma aplicação biunívoca de $\mathfrak{G}$ sobre uma parte do seu grupo de transformações, parte essa que também forma grupo.

Regressemos ao grupo $\mathfrak{G}$ e ao sistema algébrico $\mathfrak{G}'$, do começo deste número. Se tiver lugar uma correspondência $x \to x'$, $(x \in \mathfrak{G},\ x' \in \mathfrak{G}')$, de tal modo que $x\,y \to (x\,y)' = y'\,x'$, a referida correspondência diz-se um *anti-homomorfismo*. No caso da biunivocidade, tem-se um *anti-isomorfismo* ou um *isomorfismo inverso*.

Tomemos $a \in \mathfrak{G}$ fixo e a aplicação $x \to a\,x = x\,A_a^{(e)}$, de $\mathfrak{G}$ sobre $\mathfrak{G}$. É imediato que a correspondência $a \to A_a^{(e)}$ é um anti-isomorfismo. O conjunto dos $A_a^{(e)}$, tal como o dos $A_a^{(d)}$, forma um grupo, dentro do grupo das transformações de $\mathfrak{G}$.

Representemos por $\mathfrak{G}_d$ o conjunto dos $A_a^{(d)}$, por $\mathfrak{G}_e$ o conjunto dos $A_a^{(e)}$ e por $\mathfrak{T}(\mathfrak{G})$ o conjunto das transformações de $\mathfrak{G}$. Já sabemos que se tem $A_a^{(d)}\,A_b^{(e)} = A_b^{(e)}\,A_a^{(d)}$ como tradução da propriedade associativa. A igualdade acabada de assinalar interpreta se dizendo que os elementos de $\mathfrak{G}_e$ fazem parte do *comutador* de $\mathfrak{G}_d$, dentro de $\mathfrak{T}(\mathfrak{G})$. Vamos ver, mais precisamente, que $\mathfrak{G}_d$ e $\mathfrak{G}_e$ são *comutadores recíprocos*, isto é, por exemplo, que, dentro de $\mathfrak{T}(\mathfrak{G})$, qualquer transformação que comute com todas as transformações de $\mathfrak{G}_d$ pertence necessàriamente a $\mathfrak{G}_e$. Tomemos $S \in \mathfrak{T}(\mathfrak{G})$ e suponhamos

$$x \to x\,S,\quad (x\,A_a^{(d)})\,S = (x\,a)\,S = (x\,S)\,A_a^{(d)} = (x\,S)\,a.$$

Fazendo $x = u$, deverá ter-se

$$u \to u\,S = b \in \mathfrak{G},\quad (u\,A_a^{(d)})\,S = (u\,a)\,S = a\,S = (u\,S)\,a = b\,a.$$

Assim, vê-se que $a \to a\,S = b\,a = a\,A_b^{(e)}$, qualquer que seja $a \in \mathfrak{G}$. Por isso, tem-se $S = A_b^{(e)}$, como se afirmou. Podemos fixar este

TEOREMA 2: *Dado um grupo* $\mathfrak{G}$, *os grupos* $\mathfrak{G}_d$ *e* $\mathfrak{G}_e$, *contidos no grupo* $\mathfrak{T}(\mathfrak{G})$, *das transformações de* $\mathfrak{G}$, *são comutadores recíprocos dentro de* $\mathfrak{T}(\mathfrak{G})$.

3) **Sobre os grupos finitos** — Um grupo finito fica completamente conhecido, logo que se tenha uma tabela na qual se possa encontrar o produto de dois quaisquer dos seus elementos. Consideremos, por exemplo, as tabelas seguintes:

	u	a
u	u	a
a	a	u

;

	u	a	b
u	u	a	b
a	a	b	u
b	b	u	a

;

a primeira correspondente a um grupo de dois elementos, a segunda a um grupo de três elementos. No cruzamento de cada linha vertical, passando por um elemento do grupo do alto da tabela, com cada linha horizontal, passando por outro elemento da esquerda da tabela, encontra-se o produto deste último por aquele. Cada linha horizontal, como cada linha vertical, contém, dentro da tabela, todos os elementos do grupo e cada um deles uma só vez.

À interpretação da tabela interessa o enunciado dos axiomas dos grupos por uma forma diferente de todas aquelas que foram indicadas em (II, 1, 5). Poremos aqui o seguinte

SISTEMA DE POSTULADOS DOS GRUPOS: $G_1^{(V)}$) o conjunto $\mathfrak{G}$, em questão, é um grupoide; $G_2^{(V)}$) existe em $\mathfrak{G}$ uma unidade direita ε; $G_3^{(V)}$) todos os elementos de $\mathfrak{G}$ têm uma regularidade direita relativa a ε; $G_4^{(V)}$) se γ é o inverso direito de c relativamente a ε, vale a igualdade $a\,b = a\,c \cdot \gamma\,b$.

É imediato que os postulados acabados de indicar são válidos num grupo qualquer. A inversa prova-se como vai ver-se. Em primeiro lugar: .

TEOREMA 1: *Se* α *é inverso direito de* a *relativamente a* ε, *é também inverso esquerdo, no sentido de ser* $\alpha a = \varepsilon$. De facto, se α' é inverso direito de α, tem-se $\alpha a \cdot \alpha\alpha' = \alpha\alpha' = \varepsilon$, em virtude de $G_4^{(V)}$). Por outro lado, $\alpha a \cdot \alpha\alpha' = \alpha a \cdot \varepsilon = \alpha a$, o que implica $\alpha a = \varepsilon$, como se deseja. Depois:

TEOREMA 2: *A unidade direita* ε *é unidade esquerda.* Na verdade, vê-se que $b\beta \cdot b\varepsilon = \varepsilon \cdot b\varepsilon = \varepsilon b$, assim como $b\beta \cdot b\varepsilon = b\varepsilon = b$, se β é inverso direito de b. Resulta assim, para qualquer b, $\varepsilon b = b$.

Demonstrados estes teoremas, voltemos a aplicar $G_4^{(V)}$), fazendo, ~~sucessivamente~~, $b = \varepsilon = u$ (ou $a = u$). Vem $a = ac \cdot \gamma$ (ou $b = c \cdot \gamma b$). Portanto, é $a \cdot bc = (ab \cdot \beta)bc = ab \cdot c$. A propriedade associativa é válida, pelo que são válidos os axiomas do 1.º sistema de (II, 1, 5).

Feito isto, reconhece-se que o axioma $G_4^{(V)}$ se traduz na tabela dum grupo finito de modo interessante, indicado no quadro junto. Por ela se vê que, dentro da tabela dos produtos, qualquer paralelogramo cujo primeiro vértice seja u, tem, no vértice oposto a u, o produto dos dois elementos que ocupam os outros dois vértices opostos do mesmo paralelogramo, tomados na ordem conveniente.

		x		y
x^{-1}		u		$x^{-1}y$
z		zx		zy

As tabelas indicadas, no caso de 2 ou 3 elementos, são únicas. Já não sucede assim, para 4 ou 5 elementos. Pode fazer-se a este respeito uma observação: quaisquer que sejam as tabelas construídas, só a partir de 6 elementos se encontram grupos para os quais o produto ab é diferente de ba.

Como caso particular de conjunto $\mathfrak{C}$, tomemos $\mathfrak{C} = \{1, 2, \cdots, n\}$. Uma transformação $i_k = \varphi(k)$, $(k = 1, 2, \cdots, n)$, pode representar-se pelo símbolo

$$(1) \qquad \varphi = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}.$$

O conjunto das transformações deste tipo é o conjunto das *permutações de* n *elementos* e o grupo que elas formam chama-se *grupo simétrico de ordem* n. Representá-lo-emos pelo símbolo $\mathfrak{S}_n$.

Ao utilizar-se o 2.º membro de (1) para representar φ, não há necessidade de colocar como 1.ª linha horizontal os números $1, 2, \cdots, n$, pela sua ordem natural. A ordem é qualquer, contanto que a 2.ª linha horizontal contenha, em correspondência, os números correspondentes. Assim, se pusermos

$$\psi = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$$

vê-se que

$$\psi\varphi = \begin{pmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}.$$

Em geral, é $\psi\varphi \neq \varphi\psi$. A este respeito, e em correlação com o que se fez em (I, 1, 3), é importante fixar a observação a seguir. Escrevemos aqui $i_k = \varphi(k)$, colocando φ à esquerda de k. Então $\psi\varphi(k) = \psi(\varphi(k))$ significa que se efectua primeiramente φ, depois ψ. Em geral, porém, ao utilizarem-se os símbolos $S, T, \cdots$, para significarem transformações, o símbolo ST significa que se efectua primeiro S, depois T. Em tal caso, há conveniência em escrever, por exemplo, $a(ST) = (aS)T$, situando as transformações à direita de a.

Tendo em conta o teorema de CAYLEY, diremos:

TEOREMA 3: *Todo o grupo finito com* n *elementos é isomorfo dum grupo de transformações pertencentes a* $\mathfrak{S}_n$.

§ 3. Semi-grupos abelianos. Números inteiros

1) **Semi-grupos comutativos** — Um semi-grupo é *comutativo*, se o respectivo grupoide fôr comutativo.

Seja $i_1, i_2, \cdots, i_n$ uma nova disposição dos números $1, 2, \cdots, n$. O produto de n factores gosa, então, da propriedade expressa na igualdade $a_1 a_2 \cdots a_n = a_{i_1} a_{i_2} \cdots a_{i_n}$. Para a demonstrarmos, comecemos por ter em conta que ela é válida no caso de dois elementos. Admitamos, em seguida, que é $i_k = n$. Se o teorema é verdadeiro para $n - 1$ factores, prová-lo-emos para n factores. Tem-se

$$a_{i_1} a_{i_2} \cdots a_{i_{k-1}} \cdot a_{i_k} \cdot a_{i_{k+1}} \cdots a_{i_n} = a_{i_1} \cdots a_{i_{k-1}} \cdot a_n \cdot a_{i_{k+1}} \cdots a_{i_n} =$$
$$= a_{i_1} \cdots a_{i_{k-1}} \cdot a_{i_{k+1}} \cdots a_{i_n} \cdot a_n = a_1 \cdots a_{n-1} \cdot a_n = a_1 a_2 \cdots a_n.$$

Passa-se da antepenúltima para a penúltima expressão pela hipótese da indução relativa a $n-1$.

Os semi-grupos comutativos têm frequentemente a designação de *semi-grupos abelianos*. Está muito em voga o uso do sinal $+$ para representar a operação, no caso abeliano. Embora não ponhamos esta regra em absoluto, respeitá-la-emos quase sempre. Temos assim:

$$a_1 + \cdots + a_n = (a_1 + \cdots + a_{n-1}) + a_n;$$

$$A+B=a_1+\cdots+a_p,(p\leqq n+1), \text{ se } A=a_1+\cdots+a_n, B=a_{n+1}+\cdots+a_p;$$

$$n\,a=a+a+\cdots+a, \text{ (onde } n \text{ é inteiro e } a \text{ se repete } n \text{ vezes});$$

$$m\,a+n\,a=(m+n)\,a; \quad n\cdot m\,a=(n\,m)\,a.$$

Uma regra importante, que não é válida no caso não comutativo, é a seguinte: $n(a+b)=n\,a+n\,b$. Na notação que utiliza o ponto, em vez do sinal $+$, deverá escrever-se $(a\,b)^n=a^n\cdot b^n$.

Os números naturais dão um exemplo de semi-grupo comutativo, tanto relativamente à operação de soma como à operação de produto.

É para os grupos de produto comutativo que, na verdade, têm principalmente lugar as observações feitas quanto à notação. Se o sinal $+$ é o sinal de operação, tem-se um *grupo abeliano aditivo* ou *módulo*. Reveste-se de grande interesse o teorema a seguir, em cuja demonstração ainda utilizamos a operação indicada com um ponto, embora nas aplicações passemos a usar o sinal $+$.

Teorema 1: *Todo o semi-grupo abeliano em que é válida a lei de corte pode ser mergulhado num grupo abeliano.* Dado o semi-grupo $(\mathfrak{C}/\cdot)=\{a,b,c,\cdots\}$, passemos ao conjunto $\mathfrak{G}_0=\{(a,b);(c,d);\cdots\}$, de pares ordenados $(a,b),\cdots$ e introduzamos em $\mathfrak{G}_0$ a seguinte relação de equivalência ρ:

$$(a,b)\,\rho\,(c,d), \text{ se e só se } a\,d=c\,b.$$

A classe de representante (a,b) será designada por $[a,b]$. Então, algebriza-se o espaço cociente $\mathfrak{G}_0/\rho=\{[a,b];[c,d];\cdots\}$, definindo $\mathfrak{G}=(\mathfrak{G}_0/\rho/\cdot)$ por meio dum produto, nos termos seguintes:

$$[a,b]\cdot[c,d]=[a\,c,b\,d]. \tag{1}$$

Vamos ver que $\mathfrak{G}$ é um grupo abeliano. Em primeiro lugar, a definição indicada para o produto é independente dos representantes das classes, porque, supondo $(a,b)\,\rho\,(a',b')$, é $a\,b'=a'\,b$ e

$$[a',b']\cdot[c,d]=[a'\,c,b'\,d]=[a\,c,b\,d],$$

visto que $a'\,c\,b\,d=a\,c\,b'\,d$.

É imediato também que o produto indicado em (1) é comutativo e associativo. Finalmente, uma equação da forma

$$[a,b]\cdot[x,y]=[c,d]$$

resolve-se pondo $[x,y]=[b\,c,a\,d]$. O 4.º sistema de postulados, referido em (II, 1, 5), é verificado, e $\mathfrak{G}$ é um grupo, na verdade abeliano.

Para reconhecermos agora que $\mathfrak{C}$ está «mergulhado» em $\mathfrak{G}$, vamos verificar que existe em $\mathfrak{G}$ uma parte que é isomorfa de $\mathfrak{C}$. Duma maneira geral, *um sistema algébrico* $\mathfrak{S}$ *está mergulhado num sistema algébrico* $\mathfrak{T}$, *se os dois sistemas têm o mesmo domínio operacional* Ω^* *e se existe uma parte* $\mathfrak{T}_0\subseteq\mathfrak{T}$ *isomorfa de* $\mathfrak{S}$. Façamos corresponder, no caso em estudo, ao elemento $a\in\mathfrak{C}$ o elemento $[a\,b,b]\in\mathfrak{G}$, onde $b\in\mathfrak{C}$ é qualquer. A correspondência $a\to[a\,b,b]$, é um isomorfismo.

O problema de imersão que acabamos de resolver toma um aspecto muito importante no caso que passamos o estudar.

Um semi-grupo abeliano aditivo $(\mathfrak{L}/+)$, de operação indicada por $+$, diz-se um *semi-grupo abeliano ordenado*, se forem realizadas as duas condições seguintes: 1) $\mathfrak{L}$ é um conjunto ordenado por uma eventual relação de ordem, como foi indicado em (I, 1, 5); 2) se a,b,c forem elementos de $\mathfrak{L}$ tais que $a<b$, é $a+c<b+c$, qualquer que seja c. Vale, então, este

Teorema 2: *Há um e um só processo de ordenar o grupo abeliano* $\mathfrak{M}$, *em que se mergulha* $\mathfrak{L}$, *por forma que seja mantida a relação de ordem dos elementos de* $\mathfrak{L}$. Imaginemos $a<b$. Deverá ter-se $[a+c,c]<[b+c,c]$. Esta relação terá efectivamente lugar, se pusermos $[a,b]<[c,d]$, quando $a+d<c+b$. Ora vamos provar que, deste modo, é $\mathfrak{M}$ um *grupo abeliano ordenado*, isto é, que $\mathfrak{M}$ é um grupo satisfazendo às condições referidas para os semi-grupos abelianos ordenados. Na verdade: Dados $[a,b]$ e $[c,d]$, ou é $a+d<c+b$ ou $c+b<a+d$, se os dois elementos de que se partiu não são iguais; no 1.º caso, tem-se $[a,b]<[c,d]$, enquanto que, no 2.º, é $[c,d]<[a,b]$. Por outro lado, a transitividade é imediata. Finalmente, se $[a,b]<[c,d]$, também $[a,b]+[f,g]<[c,d]+[f,g]$.

Há, assim, um processo de se passar do semi-grupo para o grupo, nos termos do teorema. Para se mostrar que o processo é único, observemos que, quando $[a,b]<[c,d]$, se não fosse $a+d<c+b$, seria $c+b<a+d$, o que levaria a

$$[c+b+f,f]+[f,b+d+f]<[a+d+f,f]+[f,b+d+f],$$

ou seja a $[c,d]<[a,b]$. A proposição está completamente provada.

2) **Os números inteiros** – Os números naturais, estudados em (I, 2), constituem um semi-grupo abeliano aditivo $\mathfrak{N}$, no qual é válida a lei de corte. O processo do número anterior permite mergulhar $\mathfrak{N}$ num grupo abeliano aditivo $\mathfrak{Z}$, que se diz o conjunto dos *números inteiros*. Os números inteiros são, pois, classes $[a,b]$, onde a e b são números naturais. A identidade de $\mathfrak{Z}$ é a classe $[a,a]$, que será representada simplesmente pelo símbolo O, de nome *zero*. É, por exemplo,

$$[c,d]+[a,a]=[c+a,d+a]=[c,d].$$

O elemento inverso da classe $[a,b]$ é a classe $[b,a]$, pois que

$$[a,b]+[b,a]=[a+b,a+b]=O.$$

Um número natural $a=[a+b,b]$ será representado por a. Além disso, utilizaremos o símbolo $-a=[b,a]$, para significar inverso (aqui *simétrico*) do inteiro $a=[a,b]$.

Vamos, então, constatar: um inteiro ou é um número natural a, ou é O, ou é $-a$. Tomemos uma classe $[c,d]$. Quando se tem $d=c$, é $[c,d]=O$. Se $d\neq c$, imaginemos que, relativamente à ordenação dos números naturais introduzida em (I, 2, 2), é $d<c$, ou seja $c=f+d$, com $f\in\mathfrak{N}$. Nesse caso, escreve-se

$$[c,d]=[f+d,d]=f,$$

pelo que a classe é um número natural. Dando-se a hipótese $c<d$, tem-se $d=g+c$, e

$$[d,c]=[g+c,c]=g, \qquad [c,d]=-g.$$

O conjunto $\mathfrak{Z}$ é, pois, o seguinte:

$$\mathfrak{Z}=\{1,2,3,\cdots,n,\cdots;O;-1,-2,-3,\cdots,-n,\cdots\}.$$

Sabemos mais que a citada ordenação dos números naturais leva a uma ordenação dos números inteiros segundo a regra $[a,b]<[c,d]$,

se e só se $a+d<c+b$. Os números inteiros que precedem zero dizem-se *negativos*. Devendo ter-se, então, $[c,d]<[c,c]$, ou seja $c+c<c+d$, $c<d$, verifica-se que os números negativos são os números da forma $-a$. Se, em $[c,d]$, for $d<c$, é $[c,c]<[c,d]$. Trata-se dos números naturais, que agora se consideram *positivos*.

A ordenação obtida para os inteiros leva a escrever $\mathfrak{Z}$ sob a forma seguinte:

$$\mathfrak{Z}=\{\cdots,-n,\cdots,-3,-2,-1,0,1,2,3,\cdots,n,\cdots\}.$$

No sistema algébrico dos inteiros (módulo), é possível introduzir uma nova operação (produto), escrevendo

$$[a,b]\cdot[c,d]=[ac+bd,ad+bc]. \tag{1}$$

Na verdade, imaginemos que se tem $[a,b]=[a',b']$, $[c,d]=[c',d']$, de sorte que $a+b'=a'+b$, $c+d'=c'+d$. Vamos verificar que, sendo, à face de (1),

$$[a',b']\cdot[c',d']=[a'c'+b'd',\ a'd'+b'c'],$$

é $[ac+bd,ad+bc]=[a'c'+b'd',a'd'+b'c']$, ou seja, que se tem

$$ac+bd+a'd'+b'c'=a'c'+b'd'+ad+bc. \tag{2}$$

Ora, por hipótese, é válida a igualdade

$$\begin{aligned}(a+b')c+(a'+b)d+(c+d')a'+(c'+d)b'&=\\=(a'+b)c+(a+b')d+(c'+d)a'+(c+d')b',&\end{aligned}$$

da qual se deduz, tendo em conta o que se viu em (I, 1, 6),

$$\begin{aligned}ac+b'c+a'd+bd+ca'+d'a'+c'b'+db'&=\\=a'c+bc+ad+b'd+c'a'+da'+cb'+d'b',&\end{aligned}$$

e, portanto, a igualdade (2).

Deste modo, em (1) tem-se uma operação unívoca. Esta operação é a operação de produto definida em (I, 2, 1), quando os factores são números naturais. De facto, se se tem

$$[a,b]=[b+f,b]=f, \qquad [c,d]=[d+g,d]=g,$$

vê-se que

$$\begin{aligned}[a,b]\cdot[c,d]&=[(b+f)(d+g)+bd,(b+f)d+b(d+g)]=\\&=[bd+bg+fd+fg+bd,bd+fd+bd+bg]=[fg+bd,bd]=fg.\end{aligned}$$

Designemos por x, y, z números inteiros. Em $\mathfrak{Z}$ são válidas as as regras seguintes, além das que foram já indicadas: 1) de $x<y$, $0<z$, conclui-se $xz<yz$; 2) de $0<x$, $0<y$, conclui-se $0<x+y$, $0<xy$; 3) de $x<y$, deduz-se $x+z<y+z$; 4) de $0<x$, $y<0$, deduz-se $xy<0$; 5) de $x<0$, $y<0$, tira-se $0<xy$.

A regra 4) afirma que o produto dum inteiro positivo por um inteiro negativo é um inteiro negativo; e a regra 5) diz que o produto de dois inteiros negativos é um inteiro positivo.

Limitemo-nos a provar a regra 1). Ponhamos

$$x=[a,b], \quad y=[c,d], \quad z=[f,g],$$

com as hipóteses $a+d<c+b$, $g<f$. Então

$$xz=[af+bg,\ ag+bf] \quad yz=[cf+dg,\ cg+df],$$

pelo que devemos estabelecer a relação

$$af+bg+cg+df<cf+dg+ag+bf,$$

ou, pondo $f=g+h$, a relação

$$ag+ah+bg+cg+dg+dh<cg+ch+dg+ag+bg+bh,$$

que se simplifica para

$$ah+cg+dg+dh<cg+ch+dg+bh. \tag{3}$$

Ora, de $a+d<c+b$, concluimos $ah+dh<ch+bh$, pelo que

$$(ah+dh)+(cg+dg)<(ch+bh)+(cg+dg),$$

que é precisamente a relação (3).

Também interessa fixar que o produto dum inteiro qualquer por zero é igual a zero e que, se o produto de dois inteiros é zero, um dos factores é zero. Quanto ao 1.º facto, utilizando, de novo, a representação $[a,b]$, vê-se que

$$[a,b]\cdot[c,c]=[ac+bc,ac+bc]=0;$$

e, relativamente ao segundo, se $xy=0$, não pode ter-se qualquer das hipóteses: $0<x$, $0<y$; $0<x$, $y<0$; $x<0$, $0<y$; $x<0$, $y<0$. Daqui resulta que terá de ser $x=0$, ou $y=0$.

Os números inteiros, algebrizados com as duas operações, de soma e de produto, entram na categoria dos sistemas algébricos denominados «anéis», que serão objecto do Capítulo V.

Diz-se *valor absoluto* do inteiro x o número $|x|$, assim definido: se $0<x$, é $|x|=x$; se $x<0$, é $|x|=-x$; e, se $x=0$, é $|x|=0$. O valor absoluto é zero ou um número positivo.

No que vai seguir-se ainda neste número, as letras $a, b, c, \ldots$ passam a significar números inteiros.

Um conjunto de inteiros minorado por um inteiro tem um limite inferior que pertence ao conjunto; e um conjunto de inteiros majorado por um inteiro tem um limite superior que pertence ao conjunto. A demonstração destas afirmações é simples. Basta estudar, por exemplo, separadamente, as hipóteses que podem pôr-se, de haver no conjunto só números negativos, ou só números positivos, ou números positivos e negativos, ou números que também incluam zero. Precisamente, a segunda das afirmações é útil, a fim de estabelecermos o

ALGORITMO DE DIVISÃO: Trata-se de ver que, sendo a e $b\neq 0$ números inteiros quaisquer, é sempre possível escrever, e duma só maneira, $a=bq+r$, onde q e r são inteiros, satisfazendo r às relações $0\leqslant r<|b|$. Para isso consideremos o conjunto $\mathfrak{C}$ dos números inteiros x nas condições seguintes: $x|b|\leqslant a$. Esse conjunto não é vazio, porque, de $|a|\leqslant|a|\cdot|b|$, concluimos $-(|a|\cdot|b|)\leqslant-|a|\leqslant a$. Então, seja v_0 o limite superior do conjunto $\mathfrak{C}$. Vale a igualdade

$$a=v_0|b|+r_0, \text{ com } 0\leqslant r_0,$$

pois que, se um inteiro x é menor do que um inteiro y, tem lugar uma relação da forma $y=x+z$, sendo z um inteiro positivo.

Pelo facto de se ter

$$a<(v_0+1)|b|, \text{ ou } v_0|b|+r_0<v_0|b|+|b|,$$

vê-se que é $r_0<|b|$. Consequentemente, se $0<b$, como $|b|=b$, vem $a=v_0b+r_0$, com $0\leqslant r_0<|b|$; se, pelo contrário, $b<0$, como $|b|=-b$, tem-se $a=v_0(-b)+r_0$, ou $a=(-v_0)\cdot b+r_0$, com $0\leqslant r_0<|b|$. Portanto, com $q=v_0$ ou $q=-v_0$ e $r=r_0$ está conseguida a decomposição $a=bq+r$.

De resto, essa decomposição é única, dado que, com

$$a=bq+r, \quad a=bq'+r', \tag{4}$$

se $r\leqslant r'$, se obtém

$$0=b(q'-q)+(r'-r), \quad r'-r=b(q-q'), \tag{5}$$

onde, por abreviatura, se escreve $x - y$ em vez de $x + (-y)$. Ora a última igualdade (5) levaria a $|r' - r| = |b| \cdot |q - q'|$, que fàcilmente se reconhece ser um absurdo, a não ser que se tenha $r' = r$, $q' = q$. As duas decomposições (4) são idênticas.

Dados dois números inteiros a e b, se for $a = bc$, onde c é outro inteiro, diz-se que b é *divisor* de a ou que a é múltiplo de b. As nossas considerações sobre inteiros vão terminar pela teoria do *máximo divisor comum* e pela teoria do *menor múltiplo comum*.

Tomemos os inteiros a e b. Diz-se que d é o máximo divisor comum de a e b, se d gosa das duas propriedades seguintes: 1) d divide a e b; 2) qualquer divisor comum de a e b é divisor de d. Esta definição é equivalente a dizer que existem inteiros q, q', r', s' tais que

$$a = dq, \quad b = dq', \quad d = ar' + bs'. \tag{6}$$

É imediato, com efeito, que, suposto d a verificar as igualdades (6), as propriedades 1) e 2) são também verificadas. Para se demonstrar a inversa, tomemos a, b e d e admitamos 1) e 2). Consideremos, depois, todos os inteiros da forma $ax + by$, entre os quais há inteiros positivos formando um conjunto P. Designemos por t_0 o menor inteiro positivo pertencente a P. Será $t_0 = ar + bs$, tendo-se também $a = t_0 q + r_0$, com $0 \leqq r_0 < t_0$. Então é

$$r_0 = a - t_0 q = a - (ar + bs)q = a(1 - rq) + b \cdot (-qs).$$

Por aqui se vê que $r_0 = 0$, visto que, a ter lugar a propriedade $0 < r_0 < t_0$, cairíamos no absurdo $r_0 \in P, r_0 < t_0$. Assim, chega-se a $a = t_0 q_1$. Anàlogamente se chegaria a $b = t_0 q_1'$. Visto que t_0 divide a e b, a propriedade 2) afirma que t_0 divide d. Em virtude de se ter, porém, $a = dq_0, b = dq_0', t_0 = ar + bs = d(q_0 r + q_0' s)$, também d divide t_0. Será, necessàriamente, $d = \pm t_0$, consequentemente $d = \pm(ar + bs)$, como o exige a última relação (6).

O menor múltiplo comum f, de dois inteiros a e b, é um múltiplo de a e de b, tal que qualquer outro múltiplo comum é também múltiplo de f. O valor de f é dado pela igualdade $ab = f \cdot d$, na qual $d =$ máximo divisor comum.

Observação: Se d satisfaz a relações do tipo (6), também $-d$ está nas mesmas condições. As definições de máximo divisor comum

e de menor múltiplo comum são dadas a «menos de sinal»: d ou $-d$, f ou $-f$.

3) **A potência nula e as potências negativas de elementos regulares**—Foram definidas, em (II, 1, 2), as potências positivas a^n dum elemento dum grupoide qualquer. Nos semi-grupos com identidade u, define-se a potência zero dum elemento a, pondo $a^0 = u$, e, se a é regular, muito fàcilmente se reconhece, por via de indução, que, suposto α o inverso de a, é α^n o inverso de a^n. Então, introduziremos a potência negativa a^{-n}, do elemento regular a, pondo, por definição, $a^n \cdot a^{-n} = u$, ou seja, escrevendo $a^{-n} = (a^n)^{-1}$. Vamos mostrar ainda que $a^{-n} = (a^{-1})^n$, servindo-nos igualmente do método de indução. Temos $a^{-1} = (a^{-1})^1$, quando $n = 1$. Quando se toma $n + 1$, vem $a^{n+1} \cdot a^{-(n+1)} = u$, sendo também $a^{n+1} \cdot (a^{-1})^{n+1} = a^1 a^n \cdot (a^{-1})^n a^{-1} = a^1 \cdot a^n (a^{-1})^n \cdot a^{-1} = a^1 u a^{-1} = u$, pois que, pela hipótese da indução, é $a^{-n} = (a^{-1})^n$. Concluimos que $(a^{-1})^{n+1}$ é inverso de a^{n+1}, ou seja, que $(a^{-1})^{n+1} = a^{-(n+1)}$, como se deseja.

Para expoentes negativos, valem as igualdades

$$(a^n)^{-m} = a^{-mn}, \quad a^n \cdot a^{-m} = a^{n-m}. \tag{1}$$

Justifiquemos a última. Quando $m = 1$, a regra é válida. Admitindo que ela é válida, então, mudando m em $m + 1$, vem

$$a^n \cdot a^{-(m+1)} = a^n \cdot a^{-m} a^{-1} = a^{n-m} a^{-1}.$$

Se fôr $n > m$, o último membro pode tomar a forma $a^{n-m-1} a \cdot a^{-1} = a^{n-(m+1)}$; se for $n < m$, podemos escrevê-lo $a^{-(m-n)} \cdot a^{-1} = (a^{-1})^{m-n+1} = a^{n-(m+1)}$. Em todos os casos, a 2.ª fórmula (1) é válida. Claro que o caso $n = m$ leva a $a^n \cdot a^{-n} = a^{n-n} = a^0 = u$, não carecendo de demonstração.

As modificações de notação a ter em conta, quando se trata de grupos abelianos, na mesma ordem das ideias de (II, 3, 1), são as seguintes:

1) Para harmonia de escrita, convém utilizar 0, em vez de u, por sugestão do que se fez nos números inteiros, de modo que é $a + 0 = a$;

2) escreve-se $-a$ em vez de a^{-1}, tendo-se, portanto, $a + (-a) = 0$;

3) pór simplicidade, $a - b$ é abreviatura de $a + (-b)$;

4) tem-se $na+(-n)a=0$; $(-n)a=-na=n(-a)$, assim como $-m\cdot na=-mna$, $na+(-m)a=(n-m)a$, e $-m(-na)=m(-(-na))=mna$.

BIBLIOGRAFIA

B. L. VAN DER WAERDEN, *Moderne Algebra*, erster Teil, Berlin, 1930.

A. ALMEIDA COSTA, *Elementos da Teoria dos Grupos*, Porto, Centro de Estudos Matemáticos, 1942.

R. H. BRUCK, *Contributions to the theory of loops*, «Transactions of the American Mathematical Society», vol. 60, 1946, pgs. 245-354.

N. JACOBSON, *Lectures in Abstract Algebra*, vol. I, New York, 1951.

J. TIAGO DE OLIVEIRA, *Residuais de sistemas e radicais de anéis*, «Revista da Faculdade de Ciências de Lisboa, vol. V, 1956, pgs. 177-245.

CAPÍTULO III

Grupos

§ 1. Subgrupos. Grupos cíclicos. Invariantes. Grupo factor.

1) **Generalização da ideia de operação. Congruências** — Em (II, 2, 1), ao regressarmos à noção de espaço algébrico, ainda nos limitámos a falar de operações binárias. Vamos estender a ideia de operação.

Diz-se uma *operação de ordem k* num conjunto $\mathfrak{C}$ uma aplicação do produto $\mathfrak{C}\times\mathfrak{C}\times\cdots\times\mathfrak{C}$ (com k factores) no conjunto $\mathfrak{C}$. De k elementos ordenados de $\mathfrak{C}$, passa se a um elemento de $\mathfrak{C}$. Em particular, se $k=1$, obtem-se uma *operação unária*, que é, na verdade, uma aplicação de $\mathfrak{C}$ em $\mathfrak{C}$. As operações unárias também recebem o nome de *operadores*.

Finalmente, introduziremos as *operações de ordem zero*, que fazem passar dum conjunto vazio de elementos de $\mathfrak{C}$ a um elemento de $\mathfrak{C}$. Por outras palavras: dar uma operação de ordem zero é fixar um elemento de $\mathfrak{C}$. Num espaço algébrico poderá haver tantas operações de ordem zero quantos os seus elementos.

Com o símbolo $\mathfrak{S}=(\mathfrak{C}/\Omega,\Omega^*)$ designaremos um espaco algébrico, no qual há operadores, formando um conjunto $\Omega=\{\lambda,\mu,\nu,\cdots\}$, e operações binárias, formando um conjunto $\Omega^*=\{\lambda^*,\mu^*,\nu^*,\tau^*,\cdots\}$. Se existir uma operação de ordem zero, ela será particularmente indicada, sempre que nisso haja interesse.

Posto isto, tomemos $\mathfrak{S} = (\mathfrak{C}/\Omega, \Omega^*)$ e imaginemos uma relação de equivalência ϱ no suporte $\mathfrak{C}$. Diz-se que ϱ é uma *relação de congruência*, se $a \varrho a_1$, $b \varrho b_1$ implicarem $(a\lambda) \varrho (a_1 \lambda)$, $(a\lambda^* b) \varrho (a_1 \lambda^* b_1)$, quaisquer que sejam $\lambda \in \Omega, \lambda^* \in \Omega^*$.

Estes factos permitem algebrizar o conjunto cociente $\mathfrak{C}' = |C_a, C_b, \cdots| = \mathfrak{C}/\varrho$, introduzindo em $\mathfrak{C}'$ os mesmos domínios Ω e Ω^*. Basta pôr

$$C_a \lambda = C_{a\lambda}, \qquad C_a \lambda^* C_b = C_{a\lambda^* b}.$$

Então, com efeito, se a_1 fôr outro elemento de C_a, é $C_{a_1} = C_a$ e $C_{a_1 \lambda} = C_{a\lambda}$, pois que $a_1\lambda$ e $a\lambda$ pertencem à mesma classe de equivalência. Também se tem $C_{a\lambda^* b} = C_{a_1 \lambda^* b_1}$, pela mesma razão. Escrevendo $\mathfrak{S}' = (\mathfrak{C}'/\Omega, \Omega^*) = (\mathfrak{C}/\varrho\,|\,\Omega, \Omega^*)$, diremos que $\mathfrak{S}'$ é o *sistema algébrico cociente* de $\mathfrak{S}$ segundo a relação de congruência e poremos $\mathfrak{S}' = \mathfrak{S}/\varrho$.

A noção de homomorfismo e outras noções aparentadas, introduzidas em (II, 2, 1), no caso de existirem operadores, são tais que, supondo

$$a \to a', \text{ também darão } a\lambda \to a'\lambda, \ (\lambda \in \Omega).$$

Relativamente a uma operação de ordem zero, uma homomorfia levará dum elemento fixado em $\mathfrak{S}$ a um elemento fixado em $\mathfrak{S}' = (\mathfrak{C}'/\Omega, \Omega^*)$.

É fácil de concluir que, tomados $\mathfrak{S} = (\mathfrak{C}/\Omega, \Omega^*)$ e $\mathfrak{S}' = (\mathfrak{C}/\varrho\,|\,\Omega, \Omega^*)$, a correspondência $a \to C_a$ é um homomorfismo. Recìprocamente, dum homomorfismo entre dois sistemas algébricos *semelhantes*, isto é, com os mesmos domínios Ω e Ω^*, deduz-se uma relação de congruência ϱ, em $\mathfrak{S}$, tomando como equivalentes os elementos que têm o mesmo correspondente em $\mathfrak{S}'$. As duas afirmações, directa e recíproca, que acabamos de fazer, constituem o que costuma designar-se por «teorema do homomorfismo». Duma maneira mais expressa, tratá-lo-emos em (III, 1, 9), para o caso especial dos grupos.

O produto $\alpha\beta$ de duas relações de equivalência, nos termos em que foi definido em (I, 1, 4), não é, em geral, uma relação de equivalência. De $a(\alpha\beta)b$ não se deduz, em geral, $b(\alpha\beta)a$, mas simplesmente se deduz $b(\beta\alpha)a$. Tem lugar, porém, o seguinte

TEOREMA: *É condição necessária e suficiente, para que o produto de duas relações de equivalência (ou de congruência) seja uma relação de equivalência (de congruência), que as referidas relações sejam comutáveis:* $\alpha\beta = \beta\alpha$. De facto, se $\alpha\beta$ é uma relação de equivalência, de $a(\alpha\beta)b$ deduz-se $b(\alpha\beta)a$, consequentemente $b\alpha x$, $x\beta a$, para um certo x. Depois, de $a\beta x$, $x\alpha b$, conclui-se $a(\beta\alpha)b$. Assim $\alpha\beta \gtrless \beta\alpha$, na notação introduzida em (I, 1, 5). Anàlogamente, é $\beta\alpha \gtrless \alpha\beta$, pelo que $\alpha\beta = \beta\alpha$. Inversamente, tendo-se $\alpha\beta = \beta\alpha$, fácil é de demonstrar a transitividade do produto, por exemplo. Na verdade, sendo $a(\alpha\beta)b$, $b(\alpha\beta)c$, vem $a[(\alpha\beta)(\alpha\beta)]c = a(\alpha^2\beta^2)c$, desde que se escreva $\alpha\alpha = \alpha^2$, $\beta\beta = \beta^2$. A reflexividade e a transitividade de α levam a $\alpha^2 = \alpha$, de sorte que $a(\alpha^2\beta^2)c = a(\alpha\beta)c$, o que exprime a transitividade de $\alpha\beta$. Quanto às congruências, tomemos duas relações de congruência θ_1 e θ_2. Do facto de ser $a(\theta_1\theta_2)b$, $c(\theta_1\theta_2)d$, tira-se $a\theta_1 x$, $x\theta_2 b$, assim como $c\theta_1 y$, $y\theta_2 d$. Logo é $(a\lambda^* c)\theta(x\lambda^* y)$, $(x\lambda^* y)\theta_2(b\lambda^* d)$, consequentemente $(a\lambda^* c)(\theta_1\theta_2)(b\lambda^* d)$, como se deseja.

2) **Subgrupos** — No § 1 do capítulo anterior, situámos já, dentro da teoria geral dos grupoides e dos semi grupos, aqueles semi-grupos que são formados de elementos todos regulares e aos quais demos a designação de grupos. Em termos de operações o grupo apareceu-nos como um sistema algébrico com uma operação binária (produto), uma operação de ordem zero (fixação do elemento u = identidade) e uma operação unária (correspondência biunívoca $a \leftrightarrow a^{-1}$). Além disso era válida a lei associativa.

Seja $\mathfrak{G}$ um grupo. Um conjunto $\mathfrak{g}$, de elementos de $\mathfrak{G}$, diz-se um *subgrupo*, se for um grupo. Em $\mathfrak{g}$ verificar-se-ão, portanto, os postulados que constituem o 4.º sistema indicado em (II, 1, 5). O postulado da associatividade é aqui uma consequência necessária, logo que tenha lugar G_1'''). Assim, podemos dizer que $\mathfrak{g}$ é subgrupo, se: 1) supondo $a, b \in \mathfrak{g}$, é $ab \in \mathfrak{g}$; 2) as equações $xa = b$ e $ay = b$ são solúveis em $\mathfrak{g}$. Como a solução de $xa = b$ é ba^{-1}, vamos provar o seguinte

TEOREMA 1: *É necessário e suficiente, para que* $\mathfrak{g}$ *seja um subgrupo, que, com* a *e* b, *contenha* ba^{-1} (*ou* $a^{-1}b$). Vimos já que a condição é necessária. Vamos provar a suficiência. Sendo $a \in \mathfrak{g}$, a hipótese garante ser $aa^{-1} = u \in \mathfrak{g}$. O postulado G_3''), de (II, 1, 5), é verificado. Em seguida, pertencendo a e u a $\mathfrak{g}$, também $ua^{-1} = a^{-1} \in \mathfrak{g}$, o que mostra ser válido o postulado G_4''), do mesmo

lugar. Como o postulado G_2'') é verificado, se tiver lugar o postulado G_1''), é este último que nos resta demonstrar. Supondo $a, b \in \mathfrak{g}$, sabemos que $a^{-1} \in \mathfrak{g}$. Então, $b(a^{-1})^{-1} = ba \in \mathfrak{g}$ e o teorema fica estabelecido. [Se tratássemos a equação $ay = b$, obteríamos como critério de subgrupo a condição $a^{-1}b \in \mathfrak{g}$. Por outro lado, se a e b se trocam, também podemos pôr qualquer das condições: $ab^{-1} \in \mathfrak{g}$, $b^{-1}a \in \mathfrak{g}$].

Entre os subgrupos dum grupo figura sempre o *grupo unidade*, formado pelo único elemento u do grupo.

Um subgrupo é *próprio*, quando é diferente do grupo. Também o grupo se considera um subgrupo (*impróprio*) do grupo.

Considerando $\mathfrak{G}$ como um semi-grupo, se $\mathfrak{H}$ fôr um subsemi-grupo, a hipótese de $\mathfrak{H}$ ser finito implica que $\mathfrak{H}$ seja subgrupo [Teorema 2 de (II, 1, 5)].

Tomemos um conjunto de elementos $a, b, c, \cdots \in \mathfrak{G}$, conjunto que pode ser finito ou infinito. Diz-se *subgrupo gerado* por estes elementos o mais pequeno subgrupo que os contém. Qualquer subgrupo que contenha os elementos contém necessàriamente todos os elementos da forma

$$(1) \qquad a^r \cdots b^s \cdots c^t \cdots a^{-r'} \cdots b^{-s'} \cdots c^{-t'},$$

em cada um dos quais o número de factores é finito e os expoentes são inteiros. Vamos verificar que a totalidade dos elementos do tipo (1) constitui um subgrupo, ao qual pertencem $a, b, c, \cdots$. Será, por isso, o subgrupo procurado. Claramente que $a, b, c, \cdots$ entram no tipo (1). O inverso dum elemento do tipo (1) tendo o aspecto

$$c^{t'} \cdots b^{s'} \cdots a^{r'} \cdots c^{-t} \cdots b^{-s} \cdots a^{-r}$$

é ainda da mesma forma, o mesmo se dizendo do produto de dois elementos do tipo (1). O critério de subgrupo é aplicável e a afirmação fica demonstrada.

Observação: Ao escrever-se (1), dizendo que os expoentes r, s, etc. são inteiros, não havia necessidade de utilizar os expoentes $-r$, $-s$, etc. Se isso se faz, é ùnicamente com o objectivo de chamar a atenção para os expoentes negativos.

A noção de subgrupo entra na definição geral de subsistema algébrico dada em (II, 2, 1).

3) **Grupos cíclicos** — Entre os subgrupos gerados por certos elementos, vamos destacar o subgrupo gerado por um único elemento $a \in \mathfrak{G}$. Esse subgrupo será da forma

$$(1) \qquad \mathfrak{Z} = \{ \cdots, a^{-r}, \cdots, u, a, \cdots, a^n, \cdots \}.$$

Em princípio, todas as potências de a são distintas. Vamos ver, porém, que, se houver duas potências iguais, o subgrupo $\mathfrak{Z}$, chamado *grupo cíclico gerado por* a, tem apenas um número finito de elementos. Esse número, m por exemplo, diz-se, então, *ordem* do elemento a e *ordem do grupo* $\mathfrak{Z}$. Ponhamos $a^h = a^k$ e admitamos $h > k$. Da igualdade anterior, tira-se $a^{h-k} = a^k \cdot a^{-k} = u$. Conclui-se, assim, que há potências de expoente $h - k > 0$ tais que $a^{h-k} = u$. Designemos por m o mais pequeno expoente positivo tal que $a^m = u$. Mostraremos que o grupo cíclico se compõe dos m elementos seguintes:

$$(2) \qquad \mathfrak{Z} = \{ u, a, a^2, \cdots, a^{m-1} \}.$$

Para isso, teremos de provar os dois factos seguintes: 1) que as potências de a, figurando em (2), são todas diferentes: 2) que qualquer outra potência de a é igual a uma daquelas. Se houvesse, em (2), duas potências iguais, teríamos $a^r = a^{r'}$, $r > r'$, $r - r' < m$, e seria $a^{r-r'} = u$, havendo um expoente positivo $q < m$ para o qual $a^q = u$, o que não pode ter lugar. Os elementos de (2) são, pois, todos distintos. Seja agora uma potência a^s, com $s \neq 0, 1, 2, \cdots, m-1$. Podemos escrever sempre, como vimos em (II, 3, 2), $s = mq + r$, onde $0 \leqslant r < m$. Este facto acarreta $a^s = a^{mq+r} = a^{mq} \cdot a^r = (a^m)^q \cdot a^r = a^r$, de modo que se reproduz um elemento de $\mathfrak{Z}$ da forma (2), como se afirmou.

A ordem do elemento a é *infinita*, quando o subgrupo $\mathfrak{Z}$ tem uma infinidade de elementos.

De futuro, sempre que tenhamos de utilizar números inteiros, admitiremos para estes as diferentes propriedades conhecidas. Os números pares formam, no grupo aditivo dos inteiros, um grupo cíclico. O elemento gerador é 2. O próprio grupo dos inteiros é um grupo cíclico gerado por 1.

Consideremos o grupo cíclico (1) e um seu subgrupo $\mathfrak{g} = \{ \cdots, a^{-t}, \cdots, a^{-v}, \cdots, u, \cdots, a^{v'}, \cdots, a^{t'}, \cdots \}$. Vamos provar o seguinte

TEOREMA 1: *Todo o subgrupo dum grupo cíclico é igualmente um grupo cíclico.* Designemos por a^p a potência de menor expoente positivo que figura no subgrupo. Suporemos, é claro, $p \neq 0$, pois que, se não houvesse potências positivas no subgrupo, também não podia haver potências negativas, e o subgrupo reduzir-se-ia ao grupo unidade. Se $a^{v'}$ é agora outra poténcia de expoente positivo, também pertencente a $\mathfrak{g}$, pondo $v' = cp + r$, com $0 \leqslant r < p$, tem-se $a^{v'} = a^{cp+r} = (a^p)^c \cdot a^r$. Se $r = 0$, $a^{v'}$ é uma poténcia de a^p. Supondo $r \neq 0$, como $a^{v'}$ e $(a^p)^c$ pertencem ao subgrupo, a^r pertencerá igualmente ao subgrupo, o que não pode ter lugar, por ser $r < p$. Assim, todas as potências de expoente positivo são potências do elemento a^p. Relativamente a uma potência de expoente negativo a^{-v}, vale, para o seu inverso, $a^v = (a^p)^d$, pelo que $a^{-v} = (a^p)^{-d}$. O subgrupo $\mathfrak{g}$ é, pois, gerado por a^p.

No caso dos grupos cíclicos finitos, pode precisar-se que o expoente p é divisor da ordem do grupo $\mathfrak{Z}$. Seja n essa ordem. Se p não dividisse n, este último estaria compreendido entre dois múltiplos consecutivos de p, a saber: $(k-1)p < n < kp$. A diferença $kp - n > 0$ seria inferior a p, e, tendo-se $a^{kp-n} = a^{kp} \cdot a^{-n} = a^{kp}$, o subgrupo conteria o elemento $a^{kp} = a^{kp-a}$, no qual o expoente de a seria inferior a p, contra a hipótese.

Vê-se, como consequência, que todos os elementos do subgrupo do grupo cíclico são potências cujos expoentes têm factores comuns com n. Se um subgrupo tem uma potência com um expoente primo com n, o subgrupo é necessàriamente igual ao grupo. É válido este

TEOREMA 2: *Se a ordem dum elemento* a *dum grupo é igual a* n, *a ordem do elemento* a^q, *supondo* q *primo com* n, *é também igual a* n. Se supusermos $a^q = b$, resulta o seguinte

COROLÁRIO 1: *A equação* $b^x = a^r$, *na incógnita* x, *é sempre solúvel.*

As considerações feitas podem resumir-se neste

TEOREMA 3: *Sejam* $\mathfrak{Z}$ *um grupo cíclico gerado por* a *e* $\mathfrak{g}$ *um subgrupo de* $\mathfrak{Z}$ *diferente do grupo unidade. Supondo* p *o mais pequeno inteiro positivo tal que* $a^p \in \mathfrak{g}$, *é* a^p *o elemento gerador de* $\mathfrak{g}$. *Se* $\mathfrak{Z}$ *é infinito, a correspondência* $\mathfrak{g} \to p$ *é uma correspondência biunívoca entre os subgrupos de* $\mathfrak{Z}$ *diferentes do grupo unidade e os números inteiros e positivos. Se* $\mathfrak{Z}$ *é finito, de ordem* n, *a correspondência* $\mathfrak{g} \to p$ *é uma correspondência biunívoca entre os subgrupos de* $\mathfrak{Z}$ *diferentes do grupo unidade e os números inteiros e positivos que são divisores de* n. *Continuando a supôr* $\mathfrak{Z}$ *finito, todo o seu subgrupo tem uma ordem que divide a ordem de* $\mathfrak{Z}$, *havendo em* $\mathfrak{Z}$ *um único subgrupo de cada ordem possível.*

Consideremos agora um grupo cíclico $\mathfrak{Z}$, de ordem $n = tm$, em que t e m são primos entre si. Se a for o gerador, tem lugar o

TEOREMA 4: *O gerador* a, *de* $\mathfrak{Z}$, *pode representar-se, e de uma só maneira, como produto de dois elementos de* $\mathfrak{Z}$, *de ordens* t *e* m, *respectivamente.* Ponhamos $a^t = \gamma$, $a^m = \beta$. A ordem de γ é m e a ordem de β é t. Formemos, em seguida, os produtos da forma $\beta^r \gamma^s, (r = 1, 2, \cdots, t;\ s = 1, 2, \cdots, m)$. Vamos ver que os tm elementos do grupo cíclico, assim obtidos, são todos diferentes. Imaginemos que poderia ser $\beta^r \gamma^s = \beta^{r'} \gamma^{s'}$, ou $\beta^{r-r'} = \gamma^{s'-s} = d$. O elemento d pertenceria simultâneamente aos dois grupos cíclicos

$$|\, \beta^0 = u, \beta, \cdots, \beta^{t-1} \,|, \quad |\, \gamma^0 = u, \cdots, \gamma^{m-1} \,|.$$

O subgrupo cíclico de $\mathfrak{Z}$, gerado por d, teria uma ordem que dividiria t e m. Essa ordem seria a unidade, o que levaria a $d = u$, ou seja a $\beta^r = \beta^{r'}$, $\gamma^s = \gamma^{s'}$, $r = r'$, $s = s'$, contra a hipótese de um dos números r' ou s', pelo menos, ser diferente de um dos números r ou s. Existem, pois, números $r_1 \leqslant t$, $s_1 \leqslant m$ tais que $\beta^{r_1} \gamma^{s_1} = a^{mr_1 + ts_1} = a$. A soma $mr_1 + ts_1$ não podendo ser superior a $2tm$, mas sendo superior à unidade, é tal que $mr_1 + ts_1 = tm + 1$, ou $ts_1 + m(r_1 - t) = 1$, o que incidentalmente nos mostra o seguinte: dados dois números primos entre si, t e m, existem números inteiros s'' e r'' tais que $ts'' + mr'' = 1$. Pondo $\beta^{r_1} = a^{mr_1} = b$, $\gamma^{s_1} = a^{ts_1} = c$, é, assim, $bc = a$. Ora, as ordens de b e c são, respectivamente, t e m. Se, com efeito, a ordem de b, por exemplo, pudesse ser $t' < t$, ter-se-ia $(bc)^{t'm} = a^{t'm} = b^{t'm} \cdot c^{t'm} = c^{t'm} = a^{ts_1 t'm} = u$, e a ordem do grupo (ordem de a) seria inferior a tm, contra a hipótese. Vê-se, finalmente, que não pode haver duas potências a^p e a^q, diferentes das anteriores potências a^{mr_1} e a^{ts_1}, das ordens t e m, respectivamente, e tais que $a^{p+q} = a$, raciocinando do modo seguinte: se fosse $a = a^p \cdot a^q = a^{p+q} = a^{mr_1 + ts_1}$, com $a^{pt} = u$, $a^{qm} = u$, ter-se-ia $a^{p+q-(mr_1+ts_1)} = u$, com $p + q = mr_1 + ts_1$. De facto, como a soma $p + q$ não chega a ser $2tm$ e

como $mr_1+ts_1=tm+1$, não há outra possibilidade. Mas é $pt=ktm$, $qm=k'tm$, com certos inteiros k e k'. Então, vem $p=km$, $q=k't$ e $km+k't=mr_1+ts_1$ ou $m(k-r_1)=t(s_1-k')$. Desta relação conclui-se $s_1-k'=\alpha m$, $k-r_1=\beta t=\alpha t$, e, portanto,

$$a^p=a^{km}=a^{r_1m+\alpha tm}=a^{r_1m}, \qquad a^q=a^{k't}=a^{s_1t-\alpha mt}=a^{s_1t},$$

como se queria demonstrar.

Dum modo geral, seja N a ordem dum grupo cíclico gerado pelo elemento a. Escrevendo $N=p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$, onde $p_1,p_2,\cdots,p_s$ são números primos diferentes, vê-se que a é sempre um produto de s elementos do grupo cíclico, de ordens $p_1^{r_1},p_2^{r_2},\cdots,p_s^{r_s}$, respectivamente. Basta, na verdade, começar por pôr $t=p_1^{r_1}$, $m=p_2^{r_2}\cdots p_s^{r_s}$, e continuar o processo, que, em segundo lugar, se aplica ao elemento gerador dum grupo cíclico de ordem m. No número 5 mostraremos que os diferentes factores de a são ainda bem determinados.

4) **Complexos associados dum subgrupo** — Sejam $\mathfrak{G}$ um grupo e $\mathfrak{g}$ um subgrupo. É fácil de demonstrar que a seguinte relação ρ é uma relação de equivalência em $\mathfrak{G}$: $a\rho b$, se e só se $b\in a\mathfrak{g}$. Demonstremos, por exemplo, a propriedade simétrica. Admitamos que se tem $a\rho b$; precisamos de provar que $b\rho a$, ou seja que $a\in b\mathfrak{g}$. Na verdade, supondo $b=ag$, com $g\in\mathfrak{g}$, é também $a=bg^{-1}$, com $g^{-1}\in\mathfrak{g}$.

A referida relação de equivalência permite dividir $\mathfrak{G}$ em classes de equivalência, podendo escrever-se aqui, de harmonia com (I, 1, 4), e pondo $\rho=\rho_e$:

$$\mathfrak{G}/\rho_e=|\,\mathfrak{g},a\mathfrak{g},b\mathfrak{g},\cdots\,|. \tag{1}$$

Estas classes chamam-se *complexos associados esquerdos do subgrupo* $\mathfrak{g}$ ou *classes associadas esquerdas* do mesmo subgrupo.

Se o grupo $\mathfrak{G}$ for finito, as diferentes classes têm todas o mesmo número de elementos.

Poderíamos ter definido, anàlogamente, as *classes associadas direitas* de $\mathfrak{g}$ e dividir $\mathfrak{G}$ em classes de equivalência sob a forma

$$\mathfrak{G}/\rho_d=|\,\mathfrak{g},\mathfrak{g}a,\mathfrak{g}b,\cdots\,|. \tag{2}$$

É evidente que, no geral, as classes direitas são distintas das classes esquerdas com o mesmo representante. E, de $a\mathfrak{g}\neq\mathfrak{g}a$, conclui-se $\rho_e\neq\rho_d$. Passa-se fàcilmente das classes esquerdas às direitas. Por

exemplo: $(a\mathfrak{g})^{-1}=\mathfrak{g}^{-1}a^{-1}=\mathfrak{g}a^{-1}$, visto que $\mathfrak{g}^{-1}=\mathfrak{g}$, se $\mathfrak{g}^{-1}$ representar o conjunto dos elementos inversos dos elementos de $\mathfrak{g}$. De cada classe esquerda, obtém-se, pelo processo indicado, uma e uma só classe direita. E a classes esquerdas distintas correspondem classes direitas distintas, pois que, inversamente, se passa das direitas para as esquerdas.

Dividido $\mathfrak{G}$ em classes esquerdas, por exemplo, cada classe contém, como sabemos, os diferentes elementos do grupo que são equivalentes a qualquer elemento da classe. Supondo $a\rho a_1$, é indiferente tomar a ou a_1 como representante da classe. O critério de equivalência de a e a_1 é $a^{-1}a_1\in\mathfrak{g}$, ou $a_1^{-1}a\in\mathfrak{g}$. Para a divisão em classes direitas, esse critério é $aa_1^{-1}\in\mathfrak{g}$, ou $a_1a^{-1}\in\mathfrak{g}$.

A intersecção $\mathfrak{g}\cap\mathfrak{h}$, de dois subgrupos de $\mathfrak{G}$, é também um subgrupo. Se ρ e σ forem as relações de equivalência respectivamente definidas pelos subgrupos, é $\rho\wedge\sigma$ a relação de equivalência definida pelo subgrupo intersecção [cfr. (I, 1, 6)].

No caso dos grupos finitos, o número de classes (1) ou (2) diz-se *índice* do subgrupo. E o número de elementos do grupo diz-se *ordem* do grupo. Para os grupos finitos, é válido, pois, este

TEOREMA 1: *O índice* i, *dum subgrupo, é divisor da ordem* N *do grupo.* Basta ter em conta, com efeito, que as diferentes classes associadas dum subgrupo têm todas o mesmo número de elementos, que é o número n dos elementos do subgrupo. É válida a relação $N=in$. Resulta daqui esta proposição de *Lagrange*:

COROLÁRIO 1: *Nos grupos finitos, a ordem dum subgrupo é um divisor da ordem do grupo.* Em particular:

COROLÁRIO 2: *Nos grupos finitos, a ordem de qualquer elemento é um divisor da ordem do grupo.*

5) **Aplicação** — Em correlação com os resultados estabelecidos nos dois números anteriores, daremos aqui algumas proposições. Assim:

TEOREMA 1: *Se* a *e* b *são dois elementos comutáveis dum grupo* $\mathfrak{G}$, *de ordens* p *e* q, *primas entre si, o produto* ab *é da ordem* pq. Por hipótese, tem-se $a^p=u$, $b^q=u$, $(ab)^{pq}=(a^p)^q(b^q)^p=u$. Deste

modo, pq é um múltiplo do ordem de ab. Se essa ordem pudesse ser $h<pq$, ter-se-ia $a^h \cdot b^h = u$ e $a^h = b^{-h}$. Pondo $d = a^h = b^{-h}$, o elemento d, que pertenceria aos subgrupos cíclicos gerados por a e b, seria duma ordem que dividiria as ordens de a e de b. Só poderia ter-se $d = u$, e, então, $a^h = b^h = u$ mostraria que h seria um múltiplo comum de p e de q, pelo menos igual ao seu menor múltiplo comum pq.

Existe um teorema que, em certo sentido, se pode imaginar inverso do anterior. É o seguinte.

TEOREMA 2: *Num grupo qualquer, um elemento* a, *da ordem* $n = tm$, *em que* t *e* m, *são primos entre si, é sempre o produto de dois elementos comutáveis,* b *e* c, *de ordens* t *e* m, *respectivamente.* Consideremos o grupo cíclico gerado por a. Os elementos b e c, referidos no n.º 3, teorema 4, satisfazem ao enunciado. Provaremos mais este

ADITAMENTO AO TEOREMA 2: *A decomposição enunciada para* a *tem lugar no grupo cíclico gerado por* a *e apenas nesse grupo.* Suponhamos, com efeito, que dois elementos d e f do grupo respondem à questão. Vamos demonstrar que são idênticos a b e c, respectivamente. Pondo $a = df$, $a^t = d^t f^t = f^t$, vê-se que f^t é uma potência de a. No grupo cíclico gerado por f, grupo que é da ordem m, por hipótese, o elemento f^t, cujo expoente é primo com m e podemos supor menor que m, gera o mesmo grupo que f. Isso significa que f é uma potência de f^t, e, portanto, uma potência de a. Mas, então, d é igualmente uma potência de a e o aditamento fica justificado.

Retomemos agora as considerações finais de (III, 1, 3). Se chegamos a escrever $a = a_1 a_2 \cdots a_s$, com a_i de ordem $p_i^{r_i}$, $(i = 1, 2, \cdots s)$, sabemos que $b = a_1$ tem a ordem $p_1^{r_1}$ e $c = a_2 \cdots a_s$ tem a ordem $p_2^{r_2} \cdots p_s^{r_s}$. Então, a_1 e c são bem determinados. Desde que a_2 tem a ordem $p_2^{r_2}$ e $d = a_3 \cdots a_s$ a ordem $p_3^{r_3} \cdots p_s^{r_s}$, tanto a_2 como d são bem determinados. E o raciocínio prossegue, a fim de se concluir, como lá se afirmou, que os a_i são bem determinados.

6) **Divisores normais ou subgrupos invariantes** — Dados um grupo $\mathfrak{G}$ e um subgrupo $\mathfrak{g}$, este último diz-se um *divisor normal* ou um *subgrupo invariante*, se, para cada $a \in \mathfrak{G}$, pôr $a\mathfrak{g} = \mathfrak{g}a$. Toda a classe associada esquerda de $\mathfrak{g}$ é também classe associada direita.

Um grupo diz-se *simples* ou *irredutível*, se os seus subgrupos invariantes (mais simplesmente: os seus invariantes) forem apenas o grupo unidade e o próprio grupo.

Tomemos, por exemplo, um subgrupo $\mathfrak{g}$, de índice 2. O grupo divide-se em duas classes esquerdas, $\mathfrak{g}$ e $a\mathfrak{g}$, ou em duas classes direitas, $\mathfrak{g}$ e $\mathfrak{g}b$. O elemento a não pertence a $\mathfrak{g}$, pelo que pertence a $\mathfrak{g}b$. Esta última classe direita admite, assim, o elemento a como representante. Será $\mathfrak{g}b = \mathfrak{g}a$, e, consequentemente, $\mathfrak{g}a = a\mathfrak{g}$. Logo: todo o subgrupo de índice 2 é um invariante.

Todo o invariante dum grupo é invariante dum subgrupo que o contenha, como resulta imediatamente da definição. Utilizaremos frequentemente a letra $\mathfrak{H}$ para significar invariante de $\mathfrak{G}$.

Regressaremos a $\mathfrak{G}$ e a um subgrupo qualquer $\mathfrak{g}$. Consideremos a equivalência ϱ_e, referida em (III, 1, 4), e procuremos uma condição necessária e suficiente a que deva satisfazer $\mathfrak{G}$, a fim de que, supondo $x \varrho_e y$, $x' \varrho_e y'$, se tenha também $(xx') \varrho_e (yy')$. Das condições $y \in x\mathfrak{g}$, $y' \in x'\mathfrak{g}$ deverá resultar $yy' \in (xx')\mathfrak{g}$, ou seja $x\mathfrak{g} \cdot x'\mathfrak{g} \subseteq (xx')\mathfrak{g}$, sendo x e x' arbitrários. A inclusão anterior é equivalente a $\mathfrak{g}x'\mathfrak{g} \subseteq x'\mathfrak{g}$, deduzindo-se daqui $\mathfrak{g}x' \subseteq x'\mathfrak{g}$, que, por sua vez é equivalente aquela. Assim, uma condição necessária e suficiente, para que ϱ_e tenha a propriedade indicada é a seguinte:

$$\mathfrak{g}x' \subseteq x'\mathfrak{g}, \qquad (x' \in \mathfrak{g}). \tag{1}$$

Esta condição leva a $x'^{-1}\mathfrak{g}x' \subseteq \mathfrak{g}$, e, substituindo x' por x'^{-1}, leva também a $x'\mathfrak{g}x'^{-1} \subseteq \mathfrak{g}$. Será, pois, $\mathfrak{g} \subseteq x'^{-1}\mathfrak{g}x'$, o que acarreta $\mathfrak{g} = x'^{-1}\mathfrak{g}x'$ ou $x'\mathfrak{g} = \mathfrak{g}x'$. Inversamente, desta última igualdade deduz-se (1). Podemos dizer:

TEOREMA 1: *É condição necessária e suficiente, para que* $\mathfrak{H}$ *seja um invariante, que se tenha, quaisquer que sejam* $x, x' \in \mathfrak{G}$, $(x\mathfrak{H})(x'\mathfrak{H}) \subseteq (xx')\mathfrak{H}$. *Mais precisamente: que se tenha* $(x\mathfrak{H})(x'\mathfrak{H}) = (xx')\mathfrak{H}$. Efectivamente, se $\mathfrak{H}$ é invariante, tem-se $(x\mathfrak{H})(x'\mathfrak{H}) = x(\mathfrak{H}x')\mathfrak{H} = (xx')\mathfrak{H}\mathfrak{H} = (xx')\mathfrak{H}$. Por outro lado, uma igualdade implica inclusão em qualquer dos sentidos.

7) **Algumas propriedades dos invariantes** — Sejam $\mathfrak{h}$ e $\mathfrak{g}$ dois subgrupos e entenda-se o produto $\mathfrak{h}\mathfrak{g}$ como o conjunto dos elementos obtidos multiplicando um elemento de $\mathfrak{h}$ por um elemento de $\mathfrak{g}$. Em

geral, $\mathfrak{h}\mathfrak{g}$ não é um subgrupo. Tem lugar, todavia, a seguinte proposição:

TEOREMA 1: *O produto $\mathfrak{h}\mathfrak{g}$ é um subgrupo, se $\mathfrak{g}$ for um invariante.* Trata-se de utilizar o critério de subgrupo e de demonstrar que, sendo $hg \in \mathfrak{h}\mathfrak{g}$, $h'g' \in \mathfrak{h}\mathfrak{g}$, com $h, h' \in \mathfrak{h}$ e $g, g' \in \mathfrak{g}$, se tem $(hg)(h'g')^{-1} \in \mathfrak{h}\mathfrak{g}$. Ora $hg(h'g')^{-1} = hgg'^{-1}h'^{-1} = hg''h'^{-1} = hh'^{-1}g''' = h''g''' \in \mathfrak{h}\mathfrak{g}$, [$gg'^{-1} = g'' \in \mathfrak{g}$, $hh'^{-1} = h'' \in \mathfrak{h}$]. Na passagem da antepenúltima para a penúltima expressão, na sucessão anterior de igualdades, utilizámos a propriedade de ser $\mathfrak{g}$ um invariante, de sorte que a condição $\mathfrak{g}h'^{-1} = h'^{-1}\mathfrak{g}$ implica se tenha $g''h'^{-1} = h'^{-1}g'''$, para um certo $g''' \in \mathfrak{g}$. Podemos observar que se tem $\mathfrak{h}\mathfrak{g} = \mathfrak{g}\mathfrak{h}$ e que o subgrupo $\mathfrak{h}\mathfrak{g}$ é o mais pequeno subgrupo contendo $\mathfrak{h}$ e $\mathfrak{g}$. É, por isso, o subgrupo gerado por $\mathfrak{h}$ e $\mathfrak{g}$.

Sejam $\mathfrak{H}$ e $\mathfrak{H}'$ dois invariantes e ponhamos $\mathfrak{P} = \mathfrak{H}\mathfrak{H}'$. Vamos mostrar que $\mathfrak{P}$ é um invariante. Fá-lo-emos verificando ser $a\mathfrak{P}a^{-1} \subseteq \mathfrak{P}$, para qualquer $a \in \mathfrak{G}$. Ora $a\mathfrak{P}a^{-1} = a\mathfrak{H}\mathfrak{H}'a^{-1} = a\mathfrak{H}a^{-1} \cdot a\mathfrak{H}'a^{-1} \subseteq \mathfrak{H}\mathfrak{H}' = \mathfrak{P}$, pois que $a\mathfrak{H}a^{-1} \subseteq \mathfrak{H}$, $a\mathfrak{H}'a^{-1} \subseteq \mathfrak{H}'$.

Também a intersecção de dois invariantes é um invariante. Trata-se de provar que, sendo $\mathfrak{H}$ e $\mathfrak{H}'$ dois invariantes, é $\mathfrak{D} = \mathfrak{H} \cap \mathfrak{H}'$ um invariante. Tendo-se $a\mathfrak{D}a^{-1} \subseteq a\mathfrak{H}a^{-1} \subseteq \mathfrak{H}$, e, anàlogamente, $a\mathfrak{D}a^{-1} \subseteq a\mathfrak{H}'a^{-1} \subseteq \mathfrak{H}'$, vê-se que $a\mathfrak{D}a^{-1} \subseteq \mathfrak{H} \cap \mathfrak{H}' = \mathfrak{D}$, o que justifica a afirmação. Convém fixar este

TEOREMA 2: *O produto e a intersecção de invariantes são invariantes.*

Provaremos agora as proposições a seguir.

TEOREMA 3: *Se $\mathfrak{g}$ é um subgrupo e $\mathfrak{H}$ um invariante, a intersecção $\mathfrak{g} \cap \mathfrak{H}$ é um invariante em $\mathfrak{g}$.* Temos de estabelecer a relação de inclusão $a(\mathfrak{g} \cap \mathfrak{H})a^{-1} \subseteq \mathfrak{g} \cap \mathfrak{H}$, $(a \in \mathfrak{g})$. Se observarmos que $a\mathfrak{g}a^{-1} \subseteq \mathfrak{g}$, $a(\mathfrak{g} \cap \mathfrak{H})a^{-1} \subseteq \mathfrak{g}$, $a\mathfrak{H}a^{-1} \subseteq \mathfrak{H}$, $a(\mathfrak{g} \cap \mathfrak{H})a^{-1} \subseteq \mathfrak{H}$, concluimos, como se deseja, $a(\mathfrak{g} \cap \mathfrak{H})a^{-1} \subseteq \mathfrak{g} \cap \mathfrak{H}$.

TEOREMA 4: *Se dois invariantes $\mathfrak{H}$ e $\mathfrak{H}'$ têm como único elemento comum o elemento um, os elementos de cada um deles comutam individualmente com os elementos do outro.* Para fazermos a demonstração, começemos por definir o *comutador* de dois elementos. Dados $a, b \in \mathfrak{G}$, o seu comutador é o elemento $(ab)(ba)^{-1} = abab^{-1}a^{-1}b^{-1}$. Feito isto, sejam $a \in \mathfrak{H}$, $a' \in \mathfrak{H}'$. O comutador $(aa')(a'a)^{-1} = aa'a^{-1}a'^{-1}$ pode escrever-se de duas maneiras diferentes: sob a forma $aa'a^{-1} \cdot a'^{-1}$, vê-se que pertence a $\mathfrak{H}'$, por ser o produto de dois elementos de $\mathfrak{H}'$; sob a forma $a \cdot a'a^{-1}a'^{-1}$, vê-se que pertence a $\mathfrak{H}$, por ser o produto de dois elementos de $\mathfrak{H}$. Será, assim, $aa'(a'a)^{-1} = u$, ou seja $aa' = a'a$. Os elementos a e a' comutam, como se afirmou.

8) **Homomorfismos e isomorfismos** — Démos em (II, 2, 1) as definições gerais que se prendem com a noção de homomorfismo. Em particular, no caso dos grupos, podemos afirmar, como já fizemos em (II, 2, 2):

TEOREMA 1: *Considerado o homomorfismo $\mathfrak{G} \sim \mathfrak{G}'$, se $\mathfrak{G}$ é grupo e $\mathfrak{G}'$ é um grupoide, então $\mathfrak{G}'$ é um grupo.* Neste enunciado pressupõe-se que o homomorfismo respeita à única operação de produto. Isso basta para que o homomorfismo tenha também lugar para a operação de ordem zero e para a operação unária, que existem em $\mathfrak{G}$, por hipótese. Depois, a propriedade associativa em $\mathfrak{G}'$ é também uma consequência necessária.

Tomemos o grupo $\mathfrak{G}$ e consideremos o endomorfismo $x \to x' \in \mathfrak{G}$. Escreveremos $x' = x\eta$, utilizando a letra grega η para significar o endomorfismo. Podemos dizer:

COROLÁRIO 1: *Se η é um endomorfismo de $\mathfrak{G}$, então $\mathfrak{G}\eta$ é um subgrupo de $\mathfrak{G}$.*

Tendo-se um homomorfismo do espaço algébrico $\mathfrak{S}$ sobre $\mathfrak{S}^*$ e deste sobre $\mathfrak{S}^{**}$, pode definir-se um homomorfismo $\mathfrak{S} \sim \mathfrak{S}^{**}$, por intermédio de $\mathfrak{S}^*$. Vê-se, assim, que *a relação de homomorfismo é transitiva.* A referida relação é também reflexa, pois podemos imaginar os elementos de $\mathfrak{S}$ como as suas próprias imagens.

A relação de isomorfismo é reflexa, simétrica e transitiva, como se conclui muito simplesmente.

Em correlação com os conceitos de meromorfismo e de automorfismo, têm lugar certos resultados de que passamos a ocupar-nos.

TEOREMA 2: *Se um grupo $\mathfrak{G}$ possui um meromorfismo autêntico $\mathfrak{G} \simeq \mathfrak{G}\sigma$, o grupo admite a cadeia infinita de subgrupos $\mathfrak{G} \supset \mathfrak{G}\sigma \supset \mathfrak{G}\sigma^2 \supset \cdots$, sem sinal = entre quaisquer termos da sucessão.* Claramente que, no enunciado, deve entender-se que $\mathfrak{G}\sigma^{k+1} =$

$=(\mathfrak{G}\sigma^k)\sigma$. Por hipótese, σ é meromorfismo autêntico, ou seja $\mathfrak{G}\supset\mathfrak{G}\sigma$ significa uma inclusão no sentido próprio. Será necessàriamente $\mathfrak{G}\sigma\supset\mathfrak{G}\sigma^2$, porque, sendo $\mathfrak{G}\simeq\mathfrak{G}\sigma$, aos elementos $\mathfrak{G}\sigma$, contidos em $\mathfrak{G}$, correspondem os elementos $(\mathfrak{G}\sigma)\sigma=\mathfrak{G}\sigma^2$, de $\mathfrak{G}\sigma$, que não podem abranger a totalidade deste último, visto que essa totalidade corresponde a $\mathfrak{G}$.

COROLÁRIO 2: *Num grupo finito não pode haver um meromorfismo autêntico.*

Os automorfismos dum espaço algébrico $\mathfrak{G}$ formam um grupo. Se o espaço é um grupo $\mathfrak{G}$, define-se o chamado *grupo automórfico* de $\mathfrak{G}$, que representaremos por $A_{\mathfrak{G}}$.

Dado $x\in\mathfrak{G}$, consideremos a correspondência $x\to axa^{-1}=x'$, em que $a\in\mathfrak{G}$ é elemento fixo. Vamos verificar que tal correspondência é um automorfismo. Em primeiro lugar, todo o elemento de $\mathfrak{G}$ é imagem dum elemento de $\mathfrak{G}$. Para se obter $axa^{-1}=d$, basta pôr $d=a^{-1}da$. Em segundo lugar, supondo $x\neq y$, é $x'\neq y'$, visto que, se pudesse ter-se $axa^{-1}=aya^{-1}$, deduzíamos imediatamente $x=y$, contra a hipótese. Finalmente, tomemos xy. O seu correspondente é $a(xy)a^{-1}=axa^{-1}\cdot aya^{-1}$. Realizam-se as condições de automorfismo, de acordo com a definição dada em (II, 2, 1).

Estes automorfismos de $\mathfrak{G}$ dizem-se *internos*. É válido o seguinte

TEOREMA 3: *Os automorfismos internos dum grupo $\mathfrak{G}$ formam um grupo $J_{\mathfrak{G}}$, subgrupo de $A_{\mathfrak{G}}$.* Designemos por X o automorfismo interno definido pelo elemento $x\in\mathfrak{G}$. Tem-se $a\to xax^{-1}=aX$. Se Y é definido por y, tem-se igualmente $a\to yay^{-1}=aY$. O automorfismo Y^{-1} levará de yay^{-1} ao elemento a: $(yay^{-1})Y^{-1}=a$. Vê-se que é definido por y^{-1}, pois $y^{-1}\cdot yay^{-1}\cdot y=a$. Agora conclui-se $aY^{-1}X=(aY^{-1})X=(y^{-1}ay)X=x\cdot y^{-1}ay\cdot x^{-1}=xy^{-1}\cdot a(xy^{-1})^{-1}$, de sorte que o automorfismo $Y^{-1}X$ é interno, por ser definido pelo elemento xy^{-1}. O critério de subgrupo é satisfeito por $J_{\mathfrak{G}}$.

TEOREMA 4: *O subgrupo $J_{\mathfrak{G}}$, de $A_{\mathfrak{G}}$, é um invariante.* Conforme as considerações feitas no n.º 6, concluiremos o teorema, provando que, quaisquer que sejam $X\in J_{\mathfrak{G}}$ e $\Theta\in A_{\mathfrak{G}}$, é $\Theta X\Theta^{-1}\in J_{\mathfrak{G}}$. Ora $a\Theta X\Theta^{-1}=(x(a\Theta)x^{-1})\Theta^{-1}=x\Theta^{-1}\cdot a\Theta\Theta^{-1}\cdot x^{-1}\Theta^{-1}=(x\Theta^{-1})a(x\Theta^{-1})^{-1}$, pois que $x^{-1}\Theta^{-1}=(x\Theta^{-1})^{-1}$. Vê-se que $\Theta X\Theta^{-1}$ é o automorfismo interno definido pelo elemento $x\Theta^{-1}$. O teorema está demonstrado.

Se $a\in\mathfrak{G}$ fôr um elemento fixo, chamam-se *conjugados* de a todos os elementos da forma xax^{-1}, em que x percorre $\mathfrak{G}$. Se considerarmos como elementos equivalentes os elementos conjugados, define-se, de facto, uma relação de equivalência. Por meio desta relação, fica o grupo dividido em classes de equivalência ou classes de elementos conjugados. É válido este

TEOREMA 5: *Os elementos conjugados têm a mesma ordem.*

Se a ordem de a for n, tem se $a^n=u$, sendo $a^m\neq u$, se $m<n$. Consideremos o conjugado yay^{-1}. Tem-se $(yay^{-1})^n=yay^{-1}\cdot yay^{-1}\cdots yay^{-1}=ya^ny^{-1}=yuy^{-1}=u$. Se pudesse ter-se $(yay^{-1})^m=u$, viria $ya^my^{-1}=u$, ou $a^m=u$, o que não tem lugar.

A caracterização dum invariante pela condição $x\mathfrak{H}x^{-1}\subseteq\mathfrak{H}$ mostra que um subgrupo invariante pode definir-se, dizendo: *$\mathfrak{H}$ é um invariante, se, e apenas se, com cada elemento, contém todos os conjugados desse elemento.*

Um caso importante de invariante (abeliano) dum grupo é dado pelo *centro* do grupo, ou seja pelo conjunto dos elementos de $\mathfrak{G}$ que comutam com todos os elementos de $\mathfrak{G}$. O centro nunca é vazio, visto que contém, pelo menos, o elemento um. Uma caracterização dos elementos do centro é a seguinte: um elemento de $\mathfrak{G}$ pertence ao centro, se e só se a totalidade dos seus conjugados se reduz ao próprio elemento.

9) **Grupo factor. Teorema do homomorfismo** — Vimos, no final de (III, 1, 6), que era condição necessária e suficiente, para que o produto de duas classes esquerdas arbitrárias, $a\mathfrak{g}$ e $b\mathfrak{g}$, fosse uma classe esquerda (e, então, necessàriamente, a classe $ab\mathfrak{g}$), que $\mathfrak{g}$ fosse um invariante. Quando $\mathfrak{g}$ é um invariante, existe, pois, uma operação binária no conjunto

$$|\mathfrak{g}, a\mathfrak{g}, b\mathfrak{g}, \cdots| . \tag{1}$$

À face dessa operação, o conjunto anterior é um grupo. O seu elemento um é o complexo $\mathfrak{g}$, o inverso de $a\mathfrak{g}$ é o complexo $a^{-1}\mathfrak{g}$ e a propriedade associativa é válida, por ser válida em $\mathfrak{G}$. O grupo (1) diz-se *grupo factor* ou *grupo cociente* de $\mathfrak{G}$ segundo $\mathfrak{g}$. Substituindo $\mathfrak{g}$ por $\mathfrak{H}$, representaremos o grupo cociente por $\mathfrak{G}/\mathfrak{H}$.

Existe um homomorfismo $\mathfrak{G}\sim\mathfrak{G}/\mathfrak{H}$, fazendo corresponder a cada

elemento de $\mathfrak{G}$ a classe a que o elemento pertence. Claramente que, sendo $\mathfrak{H}$ um invariante o grupo (1) é, indiferentemente,

$$|\mathfrak{H}, a\mathfrak{H}, b\mathfrak{H}, \cdots| \text{ ou } |\mathfrak{H}, \mathfrak{H}a, \mathfrak{H}b, \cdots|.$$

Consideremos um subgrupo do grupo cociente. Vamos provar que, se se tratar dum grupo finito, o subgrupo em questão, uma vez individualizados os elementos do grupo $\mathfrak{G}$ que esse subgrupo contém, forma um subgrupo de $\mathfrak{G}$, que tem em $\mathfrak{G}$ o mesmo índice que o subgrupo do grupo cociente tem neste último. Sejam N o número de elementos de $\mathfrak{G}$ e n a ordem de $\mathfrak{H}$. Então, $N/n = r$ é o índice de $\mathfrak{H}$ em $\mathfrak{G}$ e também a ordem do grupo cociente $\mathfrak{G}/\mathfrak{H}$. Se, agora, s for a ordem do subgrupo do grupo cociente, o seu índice neste será $i = r/s$. Mas o número de elementos de $\mathfrak{G}$ que aquele subgrupo contém é sn, de modo que o índice do subgrupo de $\mathfrak{G}$ formado pelos elementos individualizados é $N/sn = nr/sn = r/s = i$, como se afirmou.

A demonstração de que os elementos individualizados constituem um subgrupo de $\mathfrak{G}$ pode fazer-se assim: sejam a e b dois elementos individualizados, pertencentes, respectivamente, às classes $a\mathfrak{H}$ e $b\mathfrak{H}$, as quais fazem parte do subgrupo do grupo cociente. Nesse caso, também $b^{-1}\mathfrak{H}$ pertence a esse subgrupo, o mesmo se dizendo de $a\mathfrak{H} \cdot b^{-1}\mathfrak{H} = ab^{-1}\mathfrak{H}$, o que mostra ser ab^{-1} um elemento individualizado. O critério de subgrupo é válido e a demonstração está feita.

Também sob a hipótese de $\mathfrak{G}$ ser finito, tem lugar o interessante resultado seguinte: *dado um grupo finito* $\mathfrak{G}$, *se* s *é o expoente mínimo do elemento* $a \in \mathfrak{G}$ *tal que* a^s *figura num divisor normal* $\mathfrak{H}$, *então* s *é divisor da ordem do grupo cociente* $\mathfrak{G}/\mathfrak{H}$. Bem entendido que se exclui no enunciado o caso $s = 0$. Consideremos, de facto, o seguinte conjunto de elementos de $\mathfrak{G}/\mathfrak{H}$: $\mathfrak{C} = |\mathfrak{H}, \mathfrak{H}a, \cdots, \mathfrak{H}a^{s-1}|$. Os diferentes elementos são distintos, pois que $\mathfrak{H}a^h = \mathfrak{H}a^k$, com $h \neq k$, levaria a $\mathfrak{H}a^{h-k} = \mathfrak{H}$, com $s > h - k > 0$ (suposto $h > k$), donde se concluiria ser $a^{h-k} \in \mathfrak{H}$, o que não pode ter lugar. O conjunto $\mathfrak{C}$ é um grupo de s elementos. Ora a ordem s, do subgrupo $\mathfrak{C}$, de $\mathfrak{G}/\mathfrak{H}$, divide a ordem deste último, como se afirmou.

No caso dos grupos abelianos, se $\mathfrak{M}$ é o grupo e $\mathfrak{N}$ um seu subgrupo (aqui todos os subgrupos são invariantes), o grupo cociente $\mathfrak{M}/\mathfrak{N}$ também se representa por $\mathfrak{M} - \mathfrak{N}$ e diz-se, então, *grupo diferença*. Um elemento do grupo diferença tem a forma $a + \mathfrak{N}$ e o critério para que duas classes $a + \mathfrak{N}$ e $a' + \mathfrak{N}$ sejam idênticas é: $a' - a \in \mathfrak{N}$.

A teoria dos invariantes será posta em ligação, no número próximo, com as considerações desenvolvidas em (III, 1, 1). Aqui vamos dar uma demonstração, para o caso dos grupos, do teorema do homomorfismo, conforme anunciámos em (III, 1, 1).

TEOREMA DO HOMOMORFISMO: *Se* $\mathfrak{G}$ *é um grupo e* $\mathfrak{G}/\mathfrak{H} = \overline{\mathfrak{G}}$ *é um grupo cociente, tem lugar o homomorfismo* $\mathfrak{G} \sim \overline{\mathfrak{G}} = \mathfrak{G}/\mathfrak{H}$; *reciprocamente, se* $\mathfrak{G} \sim \overline{\mathfrak{G}}$, *então* $\overline{\mathfrak{G}}$, *a menos de isomorfismo, é um grupo cociente.* A 1.ª parte do teorema foi demonstrada no número anterior. Seja agora $\overline{\mathfrak{G}}$ uma imagem homomorfa de $\mathfrak{G}$ e tomemos o elemento um $= \overline{u} \in \overline{\mathfrak{G}}$. Consideremos o conjunto de elementos

$$u, a, b, \cdots \in \mathfrak{G} \to \overline{u}, \tag{2}$$

isto é, aqueles elementos de $\mathfrak{G}$ que têm o elemento um de $\overline{\mathfrak{G}}$ como correspondente. Vamos ver que o conjunto (2) forma um subgrupo invariante. Se $a \to \overline{u}$, $b \to \overline{u}$, também $a^{-1} \to \overline{u}$ e $ba^{-1} \to \overline{u}$. Em (2), com a e b, encontramos ba^{-1}. Resta provar o caracter de invariante do subgrupo (2), que designaremos por $\mathfrak{H}$. Tomemos $x\mathfrak{H}, (x \in \mathfrak{G})$. Os elementos de $x\mathfrak{H}$ têm todos o mesmo correspondente $\overline{x} \in \overline{\mathfrak{G}}$. Inversamente, se um elemento $y \in \mathfrak{G}$ tem $\overline{x}$ como correspondente, como x^{-1} tem $\overline{x}^{-1}$ como correspondente, o elemento $x^{-1}y$, de correspondente $\overline{u}$, pertencerá a $\mathfrak{H}$. Da relação $x^{-1}y \in \mathfrak{H}$, deduz-se $y \in x\mathfrak{H}$. Deste modo, $x\mathfrak{H}$ representa a totalidade dos elementos de $\mathfrak{G}$ que têm $\overline{x}$ como correspondente. Demonstra-se anàlogamente que essa totalidade é $\mathfrak{H}x$, de sorte que $x\mathfrak{H} = \mathfrak{H}x$, qualquer que seja $x \in \mathfrak{G}$. $\mathfrak{H}$ é, efectivamente, um invariante.

Verifica-se, pois, que a cada classe de $\mathfrak{G}/\mathfrak{H}$ corresponde um elemento bem determinado de $\overline{\mathfrak{G}}$. Provaremos, em seguida, que a classes diferentes correspondem elementos diferentes e que ao produto de duas classes corresponde o produto dos elementos correspondentes, Então, a correspondência em causa será um isomorfismo. Ora, tomemos duas classes distintas $x\mathfrak{H}$ e $y\mathfrak{H}$. Não pode ter-se $\overline{x} = \overline{y}$, pois que, de contrário, seria $x^{-1}y \to \overline{u}$ e isto acarretaria $x^{-1}y \in \mathfrak{H}$, ou seja a igualdades das classes, contra a hipótese. A afirmação relativa ao produto é imediata. O teorema do homomorfismo está demonstrado.

10) **Sobre as relações de congruência nos grupos** — Como afirmámos no número anterior, vamos ligar a teoria dos subgrupos invariantes e a teoria do grupo cociente às considerações desenvolvi-

das no começo do Capítulo. Antes de mais, se tivermos em conta o operador e as operações a que fizemos referência em (III, 1, 2), os raciocínios de (III, 1, 1) mostram que, a menos de isomorfismos entre grupos, existe uma correspondência biunívoca completa entre os homomorfismos dum grupo e as relações de congruência possíveis no mesmo grupo. Por outro lado, no número anterior, estabeleceu-se uma correspondência biunívoca completa entre os homomorfismos dum grupo e os seus invariantes. Há, pois, uma correspondência biunívoca completa entre as congruências e os invariantes, como se verifica directamente do modo que vai mostrar-se.

As duas relações de equivalência ρ_d e ρ_e, definidas como se viu em (III, 1, 4), a partir dum subgrupo, são relações iguais, se o subgrupo é um invariante, como resulta de se ter, então, $a\,\mathfrak{H} = \mathfrak{H}\,a$, para qualquer $a \in \mathfrak{G}$. Além disso, do facto de ser $a\,\mathfrak{H} \cdot b\,\mathfrak{H} = (a\,b)\,\mathfrak{H}$, conclui-se mais ser $\rho_d = \rho_e = \rho$ uma relação de congruência, [cfr. o teorema 1 de (III, 1, 8)]. Inversamente, pode perguntar-se se não será verificada a hipótese de haver mais do que uma congruência levando ao mesmo divisor normal $\mathfrak{H}$. Ora, desde que uma relação de congruência define um homomorfismo, os raciocínios do número anterior mostram claramente que só pode haver uma decomposição correspondente em classes de congruência.

É imediato que a intersecção de duas congruências é uma congruência. Nessas condições, a intersecção de dois invariantes é um invariante, precisamente, o invariante em correspondência com a congruência intersecção.

Nos grupos, tem lugar a condição referida no teorema demonstrado em (III, 1, 3): as relações de congruência são comutáveis. A congruência produto corresponde ao produto dos invariantes correspondentes, como se reconhece fàcilmente. Vimos já, em (III, 1, 7) que, na verdade, o produto de dois invariantes é um invariante.

As relações de congruência nos grupos verificam a condição seguinte: de $(a\,b)\,\rho\,(a\,c)$, conclui se $b\,\rho\,c$. Na verdade, supondo $\mathfrak{H}$ o invariante correspondente e tendo em conta que $\mathfrak{G}/\mathfrak{H}$ é um grupo, de

$$(a\,b)\,\mathfrak{H} = (a\,\mathfrak{H})(b\,\mathfrak{H}) = (a\,c)\,\mathfrak{H} = (a\,\mathfrak{H})(c\,\mathfrak{H}),$$

deduz-se $b\,\mathfrak{H} = c\,\mathfrak{H}$, ou seja $b\,\rho\,c$. Diz-se, por isso, que toda a congruência num grupo é *normal*.

11) **Normalizadores. Grupo comutador** — Dado o grupo $\mathfrak{G}$, tomemos $a \in \mathfrak{G}$. O conjunto dos elementos de $\mathfrak{G}$ que comutam com a diz-se *normalizador* de a. É imediato que esse conjunto é um subgrupo $\mathfrak{g}$. Como as potências de a comutam com a, segue-se que $\mathfrak{g}$ contém o grupo cíclico $\mathfrak{h}$, gerado por a. Para cada $x \in \mathfrak{g}$ é $x\,\mathfrak{h} = \mathfrak{h}\,x$, pelo que:

TEOREMA 1: *O grupo cíclico gerado por* a *é subgrupo invariante do normalizador de* a.

Sejam agora os complexos associados de $\mathfrak{g}$, em $\mathfrak{G}$. Tem-se

$$\mathfrak{G} = \mathfrak{g} \cup b_1\mathfrak{g} \cup b_2\mathfrak{g} \cup \cdots,$$

significando com isto que $\mathfrak{G}$ é o conjunto unido das classes esquerdas de representantes u, b_1, b_2 etc., classes que são disjuntas. Determinemos agora os elementos conjugados de a, servindo-nos da expressão $y\,a\,y^{-1}$, mas fazendo coincidir y sucessivamente com os elementos de cada complexo $b_i\mathfrak{g}$. Tem-se

$$b_i g \cdot a \cdot g^{-1} b_i^{-1} = b_i\,a\,b_i^{-1}, \quad (g \in \mathfrak{g}),$$

resultado que mostra levarem os elementos do referido complexo a um mesmo conjugado. Vamos ver mais que complexos diferentes levam a conjugados diferentes. Se pudesse ser $b_j\,a\,b_j^{-1} = b_i\,a\,b_i^{-1}$, ter-se-ia $a = b_i^{-1} b_j \cdot a \cdot b_j^{-1} b_i = b_i^{-1} b_j \cdot a \cdot (b_i^{-1} b_j)^{-1}$, ou seja $a \cdot b_i^{-1} b_j = b_i^{-1} b_j \cdot a$. Este resultado mostra que $b_i^{-1} b_j$ pertenceria ao normalizador, pelo que não seriam diferentes as classes $b_i\mathfrak{g}$ e $b_j\mathfrak{g}$, contra o que se supôs. Claramente que a utilização de todos os complexos leva à utilização de todos os elementos do grupo, e, portanto, a todos os conjugados de a. É válido o

TEOREMA 2: *Há uma correspondência biunívoca completa entre os conjugados dum elemento* $a \in \mathfrak{G}$ *e os complexos associados do normalizador de* a.

Se $\mathfrak{G}$ for finito, o número de conjugados de a é igual ao índice do seu normalizador. Como esse índice é um divisor da ordem do grupo, tem-se:

TEOREMA 3: *Num grupo finito, o número de conjugados dum elemento é um divisor da ordem do grupo.*

Passemos à noção de *normalizador dum subgrupo* $\mathfrak{g}$. Consideram-se em $\mathfrak{G}$ todos os elementos a tais que $a\mathfrak{g} = \mathfrak{g}a$. Se $\mathfrak{h}$ for o conjunto desses elementos, $\mathfrak{h}$ é um subgrupo chamado normalizador de $\mathfrak{g}$. Ve se que $\mathfrak{h}$ contém o próprio subgrupo $\mathfrak{g}$, o qual é invariante de $\mathfrak{h}$. Escrevendo $\mathfrak{G}$ sob a forma

$$\mathfrak{G} = \mathfrak{h} \cup b_1\mathfrak{h} \cup b_2\mathfrak{h} \cup \cdots,$$

vamos mostrar que os elementos dum mesmo complexo $b_i\mathfrak{h}$ levam todos ao mesmo *subgrupo conjugado de* $\mathfrak{g}$. Com esta última locução, significa-se um subgrupo da forma $a\mathfrak{g}a^{-1}$, $(a \in \mathfrak{G})$. De facto, tem-se $b_i h \cdot \mathfrak{g} \cdot h^{-1}b_i^{-1} = b_i(h\mathfrak{g}h^{-1})b_i^{-1} = b_i\mathfrak{g}b_i^{-1}$, $(h \in \mathfrak{h})$. Como no caso do normalizador dum elemento, também aqui complexos diferentes levam a subgrupos conjugados diferentes, e, àlem disso, os complexos levam a todos os subgrupos conjugados de $\mathfrak{g}$. Podemos dizer:

TEOREMA 4: *Há uma correspondência biunívoca completa entre os subgrupos conjugados dum subgrupo* $\mathfrak{g}$ *e os complexos associados do normalizador de* $\mathfrak{g}$.

Passemos à noção de *grupo comutador*. Da definição de comutador de dois elementos, dada em (III, 1, 7), resulta imediatamente que é condição necessária e suficiente, para que o comutador dos elementos a e b seja u, que os dois elementos sejam comutáveis. Diz-se grupo comutador $\mathfrak{C}$, dum grupo $\mathfrak{G}$, o subgrupo de $\mathfrak{G}$ gerado pelos comutadores.

TEOREMA 5: *O grupo comutador é um invariante do grupo dado.* Seja $x \in \mathfrak{G}$. Podemos escrever sucessivamente:

$$x \cdot ab(ba)^{-1} \cdot x^{-1} = xaba^{-1}b^{-1}x^{-1} = xab \cdot (a \cdot xb)^{-1}(a \cdot xb) \cdot (xb \cdot a)^{-1} =$$
$$= xabb^{-1}x^{-1}a^{-1} \cdot (a \cdot xb) \cdot (xb \cdot a)^{-1} = [xa \cdot (ax)^{-1}] \cdot [(a \cdot xb) \cdot (xb \cdot a)^{-1}].$$

Como esta última expressão é o produto de dois comutadores, ela representa um elemento do grupo comutador. Tendo em conta o aspecto do 1.º membro das igualdades anteriores, concluimos que o conjugado dum comutador pertence ao grupo comutador. Seja agora o produto de dois comutadores. Vê-se que $x[(ab)(ba)^{-1} \cdot (cd)(dc)^{-1}]x^{-1} = x[(ab)(ba)^{-1}]x^{-1} \cdot x[(cd)(dc)^{-1}]x^{-1}$, pelo que os conjugados do produto também pertencem ao grupo comutador. Como o inverso dum comutador é um comutador, podemos afirmar que o grupo comutador gosa da propriedade de conter os conjugados dos seus elementos. É um invariante.

TEOREMA 6: *O grupo cociente* $\mathfrak{G}/\mathfrak{C}$ *é abeliano.* Na verdade tem-se $x\mathfrak{C} \cdot y\mathfrak{C} = (xy)\mathfrak{C}$, $y\mathfrak{C} \cdot x\mathfrak{C} = (yx)\mathfrak{C}$. Representando por c o comutador de x e y, é $(xy)(yx)^{-1} = c \in \mathfrak{C}$, ou seja $xy \in \mathfrak{C}(yx)$, o que mostra serem idênticas as classes $\mathfrak{C}(xy)$ e $\mathfrak{C}(yx)$, portanto as classes $(xy)\mathfrak{C}$ e $(yx)\mathfrak{C}$. O produto $x\mathfrak{C} \cdot y\mathfrak{C}$ é comutativo, como afirma o teorema.

O grupo comutador tem uma definição curiosa, que assenta neste

TEOREMA 7: *O grupo comutador está contido em todo o invariante cujo grupo cociente seja abeliano.* Seja $\mathfrak{D}$ um invariante nas condições do enunciado. Dados $a, b \in \mathfrak{G}$, tem-se $a\mathfrak{D} \cdot b\mathfrak{D} = b\mathfrak{D} \cdot a\mathfrak{D}$. Trata-se de provar que $\mathfrak{D}$ contém o comutador $(ab)(ba)^{-1}$. De facto, sendo $(ab)\mathfrak{D} = \mathfrak{D}(ba)$, existe $c \in \mathfrak{D}$ tal que $ab = c \cdot ba$, o que leva a $c = ab(ba)^{-1} \in \mathfrak{D}$, como se deseja. É válida, pois, esta definição: *o grupo comutador é intersecção de todos os invariantes de* $\mathfrak{G}$ *aos quais correspondem grupos cocientes abelianos.*

Partindo do grupo $\mathfrak{G}$, o grupo comutador $\mathfrak{C} = \mathfrak{G}' = |u, c_1, c_2 \cdots|$ diz-se grupo primeiro derivado ou *derivada primeira* do grupo $\mathfrak{G}$. O grupo comutador $\mathfrak{G}''$, de $\mathfrak{G}'$, diz-se *derivada segunda* de $\mathfrak{G}$, etc. Tem lugar o

TEOREMA 8: *A derivada segunda de* $\mathfrak{G}$ *é um invariante de* $\mathfrak{G}$. Para fazermos a demonstração, comecemos por uma nota muito simples. Se c é o comutador de a e b, o comutador de xax^{-1} e xbx^{-1} é xcx^{-1}. Nessas condições, se pomos $\mathfrak{G}'' = |u, C_1, C_2, \cdots|$, imaginemos ser $C_i = c_1c_2(c_2c_1)^{-1}$, $(c_i \in \mathfrak{G}')$. Será também xC_ix^{-1} o comutador de xc_1x^{-1} e xc_2x^{-1}. Ora, como estes dois últimos elementos pertencem a $\mathfrak{G}'$, o seu comutador pertencerá a $\mathfrak{G}''$. Se C_i for um produto de dois comutadores, encontra-se anàlogamente $xC_ix^{-1} \in \mathfrak{G}''$, por ser o produto de dois elementos de $\mathfrak{G}''$. O teorema é agora imediato.

§ 2. O grupo simétrico

1) **Representação cíclica das permutações de n elementos** — Definimos o grupo simétrico $\mathfrak{S}_n$ em (II, 2, 3). Consideremos os q elementos $i_1, i_2, \cdots, i_q$, dos n elementos $1, 2, \cdots, n$. Um ciclo $(i_1 i_2 \cdots i_q)$

é a permutação

$$\begin{pmatrix} \cdots i_1 \cdots i_2 \cdots i_q \cdots \\ \cdots i_2 \cdots i_3 \cdots i_1 \cdots \end{pmatrix},$$

que muda i_1 em i_2, i_2 em i_3, etc., até i_q, que muda em i_1. É válido o

TEOREMA 1: *Toda a permutação é um produto de ciclos.* Seja, com efeito,

$$i \to \varphi(i) = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}.$$

Escrevamos o ciclo $(i_1 j_1 k_1 \cdots l_1)$, que transforma i_1 em j_1, j_1 em k_1, etc., tal como em $\varphi(i)$. Chega-se, certamente, a um elemento l_1 que tem i_1, primeiro elemento do ciclo, como correspondente. Em seguida, tomemos um elemento i_r, que não coincida com qualquer dos elementos do ciclo já considerado, e escrevamos o segundo ciclo $(i_r j_r \cdots p_r)$, no qual se supõe ser i_r o correspondente de p_r. Prosseguindo da mesma maneira, chega-se necessàriamente à decomposição em ciclos, visto que um ciclo tem, pelo menos, um elemento, e o número de elementos em causa é igual a n.

Convém fazer as seguintes observações: 1) um ciclo com um elemento, por exemplo (j), significa a permutação identidade; 2) um ciclo $(i_1 i_2 i_3 \cdots i_q)$ pode escrever-se ainda $(i_2 i_3 \cdots i_q i_1)$, ou $(i_3 i_4 \cdots i_q i_1 i_2)$, etc.; 3) na decomposição de uma permutação como produto de ciclos, é indiferente a ordem pela qual os mesmos se escrevem, como resulta do facto de não haver dois ciclos com elemento comum; 4) deixando de escrever os ciclos com um elemento, ou, pelo menos, sujeitando-nos ao processo indicado para a decomposição, que não permite repetição de qualquer dos números $1, 2, \cdots, n$ nos ciclos sucessivos, *a factorização é única.*

Usando a notação cíclica, os elementos dos grupos simétricos $\mathfrak{S}_1, \mathfrak{S}_2, \mathfrak{S}_3$ podem escrever-se:

$$\mathfrak{S}_1: (1); \quad \mathfrak{S}_2: (1), (1\,2);$$
$$\mathfrak{S}_3: (1), (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2).$$

2) **Permutações pares e ímpares** — Um ciclo da forma (ij) diz-se uma *transposição.* Pode dar-se este enunciado:

TEOREMA 1: *Toda a permutação é um produto de transposições. O número de factores do produto tem uma paridade determinada.* A primeira parte do teorema fica provada, mostrando que ela é válida para um ciclo qualquer. Ora $(i_1 i_2 \cdots i_q) = (i_1 i_q)(i_1 i_{q-1}) \cdots (i_1 i_2)$, como se verifica imediatamente. Quanto à segunda parte, utilizaremos as duas igualdades seguintes:

$$(a\,b)(a\,i_1\,i_2 \cdots i_h\ b\,j_1 \cdots j_k) = (b\,j_1 \cdots j_k)(a\,i_1 \cdots i_h),$$
$$(a\,b)(b\,j_1 \cdots j_k)(a\,i_1 \cdots i_h) = (a\,i_1 \cdots i_h\ b\,j_1 \cdots j_k).$$

Na verdade, suponhamos $\varphi = (i_1 \cdots i_q)(j_1 \cdots j_r) \cdots (k_1 \cdots k_s)$ uma decomposição de φ em ciclos disjuntos e associemos a φ o número $N(\varphi) = (q-1) + (r-1) + \cdots + (s-1)$. Então, o número $N[(a\,b)\varphi]$, no caso de a e b pertencerem ao mesmo ciclo de φ, verifica a relação $N[(a\,b)\varphi] = N(\varphi) - 1$, como se conclui da primeira igualdade citada; pelo contrário, se a e b pertencem a ciclos diferentes, a segunda igualdade mostra que se tem $N[(a\,b)\varphi] = N(\varphi) + 1$. Admitindo ser $\varphi = (a\,b)(c\,d) \cdots (p\,q)$ um produto de m transposições, vê-se que tem lugar a relação

$$(p\,q) \cdots (c\,d)(a\,b)\varphi = u = \text{permutação identidade},$$

pois as transposições são iguais às suas inversas. Como, porém, $N(u) = 0$, existe uma relação $\pm 1 \pm 1 \pm \cdots \pm 1 + N(\varphi) = 0$, onde o algarismo 1 está escrito m vezes. A paridade de m é, assim, a do número bem determinado $N(\varphi)$. O teorema está completamente demonstrado. Dele resulta este

COROLÁRIO 1: *O grupo $\mathfrak{S}_n$ é gerado pelas transposições $(1\,2), (1\,3), \cdots (1\,n)$.* Basta ter em conta a igualdade $(ij) = (1\,j)(1\,i)(1\,j), (i \neq 1)$, para o reconhecer.

As considerações feitas justificam a seguinte definição: uma permutação é *par*, se pode escrever-se como produto dum número par de transposições, e é *ímpar*, no caso contrário.

COROLÁRIO 2: *As permutações pares, contidas em $\mathfrak{S}_n$, formam um subgrupo $\mathfrak{A}_n$, chamado grupo alterno.* De facto, o produto de duas permutações pares é uma permutação par, e, para os grupos finitos, tem lugar o seguinte critério de subgrupo: *num grupo finito, um conjunto é subgrupo, se for fechado relativamente ao produto,* [Cfr. (III, 1, 2)].

3) **Os ciclos de 3 elementos** — No estudo do grupo alterno $\mathfrak{A}_n$ têm especial interesse os ciclos (ijk), nos quais figuram 3 elementos. Assim:

TEOREMA 1: *O grupo alterno é gerado pelos ciclos* (i j k). Com efeito, dada uma permutação par, escrevamo-la como produto dum número par de transposições. Se duas transposições consecutivas não têm elemento comum, o seu produto é da forma $(k\,l)(i\,j) = (i\,k\,l)(i\,j\,l)$, isto é, reduz-se ao produto de dois ciclos de 3 elementos; se, pelo contrário, as duas transposições contêm um mesmo elemento, então o seu produto é da forma $(i\,k)(i\,j) = (i\,j\,k)$, reduzindo-se a um único ciclo de 3 elementos. Em todos os casos, a permutação par é um produto de ciclos $(i\,j\,k)$, pelo que o teorema fica provado. Podemos precisar e dizer:

TEOREMA 2: *O grupo alterno é gerado pelos ciclos* $(1\,2\,3), (1\,2\,4), \cdots, (1\,2\,n)$. O grupo $\mathfrak{A}_3$, por exemplo, é um grupo cíclico de 3 elementos, tendo $(1\,2\,3)$ como elemento gerador. Supondo, porém, $n \geqq 4$, consideremos um ciclo da forma $(i\,j\,k)$, no qual não figuram os números 1 ou 2. Tem lugar as relações

$$(i\,j\,k) = (1\,i\,j)(1\,j\,k)$$
$$(1\,i\,j) = (1\,2\,j)^2(1\,2\,i)(1\,2\,j),$$

que mostram pertencer $(i\,j\,k)$ ao grupo gerado pelos ciclos referidos no enunciado. Quando se tiver $(i\,j\,k)=(i\,j\,2)$, escrevendo ainda $(i\,j\,2)= =(1\,i\,j)(1\,j\,2)$, e tendo em conta ser $(1\,j\,2) = (1\,2\,j)^2$, a conclusão é a mesma. Assim, quaisquer que sejam as hipóteses formuladas sobre $(i\,j\,k)$, a afirmação do teorema é válida para tais ciclos, e, consequentemente, para $\mathfrak{A}_n$.

4) **As classes de conjugados em** $\mathfrak{S}_n$ — Se considerármos a permutação

$$i \to \varphi(i) = \begin{pmatrix} 1 & 2 & \cdots & n \\ \varphi(1) & \varphi(2) & & \varphi(n) \end{pmatrix},$$

e tomarmos, em seguida, a permutação $i \to \psi(i)$, verifica-se imediatamente a igualdade

$$\psi\varphi\psi^{-1} = \begin{pmatrix} \psi(1) & \psi(2) & \cdots & \psi(n) \\ \psi\varphi(1) & \psi\varphi(2) & \cdot\ \cdot & \psi\varphi(n) \end{pmatrix}.$$

Deste modo, partindo de $i \to \varphi(i)$, vê-se que $\psi\varphi\psi^{-1}$ determina a correspondência $\psi(i) \to \psi\varphi(i)$. Assim, se supusermos

$$\varphi = (i_1\, i_2 \cdots i_q)(j_1 j_2 \cdots j_r)(k_1 k_2 \cdots k_s),$$

vê-se que, de $i_1 \to \varphi(i_1) = i_2$, se deduz $\psi(i_1) \to \psi\varphi(i_1) = \psi(i_2)$; portanto, tem-se:

$$\psi\varphi\psi^{-1} = (\psi(i_1), \psi(i_2), \cdots, \psi(i_q)) \cdots (\psi(k_1), \psi(k_2), \cdots, \psi(k_s)),$$

como decomposição em ciclos da permutação do 1.º membro. Vamos supor, o que é sempre possível, que as decomposições em ciclos disjuntos, como a de φ, satisfazem às relações

$$q \geqq r \geqq \cdots \geqq s, \quad q + r + \cdots + s = n.$$

Tais decomposições, a menos da ordem de ciclos com o mesmo número de elementos, ficam univocamente determinadas. E diz-se que se tem uma *partição* do número n, representando-se por $p(n)$ o número de parcelas de n. Os raciocínios feitos provam que a cada classe de conjugados de $\mathfrak{S}_n$ corresponde uma partição de n. Por outro lado, se duas permutações levam à mesma partição, elas são necessàriamente conjugadas, pois que, de

$$\varphi = (i_1\, i_2 \cdots i_q)(j_1 j_2 \cdots j_r) \cdots (k_1 k_2 \cdots k_s),$$
$$\theta = (i'_1\, i'_2 \cdots i'_q)(j'_1 j'_2 \cdots j'_r) \cdots (k'_1 k'_2 \cdots k'_s),$$

concluimos $\theta = \psi\varphi\psi^{-1}$, pondo

$$\psi = \begin{pmatrix} i_1 \cdots i_q\ j_1 \cdots j_r \cdots k_1 \cdots k_s \\ i'_1 \cdots i'_q\ j'_1 \cdots j'_r \cdots k'_1 \cdots k'_s \end{pmatrix}.$$

Reciprocamente, dada uma partição de n, é claro que podemos construir uma permutação que seja um produto de ciclos determinando a referida partição. Em suma:

TEOREMA 1: *O número de partições de* n *é igual ao número de classes conjugadas do grupo simétrico* $\mathfrak{S}_n$.

Pode verificar-se que se tem $p(2) = 2$, $p(3) = 3$, $p(4) = 5$, $p(5) = 7$, etc.

Suponhamos $n > 2$. Se uma permutação $\varphi \in \mathfrak{S}_n$ for diferente da permutação idêntica, a decomposição em ciclos leva necessàriamente a $q > 1$. Por exemplo, supondo $n = 3$, podemos considerar $\varphi = (12)(3)$. Uma conjugada de φ é da forma $\psi\varphi\psi^{-1} = (\psi(1),\ \psi(2))(\psi(3))$, de sorte que, se admitirmos que $\psi(3) \neq 3$, é já $\psi\varphi\psi^{-1} \neq \varphi$, ou seja

$\psi\varphi \neq \varphi\psi$. Nenhuma permutação φ comuta com todas as permutações, valendo este

TEOREMA 2: *O centro de* $\mathfrak{S}_n$, *sob a hipótese* $n > 2$, *reduz-se ao grupo unidade. Para* $n \gtrless 2$, *o centro é o próprio grupo* $\mathfrak{S}_n$.[1]

5) **A simplicidade do grupo alterno** – A proposição fundamental a demonstrar neste número é a seguinte:

TEOREMA 1: *O grupo alterno* $\mathfrak{A}_n$, *se for* $n > 4$, *é um grupo simples*. Utilizaremos na demonstração este

LEMA 1: *Supondo* $n > 2$, *todo o invariante* $\mathfrak{N}$, *de* $\mathfrak{A}_n$, *que contenha um ciclo de 3 elementos, é idêntico a* $\mathfrak{A}_n$. Se for $n = 3$ e $\mathfrak{N}$ contiver $(1\,2\,3)$, sabemos já que a afirmação é válida, [cfr. (III, 2, 3)]. O mesmo se diz, supondo $(1\,3\,2) \in \mathfrak{N}$, pois que $(1\,3\,2)^2 = (1\,2\,3)$. Para o caso $n > 3$, comecemos por admitir $(1\,2\,k) \in \mathfrak{N}$. Então, $(1\,k\,2) = (1\,2\,k)^2 \in \mathfrak{N}$. E, pondo $\rho = (1\,2)(k\,t)$, $(k, t \neq 1, 2)$, vê-se que $\rho \cdot (1\,k\,2) \cdot \rho^{-1} = (1\,2\,t) \in \mathfrak{N}$, qualquer que seja t. Tem se $\mathfrak{N} = \mathfrak{A}_n$. Em seguida, posta a hipótese $(1\,i\,k) \in \mathfrak{N}$, com $(i, k \neq 2)$, basta escrever $\tau = (1\,k)(i\,2)$, para se reconhecer que $\tau \cdot (1\,i\,k) \cdot \tau^{-1} = (1\,k\,2) \in \mathfrak{N}$. Finalmente, supondo $(i\,j\,k) \in \mathfrak{N}$, com $i, j, k \neq 1$, e definindo σ pela relação $\sigma = (i\,k)(j\,1)$, encontra-se $\sigma(i\,j\,k)\sigma^{-1} = (1\,i\,k)$. O lema fica demonstrado.

Passemos ao teorema. Tomemos $\mathfrak{A}_n$, com $n > 4$. Trata-se de provar que, dado o invariante $\mathfrak{N} \neq (1)$, é $\mathfrak{N} = \mathfrak{A}_n$. Em primeiro lugar, consideremos uma permutação $\sigma \neq (1)$, pertencente a $\mathfrak{N}$, a qual deixe fixos o maior número possível de elementos. Essa permutação não pode ser decomposta em ciclos com elementos em número diferente, pois, se fosse $\sigma = (t_1 \cdots t_p)(m_1 \cdots m_q) \cdots$, com $p > q$, a permutação σ^q conservaria todos os elementos que σ deixa invariantes, e, além destes, ainda os elementos $m_1, \cdots, m_q$. Todavia seria $\sigma^q \neq (1)$, visto que o elemento t_1 não seria conservado. Em segundo lugar, a permutação σ não pode deslocar mais de 4 elementos. De contrário, com efeito, teria σ uma das formas

$$\sigma = (i\,k)(t\,m) \cdots (p\,n), \qquad \sigma = (i\,k\,p) \cdots (t\,m\,n),$$
$$\sigma = (i\,k\,t\,m) \cdots (p\,r\,s\,n), \qquad \sigma = (i\,k\,t\,m \cdots n) \cdots .$$

Em qualquer dos casos, haveria dois elementos, t e m, pertencentes ao mesmo ciclo e diferentes dos elementos i, k, n. A permutação

$\sigma' = (i\,k\,n) \cdot \sigma \cdot (i\,k\,n)^{-1}$, como fàcilmente se verifica, mudaria k em n e t em m. Ela seria, todavia, diferente de σ, pois σ não muda k em n. E, visto que σ e σ' pertenceriam ambas a $\mathfrak{N}$, ter-se-ia também $\sigma^{-1}\sigma' \in \mathfrak{N}$. Esta última permutação, sendo $\sigma \neq \sigma'$, é diferente da identidade. Pode ver-se, porém, que ela conserva o elemento t, o que σ não faz. Ora σ conserva certos elementos, mas não conserva i, k, ou n. Então, σ' conserva todos os elementos que σ deixa fixos. Deste modo $\sigma^{-1}\sigma'$ conservaria mais elementos que σ, o que não pode ter lugar.

As duas conclusões assinaladas, quanto a σ, provam que só pode ter-se $\sigma = (i\,j)(k\,t)$ ou $\sigma = (i\,j\,k)$. A última igualdade, em face do lema 1, dará $\mathfrak{N} = \mathfrak{A}_n$. Se for válida a primeira igualdade, como se tem $n > 4$, ponhamos $\sigma' = (k\,t\,m) \cdot \sigma \cdot (k\,t\,m)^{-1} = (i\,j)(t\,m)$, com $m \neq i, j, k, t$. Vê-se que $\sigma' \in \mathfrak{N}$, tendo-se também $\sigma\sigma' = (k\,t\,m) \in \mathfrak{N}$. Ainda pelo lema, será $\mathfrak{N} = \mathfrak{A}_n$. A demonstração está feita.

Observe-se que, quando $n = 4$, a demonstração anterior falha em vários pontos.

NOTA IMPORTANTE: Por ser $\mathfrak{A}_n$ um subgrupo de índice 2 em $\mathfrak{S}_n$ segue-se que, supondo $n > 4$, a cadeia de invariantes $\mathfrak{S}_n \supset \mathfrak{A}_n \supset (1)$ é tal que não é possível, inserir entre dois deles consecutivos qualquer subgrupo que seja invariante no anterior. No caso $n = 4$, há, em $\mathfrak{S}_4$, além dos invariantes (1) e $\mathfrak{S}_4$, o invariante $\mathfrak{A}_4$ e este outro, que é composto de 4 elementos e se designa por *grupo de 4 elementos de* KLEIN: $\mathfrak{W} = \{(1); (1\,2)(3\,4); (1\,3)(2\,4); (1\,4)(2\,3)\}$. Neste subgrupo, a permutação idêntica e cada um dos outros elementos formam, por sua vez, um subgrupo cíclico de 2.ª ordem, que é divisor normal do grupo de KLEIN. A cadeia de invariantes $\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset \mathfrak{W} \supset \{(1); (1\,2)\cdot(3\,4)\} \supset (1)$ também não permite a inserção de qualquer subgrupo que venha a ser invariante no elemento da cadeia que o precede.

§ 3. Grupos transitivos e intransitivos. Grupos primitivos e imprimitivos.

1) **Grupos transitivos e intransitivos** – Sejam $\mathfrak{C} = \{a, b, c, \cdots, x, y, \cdots\}$ um conjunto qualquer e $\mathfrak{G} = \{U, A, \cdots, L, R, S, T, \cdots X, Y, Z, \cdots\}$ um grupo de transformações de $\mathfrak{C}$. $\mathfrak{G}$ diz-se *transitivo sobre* $\mathfrak{C}$, se, dados $x, y \in \mathfrak{C}$ arbitrários, existir $R \in \mathfrak{G}$ tal que $xR = y$.

TEOREMA 1: *É condição necessária e suficiente, para que* $\mathfrak{G}$ *seja transitivo sobre* $\mathfrak{C}$, *que exista um certo* $a \in \mathfrak{C}$ *tal que, para cada* $z \in \mathfrak{C}$, *possa determinar-se* $S \in \mathfrak{G}$, *por forma a ter-se* $aS = z$. Da definição resulta imediatamente que a condição é necessária. O elemento a é qualquer. Para se ver que é suficiente, tomemos $x, y \in \mathfrak{C}$ arbitràriamente. Por ser, fixado a, $aX = x$, $aY = y$, para certos X e Y, vê-se que $a = xX^{-1}$, $aY = xX^{-1}Y = y$. O elemento $S = X^{-1}Y \in \mathfrak{G}$ é tal que $xS = y$. O teorema está provado.

Se $\mathfrak{G}$ não é transitivo, diz-se *intransitivo* sobre $\mathfrak{C}$. Suponhamos, então, $a, b \in \mathfrak{C}$ tais que existe $L \in \mathfrak{G}$ verificando a igualdade $b = aL$. Define-se uma relação de equivalência, considerando, nesse caso, a e b como equivalentes. Por meio dessa relação de equivalência, divide-se $\mathfrak{C}$ em classes de equivalentes chamadas *domínios de transitividade*, pelo facto de $\mathfrak{G}$ ser transitivo sobre cada classe. Quando $\mathfrak{G}$ é transitivo, há um só domínio de transitividade, que é o conjunto $\mathfrak{C}$.

Admitamos que $\mathfrak{G}$ é transitivo e fixemos um elemento a: Além da identidade U, de $\mathfrak{G}$, pode haver outras transformações pertencentes a $\mathfrak{G}$ que deixem a invariante. A sua totalidade forma um subgrupo $\mathfrak{G}_a$, de $\mathfrak{G}$. Tem lugar este

TEOREMA 2: *Há uma correspondência biunívoca completa entre as classes associadas de* $\mathfrak{G}_a$ *e os elementos de* $\mathfrak{C}$. De facto, todos os elementos de uma classe $\mathfrak{G}_a S$ transformam a no mesmo elemento aS; e, assim, a cada classe corresponde um elemento de $\mathfrak{C}$. Se for $\mathfrak{G}_a S \neq \mathfrak{G}_a R$, é $aS \neq aR$, pois que a igualdade destes últimos daria $aS = aR$, $a = aRS^{-1}$, ou seja $RS^{-1} \in \mathfrak{G}_a$; e, daqui, ser-se-ia levado à igualdade das classes. Finalmente, todos os elementos de $\mathfrak{C}$ são obtidos como transformados de a pelas classes.

Relativamente à comparação de dois subgrupos $\mathfrak{G}_a$ e $\mathfrak{G}_b$, podemos afirmar:

TEOREMA 3: *Há correspondência biunívoca completa entre os elementos de* $\mathfrak{G}_a$ *e os elementos de* $\mathfrak{G}_b$. Suponhamos $b = aT$. Então, $T^{-1}\mathfrak{G}_a T$ é um subgrupo conjugado de $\mathfrak{G}_a$, que conserva b. Inversamente, se $bS = b$, então $aTS = aT$, ou $a = aTST^{-1}$. Será $TST^{-1} \in \mathfrak{G}_a$ e $S \in T^{-1}\mathfrak{G}_a T$. O teorema fica provado, precisamente pelo facto de ser $\mathfrak{G}_b = T^{-1}\mathfrak{G}_a T$.

COROLÁRIO 1: *Se* $\mathfrak{G}$ *é um grupo finito transitivo sobre* $\mathfrak{C}$, *todos os grupos* $\mathfrak{G}_a$ *contêm o mesmo número de elementos.* $\mathfrak{C}$ *é, então, um conjunto finito, e o número de classes associadas de* $\mathfrak{G}_a$ *é igual ao número de elementos de* $\mathfrak{C}$. *O número de elementos de* $\mathfrak{C}$ *é um divisor da ordem de* $\mathfrak{G}$.

Quando se toma para $\mathfrak{G}$ o grupo $\mathfrak{T}$ de transformações de $\mathfrak{C}$, claramente que $\mathfrak{G} = \mathfrak{T}$ é transitivo sobre $\mathfrak{C}$. Na hipótese $\mathfrak{G} \subset \mathfrak{T}$, em geral há vários domínios de transitividade, da forma $a\mathfrak{G}, b\mathfrak{G}, \cdots$, dividindo-se $\mathfrak{C}$, como se disse, em classes de equivalência da forma

$$(1) \qquad |a\mathfrak{G}, b\mathfrak{G}, \cdots, c\mathfrak{G}, \cdots, f\mathfrak{G}, \cdots| .$$

Reciprocamente, consideremos uma relação de equivalência em $\mathfrak{C}$ e a respectiva divisão em classes de equivalência: $|C_a, C_b, \cdots|$. Pode sempre determinar-se um subgrupo $\mathfrak{G}$, de $\mathfrak{T}$, tal que $C_a = a\mathfrak{G}$, $C_b = b\mathfrak{G}$, etc. Basta, por exemplo, tomar para $\mathfrak{G}$ o subgrupo de $\mathfrak{T}$ gerado pelas transposições que trocam ou dois elementos de C_a, ou dois elementos de C_b, etc. Se tivermos em conta a existência de subgrupos de $\mathfrak{T}$ que não são gerados por transposições, concluimos, todavia, poder haver subgrupos diferentes, $\mathfrak{G}_1$ e $\mathfrak{G}_2$, tais que $a\mathfrak{G}_1 = a\mathfrak{G}_2$, para todo o $a \in \mathfrak{C}$. Não obstante, o uso dos subgrugos de $\mathfrak{T}$, no sentido que acabamos de assinalar, traz vantagens em certas questões de que nos ocuparemos noutro lugar.

Tomemos de novo a relação de equivalência ρ, que acabamos de referir, assim como o espaço cociente $\mathfrak{C}' = |a\mathfrak{G}, b\mathfrak{G}, \cdots|$, definido em (1). Se $\mathfrak{H}$ for o subgrupo de $\mathfrak{T}$ gerado por todos os subgrupos de $\mathfrak{T}$ levando ao mesmo espaço cociente $\mathfrak{C}'$, $\mathfrak{H}$ é bem determinado. Consideremos $\mathfrak{C}$, em seguida, como um espaço algébrico com o domínio operatório $\Omega = \mathfrak{Q} \subseteq \mathfrak{T}$, em que $\mathfrak{Q}$ é um conjunto qualquer de transformações pertencentes a $\mathfrak{T}$, e com um domínio de operações binárias formando um conjunto vazio $\Omega^* = O$. Na verdade, dada ρ, existe um domínio operatório máximo $\mathfrak{Q} = \mathfrak{H}$, que é composto pela totalidade das transformações para as quais $\mathfrak{C}' = \mathfrak{C}/\rho$ é uma divisão de $\mathfrak{C}$ em classes de congruência. $\mathfrak{H}$ é bem determinado e é um subgrupo de $\mathfrak{T}$, como vamos ver.

Se $S \in \mathfrak{H}$, deverá ter-se $(a\mathfrak{G})S \subseteq (aS)\mathfrak{G}$, mais precisamente, pois que S é uma transformação, $(a\mathfrak{G})S = (aS)\mathfrak{G}$. Se é também $T \in \mathfrak{H}$, então

$$(a\mathfrak{G})(ST) = ((a\mathfrak{G})S)T = ((aS)\mathfrak{G})T = (aST)\mathfrak{G} .$$

Por outro lado, de $(a\,\mathfrak{G})\,S = (a\,S)\,\mathfrak{G}$, conclui-se

$$(a\,S^{-1}\,\mathfrak{G})\,S = a\,\mathfrak{G}, \text{ ou } (a\,S^{-1})\,\mathfrak{G} = (a\,\mathfrak{G})\,S^{-1}.$$

Resulta daqui que $\mathfrak{H}$ é subgrupo, como se afirmou.

Os elementos de $\mathfrak{H}$ induzem transformações em $\mathfrak{C}'$, que formam um subgrupo $\mathfrak{H}'$, homomorfo de $\mathfrak{H}$, contido no grupo $\mathfrak{T}'$, de transformações de $\mathfrak{C}'$. O núcleo desse homomorfismo é precisamente $\mathfrak{h}$. Resulta, assim, o seguinte

TEOREMA 4: *Uma relação de equivalência ρ num conjunto $\mathfrak{C}$, com um grupo $\mathfrak{T}$ de transformações, é uma relação de congruência relativamente a um subgrupo máximo $\mathfrak{H}$, de $\mathfrak{T}$. Os elementos de $\mathfrak{H}$ induzem um grupo de transformações $\mathfrak{H}'$, no espaço cociente $\mathfrak{C}' = \mathfrak{C}/\rho$. O núcleo do homomorfismo $\mathfrak{H} \sim \mathfrak{H}'$ é o subgrupo $\mathfrak{h}$, gerado por todos os subgrupos de $\mathfrak{T}$ que levam à mesma divisão em classes de equivalência.*

Observe-se que, suposto $\mathfrak{G}$ um invariante em $\mathfrak{T}$, a relação de equivalência correspondente é uma relação de congruência relativamente a $\mathfrak{T}$. Tem-se, portanto:

COROLÁRIO 2: *Se $\mathfrak{G}$ é um invariante do grupo $\mathfrak{T}$, existe um invariante $\mathfrak{h}$, de $\mathfrak{T}$, intermédio entre $\mathfrak{G}$ e $\mathfrak{T}$, tal que $\mathfrak{T}/\mathfrak{h}$ se concretiza como grupo de transformações do conjunto $\mathfrak{C}' = \{a\,\mathfrak{G}, b\,\mathfrak{G}, \cdots\}$.*

Qualquer que seja o subgrupo $\mathfrak{G}$, o subgrupo $\mathfrak{H}$ contém $\mathfrak{G}$, assim como o normalizador de $\mathfrak{G}$ em $\mathfrak{T}$. Inversamente, tomado arbitràriamente um subgrupo $\mathfrak{T}_0$, de $\mathfrak{T}$, ele é sempre domínio operatório relativo a uma congruência definida por $\mathfrak{G}$ = grupo unidade, $\mathfrak{G} = \mathfrak{T}_0$, ou $\mathfrak{G} = \mathfrak{T}$.

2) **Grupos primitivos e imprimitivos** — Admitamos que $\mathfrak{G}$ é transitivo sobre $\mathfrak{C}$. $\mathfrak{G}$ diz-se *imprimitivo*, se for possível decompor $\mathfrak{C}$ sob a forma $\mathfrak{C} = \{\mathfrak{C}_i, \mathfrak{C}_j, \cdots, \mathfrak{C}_k, \cdots\}$, em subconjuntos $\mathfrak{C}_i$, nas condições seguintes: 1) os $\mathfrak{C}_i$ são disjuntos; 2) há, pelo menos, dois conjuntos $\mathfrak{C}_i$; 3) entre os conjuntos $\mathfrak{C}_i$, há um, pelo menos, com mais do que um elemento; 4) qualquer $\lambda \in \mathfrak{G}$ transforma exactamente um $\mathfrak{C}_i$ noutro subconjunto $\mathfrak{C}_j$.

Desta definição, tendo em conta a transitividade, resulta imediatamente que, dados $\mathfrak{C}_i$ e $\mathfrak{C}_j$ arbitrários, existe um $\sigma \in \mathfrak{G}$ tal que $\mathfrak{C}_i\sigma = \mathfrak{C}_j$.

Se $\mathfrak{G}$, sempre transitivo, não é imprimitivo, diz-se *primitivo*. Os conjuntos $\mathfrak{C}_i$, acima referidos, dizem-se *domínios de imprimitividade*.

Admitamos que $\mathfrak{G}$ é imprimitivo e fixemos $\mathfrak{C}_k$. Além da identidade $\varepsilon \in \mathfrak{G}$, pode haver outras transformações que deixem $\mathfrak{C}_k$ globalmente invariante. A sua totalidade forma um subgrupo $\mathfrak{G}_k$, de $\mathfrak{G}$. Tem lugar este

TEOREMA 1: *Há uma correspondência biunívoca completa entre as classes associadas de $\mathfrak{G}_k$ e os conjuntos $\mathfrak{C}_i$.* A demonstração é a mesma que a do teorema 2 do número anterior.

Uma proposição análoga à do teorema 3, de (III, 3, 1), é também válida aqui. Outro tanto se diz do corolário 1, igualmente de (III, 3, 1). Podemos observar ainda que o número de elementos dos diferentes $\mathfrak{C}_i$ é o mesmo.

Os grupos imprimitivos sobre $\mathfrak{C}$ podem reconhecer-se por via do seguinte

TEOREMA 2: *Se $\mathfrak{G}$ é um grupo transitivo sobre $\mathfrak{C}$ e $\mathfrak{G}_a$ é o subgrupo que deixa fixo o elemento $a \in \mathfrak{C}$, existe um subgrupo $\mathfrak{H}$, de $\mathfrak{G}$, intermediário entre $\mathfrak{G}_a$ e $\mathfrak{G}$, sempre que $\mathfrak{G}$ é imprimitivo; e, inversamente, a existência de $\mathfrak{H}$, nas condições indicadas, garante que $\mathfrak{G}$ é imprimitivo.*

Admitamos que $\mathfrak{G}$ é imprimitivo. Se designarmos por $\mathfrak{H}$ o subgrupo que deixa invariante o domínio de imprimitividade $\mathfrak{C}_1$, que contém a, esse subgrupo contém necessàriamente o subgrupo $\mathfrak{G}_a$, pois toda a transformação muda, por hipótese, um $\mathfrak{C}_i$ num $\mathfrak{C}_j$, determinando-se este último pela aplicação da transformação em causa a um elemento de $\mathfrak{C}_i$. Há, porém, elementos de $\mathfrak{H}$ que não pertencem a $\mathfrak{G}_a$, visto que, se for b um segundo elemento de $\mathfrak{C}_1$, a transformação que muda a em b pertence a $\mathfrak{H}$, mas não pertence a $\mathfrak{G}_a$. Como, por hipótese ainda, além de $\mathfrak{C}_1$, existe um $\mathfrak{C}_2$, pelo menos, uma transformação que mude um elemento de $\mathfrak{C}_1$ num elemento de $\mathfrak{C}_2$ pertence a $\mathfrak{G}$ mas não pertence a $\mathfrak{H}$. Tem-se, como se afirma no teorema, $\mathfrak{G}_a \subset \mathfrak{H} \subset \mathfrak{G}$.

Inversamente, dado $\mathfrak{H}$ nas condições indicadas, escrevamos $\mathfrak{G} = \mathfrak{H} \cup \mathfrak{H}\rho \cup \mathfrak{H}\sigma \cup \cdots$, $\mathfrak{H} = \mathfrak{G}_a \cup \mathfrak{G}_a\alpha \cup \mathfrak{G}_a\beta \cup \cdots$, e, portanto,

$$(1) \qquad \mathfrak{G} = (\mathfrak{G}_a \cup \mathfrak{G}_a\alpha \cup \cdots) \cup (\mathfrak{G}_a\rho \cup \mathfrak{G}_a\alpha\rho \cup \cdots) \cup \cdots.$$

Em seguida, ponhamos $a\,\mathfrak{H} = \mathfrak{C}_1$, $a\,\mathfrak{H}\rho = \mathfrak{C}_2$, $a\,\mathfrak{H}\sigma = \mathfrak{C}_3$, etc. Vamos ver que os $\mathfrak{C}_i$ assim determinados são, efectivamente, domínios de imprimitividade de $\mathfrak{G}$ sobre $\mathfrak{C}$. Em primeiro lugar, convém notar

que, na determinação de $\mathfrak{C}_1$, por exemplo, cada classe associada da decomposição $\mathfrak{H} = \mathfrak{G}_a \cup \mathfrak{G}_a\alpha \cup \cdots$ vai dar um só elemento de $\mathfrak{C}_1$. O teorema 2, de (III, 3, 1), garante que o processo indicado leva a todos os elementos de $\mathfrak{C}$, aparecendo cada elemento de $\mathfrak{C}$ uma só vez, quando se usa a decomposição (1), de $\mathfrak{G}$. Os $\mathfrak{C}_i$ são, pois, disjuntos. Do facto de ser $\mathfrak{G} \supset \mathfrak{H}$, resulta existirem dois conjunto $\mathfrak{C}_i$, pelo menos. E, por ser $\mathfrak{H} \supset \mathfrak{G}_a$, cada $\mathfrak{C}_i$ tem mais do que um elemento. Finalmente, uma transformação λ muda um $\mathfrak{C}_i$ num $\mathfrak{C}_j$.

Acabada a demonstração do teorema, podemos fazer estas duas observações: 1.ª) o subgrupo $\mathfrak{H}$ deixa invariante $\mathfrak{C}_1$, enquanto que os seus complexos associados transformam $\mathfrak{C}_1$ nos diferentes $\mathfrak{C}_i$; 2.ª) o grupo $\mathfrak{H}$ é transitivo sobre $\mathfrak{C}_1$.

Como aplicação interessante dos raciocínios deste §, tomemos o grupo de 4 elementos de KLEIN e ponhamos

$$\mathfrak{C} = \{\{1,2\},\{3,4\}\} = \{\{1,3\},\{2,4\}\} = \{\{1,4\},\{2,3\}\}.$$

Vê-se imediatamente que o conjunto $\mathfrak{C}$ dos quatro primeiros números naturais se pode decompor, dos modos indicados, em domínios de imprimitividade, relativamente ao grupo de KLEIN.

O grupo simétrico $\mathfrak{S}_n$ é primitivo sobre o conjunto $\mathfrak{C}$ dos n números a que respeita. De facto, por um lado, é transitivo. Suponhamos, por outro lado, que era possível decompor $\mathfrak{C}$ em domínios de imprimitividade. Excluídos os casos $n = 2^{\nu}$ ($\nu = 1$) para os quais a primitividade é banal, imaginemos $n \geqslant 4$. Então, $\mathfrak{C}$ poderia tomar, por exemplo, a forma $\mathfrak{C} = \{\{j, \cdots, k\}, \cdots, \{i, \cdots\}\}$. A permutação que mudasse $j, \cdots, k$ em $j, \cdots, i$ não transformaria entre si os domínios de decomposição de $\mathfrak{C}$, contra a hipótese.

BIBLIOGRAFIA

A. SPEISER, *Die Theorie der Gruppen von endlicher Ordnung*, zweite Ausgabe, Berlin, Springer, 1927.

B. L. VAN DER WAERDEN, *Moderne Algebra*, erster Teil, Berlin, Springer, 1930.

H. ZASSENHAUS, *Lehrbuch der Gruppentheorie*, Berlin, Teubner, 1937.

A. ALMEIDA COSTA, *Elementos da Teoria dos Grupos*, Porto, Centro de Estudos Matemáticos, 1942.

N JACOBSON, *Lectures in Abstract Algebra*, vol. I, New York, van Nostrand, 1951.

H. HERMES, *Einführung in die Verbandstheorie*, Berlin, Springer, 1955.

J. TIAGO DE OLIVEIRA, *Residuais de sistemas e radicais de anéis*, «Revista da Faculdade de Ciências de Lisboa», vol. V, 1956, pags. 177-245.

A. ALMEIDA COSTA, *Sur le suprêmum d'une famille de relations d'équivalence*, Revista da Faculdade de Ciências de Lisboa, vol. VII, 1958.

CAPÍTULO IV

Grupos com operadores

§ 1. Generalidades. Teoremas do isomorfismo

1) **Generalidades** — A noção geral de operador ou de operação unária foi introduzida em (III, 1, 1). Os grupos vão ser estudados agora nas condições seguintes: 1) consideram-se espaços algébricos $\mathfrak{G} = (\mathfrak{C}/\Omega, \Omega^*)$, onde $\Omega = \{\lambda, \mu, \nu, \cdots, \sigma, \omega, \cdots\}$ é o domínio dos operadores e onde Ω^* se reduz à operação binária do produto; 2) admitem-se os postulados referidos em qualquer dos sistemas citados em (II, 1, 5); 3) os operadores supõem-se distributivos, isto é, admite-se que $(ab)\sigma = a\sigma \cdot b\sigma$, quaisquer que sejam $a, b \in \mathfrak{G}$.

A aplicação $a \to a\sigma$ é um endomorfismo de $\mathfrak{G}$, como resulta de 3). Pode acontecer, porém, que operadores diferentes determinem o mesmo endomorfismo. Esse facto, que, em termos de operação, mal se compreende, será justificado um pouco mais adiante. Quando a operadores distintos corresponderem endomorfismos distintos, podemos identificar os operadores com os endomorfismos que eles determinam.

Em (III, 1, 8), dissemos o que devia entender-se por grupo automórfico de $\mathfrak{G}$, grupo que designámos por $A_{\mathfrak{G}}$. O conjunto $A_{\mathfrak{G}}$ poderia tomar-se como um sistema de operadores.

Os teoremas demonstrados no Capítulo III, nos quais intervêm as noções de subgrupo e de invariante, são igualmente válidos para os grupos com operadores, mediante as restrições seguintes: 1) como

subgrupos apenas se consideram os *subgrupos-Ω*, também designados *subgrupos admissíveis*, isto é aqueles subgrupos que são subsistemas de $\mathfrak{G} = (\mathfrak{C}/\Omega, \Omega^*)$; trata-se, portanto, de subgrupos $\mathfrak{g}$ tais que, para cada $c \in \mathfrak{g}$, é também $c\sigma \in \mathfrak{g}$, com $\sigma \in \Omega$ arbitrário; 2) como invariantes apenas se consideram os *invariantes-Ω*, ou *invariantes admissíveis*, isto é aqueles invariantes $\mathfrak{H}$, tais que, para cada $c \in \mathfrak{H}$, é $c\sigma \in \mathfrak{H}$; são os invariantes que se põem em correspondência biunívoca completa com as congruências, nos termos indicados em (III, 1, 10), tendo em conta a definição geral de congruência dada em (III, 1, 1), que aqui tem de respeitar o facto de existirem operações unárias; 3) como homorfismos, isomorfismos, endomorfismos e automorfismos apenas se consideram os que se tomam no sentido-Ω, isto é: suposto que o mesmo domínio Ω opera sobre o grupo $\mathfrak{G}$ e sobre a sua imagem $\mathfrak{G}'$ (nesta está também definida uma operação de produto), a correspondência $a \to a'$ obedece à lei seguinte: $a\sigma \to (a\sigma)' = a'\sigma$, com σ arbitrário. Conforme a terminologia de (III, 1, 1), os dois sistemas $\mathfrak{G}$ e $\mathfrak{G}'$ são semelhantes: os homorfismos e correspondências similares são entendidos no sentido fixado naquele lugar.

A circunstância de haver em causa uma única operação arrasta que não haja necessidade de a pôr em evidência. Justifica-se que se diga, como já fizemos em parte: subgrupo-Ω, invariante-Ω, homomorfismo-Ω, etc.

Nesta ordem de ideias, podemos enunciar, por exemplo, o teorema 1, de (III, 1, 7), desta maneira: o produto $\mathfrak{h}\mathfrak{g}$ é um subgrupo-Ω, de $\mathfrak{G}$, suposto este um grupo-Ω, se $\mathfrak{g}$ for um invariante-Ω e $\mathfrak{h}$ um subgrupo-Ω.

A noção de grupo factor exige que o invariante $\mathfrak{H}$ seja invariante-Ω. Nessas condições, $\mathfrak{G}/\mathfrak{H}$ admite o domínio operatário Ω, como, em particular, vamos verificar. Tomemos $x\mathfrak{H}$ e escrevamos, por definição $(x\mathfrak{H})\sigma = (x\sigma)\mathfrak{H}$. A coerência da definição exige que, sendo $x\mathfrak{H} = y\mathfrak{H}$, seja também $(x\sigma)\mathfrak{H} = (y\sigma)\mathfrak{H}$. Ora a hipótese $x = yh$, para um certo $h \in \mathfrak{H}$, dá $x\sigma = (yh)\sigma = y\sigma \cdot h\sigma = y\sigma \cdot h'$, se se põe $h\sigma = h' \in \mathfrak{H}$. Como a condição $h\sigma \in \mathfrak{H}$ é realizada, vê-se que os elementos $x\sigma$ e $y\sigma$ definem o mesmo complexo, tendo-se portanto, como se deseja, $(x\sigma)\mathfrak{H} = (y\sigma)\mathfrak{H}$. A distributividade dos operadores também se realiza.

O grupo factor $\mathfrak{G}/\mathfrak{H}$ é semelhante a $\mathfrak{G}$. O enunciado do teorema do homomorfismo, que, para grupos-Ω, deverá substituir o que se deu em (III, 1, 9), é o seguinte: se $\mathfrak{G}$ é um grupo-Ω e $\mathfrak{H}$ um invariante-Ω, então $\mathfrak{G}/\mathfrak{H} = \overline{\mathfrak{G}}$ é um grupo-Ω cociente, tendo lugar o seguinte homomorfismo-Ω: $\mathfrak{G} \sim \overline{\mathfrak{G}}$; reciprocamente, se $\mathfrak{G} \sim \overline{\mathfrak{G}}$ é um homomorfismo-Ω entre dois grupos-Ω, segue-se que $\overline{\mathfrak{G}}$, a menos de isomorfismo-Ω, é um grupo-Ω cociente.

É ocasião de fazermos a justificação a que já nos referimos, relativa à existência de operadores iguais. Quando se passa de $\mathfrak{G}$ a $\mathfrak{G}/\mathfrak{H}$, ao admitir-se que o domínio operatório Ω, de $\mathfrak{G}$, também o é do grupo cociente, nada impede que dois operadores λ e μ não possam ser tais que $(x\mathfrak{H})\lambda = (x\mathfrak{H})\mu$, para todas as classes $x\mathfrak{H}$. Imaginemos, por exemplo, que λ e μ aplicam $\mathfrak{G}$ em $\mathfrak{H}$. Então, no grupo cociente, é $(x\mathfrak{H})\lambda = (x\mathfrak{H})\mu = \mathfrak{H}$, qualquer que seja $x\mathfrak{H}$.

EXEMPLOS IMPORTANTES DE DOMÍNIOS Ω: Quando se faz Ω = totalidade dos automorfismos internos de $\mathfrak{G}$, os subgrupos admissíveis são os invariantes; se se toma Ω = totalidade dos automorfismos de $\mathfrak{G}$, os subgrupos admissíveis são determinados invariantes, que se dizem *subgrupos característicos*; e, finalmente, se Ω = totalidade dos endomorfismos de $\mathfrak{G}$, os subgrupos admissíveis são determinados subgrupos característicos, que se dizem *invariantes completos*.

OBSERVAÇÃO: Tendo em conta certas conveniências, também utilizaremos neste Capítulo, ao lado da letra $\mathfrak{G}$, a letra $\mathfrak{P}$ para significar grupo.

2) **Os homomorfismos-Ω e a correspondência entre subgrupos** — Seja $\mathfrak{G} \sim \mathfrak{G}'$ um homomorfismo-Ω. Como se trata duma aplicação dum grupo sobre outro, escreveremos $a \to a' = a\varphi$, para significar o referido homomorfismo. Se o núcleo é $\mathfrak{N}$, para qualquer subconjunto $\mathfrak{C} \subseteq \mathfrak{G}$, tem-se $\mathfrak{C}\varphi\varphi^{-1} = \mathfrak{C}\mathfrak{N}$. O símbolo φ^{-1} é usado aqui no sentido que foi esclarecido em (I, 1, 3): trata-se de imagem completa inversa. Então, na verdade, por via de φ, passa-se de $\mathfrak{C}$ a $\mathfrak{C}\varphi = \mathfrak{C}'$, tendo-se $\mathfrak{C}'\varphi^{-1} = \mathfrak{C}\varphi\varphi^{-1} = \mathfrak{C}\mathfrak{N}$, pois que $a\mathfrak{N} = a'\varphi^{-1}$ é a totalidade dos elementos de $\mathfrak{G}$ de imagem a'.

Se $\mathfrak{C}$ e $\mathfrak{D}$ forem dois subconjuntos de $\mathfrak{G}$, de imagens $\mathfrak{C}'$ e $\mathfrak{D}'$, e se for já $\mathfrak{D} = \mathfrak{D}'\varphi^{-1} = \mathfrak{D}\mathfrak{N}$, tem-se $(\mathfrak{C}'\mathfrak{D}')\varphi^{-1} = \mathfrak{C}\mathfrak{D}$, e isto porque $(\mathfrak{C}'\mathfrak{D}')\varphi^{-1} = (\mathfrak{C}\mathfrak{D})\mathfrak{N} = \mathfrak{C}(\mathfrak{D}\mathfrak{N}) = \mathfrak{C}\mathfrak{D}$.

Quando $\mathfrak{C}'$ é um subbrupo-Ω, também $\mathfrak{C}'\varphi^{-1}$ é subgrupo-Ω, e, quando $\mathfrak{H}'$ é invariante-Ω, é igualmente invariante-Ω a imagem completa inversa $\mathfrak{H}'\varphi^{-1}$. Reconheçamos, por exemplo, o carácter de subgrupo de $\mathfrak{C}'\varphi^{-1}$. Para isso, provaremos que, sendo $s \in \mathfrak{C}'\varphi^{-1}$, é $s(\mathfrak{C}'\varphi^{-1}) = \mathfrak{C}'\varphi^{-1}$, e que se tem $(\mathfrak{C}'\varphi^{-1})\lambda \subseteq \mathfrak{C}'\varphi^{-1}$, para qualquer $\lambda \in \Omega$.

A imagem de $s(\mathfrak{C}'\varphi^{-1})$ é $s'\mathfrak{C}' = \mathfrak{C}'$, de sorte que $s(\mathfrak{C}'\varphi^{-1}) \subseteq \mathfrak{C}'\varphi^{-1}$. Mas $[s(\mathfrak{C}'\varphi^{-1})]\mathfrak{N} = \mathfrak{C}'\varphi^{-1}$. Como o 1.º membro desta última igualdade se pode ainda escrever $s(\mathfrak{C}'\varphi^{-1}\cdot\mathfrak{N}) = s(\mathfrak{C}'\varphi^{-1})$, resulta $s(\mathfrak{C}'\varphi^{-1}) = \mathfrak{C}'\varphi^{-1}$. Quanto a $(\mathfrak{C}'\varphi^{-1})\lambda$, notemos que a sua imagem é $\mathfrak{C}'\lambda \subseteq \mathfrak{C}'$. Daí se conclui imediatamente $(\mathfrak{C}'\varphi^{-1})\lambda \subseteq \mathfrak{C}'\varphi^{-1}$.

O facto de que $\mathfrak{C}\varphi$ é subgrupo-Ω ou invariante-Ω, conforme $\mathfrak{C}$ for subgrupo ou invariante-Ω, é imediato. Convém fixar o seguinte

TEOREMA: *Se $\mathfrak{G} \sim \mathfrak{G}'$ é um homomorfismo-Ω entre dois grupos-Ω, de núcleo $\mathfrak{N}$ e definido escrevendo $a \to a' = a\varphi$, pode afirmar-se:* 1) *suposto $\mathfrak{C}$ um subconjunto de elementos de $\mathfrak{G}$, é $\mathfrak{C}\varphi\varphi^{-1} = \mathfrak{C}\mathfrak{N}$;* 2) *supostos $\mathfrak{C}$ e $\mathfrak{D}$ dois subconjuntos de elementos de $\mathfrak{G}$, de imagens $\mathfrak{C}'$ e $\mathfrak{D}'$, então, sob a hipótese $\mathfrak{D}'\varphi^{-1} = \mathfrak{D}\mathfrak{N} = \mathfrak{D}$, é $(\mathfrak{C}'\mathfrak{D}')\varphi^{-1} = \mathfrak{C}\mathfrak{D}$;* 3) *tomados um snbgrupo-Ω e um invariante-Ω, de $\mathfrak{G}'$, também as suas imagens completas inversas são, respectivamente, subgrupo-Ω e invariante-Ω;* 4) *finalmente, se $\mathfrak{C}$ e $\mathfrak{D}$ são, respectivamente, subgrupo-Ω e invariante-Ω, as suas imagens $\mathfrak{C}\varphi$ e $\mathfrak{D}\varphi$ estão nas mesmas condições.*

A afirmação 3) do teorema pode precisar-se, nos termos seguintes: *a aplicação $\mathfrak{C}' \to \mathfrak{C}'\varphi^{-1}$ é uma aplicação biunívoca completa de subgrupos em subgrupos e de invariantes em invariantes; os diferentes $\mathfrak{C}'\varphi^{-1}$ contêm sempre o núcleo do homomorfismo.*

De futuro, sempre que falarmos de subgrupos ou de invariantes, assim como de homomorfismos, devem os mesmos ser entendidos no «sentido-Ω». A maior parte das demonstrações dos teoremas do Capítulo, embora tendo sempre em mente que estão em jogo grupos-Ω, será feita como se tratasse de grupos sem operadores. Esse facto tem a sua justificação na circunstância de que aquilo que nas referidas demonstrações faz intervir os operadores se reveste de carácter quase imediato.

3) **Os teoremas do isomorfismo** — Os resultados do número anterior permitem-nos estabelecer, de modo quase imediato, dois teoremas que são conhecidos sob os nomes de 1.º e 2.º teoremas do isomorfismo. Existe um terceiro teorema do isomorfismo, devido a H. ZASSENHAUS, de que aqui também nos ocuparemos.

1.º TEOREMA DO ISOMORFISMO: *Tomemos o homomorfismo $\mathfrak{G} \sim \mathfrak{G}' = \mathfrak{G}\varphi$, entre dois grupos. Se $\mathfrak{N}$ for o núcleo, a cada invariante $\mathfrak{H} \supseteq \mathfrak{N}$ corresponde um invariante $\mathfrak{H}' = \mathfrak{H}\varphi$, de tal modo que tem lugar o isomorfismo $\mathfrak{G}/\mathfrak{H} \simeq \mathfrak{G}'/\mathfrak{H}'$.* De facto, consideremos os dois homomorfismos

$$\mathfrak{G} \sim \mathfrak{G}' \sim \mathfrak{G}'/\mathfrak{H}', \text{ dos quais resulta } \mathfrak{G} \sim \mathfrak{G}'/\mathfrak{H}'.$$

O núcleo deste último homomorfismo é exactamente $\mathfrak{H}$. Pelo teorema do homomorfismo, tem-se, então,

$$\mathfrak{G}/\mathfrak{H} \simeq \mathfrak{G}'/\mathfrak{H}', \text{ numa correspondência } a\mathfrak{H} \leftrightarrow (a\varphi)\mathfrak{H}' = (a\varphi)(\mathfrak{H}\varphi).$$

COROLÁRIO: *Considerado o homomorfismo $\mathfrak{G} \sim \mathfrak{G}/\mathfrak{N}$ e tomado o invariante $\mathfrak{H} \supseteq \mathfrak{N}$, tem se $\mathfrak{G}/\mathfrak{H} \simeq (\mathfrak{G}/\mathfrak{N})/(\mathfrak{H}/\mathfrak{N})$.*

2.º TEOREMA DO ISOMORFISMO: *Se $\mathfrak{G}$ é um grupo, $\mathfrak{h}$ um subgrupo e $\mathfrak{N}$ um invariante, tem lugar o isomorfismo seguinte: $\mathfrak{h}\mathfrak{N}/\mathfrak{N} \simeq \mathfrak{h}/\mathfrak{h}\cap\mathfrak{N}$.* Sabemos, na verdade, que $\mathfrak{N}$ é invariante de $\mathfrak{h}\mathfrak{N}$. No homomorfismo $\mathfrak{h}\mathfrak{N} \sim \mathfrak{h}\mathfrak{N}/\mathfrak{N}$, já $\mathfrak{h}$ tem todo o grupo factor $\mathfrak{h}\mathfrak{N}/\mathfrak{N}$ como imagem. Neste homomorfismo $\mathfrak{h} \sim \mathfrak{h}\mathfrak{N}/\mathfrak{N}$, o núcleo é $\mathfrak{h}\cap\mathfrak{N}$. Então, o teorema resulta do teorema do homomorfismo.

3.º TEOREMA DO ISOMORFISMO: *Supostos $\mathfrak{G}$ um grupo, $\mathfrak{G}_1$ e $\mathfrak{G}_2$ dois subgrupos e $\mathfrak{G}'_1$ e $\mathfrak{G}'_2$ dois invariantes de $\mathfrak{G}_1$ e $\mathfrak{G}_2$, respectivamente, tem lugar o isomorfismo seguinte:*

$$(1)\quad (\mathfrak{G}_1\cap\mathfrak{G}_2)\mathfrak{G}'_1/(\mathfrak{G}_1\cap\mathfrak{G}'_2)\mathfrak{G}'_1 \simeq (\mathfrak{G}_1\cap\mathfrak{G}_2)\mathfrak{G}'_2/(\mathfrak{G}'_1\cap\mathfrak{G}_2)\mathfrak{G}'_2.$$

Consideremos o grupo $\mathfrak{G}_1$, no qual $\mathfrak{G}_1\cap\mathfrak{G}_2$ é um subgrupo e $\mathfrak{G}'_1$ é invariante. Sabemos que $(\mathfrak{G}_1\cap\mathfrak{G}_2)\cap\mathfrak{G}'_1 = \mathfrak{G}'_1\cap\mathfrak{G}_2$ é invariante em $\mathfrak{G}_1\cap\mathfrak{G}_2$. De modo análogo se vê que $\mathfrak{G}_1\cap\mathfrak{G}'_2$ é também invariante em $\mathfrak{G}_1\cap\mathfrak{G}_2$. Provaremos que se tem

$$(2)\quad (\mathfrak{G}_1\cap\mathfrak{G}_2)/(\mathfrak{G}'_1\cap\mathfrak{G}_2)(\mathfrak{G}_1\cap\mathfrak{G}'_2) \simeq (\mathfrak{G}_1\cap\mathfrak{G}_2)\mathfrak{G}'_1/(\mathfrak{G}_1\cap\mathfrak{G}'_2)\mathfrak{G}'_1.$$

Então, tendo em conta que o 1.º membro desta relação é simétrico nos dois índices 1 e 2, o teorema é consequência imediata da transitividade e da simetria do isomorfismo. Consideremos os homomorfismos

$$(3)\qquad \mathfrak{G}_1 \sim \mathfrak{G}_1/\mathfrak{G}'_1,\ \mathfrak{G}_1\cap\mathfrak{G}_2 \sim (\mathfrak{G}_1\cap\mathfrak{G}_2)\mathfrak{G}'_1/\mathfrak{G}'_1,$$

o segundo dos quais é uma parte do primeiro. Deste segundo homomorfismo, concluimos outro, a saber:

$$(\mathfrak{G}'_1\cap\mathfrak{G}_2)(\mathfrak{G}_1\cap\mathfrak{G}'_2) \sim (\mathfrak{G}'_1\cap\mathfrak{G}_2)(\mathfrak{G}_1\cap\mathfrak{G}'_2)\mathfrak{G}'_1/\mathfrak{G}'_1 = (\mathfrak{G}_1\cap\mathfrak{G}'_2)\mathfrak{G}'_1/\mathfrak{G}'_1.$$

O produto indicado em primeiro lugar é um produto de dois invariantes de $\mathfrak{G}_1 \cap \mathfrak{G}_2$. Então, tendo em conta o 1.º teorema do isomorfismo, o 2.º homomorfismo (3) e o anterior, somos levados a

$$(4)\quad \mathfrak{G}_1\cap\mathfrak{G}_2/(\mathfrak{G}'_1\cap\mathfrak{G}_2)(\mathfrak{G}_1\cap\mathfrak{G}'_2)\simeq[(\mathfrak{G}_1\cap\mathfrak{G}_2)\mathfrak{G}'_1/\mathfrak{G}'_1]/[(\mathfrak{G}_1\cap\mathfrak{G}'_2)\mathfrak{G}'_1/\mathfrak{G}'_1].$$

Estudando agora o homomorfismo

$$(5)\qquad (\mathfrak{G}_1\cap\mathfrak{G}_2)\mathfrak{G}'_1\sim(\mathfrak{G}_1\cap\mathfrak{G}_2)\mathfrak{G}'_1/\mathfrak{G}'_1,$$

a circunstância de $(\mathfrak{G}_1\cap\mathfrak{G}'_2)\mathfrak{G}'_1/\mathfrak{G}'_1$, como se vê em (4), ser um invariante do 2.º membro de (5) faz-nos passar ao invariante $(\mathfrak{G}_1\cap\mathfrak{G}'_2)\mathfrak{G}'_1$, do 1.º membro de (5), sendo $(\mathfrak{G}_1\cap\mathfrak{G}_2)\mathfrak{G}'_1/(\mathfrak{G}_1\cap\mathfrak{G}'_2)\mathfrak{G}'_1$ isomorfo do 2.º membro de (4), e, portanto, do 1.º membro de (4), como se deseja.

Observação: Na demonstração do 3.º teorema do isomorfismo, utilizámos o 1.º teorema do isomorfismo, assim como certas propriedades demonstradas no número anterior. Pode demonstrar-se agora o 2.º teorema do isomorfismo, aplicando o 3.º em condições especiais. Tomemos, com efeito, o subgrupo $\mathfrak{G}_1=\mathfrak{h}$, o seu invariante $\mathfrak{G}'_1=\{u\}$, assim como um invariante $\mathfrak{G}'_2=\mathfrak{N}$, de $\mathfrak{G}$, e o subgrupo $\mathfrak{G}_2=\mathfrak{h}\mathfrak{N}$. Vem, em vez de (1), $\mathfrak{h}/\mathfrak{h}\cap\mathfrak{N}\simeq\mathfrak{h}\mathfrak{N}/\mathfrak{N}$, precisamente o 2.º teorema do isomorfismo, na notação que para o mesmo foi utilizada.

§ 2. Séries de composição. Condições de cadeia. Grupos resolúveis.

1) **Definições** — Seja $\mathfrak{G}=\mathfrak{G}_0$ um grupo dado e sejam $\mathfrak{G}_1,\mathfrak{G}_2,\cdots,\mathfrak{G}_c$ subgrupos de $\mathfrak{G}_0$ satisfazendo às duas condições seguintes: 1) tem-se $\mathfrak{G}_0\supseteq\mathfrak{G}_1\supseteq\cdots\supseteq\mathfrak{G}_c=\{u\}$, isto é, cada subgrupo contém o seguinte e o último é o subgrupo unidade; 2) cada $\mathfrak{G}_i$ é invariante de $\mathfrak{G}_{i-1}$. Supondo $\mathfrak{G}_0\supset\mathfrak{G}_1\supset\cdots\supset\mathfrak{G}_c\not\supset\{u\}$, diz-se que se tem uma *série normal* do grupo dado, sem repetições. O número c diz-se *comprimento* da série. Esse número é também dado pelo número de grupos factores $\mathfrak{G}_{i-1}/\mathfrak{G}_i$.

A série normal pode «refinar-se», introduzindo entre dois subgrupos consecutivos outros subgrupos, por forma a ter-se uma nova série normal. Se a série normal é tal que não tem repetições (não há dois

$\mathfrak{G}_i$ consecutivos iguais) e não pode «refinar-se» sem repetições, diz-se uma *série de composição*. Os grupos factores correspondentes, que são, então, grupos simples, dizem-se *factores de composição*.

Duas séries de composição dizem-se *equivalentes*, se os seus factores de composição são isomorfos. A definição não exige, porém, que os factores de composição isomorfos se localizem igualmente nas duas séries de composição, mas exige, evidentemente, que sejam iguais os números dos elementos que compõem cada série.

Também, para duas séries normais, se define uma equivalência, em termos análogos aos que acabam de indicar-se, devendo precisar-se que a existência de repetições numa delas implica necessàriamente a existência de repetições na outra.

2) **O teorema de Schreier** — O terceiro teorema do isomorfismo permite dar uma demonstração construtiva dum teorema importante, devido a O. Schreier, que tem este enunciado:

Teorema 1: *Duas séries normais dum grupo qualquer têm sempre refinamentos equivalentes.* Tomemos o grupo $\mathfrak{G}=\mathfrak{G}_1=\mathfrak{H}_1$ e consideremos as duas séries normais

$$\mathfrak{G}_1\supseteq\mathfrak{G}_2\supseteq\cdots\supseteq\mathfrak{G}_{s+1}=\{u\},\quad \mathfrak{H}_1\supseteq\mathfrak{H}_2\supseteq\cdots\supseteq\mathfrak{H}_{t+1}=\{u\},$$

do referido grupo. Façamos

$$\mathfrak{G}_{ij}=\mathfrak{G}_{i+1}\cdot(\mathfrak{G}_i\cap\mathfrak{H}_j),\quad \mathfrak{H}_{ji}=\mathfrak{H}_{j+1}\cdot(\mathfrak{H}_j\cap\mathfrak{G}_i).$$

Na primeira igualdade, supõe-se $(i=1,2,\cdots,s),(j=1,2,\cdots t+1)$; e, na segunda, supõe-se $(j=1,2,\cdots,t),(i=1,2,\cdots,s+1)$. Vê-se que se tem

$$\mathfrak{G}_1=\mathfrak{G}_{11}\supseteq\mathfrak{G}_{12}\supseteq\cdots\supseteq\mathfrak{G}_{1t}\supseteq\mathfrak{G}_{1,t+1}=\mathfrak{G}_2=\mathfrak{G}_{21}\supseteq\cdots\supseteq\mathfrak{G}_{2,t+1}=\mathfrak{G}_3=\mathfrak{G}_{31}\supseteq\cdots$$

$$(1)\qquad \supseteq\mathfrak{G}_{s-1,t+1}=\mathfrak{G}_s=\mathfrak{G}_{s1}\supseteq\cdots\supseteq\mathfrak{G}_{s,t+1}=\{u\};$$

$$\mathfrak{H}_1=\mathfrak{H}_{11}\supseteq\mathfrak{H}_{12}\supseteq\cdots\supseteq\mathfrak{H}_{1s}\supseteq\mathfrak{H}_{1,s+1}=\mathfrak{H}_2=\mathfrak{H}_{21}\supseteq\cdots\supseteq\mathfrak{H}_{2,s+1}=\mathfrak{H}_3=\mathfrak{H}_{31}\supseteq\cdots$$

$$(2)\qquad \supseteq\mathfrak{H}_{t-1,s+1}=\mathfrak{H}_t=\mathfrak{H}_{t1}\supseteq\cdots\supseteq\mathfrak{H}_{t,s+1}=\{u\}.$$

Vamos reconhecer que, tanto (1) como (2), são séries normais. Para isso, reconheçamos, por exemplo, que $\mathfrak{H}_{j,i+1}$ é invariante de $\mathfrak{H}_{ji}$. Se, com as notações usadas na demonstração do 3.º teorema do isomorfismo, pusermos

$$\mathfrak{G}_1=\mathfrak{H}_j,\quad \mathfrak{G}'_1=\mathfrak{H}_{j+1},\quad \mathfrak{G}_2=\mathfrak{G}_i,\quad \mathfrak{G}'_2=\mathfrak{G}_{i+1},$$

vemos que $(\mathfrak{G}_1 \cap \mathfrak{G}_2)\mathfrak{G}'_1 = \mathfrak{H}_{j+1} \cdot (\mathfrak{H}_j \cap \mathfrak{G}_i) = \mathfrak{H}_{ji}$, enquanto que $(\mathfrak{G}_1 \cap \mathfrak{G}'_2)\mathfrak{G}'_1 = \mathfrak{H}_{j+1} \cdot (\mathfrak{H}_j \cap \mathfrak{G}_{i+1}) = \mathfrak{H}_{j,i+1}$. O reconhecimento anunciado está feito. Também $\mathfrak{G}_{i,j+1}$ é invariante de $\mathfrak{G}_{ij}$. Por outro lado, nos termos precisos do 3.º teorema do isomorfismo, é $\mathfrak{G}_{ij}/\mathfrak{G}_{i,j+1} \simeq \mathfrak{H}_{ji}/\mathfrak{H}_{j,i+1}$. As duas séries normais (1) e (2), cada uma das quais contém $s\,t + 1$ termos, são, de facto, equivalentes.

Uma consequência notável do teorema de SCHREIER está contida na proposição seguinte:

TEOREMA DE JORDAN-HÖLDER: *Se um grupo tem séries de composição, duas séries de composição são equivalentes.* Na verdade, à face do teorema de SCHREIER, as duas séries de composição têm refinamentos equivalentes. Como, por outro lado, tais refinamentos não existem (a não ser que se considerem repetições), a afirmação resulta imediatamente.

Vamos estudar alguns casos particulares. Suponhamos Ω reduzido aos automorfismos internos. Dissémos, em (IV, 1, 1), que os subgrupos admissíveis são os invariantes. Uma série de composição diz-se, neste caso, uma *série principal*: trata-se duma cadeia de invariantes de $\mathfrak{G}$, cada um deles máximo no anterior. Se Ω se reduz à totalidade dos automorfismos, uma série de composição diz-se uma *série característica*; finalmente, se Ω se reduz à totalidade dos endomorfismos, a série de composição toma o nome de *série de invariantes completos.* Podemos dizer:

TEOREMA 2: *Duas séries principais, ou características ou de invariantes completos têm o mesmo comprimento.*

Outro exemplo de interesse é fornecido pelo grupo simétrico $\mathfrak{S}_n$, do qual démos já propriedades em (III, 2). Suporemos vazio o domínio Ω. Então, suposto $n > 4$, como o grupo alterno $\mathfrak{A}_n$ é simples, o que se demonstrou em (III, 2, 5), a série de composição de $\mathfrak{S}_n$ reduz-se a $\mathfrak{S}_n \supset \mathfrak{A}_n \supset (1)$. Para $n = 4$, tem-se a série de composição $\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset \mathfrak{B} \supset |(1), (1\,2)\cdot(3\,4)| \supset (1)$. onde $\mathfrak{B}$ é o grupo de 4 elementos de KLEIN. Estes resultados jogam com a nota feita no final do referido lugar (III, 2, 5).

3) **As condições de cadeia** — A extensão aos grupos infinitos de certos teoremas primeiramente demonstrados para grupos finitos pode fazer-se mediante as *condições de cadeia*, que vamos definir e analisar.

Um grupo $\mathfrak{G}$ satisfaz à *condição de cadeia descendente*, se toda a cadeia da forma $\mathfrak{G}_1 \supset \mathfrak{G}_2 \supset \cdots$, começada num divisor normal de $\mathfrak{G}$ e continuada sob a hipótese de $\mathfrak{G}_i$ ser invariante de $\mathfrak{G}_{i-1}$, for finita.

Um grupo $\mathfrak{G}$ satisfaz à *condição de cadeia ascendente*, se nele se verificar o seguinte: [illegible], toda a cadeia ascendente da forma $\mathfrak{H}_1 \subset \mathfrak{H}_2 \subset \cdots$, na qual figuram apenas invariantes de $\mathfrak{H}_i$, é finita.

Eis agora algumas proposições que fazem intervir a condição de cadeia ascendente.

TEOREMA 1: *Num grupo $\mathfrak{G}$ satisfazendo à condição de cadeia ascendente, é condição necessária e suficiente, para que um endomorfismo φ seja um automorfismo, que se tenha $\mathfrak{G}\varphi = \mathfrak{G}$.* A afirmação da «necessidade» é trivial. Para verificarmos a suficiência, comecemos por observar que, designando por $\mathfrak{N}_\varphi$ o núcleo do endomorfismo, e, duma maneira geral, por $\mathfrak{N}_{\varphi^k}$, o núcleo do endomorfismo $\varphi^k = \varphi \cdots \varphi$ (k vezes), é

$$|u| \subseteq \mathfrak{N}_\varphi \subseteq \mathfrak{N}_{\varphi^2} \subseteq \cdots . \tag{1}$$

Vamos ver que se tem $\mathfrak{N}_\varphi = |u|$, se for $\mathfrak{G}\varphi = \mathfrak{G}$. Daí se conclui a suficiência em questão. Para se provar a igualdade $\mathfrak{N}_\varphi = |u|$, mostraremos que a inclusão $|u| \subset \mathfrak{N}_\varphi$, no sentido próprio, implica que a cadeia (1) seja infinita. Mais precisamente ainda, limitamo-nos a mostrar que a hipótese $|u| \subset \mathfrak{N}_\varphi$ leva a $\mathfrak{N}_\varphi \subset \mathfrak{N}_{\varphi^2}$. Se fosse $\mathfrak{N}_\varphi = \mathfrak{N}_{\varphi^2}$, ter-se-ia $z\varphi = u$, sempre que $z\varphi^2 = u$, $(z \in \mathfrak{G})$. Ora, sendo $\mathfrak{G}\varphi = \mathfrak{G}$, de $v\varphi = u$, pondo $v = x\varphi$, deduzimos $x\varphi^2 = u$, portanto $x\varphi = v = u$. A igualdade $\mathfrak{N}_\varphi = \mathfrak{N}_{\varphi^2}$ arrastaria $\mathfrak{N}_\varphi = |u|$, contra a hipótese. O teorema considera se assim demonstrado.

Voltemos ao endomorfismo φ e a admitir a condição de cadeia ascendente. Na cadeia (1), suponhamos k o inteiro mínimo para o qual $\mathfrak{N}_{\varphi^k} = \mathfrak{N}_{\varphi^{k+1}}$. Vamos provar este

TEOREMA 2: *Suposto $\mathfrak{G}$ um grupo satisfazendo à condição de cadeia ascendente e admitindo que, na cadeia (1), $\mathfrak{N}_{\varphi^k}$ é o primeiro elemento igual ao seguinte, tem lugar a igualdade $\mathfrak{N}_{\varphi^k} \cap \mathfrak{G}\varphi^k = |u|$.* De facto, se x pertence à intersecção em causa, existe $y \in \mathfrak{G}$ tal que $x = y\varphi^k$. Então, da hipótese $x\varphi^k = u$, resulta $y\varphi^{2k} = u$, o que leva a $y \in \mathfrak{N}_{\varphi^{2k}} = \mathfrak{N}_{\varphi^k}$, e, portanto, a $y\varphi^k = u = x$, como se deseja.

Por isto, diremos que σ é um *endomorfismo normal* de $\mathfrak{G}$, se comutar com todos os automorfismos internos. Para tais endomorfismos, é válida a proposição a seguir.

TEOREMA 3: *Se σ for um endomorfismo normal, dado um invariante $\mathfrak{H}$, também $\mathfrak{H}\sigma$ é um invariante; suposto ψ igualmente normal, o mesmo se diz de $\sigma\psi$; e, finalmente, para cada $x \in \mathfrak{G}$ tem-se $x\sigma = x \cdot c$, onde c é um elemento que comuta com qualquer elemento de $\mathfrak{G}\sigma$.* Tomemos $\mathfrak{H}\sigma$. Tem-se $x(\mathfrak{H}\sigma)x^{-1} = (x\mathfrak{H}x^{-1})\sigma \subseteq \mathfrak{H}\sigma$, o que caracteriza $\mathfrak{H}\sigma$ como invariante. Passando ao estudo de $\sigma\psi$, vê-se que $(xax^{-1})\sigma\psi = [x(a\sigma)x^{-1}]\psi = x(a\sigma\psi)x^{-1}$, de sorte que $\sigma\psi$ é normal. Para a última parte do teorema, observemos que

$$x(a\sigma)x^{-1} = (xax^{-1})\sigma, \quad \text{ou} \quad x(a\sigma)x^{-1} = (x\sigma)(a\sigma)(x\sigma)^{-1}.$$

Daqui tira-se

$$x(a\sigma)x^{-1} \cdot x\sigma = (x\sigma)(a\sigma), \quad \text{ou} \quad x(a\sigma)x^{-1}(x\sigma)(a\sigma)^{-1} = x\sigma.$$

Por outro lado, porém, é $x\sigma = x(x^{-1} \cdot x\sigma)$, de sorte que $x^{-1} \cdot x\sigma = (a\sigma)x^{-1}(x\sigma)(a\sigma)^{-1}$, igualdade donde se deduz $(x^{-1} \cdot x\sigma)(a\sigma) = (a\sigma)(x^{-1} \cdot x\sigma)$, que mostra ser $x^{-1} \cdot x\sigma$ comutável com $a\sigma$, qualquer que seja a. Assim, $x\sigma = x \cdot (x^{-1} \cdot x\sigma) = x \cdot c$, como se afirmou.

Quando o grupo satisfaz à condição de cadeia descendente e o endomorfismo σ se supõe normal, são válidos dois teoremas que, em certo sentido, estão em correlação com os teoremas 1 e 2. Tem-se:

TEOREMA 1': *Num grupo satisfazendo à condição de cadeia descendente, suposto σ um endomorfismo normal, é necessário e basta, para que σ seja um automorfismo, que seja um meromorfismo.* A afirmação da «necessidade» é trivial. Para verificarmos a suficiência, comecemos por observar que é

$$\mathfrak{G} \supseteq \mathfrak{G}\sigma \supseteq \mathfrak{G}\sigma^2 \supseteq \cdots. \tag{2}$$

Vamos ver que se tem $\mathfrak{G}\sigma = \mathfrak{G}$, se for $\mathfrak{N}_\sigma = \{u\}$. Daí se conclui a suficiência em questão. Para se provar a igualdade $\mathfrak{G}\sigma = \mathfrak{G}$, mostraremos que a inclusão $\mathfrak{G} \supset \mathfrak{G}\sigma$, no sentido próprio, implica que a cadeia (2) seja infinita. Mais precisamente ainda, limitamo-nos a mostrar que a hipótese $\mathfrak{G} \supset \mathfrak{G}\sigma$ leva a $\mathfrak{G}\sigma \supset \mathfrak{G}\sigma^2$. Os raciocínios indicarão claramente como se generaliza a conclusão. Em $\mathfrak{G} \sim \mathfrak{G}\sigma$, por ser σ um meromorfismo, a parte correspondente de $\mathfrak{G}\sigma \subset \mathfrak{G}$ será $\mathfrak{G}\sigma^2 \subset \mathfrak{G}\sigma$. É o que se deseja.

TEOREMA 2': *Suposto $\mathfrak{G}$ um grupo satisfazendo à condição de cadeia descendente e admitindo que, na cadeia (2), $\mathfrak{G}\sigma^l$ é o primeiro elemento igual ao seguinte, tem lugar a igualdade $\mathfrak{N}_{\sigma^l} \cdot \mathfrak{G}\sigma^l = \mathfrak{G}$, sob a hipótese, é claro, de σ ser normal.* Tomando x qualquer, é, por hipótese, para um certo y, $x\sigma^l = y\sigma^{2l}$, o que nos leva a $(x \cdot y^{-1}\sigma^l)\sigma^l = u$. Então, escrevendo $x = [x(y^{-1}\sigma^l)](y\sigma^l)$, vê-se que $x(y^{-1}\sigma^l) \in \mathfrak{N}_{\sigma^l}$. E, como $y\sigma^l \in \mathfrak{G}\sigma^l$, o teorema está demonstrado.

Seja agora um grupo satisfazendo às duas condições de cadeia e admitamos que τ é um endomorfismo normal. São válidos os dois teoremas que passamos a enunciar.

TEOREMA 1'': *Se $\mathfrak{G}$ satisfaz às duas condições de cadeia e τ é um endomorfismo normal, é condição necessária e suficiente, para que se tenha $\mathfrak{G}\tau = \mathfrak{G}$, que seja $\mathfrak{N}_\tau = \{u\}$.* A parte «necessária» é consequência do teorema 1; a parte «suficiente» é consequência do teorema 1'.

TEOREMA 2'': *Se $\mathfrak{G}$ satisfaz às duas condições de cadeia e τ é um endomorfismo normal, os dois números k e l, dos teoremas 2 e 2' são iguais.* De facto, sendo $\mathfrak{N}_{\tau^k} \cap \mathfrak{G}\tau^k = \{u\}$, será *a fortiori* $\mathfrak{N}_\tau \cap \mathfrak{G}\tau^k = \{u\}$. Não há elemento em $\mathfrak{G}\tau^k$, salvo u, que seja aplicado por τ no elemento u. Então, τ é um meromorfismo em $\mathfrak{G}\tau^k$, e como este subgrupo é um invariante e *as condições de cadeia se transportam dum grupo para os seus invariantes*, segue-se que τ é um automorfismo em $\mathfrak{G}\tau^k$, o que leva a $\mathfrak{G}\tau^k = \mathfrak{G}\tau^{k+1} = \cdots$ e implica $k \gtreqless l$. Por outro lado, sabemos que $\mathfrak{G}\tau^l = \mathfrak{G}\tau^{l+1} = (\mathfrak{G}\tau^l)\tau$. Então, τ é um endomorfismo de $\mathfrak{G}\tau^l$, que é um homomorfismo. Será um automorfismo, o que implica $\mathfrak{G}\tau^l \cap \mathfrak{N}_\tau = \{u\}$. Tomemos agora $y \in \mathfrak{G}$ tal que $y\tau^{l+1} = (y\tau^l)\tau = u$. Do que acaba de ver-se, conclui-se $y\tau^l = u$, pelo que $y \in \mathfrak{N}_{\tau^l}$. Será, portanto, $\mathfrak{N}_{\tau^l} = \mathfrak{N}_{\tau^{l+1}}$, o que leva a $l \gtreqless k$. Será necessàriamente $k = l$, como afirma o teorema.

Terminaremos este número, demonstrando o importante teorema a seguir, que justifica a afirmação feita logo no seu começo, relativa à extensão a grupos infinitos, de proposições primeiramente estabelecidas para grupos finitos.

TEOREMA 4: *É condição necessária e suficiente, para que um grupo tenha série de composição, que verifique as duas condições de cadeia.* A condição é *necessária*: — Se existe série de composição, esta terá um certo comprimento c. Não poderá, então, formar-se uma cadeia

ascendente ou uma cadeia descendente, nos termos indicados nas respectivas definições, com mais de $c+1$ elementos.

A condição é *suficiente*: Supostas válidas as condições de cadeia, partamos de $\mathfrak{G}$. Se o grupo for simples (irredutível), a série de composição é $\mathfrak{G} \supset \{u\}$. Não o sendo, tomemos o invariante $\mathfrak{K}_1$, de $\mathfrak{G}$. Pode acontecer que seja $\mathfrak{K}_1$ um invariante máximo em $\mathfrak{G}$, de sorte que $\mathfrak{G}/\mathfrak{K}_1$ é simples. Então, $\mathfrak{G} \supset \mathfrak{K}_1$ é um começo de série de composição. Se $\mathfrak{K}_1$ não é máximo, existe $\mathfrak{K}_2$ tal que $\mathfrak{G} \supset \mathfrak{K}_2 \supset \mathfrak{K}_1$. À face da condição ascendente de cadeia, chega-se a $\mathfrak{K}_i = \mathfrak{G}_1$ tal que $\mathfrak{G} \supset \mathfrak{G}_1$ é um começo de série de composição. O facto de $\mathfrak{G}_1$ ser invariante em $\mathfrak{G}$ transporta para aqui as condições de cadeia, de sorte que se chega a $\mathfrak{G} \supset \mathfrak{G}_1 \supset \mathfrak{G}_2$, com $\mathfrak{G}_2$ máximo em $\mathfrak{G}_1$. O processo continua, mas é limitado pela condição de cadeia descendente. O teorema está provado.

OBSERVAÇÕES: No caso dos grupos comutativos, as condições de cadeia têm os enunciados mais simples seguintes: I) a condição descendente é válida, se toda a cadeia de subgrupos da forma $\mathfrak{M}_1 \supset \mathfrak{M}_2 \supset \cdots$ for finita; II) a cadeia ascendente é válida, se toda a cadeia de subgrupos da forma $\mathfrak{M}_1 \subset \mathfrak{M}_2 \subset \cdots$ for finita.

Devem-se a ARTIN enunciados equivalentes, conhecidos sob os nomes de *condição de mínimo* e *condição de máximo*. Assim, em vez de I), podemos dizer: em todo o conjunto de subgrupos, há um subgrupo mínimo, ou seja um subgrupo que não contém outro subgrupo do conjunto. E, em vez de II), tem-se: em todo o conjunto de subgrupos, há um subgrupo máximo, ou seja um subgrupo que não está contido noutro subgrupo do conjunto.

4) **Grupos resolúveis** — Razões sobre as quais não é possível falar neste momento levaram a designar por *grupos resolúveis* aqueles grupos que têm qualquer das três propriedades seguintes:

I) possuem uma série normal, para a qual os grupos cocientes respectivos são abelianos;

II) possuem uma série normal, só composta de invariantes, para a qual os grupos cocientes são abelianos;

III) possuem uma *série derivada* finita.

A propriedade III) é entendida no sentido seguinte: Se $\mathfrak{G}', \mathfrak{G}'', \cdots$ são os grupos derivados sucessivos do grupo $\mathfrak{G}$, tal como foram definem (III, 1, 11), tem-se $\mathfrak{G} \supset \mathfrak{G}' \supset \mathfrak{G}'' \supset \cdots \supset \mathfrak{G}^{(n)} = \{u\}$.

Antes de demonstrarmos a equivalência das três propriedades indicadas, vamos provar um teorema que nos será útil. No referido lugar (III, 1, 11), vimos que o primeiro e o segundo derivado dum grupo são invariantes do grupo. Dum modo geral, tem-se:

TEOREMA 1: *Os subgrupos derivados sucessivos de* $\mathfrak{G}$ *são invariantes de* $\mathfrak{G}$. Em primeiro lugar, dado $\mathfrak{G}$, *o derivado* $\mathfrak{G}'$ *é invariante completo de* $\mathfrak{G}$, porque, se φ for um endomorfismo qualquer do grupo, tem-se $[(a\,b)(b\,a)^{-1}]\varphi = (a\varphi \cdot b\varphi))(b\varphi \cdot a\varphi)^{-1}$, o que mostra que a aplicação φ leva dum comutador de dois elementos a um comutador de dois elementos. Nestas condições $\mathfrak{G}^{(k)}$, como derivado de $\mathfrak{G}^{(k-1)}$, é invariante completo deste último. Em segundo lugar, a «propriedade de invariante completo é transitiva», isto é: se $\mathfrak{K}$ for invariante completo de $\mathfrak{L}$ e este for invariante completo de $\mathfrak{Q}$, é $\mathfrak{K}$ invariante completo de $\mathfrak{Q}$. Na verdade, um endomorfismo qualquer de $\mathfrak{Q}$ aplica $\mathfrak{L}$ em si, definindo um endomorfismo de $\mathfrak{L}$, de sorte que a sua aplicação a $\mathfrak{K}$, que é invariante completo de $\mathfrak{L}$, define um endomorfismo de $\mathfrak{K}$. O teorema é agora imediato.

Há também interesse incidental em fixar esta proposição:

TEOREMA 2: *Se, tomado o homomorfismo* $\mathfrak{G} \sim \mathfrak{G}/\mathfrak{H}$, *for o grupo cociente um grupo abeliano, então, qualquer subgrupo* $\mathfrak{K}$, *que contenha* $\mathfrak{H}$, *é invariante de* $\mathfrak{G}$. De facto, $\mathfrak{K}/\mathfrak{H}$, como subgrupo de $\mathfrak{G}/\mathfrak{H}$, é seu invariante. ~~Pelo 1.º teorema do isomorfismo, será~~ $\mathfrak{K}$ invariante de $\mathfrak{G}$. Feito isto, demonstremos o

TEOREMA 3: *As propriedades* I), II) *e* III) *são equivalentes*. Sem dúvida que II) implica I). Mostraremos que III) implica II) e que I) implica III). Se III) é válida, tem-se $\mathfrak{G} \supset \mathfrak{G}' \supset \cdots \supset \mathfrak{G}^{(n)} = \{u\}$. O teorema 1, junto ao teorema 6 de (III, 1, 11), mostra que II) tem lugar. Finalmente, se I) é válida, tomemos a respectiva série normal $\mathfrak{G} \supset \mathfrak{G}_1 \supset \cdots \supset \mathfrak{G}_s \supset \{u\}$. Como $\mathfrak{G}/\mathfrak{G}_1$ é abeliano, vimos em (III, 1, 11), que $\mathfrak{G}' \subseteq \mathfrak{G}_1$. Se admitirmos que $\mathfrak{G}^{(k)} \subseteq \mathfrak{G}_k$, vamos provar que $\mathfrak{G}^{(k+1)} \subseteq \mathfrak{G}_{k+1}$. Ora $\mathfrak{G}_k/\mathfrak{G}_{k+1}$ é abeliano, o que leva a $\mathfrak{G}'_k \subseteq \mathfrak{G}_{k+1}$; como, porém, de $\mathfrak{G}^{(k)} \subseteq \mathfrak{G}_k$, se conclui $\mathfrak{G}^{(k+1)} \subseteq \mathfrak{G}'_k$, vê-se que, efectivamente, $\mathfrak{G}^{(k+1)} \subseteq \mathfrak{G}_{k+1}$. Será, necessàriamente, $\mathfrak{G}^{(k)} = \{u\}$. O teorema fica assim estabelecido.

Dada uma série normal dum grupo resolúvel, ela tem sempre um refinamento para o qual os grupos factores correspondentes são abelianos, como resulta imediatamente do teorema de SCHREIER, pois que

um refinamento duma série normal com grupos cocientes abelianos possui ainda grupos cocientes abelianos. Em particular, se um grupo resolúvel tem série de composição, os factores de composição são abelianos.

Para estabelecermos a proposição que abaixo indicamos como teorema 4, carecemos do seguinte

LEMA: *Tomada a série normal* $\mathfrak{G}\supset\mathfrak{G}_1\supset\cdots\supset\mathfrak{G}_s\supset\{u\}$ *e suposto* $\mathfrak{h}$ um subgrupo de $\mathfrak{G}$, é $\mathfrak{h}\supset(\mathfrak{h}\cap\mathfrak{G}_1)\supset\cdots\supset(\mathfrak{h}\cap\mathfrak{G}_s)\supset\{u\}$ *uma série normal de* $\mathfrak{h}$, *para a qual os grupos cocientes respectivos são isomorfos de subgrupos dos grupos cocientes correspondentes da série normal dada.* Sem dúvida que a série indicada para $\mathfrak{h}$ é normal. Então, de $\mathfrak{h}/\mathfrak{h}\cap\mathfrak{G}_1\simeq\mathfrak{h}\mathfrak{G}_1/\mathfrak{G}_1$, concluimos que o seu 1.º grupo cociente é isomorfo dum subgrupo de $\mathfrak{G}/\mathfrak{G}_1$. Anàlogamente, de $\mathfrak{h}\cap\mathfrak{G}_1/\mathfrak{h}\cap\mathfrak{G}_2\simeq(\mathfrak{h}\cap\mathfrak{G}_1)\mathfrak{G}_2/\mathfrak{G}_2$, concluimos que o 2.º grupo cociente da série normal de $\mathfrak{h}$ é isomorfo dum subgrupo de $\mathfrak{G}_1/\mathfrak{G}_2$, etc. É válido, então, este

TEOREMA 4: *Um subgrupo dum grupo resolúvel* $\mathfrak{G}$ *é resolúvel. Se* $\mathfrak{G}$ *tem série de composição, o mesmo acontece ao subgrupo. Os factores de composição da série relativa ao subgrupo são isomorfos de certos factores de composição da série de composição de* $\mathfrak{G}$. A primeira parte do enunciado justifica-se tendo em conta que, no lema, é $\mathfrak{h}\cap\mathfrak{G}_i/\mathfrak{h}\cap\mathfrak{G}_{i+1}$ um grupo abeliano, se $\mathfrak{G}_i/\mathfrak{G}_{i+1}$ o for. Quanto ao resto, basta observar que aquele grupo factor é simples, podendo reduzir-se ao grupo unidade.

5) **Sobre os grupos resolúveis finitos** — O transporte aos grupos finitos da noção de grupo resolúvel leva ao resultado de que nos vamos ocupar. Consideremos uma série de composição do grupo. Os factores de composição são grupos abelianos, finitos e simples; são grupos cíclicos de ordem prima.

Se um grupo abeliano é finito, é necessàriamente resolúvel.

Como exemplo de grupos resolúveis, podemos citar ainda o grupo simétrico $\mathfrak{S}_4$ e todos os grupos de ordem p^n, com p primo. Quanto a $\mathfrak{S}_4$, reconhece-se a afirmação, pelo facto de às séries de composição respectivas corresponderem factores de composição de ordens 2 e 3. Relativamente aos grupos de ordem p^n, vamos reconhecê-la, depois de algumas considerações preliminares.

Sabemos, de (III, 1, 11), que o número de elementos de uma classe de elementos conjugados é um divisor da ordem do grupo. Deste modo, se o grupo tem p^n elementos, as classes terão um número de elementos da forma p^r, com $r\gtrless n$. Se a_r for o número de classes com p^r elementos, como o conjunto das classes abrange todos os elementos do grupo, tem-se

$$p^n = a_0 + a_1 p + a_2 p^2 + \cdots + a_q p^q .$$

a_0 representa o número de classes com um elemento ou seja o número de elementos do centro do grupo. Escrevendo

$$a_0 = p\,(p^{n-1} - a_q p^{q-1} - \cdots - a_1),$$

como não pode ser $a_0 = 0$, será a_0 um múltiplo de p. Trata-se duma propriedade que convem fixar, relativa ao centro do grupo.

Tendo agora em conta que o centro dum grupo é um invariante abeliano do mesmo, segue-se que um grupo simples de ordem p^n é idêntico ao seu centro. Só pode ser, de resto, como já dissemos, $p=1$. /n

Posto isto, tomemos, então, um grupo $\mathfrak{G}$, de ordem p^n. Se é simples, acabamos de ver que é resolúvel. Se não é simples, seja $\mathfrak{H}$ um invariante do grupo. A ordem de $\mathfrak{H}$ é da forma p^λ, com $\lambda<n$. O grupo cociente $\mathfrak{G}/\mathfrak{H}$ é da ordem $p^{n-\lambda}$, de sorte que, construida uma série de composição de $\mathfrak{G}$, todos os factores de composição são abelianos, da ordem p, pelo que $\mathfrak{G}$, como se afirmou, é resolúvel.

§ 3 Produtos directos

1) **Construção de produtos directos** — Suponhamos dados n grupos $\mathfrak{P}_i, (i=1,2,\cdots,n)$, e formemos os sistemas da forma $(a_1, a_2, \cdots, a_n)$, com $a_i \in \mathfrak{P}_i$. Para esses sistemas, introduziremos um produto mediante a regra

$$(a_1,\cdots,a_n)\cdot(b_1,\cdots,b_n) = (a_1 b_1, \cdots a_n b_n), \qquad (b_i \in \mathfrak{P}_i).$$

A aplicação dum operador λ será definida pela igualdade $(a_1\cdots,a_n)\lambda = (a_1\lambda, \cdots a_n\lambda)$, pois se admite que os $\mathfrak{P}_i$ são semelhantes. Então, com as duas regras acabadas de dar, o conjunto dos sistemas

$(a_1, \cdots, a_n)$ forma um grupo-Ω, para o qual o elemento um é $(u_1, \cdots, u_n)$, suposto u_i o elemento um de $\mathfrak{P}_i$. Escreveremos

$$\mathfrak{P} = \mathfrak{P}_1 \times \cdots \times \mathfrak{P}_n \tag{1}$$

e diremos que $\mathfrak{P}$ é o *produto directo* dos $\mathfrak{P}_i$.

Constituem grupos isomorfos de $\mathfrak{P}$ os grupos da forma

$$(\mathfrak{P}_{i_1} \times \cdots \times \mathfrak{P}_{i_h}) \times (\mathfrak{P}_{i_{h+1}} \times \cdots \times \mathfrak{P}_{i_k}) \times \cdots \times (\mathfrak{P}_{i_l} \times \cdots \times \mathfrak{P}_{i_n}), \tag{2}$$

desde que se ponha a correspondência biunívoca

$$(a_1, \cdots, a_n) \longleftrightarrow ((a_{i_1}, \cdots, a_{i_h}); (a_{i_{h+1}}, \cdots, a_{i_k}); \cdots; (a_{i_l}, \cdots, a_{i_n})).$$

Por esse facto, diremos que o produto directo é comutativo e associativo: não distinguiremos entre o grupo (1) e o grupo (2).

Tratando-se de módulos, substituiremos a igualdade (1) pela seguinte:

$$\mathfrak{M} = \mathfrak{M}_1 + \cdots + \mathfrak{M}_n. \tag{3}$$

Enquanto, em (1), cada $\mathfrak{P}_i$ se diz *factor directo* dum produto directo igual a $\mathfrak{P}$, em (3), cada $\mathfrak{M}_i$ é *parcela directa* duma *soma directa* igual a $\mathfrak{M}$.

2) **Os invariantes $\mathfrak{P}'_i$** — Estudemos, dentro do produto directo, os sistemas de elementos da forma $(a_1, u_2, \cdots, u_n)$, por exemplo. Os raciocínios que vamos fazer aplicam-se inteiramente ao estudo de sistemas de elementos da forma $(u_1, \cdots, u_{i-1}, a_i, u_{i+1}, \cdots, u_n)$.

Reconhece-se imediatamente que os elementos em questão formam subgrupo. Vamos ver que se trata de invariante em $\mathfrak{P}$. Tem-se:

$$(b_1, \cdots, b_n)(a_1, u_2, \cdots, u_n)(b_1, \cdots, b_n)^{-1} =$$
$$= (b_1, \cdots, b_n)(a_1, u_2, \cdots, u_n)(b_1^{-1}, \cdots, b_n^{-1}) = (b_1 a_1 b_1^{-1}, u_2, \cdots, u_n),$$

resultado que justifica a afirmação, pois que é também $(a_1, u_2, \cdots, u_n)\lambda = (a_1\lambda, u_2, \cdots, u_n)$. Representaremos por $\mathfrak{P}'_1$ o invariante em questão. Anàlogamente se define $\mathfrak{P}'_i$.

Os invariantes $\mathfrak{P}'_i$ satisfazem às duas condições seguintes:

I) $\mathfrak{P}'_1 \mathfrak{P}'_2 \cdots \mathfrak{P}'_n = \mathfrak{P}$;

II) $\mathfrak{P}'_1 \cdots \mathfrak{P}'_{i-1} \mathfrak{P}'_{i+1} \cdots \mathfrak{P}'_n \cap \mathfrak{P}'_i = u$ = elemento um de $\mathfrak{P}$.

A propriedade I) é imediata. Quanto a II), se $(c_1, \cdots, c_n)$ é um elemento da intersecção em causa, terá, por um lado, a forma $(a_1, \cdots, a_{i-1}, u_i, a_{i+1}, \cdots, u_n)$; por outro, porém, essa forma é $(u_1, \cdots, u_{i-1}, a_i, u_{i+1}, \cdots, u_n)$. Daqui resulta que se tem $c_i = a_i = u_i$, $c_j = a_j = u_j$, $(j \neq i)$, pelo que $(c_1, \cdots, c_n) = u$, como se afirmou.

Admitamos, em seguida, que, dentro dum grupo $\mathfrak{P}$, há um sistema de invariantes $\mathfrak{P}'_i$, verificando I) e II). Se construirmos grupos abstractos $\mathfrak{P}_i$, isomorfos dos $\mathfrak{P}'_i$, num isomorfismo $a_i \to a'_i \in \mathfrak{P}'_i$, e, depois, se considerarmos a correspondência

$$(a_1, a_2, \cdots, a_n) \to a'_1 a'_2 \cdots a'_n, \tag{1}$$

vamos provar que tal correspondência é um isomorfismo entre o produto directo dos $\mathfrak{P}_i$ e o produto $\mathfrak{P}'_1 \cdots \mathfrak{P}'_n$. Do facto de se ter $\mathfrak{P}'_i \cap \mathfrak{P}'_j = u$, se $i \neq j$, resulta, como se viu em (III, 1, 7), que $a'_i a'_j = a'_j \cdot a'_i$. Então, se for

$$(b_1, b_2, \cdots, b_n) \to b'_1 b'_2 \cdots b'_n,$$

é também

$$(a_1, \cdots, a_n)(b_1, \cdots, b_n) = (a_1 b_1, \cdots, a_n b_n) \to (a'_1 b'_1) \cdots (a'_n b'_n) =$$
$$= (a'_1 \cdots a'_n)(b'_1 \cdots b'_n).$$

A correspondência (1) é um homomorfismo. Tomado, porém, $u \in \mathfrak{P}$, será, em (1), $a'_1 = \cdots = a'_n = u$, porque, de $a'_1 \cdots a'_n = u$, deduzimos, por exemplo, $a'^{-1}_i = a'_1 \cdots a'_{i-1} a'_{i+1} \cdots a'_n$, o que, pela condição II), implica $a'^{-1}_i = u$, $a'_i = u$, qualquer que seja i. Ter-se-à $a_1 = u_1, \cdots, a_n = u_n$, de sorte que se obtem $(u_1, \cdots, u_n)$ como elemento único, de correspondente u. Em suma: Tem lugar este

TEOREMA: *É condição necessária e suficiente, para que $\mathfrak{P}$ seja isomorfo do produto directo* (1), *do número anterior, que existam invariantes $\mathfrak{P}'_i$ em $\mathfrak{P}$, $(i = 1, 2, \cdots, n)$, tais que tenham lugar as condições* I) *e* II). *Diz-se também que $\mathfrak{P}$ é produto directo dos seus invariantes $\mathfrak{P}'_i$.*

3) **Outro critério de produto directo** — Nas aplicações, principalmente na teoria dos módulos, é útil reconhecer que um grupo $\mathfrak{P}$ é produto directo de certos dos seus invariantes, empregando o critério contido no seguinte

TEOREMA 1: *É condição necessária e suficiente, para que* $\mathfrak{P}$ *seja produto directo dos seus subgrupos* $\mathfrak{P}_i$, $(i = 1, 2, \cdots, n)$, *que se verifiquem as propriedades seguintes:* 1) *Tomados* $a_i \in \mathfrak{P}_i$, $a_j \in \mathfrak{P}_j$, *é* $a_i a_j = a_j a_i$, *se* $i \neq j$; 2) *cada elemento* a *do grupo pode escrever-se, duma maneira única, sob a forma* $a = a_1 a_2 \cdots a_n$. A condição é *necessária*: — Quando se afirma que $\mathfrak{P}$ é produto directo dos $\mathfrak{P}_i$, estes são subentendidos como invariantes, no sentido indicado na parte final do teorema do número anterior. Vimos, então, que $a_i a_j = a_j a_i$, $(i \neq j)$, assim como mostámos ter-se $a = a_1 a_2 \cdots a_n$, $(a_i \in \mathfrak{P}_i)$. Para se provar que, supondo $a_1 \cdots a_n = b_1 \cdots b_n$, é $a_i = b_i$, observemos que, da igualdade $a_n b_n^{-1} = (a_1^{-1} b_1) \cdots (a_{n-1}^{-1} b_{n-1})$, à face da propriedade II) do número anterior, se conclui $a_n b_n^{-1} = \phi$, ou seja $a_n = b_n$. Partindo agora de $a_1 \cdots a_{n-1} = b_1 \cdots b_{n-1}$, ou aproveitando imediatamente a comutatividade dos elementos a_i e a_j, à mesma conclusão se é levado para qualquer índice: $a_i = b_i$.

A condição é *suficiente*: — Comecemos por provar que, sob as hipóteses do teorema, os $\mathfrak{P}_i$ são invariantes. Tomemos $g_i \in \mathfrak{P}_i$ e escrevamos $a g_i a^{-1} = a_1 \cdots a_n g_i a_n^{-1} \cdots a_1^{-1} = a_1 \cdots (a_i g_i a_i^{-1}) a_n^{-1} \cdots$. Como $a_i g_i a_i^{-1} \in \mathfrak{P}_i$, a hipótese da comutatividade leva ainda a $a g_i a^{-1} = a_i g_i a_i^{-1}$, precisamente um resultado que leva à conclusão desejada. A condição I) do número anterior é realizada por hipótese. Quanto à condição II), também do número anterior, observemos que uma igualdade $a_i = a_1 \cdots a_{i-1} a_{i+1} \cdots a_n$, à qual pode dar-se a forma $u \cdots u a_i u \cdots u = a_1 \cdots a_{i-1} u a_{i+1} \cdots a_n$, exige que se tenha $a_i = u$, como se conclui da propriedade 2) do enunciado do teorema actual. A referida condição II) está verificada e a proposição fica estabelecida.

EXEMPLO DE PRODUTO DIRECTO: No estudo dos grupos cíclicos, vimos, em (III, 1, 3) e em (III, 1, 5), que, suposta $N = p_1^{r_1} \cdots p_s^{r_s}$ a ordem do grupo, o seu elemento gerador a se podia escrever sob a forma $a = a_1 \cdots a_s$, onde a_i é de ordem $p_i^{r_i}$, $(i = 1, 2, \cdots, s)$. Tem-se, precisamente, $[a] = [a_1] \times \cdots \times [a_s]$, significando $[a_i]$ o grupo cíclico gerado por a_i.

Outro exemplo importante de produto directo foi encontrado em (IV, 2, 3), em correlação com os teoremas 2, 2' e 2'', aí estabelecidos. Podemos dar, com efeito, este enunciado:

TEOREMA 2 (FITTING): *Se* $\mathfrak{P}$ *é um grupo satisfazendo às duas condições de cadeia e se* φ *é um endomorfismo normal, pode escrever-se* $\mathfrak{P} = (\mathfrak{P}_{\varphi^k}) \times \mathfrak{N}_{\varphi^k}$, *para um certo inteiro* k. *Em* $\mathfrak{P}_{\varphi^k}$, *o endomorfismo* φ *determina um automorfismo, e, para cada* $z \in \mathfrak{N}_{\varphi^k}$, *tem-se* $z\varphi^k = u$.

OBSERVAÇÕES: 1) É imediato que uma parte dum produto directo é um produto directo. Assim, se for $\mathfrak{P} = \mathfrak{P}_1 \times \mathfrak{P}_2 \times \cdots \times \mathfrak{P}_n$, podemos também escrever $\mathfrak{P} = \mathfrak{Q}_1 \times \mathfrak{Q}_2 \times \cdots \times \mathfrak{Q}_s$, se supusermos $\mathfrak{Q}_1 = \mathfrak{P}_1 \times \cdots \times \mathfrak{P}_{n_1}$, $\mathfrak{Q}_2 = \mathfrak{P}_{n_1+1} \times \cdots \times \mathfrak{P}_{n_2}$, etc. Dum modo geral, recorrendo à associatividade e à comutatividade dos *factores directos* $\mathfrak{P}_i$, podem dar-se ao produto $\mathfrak{P}$ formas diversas.

2) Se for $\mathfrak{P} = \mathfrak{P}_1 \times \mathfrak{P}_2$, o segundo teorema do isomorfismo dá $\mathfrak{P}_1 \simeq \mathfrak{P} / \mathfrak{P}_2$, $\mathfrak{P}_2 \simeq \mathfrak{P} / \mathfrak{P}_1$. Admitindo, porém, que $\mathfrak{P} = \mathfrak{P}_1 \mathfrak{P}_2$ é simplesmente um produto de dois invariantes já a mesma conclusão se não pode tirar.

3) Tomemos, então, $\mathfrak{P} = \mathfrak{P}_1 \mathfrak{P}_2$ e suponhamos que $\mathfrak{P}$ tem série de composição de comprimento $c(\mathfrak{P})$. Vamos demonstrar a igualdade

$$c(\mathfrak{P}) + c(\mathfrak{P}_1 \cap \mathfrak{P}_2) = c(\mathfrak{P}_1) + c(\mathfrak{P}_2), \tag{1}$$

na qual os diferentes símbolos representam comprimentos de séries de composição. Ponhamos $\mathfrak{P}_1 \cap \mathfrak{P}_2 = \mathfrak{P}_3$. Fàcilmente se vê que é

$$\mathfrak{P} / \mathfrak{P}_3 = (\mathfrak{P}_1 / \mathfrak{P}_3) \times (\mathfrak{P}_2 / \mathfrak{P}_3). \tag{2}$$

Imaginemos, com efeito, que podemos dar a um elemento do segundo membro os dois aspectos contidos na igualdade

$$(a_1 \mathfrak{P}_3) \cdot (a_2 \mathfrak{P}_3) = (a'_1 \mathfrak{P}_3) \cdot (a'_2 \mathfrak{P}_3), \quad (a_i, a'_i \in \mathfrak{P}_i).$$

Concluiríamos, tendo sempre em conta que os $\mathfrak{P}_i$ são invariantes, as relações seguintes: $a_1 a_2 = (a'_1 a'_2) a'_3$, $(a'_1 a'_2)^{-1} (a_1 a_2) = a'^{-1}_2 (a'^{-1}_1 a_1) a_2 = (a'^{-1}_2 a_2) a''_1 = a'_3$, onde $a'_3 \in \mathfrak{P}_3$, $a''_1 \in \mathfrak{P}_1$. A inclusão $\mathfrak{P}_3 \subseteq \mathfrak{P}_1$ mostra que $a'^{-1}_2 a_2 \in \mathfrak{P}_1 \cap \mathfrak{P}_2 = \mathfrak{P}_3$, de sorte que $a_2 \mathfrak{P}_3 = a'_2 \mathfrak{P}_3$. De modo análogo se provaria a igualdade $a_1 \mathfrak{P}_3 = a'_1 \mathfrak{P}_3$. Considerando, em seguida, a equação $a_1 a_2 = (a_2 a_1) x$, vê-se que $x = a_1^{-1} a_2^{-1} a_1 \cdot a_2 = a_1^{-1} \cdot a_2^{-1} a_1 a_2 \in \mathfrak{P}_3$, pelo que $(a_1 \mathfrak{P}_3)(a_2 \mathfrak{P}_3) = (a_2 \mathfrak{P}_3)(a_1 \mathfrak{P}_3)$. À face do critério de produto directo dado neste número, o produto (2) é um produto directo. Resulta daí a igualdade

$$c(\mathfrak{P} / \mathfrak{P}_3) = c(\mathfrak{P}_1 / \mathfrak{P}_3) + c(\mathfrak{P}_2 / \mathfrak{P}_3). \tag{3}$$

Ora é muito fácil de ver que, por exemplo,

$$c(\mathfrak{P}) = c(\mathfrak{P}_3) + c(\mathfrak{P}/\mathfrak{P}_3).$$

Então, de (3). deduz-se

$$c(\mathfrak{P}) - c(\mathfrak{P}_3) = c(\mathfrak{P}_1) - c(\mathfrak{P}_3) + c(\mathfrak{P}_2) - c(\mathfrak{P}_3),$$

consequentemente a relação desejada (1).

4) Tomemos dois grupos $\mathfrak{G}$ e $\mathfrak{P}$ com as séries de composição

$$\mathfrak{G} \supset \mathfrak{G}' \supset \mathfrak{G}'' \supset \cdots \supset |u_1|, \qquad \mathfrak{P} \supset \mathfrak{P}' \supset \mathfrak{P}'' \supset \cdots \supset |u_2|,$$

de comprimentos m e n, respectivamente. O produto directo $\mathfrak{G} \times \mathfrak{P}$ admite as duas séries de composição

$$\mathfrak{G} \times \mathfrak{P} \supset \mathfrak{G} \times \mathfrak{P}' \supset \cdots \supset \mathfrak{G} \times |u_2| \supset \mathfrak{G}' \times |u_2| \supset \cdots \supset |u_1| \times |u_2|,$$
$$\mathfrak{P} \times \mathfrak{G} \supset \mathfrak{P} \times \mathfrak{G}' \supset \cdots \supset \mathfrak{P} \times |u_1| \supset \mathfrak{P}' \times |u_1| \supset \cdots \supset |u_2| \times |u_1|,$$

de comprimento $m + n$ Deixamos a demonstração ao cuidado do leitor.

5) A última observação é a seguinte. Suponhamos $\mathfrak{G} = \mathfrak{A} \times \mathfrak{B}$. Claramente que se tem $\mathfrak{G} \supseteq \mathfrak{A}$, $\mathfrak{B} = \mathfrak{G} \cap \mathfrak{B}$, de sorte que podemos escrever $\mathfrak{G} = \mathfrak{A} \times (\mathfrak{G} \cap \mathfrak{B})$. Seja agora $\mathfrak{G}_0$ um subgrupo, para o qual é também $\mathfrak{G}_0 \supseteq \mathfrak{A}$. Vamos demonstrar que se tem $\mathfrak{G}_0 = \mathfrak{A} \times (\mathfrak{G}_0 \cap \mathfrak{B})$. Em primeiro lugar. os elementos de $\mathfrak{A}$ comutam com os elementos de $\mathfrak{G}_0 \cap \mathfrak{B}$. Em seguida, tomemos um elemento $g_0 \in \mathfrak{G}_0$; há dois elementos bem determinados $a \in \mathfrak{A}$, $b \in \mathfrak{B}$ tais que $g_0 = ab$, podendo afirmar-se que $b \in \mathfrak{G}_0$, em virtude de lhe pertencerem g_0 e a. Isto significa $b \in \mathfrak{G}_0 \cap \mathfrak{B}$. Então, $\mathfrak{G}_0$ tem, na verdade, a forma indicada de produto directo.

4) **Os grupos completamente redutíveis** – Um grupo $\mathfrak{G}$ diz-se *completamente redutível*, se é produto directo de grupos simples. É válido este

Teorema 1: *Se $\mathfrak{G}$ é completamente redutível, um divisor normal $\mathfrak{H}$ é sempre factor directo dum produto directo igual a $\mathfrak{G}$.* Escrevamos $\mathfrak{G} = \mathfrak{G}_1 \times \cdots \times \mathfrak{G}_n$, em que os $\mathfrak{G}_i$ são simples. Sem dúvida que se tem $\mathfrak{H} \cdot \mathfrak{G} = \mathfrak{G} = \mathfrak{H}\mathfrak{G}_1 \cdots \mathfrak{G}_n$. Então, $\mathfrak{H}\mathfrak{G}_1$ ou é um produto directo ou é igual a $\mathfrak{H}$. Neste último caso, o factor $\mathfrak{G}_1$ torna-se desnecessário no produto. Em seguida, os produtos $\mathfrak{H}\mathfrak{G}_2$ ou $(\mathfrak{H} \times \mathfrak{G}_1) \cdot \mathfrak{G}_2$ são tais

que, ou deve eliminar-se o factor $\mathfrak{G}_2$ ou substituir o sinal $\cdot$ que o precede pelo sinal de produto directo. O processo continua até se demonstrar a afirmação. Podemos precisar e dizer: é sempre $\mathfrak{G} = \mathfrak{H} \times \mathfrak{G}_{j_1} \times \cdots \times \mathfrak{G}_{j_k}$, onde $j_1, \cdots, j_k$ são alguns dos índices $1, 2, \cdots, n$.

Uma consequência interessante do teorema anterior, que assenta ainda no 2.º teorema do isomorfismo, é esta:

Corolário: *Uma imagem homomorfa dum grupo completamente redutível é imagem isomorfa do produto directo dum certo número dos factores simples da decomposição do grupo dado.*

É conveniente observar que pode haver outros invariantes $\mathfrak{H}'$ por forma que se tenha $\mathfrak{G} = \mathfrak{H} \times \mathfrak{G}_{j_1} \times \cdots \times \mathfrak{G}_{j_k} = \mathfrak{H}' \times \mathfrak{G}_{j_1} \times \cdots \times \mathfrak{G}_{j_k}$. Apenas se pode afirmar que tais invariantes são isomorfos de $\mathfrak{H}$.

§ 4. O teorema de Krull-Schmidt

1) **Sobre as aplicações dum grupo em si próprio** - O conceito geral de aplicação foi dado em (I, 1, 3). Neste momento, vamos estudar, em especial, as aplicações dum grupo $\mathfrak{G}$ em si mesmo. Elas formam um conjunto $\mathfrak{a}(\mathfrak{G}) = |A, B, C \cdots|$. Em $\mathfrak{a}(\mathfrak{G})$, definiremos uma *soma* $A + B$, escrevendo

$$x(A + B) = xA \cdot xB,$$

e definiremos um *produto* $A \cdot B = AB$, pondo

$$x(AB) = (xA)B.$$

Vê-se imediatamente que se tem este

Teorema 1: *O conjunto $\mathfrak{a}(\mathfrak{G})$ é grupo relativamente à soma.* De facto: 1) $A + B \in \mathfrak{a}(\mathfrak{G})$; 2) existe elemento um, que representaremos 0 (zero), o qual é a aplicação que a todo o elemento $x \in \mathfrak{G}$ faz corresponder $u \in \mathfrak{G} : x0 = u$; 3) existe aplicação simétrica $-A$, de cada aplicação A, como se reconhece pondo $x(-A) = (xA)^{-1}$; 4) é válida a propriedade associativa: $(A + B) + C = A + (B + C)$. E também se tem:

TEOREMA 2: *O conjunto* $\mathcal{A}(\mathfrak{G})$ *é semi-grupo com identidade relativamente à operação de produto.* De facto: 1') $AB \in \mathcal{A}(\mathfrak{G})$; 2') é válida a propriedade associativa: $(AB)C = A(BC)$; 3') existe elemento um, que é a transformação identidade.

Nas relações que envolvem soma e produto, tem lugar a igualdade

$$A(B+C) = AB + AC,$$

que se demonstra do modo seguinte: é $x[A(B+C)] = xA \cdot (B+C) = xAB \cdot xAC = x(AB + AC)$.

Observe-se que é, em geral, $A+B \neq B+A$, pois que $x(A+B) = xA \cdot xB \neq xB \cdot xA = x(B+A)$. Também não é válida, em geral, a igualdade $(B+C)A = BA+CA$, visto que $x(B+C)A = (xB \cdot xC)A$ e nós não definimos ainda o que se entende por aplicação de A a um produto de dois elementos.

Restrinjamo-nos, porém, dentro de $\mathcal{A}(\mathfrak{G})$, ao subconjunto, $\mathcal{E}(\mathfrak{G})$, dos endomorfismos de $\mathfrak{G}$, definidos, como sabemos, por meio de igualdades da forma

$$(xy)A = xA \cdot yA.$$

Fàcilmente se verifica que este conjunto $\mathcal{E}(\mathfrak{G})$ é fechado relativamente ao produto. Então, já é válida a igualdade

$$(B+C)A = BA + CA,$$

se se supuser $A \in \mathcal{E}(\mathfrak{G})$.

Finalmente, admitindo que $\mathfrak{G}$ é um grupo abeliano, reconhece-se que $\mathcal{E}(\mathfrak{G})$ é fechado para a soma e para o produto e que $A+B = B+A$. Daremos este enunciado:

TEOREMA 3: *No conjunto* $\mathcal{A}(\mathfrak{G})$, *é válida a igualdade* $A(B+C) = AB + AC$. *E, representando por* $\mathcal{E}(\mathfrak{G}) \subseteq \mathcal{A}(\mathfrak{G})$ *o conjunto dos endomorfismos de* $\mathfrak{G}$, *é* $(B+C)A = BA + CA$, *se* $A \in \mathcal{E}(\mathfrak{G})$. *O conjunto* $\mathcal{E}(\mathfrak{G})$, *suposto* $\mathfrak{G}$ *um grupo comutativo, é fechado para a soma e para o produto, valendo* $A + B = B + A$.

2) **Projecções** – Regressemos ao produto directo $\mathfrak{P} = \mathfrak{P}_1 \times \cdots \times \mathfrak{P}_n$. Ao escrevermos $a = a_1 \cdots a_n$, definem-se correspondências $a \to a_i$, que são endomorfismos – Ω normais do grupo, como vamos verificar, limitando-nos, porém, à «normalidade». Representando por $E_i, (i = 1, 2, \cdots, n)$, esses endomorfismos, tem-se $a_i = aE_i$. Trata-se de provar a igualdade

$$b(aE_i)b^{-1} = (bab^{-1})E_i, \qquad (b \in \mathfrak{P}).$$

Ora é, sucessivamente:

$$b(aE_i)b^{-1} = baib^{-1} = (b_1 \cdots b_n)a_i(b_n^{-1} \cdots b_1^{-1}) = (b_1 \cdots b_i)a_i(b_i^{-1} \cdots b_1^{-1}) =$$
$$= (b_1 \cdots b_{i-1})(b_i a_i b_i^{-1})(b_{i-1}^{-1} \cdots b_1) = b_i a_i b_i^{-1} = (bE_i)(aE_i)(bE_i)^{-1} = (bab^{-1})E_i.$$

Os endomorfismos E_i satisfazem às igualdades

$$E_i^2 = E_i E_i = E_i, \qquad E_i E_j = 0, \text{ se } i \neq j.$$

Aqui, podemos designar 0 por *endomorfismo nulo*. Um exemplo de endomorfismo nulo encontrámos já no endomorfismo normal φ^k do teorema 2, de (IV, 3, 3), quando aplicado a $\mathfrak{N}_{\varphi^k}$. Diz-se, por esse facto, que φ é *nilpotente* em $\mathfrak{N}_{\varphi^k}$. A igualdade $E_i^2 = E_i$ leva a designar E_i por *idempotente*.

Outras propriedades podem ser constatadas para os E_i. Assim:

- I_e) $1 = E_1 + \cdots + E_n$, onde 1 é o endomorfismo identidade (transformação identidade);
- II_e) $E_i + E_j = E_j + E_i$, se $i \neq j$;
- III_e) $E_{i_1} + \cdots + E_{i_h}$ é endomorfismo normal, se os i_k forem distintos;
- IV_e) $\mathfrak{P}_i = \mathfrak{P}E_i$.

Um endomorfismo normal idempotente diz-se uma *projecção*. Os E_i são projecções. As igualdades $E_i E_j = 0$ levam a dizer que cada E_i é *ortogonal* a $E_j, (i \neq j)$.

Imaginemos agora, em situação recíproca, que são dados n endomorfismos normais idempotentes e ortogonais $E_i, (i = 1, 2, \cdots, n)$, verificando as condições I_e), II_e) e III_e). Fàcilmente se vê que, pondo $\mathfrak{P}E_i = \mathfrak{P}_i$, é $\mathfrak{P} = \mathfrak{P}_1 \times \cdots \times \mathfrak{P}_n$. De facto, utilizaremos o teorema demonstrado em (IV, 3, 2), começando por ver que os $\mathfrak{P}_i$ são invariantes. Tem-se, pois que os E_i são normais,

$$b(aE_i)b^{-1} = (bab^{-1})E_i \in \mathfrak{P}_i,$$

como, aliás, tinhamos observado já em (IV, 2, 3).

Relativamente às propriedades I) e II), citadas no referido teorema, como se tem $a = a(E_1 + \cdots + E_n) = a E_1 \cdots a E_n = a_1 \cdots a_n$, $(a_i \in \mathfrak{P}_i)$, constata-se que 1) é válida; por outro lado, supondo $z E_i = z_2 E_2 \cdots z_{i-1} E_{i-1} z_{i+1} E_{i+1} \cdots z_n E_n$, $(z, z_j \in \mathfrak{P}; j = 1, 2, \cdots, i-1, i+1, \cdots, n)$, vê-se que, aplicando E_i a ambos os membros, se conclui $z E_i = u$. A afirmação de que $\mathfrak{P}$ é o produto directo indicado está justificada.

3) **Projecções primitivas. Grupos indecomponíveis** — Uma projecção E diz-se *primitiva*, se não pode decompor-se numa soma de duas projecções ortogonais, isto é, se não pode ter-se $E = E' + E''$, $E' E'' = E'' E' = 0$, salvo se alguma parcela for nula.

Um grupo $\mathfrak{P}$ diz-se *indecomponível*, se não puder escrever-se sob a forma de produto directo, salvo se um dos factores é o grupo unidade. De contrário, diz-se *decomponível*. Vê-se imediatamente que tem lugar este

TEOREMA 1: *É condição necessária e suficiente, para que $\mathfrak{P}$ seja um grupo indecomponível, que o endomorfismo identidade seja uma projecção primitiva.* Tendo em conta o teorema de FITTING, também se vê que é válido o

TEOREMA 2: *Se, num grupo indecomponível, são válidas as duas condições de cadeia, todo o endomorfismo normal é nilpotente, se não for um automorfismo.* Na verdade, escrevendo $\mathfrak{P} = (\mathfrak{P}_{\varphi^k}) \times \mathfrak{N}_{\varphi^k}$, o facto de poder existir apenas um factor leva a $\mathfrak{P}_{\varphi^k} = |u|$, se não for $\mathfrak{N}_{\varphi^k} = |u|$, esta última igualdade implicando $\mathfrak{N}_\varphi = |u|$.

São de interesse as proposições a que vamos agora referir-nos.

TEOREMA 3: *Se o grupo $\mathfrak{P}$ verifica a condição de cadeia descendente, pode escrever-se como produto directo de grupos indecomponíveis.* Suposto $\mathfrak{P}$ indecomponível, o teorema é trivial. Se $\mathfrak{P}$ pode tomar a forma $\mathfrak{P} = \mathfrak{P}_1 \times \mathfrak{P}_2$, com $\mathfrak{P} \supset \mathfrak{P}_1$, pode acontecer que $\mathfrak{P}_1$ seja indecomponível. Será, então, um primeiro factor directo. Não acontecendo assim, pode escrever-se $\mathfrak{P}_1 = \mathfrak{P}'_1 \times \mathfrak{P}''_1$ e $\mathfrak{P}_1 = \mathfrak{P}'_1 \times \mathfrak{P}''_1 \times \mathfrak{P}_2$, ao mesmo tempo que $\mathfrak{P} \supset \mathfrak{P}_1 \supset \mathfrak{P}'_1$. A condição de cadeia descendente limita a cadeia $\mathfrak{P} \supset \mathfrak{P}_1 \supset \mathfrak{P}'_1 \supset \cdots$, pelo que chegamos a encontrar um primeiro factor indecomponível, a figurar na expressão de $\mathfrak{P}$. Representando esse factor novamente por $\mathfrak{P}_1$ e pondo $\mathfrak{P} = \mathfrak{P}_1 \times \mathfrak{P}'_2$,

sabemos que $\mathfrak{P}'_2$ também verifica a condição descendente, tendo-se $\mathfrak{P}'_2 = \mathfrak{P}_2 \times \mathfrak{P}'_3$, em que $\mathfrak{P}_2$ é indecomponível. Chegamos a $\mathfrak{P} = \mathfrak{P}_1 \times \mathfrak{P}_2 \times \mathfrak{P}'_3$. O facto de ser $\mathfrak{P} \supset \mathfrak{P}'_2 \supset \mathfrak{P}'_3 \supset \cdots$ limita o processo e o teorema está demonstrado.

TEOREMA 4: *Se $\mathfrak{P}$ é um grupo indecomponível no qual valem as duas condições de cadeia, então, supostos φ e ψ dois endomorfismos normais tais que $\varphi + \psi = 1$, um deles é um automorfismo.* Visto que $\varphi + \psi = 1$, temos

$$(\varphi + \psi)\varphi = \varphi^2 + \psi\varphi = \varphi, \qquad \varphi(\varphi + \psi) = \varphi^2 + \varphi\psi = \varphi,$$

pelo que $\psi\varphi = \varphi\psi$. Os dois endomorfismos comutam. À face dessa comutabilidade, podemos dar o desenvolvimento seguinte:

$$(\varphi + \psi)^m = \sum \varphi^r \psi^s, \text{ com } r + s = m.$$

Em virtude do teorema 2, se φ e ψ não são automorfismos, são ambos nilpotentes. Podemos, então, imaginar m suficientemente grande, para que cada parcela $\varphi^r \psi^s$ seja o endomorfismo nulo. Daí resulta $(\varphi + \psi)^m = 1 = 0$, o que é um absurdo. Assim, um dos endomorfismos φ ou ψ é um automorfismo.

4) **O teorema fundamental** — Tomemos um grupo $\mathfrak{P} = \mathfrak{G}$, para o qual sejam válidas as duas condições de cadeia e suponhamos que têm lugar as duas decomposições seguintes, em grupos indecomponíveis:

$$(1) \qquad \mathfrak{P} = \mathfrak{P}_1 \times \mathfrak{P}_2 \times \cdots \times \mathfrak{P}_n, \qquad \mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_m.$$

As projecções relativas à 1.ª decomposição serão representadas por $E_i, (i = 1, 2, \cdots, n)$, e as que são relativas à segunda serão designadas por $F_j, (j = 1, 2, \cdots, m)$. Em virtude de se ter $(F_1 + F_2 + \cdots + F_m) E_1 = F_1 E_1 + \cdots + F_m E_1 = E_1$ e de E_1 ser o endomorfismo unidade de $\mathfrak{P}_1$ e de cada um dos $F_j E_1$ ser um endomorfismo normal de $\mathfrak{P}_1$, o teorema 4 do número anterior afirma-nos que, não sendo $F_1 E_1$ um automorfismo de $\mathfrak{P}_1$, é $F_2 E_1 + \cdots + F_m E_1 = \varphi$ um automorfismo de $\mathfrak{P}_1$. Nessas condições, tendo-se $F_2 E_1 \varphi^{-1} + \cdots + F_m E_1 \varphi^{-1} = E_1$, se não for $F_2 E_1 \varphi^{-1}$ um automorfismo de $\mathfrak{P}_1$, sê-lo-á $F_3 E_1 \varphi^{-1} + \cdots + F_m E_1 \varphi^{-1} = \psi$. Agora, do mesmo modo, ou $F_3 E_1 \varphi^{-1} \psi^{-1}$ é um automorfismo de $\mathfrak{P}_1$, ou, de contrário, isso acontece com $F_4 E_1 \varphi^{-1} \psi^{-1} + \cdots + F_m E_1 \varphi^{-1} \psi^{-1}$. Continuando o processo, chegamos

a estabelecer que uma expressão do tipo $F_j E_1 \varphi^{-1}\psi^{-1}\cdots\eta^{-1}$ é um automorfismo de $\mathfrak{P}_1$. Por consequência:

TEOREMA 1: *Num grupo em que são válidas as duas condições de cadeia, se forem dadas as duas decomposições* (1) *em grupos indecomponíveis, então, representando as respectivas projecções por* $E_i, (i = 1, 2, \cdots, n)$, *e por* $F_j, (j = 1, 2, \cdots, m)$, *podemos afirmar que há um produto* $F_j E_1$ *que é um automorfismo de* $\mathfrak{P}_1$.

Visto que nos produtos directos podemos alterar a ordem dos factores, admitiremos que $F_1 E_1$ é um automorfismo de $\mathfrak{P}_1$. Nessas condições, $\mathfrak{P}_1 \sim \mathfrak{P}_1 F_1$ é um isomorfismo, tendo-se $\mathfrak{P}_1 \simeq \mathfrak{P}_1 F_1 = \mathfrak{G}_1$, assim como $\mathfrak{G}_1 \simeq \mathfrak{G}_1 E_1 = \mathfrak{P}_1$. De facto, se $\mathfrak{P}_1 \sim \mathfrak{P}_1 F_1$ não fosse um isomorfismo, existiriam dois elementos $p_1, p'_1 \in \mathfrak{P}_1$ para os quais $p_1 F_1 = p'_1 F_1$. Daí resultaria $p_1 F_1 E_1 = p'_1 F_1 E_1$, consequentemente, pois que $F_1 E_1$ é automorfismo, $p_1 = p'_1$. Para se chegar à igualdade $\mathfrak{G}_1 = \mathfrak{P}_1 F_1$, designemos por $\mathfrak{g}_1$ o núcleo do homomorfismo $\mathfrak{G}_1 \sim \mathfrak{G}_1 E_1$. Para cada $x \in \mathfrak{g}_1$ é $x E_1 = u$. Tomado $y \in \mathfrak{G}_1$, é $y E_1 \in \mathfrak{P}_1$, mas como $\mathfrak{P}_1 F_1 E_1 = \mathfrak{P}_1$, todo o elemento $t \in \mathfrak{P}_1$, em particular $y E_1$, tem a forma $z F_1 E_1$, o que leva a $y E_1 = z F_1 E_1$, com $z \in \mathfrak{P}_1$. Escrevendo agora $y = y(zF_1)^{-1}(zF_1)$, em virtude de ser $[y(z^{-1}F_1)]E_1 = yE_1 \cdot z^{-1}F_1 E_1 = yE_1 \cdot (zF_1E_1)^{-1} = u$, concluímos que é $y(z^{-1}F_1) = y(zF_1)^{-1} \in \mathfrak{g}_1$, e que, portanto, é válida a igualdade $\mathfrak{G}_1 = \mathfrak{g}_1 \cdot \mathfrak{P}_1 F_1$. Vamos reconhecer que este produto é directo. Um elemento $x \in \mathfrak{g}_1 \cap \mathfrak{P}_1 F_1$ leva, por um lado, a $xE_1 = u$, por outro a $xE_1 = (p_1F_1)E_1 = p_1F_1E_1 = u$, com $x = p_1F_1, p_1 \in \mathfrak{P}_1$. Obtem-se, pois, $p_1 = u, x = u$. A afirmação fica justificada. Mas, sendo $\mathfrak{G}_1 = \mathfrak{g}_1 \times \mathfrak{P}_1 F_1$ um grupo indecomponível, ou será $\mathfrak{G}_1 = \mathfrak{g}_1$, ou $\mathfrak{G}_1 = \mathfrak{P}_1 F_1$. [1] Se valesse a 1.ª igualdade, viria, para cada $g_1 \in \mathfrak{G}_1, g_1 E_1 = g_1 F_1 E_1 = u$, o que, ainda pela circunstância de F_1E_1 ser automorfismo, implicaria $g_1 = u$, $\mathfrak{G}_1 = \{u\}$. Valerá, pois, a relação $\mathfrak{G}_1 = \mathfrak{P}_1 F_1$, consequentemente será também $\mathfrak{G}_1 E_1 = \mathfrak{P}_1 F_1 E_1 = \mathfrak{P}_1$. Em resumo:

TEOREMA 2: *Nas condições do teorema* 1, *suposto que as decomposições são tais que, para os primeiros factores das referidas decomposições,* $F_1 E_1$ *um automorfismo de* $\mathfrak{P}_1$, *podemos afirmar:* 1) *que* F_1 *é um isomorfismo, tendo-se* $\mathfrak{P}_1 \simeq \mathfrak{P}_1 F_1 = \mathfrak{G}_1$; 2) *que* E_1 *é um isomorfismo, tendo-se* $\mathfrak{G}_1 \simeq \mathfrak{G}_1 E_1 = \mathfrak{P}_1$.

Para continuarmos, estabeleceremos seguidamente este

LEMA: *Tomado o produto directo* $\mathfrak{G} = \mathfrak{G}_1 \times \cdots \times \mathfrak{G}_m$ *e suposto* $\mathfrak{G}'$ *um invariante de* $\mathfrak{G}$ *tal que* $\mathfrak{G}' = \mathfrak{G}'_1 \times \cdots \times \mathfrak{G}'_m$, *onde* $\mathfrak{G}'_i = \mathfrak{G}_i A_i$ *é imagem homomorfa definida pelo endomorfismo normal* A_i, *de* $\mathfrak{G}$ $(i = 1, 2, \cdots, m)$, *então* $F_1 A_1 + \cdots + F_m A_m$ *é um endomorfismo normal de* $\mathfrak{G}$. [1] De facto, $F_1 A_1$, por exemplo, dá, para $x, y \in \mathfrak{G}$, $xF_1A_1 = (xF_1)A_1 \in \mathfrak{G}'_1$; $(xy)F_1A_1 = (xF_1 \cdot yF_1)A_1 = xF_1A_1 \cdot yF_1A_1 \in \mathfrak{G}'_1$, o que mostra ser F_1A_1 um endomorfismo de $\mathfrak{G}$. Então, $F_1A_1 + \cdots + F_mA_m$ é tambem um endomorfismo de $\mathfrak{G}$ para $\mathfrak{G}'$, [2] Restaver que é normal. Ora, supostos $a, x \in \mathfrak{G}$, $a = a_1 a_2 \cdots a_m$, $x = x_1 x_2 \cdots x_m$, $(a_i, x_i \in \mathfrak{G}_i; i = 1, 2, \cdots m)$, tem-se, sucessivamente:

$$a[x(F_1A_1 + \cdots + F_mA_m)]a^{-1} = a(xF_1A_1 \cdots xF_mA_m)a^{-1} =$$

$$= a_1a_2\cdots a_m(xF_1A_1\cdots xF_mA_m)a_m^{-1}\cdots a_2^{-1} =$$

$$= a_1(x_1A_1)a_1^{-1}\cdots a_m(x_mA_m)a_m^{-1} = (a_1x_1a_1^{-1})A_1\cdots(a_mx_ma_m^{-1})A_m =$$

$$= (axa^{-1})F_1A_1\cdots(axa^{-1})F_mA_m = (axa^{-1})(F_1A_1 + \cdots + F_mA_m).$$

Este resultado demonstra o lema.

Regressemos à análise das duas decomposições (1), sobre as quais foram já demonstrados os teoremas (1) e (2), e estudemos o produto $\mathfrak{G}_1 \mathfrak{P}_2 \cdots \mathfrak{P}_n = \mathfrak{P}'$. Vê-se que, se for $x \in \mathfrak{G}_1 \cap \mathfrak{P}_2 \cdots \mathfrak{P}_n$, é $x = g_1 = p_2 \cdots p_n$, $(g_1 \in \mathfrak{G}_1, p_i \in \mathfrak{P}_i)$. Por aplicação de E_1, tem-se $xE_1 = g_1E_1 = u$. Sendo E_1, porém, um isomorfismo que leva de $\mathfrak{G}_1$ a $\mathfrak{P}_1$, é $g_1 = x = u$. Nestas condições, é $\mathfrak{P}' = \mathfrak{G}_1 \times \mathfrak{P}_2 \times \cdots \times \mathfrak{P}_n$ um produto directo, à face do teorema provado em (IV, 3, 2) e da primeira observação feita em (IV, 3, 3). O lema mostra, em seguida, que $H_1 = E_1F_1 + E_2E_2 + \cdots + E_nE_n = E_1F_1 + E_2 + \cdots + E_n$ é um endomorfismo normal de $\mathfrak{G}$. Procuremos o núcleo. Se $zH_1 = u$, $(z \in \mathfrak{G})$, vê-se que, com $z = z_1 z_2 \cdots z_n$, $(z_i \in \mathfrak{P}_i)$, é $zH_1 = z_1H_1 \cdot z_2H_1 \cdots z_nH_1 = z_1F_1 \cdot z_2 \cdots z_n = u$. O facto já reconhecido, de ser $\mathfrak{P}'$ um produto directo, leva agora a $z_1F_1 = u$, $z_2 = \cdots = z_n = u$; depois, por ser F_1 um isomorfismo de $\mathfrak{P}_1$ para $\mathfrak{G}_1$, vê-se que $z_1 = u$. Assim, é $z = u$, o que leva a concluir-se que H_1 é um meromorfismo, portanto um automorfismo de $\mathfrak{G}$. Tem-se $\mathfrak{P}' = \mathfrak{P}$ e $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{P}_2 \times \cdots \times \mathfrak{P}_n$.

O resto da demonstração que pretendemos vai ser feito por um método de indução. Partamos da hipótese de que $\mathfrak{P}_1$ e $\mathfrak{G}_1$, $\mathfrak{P}_2$ e $\mathfrak{G}_2, \cdots$, $\mathfrak{P}_r$ e $\mathfrak{G}_r$ já se associaram por forma a serem realizadas as condições seguintes: 1) $E_1, E_2, \cdots, E_r$ são isomorfismos levando dos $\mathfrak{G}_i, (i = 1, 2, \cdots, r)$, aos $\mathfrak{P}_i$; 2) $F_1, F_2, \cdots, F_r$ são isomorfismos levando dos $\mathfrak{P}_i$ aos $\mathfrak{G}_i$; 3) $\mathfrak{G}$ tem a forma de produto directo

$\mathfrak{G} = \mathfrak{G}_1 \times \cdots \times \mathfrak{G}_r \times \mathfrak{P}_{r+1} \times \cdots \times \mathfrak{P}_n$; 4) $H_r = E_1 F_1 + \cdots + E_r F_r + E_{r+1} + \cdots + E_n$ é um automorfismo de $\mathfrak{G}$; então, vamos concluir que é possível encontrar um novo par $\{\mathfrak{P}_{r+1}, \mathfrak{G}_{r+1}\}$, o qual, junto aos r pares já indicados, leva a um conjunto de pares realizando as condições que se enunciam mudando r em $r+1$ nas 4 condições acima indicadas.

Para isso, consideremos o grupo diferença $\overline{\mathfrak{G}} = \mathfrak{P}/\Delta$, onde $\Delta = \mathfrak{G}_1 \times \cdots \times \mathfrak{G}_r$. Verificaremos que se tem

$$(2) \qquad \overline{\mathfrak{G}} = \overline{\mathfrak{P}}_{r+1} \times \cdots \times \overline{\mathfrak{P}}_n, \qquad \overline{\mathfrak{G}} = \overline{\mathfrak{G}}_{r+1} \times \cdots \times \overline{\mathfrak{G}}_m$$

onde, bem entendido,

$$\overline{\mathfrak{P}}_k = \mathfrak{P}_k \Delta/\Delta, \qquad \overline{\mathfrak{G}}_j = \mathfrak{G}_j \Delta/\Delta, \qquad \begin{cases} k = r+1, \cdots, n; \\ j = r+1, \cdots, m. \end{cases}$$

Analisemos o primeiro produto directo (2). Sem dúvida que $\overline{\mathfrak{G}} = \overline{\mathfrak{P}}_{r+1} \cdots \overline{\mathfrak{P}}_n$. Este produto é directo, porque, se for $\overline{p}_{r+1} \cdots \overline{p}_n = \overline{u}$ = elemento um de $\overline{\mathfrak{G}}$, com $\overline{p}_i \in \overline{\mathfrak{P}}_i$, $(i = r+1, \cdots, n)$, e se designarmos por $p_i \in \mathfrak{P}_i$ um elemento de correspondente $\overline{p}_i$ no homomorfismo $\mathfrak{G} \sim \overline{\mathfrak{G}}$, obtemos $p_{r+1} \cdots p_n = p_1 p_2 \cdots p_r$, $(p_l \in \mathfrak{P}_l; l = 1, 2, \cdots, r)$, ou seja $p_1 = \cdots = p_r = p_{r+1} = \cdots = p_n = u$, assim como $\overline{p}_{r+1} = \cdots = \overline{p}_n = \overline{u}$. O produto em questão é directo, efectivamente. Do raciocínio feito, transparecem claramente, de resto, os isomorfismos $\overline{\mathfrak{P}}_k \simeq \mathfrak{P}_k$, $\overline{\mathfrak{G}}_j \simeq \mathfrak{G}_j$. Nestas condições, os dois produtos directos (2) estão exactamente na situação dos dois produtos directos (1). Designaremos por $\overline{E}_k$ e $\overline{F}_j$ as projecções correspondentes.

Podemos afirmar que é possível encontrar um índice j tal que $\overline{F}_j$ e $\overline{E}_{r+1}$ têm as propriedades que vamos enunciar, supondo, entretanto, que se toma desde logo $j = r+1$: 1') $\overline{F}_{r+1} \overline{E}_{r+1}$ é um automorfismo de $\overline{\mathfrak{P}}_{r+1}$; 2') $\overline{F}_{r+1}$ é um isomorfismo, tendo-se $\overline{\mathfrak{P}}_{r+1} \simeq \overline{\mathfrak{P}}_{r+1} \overline{F}_{r+1} = \overline{\mathfrak{G}}_{r+1}$; 3') $\overline{E}_{r+1}$ é um isomorfismo, tendo-se $\overline{\mathfrak{G}}_{r+1} \simeq \overline{\mathfrak{G}}_{r+1} \overline{E}_{r+1} = \overline{\mathfrak{P}}_{r+1}$; 4') $\overline{H}_{r+1} = \overline{E}_{r+1} \overline{F}_{r+1} + \overline{E}_{r+2} + \cdots + \overline{E}_n$ é um automorfismo de $\overline{\mathfrak{G}}$; 5') $\overline{\mathfrak{G}}$ é um produto directo da forma

$$3) \qquad \overline{\mathfrak{G}} = \overline{\mathfrak{G}}_{r+1} \times \overline{\mathfrak{P}}_{r+2} \times \cdots \times \overline{\mathfrak{P}}_n.$$

É útil observar em seguida que, se, por via de $\overline{F}_{r+1}$, se passa de $\overline{p}_{r+1}$ para $\overline{g}_{r+1} \in \overline{\mathfrak{G}}_{r+1}$, então, por via de F_{r+1}, passa-se de $p_{r+1} \in \mathfrak{P}_{r+1}$ para $g_{r+1} \in \mathfrak{G}_{r+1}$, estes dois últimos elementos sendo os correspondentes daqueles nos isomorfismos já referidos. Na verdade, partamos de $\overline{p}_{r+1}$ e utilizemos o segundo produto directo (2), a fim de escrevermos $\overline{p}_{r+1} = \overline{g}_{r+1} \cdots \overline{g}_m$, $(\overline{g}_k \in \overline{\mathfrak{G}}_k)$. Passando ao grupo $\mathfrak{G}$, obtem-se $p_{r+1} = g_{r+1} \cdots g_m$, $(g_k \in \mathfrak{G}_k)$. Esta última igualdade traduz precisamente a afirmação feita de que $p_{r+1} F_{r+1} = g_{r+1}$.

Consideremos agora o produto (3), para provarmos que

$$(4) \qquad \mathfrak{G}_1 \times \cdots \times \mathfrak{G}_r \times \mathfrak{G}_{r+1} \times \mathfrak{P}_{r+2} \times \cdots \times \mathfrak{P}_n$$

é produto directo. A demonstração faz-se do modo a seguir. Tomemos $x \in \mathfrak{G}_1 \cdots \mathfrak{G}_{r+1} \cap \mathfrak{P}_{r+2} \cdots \mathfrak{P}_n$. Se $\overline{x} \in \overline{\mathfrak{G}}$ é o seu correspondente, tem-se $\overline{x} = x\Delta \in \overline{\mathfrak{G}}_{r+1} \cap \overline{\mathfrak{P}}_{r+2} \cdots \overline{\mathfrak{P}}_n = \overline{u} \in \overline{\mathfrak{G}}$. Assim, é $x = g_1 \cdots g_{r+1} = p_{r+2} \cdots p_n \in \Delta$, o que nos leva a $x = u$. Se pusermos $\Delta' = \mathfrak{G}_1 \times \cdots \times \mathfrak{G}_{r+1}$, $\Delta'' = \mathfrak{P}_{r+2} \times \cdots \times \mathfrak{P}_n$, o produto $\Delta' \times \Delta''$ é directo, o mesmo se dizendo do produto (4).

Voltemos a considerar o primeiro produto directo (1) e designemos por $\mathfrak{G}'$ o produto directo (4). Uma nova aplicação do lema mostra-nos que $H_{r+1} = E_1 F_1 + \cdots + E_r F_r + E_{r+1} F_{r+1} + E_{r+2} + \cdots + E_n$ é um endomorfismo normal de $\mathfrak{G}$. Para estabelecermos que se trata dum automorfismo, lembremo-nos de que o isomorfismo $\mathfrak{P}_{r+1} \simeq \mathfrak{P}_{r+1} F_{r+1} = \mathfrak{G}_{r+1}$ nos garante que, sempre que $p_{r+1} F_{r+1} = u$, se tem $p_{r+1} = u$. Então, seja $z \in \mathfrak{G}$ um elemento da forma $z = z_1 \cdots z_n$, $(z_i \in \mathfrak{P}_i)$, e suponhamos $z H_{r+1} = z_1 H_{r+1} \cdots z_n H_{r+1} = z_1 F_1 \cdots z_{r+1} F_{r+1} z_{r+2} \cdots z_n = u$. Tendo em conta (4), obtem-se $z_1 F_1 = u, \cdots, z_{r+1} F_{r+1} = u$, $z_{r+2} = \cdots = z_n = u$, consequentemente $z_1 = u, \cdots, z_{r+1} = u, z = u$. O endomorfismo H_{r+1} é meromorfismo, portanto automorfismo, o que nos leva a concluir que o produto (4) representa $\mathfrak{G}$.

Como resumo de todas as considerações que seguiram o lema, formularemos agora o teorema fundamental ou

TEOREMA DE KRULL-SCHMIDT: *Seja $\mathfrak{G}$ um grupo-Ω que verifica as duas condições de cadeia e suponhamos que têm lugar as duas decomposições* (1) *em grupos indecomponíveis. Podemos, então, afirmar:* 1) *que* $n = m$; 2) *que é possível dispor os $\mathfrak{G}_j$ por uma ordem tal que, para cada* $r = 1, 2, \cdots, n$, *é válida a igualdade* $\mathfrak{G} = \mathfrak{G}_1 \times \cdots \times \mathfrak{G}_r \times \mathfrak{P}_{r+1} \times \cdots \times \mathfrak{P}_n$; 3) *que os $\mathfrak{P}_i$ e os $\mathfrak{G}_i$ são, nesse caso, isomorfos-Ω*; 4) *que existem automorfismos-Ω, de $\mathfrak{G}$, da forma* $H_r = E_1 F_1 + \cdots + E_r F_r + E_{r+1} + \cdots + E_n$; 5) *que o automorfismo* $H = E_1 F_1 + \cdots + E_n F_n$ *é tal que* $\mathfrak{P}_1 H = \mathfrak{G}_1$.

BIBLIOGRAFIA

B. VAN DER WAERDEN, *Moderne Algebra*, erster Teil, Berlin, 1930.

A. COIMBRA AIRES DE MATOS, *Sobre sistemas de divisão direitos com unidade direita*, «Revista da Faculdade de Ciências de Lisboa», Vol. VII, 1958.

H. ZASSENHAUS, *Lehrbuch der Gruppentheorie*, Berlin, 1937.

N. JACOBSON, *The Theory of Rings*, New York, 1943.

A. ALMEIDA COSTA, *Elementos da Teoria dos Grupos*, Centro de Estudos Matemáticos, Porto, 1942.

A. G. KUROSH, *The Theory of Groups*, vol. 1, New York, 1955.

———, *The Theory of Groups*, vol. 2 New York, 1956.

N. JACOBSON, *Lectures in Abstract Algebra*, vol. 1, New York, 1951.

O. SCHMIDT, *Über unendliche Gruppen mit endlicher Kette* «Mathematische Zeitschrift», Band 29, 1929.

E. NOETHER, *Hyperkomplexe Grössen und Darstellugstheorie*, «Mathematische Zeitschrift», Band 30, 1929.

W. KRULL, *Über verallgemeinerte endliche Abelsche Gruppen*, «Mathematische Zeitschrift», Band 23, 1925.

CAPÍTULO V

Generalidades sobre anéis e ideais. Números racionais. Corpos ordenados. Números reais.

§1. Postulados dos anéis. Regras de cálculo

1) **Definição de anel** — Um *anel* é um sistema algébrico $\mathfrak{A} = (\mathfrak{C} / + \cdot)$ com duas operações binárias $+$ e $\cdot$, verificando as leis a seguir: 1) relativamente à operação $+$, o sistema $\mathfrak{A}$ é um grupo abeliano aditivo; 2) relativamente à operação $\cdot$, o sistema $\mathfrak{A}$ é um semi-grupo; 3) as duas operações satisfazem às leis distributivas $a \cdot (b + c) = a \cdot b + a \cdot c$; $(b + c) \cdot a = b \cdot a + c \cdot a$.

No que vai seguir-se o sinal $\cdot$ será geralmente suprimido. Dando um pouco mais de desenvolvimento à definição anterior, formularemos aqui, sob a forma que vai ver-se, o

SISTEMA DE POSTULADOS PARA ANÉIS: A_1) $\mathfrak{A}$ é *fechado* relativamente à operação $+$ (soma), isto é, deduz-se um elemento de $\mathfrak{A}$ por via da operação: $a + b = c \in \mathfrak{A}$; A_2) é válida a *lei associativa*: $(a + b) + c = a + (b + c)$; A_3) é válida a *lei comutativa*: $a + b = b + a$; A_4) a equação $a + x = b$ é solúvel em $\mathfrak{A}$; A_5) $\mathfrak{A}$ é *fechado* relativamente ao produto; A_6) é válida a *lei associativa* $ab \cdot c = a \cdot bc$; A_7) é válida a *lei distributiva esquerda*: $a(b + c) = ab + ac$; A_8) é válida a *lei distributiva direita*: $(b + c)a = ba + ca$.

O grupo abeliano relativo à soma recebe o nome de *grupo aditivo do anel*; o semi-grupo relativo ao produto designa-se por *semi-grupo multiplicativo do anel.*

No anel $\mathfrak{A}$, tomado como simples módulo, cada inteiro n determina um endomorfismo $a \to na$, o número inteiro 1 define o endomorfismo identidade; e o inteiro zero define o *endomorfismo nulo*, isto é, o endomorfismo que aplica todos os elementós de $\mathfrak{A}$ no único elemento zero.

Pode acontecer, porém, que haja inteiros não nulos que determinem em $\mathfrak{A}$ o endomorfismo nulo. Se m e n estão nessas condições, também o estão $m-n$ e mn. O primeiro facto garante que o conjunto de tais inteiros constitui um submódulo do módulo $\mathfrak{J}$ dos inteiros, pelo que será gerado por um inteiro $q > 0$. Este número q diz-se *característica* do anel. Representa a ordem máxima[1] dos elementos do grupo aditivo do anel. Quando apenas o número zero anular todos os elementos do anel, há elementos cuja ordem é superior a todo o número inteiro dado. Neste caso, tanto se diz que o anel tem *característica zero* como que tem *característica infinita.*

Os inteiros dão um exemplo de anel. E os raciocínios desenvolvidos em (IV, 4, 1), que levaram ao teorema 3, também aí consignado, podem resumir-se na proposição seguinte:

TEOREMA 1: *O conjunto* $\mathfrak{F}(\mathfrak{M})$, *dos endomorfismos dum grupo abeliano* $\mathfrak{M}$, *forma um anel.*

No Capítulo II, estudámos já as consequências que resultam de ser $\mathfrak{A}$ um grupo abeliano aditivo. As propriedades associativas também foram analisadas no mesmo Capítulo. As consequências dos postulados que vamos agora considerar lidam com as propriedades distributivas. Fácil é de concluir, por indução, que se tem

$$a(b_1 + \cdots + b_n) = ab_1 + \cdots + ab_n; \quad (b_1 + \cdots + b_n)a = b_1a + \cdots + b_na.$$

Da combinação das duas leis distributivas e do facto de $\mathfrak{A}$ ser um grupo abeliano aditivo, resulta a igualdade

$$(a_1 + \cdots + a_n) \cdot (b_1 + \cdots + b_m) = \sum_{i,k} a_i b_k,$$

onde o índice i varia de 1 a n e o índice k de 1 a m.

Efectuemos a operação que se indica com $a(b + (-c)) = a(b-c)$. Se pusermos $b - c = d$, é $b = c + d$ e tem-se $a(b-c) = ad$. Trata-se de demonstrar que é $ad = ab - ac$. Ora isto é imediato, visto que $ad + ac = a(c+d) = ab$. Assim, é válida a igualdade $a(b-c) = ab - ac$. No caso particular de ser $c = b$, vem $a(b-b) = ab - ab = 0$, pelo que $a \cdot 0 = 0$. Daqui este

TEOREMA 2: *O produto dum elemento qualquer pelo elemento zero (ou deste por um elemento qualquer) leva ao elemento zero.*

Este teorema sugere imediatamente que se indague àcerca da sua inversão. Consideremos, por exemplo, um conjunto de elementos da forma (a, b), onde a e b são números inteiros, e definamos, nesse conjunto, as operações de soma e de produto segundo as regras.

$$(a, b) + (c, d) = (a + c,\ b + d),$$
$$(a, b) \cdot (c, d) = (ac,\ bd).$$

O conjunto em questão é um anel, cujo elemento zero é $(0, 0)$. Ora, se considerarmos o produto $(a, 0) \cdot (0, b) = (0, 0)$, vê-se que se obtem o elemento zero por um produto de dois elementos, nenhum dos quais é zero. A inversa do teorema 1 não é verdadeira.

Dado, em $\mathfrak{A}$, um elemento $a \neq 0$, se $b \neq 0$ é tal que $ab = 0$, diz-se que b é um *divisor de zero à direita* e a um *divisor de zero à esquerda.* Podemos incluir o elemento zero nos divisores de zero, dizendo: se $a \neq 0$ e b for tal que $ab = 0$, b é um divisor de zero à direita; se $a \neq 0$ e b for tal que $ba = 0$, b é um divisor de zero à esquerda.

Um anel para o qual se tenha: $A_{8'})$ $ab = ba$ diz-se *comutativo.*

Consideraremos como compatíveis os diferentes postulados dos anéis (comutativos ou não), pelo facto de eles terem lugar no anel dos inteiros.

2) **Anéis de divisão. Corpos. Domínios de integridade** — Chama-se *anel de divisão* ou *corpo-s*, todo o anel no qual é ainda válido este novo sistema de axiomas: $A_9)$ existe elemento diferente do elemento zero; $A_{10})$ as equações $xa = b$, $ay = b$, quando $a \neq 0$, são solúveis no anel, qualquer que seja b.

A restrição introduzida com $a \neq 0$ no último postulado é exigida pela compatibilidade de $A_9)$ com $A_{10})$. Se pudesse ser $a = 0$, então

a solução de $xa = b$, com b qualquer, levaria a $xa = b = 0$, pelo que não haveria elemento $\neq 0$.

Um anel de divisão diz-se um *corpo* (DEDEKIND), se tiver ainda lugar $A_{10'}$) $ab = ba$. A designação de *domínio de racionalidade*, introduzida por KRONECKER com o significado de corpo, não é hoje usada.

Um *domínio de integridade* é um anel em que são válidos ainda os axiomas a seguir: $A_{9''}$) existe elemento diferente do elemento zero; $A_{10''}$) $ab = ba$; $A_{11''}$) se a equação $ax = b$, com $a \neq 0$, é solúvel, a solução é única.

Hoje também se consideram *domínios de integridade não comutativos*, assim definidos: são anéis para os quais se verificam mais êstes axiomas: $A_{9'''}$) existe elemento diferente do elemento zero; $A_{10'''}$) se as equações $xa = b$ e $ay = b$, com $a \neq 0$ são solúveis, as respectivas soluções são únicas.

Estudemos algumas propriedades dos anéis de divisão. Em primeiro lugar, existe *elemento um* $= u$. Como em (II, 1, 5), pode provar-se essa existência do modo a seguir. Tomemos a equação $ay = a$, $(a \neq 0)$, e designemos por u' uma solução. Será necessàriamente $u' \neq 0$. Se, agora, $xa = c$ for uma equação cuja solução é x, temos $(xa)u' = cu' = x(au') = xa = c$. A relação $cu' = c$, por ser c arbitrário, mostra que u' é unidade direita. O estudo da equação $xa = a$ levaria anàlogamente à existência de unidade esquerda u''. Então, de $u''u' = u'' = u'$, resulta a existência da identidade $u = u' = u''$, pois que, na verdade, é também $o \cdot u = u \cdot o = o$.

Prova-se agora que cada elemento $a \neq o$ tem inverso a^{-1}. Pondo $ay = u$, a solução α desta equação é, de facto, um inverso direito de a. Mas, como é $\alpha \neq o$, designemos por α' o seu inverso direito: $\alpha\alpha' = u$. Tem-se $a\alpha = u$, $aa\alpha = a$, $aa\alpha\alpha' = a\alpha' = aa = u$, o que mostra ser α inverso esquerdo de a: $\alpha = a^{-1}$.

Pode concluir-se daqui que um anel de divisão não tem divisores de zero. De facto, se $ab = 0$, tem-se, se $a \neq 0$, $a^{-1}ab = b = 0$. Portanto:

TEOREMA 1: *Num anel de divisão existe identidade, todo o elemento* $a \neq 0$ *tem inverso e não há divisores de zero, salvo zero.*

COROLÁRIO: *Pondo de parte o elemento zero dum anel de divisão, os restantes elementos formam um grupo relativamente ao produto. A inversa é verdadeira.* Efectivamente, os elementos considerados (não nulos) verificam o 4.º sistema de axiomas indicado em (II, 1, 5). Quanto à inversa, observemos que, da hipótese de os elementos não nulos formarem grupo com respeito ao produto, resultam imediatamente os axiomas A_9) e A_{10}). Em particular, o elemento nulo (zero) é solução das equações $xa = 0$ e $ay = 0$, se $a \neq 0$.

Também no caso dos domínios de integridade não há divisores de zero, além de zero. Se $ab = 0$, com $a \neq 0$, como é $a \cdot 0 = 0$, segue-se $b = 0$. O conjunto dos elementos não nulos forma um subsemi-grupo do semi-grupo multiplicativo do domínio de integridade. O teorema 1, de (II, 1, 5), é aplicável e a *lei do corte* é válida, se o elemento «cortado» for $\neq 0$.

Inversamente, um anel em que seja válida a lei do corte para os elementos não nulos é um domínio de integridade, não possuindo divisores de zero. Na verdade, se $a \neq 0$, a equação $ay = b$, por exemplo, só pode ter uma solução, pois $ay = ay' = b$ implica $y = y'$. É válido este

TEOREMA 2: *É condição necessária e suficiente, para que um anel* $\mathfrak{A}$ *(comutativo ou não), com elementos diferentes de zero, seja um domínio de integridade, que não existam divisores de zero, salvo zero.*

Os números inteiros constituem um domínio de integridade comutativo. Achamos interessante indicar também aqui como pode construir-se um corpo com quatro elementos: $0, u, a, b$. Para isso, comecemos por mostrar que é $-u = u$. Se fosse $-u \neq u$, as duas hipóteses possíveis $-u \neq 2u$, $-u = 2u$ conduziriam a absurdo, como vamos constatar. Estudemos a primeira. Fàcilmente se conclui que os elementos $0, u, -u, 2u$ são distintos. Nessas circunstâncias, a tabela do grupo multiplicativo (com $a = -u$, $b = 2u$) dará

	u	a	b
u	u	a	b
a	a	b	u
b	b	u	a

,

donde se tira, por exemplo, $2u \cdot (-u) = (u+u) \cdot (-u) = (-u) + (-u) = -2u = u$, que é falso, por hipótese. Quanto ao outro caso, $-u = 2u$, sempre sob a condição de *existir* o corpo de 4 elementos,

ter-se ão, para elementos do corpo, os seguintes: $0, u, 2u, a$. O elemento $a+u$ não pode, porém, ser igual a qualquer dos 4 elementos: $a+u=0$, daria $a=-u=2u$; $a+u=u$, daria $a=0$; $a+u=2u$, levaria a $a=u$; e, de $a+u=a$, concluiríamos $u=0$. Será, pois, necessàriamente, $-u=u$, $2u=0$. Então, $2a=2b=0$ e a tabela da soma toma o aspecto

	0	u	a	b
0	0	u	a	b
u	u	0	b	a
a	a	b	0	u
b	b	a	u	0

Construídas as tabelas *únicas* dos grupos aditivo e multiplicativo, verificam-se, em seguida, os postulados dos corpos. O corpo correspondente tem a característica dois. Os seus elementos são $0, u, a, a+u$.

3) **O elemento um e o inverso dum elemento** — Dos postulados enunciados para os anéis, não se conclui que exista um elemento do anel com a propriedade do elemento um dum grupo ou dum corpo, no tocante à operação do produto. Basta considerar o anel dos números pares para o reconhecer. Imaginemos ainda o conjunto dos elementos (a, b), onde a e b pertencem a um grupo abeliano aditivo e onde os preceitos de soma e de produtos se introduzem pelas regras $(a, b)+(c, d)=(a+c, b+d)$; $(a, b)\cdot(c, d)=(0, 0)$. Tal conjunto é um anel sem unidade, direita ou esquerda.

Quando existe uma unidade direita u_d, não pode afirmar-se que ela seja única. Se u'_d é uma segunda unidade direita, tem-se $a u_d = a u'_d = a$, e, portanto, $a(u_d - u'_d)=0$. A conclusão $u_d = u'_d$ só pode tirar-se se existir um elemento do anel que não seja divisor de zero à esquerda. Conclusão análoga tem lugar para unidades esquerdas.

Imaginemos, porém, que existem uma unidade direita u_d e uma unidade esquerda u_e. Vimos, em (II, 1, 1), que essas unidades são iguais. Podemos dar este enunciado:

TEOREMA 1: *Se um anel tem uma unidade direita e uma unidade esquerda, essas unidades são iguais. Há, então, uma só unidade direita e esquerda, que se diz* elemento um *do anel e se representa geralmente por* u. Na terminologia de (II, 1, 1), o elemento um é unidade bilateral ou identidade.

Na mesma ordem de ideias é interessante esta afirmação:

TEOREMA 2: *A existência de uma* única *unidade esquerda* u_e *implica que* u_e *seja elemento um (identidade).* De facto, tomemos a e b quaisquer. Escrevendo $(a u_e - a + u_e)b = ab - ab + b = b$, conclui-se $a u_e - a + u_e = u_e$, ou $a u_e = a$, como se deseja.

Quanto ao inverso dum elemento, fazem-se considerações análogas. No anel dos números pares, como no outro exemplo deste número, nenhum elemento tem inverso.

Seja um anel $\mathfrak{A}$ com elemento um. Se a tem inverso direito a_d^{-1}, não pode afirmar-se que esse elemento seja único. Se a'^{-1}_d é um segundo inverso direito, da igualdade $a a_d^{-1} = a a'^{-1}_d$ deduz-se $a(a_d^{-1} - a'^{-1}_d)=0$, mas não pode concluir-se $a_d^{-1} = a'^{-1}_d$, a não ser que se saiba ser a um elemento que não é divisor de zero à esquerda.

Imaginemos agora que existem um inverso direito e um inverso esquerdo a_e^{-1}, de a. Conforme vimos em (II, 1, 4), é válido este

TEOREMA 3: *Se um elemento* a *dum anel tem inverso direito e esquerdo, esses inversos são iguais. O elemento* a *tem inverso, que se representa por* a^{-1}.

Claramente que um divisor de zero não pode ter inverso. Conformes com (II, 1, 4), designaremos por *unidades* os elementos dum anel com inverso. Aqui é fácil de ver que as unidades dum anel formam grupo.

Acabaremos este número com uma proposição curiosa de KAPLANSKY, ainda relativa a inversos.

TEOREMA 4: *Se um anel tem identidade* u, *a existência de mais do que um inverso direito para* a *é bastante para assegurar a existência de uma infinidade de inversos direitos daquele elemento.* Suponhamos α e α_1 dois inversos direitos distintos de a. Façamos $\beta_1 = \alpha_1 a - u$. Vê-se que $\beta_1 \neq 0$, $a\beta_1 = 0$, $\beta_1 \alpha_1 = 0$. Em seguida, ponhamos $\alpha_2 = \alpha_1 + \beta_1$. Também α_2 é um inverso direito de a, a partir do qual construiremos $\beta_2 = \alpha_2 a - u \neq 0$, com $a\beta_2 = 0$, $\beta_2 \alpha_2 = 0$. Duma maneira geral, chegados a α_n, faremos $\beta_n = \alpha_n a - u$ e verificaremos ser $\beta_n \neq 0$, $a\beta_n = 0$, $\beta_n \alpha_n = 0$. Depois, prosseguiremos com $\alpha_{n+1} = \alpha_n + \beta_n$, etc. Se provarmos que os β_i são todos distin-

tos, ficará construida uma infinidade de inversos direitos distintos de a, a saber: $\alpha_1 + \beta_i, (i = 1, 2, \cdots, n, \cdots)$.

Ora, sendo $\beta_{n+1} = \alpha_{n+1} a - u = (\alpha_n + \beta_n) a - u = \alpha_n a + \beta_n a - u = \beta_n + \beta_n a = \beta_n (u + a)$, conclui-se a sucessão de igualdades

$$\beta_{n+1} = \beta_n (u + a) = \beta_{n-1} (u + a)^2 = \cdots = \beta_1 (u + a)^n ,$$

das quais se tira $\beta_k = \beta_i (u + a)^l$, $(k > i;\ k = l + i)$. O facto de u e a serem comutáveis permite a aplicação da fórmula do binómio, o que dá

$$\beta_k = \beta_i \left[u + l a + \binom{l}{2} a^2 + \cdots + l a^{l-1} + a^l \right],$$

$$\beta_k - \beta_i = l \beta_i a + \binom{l}{2} \beta_i a^2 + \cdots + l \beta_i a^{l-1} + \beta_i a^l . \quad (1)$$

Multiplicando ambos os membros desta última igualdade, à direita, por α_i^l, encontra-se $(\beta_k - \beta_i) \alpha_i^l = \beta_i a^l \alpha_i^l = \beta_i$, pois $\binom{l}{r} \beta_i a^r \alpha_i^l = \binom{l}{r} \beta_i a^r \alpha_i^r \alpha_i^{l-r} = \binom{l}{r} \beta_i \alpha_i^{l-r} = 0$, por ser $a \alpha_i = u$, $\beta_i \alpha_i = 0$. Não pode ter-se $\beta_k - \beta_i = 0$, e o teorema fica demonstrado.

4) **Outras regras de cálculo** — Dissemos já, em (II, 1, 2), que se põe $a_n = a \cdots a$, (com n factores), e que $a^m \cdot a^n = a^{m+n}$, $(a^m)^n = a^{nm}$. Se o anel tem elemento um e a tem inverso, também vimos, em (II, 3, 3), que se põe $a^0 = u$ e que $a^{-n} = (a^n)^{-1} = (a^{-1})^n$. Além disto, provámos as igualdades $a^n \cdot a^{-m} = a^{n-m}, (a^n)^{-m} = a^{-mn}$.

Uma regra que não tem equivalente na Teoria dos Grupos é expressa nas igualdades seguintes

$$n \cdot ab = na \cdot b = a \cdot nb ,$$

que se demonstram por indução. O «produto» $n \cdot ab$ representa-se simplesmente por nab.

Consideremos agora o elemento $-nab$. É $nab - nab = 0$. Mas $-na \cdot b + na \cdot b = -na \cdot b + nab = (-na + na) b = 0$, pelo que $-nab = -na \cdot b$. Também se vê que $-nab = a \cdot (-nb)$, convindo, assim, fixar as regras

$$-nab = -na \cdot b = a \cdot (-nb) .$$

Tomemos ainda uma expressão do tipo $-n \cdot ab$. O anel $\mathfrak{A}$, como grupo abeliano aditivo, dá $-n \cdot ab = -nab$. Por isso se tem

$$-n \cdot ab = -nab = -na \cdot b = a \cdot (-nb) = n(-a) \cdot b = a \cdot n(-b) = (-n \cdot a) b = a \cdot (-n \cdot b) .$$

Para terminarmos este número, faremos as observações seguintes: 1) se a comuta com b, então comuta com $-b$, nb e b^{-1}, se este último existe; 2) se a comuta com b e c, comuta com $b + c$ e bc.

§ 2. Subanéis e extensões de anéis. Ideais e homomorfismos. Anéis de cocientes. Números racionais.

1) **Critério de subanel** — Dum modo geral, dado um conjunto $\mathfrak{C}$, suporte dum sistema algébrico $\mathfrak{A}$, dissemos já, em (II, 2, 1), que uma parte de $\mathfrak{A}$, verificando as mesmas leis inpostas a $\mathfrak{A}$, se diz um subsistema de $\mathfrak{A}$.

Quando $\mathfrak{A}$ é um anel, um subsistema diz-se um subanel. A este respeito, enunciaremos a proposição seguinte:

TEOREMA 1: *$\mathfrak{A}_1$ é um subanel do anel $\mathfrak{A}$, se, com* a *e* b, *contiver* a − b *e* ab; *$\mathfrak{D}_1$ é um subanel de divisão do anel de divisão $\mathfrak{D}$, se, com* a *e* b, *contiver* a − b, *assim como* ba^{-1}, *quando* $a \neq 0$; *$\mathfrak{S}_1$ é um subdomínio de integridade do domínio de integridade $\mathfrak{S}$, (comutativo ou não), se for subanel e contiver, pelo menos, dois elementos.* Tratemos, por exemplo, o caso dos subanéis de divisão. A hipótese $a - b \in \mathfrak{D}_1$ garante ser $\mathfrak{D}_1$ um grupo abeliano. Como se admite a existência dum elemento $a \neq 0$, o postulado A_9), de (V, 1, 2), é verificado. Então, os elementos não nulos de $\mathfrak{D}_1$ satisfazem o critério de subgrupo, pelo que, em $\mathfrak{D}_1$, o produto desses elementos é fechado. A inclusão do zero não altera esse facto. Resulta daí que $\mathfrak{D}_1$ é um subanel cujos elementos não nulos formam um grupo. Portanto, $\mathfrak{D}_1$ é subanel de divisão.

A intersecção de subdomínios de integridade (comutativos ou não), se contém mais do que um elemento, é um subdomínio de integridade. A intersecção de subanéis de divisão é um subanel de divisão. Neste último caso não há necessidade de exigir que a referida intersecção

tenha mais do que um elemento, visto que ela contém necessàriamente 0 e u.

Tratando-se de corpos, introduz-se a designação de *corpo primo* para todo aquele que não contém subcorpo próprio. A intersecção de todos os subcorpos dum corpo é um corpo primo.

Seja $\mathfrak{K}$ um corpo e tomemos $u \in \mathfrak{K}$. O subcorpo primo de $\mathfrak{K}$ contém todos os elementos da forma mu, com m inteiro. Esses elementos podem não ser todos distintos, como no exemplo tabelado em (V, 1, 2), no qual era $2u = 0$. O conjunto dos elementos distintos mu é um domínio de integridade.

Quando um domínio de integridade $\mathfrak{S}$ tem elemento u, o conjunto dos elementos da forma mu constitui um subdomínio de integridade. A característica de $\mathfrak{S}$ é a mesma que a deste subdomínio, por ser igual ao menor inteiro que anula u. É o que se conclui no texto da demonstração deste

TEOREMA 2: *Um domínio de integridade* $\mathfrak{S}$, *com elemento* u, *tem por característica um número primo* p, *quando essa característica é* $\neq 0$. Se q é a característica, tem-se $qu = 0$. Admitindo que poderia ser $q = rs$, com $r, s \neq 1$, seria também $(rs)u = ru \cdot su = 0$, o que implicaria $ru = 0$, ou $su = 0$. Então, se fosse, por exemplo, $ru = 0$, seria também, para cada $a \in \mathfrak{S}$, $ra = ru \cdot a = 0$, com $r < q$, o que é absurdo.

Diz-se *centro* dum anel o conjunto dos seus elementos que comutam com todos os elementos do anel. O centro é um subanel. Os anéis de divisão contêm no seu centro um corpo primo.

2) **A noção de isomorfismo e o teorema correspondente ao de Cayley** — Sejam $\mathfrak{A}$ um anel e $\mathfrak{A}'$ um sistema algébrico semelhante, nos termos indicados em (III, 1, 1). Se tiver lugar um homomorfismo $\mathfrak{A} \sim \mathfrak{A}'$, o facto de $\mathfrak{A}$ ser um anel implica que $\mathfrak{A}'$ seja um anel. O homomorfismo em questão pode receber o nome de *homomorfismo anular*. No caso de isomorfismo, também se utiliza a designação de *isomorfismo anular*, escrevendo-se $\mathfrak{A} \simeq \mathfrak{A}'$.

Posto isto, consideremos um anel $\mathfrak{A}$, e tomemos $a \in \mathfrak{A}$, fixo, e $x \in \mathfrak{A}$, arbitrário. A correspondência $x \to xa$ é um endomorfismo do grupo aditivo do anel. Escreveremos $xa = x E_a^{(d)}$, de sorte que $E_a^{(d)}$ é

o *endomorfismo definido pela multiplicação, à direita por* a. A correspondência $x \to ax = x E_a^{(e)}$ leva ao significado de $E_a^{(e)}$ como *endomorfismo definido pela multiplicação, à esquerda, por* a.

Estudemos, em seguida, a nova correspondência $a \to E_a^{(d)}$. Das relações $x(a+b) = xa + xb = x E_a^{(d)} + x E_b^{(d)} = x(E_a^{(d)} + E_b^{(d)})$, conclui-se

$$a \to E_a^{(d)}, \quad b \to E_b^{(d)}, \quad a+b \to E_{a+b}^{(d)} = E_a^{(d)} + E_b^{(d)}.$$

E, das relações $x(ab) = (xa)b = x E_a^{(d)} E_b^{(d)}$, deduz-se

$$ab \to E_{ab}^{(d)} = E_a^{(d)} E_b^{(d)}.$$

A correspondência $a \to E_a^{(d)}$ é um homomorfismo anular. O conjunto dos endomorfismos $E_a^{(d)}$ é um subanel $\mathfrak{A}_d$, do anel $\mathfrak{F}(\mathfrak{A})$, dos endomorfismos do grupo aditivo de $\mathfrak{A}$. Se existir elemento $u \in \mathfrak{A}$, então, suposto $a \neq b$, é $u \to ua = a = u E_a^{(d)}$, $u \to ub = b = u E_b^{(d)}$, de sorte que $E_a^{(d)} \neq E_b^{(d)}$. Tem lugar o teorema a seguir, que corresponde ao teorema de CAYLEY, indicado em (II, 2, 2):

TEOREMA 1: *Um anel com identidade é isomorfo dum subanel do do anel dos endomorfismos do seu grupo aditivo.*

À semelhança do que também se fez no referido lugar (II, 2, 2), definiremos *anti-homomorfismo anular* como uma correspondência entre anéis, verificando as condições seguintes:

$$a \to a', \quad b \to b', \quad a+b \to (a+b)' = a' + b', \quad ab \to (ab)' = b'a'.$$

No caso de biunivocidade, tem-se um *anti-isomorfismo* ou um *isomorfismo inverso*. A correspondência $a \to E_a^{(e)}$, onde $E_a^{(e)}$ tem o significado já indicado, é um anti-homomorfismo. Se existe $u \in \mathfrak{A}$, obtem-se um anti-isomorfismo. O conjunto dos $E_a^{(e)}$ é um subanel $\mathfrak{A}_e$, de $\mathfrak{F}(\mathfrak{A})$. É válido este

TEOREMA 2: *Dado gm anel* $\mathfrak{A}$ *com identidade, os subanéis* $\mathfrak{A}_d$ *e* $\mathfrak{A}_e$ *são comutadores reciprocos dentro de* $\mathfrak{F}(\mathfrak{A})$. A demonstração faz-se como para o teorema 2, de enunciado análogo, que se provou em (II, 2, 2).

3) **Extensões de anéis** — Dado um anel $\mathfrak{A}$, se o anel $\mathfrak{A}'$ contém $\mathfrak{A}$, diz-se uma *ampliação* ou *extensão* de $\mathfrak{A}$. Com o objectivo de simplificarmos o enunciado da importante proposição que neste número

daremos em primeiro lugar, há conveniência em usar a notação e a terminologia a que vamos referir-nos.

O símbolo $\{\mathfrak{C}_\alpha\}_{\alpha\in A}$ representa uma família de conjuntos. O índice variável α percorre os elementos dum conjunto A, existindo uma correspondência biunívoca completa entre os $\mathfrak{C}_\alpha$ e os elementos de A. A família $\mathfrak{C}_\alpha$ diz-se uma *família filtrante*, se, dados dois elementos da família, existir um elemento da família contendo aqueles dois.

Podemos dar, então, o enunciado seguinte:

TEOREMA 1: *Seja* $\{\mathfrak{A}_\alpha\}_{\alpha\in A}$ *uma família filtrante, finita ou infinita, de anéis* $\mathfrak{A}_\alpha$. *O conjunto unido* $\mathfrak{U}=\bigcup\mathfrak{A}_\alpha$ *é um anel, extensão dos* $\mathfrak{A}_\alpha$. A respectiva demonstração faz-se verificando em $\mathfrak{U}$ os postulados dos anéis. Sejam, por exemplo, $a,b\in\mathfrak{U}$. Se for $a\in\mathfrak{A}_\alpha$, $b\in\mathfrak{A}_\beta$, $(\beta\in A)$, existe $\mathfrak{A}_\gamma$ $(\gamma\in A)$, que contém aqueles dois anéis, nele se podendo definir uma soma $a+b$. Essa soma é independente do anel a que pertençam simultâneamente a e b, pois, se $\mathfrak{A}_\delta\neq\mathfrak{A}_\gamma$ for outro anel nessas condições, existe um novo anel $\mathfrak{A}_\varepsilon$ da família, no qual estão contidos $\mathfrak{A}_\gamma$ e $\mathfrak{A}_\delta$ e no qual a soma $a+b$ é a mesma que em $\mathfrak{A}_\gamma$ e $\mathfrak{A}_\delta$. O postulado A_1), de (V, 1, 1), é verificado em $\mathfrak{U}$. Se quiséssemos provar a lei associativa $ab\cdot c=a\cdot bc$, não teríamos mais do que considerar um anel da família ao qual pertencessem os três elementos a, b e c. A demonstração de qualquer dos postulados é feita sempre nos mesmos moldes. Por outro lado, é imediato que $\mathfrak{U}$ é extensão de qualquer $\mathfrak{A}_\alpha$.

No caso particular de os $\mathfrak{A}_\alpha$ serem corpos $\mathfrak{K}_\alpha$, o conjunto unido é ainda um corpo. Convém notar que não foi feita a hipótese inicial de os diferentes $\mathfrak{A}_\alpha$ serem subanéis dum mesmo anel. Também se não estabelece que $\mathfrak{U}$ seja um anel pertencente à família de que se parte.

No número anterior, verificámos ser $\mathfrak{F}(\mathfrak{A})$, em geral, uma extensão de $\mathfrak{A}_d$ e de $\mathfrak{A}_c$. Eis agora um teorema de muito interesse:

TEOREMA 2: *Um anel* $\mathfrak{A}_0$, *sem elemento um, pode «mergulhar-se» sempre num anel* $\mathfrak{A}$, *com elemento um.* O enunciado deve interpretar-se como se indicou em (II, 3, 1), da maneira seguinte: pode construir-se um anel $\mathfrak{A}$ contendo uma parte $\mathfrak{A}'_0$ isomorfa (anular) de $\mathfrak{A}_0$. Sob o ponto de vista abstracto, é legítima a substituição de $\mathfrak{A}'_0$ por $\mathfrak{A}_0$, dentro de $\mathfrak{A}$, pois que, tendo lugar a correspondência biunívoca $a_0\rightarrow a'_0$, $(a_0\in\gamma_0, a'_0\in\mathfrak{A}'_0)$, qualquer relação entre elementos não acentuados se transfere para elementos acentuados e reciprocamente. Por

outro lado, nas relações, dentro de $\mathfrak{A}$, em que intervenham elementos de $\mathfrak{A}'_0$ e elementos não pertencentes a $\mathfrak{A}'_0$, a substituição de a'_0 por a_0 é meramente formal.

Passemos ao teorema. Seja $a_0\in\mathfrak{A}_0$. O anel $\mathfrak{A}$ será constituído pelos elementos $[m,a_0]$, onde m é inteiro, e onde, suposto $b_0\in\mathfrak{A}_0$ e n inteiro, os preceitos de soma e de produto são definidos pelas igualdades

$$[m,a_0]+[n,b_0]=[m+n,a_0+b_0];$$

$$[m,a_0]\cdot[n,b_0]=[mn,mb_0+na_0+a_0b_0].$$

De facto, em $\mathfrak{A}$ são verificados os postulados dos anéis, como é fácil de reconher. O elemento $[1,0]$ é o elemento um de $\mathfrak{A}$. E, por via da correspondência $a_0\rightarrow[0,a_0]$, determina-se a parte $\mathfrak{A}'_0$, de $\mathfrak{A}$, isomorfa de $\mathfrak{A}_0$.

O teorema 1 do número anterior pode agora revestir-se do aspecto preciso do teorema de CAYLEY:

TEOREMA 3: *Todo o anel é isomorfo dum anel de endomorfismos.*

No estudo das relações entre $\mathfrak{A}_0$ e $\mathfrak{A}$, existem certos factos importantes, entre os quais assinalaremos o que vai seguir-se. Um elemento a dum anel diz-se *nilpotente*, se houver uma potência a^r, $(r>0)$, tal que $a^r=0$. Claramente que, se a_0 for nilpotente em $\mathfrak{A}_0$, é nilpotente em $\mathfrak{A}$. Vamos ver que, inversamente, supondo $a\in\mathfrak{A}$ tal que $a^t=0$, é $a\in\mathfrak{A}_0$. De facto, escrevamos $a=[m,a_0]$. Como se tem $a^t=[m^t,b_0]=[0,0]$, deverá ser $m^t=0$, $m=0$, e, portanto, $a=[0,a_0]=a_0$. Tem-se

TEOREMA 4: *Na extensão de* $\mathfrak{A}_0$ *para* $\mathfrak{A}$, *há conservação dos elementos nilpotentes.*

4) **Ideais** — Um subconjunto $\mathfrak{r}$, do anel $\mathfrak{A}$, diz-se um *ideal direito*, se forem verificadas as duas condições seguintes: I_1) $\mathfrak{r}$ contém, com a e b, o elemento $a-b$; I_2) $\mathfrak{r}$ contém, com a, todos os produtos ar, em que $r\in\mathfrak{A}$.

Um *ideal esquerdo* $\mathfrak{e}$, de $\mathfrak{A}$, satisfaz a I_1) e à condição seguinte: I'_2) $\mathfrak{e}$ contém, com a, todos os produtos sa, em que $s\in\mathfrak{A}$.

Um *ideal bilateral*, ou, mais simplesmente, um *ideal*, é um subconjunto $\mathfrak{a}$, de $\mathfrak{A}$, que é simultâneamente ideal direito e esquerdo.

É possível utilizar a linguagem dos grupos com operadores, introduzida em (IV, 1, 1), para caracterizar os diferentes tipos de ideais. Na verdade, um anel $\mathfrak{A}$ é sempre um grupo abeliano com os seguintes operadores: os elementos de $\mathfrak{A}$. Então, um ideal direito é um submódulo admissível de $\mathfrak{A}$, se os elementos do anel se consideram a operar à direita; um ideal esquerdo é um submódulo admissível, se os elementos do anel se consideram a operar à esquerda; e um ideal bilateral pode imaginar-se ainda como submódulo admissível, supondo haver dois domínios operatórios (os elementos de $\mathfrak{A}$), um deles a operar à direita, outro à esquerda.

Vamos dar exemplos de ideais. Diz-se *ideal principal esquerdo gerado por* a o conjunto $(a)_e$ dos elementos $sa + na$, onde $s \in \mathfrak{A}$ e n é inteiro. O *ideal principal direito gerado por* a é o conjunto $(a)_d$ dos elementos $ar + na$, $(r \in \mathfrak{A})$, e o *ideal gerado por* a é o conjunto (a) dos elementos $sa + ar + \sum paq + na$, onde o somatório tem um número finito de parcelas e $p, q \in \mathfrak{A}$.

As definições estendem-se a ideais gerados por vários elementos. Se $a_1, a_2, \cdots, a_p$ são os elementos geradores, têm-se os conjuntos

$$\{s_1 a_1 + \cdots + s_p a_p + n_1 a_1 + \cdots + n_p a_p\},$$
$$\{a_1 r_1 + \cdots + a_p r_p + n_1 a_1 + \cdots + n_p a_p\},$$

nos quais s_i, $r_i \in \mathfrak{A}$ e os n_j são inteiros, para definir, respectivamente, um ideal esquerdo e um ideal direito gerado pelos a_i. Os elementos a_i pertencem, em ambos os casos, aos ideais. Basta fazer $s_1 = \cdots = s_p = 0$, $n_2 = \cdots = n_p = 0$, $n_1 = 1$, para se ter, no primeiro dos casos, o elemento a_1. Diz-se, então, que os elementos a_i constituem uma *base* para o respectivo ideal e escreve-se

$$(a_1, \cdots, a_p)_e = \left\{\sum s_i a_i + \sum n_i a_i\right\}, \quad (a_1, \cdots, a_p)_d = \left\{\sum a_i r_i + \sum n_i a_i\right\},$$
$$(a_1, \cdots, a_p) = \left\{\sum s_i a_i + \sum a_i r_i + \sum p a_i q + \sum n_i a_i\right\}.$$

A última igualdade define o ideal bilateral gerado por $a_1, \cdots a_p$.

Em todos os casos, os ideais em questão são os ideais mínimos que contêm $a_1, \cdots, a_p$. Se tomarmos, por exemplo, um ideal esquerdo que contenha $a_1, \cdots, a_p$, esse ideal conterá $s_1 a_1, \cdots, s_p a_p$, conterá a soma $s_1 a_1 + \cdots + s_p a_p$, assim como $n_1 a_1 + \cdots + n_p a_p$ e a soma $\sum s_i a_i + \sum n_i a_i$.

O ideal esquerdo gerado por $a_1, \cdots, a_p$ pode, assim, considerar-se como a intersecção de todos os ideais esquerdos que contêm aqueles elementos.

Se os elementos geradores são em número infinito, o ideal direito, por exemplo, que eles geram, é o conjunto dos somatórios finitos da forma $\sum a_i r_i + \sum n_i a_i$, em cada um dos quais figura um número finito de elementos a_i, tomados nos elementos dados. É assim que podemos dizer: o ideal bilateral gerado por a é o ideal esquerdo gerado pelos elementos do ideal direito gerado por a, ou o ideal direito gerado pelos elementos do ideal esquerdo gerado por a.

Há sempre dois ideais particulares: o *ideal nulo* $= (0)$, composto do único elemento zero, e o *ideal unidade*, que é o próprio anel.

Se existe $u \in \mathfrak{A}$, o ideal direito gerado por $a_1, \cdots, a_p$ é simplesmente o conjunto dos elementos da forma $a_1 t_1 + \cdots + a_p t_p$, $(t_i \in \mathfrak{A})$, pois que

$$a_1 r_1 + \cdots + a_p r_p + n_1 a_1 + \cdots + n_p a_p =$$
$$= a_1 (r_1 + n_1 u) + \cdots + a_p (r_p + n_p u) = a_1 t_1 + \cdots + a_p t_p.$$

No anel dos números inteiros, (no qual, por ser comutativo, se não distinguem ideais direitos, esquerdos e bilaterais), estudemos o ideal gerado pelos números 2 e 3. Como há elemento um, tem de considerar-se o conjunto $n \cdot 2 + m \cdot 3 = n \cdot 2 + m \cdot (2 + 1) = n' \cdot 2 + m'$. Este conjunto representa o ideal unidade, por conter todos os números inteiros.

Supondo $a \in \mathfrak{A}$ fixo e $r, s \in \mathfrak{A}$ arbitrários, os conjuntos $\{ar\}$ e $\{sa\}$ representam, respectivamente, em todos os casos, um ideal direito e um ideal esquerdo.

Nas diferentes teorias da *Álgebra abstracta*, o conceito de ideal desempenha um papel fundamental. Nessas teorias, as *operações sobre ideais*, que permitem estabelecer processos, segundo os quais se deduzem ideais doutros ideais dados, têm aplicação constante. Se $\mathfrak{e}$ e $\mathfrak{e}'$ são dois ideais esquerdos de $\mathfrak{A}$, chamaremos ideal esquerdo *soma* $(\mathfrak{e}, \mathfrak{e}')$ o ideal esquerdo que é o conjunto dos elementos obtidos por adição dum elemento de $\mathfrak{e}$ a um elemento de $\mathfrak{e}'$. O conjunto $\mathfrak{e} \cap \mathfrak{e}'$ é também um ideal esquerdo, que se diz *intersecção* dos dois ideais dados.

Sejam $\mathfrak{m}$ e $\mathfrak{m}'$ dois submódulos do grupo aditivo de $\mathfrak{A}$. Com o símbolo $\mathfrak{m}\mathfrak{m}'$, significaremos o conjunto de elementos $\sum b b' \in \mathfrak{A}$, obtidos por somatório finito, quando $b \in \mathfrak{m}$, $b' \in \mathfrak{m}'$. Esse conjunto

é um novo submódulo, como se verifica imediatamente. No caso particular de se ter $\mathfrak{m} = \mathfrak{e}$, o *produto* $\mathfrak{e}\mathfrak{m}'$ é um ideal esquerdo; se for $\mathfrak{m}' = \mathfrak{r}$, o *produto* $\mathfrak{m}\mathfrak{r}$ é um ideal direito. Ainda mesmo que $\mathfrak{C}$ seja um conjunto qualquer de elementos de $\mathfrak{A}$, o produto $\mathfrak{C}\mathfrak{r}$ é um ideal direito e o produto $\mathfrak{e}\mathfrak{C}$ um ideal esquerdo. São válidas, por exemplo, as seguintes regras de cálculo:

$$\mathfrak{C}\cdot(\mathfrak{r},\mathfrak{r}') = (\mathfrak{C}\mathfrak{r},\mathfrak{C}\mathfrak{r}'), \qquad \mathfrak{C}\cdot\mathfrak{r}\mathfrak{r}' = \mathfrak{C}\mathfrak{r}\cdot\mathfrak{r}'.$$

O produto $\mathfrak{e}\mathfrak{r}$ é um ideal bilateral e a soma $(\mathfrak{r},\mathfrak{A}\mathfrak{r})$ é o *ideal bilateral gerado pelo ideal direito* $\mathfrak{r}$. Anàlogamente, $(\mathfrak{e},\mathfrak{e}\mathfrak{A})$ é o *ideal bilateral gerado por* $\mathfrak{e}$.

O *cociente* $(\mathfrak{e}:\mathfrak{C})_d$, do ideal esquerdo $\mathfrak{e}$ pelo conjunto $\mathfrak{C}$, define-se como o conjunto dos elementos $t \in \mathfrak{A}$ tais que $t\mathfrak{C} \subseteq \mathfrak{e}$. É um ideal esquerdo. O cociente $(\mathfrak{e}:\mathfrak{A})_d$ é um ideal bilateral. Dá-se, anàlogamente, a definição de cociente $(\mathfrak{r}:\mathfrak{C})_e$, do ideal direito $\mathfrak{r}$ pelo conjunto $\mathfrak{C}$. Será $t \in (\mathfrak{r}:\mathfrak{C})_e$, se $\mathfrak{C}t \subseteq \mathfrak{r}$.

5) **Subanel gerado por um conjunto de elementos** — Consideremos um conjunto $\Omega = \{a, b, c, \cdots, t, \cdots\}$ de elementos dum anel $\mathfrak{A}$, conjunto que pode ser finito ou infinito. Diz-se *subanel gerado por* Ω o mais pequeno subanel que contém Ω. Qualquer subanel que contenha Ω, contém necessàriamente todos os elementos da forma $\sum \pm a b \cdots t$, onde o somatório é finito e o número de factores de cada parcela é igualmente finito. E como o conjunto de tais elementos é um subanel. esse conjunto será o subanel gerado por Ω.

No anel $\mathfrak{A}$, se for $\mathfrak{C} \subseteq \mathfrak{A}$ um conjunto qualquer, diz-se *comutador de* $\mathfrak{C}$, e representa-se por $C(\mathfrak{C})$, o conjunto dos elementos de $\mathfrak{A}$ que comutam com todos os elementos de $\mathfrak{C}$. Esse comutador é sempre um subanel. Se for $\mathfrak{C}_1 \subseteq \mathfrak{C}_2$, tem-se $C(\mathfrak{C}_1) \supseteq C(\mathfrak{C}_2)$. São de fácil verificação as relações seguintes:

$$C(C(\Omega)) \supseteq \Omega, \qquad C(C(C(\Omega))) = C(\Omega).$$

Podemos agora ligar às ideias do número 2 deste parágrafo as diferentes noções de ideal. Se representarmos por 1 o endomorfismo idêntico de $\mathfrak{A}$, vê se que, no anel $\mathfrak{F}(\mathfrak{A})$, dos endomorfismos de $\mathfrak{A}$, o subanel gerado por 1 e $\mathfrak{A}_d$, que aqui podemos designar por $\mathfrak{F}(1, \mathfrak{A}_d)$, é o conjunto de elementos da forma $\sum \pm 1\, E_r^{(d)} \cdots E_s^{(d)}$, e que o subanel gerado por 1, $\mathfrak{A}_d$ e $\mathfrak{A}_e$, representado por $\mathfrak{F}(1, \mathfrak{A}_d, \mathfrak{A}_e)$, é o conjunto de elementos da forma $\sum \pm 1\, E_r^{(d)} \cdots E_s^{(d)} E_t^{(e)} \cdots E_v^{(e)}$. Então, tem-se:

$$(a)_d = a\,\mathfrak{F}(1, \mathfrak{A}_d), \qquad (a) = a\,\mathfrak{F}(1, \mathfrak{A}_d, \mathfrak{A}_e),$$

subentendendo, é claro, que um símbolo da forma $a\mathfrak{B}$, onde $\mathfrak{B} \subseteq \mathfrak{F}(\mathfrak{A})$, representa o conjunto de elementos de aspecto aS, com $S \in \mathfrak{B}$.

6) **Homomorfismos e isomorfismos** — Em (V, 2, 2), introduzimos já as noções de homomorfismo anular e de isomorfismo anular, dentro dos conceitos gerais correspondentes, relativos a espaços algébricos quaisquer. Quando se trata dum homomorfismo $\mathfrak{A} \sim \mathfrak{A}'$, a imagem de 0 é $0' = \text{zero} \in \mathfrak{A}'$, e a imagem de $u \in \mathfrak{A}$, se tal elemento existe, é a identidade de $\mathfrak{A}'$. Convém, entretanto, fazer a observação de que pode existir identidade em $\mathfrak{A}'$ sem que exista em $\mathfrak{A}$.

Tomemos o ideal direito $\mathfrak{r}$, de $\mathfrak{A}$. Existe um grupo diferença $\mathfrak{A} - \mathfrak{r}$, considerados $\mathfrak{A}$ como «módulo $-\mathfrak{A}$» e $\mathfrak{r}$ como submódulo admissível. É, assim, $(a+\mathfrak{r}) + (b+\mathfrak{r}) = (a+b)+\mathfrak{r}$, $(a+\mathfrak{r})s = as+\mathfrak{r}$. Procuremos ver se o elemento $ab+\mathfrak{r}$ do grupo diferença verifica a relação $(a+\mathfrak{r})(b+\mathfrak{r}) = ab+\mathfrak{r}$. O produto indicado no primeiro membro, da forma $ab + a\mathfrak{r} + \mathfrak{r}b + \mathfrak{r}$, mostra que ab vem adicionado a uma expressão que, em geral, não pertence a $\mathfrak{r}$.

Se substituirmos $\mathfrak{r}$ por um ideal bilateral $\mathfrak{a}$, a dificuldade deixa de existir e pode dar-se sentido à igualdade

$$(a+\mathfrak{a})(b+\mathfrak{a}) = ab+\mathfrak{a}.$$

Basta verificar, para isso, que o resultado indicado para o produto é o mesmo, se as classes $a+\mathfrak{a}$ e $b+\mathfrak{a}$ tiverem representantes diferentes de a e b, respectivamente. Se for $a \equiv c(\mathfrak{a})$, $b \equiv d(\mathfrak{a})$, ou seja $a = c + a'$, $b = d + a''$, com $a', a'' \in \mathfrak{a}$, é também $ab = cd + a'''$, com $a''' \in \mathfrak{a}$. Tem-se, como se deseja, $ab \equiv cd(\mathfrak{a})$.

No grupo diferença $\mathfrak{A} - \mathfrak{a}$, que escreveremos antes $\mathfrak{A}/\mathfrak{a}$, ficou dado um preceito de multiplicação, além do da adição que existia no sentido da Teoria dos Grupos.

Pode verificar-se, sucessivamente, que são válidos em $\mathfrak{A}/\mathfrak{a}$ todos os postulados dos Anéis. $\mathfrak{A}/\mathfrak{a}$ diz-se *anel diferença de* $\mathfrak{A}$ *segundo* $\mathfrak{a}$. Se a cada elemento $a \in \mathfrak{A}$ fizermos corresponder a classe $a+\mathfrak{a} = \overline{a}$, o homomorfismo $\mathfrak{A} \sim \mathfrak{A}/\mathfrak{a}$, que reconhecemos em (III, 1, 9), é homo-

$a\,d = b\,c$. Por meio dela, divide-se $\mathfrak{C}$ em classes disjuntas. Designaremos por $\mathfrak{S}$ o conjunto das classes e empregaremos a notação $[a,b]$ para significar a classe de representante (a,b). Em $\mathfrak{S}$, definiremos uma soma e um produto, pondo

$$(1)\qquad \begin{aligned} [a,b]+[c,d] &= [a\,d+b\,c,\,b\,d],\\ [a,b]\cdot[c,d] &= [a\,c,\,b\,d]. \end{aligned}$$

A coerência destas definições exige: 1.º) — que os resultados da soma e do produto sejam classes de $\mathfrak{S}$; 2.º) — que esses resultados sejam independentes dos elementos das classes utilizados como seus representantes. Ora, em (1), vê-se que $b\,d \in \mathfrak{M}$, o que satisfaz a primeira exigência. Relativamente à segunda, imaginemos, por exemplo, $[a,b] = [a',b']$, ou seja $a\,b' = b\,a'$. Então, $[a',b']+[c,d]=[a'd+b'c,\,b'd]$, tornando-se necessário provar que é $(a\,d+b\,c)\,b'\,d = b\,d\,(a'\,d+b'\,c)$. Observando ser válida a relação $a\,b' = b\,a'$, a igualdade anterior é imediata. Trata-se anàlogamente a segunda igualdade (1).

No conjunto $\mathfrak{S}$ ficaram introduzidos um preceito de soma e um preceito de produto, por via dos quais $\mathfrak{S}$ se pode considerar um anel. A este respeito, faremos algumas observações, embora não desenvolvamos a verificação dos postulados.

O elemento zero é $[0,c]$, qualquer que seja $c \in \mathfrak{M}$. O anel inicial $\mathfrak{A}$ está «mergulhado» em $\mathfrak{S}$, por via da correspondência $a \to [a\,c,\,c]$, que é um isomorfismo. A biunivocidade da referida correspondência, por exemplo, resulta deste modo: se $[a\,c,\,c] = 0 = [0,c]$, então $a\,c\cdot c = c\cdot 0 = 0$, o que exige $a = 0$. Podemos dizer:

TEOREMA: *Suponhamos $\mathfrak{A}$ um anel comutativo e $\mathfrak{M}$ um conjunto de elementos de $\mathfrak{A}$ que não contém divisores de zero e que é fechado relativamente ao produto, definido em $\mathfrak{A}$; existe um anel comutativo $\mathfrak{S}$, de classes $[a,b]$, com $a \in \mathfrak{A}$, $b \in \mathfrak{M}$, no qual os preceitos de soma e de produto são definidos pelas igualdades* (1) *e no qual $\mathfrak{A}$ se encontra «mergulhado».*

9) **Os números racionais** — Se o anel inicial $\mathfrak{A}$, referido no número anterior, for um domínio de integridade comutativo e se tomarmos para $\mathfrak{M}$ todos os elementos de $\mathfrak{A}$, salvo zero, podemos mostrar que $\mathfrak{S}$ é um corpo.

Na verdade, seja $[a,b] \in \mathfrak{S} = \mathfrak{K}$. Supondo $a \neq 0$, é $[a,b] \neq 0$. Tem sentido escrever $[b,a]$ e é $[a,b]\cdot[b,a]=[a\,b,\,a\,b]=[b,b] =$ elemento um de $\mathfrak{K}$. Todos os elementos não nulos de $\mathfrak{K}$ têm inverso, pelo que $\mathfrak{K}$ é um corpo. Logo:

TEOREMA: *Todo o domínio de integridade comutativo se pode «mergulhar» num corpo.*

Os *números racionais* constituem um corpo: é o corpo obtido pelo processo de «imersão» em causa, quando se parte do domínio de integridade comutativo, constituido pelo anel dos números inteiros. Representá-lo-emos pelo símbolo $\mathfrak{R}_0$. E, dentro de $\mathfrak{R}_0$, o elemento $[a\,c,\,c]$ substitui-se pelo inteiro a.

§ 3. Corpos ordenados. Números reais. Números complexos

1) **Corpos ordenados** — Um corpo $\mathfrak{K}$ diz-se *ordenado*, se nele se verificarem as propriedades seguintes: O_1) constitui um conjunto ordenado; O_2) suposto $a > b$, é $a + c > b + c$, qualquer que seja $c \in \mathfrak{K}$; O_3) suposto $a > b$ e $c > 0$, é $a\,c > b\,c$.

As duas primeiras propriedades, como vimos em (II, 3, 1), exprimem que o grupo aditivo de $\mathfrak{K}$ constitui um grupo abeliano ordenado.

A definição dada é equivalente a esta outra, que passamos a enunciar. $\mathfrak{K}$ diz-se ordenado, se nele tiverem lugar as propriedades seguintes: O'_1) $\mathfrak{K}$ compõe-se de três subconjuntos disjuntos, um deles formado pelo único elemento zero, outro formado pelos elementos chamados *positivos*, e o último formado pelos elementos chamados *negativos*, de tal modo que, se $a \neq 0$ é positivo, $-a$ é negativo, e reciprocamente; O'_2) escreve-se $a > 0$, quando a é positivo, escreve-se $-a > 0$, quando a é negativo, e introduz-se uma ordem total em $\mathfrak{K}$, pondo $a > b$, se $a - b > 0$; O'_3) supostos $a > 0$, $b > 0$, é $a + b > 0$ e $a\,b > 0$.

Para se demonstrar a equivalência, comecemos por admitir a primeira definição. Então, se for $a > 0$, é $a - a > -a$, ou seja $-a < 0$, e reciprocamente. Daqui se conclui O'_1). Depois tendo-se $a - b > 0$, é $a - b + b > b$, isto é, é $a > b$, e reciprocamente; então, O'_2) é válida. Finalmente, se $a > 0$, $b > 0$, tem-se $a + b > b > 0$, assim como $a\,b > 0\cdot b = 0$, de sorte que O'_3) tem lugar.

Admitamos agora a segunda definição. Vamos reconhecer que, ~~por via de O'_1) e de O'_2)~~, $\mathfrak{R}$ é, de facto, um conjunto ordenado. Dados a e b, se $a>b$, ou seja, se $a-b>0$, não é $b>a$, pois que isso implicaria $b-a=-(a-b)>0$, contràriamente à afirmação O'_2). Por outro lado, se $a>b$, $b>c$, de $a-b>0$ e $b-c>0$, concluimos, à face de O'_3) $(a-b)+(b-c)=a-c>0$, ou seja $a>c$. Fica, assim, demonstrada a propriedade O_1), com o sinal $>$ como sinal de ordenação. A propriedade O_2) é imediata. Quanto a O_3), admitindo que é $a>b$, $c>0$, vê-se que $a-b>0$, $c>0$, o que, por O'_3), dá $(a-b)c=ac-bc>0$, ou seja $ac>bc$, como se quer. A equivalência referida ficou demonstrada.

A *regra dos sinais*, já encontrada em (II, 3, 2), segundo a qual o produto de dois elementos maiores ou menores que zero é um elemento maior do que zero, e o produto de dois elementos, um maior outro menor do que zero, é um elemento menor do qne zero, justifica-se fàcilmente. Seja, por exemplo, $a<0$, $b<0$; então, tem-se $-a>0$, $-b>0$, por consequência $ab=(-a)(-b)>0$.

Mostraremos, em seguida, que, num corpo ordenado a condição $a>b$, com $a>0$, $b>0$, implica $a^{-1}<b^{-1}$. Na verdade, sendo $a-b=ab(b^{-1}-a^{-1})>0$, o facto de se ter $ab>0$ arrasta que seja $b^{-1}-a^{-1}>0$, ou $a^{-1}<b^{-1}$.

Observe-se também que $a>0$ implica $a^{-1}>0$. É o que se reconhece tendo em conta que $a\cdot u=a>0$ implica $u>0$, de sorte que $a\cdot a^{-1}=u>0$ implica $a^{-1}>0$.

Passemos a introduzir a noção de *valor absoluto*. Ainda como em (II, 3, 2), o símbolo $|a|$ representará o valor absoluto de a. Poremos, por definição, $|0|=0$; $|a|>0$, se $a\neq 0$; e $|a|=-a$, se $a<0$, $|a|=a$, se $a>0$.

Resultam daqui as relações seguintes:

$$(1)\qquad |ab|=|a|\cdot|b|,\quad |a+b|\leqq|a|+|b|.$$

Se um dos elementos, a ou b, é nulo, as duas fórmulas são imediatas. Admitindo que isso não acontece, suponhamos, por exemplo, $a<0$, $b<0$. Então, $|a|=-a$, $|b|=-b$, e $|ab|=ab=(-a)\cdot(-b)=|a|\cdot|b|$. Quanto à segunda fórmula, se $a>0$, $b>0$, tem-se $|a+b|=a+b=|a|+|b|$; se $a<0$, $b<0$, vem $|a+b|=-(a+b)=-a-b=|a|+|b|$. Resta, assim, o estudo do caso em que a e b têm «sinais» contrários. Suponhamos $a>0$, $b<0$. Tem-se

$$a+b<a<a+|b|=|a|+|b|,$$

$$-(a+b)<-b<a+|b|=|a|+|b|,$$

consequentemente $|a+b|<|a|+|b|$. A segunda fórmula (1) está justificada.

Da fórmula (1) resulta que o «quadrado» dum elemento não nulo é sempre positivo. De facto, tendo-se $a^2=(-a)^2$, é $a^2=|a|\cdot|a|>0$. Em particular, é $u^2=u>0$, como já sabiamos.

TEOREMA: *A característica dum corpo ordenado nunca pode ser finita.* Se fôsse $pu=u+\cdots+u=0$, estariamos em contradição com a propriedade O'_3).

2) **A ordenação dos números racionais** — Em (II, 3, 1) e (II, 3, 2), reconhecemos que havia um único processo de ordenar o domínio de integridade dos inteiros, por forma a manter a ordenação dos números naturais. Aqui, vamos reconhecer que há um único processo de ordenar o corpo dos números racionais, por forma a manter a ordenação dos números inteiros.

Em primeiro lugar, devendo ter-se $u=1>0$, os números inteiros positivos deverão ser também positivos no sentido da ordenação de $\mathfrak{R}_0$. Afirmação correspondente se faz, para os números inteiros negativos.

Dado, agora, um número racional $[a,b]$, de representante (a,b), também frequentemente escrito $\frac{a}{b}$, podemos imaginar sempre que o inteiro b é positivo; e isto porque, supondo $b<0$, escreveremos $[-a,-b]$, em vez de $[a,b]$. Então, mediante tal hipótese, como se tem $\frac{a}{b}\cdot b=a$, deverá ter-se $\frac{a}{b}>0$, sempre que $a>0$; e, sempre que $a<0$, deverá ser $\frac{a}{b}<0$. Finalmente, será $\frac{a}{b}>\frac{c}{d}$, se $\frac{a}{b}-\frac{c}{d}=\frac{ad-bc}{bd}>0$, isto é, se $ad-bc>0$, ou $ad>bc$. Os raciocínios feitos, ao mesmo tempo que mostram a unicidade da ordenação dos números racionais, mostram também, de modo fácil, a existência duma tal ordenação.

3) **Corpos ordenados arquimedianos** — Um corpo ordenado $\mathfrak{K}$ recebe o nome de corpo ordenado *arquimediano* (ou corpo arquimediano), se, dados os seus elementos positivos a e b, existir um número natural n tal que $na > b$. Também pode dizer-se: 1) $\mathfrak{K}$ é arquimediano, se e só se, tomado $\varepsilon > 0$, existir um número natural n tal que $nu > \varepsilon$; 2) $\mathfrak{K}$ é arquimediano, se e só se, tomado $\varepsilon > 0$, existir um número natural n tal que $0 < \frac{u}{nu} < \varepsilon$. [Dum modo geral, se a e $b \neq 0$ são elementos dum corpo, o símbolo $\frac{a}{b}$ significa ab^{-1}].

Verifiquemos, por exemplo, a equivalência entre a definição inicial e a definição 1). A passagem da definição inicial a 1) é imediata. Reciprocamente, partindo de 1), tomemos $a > 0$, de sorte que $ba^{-1} > 0$. Então, de $nu > ba^{-1}$, para um certo n, passa-se a $na > b$, como se deseja.

TEOREMA: *O corpo ordenado $\mathfrak{R}_0$ dos números racionais é arquimediano.* Tomados os dois números racionais $[a,b]$ e $[c,d]$, nos quais $b > 0$, $d > 0$, pretendemos provar que, supostos $a > 0$, $c > 0$, existe n, tal que $n[a,b] > [c,d]$. Como $n[a,b] = [na,b]$, tudo está em se estabelecer que $nad > bc$, para um certo n. O algoritmo de divisão tratado em (II, 3, 2) leva a $bc = ad \cdot q + r$, com $0 \leqslant r < ad$. Então, tem-se $bc = ad \cdot q + r < ad \cdot q + ad = ad(q+1)$. Este resultado mostra que basta tomar $n = q + 1$, para se chegar à conclusão desejada.

Se um corpo ordenado é não arquimediano, existem elementos $b > 0$ tais que, por maior que seja n, nunca se tem $nu > b$. São elementos «infinitamente grandes». Também pode dizer-se que há elementos ε positivos «infinitamente pequenos», isto é, tais que, por maior que seja n, nunca se tem $\frac{u}{nu} < \varepsilon$.

4) **Valorizações** — Se $\mathfrak{K}$ é um corpo ordenado qualquer e $\mathfrak{Q}$ um segundo corpo ordenado, define-se uma *valorização* em $\mathfrak{K}$, dando uma aplicação $a \to \Phi(a)$, de $\mathfrak{K}$ em $\mathfrak{Q}$, de tal modo que se tenha: $V_1)$ $\Phi(0) = 0$; $V_2)$ $\Phi(a) > 0$, se $a \neq 0$; $V_3)$ $\Phi(ab) = \Phi(a) \cdot \Phi(b)$; $V_4)$ $\Phi(a+b) \leqq \Phi(a) + \Phi(b)$.

Um primeiro exemplo de valorização é dado quando se introduz num corpo ordenado a noção de valor absoluto. Nesse caso, $\mathfrak{K}$ e $\mathfrak{Q}$ coincidem. Também se obtém uma valorização de $\mathfrak{K}$, pondo, para cada $a \in \mathfrak{K}$, $\Phi(a) = 1 \in \mathfrak{Q}$ e $\Phi(0) = 0 \in \mathfrak{Q}$. Esta valorização diz-se *trivial*. Pode provar-se o seguinte

TEOREMA: — *Um corpo ordenado finito só admite a valorização trivial.* A demonstração assenta sobre este

LEMA: — *Se $\mathfrak{K}$ é um corpo ordenado, a condição* $a^n = u$, *implica* $a = u$, *suposto* $a > 0$. Na verdade, por exemplo, se fosse $a < u$, a hipótese $a^{n-1} < u$ implicaria $a^n < u$, porque, de $a^{n-1} < u$, $a > 0$, se tiraria $a^{n-1} \cdot a = a^n < a < u$.

Passando ao teorema, tomemos um elemento arbitrário $x \in \mathfrak{K}$, não nulo. Como o corpo é finito, existe um número natural t tal que $x^t = u$. Então, sendo $\Phi(x^t) = [\Phi(x)]^t = \Phi(u)$, assim como $\Phi(u) = \Phi(u \cdot u) = [\Phi(u)]^2$, vê-se que $\Phi(u) = 1$, $[\Phi(x)]^t = 1$, $\Phi(x) = 1$, pois $\Phi(x) > 0$.

Para um corpo valorizado qualquer, tem-se $[\Phi(-u)]^2 = \Phi(u) = 1$, de sorte que $\Phi(-a) = \Phi(-u \cdot a) = \Phi(-u) \cdot \Phi(a) = \Phi(a)$.

Da relação $\Phi(a+b) \leqq \Phi(a) + \Phi(b)$, substituindo a por $a - b$, deduzimos $\Phi(a - b + b) = \Phi(a) \leqq \Phi(a-b) + \Phi(b)$, de sorte que $\Phi(a) - \Phi(b) \leqq \Phi(a-b)$. Também se vê que $\Phi(b) - \Phi(a) \leqq \Phi(a-b)$, pelo que podemos escrever sempre

$$|\Phi(a) - \Phi(b)| \leqq \Phi(a-b),$$

que é uma relação a ter em conta.

Para darmos um exemplo de valorização não trivial, consideremos o corpo $\mathfrak{R}_0$ dos números racionais e, tomado $a \in \mathfrak{R}_0$, não nulo, escrevamos

$a = \frac{r}{s} p^m$, com r e s inteiros não múltiplos do número primo p.

Se pusermos $\Phi(a) = p^{-m}$, $\Phi(0) = 0$, têm lugar as propriedades $V_1)$ a $V_4)$. Em particular, com $b = \frac{t}{v} p^n$, se admitirmos que é $m \geqq n$, tem-se

$$a + b = \frac{rvp^m + tsp^n}{sv} = \frac{rvp^{m-n} + ts}{sv} p^n,$$

o que leva a $\Phi(a+b) \lesseqgtr \Phi(a)+\Phi(b)$. O mesmo resultado se obteria, supondo $m \lesseqgtr n$. Esta valorização diz-se *valorização ádica-p* de $\mathfrak{R}_0$.

5) **Sucessões fundamentais** — Tomemos o corpo ordenado $\mathfrak{K}$, valorizado por intermédio do corpo $\mathfrak{Q}$. Diremos que uma sucessão $\{a_n\}$, $(a_n \in \mathfrak{K},\ n=1,2,\cdots)$, é uma *sucessão fundamental*, se, tomado $\varepsilon > 0$, $(\varepsilon \in \mathfrak{Q})$, existir um número natural n_ε tal que $\Phi(a_p - a_q) < \varepsilon$, sempre que $p > n_\varepsilon, q > n_\varepsilon$. É válido este

TEOREMA 1: *Uma sucessão fundamental é limitada superiormente.* Significa-se com isso que é possível encontrar um elemento $\mu \in \mathfrak{Q}$ tal que, para todos os elementos da sucessão $\{a_n\}$, se tenha $\Phi(a_n) < \mu$. Na verdade, de $a_p = a_q + (a_p - a_q)$, conclui-se $\Phi(a_p) \lesseqgtr \Phi(a_q) + \Phi(a_p - a_q)$, pelo que, tomado $q = n_0 > n_\varepsilon$, se obtem $\Phi(a_p) < \Phi(a_{n_0}) + \varepsilon$, se $p > n_0$. Pondo $\Phi(a_{n_0}) + \varepsilon = \mu_0$ e considerando $\sum_{i=1}^{n_0-1} \Phi(a_i)$, o elemento $\mu = \mu_0 + \sum_{i=1}^{n_0-1} \Phi(a_i) \in \mathfrak{Q}$ é tal que $\Phi(a_n) < \mu$, qualquer que seja n.

Se $\{a_n\}$ e $\{b_n\}$ forem duas sucessões fundamentais, mostraremos, em seguida, que $\{a_n\} + \{b_n\} = \{a_n + b_n\}$ é uma sucessão fundamental (chamada *soma*) e que $\{a_n\} \cdot \{b_n\} = \{a_n b_n\}$ é igualmente uma sucessão fundamental (chamada *produto*).

Pondo $a_n + b_n = c_n$, pretende-se ver que, dado $\varepsilon > 0$, é possível determinar n_ε, por forma que seja $\Phi(c_p - c_q) > \varepsilon$, quando $p > n_\varepsilon$, $q > n_\varepsilon$. Ora, tendo-se $c_p - c_q = (a_p - a_q) + (b_p - b_q)$, é $\Phi(c_p - c_q) \lesseqgtr \Phi(a_p - a_q) + \Phi(b_p - b_q)$. Então, supondo $\Phi(a_p - a_q) < \frac{\varepsilon}{2}$, quando $p > n_1$, $q > n_1$, e $\Phi(b_p - b_q) < \frac{\varepsilon}{2}$, quando $p > n_2$, $q > n_2$, reconhece-se que, designando por n_ε o maior dos números n_1 e n_2, é $\Phi(c_p - c_q) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$, se $p > n_\varepsilon, q > n_\varepsilon$. [Bem entendido que $\frac{\varepsilon}{2}$ é uma forma abreviada de escrever $\frac{\varepsilon}{2u}$, onde $u = 1 \in \mathfrak{Q}$].

Quanto ao produto, pondo $d_n = a_n b_n$, pretende-se ver que $\Phi(d_p - d_q) < \varepsilon$, se $p > n_\varepsilon$, $q > n_\varepsilon$, com $\varepsilon > 0$. Ora, tendo-se $d_p - d_q = a_p b_p - a_q b_q = a_p(b_p - b_q) + (a_p - a_q) b_q$, se designármos

por μ_1 e μ_2, respectivamente, «limites» superiores de $\{a_n\}$ e de $\{b_n\}$, e se supusermos

$$\Phi(b_p - b_q) < \frac{\varepsilon}{2\mu_1}, \qquad \Phi(a_p - a_q) < \frac{\varepsilon}{2\mu_2},$$

quando $p > n_\varepsilon$, $q > n_\varepsilon$, vemos que

$$\Phi(d_p - d_q) < \mu_1 \frac{\varepsilon}{2\mu_1} + \mu_2 \frac{\varepsilon}{2\mu_2} = \varepsilon, \quad \text{se } p > n_\varepsilon,\ q > n_\varepsilon.$$

O produto de duas sucessões fundamentais é, na verdade, uma sucessão fundamental.

Entre as sucessões fundamentais, podemos destacar aquelas para as quais $a_n = a \in \mathfrak{K}$, qualquer que seja n. De resto, um número finito de elementos duma sucessão fundamental pode ser alterado de modo arbitrário, sem que deixe de tratar-se duma sucessão fundamental. A sucessão fundamental para a qual $a_n = 0$, (n qualquer), é elemento zero para a soma de sucessões fundamentais. Tem lugar o teorema a seguir, de demonstração muito simples, na parte não demonstrada:

TEOREMA 2: — *As sucessões fundamentais constituem um anel comutativo.*

6) **O corpo derivado de $\mathfrak{K}$** — Uma sucessão fundamental chama-se uma *sucessão nula*, se, tomado $\varepsilon > 0$, existir n_ε tal que $\Phi(a_p) < \varepsilon$, quando $p > n_\varepsilon$. Tem lugar a importante proposição seguinte:

TEOREMA 1: *As sucessões nulas formam um ideal do anel das sucessões fundamentais.* A afirmação é consequência de provarmos que a diferença de duas sucessões nulas é uma sucessão nula e que o produto duma sucessão nula por uma sucessão fundamental qualquer é uma sucessão nula. Tomemos as sucessões nulas $\{a_n\}$ e $\{b_n\}$. Então

$$\Phi(a_p) < \frac{\varepsilon}{2}, \qquad \Phi(b_p) < \frac{\varepsilon}{2}, \quad \text{quando } p > n_\varepsilon,$$

onde n_ε é convenientemente escolhido. Como

$$\Phi(a_p - b_p) \lesseqgtr \Phi(a_p) + \Phi(-b_p) = \Phi(a_p) + \Phi(b_p) < \varepsilon,$$

se $p > n_\varepsilon$, concluímos que, de facto, $\{a_n - b_n\}$ é uma sucessão nula.

Em segundo lugar, sejam $\{a_n\}$ uma sucessão nula e $\{b_n\}$ uma sucessão fundamental qualpuer. Tendo-se $\Phi(b_p) < \mu$, qualquer que seja p, e $\Phi(a_p) < \frac{\varepsilon}{\mu}$ quando $p > n_\varepsilon$, vê-se

$$\Phi(a_p b_p) = \Phi(a_p)\,\Phi(b_p) < \mu \cdot \frac{\varepsilon}{\mu} = \varepsilon, \quad \text{quando } p > n_\varepsilon,$$

de sorte que $\{a_n b_n\}$ é uma sucessão nula. O teorema fica deste modo estabelecido.

Designando por $\mathfrak{A}$ o anel das sucessões fundamentais e por $\mathfrak{n}$ o ideal das sucessões nulas, é válido este outro

TEOREMA 2: *O anel diferença* $\mathfrak{A}/\mathfrak{n} = \Omega$ *é um corpo.* Designemos por $\alpha, \beta, \cdots$ as classes $\{a_n\} + \mathfrak{n}$, $\{b_n\} + \mathfrak{n}$, etc. Mostraremos que a equação $\alpha\xi = \beta$, de incógnita ξ, é solúvel. se a classe α não for a classe das sucessões nulas. Assentaremos os raciocínios no seguinte

LEMA: *Se* $\{a_n\}$ *é uma sucessão fundamental não nula, existem* $\varepsilon_0 > 0$, *assim como um número natural* n_0, *tal que* $\Phi(a_n) > \varepsilon_0$, *quando* $n > n_0$. Se assim não acontecesse, tomado qualquer $\varepsilon > 0$, por maior que fosse o número natural N, haveria sempre $k > N$ tal que $\Phi(a_k) < \frac{\varepsilon}{2}$. Mas, sendo $\Phi(a_p) \leqq \Phi(a_k) + \Phi(a_p - a_k)$, tomemos N suficientemente grande, para que, sendo $p > N$, $k > N$, seja $\Phi(a_p - a_k) < \frac{\varepsilon}{2}$. Ter-se-ia, então, $\Phi(a_p) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$, quando $p > N$, e $\{a_n\}$ seria uma sucessão nula, contra a hipótese.

Regressemos ao teorema. Na equação em causa, $\alpha\xi = \beta$, suposto $\alpha = \{a_n\} + \mathfrak{n}$ e admitindo que, quando $n > n_0$, é $\Phi(a_n) > \varepsilon_0$, podemos imaginar a classe α representada por $\{a_{n_0+1}, \cdots, a_{n_0+1}, a_{n_0+1}, a_{n_0+2}, \cdots\}$, por forma que, para qualquer a_p, seja $\Phi(a_p) > \varepsilon_0$. Nessas condições, $\{a_{n_0+1}^{-1}, \cdots, a_{n_0+1}^{-1}, a_{n_0+2}^{-1} \cdots\}$ é também uma sucessão fundamental. Na verdade, dado $\varepsilon > 0$, imaginemos que se tem $\Phi(a_p - a_q) < \varepsilon\,\varepsilon_0^2$, quando $p > n$, $q > n$. Será, necessàriamente, nas mesmas condições, $\Phi(a_p^{-1} - a_q^{-1}) < \varepsilon$, pois que, se, para um certo $p > n$ e um certo $q > n$, fosse $\Phi(a_p^{-1} - a_q^{-1}) \geqq \varepsilon$, do facto de se ter $a_p - a_q = a_p a_q \cdot (a_q^{-1} - a_p^{-1})$, deduzir-íamos $\Phi(a_p - a_q) = \Phi(a_p)\,\Phi(a_q)\,\Phi(a_p^{-1} - a_q^{-1}) > \varepsilon_0^2\,\varepsilon$, o que não pode ter lugar. Designando por α^{-1} a classe de representante $\{a_n^{-1}\}$,

a equação $\alpha\xi = \beta$ tem a solução $\alpha^{-1}\beta$, que é uma sucessão fundamental, por ser o produto de duas sucessões fundamentais. O teorema está provado.

As classes da forma $\alpha = \{a_n\} + \mathfrak{n}$, com $a_n = a$, qualquer que seja n, formam uma parte de Ω, parte que constitui um corpo isomorfo de $\mathfrak{K}$. Ω, que é, assim, uma extensão de $\mathfrak{K}$, diz-se *corpo derivado* de $\mathfrak{K}$ (por via da valorização Φ).

7) **Corpos completos** — Um corpo $\mathfrak{K}$, com uma valorização Φ, diz-se *completo*, se o corpo derivado Ω correspondente for igual a $\mathfrak{K}$. Por outras palavras: $\mathfrak{K}$ é completo, se toda a classe $\alpha = \{a_n\} + \mathfrak{n}$ tiver um representante da forma $\{a'_n\}$, com $a'_n = a$, qualquer que seja n. Neste caso, as duas sucessões fundamentais $\{a_1, \cdots, a_n, \cdots\}$, $\{a, \cdots, a, \cdots\}$ têm uma diferença que é uma sucessão nula. É $\Phi(a_p - a) < \varepsilon$, se $p > n_\varepsilon$, com n_ε convenientemente escolhido. Diz se, então, que a sucessão $\{a_n\}$, de elementos de $\mathfrak{K}$, *converge* para $a \in \mathfrak{K}$, e escreve-se, simbòlicamente,

$$\lim_{n\to\infty} a_n = a. \tag{1}$$

Pode perguntar-se, todavia, se não poderá acontecer que, num corpo completo, existam sucessões não fundamentais $\{b_n\}$ para as quais $\Phi(b_p - b) < \varepsilon$, para cada $\varepsilon > 0$ tomado arbitràriamente, contanto que $p > n_\varepsilon$, com n_ε convenientemente escolhido. A este respeito, tem lugar o seguinte

TEOREMA 1: *Num corpo completo, é condição necessária e suficiente, para que uma sucessão seja convergente, que seja uma sucessão fundamental.* Se uma sucessão é fundamental, é convergente, por definição. Inversamente, se $\{b_n\}$ é uma sucessão convergente e tem o «limite» b, é $\{b_n - b\}$ uma sucessão nula. Então, de $b_n = b + (b_n - b)$, conclui-se que é uma sucessão fundamental.

A noção de convergência (ou de limite), independentemente do facto de $\mathfrak{K}$ ser ou não completo, é dada sempre nos mesmos termos: escreveremos

$$\lim_{n\to\infty} a_n = a, \text{ se e só se } \Phi(a_p - a) < \varepsilon, \text{ quando } p > n_\varepsilon.$$

TEOREMA 2: *Uma sucessão* $\{a_n\}$ *não pode ter dois limites distintos.* Se a e a' fossem esses limites, ter-se-ia $\Phi(a-a')=\eta>0$. Por outro lado, escolhendo n_η convenientemente, seria

$$\Phi(a-a')\leqq\Phi(a-a_p)+\Phi(a_p-a')<\frac{\eta}{2}+\frac{\eta}{2}=\eta,$$

se $p>n_\eta$. Cai-se, pois, num absurdo, admitindo a existência de dois limites distintos.

No caso particular de se introduzir no corpo ordenado $\mathfrak{K}$ a valorização $\Phi(a)=|a|$, tem lugar este

TEOREMA 3: *Se* $\mathfrak{K}$ *é um corpo ordenado, o seu corpo derivado* Ω, *obtido pela valorização definida por via do valor absoluto introduzido em* $\mathfrak{K}$, *é também um corpo ordenado. A ordenação de* $\mathfrak{K}$ *é mantida em* Ω. Mostraremos que as propriedades $0'_1)$, $0'_2)$, $0'_3)$, referidas em (V, 3, 1), são válidas em Ω. Quanto a $0'_1)$, verificaremos que os elementos duma sucessão fundamental não nula têm um «sinal» determinado, a partir de certa ordem. Tomada $\{a_n\}$, não nula, o lema de (V, 3, 6) afirma que $|a_n|>\varepsilon_0$, quando $n>n_1$. Sendo, porém, $|a_p-a_q|<\varepsilon_0$, quando $p>n_0$, $q>n_0$, vê-se que, escolhido N convenientemente, é $|a_p-a_q|<\varepsilon_0$, $|a_n|>\varepsilon_0$, quando $p>N$, $q>N$, $n>N$. Então, nas condições indicadas, tem-se

$$|a_p-a_q|<|a_n|,\quad |a_p-a_{N+1}|<|a_{N+1}|,\quad (p>N).$$

Conclui-se daqui que, se for $a_{N+1}>0$, é também $a_p>0$, pois a hipótese $a_p<0$, para um certo $p>N$, daria $|a_p-a_{N+1}|=-a_p+a_{N+1}>a_{N+1}$; e também se conclui que $a_{N+1}<0$ leva a $a_p<0$. O sinal de a_p, quando $p>N$, é o sinal de a_{N+1}.

Feito isto, $0'_1)$ está satisfeita em Ω, considerando *positivas* aquelas classes de sucessões fundamentais constituídas por sucessões que «acabam» por ser compostas de elementos positivos, e considerando *negativas* aquelas classes de sucessões fundamentais constituídas por sucessões que «acabam» por ser compostas de elementos negativos. Vê-se imediatamente, com efeito, por via da igualdade $a_p=b_p+(a_p-b_p)$, que, se uma classe contém uma sucessão que acaba por elementos positivos, o mesmo acontece com qualquer outra sucessão da mesma classe, e que uma situação análoga se encontra para as sucessões que acabam por elementos negativos.

Quanto às propriedades $0'_2)$ e $0'_3)$, elas são agora imediatas em Ω, por serem válidas em $\mathfrak{K}$.

Só resta reconhecer que a ordenação de $\mathfrak{K}$ é mantida em Ω. Isso resulta do facto de Ω ser uma extensão de $\mathfrak{K}$. O teorema tem um aditamento que daremos depois de certas

OBSERVAÇÕES: Como esclarecimento à terminologia e aos raciocínios acabados de usar, faremos algumas observações 1.ª) Ao falarmos de classes positivas, devemos entender, de modo preciso, aquelas classes constituídas por sucessões que acabam por ser compostas de elementos superiores a um elemento positivo fixo conveniente. As classes negativas serão aquelas para as quais as classes constituídas pelas sucessões simétricas são positivas. Quando se escreve $a_p=b_p+(a_p-b_p)$ e se supõe $a_p>\varepsilon_0>0$, para $p>n_0$, então, se $\{a_n-b_n\}$ é uma sucessão nula, podemos imaginar n_0 suficientemente grande para que, quando $p>n_0$, nunca possa ter-se $b_p\leqq 0$. Nessas condições, imaginando que $|a_p-b_p|<\varepsilon_{0/2}$, quando $p>n_1$, será $b_p>\varepsilon_{0/2}$, quando $p>n_2$, se n_2 é convenientemente escolhido. E isto porque, se, por maior que fosse $n>n_0,n_1$, existisse $k>n$ tal que $b_k\leqq\varepsilon_{0/2}$, então seria $a_k<\varepsilon_{0/2}+\varepsilon_{0/2}=\varepsilon_0$, o que não tem lugar. 2.ª) Quando se diz que $0'_2)$ é válida em Ω por o ser em $\mathfrak{K}$, na verdade significa-se que, pondo $\alpha=\{a_n\}+\mathfrak{n}$, $\beta=\{b_n\}+\mathfrak{n}$, $\alpha-\beta=\{a_n-b_n\}+\mathfrak{n}$, é do facto de se poderem comparar em $\mathfrak{K}$ os elementos a_n e b_n, para qualquer n, que vai resultar a afirmação. Assim, se a classe $\alpha-\beta$ for positiva, escreve-se $\alpha-\beta>0$, ou $\alpha\not<\beta$.

Passemos agora ao citado

ADITAMENTO: *Se* $\mathfrak{K}$ *é arquimediano,* Ω *é arquimediano.* A justificação faz-se como segue. Tomado $\{a_n\}+\mathfrak{n}=\alpha\in\Omega$ e admitindo que $\{a_n\}$ é uma sucessão «positiva», o facto de $\{a_n\}$ ser limitada superiormente por um elemento $k\in\mathfrak{K}$ implica $\alpha\leqq k$. Então, supondo $nu>k$, é também $nu>\alpha$.

Tem interesse verificar que, independentemente de $\mathfrak{K}$ e Ω serem arquimedianos, dado $\varepsilon\in\Omega$, $(\varepsilon>0)$, existe $\varepsilon_0\in\mathfrak{K}$, $(\varepsilon_0>0)$, tal que $\varepsilon_0\leqslant\varepsilon$, (agora considerado $\varepsilon_0\in\Omega$). Na verdade, ponhamos $\frac{1}{\varepsilon}=\tau\in\Omega$ e designemos por $\{t_n\}$ uma sucessão fundamental de elementos de $\mathfrak{K}$ definindo τ. Se supomos $t_n>0$ para qualquer n, sabemos que se tem $t_n<k$, para um certo $k\in\mathfrak{K}$. Então, $\{k-t_n\}$ ou é uma sucessão fundamental nula ou define uma classe positiva. Tem-se $\tau\leqq k$, consequentemente $k^{-1}=\varepsilon_0\leqq\varepsilon$.

Estamos agora em condições de provar a importante proposição que vai seguir-se, conhecida pelo nome de

TEOREMA DE CONVERGÊNCIA DE CAUCHY: *Dado um corpo ordenado* $\mathfrak{K}$, *qualquer, o corpo derivado* Ω, *obtido pela valorização definida por via do valor absoluto introduzido em* $\mathfrak{K}$, *é um corpo completo, em face da valorização igualmente definida por via do valor absoluto introduzido em* Ω. Bem entendido que há lugar para se introduzirem em Ω as noções de valor absoluto, de sucessão fundamental e de sucessão nula, as duas últimas tendo precisamente em conta a noção de valor absoluto. Então, o teorema de CAUCHY resulta das considerações de que passamos a ocupar-nos.

Em primeiro lugar, visto que é $\mathfrak{K} \subseteq \Omega$, tomemos uma sucessão $|a_n|$ de elementos de $\mathfrak{K}$ formando uma sucessão fundamental, e suponhamos $\alpha \in \Omega$ o elemento $|a_n| + \mathfrak{n}$. Se considerármos $a_1, a_2, \cdots$ como elementos de Ω, vamos provar que se tem

$$\lim_{n\to\infty} a_n = \alpha. \tag{2}$$

Duma maneira mais explícita, vamos ver que é

$$|a_p - \alpha| < \varepsilon, \text{ para cada } \varepsilon > 0, \ (\varepsilon \in \Omega), \text{ se } p > n_\varepsilon.$$

Seja $\varepsilon_0 \in \mathfrak{K}$ um elemento para o qual se tem $\varepsilon_0 \geqq \varepsilon$. Se supusermos que é $|a_p - a_q| < \varepsilon_0$, quando $p > n_0$, $q > n_0$, é também, em Ω, $|a_p - a_q| < \varepsilon$, quando $p > n_\varepsilon$, $q > n_\varepsilon$, com $n_\varepsilon = n_0$. Estudemos agora $|a_p - \alpha|$. Sendo $\alpha = |a_n| + \mathfrak{n}$, vê-se que, logo que, na sucessão $a_1, a_2, \cdots$, se tome a_p, com $p > n_\varepsilon$, é já $|a_p - \alpha| < \varepsilon_0 \geqq \varepsilon$. A relação (2) é válida. A sucessão $|a_n - \alpha|$ é fundamental.

Em segundo lugar, vamos mostrar que toda a sucessão fundamental de elementos de Ω define uma «constante», no sentido que indica a igualdade (1) deste número: dada uma sucessão fundamental $|\alpha_n|$, existe uma sucessão fundamental $|\alpha'_n|$, com $\alpha'_n = \alpha$, qualquer que seja n, de tal modo que $|\alpha_p - \alpha| < \varepsilon$, para cada ε dado, se for $p > n_\varepsilon$, com n_ε conveniente. Se a sucessão $|\alpha_n|$ for formada de elementos iguais a partir duma certa ordem, a afirmação é trivial. Não acontecendo assim, podemos suprimir em $|\alpha_n|$ todo o elemento que seja igual ao que o precede, formando uma sucessão parcial $|\beta_n|$ para

a qual vamos verificar a afirmação. Daí resultará a convergência de $|\alpha_n|$.

Ponhamos $|\alpha_p - \alpha_{p+1}| = \gamma_p$. A sucessão $|\gamma_p|$ é uma sucessão nula, formada de elementos positivos. Se $|a_1^{(p)}, a_2^{(p)}, \cdots|$ é uma sucessão fundamental de elementos de $\mathfrak{K}$ definindo α_p, já sabemos que se pode encontrar $a_i^{(p)}$ por forma que $|a_i^{(p)} - \alpha_p| < \gamma_p$, quando $i > n_p$. Fixemos i nessas condições e façamos $a_i^{(p)} = a_p$. Então, é $|a_p - \alpha_p| < \gamma_p$. Dado $\varepsilon \in \Omega$, $(\varepsilon > 0)$, escolhamos n_1 por forma que, quando $p > n_1$, seja $\gamma_p < \frac{\varepsilon}{3}$. Isto é possível, por ser $|\gamma_p|$ uma sucessão nula. Por outro lado, escolhendo n_2 de tal modo que, quando $p > n_2$, $q > n_2$, se tenha $|\alpha_p - \alpha_q| < \frac{\varepsilon}{3}$, vê-se que, de $a_p - a_q = (a_p - \alpha_p) + (\alpha_p - \alpha_q) + (\alpha_q - a_q)$, se conclui, escolhendo n convenientemente,

$$|a_p - a_q| < \varepsilon, \quad p > n, \ q > n.$$

A sucessão $|a_n|$ é uma sucessão fundamental de elementos de $\mathfrak{K}$, pois que, escolhido ε, poderíamos ter passado a $\varepsilon_0 \in \mathfrak{K}$, em termos indicados antes de se iniciar a demonstração do teorema. Tem-se $\lim_{n\to\infty} a_n = \alpha$. Pelo facto de ser

$$\alpha_p = a_p + (\alpha_p - a_p),$$

é também $\lim_{p\to\infty} \alpha_p = \alpha$. O teorema de CAUCHY está provado.

8) **Os números reais** — Partindo do corpo ordenado arquimediano $\mathfrak{N}_0 = \mathfrak{K}$ dos números racionais, o teorema de convergência de CAUCHY estabelece que o derivado Ω correspondente é um corpo completo. $\Omega = \mathfrak{N}$ diz-se, então, o *corpo dos números reais*. O aditamento ao teorema 3 mostra, de seu lado, que $\mathfrak{N}$ é um corpo arquimediano.

A circunstância de $\mathfrak{N}_0$ e $\mathfrak{N}$ serem arquimedianos permite estabelecer uma nova propriedade, muito importante, contida na proposição geral seguinte:

TEOREMA: *No corpo* Ω, *suposto arquimediano e obtido nos termos indicados no teorema de* CAUCHY, *todo o conjunto* $\mathfrak{C} \subseteq \Omega$, *que seja majorado, tem limite superior*. Designemos por v um majorante de $\mathfrak{C}$

e tomemos $\gamma \in \mathfrak{C}$. Dado $u = 1 \in \Omega$, escreveremos $mu = m$, quando m é um número natural. Então, existe $m > -\gamma$, de sorte que é $-m < \gamma < v < M$, sendo M um número natural conveniente. Feito isto, consideremos os números naturais, e, para cada um deles, p por exemplo, supondo que r percorre igualmente os números naturais, fixemos os números racionais da forma $\frac{r}{2^p}$, para os quais $-m \leqq \frac{r}{2^p} \leqq M$. De entre esses números racionais (entre os quais figura sempre $M = \frac{M \cdot 2^p}{2^p}$ e que são em número finito), retenhamos aquele número racional a_p mínimo que seja «majorante» de $\mathfrak{C}$. Quando se passa de p a um número natural $q > p$, a fim de encontrar a_q, a circunstância de se ter $\frac{r}{2^p} = \frac{r \cdot 2^{q-p}}{2^q}$ mostra que, no cálculo de a_q, intervêm todos os $\frac{r}{2^p}$, pelo que é $a_q \gtreqless a_p$. Como $a_p - \frac{1}{2^p}$ já não é um majorante de $\mathfrak{C}$, somos levados à condição

$$a_p - \frac{1}{2^p} < a_q \gtreqless a_p , \tag{1}$$

da qual se deduz $|a_p - a_q| < \frac{1}{2^p}$. Desde que é $q > p$, vê-se que, supondo $p > n$, $q > n$, é $|a_p - a_q| < \frac{1}{2^n}$. Para cada $\varepsilon \in \Omega$, existe um número natural $s > \frac{1}{\varepsilon}$, portanto existe n tal que $2^n > \frac{1}{\varepsilon}$, ou seja tal que $\varepsilon > \frac{1}{2^n}$. Então, a condição $|a_p - a_q| < \varepsilon$, quando $p > n$, $q > n$, implica que a sucessão $\{a_p\}$ seja uma sucessão fundamental de elementos de Ω, definindo um número $\alpha \in \Omega$, $(\lim_{p \to \infty} a_p = \alpha)$. O elemento α é um majorante de $\mathfrak{C}$, visto que, se existisse $\delta \in \mathfrak{C}$ tal que $\delta > \alpha$, ter se-ia $\delta - \alpha > 0$ e existiria $2^t > (\delta - \alpha)^{-1}$, ou seja, ser-se-ia levado a $\delta - \alpha > \frac{1}{2^t}$, em que t é um certo número natural. Viria depois $a_t - \frac{1}{2^t} + \frac{1}{2^t} = a_t < \delta - \alpha + \alpha = \delta$, por ser $a_t - \frac{1}{2^t} \gtreqless \alpha$, como se reconhece tendo em conta (1) e a definição de α. O resultado $a_t < \delta$ é absurdo. Resta ver que α gosa da propriedade do limite superior. Se, na verdade, β fosse um majorante de $\mathfrak{C}$ para o qual valesse $\beta < \alpha$, pondo $\alpha - \beta > \frac{1}{2^x}$, em que x é um certo número natural, e tomando $\gamma > a_x - \frac{1}{2^x}$ (o que é possível, pelo facto de $a_x - \frac{1}{2^x}$ não ser um majorante de $\mathfrak{C}$), chegariamos a $a_x - \frac{1}{2^x} < \gamma < \beta$. Então, $a_x - \frac{1}{2^x} + \frac{1}{2^x} < \beta + \alpha - \beta$, ou seja $a_x < \alpha$, o que não tem lugar, em virtude do seguinte: por via de (1), fixado $p = x$, para cada $y > x$, é $a_y \gtreqless a_x$; consequentemente, é $\alpha \gtreqless a_x$. A demonstração está acabada. Pode dizer-se ainda: *num corpo arquimediano completo (para o valor absoluto), todo o conjunto limitado superiormente tem um limite superior.* Daqui o

COROLÁRIO: *Num corpo arquimediano completo (para o valor absoluto), toda a sucessão monotonamente crescente, limitada superiormente, é convergente.* O limite da sucessão é o seu limite superior.

Terminaremos este número com a observação de que, de futuro, sempre que tenhamos de utilizar números reais, admitiremos para estes as diferentes propriedades conhecidas.

9) **Números complexos** — Tomemos o produto cartesiano $\mathfrak{R} \times \mathfrak{R}$ de elementos (a, b), onde a e b são, portanto, números reais. A algebrização do produto por via de soma e de produto definidos pelas igualdades

$$(a, b) + (c, d) = (a + c, b + d),$$
$$(a, b) \cdot (c, d) = (ac - bd, ad + bc),$$

leva ao *corpo dos números complexos*. O elemento $(0, 0)$ é o zero da soma. Supondo $(a, b) \neq (0, 0)$, a equação

$$(a, b) \cdot (x, y) = (c, d)$$

tem a solução

$$(x, y) = \left(\frac{ac + bd}{a^2 + b^2}, \frac{ad - bc}{a^2 + b^2} \right).$$

BIBLIOGRAFIA

B. L. VAN DER WAERDEN, *Moderne Algebra*, erster Teil, 3.ª edição, 1950.
H. HASSE, *Höhere Algebra*, «Lineare Gleichungen», 2.ª edição, Berlim, 1933.
A. ALMEIDA COSTA, *Elementos da Teoria dos Anéis*, Porto, Centro de Estudos Matemáticos, 1943.
N. JACOBSON, *Lectures in Abstract Algebra*, vol. I, 1951.
E. STEINITZ, *Algebraische Theorie der Körper*, «Journal für die reine und angewandte Mathematik», Band 137, 1910.
A. ALMEIDA COSTA, *Sobre a Teoria dos Anéis e Ideais não comutativos*, tomo 1.º das «Actas do XIII Congresso Luso-Espanhol para o Progresso das Ciências», Lisboa, 1950.
A. ADRIAN ALBERT, *Modern Higher Algebra*, Chicago, 1936.
P. DUBREIL, Algèbre, Paris, 1954.

CAPÍTULO VI

Anéis primos e semi-primos. Anéis de ideais principais. Anéis de polinómios. Corpos

§ 1. Anéis primos e semi-primos

1) **Anéis primos e ideais primos** — Um anel $\mathfrak{S}$ diz-se *primo*, se, supostos $\mathfrak{a}$ e $\mathfrak{b}$ ideais de $\mathfrak{S}$, a igualdade $\mathfrak{a}\mathfrak{b}=(0)$ implicar $\mathfrak{a}=(0)$ ou $\mathfrak{b}=(0)$. Representando por $a, b, \cdots$ os elementos de $\mathfrak{S}$, sem dúvida que a hipótese de $ab=0$ levar a $a=0$ ou $b=0$ arrasta que $\mathfrak{S}$ seja primo. De facto, partindo dela, ponhamos $\mathfrak{a}\mathfrak{b}=(0)$ e admitamos que se tem $\mathfrak{a}\neq(0)$, $\mathfrak{b}\neq(0)$. Podem encontrar-se elementos não nulos $a\in\mathfrak{a}$ e $b\in\mathfrak{b}$ tais que $ab=0$, o que é uma contradição. Em (V, 1, 2) mostrámos que os domínios de integridade são precisamente caracterizados pela condição de $ab=0$ implicar $a=0$ ou $b=0$. *Os domínios de integridade são, pois, anéis primos.*

No caso comutativo, os anéis primos e os domínios de integridade coincidem. Na verdade, então, é válida a igualdade $(a)(b)=(ab)$, onde, como em (V, 2, 4), um símbolo da forma (x) significa ideal gerado por x. Nessas condições, para um anel primo comutativo, de $ab=0$, conclui-se $(ab)=(0)=(a)(b)$, e, portanto, conclui-se $(a)=(0)$ ou $(b)=(0)$, donde $a=0$ ou $b=0$.

Da definição de anel primo, resulta a proposição a seguir, que estende o teorema 2, de (V, 2, 1).

TEOREMA 1: *A característica dum anel primo é um número primo, se não for zero.* Designando por n a característica, se, supondo $n \neq 0$, pudesse ter-se $n = pq$, com $p, q \neq 1$, obteriamos $n\mathfrak{S} = (0)$, $n\mathfrak{S}^2 = p\mathfrak{S} \cdot q\mathfrak{S} = (0)$, o que implicaria $p\mathfrak{S} = (0)$ ou $q\mathfrak{S} = (0)$, contra a hipótese de a característica ser n.

Do facto dum anel primo comutativo ser um domínio de integridade, resulta o seguinte

TEOREMA 2: *O centro dum anel primo, quando não é* (0), *é um domínio de integridade.* Na verdade, sejam $\mathfrak{z}_1$ e $\mathfrak{z}_2$ dois ideais do centro e suponhamos $\mathfrak{z}_1 \mathfrak{z}_2 = (0)$. Os ideais $(\mathfrak{z}_1, \mathfrak{z}_1\mathfrak{S})$ e $(\mathfrak{z}_2, \mathfrak{z}_2\mathfrak{S})$, de $\mathfrak{S}$, gerados por $\mathfrak{z}_1$ e $\mathfrak{z}_2$, são, de facto, bilaterais. Como o seu produto é (0), um deles será (0). Ou se tem, pois, $\mathfrak{z}_1 = (0)$ ou é $\mathfrak{z}_2 = (0)$.

Supondo agora $\mathfrak{A}$ um anel qualquer, $\mathfrak{g}$ diz-se um *ideal primo*, se o anel diferença $\mathfrak{A}/\mathfrak{g} = \overline{\mathfrak{A}}$ for primo. É válido o teorema a seguir:

TEOREMA 3: *É condição necessária e suficiente, para que o ideal* $\mathfrak{g}$ *seja primo, que a condição* $\mathfrak{a}\mathfrak{b} \equiv 0(\mathfrak{g})$ *implique* $\mathfrak{a} \equiv 0(\mathfrak{g})$ *ou* $\mathfrak{b} \equiv 0(\mathfrak{g})$. Se $\mathfrak{g}$ é primo, como no homomorfismo $\mathfrak{A} \sim \overline{\mathfrak{A}}$ a imagem de $\mathfrak{a}\mathfrak{b}$ é $\overline{\mathfrak{a}}\,\overline{\mathfrak{b}} = (0)$, resulta $\overline{\mathfrak{a}} = (0)$ ou $\overline{\mathfrak{b}} = (0)$, e, portanto, resulta $\mathfrak{a} \equiv 0(\mathfrak{g})$ ou $\mathfrak{b} \equiv 0(\mathfrak{g})$. Inversamente, a validade da condição do enunciado mostra que, tomados os ideais $\overline{\mathfrak{a}}$ e $\overline{\mathfrak{b}}$, de $\overline{\mathfrak{A}}$, se supusermos $\overline{\mathfrak{a}}\,\overline{\mathfrak{b}} = (0)$, então, designando por $\mathfrak{a}$ e $\mathfrak{b}$ dois ideais de $\mathfrak{A}$ que tenham aqueles por imagens no homomorfismo $\mathfrak{A} \sim \overline{\mathfrak{A}}$, segue-se $\mathfrak{a}\mathfrak{b} \equiv 0(\mathfrak{g})$, donde se conclui que um dos ideais $\mathfrak{a}$ ou $\mathfrak{b}$ está contido em $\mathfrak{g}$, e que, portanto, um dos ideais $\overline{\mathfrak{a}}$ ou $\overline{\mathfrak{b}}$ é o ideal nulo. [Nesta demonstração, o leitor deve ter presentes os resultados estabelecidos em (IV, 1, 2).

Se o anel $\mathfrak{A}$ *é comutativo, um ideal* $\mathfrak{g}$ *é primo, se e só se* $\mathfrak{A}/\mathfrak{g}$ *for um domínio de integridade; ou ainda:* $\mathfrak{g}$ *é primo, se e só se a condição* $\mathrm{a}\,\mathrm{b} \equiv 0(\mathfrak{g})$ *implica* $\mathrm{a} \equiv 0(\mathfrak{g})$ *ou* $\mathrm{b} \equiv 0(\mathfrak{g})$.

Um *ideal* $\mathfrak{a}$ dum anel qualquer diz-se *nilpotente*, se existir uma potência $\mathfrak{a}^\sigma$, em que σ é um número natural, tal que $\mathfrak{a}^\sigma = (0)$. Um anel primo não tem ideal nilpotente $\neq (0)$. Diz-se muitas vezes que um anel não tem ideal nilpotente, quando o seu único ideal nilpotente é o ideal nulo.

Aos raciocínios que se seguem, interessa este

LEMA: *Se* $\mathfrak{P}$ *é um ideal bilateral dum anel* $\mathfrak{A}$ *tal que* $\mathfrak{A}/\mathfrak{P}$ *não tem ideal nilpotente, é condição necessária e suficiente, para que* $\mathrm{a} \in \mathfrak{P}$, *que* $\mathrm{a}\mathfrak{A} \subseteq \mathfrak{P}$. É imediato que a condição é necessária. Inversamente, se $a\mathfrak{A} \subseteq \mathfrak{P}$, seja $\mathfrak{r}$ o ideal direito gerado por a. Como $\mathfrak{r}^2$ se compõe de elementos da forma $\sum (as + ia)(as' + i'a)$, $(s, s' \in \mathfrak{A}$; i, i' inteiros), vê-se que $\mathfrak{r}^2 \subseteq a\mathfrak{A} \subseteq \mathfrak{P}$. Então, sendo $\mathfrak{r}'$ o correspondente de $\mathfrak{r}$ no homomorfismo $\mathfrak{A} \sim \mathfrak{A}/\mathfrak{P}$, vê-se que $\mathfrak{r}'^2 = (0)$, $\mathfrak{r}' = (0)$. Daqui tira-se $\mathfrak{r} \subseteq \mathfrak{P}$, $a \in \mathfrak{P}$, como se afirma no enunciado.

Voltemos aos anéis primos. Em face do lema, se $\mathfrak{g}$ é um ideal primo, tem-se $a \in \mathfrak{g}$, se e só se $a\mathfrak{A} \subseteq \mathfrak{g}$, (ou $\mathfrak{A}a \subseteq \mathfrak{g}$). Resulta imediatamente que $a \in \mathfrak{g}$, se e só se $\mathfrak{A}a\mathfrak{A} \equiv 0(\mathfrak{g})$. De facto, a hipótese $\mathfrak{A}a\mathfrak{A} \equiv 0(\mathfrak{g})$ arrasta $\mathfrak{A}a \equiv 0(\mathfrak{g})$, consequentemente $a \equiv 0(\mathfrak{g})$.

Suposto $\mathfrak{g}$ representar sempre um ideal primo, vamos ver que, de $a\mathfrak{A}b \equiv 0(\mathfrak{g})$, se conclui $a \equiv 0(\mathfrak{g})$ ou $b \equiv 0(\mathfrak{g})$. Na verdade é, então, $\mathfrak{A}a\mathfrak{A} \cdot \mathfrak{A}b\mathfrak{A} \equiv 0(\mathfrak{g})$, consequentemente $\mathfrak{A}a\mathfrak{A} \equiv 0(\mathfrak{g})$ ou $\mathfrak{A}b\mathfrak{A} \equiv 0(\mathfrak{g})$. Logo, ou é $a \in \mathfrak{g}$ ou $b \in \mathfrak{g}$. Fixaremos esta proposição:

TEOREMA 4: *Tomado o ideal primo* $\mathfrak{g}$, *é condição necessária e suficiente, para que* $\mathrm{a} \in \mathfrak{g}$, *que se realize qualquer das condições seguintes:* $\mathrm{a}\mathfrak{A} \subseteq \mathfrak{g}$, $\mathfrak{A}\mathrm{a} \subseteq \mathfrak{g}$, $\mathfrak{A}\mathrm{a}\mathfrak{A} \subseteq \mathfrak{g}$. *E, de* $\mathrm{a}\mathfrak{A}\mathrm{b} \equiv 0(\mathfrak{g})$, *conclui-se* $\mathrm{a} \equiv 0(\mathfrak{g})$ *ou* $\mathrm{b} \equiv 0(\mathfrak{g})$.

No que respeita pròpriamente à caracterização dos ideais primos, vamos dar alguns critérios.

TEOREMA 5: *É condição necessária e suficiente, para que o ideal* $\mathfrak{g}$ *seja primo, que a relação* $(\mathrm{a}\mathfrak{A})(\mathrm{b}\mathfrak{A}) \equiv 0(\mathfrak{g})$ *implique* $\mathrm{a} \equiv 0(\mathfrak{g})$ *ou* $\mathrm{b} \equiv 0(\mathfrak{g})$. A condição é *necessária*: Se $\mathfrak{g}$ é primo, de $(a\mathfrak{A})(b\mathfrak{A}) \equiv 0(\mathfrak{g})$, tira-se $\mathfrak{A}a\mathfrak{A} \cdot \mathfrak{A}b\mathfrak{A} \equiv 0(\mathfrak{g})$, consequentemente, como já se viu, $a \equiv (\mathfrak{g})$ ou $b \equiv 0(\mathfrak{g})$.

A condição é *suficiente:* Se $(a\mathfrak{A})(b\mathfrak{A}) \equiv 0(\mathfrak{g})$ implica $a \in \mathfrak{g}$ ou $b \in \mathfrak{g}$, ponhamos $\mathfrak{a}\mathfrak{b} \equiv 0(\mathfrak{g})$, com $\mathfrak{a} \not\equiv 0(\mathfrak{g})$. Em seguida, tome-se $a_1 \in \mathfrak{a}$, $a_1 \notin \mathfrak{g}$ e, bem assim, um elemento arbitrário $b_1 \in \mathfrak{b}$. Tem-se $(a_1\mathfrak{A})(b_1\mathfrak{A}) \equiv 0(\mathfrak{g})$, e, como $a_1 \notin \mathfrak{g}$, será $b_1 \in \mathfrak{g}$. Assim, $\mathfrak{b} \subseteq \mathfrak{g}$, como se deseja.

Dos teoremas 4 e 5 e da definição de ideal primo, deduzem-se os dois corolários que vamos dar.

COROLÁRIO 1: *É condição necessária e suficiente, para que o ideal* $\mathfrak{g}$ *seja primo, que* $\mathrm{a}\mathfrak{A}\mathrm{b} \equiv 0(\mathfrak{g})$ *implique* $\mathrm{a} \equiv 0(\mathfrak{g})$ *ou* $\mathrm{b} \equiv 0(\mathfrak{g})$. Já

vimos, no teorema 4, que a condição é necessária. Vamos mostrar que é suficiente. Se $a\mathfrak{A}b \equiv O(\mathfrak{g})$ implica $a \equiv O(\mathfrak{g})$ ou $b \equiv O(\mathfrak{g})$, então, suposto $(a\mathfrak{A})(b\mathfrak{A}) \equiv O(\mathfrak{g})$, ou é $b\mathfrak{A} \equiv O(\mathfrak{g})$ ou $a \equiv O(\mathfrak{g})$. Se se realiza a primeira conclusão, obtem-se $b\mathfrak{A}b \equiv O(\mathfrak{g})$, portanto $b \equiv O(\mathfrak{g})$.

COROLÁRIO 2: *É condição necessária e suficiente, para que o ideal* $\mathfrak{g}$ *seja primo, que, dados dois ideais direitos arbitrários* $\mathfrak{r}_1$ *e* $\mathfrak{r}_2$, *tais que* $\mathfrak{r}_1\mathfrak{r}_2 \equiv 0(\mathfrak{g})$, *seja* $\mathfrak{r}_1 \equiv 0(\mathfrak{g})$ *ou* $\mathfrak{r}_2 \equiv 0(\mathfrak{g})$. A suficiência da condição é imediata. A necessidade vem deste modo: Tomemos $\mathfrak{r}_1\mathfrak{r}_2 \equiv O(\mathfrak{g})$ e admitamos $\mathfrak{r}_2 \not\equiv O(\mathfrak{g})$. Seja $b \in \mathfrak{r}_2$, $b \notin \mathfrak{g}$, e consideremos $a \in \mathfrak{r}_1$. Será $a\mathfrak{A}b \equiv O(\mathfrak{g})$, o que leva a $a \in \mathfrak{g}$. Ora a é arbitrário em $\mathfrak{r}_1$, pelo que $\mathfrak{r}_1 \subseteq \mathfrak{g}$. [No enunciado, podemos substituir ideais direitos por ideais esquerdos].

2) **Sobre a construção de ideais primos** — O próprio anel $\mathfrak{A}$ é sempre um ideal primo. Quanto à exiitência de autros ideais primos, começaremos pelo teorema e pelo corolário que passamos a estabelecer.

TEOREMA 1: *Se os ideais* $\mathfrak{s}$ *e* $\mathfrak{q}$ *são tais que* $\mathfrak{s} \supset \mathfrak{q}$, *nenhum ideal existindo entre* $\mathfrak{s}$ *e* $\mathfrak{q}$, *então, o conjunto* $\mathfrak{g}$ *dos elementos* $p \in \mathfrak{A}$, *tais que* $p\mathfrak{s} \subseteq \mathfrak{q}$, *é um ideal primo.* É imediato que $\mathfrak{g} \supseteq \mathfrak{q}$ é um ideal. Para se ver que é primo, suponhamos $\mathfrak{a}\mathfrak{b} \equiv O(\mathfrak{g})$, com $\mathfrak{a} \not\equiv O(\mathfrak{g})$, $\mathfrak{b} \not\equiv O(\mathfrak{g})$. Como se tem $\mathfrak{a}\mathfrak{b}\mathfrak{s} \equiv O(\mathfrak{q})$, $\mathfrak{b}\mathfrak{s} \not\equiv O(\mathfrak{q})$, vê-se que $\mathfrak{q} \subset (\mathfrak{q}, \mathfrak{b}\mathfrak{s}) \subseteq \mathfrak{s}$, consequentemente, à face das hipóteses sobre $\mathfrak{s}$, conclui-se $(\mathfrak{q}, \mathfrak{b}\mathfrak{s}) = \mathfrak{s}$, $(\mathfrak{a}\mathfrak{q}, \mathfrak{a}\mathfrak{b}\mathfrak{s}) = \mathfrak{a}\mathfrak{s} \subseteq \mathfrak{q}$, $\mathfrak{a} \subseteq \mathfrak{g}$, o que é um absurdo. Um dos ideais $\mathfrak{a}$ ou $\mathfrak{b}$ tem de estar contido em $\mathfrak{g}$.

COROLÁRIO 1: *Se* $\mathfrak{s} \supset (O)$ *é um ideal mínimo de* $\mathfrak{s}$ *(isto é, se não contém qualquer ideal além do ideal nulo e do próprio* $\mathfrak{s}$*), o ideal* $\mathfrak{g}$, *conjunto dos elementos* p, *tais que* $p\mathfrak{s} = (O)$, *é um ideal primo.*

Em correlação com os raciocínios em causa, provaremos agora este

TEOREMA 2: *Se* $\mathfrak{s}$ *é um ideal de* $\mathfrak{A}$ *e* $\mathfrak{g}$ *é um ideal primo do mesmo anel, a intersecção* $\mathfrak{s} \cap \mathfrak{g}$ *é o ideal primo do anel* $\mathfrak{s}$. Claramente que um ideal dum anel é, em si. um anel. Então, justificaremos a afirmação, provando que, supostos $x_1, x_2 \in \mathfrak{s}$, a relação $x_1\mathfrak{s}x_2 \equiv O(\mathfrak{s} \cap \mathfrak{g})$ implica $x_1 \in \mathfrak{s} \cap \mathfrak{g}$ ou $x_2 \in \mathfrak{s} \cap \mathfrak{g}$. De facto, tendo-se $\mathfrak{A}x_2\mathfrak{A} \subseteq \mathfrak{s}$, é, por hipótese, $x_1\mathfrak{A}x_2\mathfrak{A}x_2 \equiv O(\mathfrak{g})$, o que implica $x_1 \equiv O(\mathfrak{g})$ ou

$x_2\mathfrak{A}x_2 \equiv O(\mathfrak{g})$. A primeira implicação leva a $x_1 \in \mathfrak{s} \cap \mathfrak{g}$, enquanto que a segunda leva a $x_2 \equiv O(\mathfrak{g})$, consequentemente a $x_2 \in \mathfrak{s} \cap \mathfrak{g}$.

COROLÁRIO 2: *Um ideal dum anel primo é um anel primo.* Reconhece-se fazendo $\mathfrak{g} = (O)$ no teorema acabado de demonstrar.

Terminaremos este número aproveitando uma sugestão fornecida pelo corolário 1, de (VI, 1, 1). Um conjunto M, contido no anel $\mathfrak{A}$, diz-se um *sistema-m*, se, supostos a e b pertencentes a M, existir $x \in \mathfrak{A}$ tal que $axb \in M$. Dado, então, um ideal primo $\mathfrak{g}$, se $c, d, \ldots$ são elementos do conjunto complementar $C(\mathfrak{g})$, de $\mathfrak{g}$, em $\mathfrak{A}$, sabemos, pelo referido corolário, que $c\mathfrak{A}d \not\equiv O(\mathfrak{g})$. Existe, assim, $x \in \mathfrak{A}$ tal que $cxd \in C(\mathfrak{g})$, o que prova ser $C(\mathfrak{g})$ um sistema-m. Inversamente, o complementar dum sistema-m, suposto um ideal, é um ideal primo. Fixaremos o

TEOREMA 3: *É condição necessária e suficiente, para que o ideal* $\mathfrak{g}$, *de* $\mathfrak{A}$, *seja um ideal primo, que o conjunto complementar* $C(\mathfrak{g})$, *de* $\mathfrak{g}$, *em* $\mathfrak{A}$, *seja um sistema-m.*

OBSERVAÇÃO: Os subconjuntos de $\mathfrak{A}$ fechados para a operação de produto constituem sistemas-m.

3) **Anéis semi-primos e ideais semi-primos** — Um anel $\mathfrak{S}$ diz-se *semi-primo*, se suposto $\mathfrak{a}$ ideal de $\mathfrak{S}$, a igualdade $\mathfrak{a}^2 = (O)$ implicar $\mathfrak{a} = (O)$. Os diferentes raciocínios que aqui vamos fazer inspiram-se nos dos dois números anteriores. Onde apareciam dois ideais diferentes $\mathfrak{a}$ e $\mathfrak{b}$, aparecem agora dois ideais iguais; e, onde apareciam dois elementos diferentes a e b, aparecem agora dois elementos iguais.

A definição afirma que um anel semi-primo é aquele que não tem ideais nilpotentes. São semi-primos os anéis primos, assim como os anéis para os quais $a^2 = 0$ implica $a = 0$, suposto $a \in \mathfrak{S}$. No caso comutativo, é condição necessária e suficiente, para que $\mathfrak{S}$ seja anel semi-primo, que não tenha elementos nilpotentes.

A característica dum anel semi-primo não pode ser um quadrado perfeito, assim como não pode ser múltipla do quadrado dum número primo $\neq 1$. O centro dum anel semi-primo é um anel sem elementos nilpotentes, salvo o elemento zero.

Supondo agora $\mathfrak{A}$ um anel qualquer, $\mathfrak{x}$ diz-se um *ideal semi-primo*, se o anel diferença $\mathfrak{A}/\mathfrak{x}$ for semi-primo. É válido o seguinte

TEOREMA 1: *É condição necessária e suficiente, para que* $\mathfrak{x}$ *seja ideal semi-primo, que a condição* $\mathfrak{a}^2 \subseteq \mathfrak{x}$ *implique* $\mathfrak{a} \subseteq \mathfrak{x}$. A demonstração faz-se nos moldes da do teorema 3, de (VI, 1, 1). E isso sucede, em geral, para as diferentes proposições que enunciarmos.

Se $\mathfrak{x}$ é ideal semi-primo, $\mathfrak{A}/\mathfrak{x}$ não tem ideais nilpotentes. Então, será $a \in \mathfrak{x}$, se e só se $a\,\mathfrak{A} \subseteq \mathfrak{x}$ (ou $\mathfrak{A}\,a \subseteq \mathfrak{x}$). Resulta imediatamente que $a \in \mathfrak{x}$, se e só se $\mathfrak{A}\,a\,\mathfrak{A} \subseteq \mathfrak{x}$. Suposto $\mathfrak{x}$ representar sempre um ideal semi-primo, vamos ver que. de $a\,\mathfrak{A}\,a \equiv 0(\mathfrak{x})$, se conclui $a \equiv 0(\mathfrak{x})$. Na verdade é, então, $\mathfrak{A}\,a\,\mathfrak{A} \cdot \mathfrak{A}\,a\,\mathfrak{A} \equiv 0(\mathfrak{x})$, ou seja $\mathfrak{A}\,a\,\mathfrak{A} \equiv 0(\mathfrak{x})$.

No que respeita pròpriamente à caracterização dos ideais semi-primos, fixaremos alguns critérios.

TEOREMA 2: *E condição necessária e suficiente, para que o ideal* $\mathfrak{x}$ *seja semi-primo, que a relação* $(\mathfrak{a}\,\mathfrak{A})^2 \equiv 0(\mathfrak{x})$ *implique* $\mathfrak{a} \equiv 0(\mathfrak{x})$. Este teorema corresponde ao teorema 5, de (VI, 1, 1).

COROLÁRIO 1: *É condição necessária e suficiente, para que o ideal* $\mathfrak{x}$ *seja semi-primo, que, dado um ideal direito* $\mathfrak{r}$ *tal que* $\mathfrak{r}^2 \equiv 0(\mathfrak{x})$, *seja* $\mathfrak{r} \equiv 0(\mathfrak{x})$. Este corolário corresponde ao corolário 2 de (VI, 1, 1).

COROLÁRIO 2: *É condição necessária e suficiente, para que o ideal* $\mathfrak{x}$ *seja semi-primo, que* $a\,\mathfrak{A}\,a \equiv 0(\mathfrak{x})$ *implique* $a \equiv 0(\mathfrak{x})$. Este corolário corresponde ao corolário 1, de (VI, 1, 1).

Tal como no caso dos aneis primos, também tem aqui interesse reconhecer que é válido este

TEOREMA 3: *Se* $\mathfrak{a}$ *é um ideal de* $\mathfrak{A}$ *e* $\mathfrak{x}$ *é um ideal semi-primo do mesmo anel, a intersecção* $\mathfrak{a} \cap \mathfrak{x}$ *é um ideal semi-primo do anel* $\mathfrak{a}$. Desenvolvamos agora a demonstração. Temos de mostrar que, sendo $a \in \mathfrak{a}$, de $a\,\mathfrak{a}\,a \equiv 0(\mathfrak{a} \cap \mathfrak{x})$, se conclui $a \in \mathfrak{a} \cap \mathfrak{x}$. Ora, tendo-se $a\,\mathfrak{a}\,a \equiv 0(\mathfrak{a} \cap \mathfrak{x})$, é $a(\mathfrak{A}\,a\,\mathfrak{A})\,a \subseteq a\,\mathfrak{a}\,a \subseteq \mathfrak{x}$, portanto $(a\,\mathfrak{A})^5 \equiv 0(\mathfrak{x})$. Vem $(a\,\mathfrak{A})^4 \equiv 0(\mathfrak{x})$, $(a\,\mathfrak{A})^2 \equiv 0(\mathfrak{x})$, $a\,\mathfrak{A} \equiv 0(\mathfrak{x})$, $a \equiv 0(\mathfrak{x})$, consequentemente $a \equiv 0(\mathfrak{a} \cap \mathfrak{x})$.

COROLÁRIO 3: *Um ideal dum anel semi-primo é um anel semi-primo.*

À semelhança do que fizemos no número anterior, terminaremos este número aproveitando uma sugestão fornecida pela propriedade de $\mathfrak{x}$ ser semi primo, se e só se $a\,\mathfrak{A}\,a \equiv 0(\mathfrak{x})$ implicar $a \equiv 0(\mathfrak{x})$. Um conjunto P, de elementos de $\mathfrak{A}$, diz-se um *sistema* $-p$, se e só se, tomando $c \in \mathfrak{P}$, existir $x \in \mathfrak{A}$ tal que $c\,x\,c \in P$. Tendo em conta o corolário 2, demonstra-se fàcilmente esta proposição:

TEOREMA 4: *É condição necessária e suficiente, para que o ideal* $\mathfrak{x}$ *seja semi-primo, que o seu complementar* $C(\mathfrak{x})$, *em* $\mathfrak{A}$, *seja um sistema-p.*

OBSERVAÇÃO: Todo o sistema-m é um sistema-p. A inversa pode não ser verdadeira. Todavia, é fàcil de construir um sistema-m dentro de cada sistema-p. Seja P o sistema-p e tomemos $y_0 \in P$. Para um certo $s_0 \in \mathfrak{A}$, vem $y_0 s_0 y_0 = y_1 \in P$; em seguida, para um certo $s_1 \in \mathfrak{A}$, vem $y_1 s_1 y_1 = y_2 \in P$, e assim por diante. A sucessão $\{y_0, y_1, y_2, \cdots\}$ é um sistema-m, como se reconhece deste modo: $y_0 s_0 y_0 = y_1$; $y_1 s_1 y_1 = y_2$; $y_0 s_0 y_0 s_1 y_1 = y_2$, $y_1 s_1 y_0 s_0 y_0 = y_2$; $y_2 s_2 y_2 = y_3$, $y_1 s_1 y_1 s_2 y_2 = y_3$, etc.

§ 2. Anéis de ideais principais: Caso não comutativo

1) **Definição** – Sob a designação genérica de *anel de ideais principais*, compreenderemos os anéis, comutativos ou não, que têm elemento um e para os quais todo o ideal direito ou esquerdo é gerado por um elemento (ideal principal).

2) **O algoritmo de divisão** — Dado o anel não comutativo $\mathfrak{A}$, com elemento um, diz-se que existe *algoritmo de divisão* em $\mathfrak{A}$, quando se realizarem as seguintes condições: 1.ª) — Dado um elemento $a \in \mathfrak{A}$, é possível atribuir-lhe um valor absoluto $|a|$, que é um inteiro não negativo; 2.ª) — dados dois elementos quaisquer $a \neq 0$ e b, existem uma *divisão à direita* e uma *divisão à esquerda*, conforme as regras

$$(1) \qquad \begin{cases} b = q\,a + r, \\ |r| < |a|, \end{cases} \qquad \begin{cases} b = a\,q' + r', \\ |r'| < |a|. \end{cases}$$

Quando o anel é comutativo, há coincidência das duas divisões. Em (II, 3, 2), provámos que o anel dos inteiros possui algoritmo de divisão.

É um caso preciso para o qual foi estabelecida a univocidade do algoritmo.

TEOREMA 1: *Um elemento não nulo dum anel* $\mathfrak{A}$ *com algoritmo de divisão não pode ter o valor absoluto igual a zero.* De facto, suposto $a \neq 0$ e $|a| = 0$, a divisão $b = qa + r$, com $|r| < |a|$ seria impossível. O único elemento cujo valor absoluto pode ser nulo é o elemento nulo.

TEOREMA 2: *Num anel* $\mathfrak{A}$ *com algoritmo de divisão, um ideal direito* $\mathfrak{r}$ *é sempre um ideal principal direito.* Se $\mathfrak{r} = (0)$, o teorema é banal. Supondo $\mathfrak{r} \neq (0)$, designemos por $a \neq 0$ um elemento de $\mathfrak{r}$ de valor absoluto mínimo. Se $b \in \mathfrak{r}$ é qualquer, o algoritmo de divisão permite escrever $b = aq' + r'$, com $|r'| < |a|$. Mas, sendo $r' = b - aq' \in \mathfrak{r}$, ter-se-á necessàriamente $r' = 0$, $b = aq'$, $\mathfrak{r} = (a)_d$. Existe um teorema análogo para os ideais esquerdos. Portanto:

TEOREMA 3: *Se* $\mathfrak{A}$ *é um anel não comutativo com algoritmo de divisão, é um anel de ideais principais.*

3) **A teoria do máximo divisor comum** — Seja $\mathfrak{A}$ um anel de ideais principais não comutativo. Supondo $(a)_d$ e $(b)_d$ dois ideais principais direitos de $\mathfrak{A}$, o ideal direito soma é, por hipótese, gerado por um elemento d: $((a)_d, (b)_d) = (d)_d$. Tem-se:

$$(1) \qquad a = dq, \quad b = dq', \quad d = ar + bs,$$

onde $q, q', r, s \in \mathfrak{A}$. Comparando estas igualdades com as igualdades (6) de (II, 3, 2), é natural considerar d como *máximo divisor comum* (m. d. c.) *esquerdo* de a e b. Levanta-se, porém, desde logo, a questão de se saber se não poderá haver mais do que um m. d. c. esquerdo de a e b. A resposta será dada depois do teorema que vai seguir-se:

Suponhamos que o ideal direito $(d)_d$ pode ser gerado por um segundo elemento f. Ter-se-á $f\alpha = d$, $d\beta = f$, $(\alpha, \beta \in \mathfrak{A})$, e, consequentemente, $d\beta\alpha = f\alpha = d$, $f\alpha\beta = d\beta = f$, ou seja $d(\beta\alpha - u) = 0$, $f(\alpha\beta - u) = 0$. Admitindo que $\mathfrak{A}$ não tem divisores de zero, concluir-se-á $\beta\alpha = \alpha\beta = u$. Daqui o

TEOREMA 1: *É condição necessária e suficiente, para que dois elementos* d e f, *dum anel de ideais principais sem divisores de zero, gerem o mesmo ideal principal direito, que se obtenham um do outro por multiplicação, à direita, por um elemento com inverso.*

Diremos que dois elementos de $\mathfrak{A}$, obtidos um do outro como se indica no teorema relativamente a d e f, são *associados esquerdos*. De harmonia com o que já dissemos em (II, 1, 4), introduziremos a designação de *unidades* para todos os elementos com inverso, qualquer que seja o anel em causa.

Regressemos ao m. d. c. esquerdo de a e b. Qualquer elemento gerador de $(d)_d$ é um m. d. c. esquerdo, visto que para ele se podem escrever igualdades análogas a (1). Inversamente, se um elemento $g \in \mathfrak{A}$ é tal que para ele se podem escrever as igualdades (1), com substituïção de d por g, então g é gerador de $(d)_d$. É válido o

TEOREMA 2: *Se* $\mathfrak{A}$ *é um anel de ideais principais sem divisores de zero, o m. d. c. esquerdo de dois elementos* a *e* b *pertencentes a* $\mathfrak{A}$ *é bem determinado, sob a condição de não se distinguirem elementos associados esquerdos.*

A observação feita no final de (II, 3, 2) joga com este teorema. Nas condições indicadas, o m. d. c. esquerdo d pode, de resto, definir-se também, à semelhança do que sucedeu em (II, 3, 2), por meio das duas propriedades seguintes: 1.ª) — divide a e b, à esquerda; 2.ª) — qualquer divisor esquerdo comum a a e b é divisor esquerdo de d. Sem dúvida que d tem estas duas propriedades. Inversamente, se $g \in \mathfrak{A}$ tem as propriedades, então, $(g)_d \supseteq ((a)_d, (b)_d)$, em virtude da primeira; e, pela segunda, o próprio elemento d divide g à esquerda, o que leva a $g = dt$, $(g)_d \subseteq (d)_d$, $(g)_d = (d)_d$. Os elementos d e g são associados esquerdos.

A definição de *m. d. c. direito* de dois elementos é dada de modo análogo.

4) **O algoritmo de Euclides** — Constitui um problema importante o da determinação de condições que caracterizem um anel $\mathfrak{A}$ como anel de ideais principais. É por isso que tem interesse fixar critérios para a existência de algoritmo de divisão. Este algoritmo permite, depois, supondo não haver divisores de zero em $\mathfrak{A}$, dar um processo para se chegar ao m. d. c. esquerdo (ou direito) de dois elementos.

Trata-se das divisões sucessivas ou *algoritmo de* EUCLIDES, a que vamos referir-nos em detalhe. Escrevamos as igualdades a seguir, nas quais $b \neq 0$:

$$\begin{aligned} a &= b\,q_1 + r_1, & \cdots\cdots\cdots\cdots, \\ b &= r_1 q_2 + r_2, & r_{s-3} &= r_{s-2} q_{s-1} + r_{s-1}, \\ r_1 &= r_2 q_3 + r_3, & r_{s-2} &= r_{s-1} q_s + 0, \end{aligned}$$

obtidas por divisões à esquerda, até se chegar a um resto nulo, o que necessàriamente sucederá. Vamos demonstrar que o último divisor esquerdo, r_{s-1}, é um divisor esquerdo de a e b, realizando ainda a última condição expressa na terceira igualdade (1). De facto, vê-se que r_{s-1} divide à esquerda, sucessivamente, $r_{s-2}, r_{s-3}, \cdots, b, a$; em seguida, para se chegar a $r_{s-1} = ar + bs$, basta notar as igualdades seguintes:

$$a - bq_1 = r_1; \quad b = (a - bq_1)q_2 + r_2 \quad \text{ou} \quad -aq_2 + b(u + q_1 q_2) = r_2;$$

$$a - bq_1 = [-aq_2 + b(u + q_1 q_2)]q_3 + r_3$$

ou

$$a(u + q_2 q_3) - b(q_1 + q_3 + q_1 q_2 q_3) = r_3;$$

etc. Chega-se, finalmente, a uma igualdade que contém a, b, r_{s-1} e que é do tipo desejado.

Dentro da mesma ordem de ideias, vamos demontrar um teorema que, embora não seja próprio para o cálculo do m. d. c., serve todavia para o caracterizar.

TEOREMA: *O m. d. c. esquerdo* d, *de dois elementos* a e b, *dum anel não comutativo* $\mathfrak{A}$, *sem divisores de zero e com algoritmo de divisão, é o elemento de valor absoluto mínimo, de entre os elementos não nulos da forma* at + bt', $(t, t' \in \mathfrak{A})$. Na verdade, se r e s realizam o mínimo considerado, ponhamos $d = ar + bs$. Vamos ver que d é divisor esquerdo de a e b. Se d não dividisse a, como é $d \neq 0$, o elemento r_1 da igualdade $a = dq_1 + r_1$, com $|r_1| < |d|$, seria $\neq 0$. Mas, tendo-se $r_1 = a - dq_1 = a - (ar + bs)q_1 = a(u \quad rq_1) + b(\quad sq_1)$, encontraríamos em r_1 um elemento da forma $at + bt'$, com $|r_1| < |d|$, o que seria absurdo. Do mesmo modo se demonstraria que d divide b.

Quanto ao problema de fixar critérios para a existência de algoritmo de divisão, limitar-no-emos a dizer o seguinte: nos números inteiros (caso comutativo), o algoritmo existe e é unívoco; como exemplo não comutativo, verificaremos em (VI, 4, 4), a existência e univocidade do algoritmo para polinómios.

5) **A teoria do menor múltiplo comum** — Sejam $(a)_d$ e $(b)_d$ dois ideais direitos do anel de ideais principais $\mathfrak{A}$. Pondo $(a)_d \cap (b)_d = (f)_d$, vê-se que $f = aq$, $f = bq'$. O elemento f é *múltiplo esquerdo* de a e de b. Qualquer outro múltiplo esquerdo comum daqueles elementos, como g, por exemplo, levando a $g = aq_1$, $g = bq'_1$, mostra ser $(g)_d \subseteq (f)_d$. Então, é $g = fq_2$, pelo que g aparece como múltiplo esquerdo de f. O elemento f goza, assim, das duas propriedades seguintes: 1.ª) é múltiplo esquerdo de a e b; 2.ª) qualquer múltiplo esquerdo de a e b é múltiplo esquerdo de f. De harmonia com o que fizemos já em (II, 3, 2), diremos que f é o *menor múltiplo comum* (*m. m. c.*) *esquerdo* de a e b.

Levanta-se a questão de saber se não poderá haver mais do que um m. m. c. esquerdo de dois elementos. Supondo h outro gerador de $(f)_d$, o teorema 1 de (VI, 2, 3) afirmamo-nos que se tem $h = f\varepsilon$, em que ε é unidade de $\mathfrak{A}$. Então, é também $h = a(q\varepsilon)$, $h = b(q'\varepsilon)$, $(h)_d = (a)_d \cap (b)_d$, aparecendo h como m. m. c. esquerdo. Inversamente, se um elemento h gosa das duas propriedades atribuidas ao m. m. c. esquerdo, tem-se $(h)_d \subseteq (a)_d \cap (b)_d$, em virtude da primeira; e, pela segunda, o próprio elemento f é múltiplo de h, o que levará a $f = ht$, $(f)_d \subseteq (h)_d$, e consequentemente, a $(f)_d = (h)_d$. Logo:

TEOREMA: *Se* $\mathfrak{A}$ *é um anel de ideais principais sem divisores de zero, o m. m. c. esquerdo (ou direito) de dois elementos* a, b $\in \mathfrak{A}$ *é bem determinado, sob a condição de não se distinguirem elementos associados esquerdos.*

§ 3. Anéis de ideais principais: Caso comutativo

1) **Considerações gerais** — Tomemos um domínio de integridade comutativo $\mathfrak{A}$, com elemento um. A noção de unidade é bem conhecida. As noções de *múltiplo* e de *divisor* foram utilizadas no parágrafo anterior, como o foram em (II, 3, 2). Também aqui diremos: dados $a, b \in \mathfrak{A}$, o elemento b é divisor ou *está contido* em a, e este último

é múltiplo ou *contém* b, se existir $d \in \mathfrak{A}$ tal que $a = bd$. O elemento um é divisor de qualquer elemento; e existe um elemento, o elemento nulo, que é divisivel por todos os elementos. [A divisão por $b = 0$, mesmo no caso de ser $a = 0$, não se considera]. Um elemento é sempre divisivel por si mesmo. Os divisores duma unidade são unidades.

Dois elementos a, b tais que $a = b\varepsilon$, em que ε é uma unidade, tal como no parágrafo anterior, também se chamam *associados*.

Diz-se que b é um divisor *autêntico* de a, se for $a = bq$, sem que q seja uma unidade. Neste caso a não pode ser divisor de b. Um elemento a diz-se *primo*, se é diferente de zero e se a sua decomposição num produto exigir que um dos factores seja uma unidade. Vê-se imediatamente que um elemento primo não tem divisores autenticos que não sejam unidades. As unidades entram na definição dos elementos primos; em geral, porém, não se consideram como tal e designam-se simplesmente por unidades.

A existência de elemento um é fundamental, para a maior parte das definições. Se, por exemplo, se tratar do domínio de integridade constituido pelos números pares, um elemento não é divisivel por si mesmo! A noção de divisor autêntico é a simples noção de divisor, não há unidades e falha a noção de elemento primo.

Um domínio de integridade com elemento um é, por exemplo, o anel $\mathfrak{A}$ formado por todos os elementos da forma $a/2^n$, onde a e n são inteiros quaisquer. Cada elemento do domínio pode tomar a forma «reduzida» única $g/2^h$, onde g é um número impar e h um inteiro, pois que uma igualdade $g/2^h = g'/2^{h'}$ daria $g/g' = 2^{h-h'}$, o que só é possível com $g/g' = 1$, $h = h'$. A condição necessária e suficiente, para que $g'/2^{h'}$ divida $g/2^h$ é que g' divida g. As unidades do domínio procuram-se pela condição $g/2^h \cdot x = 1$, o que dá $x = 2^h/g$. Este elemento só pode pertencer ao domínio se for $g = \pm 1$, e pertence, de facto, nesse caso. Assim, será x da forma $\pm 2^n$. Os elementos $\pm 2^n$ formam um grupo multiplicativo. Os elementos associados de b são da forma $\pm 2^n b = \pm 2^n g/2^h = \pm 2^{n'} g$, com n' qualquer. O elemento $8 = 2^3$, por ser uma unidade, pode ou não considerar-se primo. O elemento $6 = 3 \cdot 2$ não pode ser escrito sob a forma de produto, a não ser que um dos factores seja uma unidade: é um elemento primo. O elemento 9 não é primo, pois que $9 = (3 \cdot 2^n) \cdot 3/2^n$. Os elementos primos são todos aqueles que, sob a forma reduzida, têm $g =$ número impar primo, e apenas esses.

Um domínio de integridade comutativo com elemento um diz-se um *domínio euclideano*, quando forem satisfeitas as seguintes condições:

1.ª) Existe a noção de valor absoluto $= |a|$, para cada elemento do domínio, sendo $|a| \neq 0$ inteiro e positivo, se $a \neq 0$; e $|a| = 0$, se $a = 0$; 2.ª) existe algoritmo de divisão; 3.ª) é $|ab| = |a| \cdot |b|$. Os inteiros constituem um domínio euclideano. Veremos outro exemplo em (VI. 4, 5).

O número 3 deste parágrafo é destinado a uma teoria de factorização que pode pôr-se em jogo com certas noções sobre ideais de que vamos ocupar-nos no número próximo. Essas noções estão também ligadas à doutrina tratada no § 1.

2) **Ideais divisores e múltiplos de ideais. Ideais sem divisor** — Continuaremos a supor $\mathfrak{A}$ um anel comutativo. Diz-se que um ideal $\mathfrak{a}$ é *divisível* pelo ideal $\mathfrak{b}$, quando este ideal contém aquele. Diz-se também que $\mathfrak{a}$ é *múltiplo* de $\mathfrak{b}$ e que $\mathfrak{b}$ é *divisor* de $\mathfrak{a}$. Escrevendo $\mathfrak{b} \supseteq \mathfrak{a}$ significa-se, pois, indiferentemente, que o primeiro é divisor do segundo ou que o segundo é múltiplo do primeiro. Se se sabe que o ideal $=$ não pode ter lugar, o divisor ou o múltiplo dizem-se autênticos.

Para se compreenderem bem estas definições, consideremos o anel $\mathfrak{A}$ e tomemos $\mathfrak{a} = (a)$, $\mathfrak{b} = (b)$. Quando $(b) \supseteq (a)$, existe $q \in \mathfrak{A}$ tal que $a = bq$, pois $a \in (b)$. Neste caso, por consequência, (b) divisor de (a) significa, relativamente aos geradores a e b, a divisão entendida no sentido ordinário, utilizada já no parágrafo anterior.

No § 1, estudámos os anéis e os ideais primos. Entre estes últimos, distinguiremos os *ideais sem divisor*, isto é, aqueles ideais que têm como único divisor autêntico o ideal unidade. [Esta definição pode ser entendida também para o caso não comutativo]. Vamos provar o seguinte

TEOREMA: *Se $\mathfrak{A}$ é um anel comutativo com identidade, é condição necessária e suficiente, para que $\mathfrak{a}$ seja um ideal sem divisor, que o anel diferença $\mathfrak{A}/\mathfrak{a}$ seja um corpo.* A condição é *necessária*: Se $\mathfrak{a}$ é sem divisor, consideremos a equação $\overline{a}\,\overline{x} = \overline{b}$, onde $\overline{a} = a + \mathfrak{a} \neq 0$ e $\overline{b} = b + \mathfrak{a}$ é qualquer. O ideal gerado por $\mathfrak{a}$ e a é o próprio anel $\mathfrak{A}$. Assim, b pode tomar a forma $b = \alpha + at$, com $\alpha \in \mathfrak{a}$, $t \in \mathfrak{A}$. Então, é $\overline{b} = \overline{\alpha} + \overline{a}\,\overline{t} = \overline{a}\,\overline{t}$, pelo que a equação é resolvida pondo $\overline{x} = \overline{t}$.

A condição é *suficiente*: Se $\mathfrak{A}/\mathfrak{a}$ é um corpo, tomemos $\mathfrak{b} \supset \mathfrak{a}$. Mostraremos que o ideal $\mathfrak{b}$ é o ideal unidade. Seja $c \in \mathfrak{A}$ arbitrário e consideremos a equação $\overline{b}\,\overline{x} = \overline{c}$, com $\overline{b} \neq 0$, $\overline{b} \in \mathfrak{b}$. Se $\overline{x}$ é a solução, os elementos b, c, x satisfazem à relação $c - bx \in \mathfrak{a}$, de sorte que $c \in \mathfrak{b}$, tendo-se $\mathfrak{A} = \mathfrak{b}$, como se deseja.

As definições de m. d. c. e de m. m. c. podem dar-se para ideais quaisquer dum anel comutativo. Dados os ideais $\mathfrak{a}$ e $\mathfrak{b}$, a soma $(\mathfrak{a},\mathfrak{b})$ é o ideal mínimo contendo $\mathfrak{a}$ e $\mathfrak{b}$. Essa soma é o *m. d. c. dos ideais*. Ela goza das duas propriedades seguintes: 1.ª) forma um ideal divisor de cada um dos ideais dados; 2.ª) qualquer outro ideal nas mesmas condições divide também a soma.

Aplicando as considerações de (VI, 2, 3) ao caso dum anel de ideais principais comutativo sem divisores de zero, reconhece-se que o problema da determinação do m. d. c. de dois elementos é o problema da determinação do m. d. c. de dois ideais.

De modo evidente, passa se ao m. m. c. dos ideais $\mathfrak{a}$ e $\mathfrak{b}$ que vinhamos considerando. O ideal $\mathfrak{a} \cap \mathfrak{b}$ é o ideal máximo contido em $\mathfrak{a}$ e $\mathfrak{b}$. Designa-se por *m. m. c. dos dois ideais*. Ele goza das duas propriedades seguintes: 1.ª) é múltiplo de cada um dos ideais dados; 2.ª) qualquer outro ideal nas mesmas condições é múltiplo de $\mathfrak{a} \cap \mathfrak{b}$.

Aplicando as considerações de (VI, 2, 5) ao caso dum anel de ideais principais comutativo sem divisores de zero, reconhece-se que o problema da determinação do m. m c. de dois elementos é o problema da determinação do m. m. c. de dois ideais.

No § 4 particularizaremos noções e raciocínios do número anterior, deste número e do número seguinte.

3) **A teoria da factorização** — É essencial neste número supor $\mathfrak{A}$ um anel de ideais principais sem divisores de zero.

TEOREMA 1: *Um elemento primo de* $\mathfrak{A}$ *gera um ideal sem divisor.* Seja p o elemento em questão. Se o ideal (p) está contido pròpriamente em (d), tem-se $(p) \subset (d)$ e $p = dk$. O elemento k não pode ser uma unidade, visto que isso acarretaria $(p) = (d)$. Será d uma unidade, e, consequentemente, será $(d) = \mathfrak{A}$, como se deseja.

Considerado o homomorfismo $\mathfrak{A} \sim \overline{\mathfrak{A}} = \mathfrak{A}/(p)$, no qual $\overline{\mathfrak{A}}$ é um corpo, a possibilidade da resolução, em $\overline{\mathfrak{A}}$, da equação $\overline{a}\,\overline{x} = \overline{b}$, se $\overline{a} = \overline{0}$, equivale à possibilidade da resolução da congruência $ax \equiv b\,(p)$, suposto $a \notin (p)$. Ora, existindo elementos $r, r' \in \mathfrak{A}$ tais que $ar + pr' = u$, tem-se $a \cdot rb + p \cdot r'b = b$, obtendo-se para a congruência a solução $x = rb$.

Quando há algoritmo de divisão, o algoritmo de EUCLIDES leva fàcilmente à determinação de r. De facto, das igualdades

$$\begin{aligned} a &= p\,q_1 + r_1, & &\cdots\cdots\cdots\cdots\cdots\cdots, \\ p &= r_1 q_2 + r_2, & r_{s-3} &= r_{s-2}\,q_{s-1} + r_{s-1}, \\ &\cdots\cdots\cdots\cdots, & r_{s-2} &= r_{s-1}\,q_s, \end{aligned}$$

com $r_{s-1} = u$, passa-se, sucessivamente, a partir da relação $r_{s-3} = r_{s-2}\,q_{s-1} + u$, às relações entre (r_{s-4}, r_{s-3}, u), (r_{s-5}, r_{s-4}, u), $\cdots, (p, r_1, u)$, (a, p, u), figurando sempre u sem qualquer coeficiente. A relação entre (a, p, u) será a relação desejada, pois se reveste da forma $ar + ps = u$.

Com as actuais hipóteses sobre $\mathfrak{A}$, podemos, como aliás acabamos de fazer, considerar bem determinado o m. d. c. de dois elementos e chamar elementos *primos entre si* aqueles que têm o elemento um como m. d. c. Para se designar que d é m. d. c. dos elementos a e b, costuma escrever-se $(a, b) = d$. Tem-se, então:

TEOREMA 2: *Se for* $(a, b) = d$, *é* $(ac, bc) = dc$. De facto, supondo $a = dq$, $b = dq'$, $ar + bs = d$, tem-se $ac = dc \cdot q$, $bc = dc \cdot q'$, $ac \cdot r + bc \cdot s = dc$. O teorema está provado.

TEOREMA 3: *Se um elemento* g *divide um produto* ab *e é primo com um dos factores, divide necessàriamente o outro factor.* Por hipótese, é $ab = gq$, com $(b, g) = u$. Então, será também $(ab, ag) = (gq, ag) = a$. O elemento g divide gq e ga, pelo que dividirá o seu m. d. c., que é a.

COROLÁRIO 1: *Se um elemento primo* p *divide um produto* ab, *divide necessàriamente um dos factores.* Na verdade, se p não divide b, é primo com b, e, portanto, divide a.

Estes resultados permitem-nos dar agora a solução geral da congruência $ax \equiv b\,(p)$, acima referida. Supondo x uma solução, uma segunda solução y, dando $ay \equiv b\,(p)$, leva a $a(y - x) \equiv 0\,(p)$, ou $a(y - x) = fp$, $(f \in \mathfrak{A})$. Como $a \notin (p)$, será p primo com a, o que mostra ter-se $y - x = hp$, $(h \in \mathfrak{A})$, ou seja $y = x + ph$. Inversamente, qualquer que seja $h \in \mathfrak{A}$, $y = x + hp$ é solução da congruência, se o for x.

No caso do anel $\mathfrak{J}$ dos inteiros, convém fazer algumas observações. Uma congruência $ax \equiv b\,(f)$ pode reduzir-se sempre ao caso em que $|b| < |f|$, bastando escrever, se $|b| \geqslant |f|$, $b = hf + r$, com

$|r| < |f|$. É, então, condição necessária e suficiente, para que a congruência seja solúvel, que existam inteiros x e y tais que $ax+fy=b$. A resolução desta equação, conhecida sob o nome de *equação* de DIOFANTO, reduz-se ao caso em que a, f, b não têm divisor comum. Supondo realizada essa condição, podemos afirmar: 1.º) Se a e f têm um factor comum, a equação não tem soluções inteiras e a congruência não é solúvel; 2.º) se a e f são primos entre si, há uma infinidade de soluções; duma solução α, β passa-se a todas as outras, pondo $x = \alpha + fh$, $y = \beta - ah$, onde h é um inteiro qualquer.

Entrando pròpriamente na teoria da factorização, chegaremos a provar a possibilidade de decompor cada elemento de $\mathfrak{A}$ em factores primos, à custa dum certo número de teoremas.

TEOREMA 4: *Em* $\mathfrak{A}$, *é finita toda a sucessão de elementos* $a_1, a_2, \cdots$, *suposto cada elemento um divisor autêntico do anterior.* Consideremos, com efeito, os ideais (a_i). Sempre que $j > i$, será $(a_j) \supset (a_i)$, pelo facto de a_j ser divisor autêntico de a_i. O conjunto unido dos ideais (a_i) é um ideal principal (f), estando f contido no referido conjunto unido. Se for, por exemplo, $f \in (a_m)$, não pode haver, na sucessão dos a_i, um elemento de índice superior a m.

TEOREMA 5: *Se, em* $\mathfrak{A}$, *existir um elemento* $a \neq 0$ *que não seja um produto de factores primos, há um divisor autêntico de* a *que não é um produto de factores primos.* O elemento a, por hipótese, nem é uma unidade nem é primo. Pode sempre escrever-se $a = bc$, sem que b ou c sejam unidades. Tanto b como c são divisores autênticos de a. Como a não admite uma decomposição em factores primos, um dos elementos, b ou c, terá, necessàriamente, a mesma propriedade.

TEOREMA 6: *Todo o elemento* $a \neq 0$ *é um produto de factores primos.* Se a não fosse susceptível duma tal decomposição, poder-se-ia formar, em virtude do teorema anterior, uma sucessão infinita de elementos $a_1, a_2, \cdots$, cada um dos quais seria um divisor autêntico do anterior, e todos eles tendo a mesma propriedade que a. O teorema 4 afirma-nos, por outro lado, que isso é impossível. A decomposição de a, a que alude o teorema, existe.

TEOREMA 7: *A decomposição de* $a \in \mathfrak{A}$ *é unívoca.* Carecemos aqui de uma observação. Consideremos o elemento primo p e uma unidade ε. Pode escrever-se $p = p\varepsilon \cdot \varepsilon^{-1}$, ou, simplesmente, $p = p$. Dada,

por consequência, uma decomposição em factores primos, válida para um elemento a, podem substituir-se a essa decomposição outras que contenham os mesmos factores primos, não unidades, e, além disso, factores primos unidades. É claro, de resto, que o produto dum elemento primo por uma unidade é ainda um elemento primo.

Posto isto, sejam as duas decomposições

$$(1) \qquad a = p_1 p_2 \cdots p_s = p'_1 p'_2 \cdots p'_r,$$

nos quais os factores se supõem todos diferentes de unidades, pois se consideram estas fazendo parte dos p_i ou dos p'_j. Isto significa que a também não é uma unidade. O elemento primo p_1 divide o produto $p'_1 \cdots p'_r$, pelo que dividirá p'_1 ou $p'_2 \cdots p'_r$. Se é este último que é dividido, o raciocínio repete-se, até se chegar a estabelecer que p_1 divide um p'_j. Ter-se-á $p_1 = p'_j$, (a menos de unidades). Suponhamos $j = 1$. De (1), conclui-se $p_2 \cdots p_s = \varepsilon' p'_2 \cdots p'_r$, onde ε' é uma unidade. A repetição do raciocínio leva a mostrar que todos os p_i são iguais a certos p'_j, e que, além disso, é $s = r$. O teorema está provado.

Um domínio de integridade com elemento um, no qual haja uma factorização unívoca, pondo de parte unidades, diz-se um *domínio gaussiano.* Os resultados acabados de demonstrar provam este

TEOREMA 8: *Um anel de ideais principais comutativo, sem divisores de zero, é um domínio gaussiano.* E também:

TEOREMA 9: *Um domínio euclideano é um domínio gaussiano.*

4) **Aplicações** — Tal como afirmámos, em (III, 1, 3), para os números inteiros, e, em (V, 3, 8), para os números reais, também admitiremos para os números complexos as diferentes propriedades conhecidas. Limitemo-nos, então, dentro do corpo dos complexos, àqueles números da forma $a + bi$ [maneira de escrever que substitui o símbolo (a, b) indicado em (V, 3, 9)] para os quais a e b são números inteiros. Obtem-se o anel dos *números inteiros de* GAUSS. Nesse anel o ideal $(1+i)$ é primo e as unidades são os números $\pm 1, \pm i$.

Se chamarmos *norma* de $\alpha = a + bi$ o número inteiro $N(\alpha) = a^2 + b^2$, vê-se imediatamente que é válida a igualdade $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$. O elemento zero do domínio tem a norma igual a zero e é o único elemento nessas condições. Pode introduzir-se um algoritmo

de divisão como vai seguir-se. Dados α e $\beta \neq 0$, construamos, no conjunto dos números complexos, o número A' tal que $\alpha = \beta A'$. Pondo $A' = a' + b' i$, designemos por a e b os números inteiros mais próximos de a' e b', respectivamente, e ponhamos $A = a + bi$. Vamos ver que o inteiro de GAUSS $\alpha - A\beta$ tem uma norma inferior à norma de β. É $\alpha - A\beta = (\alpha - A'\beta) + (A' - A)\beta = (A' - A)\beta$. A norma, nos números complexos, define-se como no domínio de integridade dos inteiros de GAUSS, gozando, aliás, das mesmas propriedades. Então, $N(\alpha - A\beta) = N(A' - A) \cdot N(\beta)$. Ora $N(A' - A) = (a' - a)^2 + (b' - b)^2 < 1$, e, portanto, $N(\alpha - A\beta) < N(\beta)$. Pondo $\alpha = A\beta + (\alpha - A\beta)$, o algoritmo de divisão, fica, de facto, introduzido. Podemos dizer:

TEOREMA 1: *O anel dos números inteiros de* GAUSS *é um domínio euclideano, portanto, um domínio gaussiano.*

Num domínio gaussiano qualquer tem-se:

TEOREMA 2: *Se* $\mathfrak{A}$ *é um domínio gaussiano, um elemento indecomponível (isto é, primo) gera um ideal primo e um elemento decomponível gera um ideal que não é primo.* Se p é indecomponível e escrevemos $ab \equiv 0(p)$, deve p figurar como factor em a ou b, e ser, portanto, $a \equiv 0(p)$ ou $b \equiv 0(p)$. Se p é decomponível, pondo $p = ab$, onde a e b são divisores autênticos de p, vê-se que $ab \equiv 0(p)$, sem que se tenha $a \equiv 0(p)$ ou $b \equiv 0(p)$.

Voltemos ao anel $\mathfrak{A}$ de ideais principais, comutativo e sem divisores de zero. É um domínio gaussiano para o qual, no teorema anterior, se pode precisar que todo o elemento primo p gera um ideal sem divisor. [Convém observar, de resto, que o teorema 1 de (VI, 3, 3) é válido mesmo para um anel de ideais principais comutativo qualquer]. O anel diferença $\mathfrak{A}/(p)$ é corpo, existindo, portanto, cociente de classes. Vamos ver, porém, que, sendo $a \in \mathfrak{A}$ um elemento arbitrário, é possível definir ainda, para certas classes, um cociente de classes. É o que resulta dos dois teoremas a seguir.

TEOREMA 3: *No anel diferença* $\mathfrak{A}/(a)$, *se uma classe contém um elemento primo com* a, *todos os elementos da classe são primos com* a. Na verdade, se b e c pertencem à mesma classe módulo (a), tem-se $b - c = at$. Ora, se b é primo com a, é também $ar + bs = u$, com $r, s \in \mathfrak{A}$. Escrevendo $bs - cs = ats$ e $ar + bs = ar + cs + ats = u$, vem $cs + a(r + ts) = u$, o que mostra ser c primo com a.

TEOREMA 4: *O conjunto das classes de* $\mathfrak{A}/(a)$ *compostas de elementos primos com* a *constitui um grupo multiplicativo.* Na verdade: I) a classe que contém u pertence ao conjunto $\mathfrak{C}$, em causa; II) o produto de duas classes de $\mathfrak{C}$ é uma classe de $\mathfrak{C}$, visto que o produto de dois elementos primos com a é um elemento primo com a; III) se b define uma classe C_b, existe uma classe C_c tal que $C_b C_c = C_u$, e isto porque, sendo $bs + ar = u$, pondo $C_c = C_s$, vê-se que $C_b C_s = bs + (a) = u - ar + (a) = u + (a)$.

É também interessante esta outra afirmação:

TEOREMA 5: *O m. d. c. entre* a *e um elemento duma classe de* $\mathfrak{A}/(a)$ *é independente do elemento da classe.* Se, de facto, b e c pertencem a uma mesma classe, tem-se $b - c = ra$. Pondo $(a, b) = d$, a igualdade anterior mostra que d divide c. Como se tem uma relação da forma $as + bt = d$, é igualmente válida a relação $a(s + rt) + ct = d$, e o teorema fica demonstrado.

Regressemos ao teorema 4, suposto $\mathfrak{A} = \mathfrak{J}$ o anel dos inteiros. O anel diferença $\mathfrak{J}/(a)$ contém um número finito de elementos, pelo que o grupo multiplicativo referido no teorema é finito. O número de elementos desse grupo, representado por $\Phi(a)$, é igual ao número dos elementos primos com a e inferiores a a. Φ diz-se *função de* EULER. Vamos estudá-la.

Quando $a = p$ é um número primo, sabemos que $\mathfrak{J}/(p)$ é um corpo com p elementos. Das classes a que se refere o teorema 4 fazem parte todas as classes de $\mathfrak{J}/(p)$, à excepção da classe que contém o zero. Obtem-se $\Phi(p) = p - 1$. Em particular, se $p = 1$, é $\Phi(p) = 0$. Quando a não é primo, suponhamos

$$a = \prod_{i=1}^{m} p_i^{r_i} \tag{1}$$

a sua decomposição em factores primos. Vamos ver que se tem

$$\Phi(a) = a \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right). \tag{2}$$

Consideremos um grupo cíclico composto de a elementos. Se g for o elemento gerador, vimos em (III, 1, 3) que são igualmente geradores todos os elementos da forma g^t, em que t é primo com a. A função $\Phi(a)$ dá também, pois, o número de elementos geradores do

grupo cíclico, suposto $a \neq 1$. Comecemos por admitir $a = p^\nu$, com p primo. No grupo

$$\mathfrak{G} = \{u, g, \cdots, g^{p^\nu - 1}\}, \quad (g^{p^\nu} = u),$$

se for g^k um elemento de ordem inferior a p^ν, ter-se-á $g^{kr} = u$, com $r < p^\nu$. Mas, sendo $kr = p^\nu \cdot n$, com n número natural, e dando-se o caso de p^ν não estar completamente contido em r, vê-se que k é múltiplo de p, inferior a p^ν. Inversamente, um tal número k leva a g^k, que não pode gerar $\mathfrak{G}$, pelo seguinte: se fosse $\mathfrak{G} = \{u, g^k, g^{2k}, \cdots, g^{(p^\nu - 1)k}\}$, com todas as potências distintas, o facto de se ter $k = pt$ levaria a $(g^{pt})^{p^{\nu-1}}$, com $p^{\nu-1} < p^\nu - 1$, o que é impossível. Deste modo, os elementos que não geram $\mathfrak{G}$ são $u, g^p, g^{2p}, \cdots, g^{(p^{\nu-1}-1)p}$, em número de $p^\nu - 1$, e é

$$\Phi(p^\nu) = p^\nu - p^{\nu-1} = p^\nu\left(1 - \frac{1}{p}\right).$$

No caso de ser $a = mn$, em que m e n são primos entre si, diferentes de 1, fácil é de ver que $\Phi(a) = \Phi(m) \cdot \Phi(n)$. De facto, os elementos de $\mathfrak{G}$, de ordem mn, exprimem-se duma maneira única como produtos de elementos de ordens n e m, respectivamente, expressão que tem lugar no grupo cíclico gerado pelo elemento de ordem mn posto em causa, ou seja no próprio grupo $\mathfrak{G}$, como se viu em (III, 1, 5). Visto que, inversamente, o produto de dois elementos comutáveis dum grupo, de ordens m e n, primas entre si, é um elemento de ordem mn, segue-se que os geradores de $\mathfrak{G}$ se obtêm multiplicando todos os elementos de $\mathfrak{G}$ de ordem m por todos os elementos de $\mathfrak{G}$ de ordem n. Ora, qualquer elemento de $\mathfrak{G}$ de ordem m faz parte do grupo cíclico gerado por g^n, pois, se g^k está nessas condições tem-se $g^{km} = u$, $km = mnq$, $k = nq$, $g^k = (g^n)^q$. A igualdade indicada para Φ está demonstrada. Se a tem a decomposição (1), valerá a relação

$$\Phi(a) = \prod_{i=1}^{m} \Phi(p_i^{r_i}) = \prod_{i=1}^{m} p_i^{r_i}\left(1 - \frac{1}{p_i}\right) = a\prod_{i=1}^{m}\left(1 - \frac{1}{p^i}\right),$$

que é a fórmula desejada. Diremos:

TEOREMA 6: *Se o inteiro* a *é diferente de* 1, *o número de elementos primos com* a, *inferiores a* a, *é dado pela relação* (2), *suposta* (1) *a decomposição de* a *em factores primos.*

É oportuno dar agora a seguinte proposição:

TEOREMA 7 (FERMAT): *Se* p *é um número natural primo e* a *é um número natural primo com* p, *tem lugar a congruência* $a^{\Phi(p)} \equiv 1 \pmod{p}$. Tomemos o anel $\mathfrak{I}$ dos inteiros e o corpo $\mathfrak{I}/(p)$. Para cada elemento $\overline{a} = a + (p) \neq 0$, daquele corpo, é válida a relação $\overline{a}^{p-1} = 1 + (p) = a^{p-1} + (p)$, que traduz precisamente a afirmação.

§ 4. Anéis de polinómios.

1) **Definição geral** – Estreitamente ligada com a teoria das ampliações dum anel, e muito especialmente com o problema das extensões dos corpos, está a teoria dos *anéis de polinómios*, de que nos vamos ocupar.

Dado um anel arbitrário $\mathfrak{A}$, consideremos o conjunto dos quadros de dupla entrada, formados por elementos daquele anel:

$$(1) \qquad \begin{vmatrix} a_{00} & a_{01} & a_{02} & \cdots \\ a_{10} & a_{11} & a_{12} & \cdots \\ a_{20} & a_{21} & a_{22} & \cdots \\ \cdots\cdots & & & \end{vmatrix}.$$

Suporemos que há apenas um número finito de elementos $a_{\lambda\mu}$ diferentes do elemento nulo de $\mathfrak{A}$.

Definamos, no conjunto dos quadros, um preceito de soma e outro de produto, pondo: I) para a soma: $c_{\lambda\mu} = a_{\lambda\mu} + b_{\lambda\mu}$, se os elementos $b_{\lambda\mu}$ pertencem a um quadro análogo ao dos $a_{\lambda\mu}$; II) para o produto: $c_{\lambda\mu} = \sum a_{mp} b_{qr}$, estendendo o somatório a m, p, q, r, de tal modo que $m + q = \lambda$, $p + r = \mu$. É fácil de ver que os quadros relativos aos $c_{\lambda\mu}$, tanto para a soma como para o produto, têm um número finito de elementos diferentes de zero. A afirmação é evidente para a soma. Quanto ao produto, reconhece-se o facto, notando que, se forem a_{MN} e b_{QR} dois elementos dos dois quadros factores não nulos e tais que as somas $M + N$ e $Q + R$ tenham valores máximos, todos os $c_{\lambda\mu}$, para os quais $\lambda + \mu$ exceda em uma unidade, pelo menos, a soma daqueles dois máximos, são nulos.

O conjunto dos quadros (1) forma um sistema de dupla composição, que é um anel $\mathfrak{B}$. É isto simples de reconhecer, tratando sucessivamente os diferentes postulados da Teoria dos Anéis.

$\mathfrak{B}$ contém um subconjunto de elementos da forma

$$(2)\qquad \begin{vmatrix} a_{00} & 0 & 0 & \cdots \\ 0 & 0 & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{vmatrix},$$

os quais, por soma e produto, dão ainda elementos da mesma forma. Substituindo, em $\mathfrak{B}$, estes elementos (2) pelos elementos $a_{00} \in \mathfrak{A}$, obtém-se um novo anel $\mathfrak{B}'$, ampliação de $\mathfrak{A}$. Aos elementos de $\mathfrak{B}'$ podemos dar uma representação mais cómoda, escrevendo:

$$\begin{vmatrix} 0 & 0 & \cdots \\ a_{10} & 0 & \cdots \\ \cdots & \cdots & \cdots \end{vmatrix} = a_{10}x, \qquad \begin{vmatrix} 0 & a_{01} & 0 & \cdots \\ 0 & 0 & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{vmatrix} = a_{01}y,$$

$$\begin{vmatrix} 0 & 0 & 0 & \cdots \\ 0 & a_{11} & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{vmatrix} = a_{11}xy, \qquad \begin{vmatrix} a_{00} & a_{01} & 0 & \cdots \\ a_{10} & a_{10} & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{vmatrix} = a_{00} + a_{01}y + a_{10}x + a_{11}xy,$$

conforme regras que fàcilmente se reconhecem. A nova representação é coerente, pois que a expressão de soma expressa pelo sinal $+$, que ela introduz, é a mesma que a que foi prèviamente introduzida em $\mathfrak{B}'$. Utilizaremos, assim, a notação

$$(3)\qquad \sum_{i,j=0}^{\infty} a_{ij}x^i y^j, \qquad (a_{ij} \in \mathfrak{A}),$$

onde apenas um número finito de «coeficientes» a_{ij} se supõem diferentes de zero.

A regra de produto leva a igualdade

$$\sum_{m,p=0}^{\infty} a_{mp}x^m y^p \cdot \sum_{q,r=0}^{\infty} b_{qr}x^q y^r = \sum_{\lambda,\mu=0}^{\infty} c_{\lambda\mu}x^\lambda y^\mu,$$

com $m+q=\lambda$, $p+r=\mu$, como acima se viu.

Conclui-se deste modo que o uso dos símbolos (3) implica a comutabilidade das «indeterminadas» x e y, assim como a comutabilidade destas com os elementos a_{ij}.

A justificação do vocábulo «indeterminada», aplicado a x e a y, pode fazer-se do modo a seguir: 1.º) Tanto x como y não são susceptíveis de qualquer determinação a partir do anel $\mathfrak{A}$, não satisfazendo a equações do tipo

$$\sum_{h=0}^{\infty} a_h x^h = 0, \quad \text{ou} \quad \sum_{h=0}^{\infty} b_h y^h = 0,$$

salvo no caso banal de os a_h e os b_h serem nulos. É o que se exprime também dizendo que x e y são *transcendentes* e que o anel $\mathfrak{B}' = \mathfrak{A}[x,y]$ resulta de $\mathfrak{A}$ por *adjunção anular transcendente* de x e y. 2.º) x e y não têm entre si qualquer relação. Ao escrever-se uma igualdade

$$\sum_{h,j=0}^{\infty} a_{hj}x^h y^j = \sum_{h,j=1}^{\infty} b_{hj}x^h y^j,$$

a única conclusão a tirar é esta: $a_{hj} = b_{hj}$. É o que se exprime dizendo que x e y são *independentes*.

O anel $\mathfrak{A}[x,y]$ diz-se *anel de polinómios em* x *e* y, com coeficientes em $\mathfrak{A}$. As representações bem determinadas (3) dizem-se *representações normais* e os elementos $a_{hj} \in \mathfrak{A}$ que nelas figuram chamam-se *coeficientes* da representação.

Claramente que o anel $\mathfrak{A}[x,y]$ se compõe, não apenas de elementos da forma (3), mas de todos os elementos da forma (3). Ele representa uma ampliação autêntica de $\mathfrak{A}$, suposto $\mathfrak{A} \neq (0)$.

O que acabamos de dizer para x e y diz-se para n indeterminadas quaisquer, $x_1, x_2, \cdots, x_n$. O anel ampliado correspondente representa-se por $\mathfrak{A}[x_1, x_2, \cdots, x_n]$ e os elementos do mesmo têm a representação unívoca

$$\sum_{k_1,\ldots k_n=0}^{\infty} a_{k_1\ldots k_n}x_1^{k_1}\cdots x_n^{k_n},$$

onde há apenas um número finito de coeficientes $a_{k_1\ldots k_n}$ que são diferentes do elemento nulo de $\mathfrak{A}$.

2) **Construção de $\mathfrak{A}[x_1, \cdots, x_n]$ por adjunções sucessivas** – O anel $\mathfrak{A}[x_1, \cdots x_n]$ pode, como vamos ver, construir-se por adjunções anulares sucessivas, pondo

$$\mathfrak{A}_1 = \mathfrak{A}[x_1], \quad \mathfrak{A}_2 = \mathfrak{A}_1[x_2], \cdots, \mathfrak{A}_n = \mathfrak{A}_{n-1}[x_n].$$

Para se demonstrar a identidade das duas construções, observemos que ela tem de facto lugar para $n=1$. Admitindo a sua validade

para $n-1$, vamos prová-la para n. Os elementos de $\mathfrak{A}_n$ são da forma

$$P_n = \sum_{k_n=0}^{\infty} A_{k_n} x_n^{k_n}, \text{ com } A_{k_n} = \sum_{k_1,\ldots,k_{n-1}=0}^{\infty} a_{k_1\ldots k_{n-1}}^{k_n} x_1^{k_1}\cdots x_{n-1}^{k_{n-1}},$$

ou seja, são da forma

$$P_n = \sum_{k_n=0}^{\infty}\left[\sum_{k_1,\ldots,k_{n-1}=0}^{\infty} a_{k_1\ldots k_{n-1}}^{k_n} x_1^{k_1}\cdots x_{n-1}^{k_{n-1}}\right] x_n^{k_n} = \tag{1}$$
$$= \sum_{k_n}\left[\sum_{k_1,\ldots,k_{n-1}} a_{k_1\ldots k_n} x_1^{k_1}\cdots x_{n-1}^{k_{n-1}}\right] x_n^{k_n},$$

pondo $a_{k_1\ldots k_n} = a_{k_1\ldots k_{n-1}}^{k_n}$. Ora há uma correspondência biunívoca completa entre os elementos (1) e os elementos de $\mathfrak{A}[x_1, \cdots, x_n]$. A identidade de $\mathfrak{A}_n$ e de $\mathfrak{A}[x_1, \cdots, x_n]$ deve ser precisamente entendida no sentido de que os dois anéis são isomorfos. É, de resto, ainda no mesmo sentido de isomorfismo anular que podemos fazer esta afirmação: o anel $\mathfrak{A}_n$ fica o mesmo, se a ordem das adjunções das indeterminadas se alterar.

3) **Algumas propriedades dos polinómios** — Suponhamos uma única indeterminada x. É válido o seguinte

TEOREMA 1: *Se $\mathfrak{A}$ é um domínio de integridade não comutativo, $\mathfrak{A}[y]$ é um domínio de integridade não comutativo.* Recorrendo, na verdade, à representação dos elementos de $\mathfrak{A}[y]$ sob a forma $\overline{|a_0 a_1 \cdots a_n \cdots}$, ponhamos $\overline{|a_0 a_1 \cdots a_n \cdots} \cdot \overline{|b_0 b_1 \cdots b_n \cdots} = 0$. Se a_p e b_q forem, respectivamente, os últimos elementos de $\mathfrak{A}$ que não são nulos nos dois factores, o produto $\overline{|c_0 c_1 \cdots c_r \cdots}$ desses factores contém o elemento

$$c_{p+q} = a_{p+q} b_0 + \cdots + a_p b_q + \cdots + a_0 b_{p+q} = a_p b_q \neq 0,$$

o que é absurdo. Ou todos os a_i ou todos os b_j serão necessàriamente nulos.

Na representação normal, os elementos de $\mathfrak{A}[y]$ têm o aspecto $P(y) = a_0 + a_1 y + \cdots + a_n y^n$, no qual põe em evidência o último coeficiente $a_n \neq 0$. O número n diz-se *grau* de $P(y)$.

No que vai seguir-se, tratando-se com polinómios numa única indeterminada, designaremos esta pela letra x.

Com a noção de grau que acaba de ser dada para os polinómios não nulos, se atribuirmos ainda o grau $-\infty$ ao polinómio nulo e utilizarmos as regras $-\infty + (-\infty) = -\infty$, $-\infty + n = -\infty$, podemos enunciar o teorema geral seguinte:

TEOREMA 2: *Se $\mathfrak{A}$ é um domínio de integridade não comutativo, o grau dum produto de dois polinómios de $\mathfrak{A}[x]$ é a soma dos respectivos graus.*

Como $\mathfrak{A}_1, \cdots, \mathfrak{A}_n$ são sucessivamente construidos a partir de domínios de integridade, segue-se que $\mathfrak{A}_n$ é um domínio de integridade não comutativo, se $\mathfrak{A}$ o for.

No caso dos polinómios de muitas indeterminadas, o *grau* é avaliado pelo valor máximo das somas dos «expoentes» nas diferentes parcelas. O polinómio nulo tem sempre, porém, o grau $-\infty$.

Um polinómio diz-se *homogéneo*, quando os seus «termos» são do mesmo grau. Um polinómio qualquer é sempre uma soma de polinómios homogéneos. Tem-se:

TEOREMA 3: *O produto de dois polinómios homogéneos de graus* m *e* q, *respectivamente, é um polinómio homogéneo do grau* m + q, *se $\mathfrak{A}$ for um domínio de integridade não comutativo.* Na verdade, sendo $\mathfrak{A}_n$ um domínio de integridade, o produto de dois elementos não nulos é $\neq 0$. Assim, o produto de dois polinómios homogéneos é um polinómio homogéneo, cujo grau é necessàriamente a soma dos graus.

Consideremos, em seguida, um produto de dois polinómios não homogéneos. As partes homogéneas do mais alto grau dão, pelo seu produto, que é diferente de zero, a parte homogénea do mais alto grau do produto, ou seja o grau do produto. Assim, *se $\mathfrak{A}$ é um domínio de integridade não comutativo, o teorema 2 é válido para os polinómios de $\mathfrak{A}[x_1, \cdots, x_n]$.*

Quando o anel $\mathfrak{A}$ é comutativo, $\mathfrak{A}_n$ é também comutativo. Se $\mathfrak{A}$ tem elemento u, este é igualmente o elemento um de $\mathfrak{A}_n$.

O anel $\mathfrak{A}_n$ nunca é um corpo, ainda que $\mathfrak{A}$ seja um corpo. O elemento $(a_0 x_1)^{-1}$, por exemplo, não existe em $\mathfrak{A}_n$, pois

$$\frac{u}{a_0 x_1} = \sum_{k_1,\ldots,k_n=0}^{\infty} a_{k_1\ldots k_n} x_1^{k_1}\cdots x_n^{k_n} \text{ daria } u = \sum_{k_1,\ldots,k_n=0}^{\infty} a_0 a_{k_1\ldots k_n} x_1^{k_1+1}\cdots x_n^{k_n},$$

igualdade que é impossível, pelo facto de não haver no 2.º membro termo que não contenha x_1.

4) **Os polimónios de uma indeterminada** — Neste número, trataremos especialmente o caso do anel $\mathfrak{A}[x]$. Vamos supor que existe $u \in \mathfrak{A}$ e introduzir um algoritmo de divisão. De resto, $\mathfrak{A}$ é um anel não comutativo qualquer.

Dado $P(x) \in \mathfrak{A}[x]$, do grau n, supondo que o polinómio divisor $D(x)$ é de grau $m \leqslant n$, faremos ainda a restrição de o coeficiente do termo de mais alto grau de $D(x)$ ser um elemento de $\mathfrak{A}$ com inverso.

Distinguiremos as *divisões à direita e à esquerda*, em sentido já conhecido de (VI, 2, 2), que aqui vamos, porém, analisar detidamente. Ponhamos

$$(1) \qquad \begin{aligned} P(x) &= a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n , \\ D(x) &= b_0 x^m + b_1 x^{m-1} + \cdots + b_{m-1} x + b_m . \end{aligned}$$

Por hipótese, é $a_0 \neq 0$ e existe b_0^{-1}. Provaremos ser possível, e de uma só maneira, escrever, no caso de uma divisão à direita,

$$(2) \qquad P(x) = Q_d(x) \cdot D(x) + R_d(x) ,$$

onde $D(x)$ é um polinómio de grau inferior a m.

Admitamos a possibilidade de (2). Uma segunda possibilidade levaria a $P(x) = Q'_d(x) \cdot D(x) + R'_d(x)$, deduzindo-se

$$[Q_d(x) - Q'_d(x)] \cdot D(x) + [R_d(x) - R'_d(x)] = 0 ,$$

ou seja $$[Q_d(x) - Q'_d(x)] \cdot D(x) = R'_d(x) - R_d(x) .$$

Sendo $Q'_d(x) \neq Q_d(x)$, o grau do 1.º membro da igualdade anterior seria m, pelo menos, enquanto que o do 2.º membro seria inferior a m. Dever-se-á ter $Q'_d(x) = Q_d(x)$, e, portanto, $R'_d(x) = R_d(x)$.

Demonstremos agora (2). Tem-se

$$(3) \qquad P(x) - a_0 b_0^{-1} x^{n-m} D(x) = P_{n-1}(x) ,$$

onde o polinómio do 2.º membro é, quando muito, do grau $n-1$. Se $n-1 \geqslant m$, e se, por exemplo, o coeficiente do termo do grau $n-1$, de $P_{n-1}(x)$, é c_{n-1}, a diferença

$$(4) \qquad P_{n-1}(x) - c_{n-1}\ b_0^{-1} x^{n-m-1}\ D(x) = P_{n-2}(x)$$

é, quando muito, do grau $n-2$. O processo continua até se chegar a

$$P(x) - (a_0 b_0^{-1} x^{n-m} + c_{n-1}\ b_0^{-1} x^{n-m-1} + \cdots + d) \cdot D(x) = R_d(x) ,$$

onde $R_d(x)$ é o segundo membro da última igualdade a escrever, análoga a (3) e a (4), a qual é obtida logo que o grau respectivo seja $< m$. Será $Q_d(x) = a_0 b_0^{-1} x^{n-m} + \cdots + d$, podendo ter-se $d = 0$.

Na divisão à esquerda, a igualdade (2) é substituida por

$$P(x) = D(x) \cdot Q_e(x) + R_e(x) .$$

No caso particular em que se tem $D(x) = x - b$, podem dar-se expressões simples para $R_d(x)$ e $R_e(x)$. Observemos, com efeito, as igualdades

$$x^n - b^n = (x^{n-1} + b\,x^{n-2} + \cdots + b^{n-2}x + b^{n-1})(x - b) ,$$

$$x^n - b^n = (x - b)(x^{n-1} + b\,x^{n-2} + \cdots + b^{n-2}x + b^{n-1}) .$$

Se $P(x)$ é o polinómio indicado em (1), tem-se, então

$$R_d(x) = a_0 b^n + a_1 b^{n-1} + \cdots + a_{n-1} b + a_n ,$$

como se vê efectuando a diferença

$$\begin{aligned} P(x) - R_d(x) &= a_0(x^n - b^n) + \cdots + a_{n-1}(x - b) = \\ &= (a_0 x^{n-1} + \cdots)(x - b) . \end{aligned}$$

Vê-se anàlogamente que é

$$R_e(x) = b^n a_0 + b^{n-1} a_1 + \cdots + b\,a_{n-1} + a_n .$$

Convém fazer uma observação. Se $D(x)$ se reduzir a $b_m = b_0$ (sempre sob a hipótese de existir b_0^{-1}), o resto de qualquer divisão é zero. O respectivo grau será $-\infty$; sendo zero o grau de $D(x)$. E podemos dizer:

TEOREMA: *Supondo $\mathfrak{D}$ um anel de divisão, há sempre algoritmo de divisão em $\mathfrak{D}[x]$.*

No número próximo daremos mais alguns pormenores relativos ao caso em que $\mathfrak{D} = \mathfrak{K}$ é um corpo, e no qual, por consequência, se não distinguem a divisão à direita e a divisão à esquerda.

5) **O algoritmo de divisão em $\mathfrak{K}[x]$** — Os resultados do número anterior, tendo em conta o teorema 3 de (VI, 2, 2), mostram que $\mathfrak{K}[x]$, em que $\mathfrak{K}$ é um corpo, é um anel de ideais principais comutativo

Vamos dar uma noção de *valor absoluto*. Se for $P \in \mathfrak{K}[x]$, representaremos ainda pelo símbolo $|P|$ o seu valor absoluto. Então, tomemos um inteiro fixo $v > 1$ e introduzamos as definições seguintes: 1) $|P| = 0$, se $P = 0$; 2) $|P| = v^n$, se n é o grau do polinómio $P \neq 0$. Com estas definições, prova-se:

$$(1) \qquad \begin{array}{ll} |P| = 0, \text{ se } P = 0; & |P| \geqslant 1, \text{ se } P \neq 0; \\ |P \pm Q| \gtrless |P| + |Q|; & |PQ| = |P| \cdot |Q|. \end{array}$$

Pelo facto de o algoritmo de divisão introduzido no número anterior levar a um resto com um valor absoluto inferior ao valor absoluto do divisor, ou de harmonia com o teorema 8, de (VI, 3, 3), podemos dar este enunciado:

TEOREMA 1: *$\mathfrak{K}[x]$ é um domínio euclideano, portanto gaussiano.*

Convém ter em conta algumas observações que vamos fazer. O elemento um do nosso domínio euclideano, satisfazendo a $P = Pu$, é tal que $|u| = 1$. Se E for uma unidade, a relação $EE^{-1} = u$ mostra que $|E| = 1$. O grau n de qualquer unidade é zero, de sorte que: *é condição necessária e suficiente, para que um elemento de $\mathfrak{K}[x]$ seja uma unidade, que ele pertença a $\mathfrak{K}$.*

Elementos associados têm o mesmo valor absoluto, e, reciprocamente, se dois elementos têm o mesmo valor absoluto e um deles divide o outro, os elementos são associados. Um divisor autêntico dum elemento $\neq 0$ tem um valor absoluto inferior ao do dividendo.

Um polinómio cujo coeficiente do termo de mais alto grau seja u diz-se *normado*. O produto de polinómios normados é um polinómio normado, o mesmo podendo dizer-se do cociente, se existe. Os polinómios primos normados dizem-se *irredutíveis*.

O teorema demonstrado em (VI, 2, 4) dá-nos um processo de caracterizar o m. d. c. de dois polinómios. Desde que não se distingam, de harmonia com o teorema 2 de (VI, 2, 3), elementos associados, podemos dizer que o m. d. c. de dois polinómios é um polinómio normado bem determinado. O algoritmo de EUCLIDES leva à determinação do m. d. c.. Em especial, provaremos aqui a univocidade de todo o algoritmo de divisão estabelecido de harmonia com (1).

TEOREMA 2: *Dados* P *e* $D \neq 0$, *pertencentes a* $\mathfrak{K}[x]$, *há uma única possibilidade de escrever* $P = DQ + R$, *com* $|R| < |D|$. Se se tivesse

$$\begin{cases} P = DQ + R, \\ |R| < |D|, \end{cases} \qquad \begin{cases} P = DQ' + R', \\ |R'| < |D|, \end{cases}$$

concluiríamos $D(Q - Q') = R' - R$, de sorte que D dividiria a diferença $R' - R$. Se fosse agora $R' \neq R$, seria também $|D| \gtrless |R' - R|$. Como, por outro lado, o grau duma diferença de dois polinómios é, quando muito, o grau do polinómio de mais alto grau, obteríamos ainda $|R' - R| < |D|$, que é uma conclusão a contradizer a anterior. Será, assim, $R' = R$, e, consequentemente, $Q' = Q$.

A teoria do m. m. c. é dominada pelo teorema provado em (VI, 2, 5).

6) **Sobre os ideais primos e os ideais sem divisor** — Os anéis de polinómios são particularmente designados para exemplificações relativas a ideais primos e a ideais sem divisor.

Quando $\mathfrak{K}$ é um corpo, todos os polinómios $ax + b \in \mathfrak{K}[x]$ são primos. Estudemos, em seguida, as condições para que $ax^2 + bx + c$, com $a \neq 0$, seja também primo Quando $c = 0$, o polinómio em causa não é primo. Então, é $b^2 - 4ac = b^2$ um quadrado perfeito em $\mathfrak{K}$. No caso geral, ponhamos $ax^2 + bx + c = a(x - f)(x - g)$, e, portanto, $g + f = -b/a$, $gf = c/a$. A possibilidade da decomposição anterior, que nos garante não ser primo o nosso polinómio, leva a $b^2 - 4ac = a^2(g - f)^2$. É necessário, pois, para que $ax^2 + bx + c$ não seja primo, que seja $b^2 - 4ac$ um quadrado perfeito em $\mathfrak{K}$. A condição é suficiente, porque, pondo $b^2 - 4ac = h^2$, fàcilmente se conclui que basta fazer $f = -(h + b)/2a$, $g = (h - b)/2a$ para se ter $ax^2 + bx + c = a(x - f)(x - g)$.

A segunda e última exemplificação refere-se à distinção entre ideais primos e ideais sem divisor. Suponhamos $\mathfrak{I}$ o anel dos números inteiros. Então, $\mathfrak{I}[x]$, como vimos em (VI, 4, 3), é um domínio de integridade comutativo com elemento um. Vamos estudar os ideais (x) e $(2, x)$, para concluirmos que são ambos primos, que o último é ideal sem divisor, mas que isso não sucede com (x). Escrevamos

$$(2, x) = 2\mathfrak{I}[x] + x\mathfrak{I}[x] = 2f + x\mathfrak{I}[x],$$

TEOREMA 3: *Um polinómio primitivo de* $\mathfrak{A}[x]$ *corresponde, nos termos do teorema anterior, a um elemento bem determinado de* $\mathfrak{K}[x]$, *pondo de parte unidades de* $\mathfrak{K}[x]$, *(elementos de* $\mathfrak{K}$*)*. A demonstração é imediata.

TEOREMA 4: *Na correspondência biunívoca definida por via dos dois teoremas anteriores, há correspondência de produto a produto, ressalvando unidades de* $\mathfrak{K}[x]$. Tem-se, com efeito, supostos $f(x)$ e $f_1(x)$ dois polinómios de $\mathfrak{K}[x]$,

$$f(x)\cdot f_1(x)=\frac{d}{a}Q(x)\cdot\frac{d_1}{a_1}Q_1(x)=\frac{dd_1}{aa_1}Q(x)\,Q_1(x),$$

onde $Q\,Q_1$ é um polinómio primitivo de $\mathfrak{A}[x]$. Recìprocamente, dado o produto $Q\,Q_1$ de dois polinómios primitivos de $\mathfrak{A}[x]$, o teorema anterior, pois, que $Q\,Q_1$ é primitivo, leva a um polinómio de $\mathfrak{K}[x]$ bem determinado, nos termos do teorema anterior, o qual é necessàriamente produto de dois polinómios bem determinados do mesmo domínio de integridade.

TEOREMA 5: *Os polinómios* f(x) *e* Q(x) *são simultâneamente primos ou não primos,* f(x) *em* $\mathfrak{K}[x]$, Q(x) *em* $\mathfrak{A}[x]$. Como em $\mathfrak{K}[x]$ as unidades são os elementos de $\mathfrak{K}$ e apenas esses elementos, dizer que $f(x)$ não é primo é dizer que é um produto de dois polinómios. Então, $Q(x)$ contém como factores os polinómios primitivos de $\mathfrak{A}[x]$ correspondentes àqueles polinómios. Se $f(x)$ é primo, $Q(x)$ é primo, visto que, se o não fosse, poderíamos encontrar uma decomposição de $f(x)$ em polinómios.

TEOREMA 6: *Os polinómios primitivos de* $\mathfrak{A}[x]$ *decompõem-se, de modo unívoco, em polinómios primitivos primos.* Dado, com efeito, o polinómio primitivo $Q(x)\in\mathfrak{A}[x]$, ele é sempre correspondente dum polinómio $f(x)=k\,Q(x)\in\mathfrak{K}[x]$, onde k é um elemento arbitrário de $\mathfrak{K}$. Fazendo a decomposição de $f(x)$ em elementos primos de $\mathfrak{K}[x]$, os polinómios primitivos $q_i(x)$, correspondentes aos factores $p_i(x)$, de $f(x)$, pondo de parte unidades de $\mathfrak{A}$, são bem determinados. Obtém-se, deste modo, $f(x)=k\,Q(x)=a\,p_1(x)\cdots p_r(x)=a'\,q_1(x)\cdots q_r(x)$, onde $k, a, a'\in\mathfrak{K}$. Ter-se-á também $\varepsilon k=a'$, onde ε é unidade de $\mathfrak{A}$, pelo que $Q(x)=\varepsilon\,q_1(x)\cdots q_r(x)$. Os polinómios $q_i(x)$ são primos. Outra decomposição de $Q(x)$ em polinómios primos não é possível, pois que ela conduziria a uma segunda decomposição de $k\,Q(x)$, em $\mathfrak{K}[x]$.

Estamos agora em condições de demonstrar o teorema fundamental que enunciámos no começo deste número.

Dado um polinómio $P(x)\in\mathfrak{A}[x]$, decompor este polinómio em factores primos ou elementos indecomponíveis é decompô-lo em factores primos constantes e em polinómios primitivos indecomponíveis, visto que um polinómio não primitivo é sempre decomponível. Consegue-se uma decomposição, escrevendo $P(x)=d\cdot Q(x)$ e decompondo d e $Q(x)$, de modo unívoco, em factores primos. Sendo dadas, então, duas decomposições $P(x)=d_1\cdots d_r\,q_1(x)\cdots q_s(x)=d'_1\,d'_2\cdots d'_{r'}\,q'_1(x)\cdots q'_{s'}(x)$, ter-se-ia, em primeiro lugar, $d_1\cdots d_r=d'_1\cdots d'_{r'}$, o que levaria à igualdade dos d_i e dos d'_j, e, em segundo lugar, $q_1(x)\cdots q_s(x)=q'_1(x)\cdots q'_{s'}(x)$, o que levaria à igualdade dos $q_k(x)$ e dos $q'_m(x)$.

Da comparação de $\mathfrak{A}[x]$ com $\mathfrak{K}[x]$ resulta agora que *um polinómio* P(x)$\in\mathfrak{A}$[x], *decomponível em* $\mathfrak{K}[x]$, *é necessàriamente decomponível em* $\mathfrak{A}[x]$. De facto, pondo $P(x)=d\,Q(x)$, uma decomposição de $P(x)$ num produto de polinómios origina uma decomposição de $Q(x)$ em polinómios primitivos. Por exemplo, um polinómio com coeficientes inteiros indecomponível também se não decompõe quando os referidos coeficientes se supõem pertencer ao corpo dos números racionais.

Fixemos ainda esta proposição:

TEOREMA 7: *Se* $\mathfrak{A}$ *é um domínio gaussiano,* $\mathfrak{A}[x_1,\cdots,x_n]$ *é um domínio gaussiano.*

8) **Sobre a irredutibilidade em** $\mathfrak{A}[x]$ — Como no número anterior, $\mathfrak{A}$ é um domínio gaussiano. O problema que vai ocupar-nos consiste em verificar condições em que um elemento $P(x)\in\mathfrak{A}[x]$ é decomponível ou não num *produto de polinómios*. Conforme vimos, é válido este

TEOREMA 1: *É necessário e basta, para que* P(x)$\in\mathfrak{A}$[x] *seja um produto de polinómios, que* P(x) *seja redutível em* $\mathfrak{K}[x]$, *onde* $\mathfrak{K}$ *é o corpo cociente de* $\mathfrak{A}$.

Seja $a\in\mathfrak{A}$. O anel $\mathfrak{A}[x]/(a)$ compõe-se de elementos da forma $a_0+a_1x+\cdots+a_nx^n+a\,\mathfrak{A}[x]$. Fazendo corresponder a cada um destes elementos um elemento $(a_0+a\,\mathfrak{A})+(a_1+a\,\mathfrak{A})x+\cdots+(a_n+a\,\mathfrak{A})x^n\in(\mathfrak{A}/(a))[x]$, a correspondência é um isomorfismo, como é fácil de ver. Os polinómios da última forma são *polinómios de* $\mathfrak{A}$[x]

módulo a. Dado $P(x) \in \mathfrak{A}[x]$, se o polinómio módulo a correspondente é do mesmo grau que $P(x)$ e irredutível, o polinómio $P(x)$ é irredutível.

Consideremos o caso de ser $\mathfrak{A} = \mathfrak{J}$ o domínio dos inteiros. Se p é um inteiro primo e se se toma $P(x) = (p-k)x + (p-k)$, com $0 < k < p$, então $P(x)$ é redutível, se supusermos que $p - k$ não é unidade, visto que $p-k$ é factor de $P(x)$. Em $(\mathfrak{J}/(p))[x]$, aquele polinómio escrever-se-á $(p-k+(p))x + (p-k+(p))$. Como $\mathfrak{J}/(p)$ é um corpo, este último polinómio é irredutível. Casos como este não estão em causa, pois que, repita-se, se trata de indagar de decomposições em produtos de polinómios.

Escrevamos agora $P(x) = (p x^3 + p q x^2 + 1)(x+2)$. O polinómio módulo p correspondente, é, digamos, $x + 2$. Este polinómio é irredutível, mas não o é o polinómio $P(x)$. Aqui houve, porém, abaixamento de grau.

Tomemos ainda o polinómio $x^4 + x + 1$. O polinómio correspondente módulo 2 é ainda $x^4 + x + 1$. No domínio $(\mathfrak{J}/(2))[x]$ os únicos polinómios irredutíveis do 1.º, 2.º e 3.º graus são

$$x, \quad x+1, \quad x^2+x+1, \quad x^3+x+1, \quad x^3+x^2+1.$$

O polinómio $x^4 + x + 1$ é irredutível módulo 2, pelo facto de não poder obter-se como produto conveniente dos polinómios irredutíveis acabados de escrever. O mesmo se diria de $x^4 + x^3 + 1$ ou de $x^4 + x^3 + x^2 + x + 1$.

Uma última hipótese a formular é relativa ao caso de um polinómio ser irredutível em $\mathfrak{J}[x]$, mas ser redutível módulo p, embora conservando o grau. Tomemos $P(x) = x^4 + 2x^3 + 5x^2 + 3x + 3$. O polinómio módulo 2 é $x^4 + x^2 + x + 1 = (x+1)(x^3 + x^2 + 1)$. Se $P(x)$ se decompõe num produto de dois polinómios, ou ambos os factores são do 2.º grau ou um é do 1.º grau e o outro do 3.º. A primeira hipótese não pode dar-se, em face da decomposição módulo 2. Fazendo a decomposição módulo 3, tem-se $x^4 + 2x^3 + 5x^2 + 3x + 3 = x^4 - x^3 - x^2 = x^2(x^2 - x - 1)$. Este resultado mostra que a decomposição de $P(x)$ só poderá ter lugar com dois factores do 2.º grau. A incompatibilidade deste resultado com o anterior mostra que o polinómio em questão é irredutível em $\mathfrak{J}[x]$.

Um critério importante de irredutibilidade é dado pelo seguinte

TEOREMA 2 (SCHÖNEMANN-EISENSTEIN): *O polinómio* $P(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathfrak{A}[x]$ *não é um produto de dois polinómios de* $\mathfrak{A}[x]$, *ou é irredutível em* $\mathfrak{K}[x]$, *se existir um elemento primo* $p \in \mathfrak{A}$ *satisfazendo às seguintes condições:* $a_n \not\equiv 0\,(p)$, $a_i \equiv 0\,(p)$, $(i = 0, 1, 2, \cdots, n-1)$, $a_0 \not\equiv 0\,(p^2)$. Suponhamos que podia pôr-se $P(x) = (b_0 + b_1 x + \cdots + b_r x^r)\cdot(c_0 + c_1 x + \cdots + c_s x^s)$, com $a_n = b_r c_s$, $a_0 = b_0 c_0$. O elemento primo p não divide b_r nem c_s, mas divide b_0 ou c_0, sem poder dividir simultaneamente estes dois últimos. Suponhamos $c_0 \equiv 0\,(p)$. Escrevendo $(b_0 + b_1 x + \cdots + b_r x^r)(c_0 + c_1 x + \cdots + c_s x^s) \equiv a_n x^n\,(p)$, podemos eliminar c_0 na congruência. Se c_k for o primeiro dos coeficientes c_i que não é divisível por p, tem-se

$$(b_0 + b_1 x + \cdots + b_r x_r)\cdot(c_k x^k + \cdots + c_s x^s) \equiv a_n x^n\,(p).$$

O inteiro k satisfaz à dupla desigualdade $0 < k \leqslant s$. No 1.º membro da congruência, o coeficiente de x^k é $b_0 c_k$, de sorte que este elemento é divisível por p. Isso exigirá, visto que c_k não está nessas condições, que o seja b_0, contra a hipótese acima formulada. A decomposição de $P(x)$ num produto é, pois, absurda.

Um caso particular de irredutibilidade é o seguinte [suposto $\mathfrak{A} = \mathfrak{J}$]:

TEOREMA 3 (SCHÖNEMANN): *O cociente*

$$\frac{x^{p^n} - u}{x^{p^{n-1}} - u} = x^{(p-1)p^{n-1}} + x^{(p-2)p^{n-1}} + \cdots + x^{2p^{n-1}} + x^{p^{n-1}} + u,$$

no qual p *é um elemento primo e* n *é um número natural qualquer, é irredutível.* A demonstração repousa sobre a observação simples de que, dados $P(x) \in \mathfrak{A}[x]$ e $a \in \mathfrak{A}$, os dois polinómios $P(x)$ e $P(x+a)$ são simultâneamente decomponíveis ou indecomponíveis. Mudando, então, x em $x + u$, tem-se

$$Q = \frac{(x+u)^{p^n} - u}{(x+u)^{p^{n-1}} - u} = \text{polinómio em } x, \text{ que, para } x = 0, \text{ se reduz a } pu.$$

Mas, sendo $(x+u)^{p^n} \equiv x^{p^n} + u\,(p)$, $(x+u)^{p^{n-1}} \equiv x^{p^{n-1}} + u\,(p)$, pode escrever-se

$$Q = \frac{x^{p^n} + p\,\Phi(x)}{x^{p^{n-1}} + p\,\Psi(x)} = pu + a_1 x + \cdots + a_\sigma x^\sigma + p\,R(x),$$

o corpo mínimo em tais condições, que recebe a designação de *corpo gerado por* $\mathfrak{K}$ *e* $\mathfrak{T}$ e se representa por $\mathfrak{K}(\mathfrak{T})$. Em $\mathfrak{K}(\mathfrak{T})$ estão contidos os elementos de Ω obtidos por operações de soma, produto, diferença e cociente efectuadas, em número finito, sobre elementos de $\mathfrak{K}$ e de $\mathfrak{T}$. E como o conjunto de elementos formados dessa maneira é corpo, tal corpo será precisamente $\mathfrak{K}(\mathfrak{T})$.

Mesmo que $\mathfrak{T}$ tenha uma infinidade de elementos, qualquer elemento de $\mathfrak{K}(\mathfrak{T})$ tem uma representação à custa dum número finito de elementos de $\mathfrak{K}$ e de $\mathfrak{T}$, pelo que pertence já a um corpo da forma $\mathfrak{K}(\mathfrak{T}')$, onde $\mathfrak{T}'$ é finito e parte de $\mathfrak{T}$.

Considerando todos os corpos da forma $\mathfrak{K}(\mathfrak{S})$, onde $\mathfrak{S}$ é uma parte qualquer de $\mathfrak{T}$, esses corpos estão nas condições de se aplicar o teorema 1, de (V, 2, 3), de sorte que $\mathfrak{K}(\mathfrak{T})$ é o conjunto unido de de todos os $\mathfrak{K}(\mathfrak{S})$. Em particular, se $\mathfrak{T}_1$ e $\mathfrak{T}_2$ são dois conjuntos em que se dividiu $\mathfrak{T}$, é fácil de ver que se tem $\mathfrak{K}(\mathfrak{T}_1)(\mathfrak{T}_2)=\mathfrak{K}(\mathfrak{T}_1)(\mathfrak{K}(\mathfrak{T}_2))= = \mathfrak{K}(\mathfrak{T}) = \mathfrak{K}(\mathfrak{T}_2)(\mathfrak{T}_1)$.

As extensões $\mathfrak{K}(\mathfrak{T})$, aqui postas em causa, levam a corpos cuja existência está assegurada dentro de Ω. Na Teoria dos Corpos criam-se extensões abstractas, em condições de que vamos dar ideia no número seguinte.

3) **Sobre as extensões simples** — Um tipo de extensão abstracta de $\mathfrak{K}$, chamada *extensão transcendente*, resulta muito fàcilmente dos raciocínios feitos sobre anéis de polinómios e anéis de cocientes. De facto, dado $\mathfrak{K}$, por adjunção de uma indeterminada x, passamos ao domínio de integridade $\mathfrak{K}[x]$, e, depois, formando o corpo dos cocientes de $\mathfrak{K}[x]$, como foi definido em (V, 2, 9), obtem-se um corpo que representaremos por $\mathfrak{K}(x)$ e que é uma extensão transcendente *simples* de $\mathfrak{K}$. A designação de «simples» vai buscar-se ao facto de ela resultar de $\mathfrak{K}$ por adjunção de um único «elemento» x.

Outro tipo de extensão simples é a *extensão algébrica simples*, que vamos analisar. Suponhamos ainda Ω um corpo e $\mathfrak{K}$ um subcorpo de Ω. Se $\Theta \in \Omega$, o corpo $\mathfrak{K}(\Theta)$ realiza as condições $\Omega \supseteq \mathfrak{K}(\Theta) \supseteq \mathfrak{K}$, podendo ter-se $\mathfrak{K}(\Theta) = \mathfrak{K}$, o que exigirá $\Theta \in \mathfrak{K}$.

Tomemos, de entre os elementos de $\mathfrak{K}(\Theta)$, aqueles que são da forma $\sum_{k=0}^{n} a_k \Theta^k = P(\Theta)$, $(a_k \in \mathfrak{K})$. Esses elementos formam um domínio de integridade $\mathfrak{A}$, que vamos comparar com o domínio de integridade $\mathfrak{K}[x]$. A correspondência $P(x) \to P(\Theta)$ determina um homomorfismo. Se $\mathfrak{a}$ for o respectivo núcleo, ter-se-á $\mathfrak{A} \simeq \mathfrak{K}[x]/\mathfrak{a}$. No caso de se ter $\mathfrak{a}=(0)$, será $\mathfrak{A} \simeq \mathfrak{K}[x]$. Em tal hipótese, o corpo $\mathfrak{K}(\Theta)$, que se identifica sempre com o corpo dos cocientes do domínio de integridade $\mathfrak{A}$, é isomorfo de $\mathfrak{K}(x)$, e Θ é um elemento de Ω transcendente relativamente a $\mathfrak{K}$: $\mathfrak{K}(\Theta) \simeq \mathfrak{K}(x)$. Supondo, porém, $\mathfrak{a} \neq (0)$, imaginemos um polinómio $\varphi(x) \in \mathfrak{K}[x]$, não nulo, de grau mínimo, pertencente a $\mathfrak{a}$. Ter-se-á, então, $\varphi(\Theta) = 0$. É fácil de ver que $\varphi(x)$ é um polinómio primo. Se $\varphi(x) = ax + b$ é do primeiro grau, a afirmação é banal. Mas, se $\varphi(x)$ é de grau superior ao primeiro, não pode escrever-se $\varphi(x) = \psi(x) \cdot \pi(x)$, visto que, da condição $\varphi(\Theta) = = \psi(\Theta) \cdot \pi(\Theta) = 0$, resultaria $\psi(\Theta) = 0$ ou $\pi(\Theta) = 0$, contra a hipótese de $\varphi(x)$ ser um polinómio de grau mínimo de correspondente zero no homomorfismo $P(x) \to P(\Theta)$.

O núcleo $\mathfrak{a}$ contém o ideal principal $(\varphi(x))$. Recorrendo ao algoritmo de divisão, vê-se que se tem $\mathfrak{a} = (\varphi(x))$. Então, como dissemos em (VI, 3, 4), ou como pode demonstrar-se directamente, $\mathfrak{K}[x]/(\varphi(x))$ é um corpo, o domínio de integridade $\mathfrak{A}$ é já um corpo, tendo-se $\mathfrak{K}(\Theta) = \mathfrak{A}$.

O grau n do polinómio $\varphi(x)$ diz-se *grau de* Θ *relativamente a* $\mathfrak{K}$. E como podemos supor sempre que $\varphi(x)$ é um polinómio normado, temos este

TEOREMA 1: *Se* $\varphi(x) \in \mathfrak{K}[x]$ *for um polinómio irredutível de grau superior ao primeiro, o anel diferença* $\mathfrak{K}(x)/(\varphi(x))$ *é um corpo. Este corpo abstracto é uma ampliação algébrica simples de* $\mathfrak{K}$, *da forma* $\mathfrak{K}(\Theta)$, *em que* Θ *verifica a equação (irredutível)* $\varphi(x) = 0$. Convém fazer algumas observações. Se $\varphi(x) = ax + b$ for do primeiro grau, a condição $a\Theta + b = 0$ mostra que se tem $\Theta = -b/a \in \mathfrak{K}$, pelo que $\mathfrak{K}(\Theta) = \mathfrak{K}$. Outra observação é a que vai seguir-se. Os elementos do corpo $\mathfrak{K}[x]/(\varphi(x))$ são da forma $P(x) + (\varphi(x))$, onde $P(x)$ é de grau inferior ao de $q(x)$. Sob forma desenvolvida, tem-se

$$P(x) + (\varphi(x)) = a_0 + a_1 x + \cdots + a_r x^r + (\varphi(x)) = (a_0 + (\varphi(x))) + + a_1 (x + (\varphi(x))) + \cdots + a_r (x + (\varphi(x)))^r .$$

Há, em particular, os elementos $a + (\varphi(x)) = \overline{a}$, que formam um corpo isomorfo de $\mathfrak{K}$. Então, podemos escrever, pondo $x + (\varphi(x)) = \Theta$ e fazendo $\overline{a} = a$,

$$P(x) + (\varphi(x)) = a_0 + a_1 \Theta + \cdots + a_r \Theta^r ,$$

o que permite identificar $\mathfrak{K}[x]/(\varphi(x))$ com o próprio corpo $\mathfrak{K}(\Theta)$. E vê-se claramente que $\varphi(\Theta) = 0$.

Sob a condição de existência, em $\mathfrak{K}[x]$, de polinómios irredutíveis de grau superior ao primeiro, ficou demonstrada a *existência* de ampliações algébricas abstractas próprias de $\mathfrak{K}$.

BIBLIOGRAFIA

J. Tiago de Oliveira, *Residuais de sistemas e radicais de anéis*, «Revista da Faculdade de Ciências de Lisboa», vol. V, 1956.

N. H. McCoy, *Prime ideals in general rings*, «American Journal of Mathematics», vol. LXXI, 1949, págs. 823-833.

A. Almeida Costa, *Sur les anneaux demi-premiers*, «Revista da Faculdade de Ciências de Lisboa», vol. VII, 1958, págs. 89-104.

———, *Anéis associativos não comutativos*, «Memórias e Estudos do Centro de Matemáticas Aplicadas ao Estudo da Energia Nuclear», n.º 3, Lisboa, 1955.

K. Asano, *Über Ringe mit Vielfachenkettensatz*, «Proceedings of the Imperial Academy», Tokyo, vol. XV, 1939, págs. 288-291.

B. L. van der Waerden, *Moderne Algebra*, ester Teil, 1930.

H. Hasse, *Höhere Algebra*, tomo 1.º, 2.ª edição, Berlim, 1933.

———, *Aufgabensammlung zur höheren Algebra*, Berlim, 1934.

A. Almeida Costa, *Elementos da Teoria dos Anéis*, Porto, 1943.

E. Steinitz, *Algebraische Theorie der Körper*, «Journal für die reine und angewandte Mathematik», Band 137, 1910.

N. Jacobson, *Lectures in Abstract Algebra*, New York, 1951.

CAPITULO VII

Grupos abelianos: Multiplicidades vectoriais. Equações lineares homogéneas

§ 1. Dependência e independência linear

1) **Grupos abelianos com operadores** — De harmonia com o que dissemos em (II, 3, 1) e em (II, 3, 3), a operação de grupo, quando ele se supõe abeliano, será indicada pelo sinal $+$. Obtem-se, assim, um módulo $\mathfrak{M} = \{0, \cdots, x, y, \cdots, z, \cdots\}$. Havendo um domínio operatório Ω, como aqui vamos supôr, poderemos escrever, por vezes, $\Omega = \{\alpha, \cdots, \lambda, \mu, \nu, \cdots, \xi, \cdots\}$; mas, se êsse domínio fôr um anel $\mathfrak{A}$, indicaremos os elementos de $\mathfrak{A}$ pondo $\mathfrak{A} = \{0, a, b, c, \cdots\}$.

Conforme referimos em (IV, 1, 1), deverá ter-se

$$\lambda x \in \mathfrak{M}, \qquad \lambda(x + y) = \lambda x + \lambda y. \tag{1}$$

Na hipótese $\Omega = \mathfrak{A}$, juntaremos ás duas igualdades anteriores mais outras duas, pondo em conjunto, se $\mathfrak{A}$ opera à direita de $\mathfrak{M}$:

$$\begin{gathered} x a \in \mathfrak{M}, \qquad (x + y) a = x a + y a, \\ x(a + b) = x a + x b, \qquad x(a b) = (x a) b. \end{gathered} \tag{2}$$

As duas últimas igualdades, que são as que não têm correspondentes em (1), indicam como deve definir-se a aplicação duma soma e a dum produto de operadores.

Um módulo $\mathfrak{M}$, com um domínio operatório anular $\mathfrak{A}$, nas condições expressas em (2), diz-se um *módulo direito sobre* $\mathfrak{A}$. Define-se análogamente um *módulo esquerdo sobre* $\mathfrak{A}$. O próprio anel $\mathfrak{A}$ é módulo direito e esquerdo sobre $\mathfrak{A}$.

Para um módulo direito, é $x(ab) = (xa)b \neq (xb)a$; e como, para um módulo esquerdo, se tem $(ab)x = a(bx)$, vê-se que a aplicação do produto ab é distinta (em geral) nos dois casos. Se $\mathfrak{A}$ fôr comutativo, cessa essa distinção.

Um exemplo importante de módulo direito sobre um anel $\mathfrak{A}$ é aquele que vamos estudar. Suponhamos existir $u \in \mathfrak{A}$. Formemos os símbolos $(a_1, \cdots, a_n)$, em cada um dos quais figuram n elementos de $\mathfrak{A}$. O conjunto dos símbolos forma um módulo direito sobre $\mathfrak{A}$, se introduzirmos as duas definições seguintes:

$$(a_1, \cdots, a_n) + (b_1, \cdots, b_n) = (a_1 + b_1, \cdots, a_n + b_n),$$
$$(a_1, \cdots, a_n)a = (a_1 a, \cdots, a_n a).$$

A última definição indica o resultado da aplicação do operador a ao elemento $(a_1, \ldots, a_n)$. Então, é muito fácil de verificar que se realizam as condições expressas em (2). Façamos, em particular,

$$e_1 = (u, 0, \cdots, 0), e_2 = (0, u, 0, \cdots, 0), \cdots, e_n = (0, \cdots, 0, u).$$

Vê-se que é $(a_1, \cdots, a_n) = e_1 a_1 + e_2 a_2 + \cdots + e_n a_n$. O elemento zero de $\mathfrak{M}$ é $(0, \cdots, 0)$, ao qual pode dar-se a forma $(0, \cdots, 0) = e_1 \cdot 0 + \cdots + e_n \cdot 0$. Qualquer elemento de $\mathfrak{M}$ tem uma única representação à custa dos e_i. O facto de a condição $e_1 a_1 + \cdots + e_n a_n = 0$ implicar $a_1 = \cdots = a_n = 0$ exprime-se dizendo que os e_i são linearmente independentes.

Se designarmos por $e_i \mathfrak{A}$ o conjunto dos elementos de $\mathfrak{M}$ da forma $e_i a$, $\mathfrak{M}$ é soma directa de sub-módulos-$\mathfrak{A}$, que são os $e_i \mathfrak{A}$, podendo escrever-se $\mathfrak{M} = e_1 \mathfrak{A} + \cdots + e_n \mathfrak{A}$. E, se nos lembrarmos de que um grupo cíclico gerado por um elemento x dum grupo abeliano aditivo se pode escrever $x\mathfrak{Z}$ (ou, melhor ainda, $\mathfrak{Z}x$), em que $\mathfrak{Z}$ é o anel dos inteiros, justifica-se a designação de grupo cíclico atribuida aos $e_i \mathfrak{A}$. $\mathfrak{M}$ aparece, pois, como uma soma directa de sub-grupos cíclicos.

Também se usa a terminologia seguinte: os e_i constituem uma *familia livre* de elementos do módulo, o qual é um *módulo livre*. Com esta última designação significaremos ainda que $\mathfrak{M}$ é um *módulo unitário*, isto é, que o elemento $u \in \mathfrak{A}$, para cada $x \in \mathfrak{M}$, satisfaz a $xu = x$.

2) **Algumas consequências de** (2) – Para facilidade dos cálculos que teremos de fazer, há conveniência em ter presentes certas regras que vamos deduzir, pondo apenas em jogo as relações (2) e a circunstância de $\mathfrak{M}$ ser um módulo. I) Qualquer que seja $x \in \mathfrak{M}$, tem-se $x0 = 0$. É o que resulta de se ter $x(a + 0) = xa = xa + x0$. II) É $x(-a) = -xa$. De facto, tendo-se $x(a-a) = xa + x(-a) = x0 = 0$, vê-se que $x(-a)$ é o simétrico de xa. III) É sempre $0a = 0$, para $0 \in \mathfrak{M}$, qualquer que seja $a \in \mathfrak{A}$. Para o verificar, basta ter em conta a igualdade $(0 + x)a = 0a + xa = xa$. IV) Tem-se $(-x)a = -xa$. É o que se conclui de $(x-x)a = 0a = 0 = xa + (-x)a$.

3) **Dependência e independência línear**—O objectivo essencial deste Capítulo é o do estudo dos *módulos finitos sobre um corpo* $\mathfrak{K}$, também designados *multiplicidades vectoriais finitas sobre* $\mathfrak{K}$, ou, apenas, *multiplicidades vectoriais*, se não há perigo de qualquer confusão.

Seja, então, $\mathfrak{A} = \mathfrak{K}$ um corpo, e suponhamos $\mathfrak{M}$ módulo sobre $\mathfrak{K}$. Os elementos de $\mathfrak{M}$ designar-se-ão por *vectores* e serão representados por $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots, \mathfrak{x}, \mathfrak{y}, \mathfrak{z}, \cdots, \cdots$. $\mathfrak{M}$ receberá, em seguida, duma maneira mais precisa, o nome de *multiplicidade vectorial linear*. Quanto aos elementos de $\mathfrak{K}$, representá-los-emos aqui por $a, b, c, \cdots$ e também $\lambda, \mu, \xi, \cdots$, afectados ou não de índices.

A multiplicidade linear diz-se *finita*, se existirem n elementos $\mathfrak{e}_1, \cdots, \mathfrak{e}_n \in \mathfrak{M}$ tais que, para cada $\mathfrak{x} \in \mathfrak{M}$, se tenha, duma maneira única

$$\mathfrak{x} = \mathfrak{e}_1 \xi_1 + \cdots + \mathfrak{e}_n \xi_n. \tag{1}$$

Em particular, o vector zero $= 0$ terá a forma $0 = \mathfrak{e}_1 \cdot 0 + \cdots + \mathfrak{e}_n \cdot 0$. O facto de a relação $\mathfrak{e}_1 \lambda_1 + \cdots + \mathfrak{e}_n \lambda_n = 0$ implicar $\lambda_1 = \cdots = \lambda_n = 0$ exprime-se, como no exemplo correspondente do número anterior, dizendo que os vectores $\mathfrak{e}_i$ são *linearmente independentes*. O número n diz-se *dimensão* da multiplicidade, facto que recordaremos escrevendo $\mathfrak{M} = \mathfrak{M}_n$.

Os vectores $\mathfrak{e}_i$ constituem o que se chama uma *base* de $\mathfrak{M}_n$, que é um módulo livre.

Imaginemos agora que, dados os vectores $\mathfrak{a}_1, \cdots, \mathfrak{a}_p$, existe uma relação

$$\mathfrak{a}_1 \mu_1 + \cdots + \mathfrak{a}_p \mu_p = 0, \tag{2}$$

sem que os μ_j sejam todos nulos; diz-se que os $\mathfrak{a}_j$ são *linearmente*

dependentes. Escrevendo $\mathfrak{a}_j = \mathfrak{e}_1 a_{1j} + \cdots + \mathfrak{e}_n a_{nj}$, $(a_{kj} \in \mathfrak{K})$, e substituindo, em (2), encontramos as relações

$$\sum_j \left(\sum_k \mathfrak{e}_k a_{kj}\right) \mu_j = \sum_k \mathfrak{e}_k \left(\sum_j a_{kj} \mu_j\right) = 0,$$

das quais se tira

$$\sum_{j=1}^{p} a_{kj} \mu_j = 0, \qquad (k = 1, 2, \cdots, n). \tag{3}$$

Dêste modo, se os $\mathfrak{a}_j$ são linearmente dependentes, estas equações (3) são satisfeitas por valores não nulos para todos os μ_j. A recíproca é igualmente válida.

Admitiremos, por se tratar de módulos livres, que as multiplicidades vectoriais lineares finitas são módulos unitários: $\mathfrak{a} u = \mathfrak{a}$, se u é o elemento um de $\mathfrak{K}$.

Então, um único vector $\mathfrak{a} \neq 0$ é sempre linearmente independente: se pudesse ter-se $\mathfrak{a}\lambda = 0$, com $\lambda \neq 0$, ter-se-ia também $(\mathfrak{a}\lambda)\lambda^{-1} = \mathfrak{a} u = \mathfrak{a} = 0$. Ainda com $\mathfrak{a} \neq 0$, também não pode ter-se $\mathfrak{a}\lambda = \mathfrak{a}\mu$, se $\lambda \neq \mu$. E isto porque, se a igualdade tivesse lugar, seria $\mathfrak{a}(\lambda - \mu) = 0$, com $\lambda - \mu \neq 0$.

Dados dois ou mais vectores, se um deles for zero, há, entre os vectores, uma dependência linear.

Conhecidos $\mathfrak{a}_1, \cdots, \mathfrak{a}_p$, se outro vector $\mathfrak{a}$ puder exprimir-se sob a forma $\mathfrak{a} = \mathfrak{a}_1\lambda_1 + \cdots + \mathfrak{a}_p\lambda_p$, diz-se que $\mathfrak{a}$ é uma *combinação linear* dos $\mathfrak{a}_j$.

Faremos ainda uma última observação, antes de demonstrarmos os dois primeiros teoremas que nos interessam. É a seguinte: cada elemento de $\mathfrak{K}$ induz um endomorfismo em $\mathfrak{M}$ e elementos diferentes induzem endomorfismos diferentes.

TEOREMA 1: *Se os vectores* $\mathfrak{a}_j$, $(j = 1, 2, \cdots, p)$, *são linearmente dependentes, um deles é combinação linear dos outros.* De facto, sendo $\mathfrak{a}_1\lambda_1 + \cdots + \mathfrak{a}_p\lambda_p = 0$, com $\lambda_1 \neq 0$, por exemplo, da equação anterior pode tirar-se $\mathfrak{a}_1 = -\mathfrak{a}_2\frac{\lambda_2}{\lambda_1} - \cdots - \mathfrak{a}_p\frac{\lambda_p}{\lambda_1}$, o que justifica a afirmação.

TEOREMA 2: *Se os vectores* $\mathfrak{a}_1, \cdots, \mathfrak{a}_p$ *são lineamente independentes, mas* $\mathfrak{a}_1, \cdots, \mathfrak{a}_{p+1}$ *são dependentes, o vector* $\mathfrak{a}_{p+1}$ *é combinação linear dos restantes.* Escrevendo $\mathfrak{a}_1\lambda_1 + \cdots + \mathfrak{a}_p\lambda_p + \mathfrak{a}_{p+1}\lambda_{p+1} = 0$, não pode ter-se $\lambda_{p+1} = 0$, visto que, de contrário, existiria uma dependência linear entre os $\mathfrak{a}_i$. Então, deduz-se $\mathfrak{a}_{p+1} = -\mathfrak{a}_1\frac{\lambda_1}{\lambda_{p+1}} - \cdots - \mathfrak{a}_p\frac{\lambda_1}{\lambda_{p+1}}$, como se deseja.

Tem grande interesse o reconhecimento do carácter de dependência ou independência dum certo número de vectores dados. Por comodidade de linguagem, chamaremos *componentes* do vector $\mathfrak{x}$ os coeficientes ξ_i que figuram na igualdade (1). Dar um vector será, então, dar as suas componentes nos $\mathfrak{e}_i$.

4) **O teorema de Steinitz** — Postos os resultados dos números anteriores, consideremos m vectores $\mathfrak{a}_1, \cdots, \mathfrak{a}_m$. Visto que um vector não nulo é linearmente independente, tomemos um dos $\mathfrak{a}_j$ não nulo, por exemplo $\mathfrak{a}_1$. Pode acontecer que todos os outros vectores se exprimam em $\mathfrak{a}_1$. Se houver, porém, um segundo vector, $\mathfrak{a}_2$ por exemplo, não exprimível em $\mathfrak{a}_1$, ou o sistema $\{\mathfrak{a}_1, \mathfrak{a}_2\}$ é tal que todos os outros vectores se exprimem nos dois vectores do sistema, ou isso não acontece e o raciocínio prossegue até se chegar a estabelecer o seguinte

TEOREMA 1: *Dados* m *vectores* $\mathfrak{a}_j$, $(j = 1, 2, \cdots, m)$, *supostos não todos nulos, há sempre* $r \leqslant m$ *vectores independentes nos quais todos se exprimem.*

É importante reconhecer, porém, que o número r, aludido no teorema, é bem determinado. É desse facto que passamos a ocupar-mos. Dois sistemas de vectores $(\mathfrak{x}_1, \cdots, \mathfrak{x}_m)$ e $(\mathfrak{y}_1, \cdots, \mathfrak{y}_p)$ dizem-se *equivalentes*, se os $\mathfrak{x}_i$ se puderem exprimir nos $\mathfrak{y}_j$, e inversamente. Demonstraremos a importante proposição, conhecida sob o nome de

TEOREMA DE STEINITZ: *Se os vectores* $\mathfrak{y}_1, \cdots, \mathfrak{y}_p$ *são independentes e exprimíveis em* $\mathfrak{x}_1, \cdots, \mathfrak{x}_m$, *é possível substituir* p *destes últimos, por exemplo* $\mathfrak{x}_{i_1}, \cdots, \mathfrak{x}_{i_p}$, *pelos* $\mathfrak{y}_j$, *de tal modo que o sistema* $(\mathfrak{y}_1, \cdots, \mathfrak{y}_p, \mathfrak{x}_{i_{p+1}}, \cdots, \mathfrak{x}_{i_m})$ *seja equivalente a* $(\mathfrak{x}_1, \cdots, \mathfrak{x}_m)$. Admitindo $p = 1$, da relação $\mathfrak{y}_1 = \mathfrak{x}_1\lambda_1 + \cdots + \mathfrak{x}_m\lambda_m$, supondo, por exemplo, $\lambda_1 \neq 0$, deduz-se $\mathfrak{x}_1 = \mathfrak{y}_1\frac{u}{\lambda_1} - \mathfrak{x}_2\frac{\lambda_2}{\lambda_1} - \cdots - \mathfrak{x}_m\frac{\lambda_m}{\lambda_1}$. Então $(\mathfrak{y}_1, \mathfrak{x}_2, \cdots, \mathfrak{x}_m)$

é equivalente a $(\mathfrak{x}_1, \cdots, \mathfrak{x}_m)$. Admitindo agora $p = 2$, o vector $\mathfrak{y}_2$ exprime-se em $\mathfrak{y}_1, \mathfrak{x}_2, \cdots, \mathfrak{x}_m$, sob a forma

$$\mathfrak{y}_2 = \mathfrak{y}_1 \lambda + \mathfrak{x}_2 \mu_2 + \cdots + \mathfrak{x}_m \mu_m , \tag{1}$$

não podendo ser nulos todos os μ_i, dada a independência de $\mathfrak{y}_1$ e $\mathfrak{y}_2$. Se for $\mu_2 \neq 0$, da igualdade anterior tiramos $\mathfrak{x}_2 = -\mathfrak{y}_1 \frac{\lambda}{\mu_2} - \mathfrak{y}_2 \frac{u}{\mu_2} - \cdots - \mathfrak{x}_m \frac{\mu_m}{\mu_2}$, pelo que os dois sistemas $(\mathfrak{y}_1, \mathfrak{x}_2, \cdots, \mathfrak{x}_m)$ e $(\mathfrak{y}_1, \mathfrak{y}_2, \mathfrak{x}_3, \cdots \mathfrak{x}_m)$ são equivalentes. A equivalência em causa é evidentemente transitiva, pelo que $(\mathfrak{x}_1, \cdots, \mathfrak{x}_m)$ e $(\mathfrak{y}_1, \mathfrak{y}_2, \mathfrak{x}_3, \cdots, \mathfrak{x}_m)$ são equivalentes. O processo continua. Logo que se tenham substituido $p-1$ dos $\mathfrak{x}_i$ por outros tantos $\mathfrak{y}_j$, passa-se à substituição de mais um dos $\mathfrak{x}_i$ pelo último dos $\mathfrak{y}_j$.

O facto de, na relação (1), não poder ter-se no 2.º membro apenas a parcela $\mathfrak{y}_1 \lambda$ mostra que, logo que $p = 2$, será, necessàriamente, $m \geqq 2$. Dum modo geral, o teorema exige que se tenha $m \geqq p$, a fim de que os $\mathfrak{y}_j$, se exprimam nos $\mathfrak{x}_i$.

COROLÁRIO: *O número* r, *referido no teorema 1, é bem determinado.* Se, por exemplo, $(\mathfrak{a}_1, \cdots, \mathfrak{a}_r)$ e $(\mathfrak{a}_{i_1}, \cdots \mathfrak{a}_{i_s})$ forem dois sistemas de vectores com as propriedades expressas no teorema 1, os dois sistemas são equivalentes. Como são independentes, o teorema de STEINITZ afirma que se tem $s \geqq r$, $r \geqq s$. Logo, é $r = s$, como se deseja.

§ 2. Matrizes

1) **Definição. Transformações simples** — Tomados m vectores $\mathfrak{a}_1, \cdots, \mathfrak{a}_m$, formemos o quadro rectangular a seguir, em cujas linhas horizontais (chamadas *vectores-linhas*, ou, simplesmente, *linhas*) figuram as componentes dos diferentes vectores:

$$\begin{bmatrix} a_{11} & a_{12} \cdots a_{1n} \\ a_{21} & a_{22} \cdots a_{2n} \\ \cdots\cdots\cdots\cdots \\ a_{m1} & a_{m2} \cdots a_{mn} \end{bmatrix} \tag{1}$$

Este quadro rectangular toma o nome de *matriz rectangular*, com m linhas e n *colunas* (linhas verticais). Quando se tem $m = n$, a matriz diz-se *quadrada*.

O problema de determinar efectivamente o número r do teorema 1 de (VII, 1, 4) vai ser resolvido neste número e no seguinte.

Partamos da matriz (1), que designaremos abreviadamente por $A = (a_{ik})$, $(i = 1, 2, \cdots, m;\ k = 1, 2, \cdots, n)$. Na notação (a_{ik}), o primeiro índice refere-se às linhas, o segundo às colunas. Chamaremos *transformações simples* de A as transformações dos tipos seguintes: 1.º) multiplicação de todos os elementos de uma linha de A por um elemento $b \in \mathfrak{K}$, não nulo; 2.º) adição, à linha de ordem k, dos elementos correspondentes da linha de ordem j, multiplicados por um elemento de $\mathfrak{K}$; 3.º) multiplicação dos elementos de uma coluna de A por um elemento $b \neq 0$; 4.º) adição, à coluna de ordem q, dos elementos correspondentes da coluna de ordem t, multiplicados por um elemento de $\mathfrak{K}$. Vamos provar o seguinte

TEOREMA 1: *As transformações simples de* A *transformam a matriz* A *noutras matrizes rectangulares com o mesmo número de linhas e de colunas de* A, *de tal modo que o número* r *(número máximo de vectores-linhas linearmente independentes) não é alterado.* Examinemos os sucessivos tipos de transformações simples. No 1.º tipo, supostas dependentes as linhas relativas a $\mathfrak{a}_{j_1}, \cdots, \mathfrak{a}_{j_{r+1}}$, de A, antes da transformação, as mesmas linhas são dependentes depois da transformação, visto que, ou não foram alteradas, ou, passando a figurar $\mathfrak{a}_{j_1} b$, por exemplo, em vez de $\mathfrak{a}_{j_1}$, de uma relação

$$\mathfrak{a}_{j_1} \lambda_1 + \cdots + \mathfrak{a}_{j_{r+1}} \lambda_{r+1} = 0 , \tag{2}$$

deduz-se a relação $(\mathfrak{a}_{j_1} b)\frac{\lambda_1}{b} + \cdots + \mathfrak{a}_{j_{r+1}} \lambda_{r+1} = 0$, sem que todos os coeficientes, numa e noutra relação, sejam nulos. No 2.º tipo, imaginemos, do mesmo modo, antes da transformação, realizada a dependência (2). Depois da transformação, se, por exemplo, $\mathfrak{a}_{j_{r+1}}$ passa a ser substituido por $\mathfrak{a}_{j_{r+1}} + \mathfrak{a}_i b$, vamos ver que tem lugar uma igualdade da forma

$$\mathfrak{a}_{j_1} \mu_1 + \cdots + (\mathfrak{a}_{j_{r+1}} + \mathfrak{a}_i b)\mu_{r+1} = 0 , \tag{3}$$

sem que todos os μ_h sejam nulos. Por um lado, com efeito, é

$$\mathfrak{a}_{j_1} \lambda_1 + \cdots + \mathfrak{a}_{j_{r+1}} \lambda_{r+1} = 0 ; \tag{4}$$

por outro, a_i não é independente dos r vectores $a_{j_1}, \cdots, a_{j_r}$, sendo, por exemplo,

$$a_{j_1}\lambda'_1 + \cdots + a_{j_r}\lambda'_r + a_i\lambda = 0. \tag{5}$$

Aqui, pode acontecer que os vectores $a_{j_1}, \cdots, a_{j_r}$ sejam dependentes, e, então, sê-lo-ão os vectores que figuram em (3); ou, de contrário, se aqueles r vectores forem independentes, será, em (5), $\lambda \neq 0$, e, em (4), $\lambda_{r+1} \neq 0$, o que permite a combinação

$$a_{j_1}\left(\frac{\lambda_1}{\lambda_{r+1}} + \frac{\lambda'_1 b}{\lambda}\right) + \cdots + a_{j_r}\left(\frac{\lambda_r}{\lambda_{r+1}} + \frac{\lambda'_r b}{\lambda}\right) + (a_{j_{r+1}} + a_i b) = 0,$$

no qual é $\neq 0$ (e igual a u) o coeficiente de $a_{j_{r+1}} + a_i b$.

Quanto ao 3.º tipo, raciocinaremos do modo a seguir. Consideremos, por exemplo, $a_1, \cdots, a_{r+1}$, e exprimamos a sua dependência linear sob a forma

$$\sum_{i=1}^{r+1} a_{ki}\lambda_i = 0, \qquad (k = 1, 2, \cdots, n). \tag{6}$$

Se uma das colunas, a 1.ª por exemplo, se multiplica por $b \neq 0$, devemos substituir o sistema (6) por outro, no qual, em vez dos a_{k1}, aparecem os coeficientes $a_{k1}b$. Como o sistema (6) admite uma solução $(\lambda_1, \lambda_2, \cdots, \lambda_{r+1})$ composta de elementos não todos nulos, também o sistema em causa admite uma solução $(\lambda_1/b, \lambda_2, \cdots, \lambda_{r+1})$, igualmente composta de elementos não todos nulos. Resta, assim, analisar o 4.º tipo. Se, por exemplo, se juntam aos elementos da 1.ª coluna os elementos da 2.ª multiplicados por b, os elementos a_{k1} aparecem substituidos por $a_{k1} + a_{k2}b$, e o sistema (6) aparece, sob forma desenvolvida, com o aspecto seguinte:

$$\begin{aligned}
&a_{11}\lambda_1 + a_{12}(\lambda_2 + b\lambda_1) + \cdots + a_{1,r+1}\lambda_{r+1} = 0,\\
&a_{21}\lambda_1 + a_{22}(\lambda_2 + b\lambda_1) + \cdots + a_{2,r+1}\lambda_{r+1} = 0,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,\\
&a_{n1}\lambda_2 + a_{n2}(\lambda_2 + b\lambda_1) + \cdots + a_{n,r+1}\lambda_{r+1} = 0.
\end{aligned}$$

Se $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ é uma solução não nula de (6), então, $(\lambda_1, \lambda_2 - \lambda_1 b, \cdots, \lambda_n)$ é uma solução não nula do sistema anterior.

Posto isto, podemos afirmar que as transformações simples não podem aumentar o número r, quando aplicadas a A. Também o não podem diminuir, visto que, se, para uma matriz A', transformada de A, fosse $r' < r$, o número de vectores-linhas independentes, ao passar-se, por transformações simples, de A' para A, aumentaria de r' para r, o que não pode ter lugar. O teorema fica demonstrado.

Passemos a fazer um estudo análogo para as colunas de A. Elas podem considerar-se vectores duma multiplicidade vectorial a m dimensões. Se, então, substituirmos (1) pela *matriz transposta*, que resulta mudando as linhas em colunas e as colunas em linhas, obtém-se

$$\begin{bmatrix} a_{11} & a_{21} \cdots a_{m1} \\ a_{12} & a_{22} \cdots a_{m2} \\ \cdots\cdots\cdots\cdots \\ a_{1n} & a_{2n} \cdots a_{mn} \end{bmatrix}. \tag{7}$$

Esta matriz rectangular, de n linhas e m colunas, sujeita a transformações simples, leva a transformadas para os quais o número máximo s, de linhas independentes, fica o mesmo. Ora essas transformações simples, quando são do 1.º ou do 2.º tipo, obtêm-se efectuando em (1) as transformações do 3.º ou do 4.º tipo, e escrevendo, em seguida, as matrizes transpostas das transformadas de (1). E, inversamente, as transformações do 3.º ou do 4.º tipo, em (7), obtêm-se, a partir das do 1.º ou 2.º tipo, efectuadas sobre (1), pelo mesmo processo de cima. O número s, relativo às linhas de (7), é o número máximo de colunas independentes de (1). As transformações simples não alteram s. Tem lugar este

TEOREMA 2: *As transformações simples de* A *transformam a matriz* A *noutras matrizes rectangulares com o mesmo número de linhas e de colunas de* A, *de tal modo que o número* s *(número máximo de vectores-colunas linearmente independentes) não é alterado.*

Dos raciocínios feitos, resulta que uma sucessão de transformações simples não altera os números r e s. Ora, uma troca de duas linhas ou de duas colunas, pode obter-se por uma sucessão de transformações simples, segundo o sistema a seguir, escrito para a troca das duas primeiras colunas:

$$\begin{aligned}
(a_{i1}, a_{i2}) \to (a_{i1}, a_{i2} + a_{i1}) \to (a_{i1}, -a_{i2} - a_{i1}) \to (-a_{i2}, -a_{i2} - a_{i1}) \to\\
\to (a_{i2}, -a_{i2} - a_{i1}) \to (a_{i2}, -a_{i1}) \to (a_{i2}, a_{i1}).
\end{aligned}$$

Por isso, as trocas de linhas ou de colunas não alteram r e s.

2) **A característica duma matriz** – A determinação prática de r é agora fácil. Tomemos a matriz (1) do número anterior e coloquemos, na 1.ª linha, por troca conveniente, uma linha cujos elementos não sejam todos nulos (admitimos a existência duma tal linha, pois que, de contrário, seriam nulos todos os elementos da matriz A e o número r seria nulo). Em seguida, por troca conveniente de colunas, ponhamos como 1.ª coluna uma coluna para a qual se venha a obter um novo a_{11}, designado por a'_{11}, diferente de zero. Multiplicando em seguida a 1.ª linha por a'^{-1}_{11}, vemos que é admissível supor $a'_{11}=u\in\mathfrak{K}$. Então, por transformações simples do 2.º e do 4.º tipo, chega-se a

$$\begin{bmatrix} u & 0 & 0 & \dots 0 \\ 0 & a'_{22} & a'_{23} & \dots a'_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & a'_{m2} & a'_{m3} & \dots a'_{mn} \end{bmatrix}.$$

Não se dando a circunstância de serem nulos todos os a'_{ik}, por trocas de linhas e de colunas, a partir da 2.ª linha e da 2.ª coluna, e por transformações análogas às que acabamos de utilizar, chegamos a

$$\begin{bmatrix} u & 0 & 0 & \dots 0 \\ 0 & u & 0 & \dots 0 \\ 0 & 0 & a''_{33} & \dots a''_{3n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & a''_{m3} & \dots a''_{mn} \end{bmatrix}.$$

O processo continua. Chega-se finalmente a uma matriz da forma

$$(1)\qquad \begin{bmatrix} u & 0 \dots 0 \dots 0 \\ 0 & u \dots 0 \dots 0 \\ \dots & \dots \\ 0 & 0 \dots u \dots 0 \\ 0 & 0 \dots 0 \dots 0 \\ \dots & \dots \\ 0 & 0 \dots 0 \dots 0 \end{bmatrix}$$

em cuja *primeira diagonal* (aquela em que figuram todos os $u\,u$) se encontra r vezes o elemento um. Sob o aspecto (1), reconhece-se mais que se tem $r=s$. Daqui o importante

TEOREMA 1: *Dada uma matriz* $A=(a_{ik})$, *o número máximo de linhas independentes é igual ao número máximo de colunas independentes.* O referido número diz-se *característica* da matriz.

COROLÁRIO 1: *Na multiplicidade vectorial* $\mathfrak{M}_n$, *há* n *vectores linearmente independentes, não podendo haver mais do que* n. Basta ver que a matriz rectangular formada pelos vectores tem sempre n colunas. O número máximo de colunas independentes é n.

COROLÁRIO 2: *Qualquer sistema de* n *vectores linearmente independentes constitui uma base de* $\mathfrak{M}_n$.

Tendo em conta o teorema de STEINITZ, de (VII, 1, 4), podemos precisar o corolário anterior, por via do seguinte

TEOREMA DA DIMENSÃO: *A dimensão* n, *de* $\mathfrak{M}_n$, *é um invariante.* O teorema significa que não só um sistema de n vectores independentes constitui uma base, mas ainda que uma base tem necessàriamente n vectores independentes.

De facto, se dois sistemas de vectores, um com m vectores, outro com n vectores, constituem bases, o teorema de STEINITZ mostra ter-se, simultâneamente, $n\leqslant m$, $m\leqslant n$.

É muito útil nas aplicações um outro teorema que vamos passar a demonstrar. Imaginemos p vectores $\mathfrak{a}_1,\dots,\mathfrak{a}_p$ e consideremos $m>p$ combinações lineares desses vectores, a saber: $\mathfrak{b}_1,\dots,\mathfrak{b}_m$. Se construirmos a matriz cujas p primeiras linhas são os $\mathfrak{a}_i$ e cujas m seguintes são os $\mathfrak{b}_j$, é claro que, por transformações simples a executar sobre as linhas, podemos reduzir a zero todos os elementos das últimas m linhas. Então, conclui-se que a matriz tem uma característica igual a p, não podendo haver mais do que p dos $\mathfrak{b}_j$ que sejam independentes. A hipótese $m>p$ implica a dependência linear dos referidos $\mathfrak{b}_j$. Tem-se:

TEOREMA 2: *Se* $\mathfrak{a}_1,\dots,\mathfrak{a}_p$ *são* p *vectores linearmente independentes, e se* $\mathfrak{b}_1,\dots,\mathfrak{b}_m$, *com* $m>p$, *são combinações lineares dos* $\mathfrak{a}_i$, *há entre os* $\mathfrak{b}_j$ *uma dependência linear.*

3) **Outro tipo de matriz reduzida** – À teoria das equações lineares, de que adiante nos ocuparemos, interessa ainda uma outra redução da matriz (1), de (VII, 2, 1), fazendo intervir ùnicamente transformações sobre linhas.

Seja r a característica. Como há r colunas linearmente independentes, vamos começar por supor que essas colunas são as primeiras. As transformações simples sobre linhas permitem levar a matriz à forma

$$(1)\qquad \begin{bmatrix} u & a'_{12} & a'_{13} & \cdots & a'_{1n} \\ 0 & a'_{22} & a'_{23} & \cdots & a'_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & a'_{m2} & a'_{m3} & \cdots & a'_{mn} \end{bmatrix},$$

visto que, na 1.ª coluna, não podem figurar elementos todos iguais a zero. Em (1) não pode, se for $r \geqslant 2$, ter-se na 2.ª coluna $a'_{22} = \cdots = a'_{m2} = 0$, visto que, de contrário, a 2.ª coluna seria uma combinação linear da primeira. Transformações simples sobre linhas fazem passar de (1) a

$$\begin{bmatrix} u & a'_{12} & a'_{13} & \cdots & a'_{1n} \\ 0 & u & a''_{23} & \cdots & a''_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & a''_{m3} & \cdots & a''_{mn} \end{bmatrix},$$

e, em seguida, a

$$\begin{bmatrix} u & 0 & a''_{13} & \cdots & a''_{1n} \\ 0 & u & a''_{23} & \cdots & a''_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & a''_{m3} & \cdots & a''_{mn} \end{bmatrix}.$$

O processo continua, até se chegar a obter nas r primeiras colunas elementos todos nulos, salvo os elementos da 1.ª diagonal. Virá

$$\begin{bmatrix} u & 0 \cdots 0 & b_{1,r+1} & \cdots & b_{1n} \\ 0 & u \cdots 0 & b_{2,r+1} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 \cdots u & b_{r,r+1} & \cdots & b_{rn} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 \cdots 0 & b_{m,r+1} & \cdots & b_{mn} \end{bmatrix}.$$

Importante é verificar agora que são compostas de elementos nulos todas as linhas, a partir da de ordem $r+1$. Estudemos, por exemplo, os elementos $b_{r+1,r+1}, \cdots, b_{m,r+1}$. Deverá ter-se $b_{r+1,r+1} = 0 \cdot b_{1,r+1} + 0 \cdot b_{2,r+1} + \cdots + 0 \cdot b_{r,r+1} = \cdots = b_{m,r+1} = 0$. Todas as colunas têm apenas elementos nulos, a partir do elemento de ordem $r+1$.

Se as r primeiras colunas da matriz de que se partiu [matriz (1) de (VII, 2, 1)] não forem independentes, e as r colunas independentes estiverem localizadas doutro modo, o método é aplicável anàlogamente; apenas, no aspecto final, não aparece o elemento u nas r primeiras colunas, mas sim noutras, deixando, por isso, de pertencer à 1.ª diagonal.

TEOREMA: *A matriz (1), de (VII, 2, 1), suposta de característica* r, *pode, por meio de transformações simples sobre linhas, reduzir-se a uma forma análoga à seguinte*

$$\begin{bmatrix} u & 0 \cdots 0 & b_{1,r+1} & \cdots & b_{1n} \\ 0 & u \cdots 0 & b_{2,r+1} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 \cdots u & b_{r,r+1} & \cdots & b_{rn} \\ 0 & 0 \cdots 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 \cdots 0 & 0 & \cdots & 0 \end{bmatrix}.$$

A localização das colunas em que figura o elemento u *pode ser diferente da que se indica.*

§ 3. Equações lineares homogéneas

1) **Submultiplicidades vectoriais** — Um submódulo-$\mathfrak{K}$, de $\mathfrak{M}_n$, diz-se uma *submultiplicidade vectorial de* $\mathfrak{M}_n$. A submultiplicidade zero compõe-se do único vector zero. Se a submultiplicidade é *própria* ($\neq \mathfrak{M}_n$), não pode conter n vectores linearmente independentes. Suponhamo-la $\neq (0)$ e admitamos que $\mathfrak{a}_1, \cdots, \mathfrak{a}_r$ constituem vectores independentes da submultiplicidade, em número máximo. O número r é bem determinado. A submultiplicidade compõe-se dos elementos da forma $\mathfrak{a}_1 \lambda_1 + \cdots + \mathfrak{a}_r \lambda_r$, e apenas desses elementos. Diz-se que r é a *dimensão da submultiplicidade*, a qual será designada por $\mathfrak{M}_r$. Tendo em conta o teorema de STEINITZ, de (VII, 1, 4), pode dar-se o seguinte enunciado:

TEOREMA 1: *Se* $\mathfrak{a}_1, \cdots, \mathfrak{a}_r$ *são vectores constituindo uma base da submultiplicidade* $\mathfrak{M}_r$, *dada a base* $\mathfrak{e}_1, \cdots, \mathfrak{e}_n$, *de* $\mathfrak{M}_n$, *é possível juntar* $n - r$ *vectores* $\mathfrak{e}_j$ *aos* $\mathfrak{a}_i$, *por forma a ter uma base para* $\mathfrak{M}_n$.

OBSERVAÇÃO: É claro que pode enunciar-se um teorema análogo ao anterior, substituindo $\mathfrak{M}_n$ por uma submultiplicidade $\mathfrak{M}_m \supseteq \mathfrak{M}_r$ e os vectores e_j por m vectores base de $\mathfrak{M}_m$.

Tomemos, em seguida, duas submultiplicidades $\mathfrak{M}_{r'}$ e $\mathfrak{M}_{r''}$. Há uma submultiplicidade intersecção $\mathfrak{D} = \mathfrak{M}_{r'} \cap \mathfrak{M}_{r''}$, de dimensão d, assim como uma submultiplicidade soma $\mathfrak{S} = (\mathfrak{M}_{r'}, \mathfrak{M}_{r''})$, de dimensão s, gerada pelas duas submultiplicidades. É válido o

TEOREMA 2: *Entre os números* r', r'', d, s *existe a relação* $r' + r'' = d + s$. Para fazermos a demonstração, tomemos uma base $a_1, \cdots, a_d$, de $\mathfrak{D}$, e completemo-la com $b_1, \cdots, b_{r'-d}$, de modo a formar uma base de $\mathfrak{M}_{r'}$; e completemo-la com $c_1, \cdots, c_{r''-d}$, de modo a formar uma base de $\mathfrak{M}_{r''}$. O conjunto dos a_i, b_j, c_k constitui uma base de $\mathfrak{S}$, como passamos a provar. Sem dúvida que eles permitem exprimir qualquer vector de $\mathfrak{S}$. Basta, portanto, verificar a sua independência. Imaginemos uma relação

$$\sum_{i=1}^{d} a_i \lambda_i + \sum_{j=1}^{r'-d} b_j \mu_j + \sum_{k=1}^{r''-d} c_k \nu_k = 0 .$$

Deduz-se dela $\sum a_i \lambda_i + \sum b_j \mu_j = -\sum c_k \nu_k$, de modo que o elemento de $\mathfrak{S}$ representado por qualquer dos membros da igualdade acabada de escrever pertence simultâneamente a $\mathfrak{M}_{r'}$ e a $\mathfrak{M}_{r''}$, ou seja a $\mathfrak{D}$. Mas, escrevendo, então, com certos ρ_i, $\sum a_i \rho_i = -\sum c_k \nu_k$ ou $\sum a_i \rho_i + \sum c_k \nu_k = 0$, vê-se que os ν_k (assim como os ρ_i) são nulos. Resulta deste modo $\sum a_i \lambda_i + \sum b_j \mu_j = 0$, e, portanto, $\lambda_i = 0$, $\mu_j = 0$, como se deseja. A dimensão de $\mathfrak{S}$ será $s = d + r' - d + r'' - d$, donde se tira $s + d = r' + r''$, como se afirmou.

2) **Sistemas lineares e homogéneos** — Um sistema de equações lineares e homogéneas, com coeficientes em $\mathfrak{K}$, é um sistema da forma

$$(1) \qquad a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = 0, \quad (i = 1, 2, \cdots, m;\ a_{ij} \in \mathfrak{K}),$$

de m equações a n incógnitas x_j. O nosso objectivo é procurar sistemas de valores, em $\mathfrak{K}$, a atribuir aos x_j, por forma a verificar as equações. Esses sistemas de valores dizem-se *soluções* do sistema.

Uma solução evidente é $(0, 0, \cdots 0)$, obtida pondo $x_j = 0$, para todos os valores de j. É aqui cómoda a linguagem a seguir. Uma solução de (1) diz-se um vector de $\mathfrak{M}_n$ (mais precisamente: os valores atribuidos aos x_j são as componentes dum vector de $\mathfrak{M}_n$, numa certa base prèviamente fixada). Então, é imediato este

TEOREMA 1: *Os vectores-solução de (1) formam uma submultiplicidade vectorial de* $\mathfrak{M}_n$. Em particular, pode acontecer que essa submultiplicidade se reduza ao único vector zero.

Para encontrarmos uma base da submultiplicidade em questão, convém-nos introduzir a noção de *sistemas equivalentes*. Dois sistemas da forma (1) dizem-se equivalentes, se tiverem as mesmas soluções.

A matriz $A = (a_{ik})$ do sistema (1) é a matriz tratada em (VII, 2, 1). Se efectuarmos em A transformações dos tipos 1.° e 2.°, a matriz modifica-se, podendo fazer-se corresponder à transformada um sistema linear de que essa transformada seja matriz. É válido este

TEOREMA 2: *Os sistemas da forma (1), que correspondem às matrizes obtidas da matriz de (1) por transformações simples envolvendo apenas linhas, são equivalentes ao sistema (1).* A demonstração, que é extremamente fácil, é deixada ao cuidado do leitor.

Posto isto, imaginemos que é r a característica da matriz A, de (1), e que as primeiras r colunas são linearmente independentes. As transformações simples que envolvem linhas podem levar a matriz à forma referida em (VII, 2, 3). Então, o sistema (1) ficará equivalente ao seguinte:

$$(2) \qquad \begin{aligned} &x_1 + b_{1,r+1}x_{r+1} + \cdots + b_{1n}x_n = 0, \\ &x_2 + b_{2,r+1}x_{r+1} + \cdots + b_{2n}x_n = 0, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots, \\ &x_r + b_{r,r+1}x_{r+1} + \cdots + b_{rn}x_n = 0 . \end{aligned}$$

É agora fácil de encontrar a base que estamos procurando. É a base da submultiplicidade solução de (2). Como há soluções, há certos valores $\alpha_{r+1}, \cdots, \alpha_n$ que podem ser atribuidos aos $x_{r+1}, \cdots, x_n$, resultando daí os valores correspondentes a atribuir aos $x_1, \cdots, x_r$. De facto, (2) revela podermos dar valores quaisquer aos $x_{r+1}, \cdots, x_n$,

resultando deles os valores correspondentes dos $x_1, \cdots, x_r$. Em suma: Se pusérmos $x_{r+1} = \alpha_{r+1}, \cdots, x_n = \alpha_n$, a solução $\mathfrak{x}$, de (2), ou de (1), é

$$\begin{aligned} \mathfrak{x} = &- \mathfrak{e}_1(b_{1,r+1}\alpha_{r+1} + \cdots + b_{1n}\alpha_n) - \mathfrak{e}_2(b_{2,r+1}\alpha_{r+1} + \cdots + b_{2n}\alpha_n) - \\ &- \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots - \\ &- \mathfrak{e}_r(b_{r,r+1}\alpha_{r+1} + \cdots + b_{rn}\alpha_n) + \mathfrak{e}_{r+1}\alpha_{r+1} + \cdots + \mathfrak{e}_n\alpha_n . \end{aligned} \tag{3}$$

Para o caso particular $\alpha_{r+1} = u = 1$, $\alpha_{r+2} = \cdots = \alpha_n = 0$, tem-se

$$\mathfrak{x}_1 = - \mathfrak{e}_1 b_{1,r+1} - \mathfrak{e}_2 b_{2,r+1} - \cdots - \mathfrak{e}_r b_{r,r+1} + \mathfrak{e}_{r+1} ; \tag{4}$$

para o caso particular $\alpha_{r+2} = u = 1$, $\alpha_{r+1} = \alpha_{r+3} = \cdots = \alpha_n = 0$, tem-se

$$\mathfrak{x}_2 = - \mathfrak{e}_1 b_{1,r+2} - \mathfrak{e}_2 b_{2,r+2} - \cdots - \mathfrak{e}_r b_{r,r+2} + \mathfrak{e}_{r+2} ; \text{ etc., até} \tag{4'}$$

$$\mathfrak{x}_{n-r} = - \mathfrak{e}_1 b_{1n} - \mathfrak{e}_2 b_{2n} - \cdots - \mathfrak{e}_r b_{rn} + \mathfrak{e}_n . \tag{4''}$$

Então, (3) pode tomar o aspecto

$$\mathfrak{x} = \mathfrak{x}_1 \alpha_{r+1} + \mathfrak{x}_2 \alpha_{r+2} + \cdots + \mathfrak{x}_{n-r}\alpha_n . \tag{5}$$

Os vectores $\mathfrak{x}_1, \cdots, \mathfrak{x}_{n-r}$ são linearmente independentes, como se conclui das suas próprias expressões, nas quais figuram, respectivamente, $\mathfrak{e}_{r+1}, \cdots, \mathfrak{e}_n$. Em (5) tem-se a totalidade das soluções de (1), o que, repetimos, deve entender-se no sentido seguinte: fixada a base $\mathfrak{e}_1, \cdots \mathfrak{e}_n$, na qual $\mathfrak{x}_1, \cdots, \mathfrak{x}_{n-r}$ têm as expressões (4), (4'), (4''), os valores a atribuir aos x_h, em cada solução, são as componentes do vector $\mathfrak{x}$, definido por (5), com os α_j arbitrários. Tem lugar o

TEOREMA 3: *Um sistema da forma (1), de característica* r *(característica da matriz do sistema), representa uma submultiplicidade vectorial de dimensão* n − r. Este teorema tem um recíproco, do qual vamos ocupar-nos no número seguinte.

3) **Equações duma submultiplicidade vectorial** — Acabámos de ver que todo o sistema linear homogéneo, como o sistema (1) do número anterior, representa uma submultiplicidade. Aqui provaremos que, reciprocamente, dada uma submultiplicidade vectorial qualquer de $\mathfrak{M}_n$ ($\mathfrak{M}_n$ é definida por meio dum sistema de n vectores $\mathfrak{e}_1, \cdots, \mathfrak{e}_n$

independentes e fixados), é possível encontrar um sistema linear e homogéneo cuja solução seja precisamente constituida pela submultiplicidade em questão. Provaremos, pois, este

TEOREMA: *Toda a submultiplicidade vectorial* $\mathfrak{M}_{n-r}$, *de* $\mathfrak{M}_n$, *de dimensão* n − r, *pode ser representada por um sistema linear e homogéneo da forma (1), de (VII, 3, 2), de característica* r. Se a representação for efectivamente possível, o sistema (1), referido, tem de conter, pelo menos r equações. Vamos encontrar exactamente r equações que dão a representação. Para simplicidade de escrita, utilizaremos o símbolo $\mathfrak{a} \cdot \mathfrak{b}$, como abreviatura de $a_1 b_1 + \cdots + a_n b_n$, supostos os a_i as componentes de $\mathfrak{a}$ e os b_j as componentes de $\mathfrak{b}$.

Sejam, então, $\mathfrak{a}_1, \cdots, \mathfrak{a}_{n-r}$ vectores base da multiplicidade dada $\mathfrak{M}_{n-r}$ e consideremos o sistema a seguir, de $n - r$ equações homogéneas:

$$\mathfrak{a}_1 \cdot \mathfrak{x} = 0, \quad \cdots \quad , \mathfrak{a}_{n-r}\,\mathfrak{x} = 0 , \tag{1}$$

com $\mathfrak{a}_i \cdot \mathfrak{x} = a_{i1}\mathfrak{x}_1 + \cdots + a_{in}x_n$; $(i = 1, 2, \cdots, n - r)$. O sistema (1) tem a característica $n - r$ e representa uma submultiplicidade vectorial de ordem r. Se $\mathfrak{b}_1, \cdots, \mathfrak{b}_r$ for uma base dessa multiplicidade, as equações

$$\mathfrak{b}_1 \cdot \mathfrak{x} = 0, \cdots \mathfrak{b}_r \cdot \mathfrak{x} = 0 , \tag{2}$$

formam um sistema de característica r, que representa uma submultiplicidade de dimensão $n - r$. Mas tendo-se, por virtude de (1), $\mathfrak{a}_i \mathfrak{b}_j = 0$, $\cdots$, $\mathfrak{a}_{n-r} \cdot \mathfrak{b}_j = 0$, $(j = 1, 2, \cdots, r)$, vê-se que (2) é satisfeito, pondo $\mathfrak{x} = \mathfrak{a}_1, \cdots, \mathfrak{a}_{n-r}$. Deste modo, (2) representa a submultiplicidade de que se partiu.

BIBLIOGRAFIA

B. VAN DER WAERDEN, *Moderne Algebra*, zweiter Teil, Berlin, 1931.

N. BOURBAKI, *Algèbre*, chapitre II, *Algèbre linéaire*, Paris, 1955.

A. ALMEIDA COSTA, *Grupos abelianos e Anéis e Ideais não comutativos*, Porto, Centro de Estudos Matemáticos, 1942.

J VICENTE GONÇALVES, *Álgebra superior*, 2.º vol., Lisboa, 1950.

E. SPERNER, *Einführung in die analytische Geometrie und Algebra*, erster Teil, Göttingen, 1948.

CAPÍTULO VIII

Espaços lineares. Equações lineares não homogéneas. Módulos sobre anéis de divisão

§ 1. Espaço linear

1) **Introdução dos pontos. Definição de espaço linear** — A noção de *espaço linear a n dimensões* que nos propomos analisar neste Capítulo assenta sobre a noção de multiplicidade vectorial estudada no Capítulo anterior.

Imaginemos uma multiplicidade vectorial $\mathfrak{M}_n$. Vamos introduzir uma noção nova: a noção de *ponto*. Fá-lo-emos à custa dos postulados seguintes: P_1) Existem pontos $A, B, C, \cdots, X, Y, \cdots$; P_2) dois pontos A e B definem um vector $\overrightarrow{AB} = \mathfrak{a} \in \mathfrak{M}_n$; P_3) dados um ponto A e um vector $\mathfrak{a}$, existe um único ponto B tal que $\overrightarrow{AB} = \mathfrak{a}$; P_4) três pontos A, B, C satisfazem à relação $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$.

Posto isto, chamaremos espaço linear a n dimensões, e representá-lo-emos pelo símbolo $\mathfrak{R}_n$, um conjunto de pontos subordinado aos postulados anteriores. É fundamental ter em conta que existe um *postulado de dimensão*, implícito em P_2) e P_3), quando se diz que os vectores postos em causa para cada ponto A constituem uma multiplicidade vectorial a n dimensões.

Devemos dizer que, na definição anterior, há postulados supérfluos. Nós vamos mostrar, por exemplo, que a propriedade associativa $(\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c})$, relativa a vectores, é consequência dos postulados introduzidos para os pontos. Seja A um ponto; construamos, «a partir» de A, o vector $\mathfrak{a}$, e ponhamos $\mathfrak{a} = \overrightarrow{AB}$; em seguida, a partir de ponto B, construamos o vector $\mathfrak{b}$, e ponhamos $\mathfrak{b} = \overrightarrow{BC}$; finalmente, a partir de C, o vector $\mathfrak{c}$ tal que $\mathfrak{c} = \overrightarrow{CD}$. Tem-se $\mathfrak{a} + \mathfrak{b} = \overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$, $(\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \overrightarrow{AC} + \overrightarrow{CD} = \overrightarrow{AD}$. Por outro lado, é $\mathfrak{b} + \mathfrak{c} = \overrightarrow{BC} + \overrightarrow{CD} = \overrightarrow{BD}$, $\mathfrak{a} + (\mathfrak{b} + \mathfrak{c}) = \overrightarrow{AB} + \overrightarrow{BD} = \overrightarrow{AD} = (\mathfrak{a} + \mathfrak{b}) + \mathfrak{c}$, como se afirmou.

Também a partir dos postulados sobre os pontos se pode demonstrar que a equação $\mathfrak{a} + \mathfrak{x} = \mathfrak{b}$ é sempre solúvel em $\mathfrak{x}$. Ponhamos $\mathfrak{a} = \overrightarrow{AB}$, $\mathfrak{b} = \overrightarrow{AC}$. A equação escrever-se-á $\overrightarrow{AB} + \mathfrak{x} = \overrightarrow{AC}$, que é satisfeita pondo $\mathfrak{x} = \overrightarrow{BC}$.

Como, porém, a conservação dos postulados que levaram à noção de multiplicidade vectorial permite o estudo duma tal multiplicidade duma maneira independente, conservaremos a definição dada de $\mathfrak{R}_n$.

TEOREMA: *Todos os pontos de* $\mathfrak{R}_n$ *são obtidos a partir de qualquer ponto* $O_0 \in \mathfrak{R}_n$, *construindo a partir de* O_0 *todos os vectores* $\mathfrak{x} \in \mathfrak{M}_n$. A demonstração é imediata.

2) **Referenciais. Coordenadas** — Chamaremos *referencial* de $\mathfrak{R}_n$ um sistema $O_0(\mathfrak{e}_1, \cdots, \mathfrak{e}_n)$, formado pelo ponto $O_0 \in \mathfrak{R}_n$, escolhido prèviamente de modo arbitrário, e por n vectores de $\mathfrak{M}_n$, linearmente independentes, aplicados a partir de O_0. Então, se X for um ponto de $\mathfrak{R}_n$, tem-se

$$\overrightarrow{O_0X} = \mathfrak{e}_1 \xi_1 + \cdots + \mathfrak{e}_n \xi_n .$$

Os elementos $\xi_i \in \mathfrak{K}$ dizem-se *coordenadas* do ponto X. Em cada referencial, um ponto tem coordenadas determinadas; recìprocamente, um conjunto de n elementos de $\mathfrak{K}$ fixa um ponto, num certo referencial.

Em particular as coordenadas do ponto O_0 são $(0, 0, \cdots, 0)$, pois que $\overrightarrow{O_0O_0} = O$, como se conclui de $\overrightarrow{AO_0} + \overrightarrow{O_0O_0} = \overrightarrow{AO_0}$.

Tomemos dois pontos P e Q, de $\mathfrak{R}_n$. As componentes do vector $\overrightarrow{PQ}$, na base $(\mathfrak{e}_1, \cdots, \mathfrak{e}_n)$, são fáceis de exprimir em função das coordenadas dos dois pontos, no referencial indicado. De facto, supondo

$$\overrightarrow{O_0P} = \mathfrak{e}_1\lambda_1 + \cdots + \mathfrak{e}_n\lambda_n, \qquad \overrightarrow{O_0Q} = \mathfrak{e}_1\mu_1 + \cdots + \mathfrak{e}_n\mu_n,$$

em virtude de se ter $\overrightarrow{O_0P} + \overrightarrow{PQ} = \overrightarrow{O_0Q}$, obtem-se

$$\sum \mathfrak{e}_i\lambda_i + \overrightarrow{PQ} = \sum \mathfrak{e}_i\mu_i, \text{ ou seja } \overrightarrow{PQ} = \sum_{i=1}^{n} \mathfrak{e}_i(\mu_i - \lambda_i).$$

Se, a partir dum ponto O'_0, construirmos os vectores duma submultiplicidade $\mathfrak{M}_h \subseteq \mathfrak{M}_n$, definimos um espaço linear $\mathfrak{R}_h \subseteq \mathfrak{R}_n$, que se diz *subespaço* de $\mathfrak{R}_n$. A dimensão de $\mathfrak{R}_h$ é a dimensão de $\mathfrak{M}_h$, como já dissemos.

Dois subespaços lineares, $\mathfrak{R}_h$ e $\mathfrak{R}_m$, de $\mathfrak{R}_n$, dizem-se *paralelos*, se uma das submultiplicidades vectoriais correspondentes estiver contida na outra. Se os dois espaços têm um ponto comum, um deles está contido no outro. Pode dar-se o caso, todavia, de não existir ponto comum. Assim:

TEOREMA 1: *Dois subespaços lineares paralelos ou não têm ponto comum ou um deles está contido no outro.* Para se encontrar dois subespaços paralelos sem ponto comum, podemos proceder do modo a seguir. Tomemos $O_0(\mathfrak{a}_1, \cdots, \mathfrak{a}_t)$ como referencial dum subespaço $\mathfrak{R}_t$, de dimensão t; depois, suposto $t < n$, tomemos um ponto $O'_0 \notin \mathfrak{R}_t$, isto é, tomemos um ponto O'_0 tal que o vector $\overrightarrow{O_0O'_0}$ não se exprima em $\mathfrak{a}_1, \cdots, \mathfrak{a}_t$. O subespaço $\mathfrak{R}_h$, de referencial $O'_0(\mathfrak{a}_1, \cdots, \mathfrak{a}_h)$, $h \leqslant t$, é paralelo a $\mathfrak{R}_t$ e não tem com ele ponto comum.

Uma outra questão interessante trataremos ainda neste número. Consideremos $p+1$ pontos de $\mathfrak{R}_n$, a saber: $O_0, O_1, \cdots, O_p$. Pode acontecer que os vectores $\overrightarrow{O_0O_1}, \overrightarrow{O_0O_2}, \cdots, \overrightarrow{O_0O_p}$ sejam linearmente independentes. Então, os $p+1$ pontos não pertencem a um subespaço linear de dimensão inferior a p. Diremos:

TEOREMA 2: *Se* p + 1 *pontos de* $\mathfrak{R}_n$ *não pertencem a um subespaço linear de dimensão menor que* p, *há um e um só subespaço linear com* p *dimensões contendo aqueles pontos.*

3) **Transformações de coordenadas** — É de grande importância para as aplicações o problema da *transformação de coordenadas*, tanto para vectores como para pontos.

Duma maneira precisa, quanto aos vectores, tomemos duas bases $(\mathfrak{e}_1, \cdots, \mathfrak{e}_n)$ e $(E_1, \cdots, E_n)$, de $\mathfrak{M}_n$. Excepcionalmente, o que também sucederá adiante, utilizamos aqui letras latinas maiúsculas para representar vectores. Então, supondo

$$E_j = \sum_{h=1}^{n} \mathfrak{e}_h p_{hj}, \qquad (j = 1, 2, \cdots n;\ p_{hj} \in \mathfrak{K}),$$

trata-se de obter as componentes η_j, dum vector $\mathfrak{x}$, na base dos E_j, admitindo que se conhecem as componentes ξ_j, de $\mathfrak{x}$, na base dos $\mathfrak{e}_j$. Pondo

$$\mathfrak{x} = \sum_{j=1}^{n} \mathfrak{e}_j\xi_j, \qquad \mathfrak{x} = \sum_{j=1}^{n} E_j\eta_j,$$

vê-se que se tem, sucessivamente:

$$\mathfrak{x} = \sum_{j=1}^{n} E_j\eta_j = \sum_{j,h} \mathfrak{e}_h p_{hj}\eta_j = \sum_{h} \mathfrak{e}_h \left(\sum_{j} p_{hj}\eta_j\right),$$

pelo que

$$\xi_h = \sum_{j=1}^{n} p_{hj}\eta_j, \qquad (h = 1, 2, \cdots, n). \tag{1}$$

Poderíamos, inversamente, imaginar os $\mathfrak{e}_j$ expressos nos E_j e chegar a obter os η_h expressos nos ξ_j. As fórmulas (1) resolvem o problema que nos intessa relativo a vectores, que não é pròpriamente um problema de transformação de coordenadas, mas de transformação de componentes.

Todavia, como vimos em (VIII, 1, 2), os ξ_j e os η_j podem ser interpretados como coordenadas dum ponto. Se imaginarmos, então,

o espaço $\mathfrak{R}_n$ e o referencial $O_0(e_1, \cdots, e_n)$, admitindo que é $\overrightarrow{O_0X} = \mathfrak{x} = \sum e_i \xi_i$, na verdade, as fórmulas (1) resolvem o que pode chamar-se o problema da *mudança de direcção dos eixos, com conservação da origem*. Os elementos η_h e ξ_h são, respectivamente, as coordenadas de X no referencial $O_0(E_1, \cdots, E_n)$ e no referencial da mesma origem O_0, mas de eixos e_j diferentes.

Se há simples *mudança de origem*, passando-se de O_0 a O'_0, mas conservando os eixos e_i, então, da relação, $\overrightarrow{O_0X} = \overrightarrow{O_0O'_0} + \overrightarrow{O'_0X}$, supondo que as coordenadas de O'_0, em $O_0(e_1, \cdots, e_n)$, são $\alpha_1, \cdots, \alpha_n$, tira-se $\sum e_i \xi_i = \sum e_i \alpha_i + \sum e_i \xi'_i$, $(i = 1, 2, \cdots, n)$, ou seja

$$\xi'_i = \xi_i - \alpha_i, \quad (i = 1, 2, \cdots n). \tag{2}$$

Finalmente, pode haver mudança de origem e da direcção dos eixos. Os dois referenciais são $O_0(e_1, \cdots, e_n)$ e $O'_0(E_1, \cdots, E_n)$. A fixação do 2.º referencial no primeiro faz-se à custa das igualdades

$$\overrightarrow{O_0O'_0} = \sum_{i=1}^{n} e_i \alpha_i, \qquad E_j = \sum_{i=1}^{n} e_i p_{ij}, \qquad (j = 1, 2, \cdots n).$$

Então, dado o ponto X, tem-se

$$\overrightarrow{O_0X} = \mathfrak{x} = \sum_{i=1}^{n} e_i \xi_i, \qquad \overrightarrow{O_0O'_0} + \overrightarrow{O'_0X} = \overrightarrow{O_0X}, \qquad \overrightarrow{O'_0X} = \mathfrak{x}' = \sum_{i=1}^{n} E_i \eta_i,$$

e, portanto,

$$\sum_{i=1}^{n} e_i \alpha_i + \sum_{j=1}^{n} E_j \eta_j = \sum_{i=1}^{n} e_i \xi_i, \qquad \sum_{i=1}^{n} e_i \alpha_i + \sum_{j,i}^{n} e_i p_{ij} \eta_j = \sum_{i=1}^{n} e_i \xi_i,$$

donde se conclui

$$\xi_i = \alpha_i + \sum_{i} p_{ij} \eta_j, \qquad (i = 1, 2, \cdots, n). \tag{3}$$

É claro que poderíamos obter fórmulas resolvidas em ordem aos η_i, desde que supuséssemos os e_j expressos nos E_i, assim como admitissemos dadas as coordenadas do ponto O_0 no referencial $O'_0(E_1, \cdots, E_n)$.

As fórmulas (1), (2) e (3) são as que desejávamos. Nas fórmulas (3) estão contidas as outras como casos particulares. Convém fazer, entretanto, algumas

OBSERVAÇÕES: Dissemos como, em vez de (1), poderíamos obter outras igualdades que dessem os η_h expressos em ξ_j. Da teoria das equações lineares, a desenvolver no § próximo e no Capítulo IX, concluir-se-á que as expressões dos η_h se obtêm também resolvendo pre-precisamente as equações (1) em ordem aos η_h. A solução existe e é única. O mesmo se diz das equações (3).

§ 2. Equações lineares não homogéneas

1) **Sobre a existência de soluções** — O problema a resolver neste § consiste em saber em que condições tem solução, em $\mathfrak{K}$, um sistema de equações lineares com coeficientes tomados em $\mathfrak{K}$, e, depois, em determinar as soluções, se existirem. De modo diferente do que aconteceu em (VII, 3, 2), há, em geral, segundos membros não nulos nas diferentes equações.

É dado o sistema

$$\begin{aligned} &a_{i1} x_1 + a_{i2} x_2 + \cdots + a_{in} x_n = b_i, \\ &(i = 1, 2, \cdots, m), \quad (a_{ij}, b_i \in \mathfrak{K}), \end{aligned} \tag{1}$$

de m equações a n incógnitas x_h.

Se houver soluções em $\mathfrak{K}$, podemos considerar cada conjunto de valores a atribuir aos x_h, por forma a satisfazer a (1), como um ponto de $\mathfrak{R}_n$, cujas coordenadas são aqueles valores, num referencial prèviamente fixado. Introduzindo ainda os vectores

$$\mathfrak{a}_h = \{a_{1h}, a_{2h}, \cdots, a_{mh}\}, \qquad \mathfrak{b} = \{b_1, \cdots, b_m\},$$

dum certo espaço $\mathfrak{R}_m$, o sistema (1) pode escrever-se abreviadamente

$$\mathfrak{a}_1 x_1 + \mathfrak{a}_2 x_2 + \cdots + \mathfrak{a}_n x_n = \mathfrak{b}. \tag{2}$$

Sob esta forma (2), reconhece-se que é condição necessária e suficiente, para que (1) tenha soluções, que a multiplicidade vectorial construida

sobre $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$, ou gerada por $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$, contenha o vector $\mathfrak{b}$. Claro que essa multiplicidade é a mesma que a que é gerada por aqueles $\mathfrak{a}_j$, de entre os $\mathfrak{a}_h$, que são linearmente independentes em $\mathfrak{M}_m$ (multiplicidade vectorial relativa a $\mathfrak{R}_m$ e não submultiplicidade de $\mathfrak{M}_n$!). E estes últimos são em número igual ao número máximo de colunas (ou de linhas) independentes da matriz

$$(3) \qquad \begin{bmatrix} a_{11} & a_{12} \cdots a_{1n} \\ a_{21} & a_{22} \cdots a_{2n} \\ \cdots\cdots\cdots\cdots \\ a_{m1} & a_{m2} \cdots a_{mn} \end{bmatrix},$$

chamada *matriz simples* do sistema (1). Como para a existência de soluções é necessário e basta que $\mathfrak{b}$ se exprima nos $\mathfrak{a}_j$, segue-se que o número máximo de colunas independentes da matriz

$$\begin{bmatrix} a_{11} & a_{12} \cdots a_{1n} & b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1} & a_{m2} \cdots a_{mn} & b_m \end{bmatrix},$$

chamada *matriz ampliada* do sistema (1), deve ser o mesmo que o de (3). Tem lugar o seguinte

TEOREMA: *É condição necessária e suficiente, para que o sistema (1), com coeficientes em* $\mathfrak{K}$, *seja solúvel em* $\mathfrak{K}$, *que sejam iguais as características da matriz simples e da matriz ampliada do referido sistema.* O valor comum das duas características diz-se, então, *característica do sistema.*

2) **Subespaços lineares** — As soluções do sistema (1) do número anterior foram já interpretadas como pontos de $\mathfrak{R}_n$, num referencial $O_0(\mathfrak{e}_1, \cdots, \mathfrak{e}_n)$, fixado prèviamente. Se $P(x_1, \cdots, x_n)$ e $Q(y_1, \cdots, y_n)$ são dois pontos soluções, o vector $\overrightarrow{PQ} = \mathfrak{z}$, de componentes $y_1 - x_1 = z_1, \cdots, y_n - x_n = z_n$ verifica o sistema homogéneo correspondente, obtido de (1) fazendo $b_i = 0$, $(i = 1, 2, \cdots, m)$. Inversamente, se o vector $\mathfrak{z}$, de componentes $z_1, \cdots, z_n$ é solução do sistema homogéneo, então, tomando o ponto $P(x_1, \cdots, x_n)$, solução de (1), também o ponto $Q(y_1 = x_1 + z_1, \cdots, y_n = x_n + z_n)$ é solução de (1). Podemos dar este enunciado:

TEOREMA 1: *A totalidade dos pontos-soluções de (1), do número anterior, constitui um espaço linear com* $n - r$ *dimensões, se* r *for a característica do sistema. Esse espaço linear é subespaço de* $\mathfrak{R}_n$. O teorema é imediato, à face das considerações feitas e da terminologia introduzida em (VIII, 1, 2). Ele tem o recíproco seguinte:

TEOREMA 2: *Todo o subespaço linear de* $\mathfrak{R}_n$, *de dimensão* $n - r$, *pode ser representado por um sistema não homogéneo, da forma (1) do número anterior, de característica* r. Dar o subespaço é dar, num certo referencial, um dos seus pontos e a multiplicidade vectorial $\mathfrak{M}_{n-r}$ correspondente. Esta multiplicidade vectorial pode ser definida por um sistema homogéneo de característica r da forma

$$a_{i1} x_1 + \cdots + a_{in} x_n = 0, \qquad (i = 1, 2, \cdots, m).$$

Se designarmos por $\xi_1, \cdots, \xi_n$ as coordenadas do ponto conhecido do subespaço, ponhamos $a_{i1} \xi_1 + \cdots + a_{in} \xi_n = b_i$, $(i = 1, 2, \cdots, m)$, e escrevamos o sistema não homogéneo

$$a_{i1} x_1 + \cdots + a_{in} x_n = b_i, \qquad (i = 1, 2, \cdots, m).$$

Este sistema é solúvel e representa, no referencial de que se partiu, o subespaço linear dado.

OBSERVAÇÃO: O sistema não homogéneo foi suposto com coeficientes em $\mathfrak{K}$ e as soluções respectivas procuraram-se em $\mathfrak{K}$. Imaginemos, porém, que $\mathfrak{K}$ se considera um subcorpo dum corpo Ω, de modo que o sistema é também um sistema com coeficientes em Ω. O reconhecimento das soluções em Ω implica as mesmas operações que o seu reconhecimento em $\mathfrak{K}$. E, assim, tem lugar este

TEOREMA 3: *Se* Ω *é um corpo e* $\mathfrak{K} \subseteq \Omega$ *um subcorpo, dado um sistema linear com coeficientes em* $\mathfrak{K}$, *a solubilidade do sistema, em* Ω, *implica a sua solubilidade em* $\mathfrak{K}$.

§ 3. Módulos sobre anéis de divisão.

1) **Considerações gerais** — Em (VII, 1, 3), ao tratarmos das multiplicidades vectoriais, indicámo-las como exemplos importantes de módulos livres sobre um corpo $\mathfrak{K}$. Vamos analisar aqui, muito ràpi-

damente, os *módulos livres sobre um anel de divisão* $\mathfrak{D}$. Suporemos, de resto, que se trata dum módulo direito sobre $\mathfrak{D}$, que representaremos por $\mathfrak{M}_0$.

As afirmações feitas em (VII, 1, 2) são de carácter geral. As noções de dependência e de independência linear, assim como os teoremas que com elas se relacionam, e que foram tratados em (VII, 1, 3), podem repetir-se textualmente para o módulo $\mathfrak{M}_0$. Deve ter-se simplesmente em conta que, por exemplo, no teorema 1 do citado lugar, se deve escrever $a_1 = -a_2\lambda_2\lambda_1^{-1} - \cdots - a_p\lambda_p\lambda_1^{-1}$, em vez do que, então, foi escrito.

O teorema de STEINITZ, demonstrado em (VII, 1, 4), também é válido para módulos sobre anéis de divisão. Ele permite, tal como em (VII, 2, 2), estabelecer a invariância da dimensão de $\mathfrak{M}_0$, quando se supõe que $\mathfrak{M}_0$ é um módulo livre finito.

Admitindo que $e_1, \cdots, e_n$ é uma base independente de $\mathfrak{M}_0$ e escrevendo $\mathfrak{M}_0 = e_1\mathfrak{D} + \cdots + e_n\mathfrak{D}$, obtem-se $\mathfrak{M}_0$ como soma directa de módulos cíclicos irredutíveis, na terminologia de (III, 1, 6). Este facto leva a provar doutro modo o teorema da invariância da dimensão, recorrendo à teoria das séries de composição, mais particularmente ao teorema de JORDAN-HÖLDER, demonstrado em (IV, 2, 2). De facto, $\mathfrak{M}_0$ admite a série de composição

$$\mathfrak{M}_0 = e_1\mathfrak{D} + \cdots + e_n\mathfrak{D} \supset e_1\mathfrak{D} + \cdots + e_{n-1}\mathfrak{D} \supset \cdots \supset e_1\mathfrak{D} \supset (0),$$

de comprimento n.

$\mathfrak{M}_0$ é um módulo completamente redutível, no sentido preciso dado em (IV, 3, 4). Do teorema desse lugar, conclui-se a proposição seguinte, que também pode justificar-se, como em (VII, 3, 1), por via do teorema de STEINITZ: Dado um submódulo $\mathfrak{M}'$, de $\mathfrak{M}_0$, é sempre $\mathfrak{M}_0 = \mathfrak{M}' + \mathfrak{M}''$, onde $\mathfrak{M}''$ é uma soma directa de certos submódulos cíclicos $e_i\mathfrak{D}$.

Inversamente, suponhamos $\mathfrak{M}_0 = e_1\mathfrak{D} + \cdots + e_n\mathfrak{D}$ e $\mathfrak{M}'$ um submódulo de $\mathfrak{M}$ da forma $\mathfrak{M}' = v_1\mathfrak{D} + \cdots + v_m\mathfrak{D}$, onde cada $v_i\mathfrak{D}$ é também simples. Vamos encontrar para $\mathfrak{M}'$ uma base do tipo

$$(1) \qquad w_i = e_i - \sum_{k=m+1}^{n} e_k a_{ki}, \qquad (a_{ki} \in \mathfrak{D};\ i = 1, 2, \cdots, m),$$

desde que os e_i se ordenem de modo conveniente.

Completemos, com efeito, os v_j com os e_k necessários à construção duma base de $\mathfrak{M}_0$. Ordenando os e_j de modo que os e_k sejam $e_{m+1}, \cdots, e_n$, a base de $\mathfrak{M}_0$ será $(v_1, \cdots, v_m;\ e_{m+1}, \cdots, e_n)$. Se se tiver

$$e_i = \sum_{j=1}^{m} v_j\alpha_j + \sum_{k=m+1}^{n} e_k\alpha_{ki}, \qquad (i = 1, 2, \cdots, m;\ \alpha_j, \alpha_{ki} \in \mathfrak{D}),$$

vê-se que é

$$w_i = e_i - \sum_{k=m+1}^{n} e_k\alpha_{ki} = \sum_{j=1}^{m} v_j\alpha_j \in \mathfrak{M}'.$$

Os elementos w_i, acabados de construir, são linearmente independentes, como resulta da sua própria expressão. Eles constituem uma base para $\mathfrak{M}'$, do tipo (1), que se diz *base normal de* $\mathfrak{M}'$.

2) **Equações lineares com coeficientes em** $\mathfrak{D}$ — Consideremos as m equações

$$(1) \qquad \sum_{k=1}^{n} a_{jk}x_k = b_j, \qquad (j = 1, 2, \cdots, m),$$

nas quais os a_{jk} e os b_j são elementos de $\mathfrak{D}$ e os x_k são incógnitas. Elas constituem um sistema de equações lineares, que nos propomos resolver. Trata-se, então, de encontrar valores em $\mathfrak{D}$, a atribuir aos x_k, por forma que sejam satisfeitas as mesmas equações.

Designando com $e_1, \cdots, e_n$ *símbolos* diferentes, imaginemos o módulo livre $\mathfrak{M}_{00}$ formado pelos elementos da forma $t = \sum c_k e_k, (c_k \in \mathfrak{D})$. Trata-se dum módulo esquerdo. Os primeiros membros das equações (1), desde que os x_k se substituam pelos e_k, são elementos t, que designaremos por $t_j, (j = 1, 2, \cdots, m)$. Dos elementos t_j, podem não ser todos linearmente independentes. Designemos por $t_1, t_2 \cdots, t_r, (r \gtrless m,\ r \gtrless n)$, os que são independentes. Então, tem-se

$$\begin{aligned} t_{r+1} &= a^{(1)}t_1 + a^{(2)}t_2 + \cdots + a^{(r)}t_r, \\ t_{r+2} &= b^{(1)}t_1 + b^{(2)}t_2 + \cdots + b^{(r)}t_r, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots, \end{aligned}$$

onde os $a^{(i)}$ e os $b^{(j)}$ pertencem a $\mathfrak{D}$.

Condições necessárias para que o sistema (1) seja solúvel é que se tenha

$$b_{r+1} = a^{(1)} b_1 + a^{(2)} b_2 + \cdots + a^{(r)} b_r ,$$
$$b_{r+2} = b^{(1)} b_1 + b^{(2)} b_2 + \cdots + b^{(r)} b_r ,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

Estas condições são suficientes, como vamos ver. Comecemos por observar que é possível encontrar $n - r$ dos símbolos e_i, os quais, juntamente com $t_1, \cdots, t_r$, constituam uma base para $\mathfrak{M}_{00}$. Sejam $e_{r+1}, \cdots, e_n$ tais e_i. Então, em particular, os n símbolos e_i admitem as expressões

$$(2) \qquad \begin{matrix} e_{r+1} = e_{r+1}, \\ \cdots\cdots\cdots \\ e_n = e_n, \end{matrix} \qquad e_i = \sum_{k=1}^{r} b_{ik} t_k + \sum_{j=r+1}^{n} c_{ij} e_j , \quad (i = 1, 2, \cdots, r),$$

sem esquecer que é

$$(3) \qquad t_j = \sum_{k=1}^{n} a_{jk} e_k , \quad (j = 1, 2, \cdots, m).$$

A substituição, nestas últimas igualdades, dos valores dados em (2), leva a r identidades (correspondentes à substituição nas primeiras r relações) nos t_j, ao mesmo tempo que dá as expressões já conhecidas de $t_{r+1}, t_{r+2}, \cdots$. Nas m igualdades (3) desaparecem, pois, entre si, todos os e_j. Nessas condições, se pusermos

$$(4) \qquad x_i = \sum_{k=1}^{r} b_{ik} b_k + \sum_{j=r+1}^{n} c_{ij} x_j , \quad (i = 1, 2, \cdots, r),$$

onde os x_j são elementos quaisquer de $\mathfrak{M}_{00}$, nas equações (1), desaparecem igualmente entre si os x_k, originando-se r identidades nos b_j, ao mesmo tempo que se obtêm as expressões já conhecidas de $b_{r+1}, b_{r+2}, \cdots$, como se deseja. As igualdades (4) dão, pois, soluções de (1).

Para se verificar que não há outras soluções, imaginemos um sistema de valores de x_k satisfazendo a (1). Como a substituição de (3) em (2) leva a identidades nos e_j, a substituição de (1) em (4) leva a r identidades nos x_i, pelo que os r primeiros dos x_i podem ter as expressões dadas em (4).

O número r, relativo ao sistema proposto, diz-se *característica do sistema*. Esse número indica o número dos primeiros membros que

são linearmente independentes e o verdadeiro número das incógnitas. As restantes $n - r$ incógnitas tomam valores arbitrários em $\mathfrak{D}$.

3) **Resolução por um número finito de operações** — A solução efectiva do sistema (1) do número anterior pode encontrar-se do modo que vai ver-se. Resolve-se a 1.ª equação (3) do mesmo número em ordem a e_1 (ou a outro e_i) e substitui-se a expressão obtida nas restantes equações. Encontram-se, assim, $e_1, t_2, \cdots, t_m$ expressos sob a forma

$$e_1 \to (t_1, e_2, \cdots, e_n); \quad t_2 \to (t_1, e_2, \cdots, e_n); \cdots; \quad t_m \to (t_1, e_2, \cdots, e_n);$$

em seguida, resolve-se a equação que dá a nova expressão de t_2 em ordem a e_2 (ou a outro e_i) e substitui-se o valor encontrado em $t_3, \cdots, t_m$, o que dará

$$e_1 \to (t_1, e_2, \cdots, e_n); \quad e_2 \to (t_1, t_2, e_3, \cdots, e_n), \cdots; \quad t_m \to (t_1, t_2, e_3, \cdots, e_n);$$

e assim sucessivamente, até

$$\begin{aligned} &e_1 \to (t_1, e_2, \cdots, e_n), \\ &e_2 \to (t_1, t_2, \cdots, e_n), \\ &\cdots\cdots\cdots\cdots, \\ &e_r \to (t_1, t_2, \cdots, t_r, e_{r+1}, \cdots, e_n), \\ &t_{r+1} \to (t_1, t_2, \cdots, t_r, e_{r+1}, \cdots, e_n) \to (t_1, t_2, \cdots, t_r), \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots, \\ &t_m \to (t_1, t_2, \cdots, t_r, e_{r+1}, \cdots, e_n) \to (t_1, t_2, \cdots, t_r), \end{aligned}$$

pois que, na verdade, ao efectuar-se a passagem às relações anteriores, não se encontram $e_{r+1}, \cdots, e_n$ nas expressões de $t_{r+1}, \cdots, t_n$.

Retrocede-se agora, substituindo a expressão encontrada para e_r em $e_{r-1}, \cdots, e_2, e_1$; depois, o valor de e_{r-1} em $e_{r-2}, \cdots, e_1$, até se chegar a obter $e_1, \cdots, e_r$ expressos, como se deseja, em $t_1, \cdots, t_r$, $e_{r+1}, \cdots, e_n$.

Este processo de *eliminação* indicará, de resto, por si mesmo, o número r.

É interessante observar que, se os coeficientes a_{ik}, que figuram no sistema dado, pertencerem a um subanel de divisão de $\mathfrak{D}$, podemos fazer afirmação análoga à do conteúdo do teorema 3, de (VIII, 2, 2).

Na verdade, o processo de eliminação, introduzindo unicamente os inversos dos elementos do subanel e os produtos dos elementos do subanel de divisão, leva a soluções com coeficientes pertencentes a esse subanel ou indica a incompatibilidade do sistema.

BIBLIOGRAFIA

H. Weyl, *Temps, espace et matière*, Blanchard, Paris, 1922.
B. L. van der Waerden, *Moderne Algebra*, zweiter Teil, 1931.
A. Almeida Costa, *Grupos abelianos e Anéis e Ideais não comutativos*, Centro de Estudos Matemáticos, Porto, 1942.
E. Sperner, *Einführung in die analytische Geometrie und Algebra*, erster Teil, 1948.
J. Vicente Gonçalves, *Algebra superior*, 2.º vol., 1950.
A. Almeida Costa, *Sistemas hipercomplexos e representações*, Centro de Estudos Matemáticos, Porto, 1948.

CAPÍTULO IX

Determinantes. Transformações lineares

§ 1. Teoria geral dos determinantes

1) **Definição e propriedades** — Em estreita correlação com as teorias desenvolvidas nos dois Capítulos anteriores, encontra-se a teoria dos determinantes, de que nos vamos ocupar.

Dada a multiplicidade $\mathfrak{M}_n$, numa certa base $e_1, \cdots, e_n$, chama-se *determinante* uma função de n vectores $a_1, \cdots, a_n$, representada por $D(a_1, \cdots, a_n)$, que satisfaz às três condições seguintes: $D_1)$ $D(a_1, \cdots a_n)$ não se altera, quando o vector a_i se substitui por $a_i + a_h, (h \neq i)$; $D_2)$ $D(a_1, \cdots, a_n)$ vem multiplicado por λ, se um dos vectores a_i se substitui por $a_i\lambda$; $D_3)$ $D(e_1, \cdots, e_n) = u \in \Re$.

Mostrar que existe uma tal função D, que ela é única e reconhecer algumas das suas propriedades fundamentais, é o objectivo essencial deste parágrafo.

A fim de simplicarmos a escrita, adoptaremos as convenções a seguir. Partindo dum certo determinante $D(a_1, \cdots, a_n)$, escreveremos depois, nas questões a tratar com esse determinante, apenas a letra D para o representar. Se algum dos vectores de D se vier a modificar, ocasionando possível alteração do valor de D, poremos apenas em evidência o vector ou os vectores alterados. O primeiro dos índices de cada vector escrito, isolado ou não, dará a sua localização em D.

Assim, $D(a_i + a_j\lambda, a_k + a_m\mu)$ significa que os vectores a_i e a_k foram alterados e, respectivamente, substituídos pelos que se indicam.

Quando não houver possibilidade de utilizar a regra indicada, usar-se-á notação conveniente, que não traga qualquer confusão.

Seja dado, então, $D(a_1, \cdots, a_n) = D$. Se supomos $a_i = 0$, D não se altera quando a_i se multiplica por $\lambda = 0$. Em virtude de D_2), podemos dizer:

TEOREMA 1: *Se, num determinante* D, *um dos vectores é nulo, o determinante é igual a zero.*

Voltemos a D. Sabemos que se tem, em face de D_2) e de D_1),

$$D(a_k\lambda_k) = D\lambda_k = D(a_i + a_k\lambda_k, a_k\lambda_k), \quad (i \neq k),$$

$$D(a_i + a_k\lambda_k, a_k\lambda_k) = D(a_i + a_k\lambda_k, a_k)\lambda_k = D\lambda_k,$$

de sorte que $D(a_i + a_k\lambda_k) = D$. Repetindo o processo, chega-se ao seguinte

TEOREMA 2: *O determinante* D *não muda de valor, se um dos vectores* a_i *se substitui por* $a_i + \sum a_k\lambda_k$, *suposto o somatório não estendido ao índice* i.

COROLÁRIO 1: *O determinante* D *é nulo, se existir uma dependência linear entre os* a_j. *Em particular é nulo um determinante com dois vectores iguais.* Seja, com efeito, $a_1\lambda_1 + \cdots a_n\lambda_n = 0$, e imaginemos, por exemplo, $\lambda_n \neq 0$. Ter-se-á $a_n = -a_1\frac{\lambda_1}{\lambda_n} - \cdots - a_{n-1}\frac{\lambda_{n-1}}{\lambda_n}$, e também, pelo teorema anterior, $D\left(a_n + a_1\frac{\lambda_1}{\lambda_n} + \cdots + a_{n-1}\frac{\lambda_{n-1}}{\lambda_n}\right) = D = D(a_n = 0) = 0$, como se deseja.

Suponhamos agora que, no determinante D, trocamos entre si dois vectores a_i e a_k. Essa troca pode ser levada a cabo à custa dum certo número de operações, segundo o esquema

$$\begin{aligned} D = D(a_i, a_k) \to D(a_i, a_k + a_i) = D \to D(a_i, -a_k - a_i) = -D \to \\ \to D(-a_k, -a_k - a_i) = -D \to D(a_k, -a_k - a_i) = \\ = D \to D(a_k, -a_i) = D \to D(a_k, a_i) = -D. \end{aligned}$$

Conclui-se:

TEOREMA 3: *Se, no determinante* D, *se trocam dois vectores, o determinante muda de sinal.* Resulta daqui a consequência a seguir, já incluída, sem qualquer excepção, no corolário 1.

COROLÁRIO 2: *Se o corpo* $\mathfrak{K}$ *tem uma característica* $\neq 2$, *um determinante com dois vectores iguais é nulo.*

É extremamente importante, para a determinação efectiva da função D, a proposição de que nos vamos ocupar. Ela exprime-se pela igualdade $D(a + b, a_2, \cdots, a_n) = D(a, a_2, \cdots, a_n) + D(b, a_2, \cdots, a_n)$, a qual tem outras análogas, supondo ser outro vector $a_i \neq a_1$ que se substitui pela soma $a + b$.

Admitindo que os vectores $a_2, \cdots, a_n$ são linearmente dependentes, a igualdade é válida, pelo facto de os três determinantes que nela figuram serem nulos. Mas, se os a_j são independentes, podemos completá-los com um vector c. por forma a ter uma base de $\mathfrak{M}_n$. Então, será $a = c\lambda + a_2\lambda_2 + \cdots + a_n\lambda_n$, $b = c\mu + a_2\mu_2 + \cdots + a_n\mu_n$, e, portanto,

$$\begin{aligned} &D(a, a_2, \cdots, a_n) = D(c\lambda, a_2, \cdots, a_n) = D(c, a_2, \cdots, a_n)\lambda, \\ &D(b, a_2, \cdots, a_n) = \qquad\qquad = D(c, a_2, \cdots, a_n)\mu, \\ &D(a + b, a_2, \cdots, a_n) = \qquad\qquad = D(c, a_2, \cdots, a_n)(\lambda + \mu), \end{aligned}$$

que levam imediatamente à igualdade em questão.

Uma repetição do raciocínio permite o enunciado seguinte, conhecido sob o nome de *teorema da adição*:

TEOREMA 4: *Supondo* $x_i = \sum_{h_i=1}^{n} a_{ih_i}\lambda_{ih_i}$, $(i = 1, 2, \cdots, n)$, *tem-se:*

$$\begin{aligned} &D(x_1, \cdots x_n) = D\left(\sum a_{1h_1}\lambda_{1h_1}, x_2, \cdots, x_n\right) = \\ &= \sum_{h_1=1}^{n} D(a_{1h_1}, x_2, \cdots, x_n)\lambda_{1h_1} = \cdots = \sum_{h_1,\ldots,h_n=1}^{n} D(a_{1h_1}, \cdots, a_{nh_n})\lambda_{1h_1}\cdots\lambda_{nh_n}. \end{aligned} \tag{1}$$

Claramente que não há necessidade de se admitir haver nas expressões de todos os x_i o mesmo número de parcelas. Alguns dos coeficientes λ_{ih_i} podem ser nulos.

COROLÁRIO 3: *Admitindo que é* $D(a_1, \cdots, a_n) = 0$, *é também* $D(x_1, \cdots, x_n) = 0$, *se os* x_i *se exprimem nos* a_j. Na verdade, os vec-

tores a_{ih_i} do teorema anterior são os mesmos para os diferentes x_i. No último somatório das igualdades (1) figura o determinante $D(a_{1h_1}, \cdots a_{nh_n})$. O primeiro dos índices dos vectores a pode suprimir-se, o que levará a

$$(2) \qquad D(x_1, \cdots, x_n) = \sum_{h_1, \ldots, h_n = 1}^{n} D(a_{h_1}, \cdots, a_{h_n}) \lambda_{1h_1} \cdots \lambda_{nh_n}.$$

Quando a dois índices h_j se dá o mesmo valor, a parcela correspondente é nula. Só há que considerar aquelas parcelas para as quais $(h_1, \cdots, h_n)$ contém todos os números $1, 2, \cdots, n$. Então, o determinante $D(a_{h_1}, \cdots, a_{h_n})$ é nulo, por ser, à parte o sinal, igual ao determinante $D(a_1, \cdots, a_n)$. As diferentes parcelas do 2.º membro de (2) são nulas e o corolário está provado.

É agora que vai intervir a condição D_3) da definição de determinante, para nos levar a uma conclusão do maior interesse, a saber:

TEOREMA 5: *Supostos* $a_1, \cdots, a_n$ *linearmente independente é* $D(a_1 \cdots, a_n) \neq 0$. Se pudesse ter-se $D = 0$, como os a_i constituem uma base de $\mathfrak{M}_n$, seria $D(x_1, \cdots, x_n) = 0$ quaisquer que fossem os x_i, em particular ter-se-ia $D(e_1, \cdots, e_n) = 0$, contra a condição D_3).

OBSERVAÇÃO: Como consequência das considerações feitas, é de observar o que vai seguir-se. Se fôsse definida uma função $\Phi(a_1, \cdots, a_n)$ com as propriedades D_1) e D_2), atribuídas a D, e com a propriedade D'_3): $\Phi(e_1, \cdots, e_n) = 0$; então a função Φ seria nula, quaisquer que fossem os a_j. Em todos os casos, uma função Φ, com as propriedades D_1) e D_2), será da forma

$$(3) \qquad \Phi(a_1, \cdots, a_n) = \Phi(e_1, \cdots, e_n) \cdot D(a_1, \cdots, a_n),$$

pois que, sendo $\Phi(e_1, \cdots, e_n) \neq 0$, é $\dfrac{\Phi(a_1, \cdots, a_n)}{\Phi(e_1, \cdots, e_n)}$ uma função com as propriedades D_1), D_2) e D_3).

2) **A existência e univocidade do determinante** — Do teorema da adição, pondo $a_i = e_1 a_{i1} + \cdots + e_n a_{in}$, $(i = 1, 2, \cdots, n)$, resulta

$$D(a_1, \cdots, a_n) = \sum_{h_1, \ldots, h_n = 1}^{n} D(e_{h_1}, \cdots, e_{h_n}) \, a_{1h_1} \cdots a_{nh_n}.$$

Como o somatório se pode estender apenas àquelas parcelas para as quais os h_i são todos diferentes, a igualdade anterior será escrita sob a forma

$$(1) \qquad D = \sum_{(h_1, \ldots, h_n)} D(e_{h_1}, \cdots, e_{h_n}) \, a_{1h_1} \cdots a_{nh_n},$$

onde o símbolo $(h_1, \cdots, h_n)$ lembra precisamente aquela circunstância. Examinemos em seguida o determinante $D(e_{h_1}, \cdots, e_{h_n})$, para o compararmos com o determinante $D(e_1, \cdots, e_n)$. Os valores de ambos podem diferir apenas no sinal. Decomponhamos a permutação $\begin{pmatrix} 1 & 2 & \cdots & n \\ h_1 & h_2 & \cdots & h_n \end{pmatrix}$ em transposições. Se a cada transposição (ij) fizermos corresponder uma troca dos vectores e_i e e_j, num determinante em que $e_1, \cdots, e_n$ se encontram numa ordem qualquer, vemos que, partindo do determinante $D(e_1, \cdots, e_n)$, e efectuando, sucessivamente, as trocas indicadas pelas transposições que figuram como factores na decomposição da permutação em causa, pela ordem pela qual se devem considerar esses mesmos factores na referida decomposição, se chega precisamente a $D(e_{h_1}, \cdots, e_{h_n}) = \pm D(e_1, \cdots, e_n)$, conforme for par ou ímpar o número de transposições em questão. A igualdade (1) reduz-se desta forma a

$$(2) \qquad D(a_1, \cdots, a_n) = \sum_{(h_1, \ldots, h_n)} P(h_1, \cdots, h_n) \, a_{1h_1} \cdots a_{nh_n},$$

onde $P(h_1, \cdots, h_n) = \pm 1$ indica a paridade da permutação em estudo, também chamada paridade de $(h_1, \cdots, h_n)$. Um processo para a determinação dessa paridade é o que vai seguir-se. Suponhamos que, em $(h_1, \cdots, h_n)$, há m_1 números superiores a 1 precedendo 1, ou, como costuma dizer-se, há m_1 inversões relativamente a 1. Por meio de m_1 trocas consecutivas, pode colocar-se 1 em primeiro lugar, partindo de $(h_1, \cdots, h_n)$. Depois, se houver m_2 inversões relativamente a 2, na nova permutação obtida [número que é o mesmo que em $(h_1, \cdots, h_n)$], fazem-se m_2 trocas, a fim de se colocar 2 em segundo lugar. O processo continua, até se dispôrem todos os números na sua ordem natural, à custa de $m_1 + m_2 + \cdots + m_\varrho$ trocas, tantas quantas as inversões em $(h_1, \cdots, h_n)$. Será, precisamente, $P(h_1, \cdots, h_n) = (-1)^{m_1 + m_2 + \cdots + m_\varrho}$.

Para que o leitor compreenda perfeitamente esta igualdade, vamos tomar um exemplo. Em (2 4 3 5 1), há as inversões $2-1, 4-1, 3-1, 5-1$, relativas ao número 1, e a inversão $4-3$, relativa ao número 3. É

$m_1 = 4$, $m_2 = m_4 = m_5 = 0$, $m_3 = 1$, e $m_1 + m_2 + \cdots + m_5 = 5$. Ora tem-se também

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} = (12)\,(14)\,(13)\,(15)\,(34)\,.$$

É $P(2,4,3,5,1) = (-1)^5 = -1$.

OBSERVAÇÃO: Ser-nos-à útil posteriormente uma observação que vamos fazer. Tomemos uma permutação

$$\begin{pmatrix} 1 & 2 \cdots n \\ i_1 & i_2 \cdots i_n \end{pmatrix}.$$

Se trocármos dois dos i_j, como isso equivale a multiplicá-la por uma transposição, segue-se que, na disposição dos i_k, muda a paridade das inversões. Quando se escreve um produto

$$a_{i_1 j_1}\ a_{i_2 j_2} \cdots a_{i_n j_n}\,, \tag{3}$$

onde os i_k e os j_m vão de 1 a n, se somármos às inversões nos i_k as inversões nos j_m, obtemos um número cuja paridade não é alterada por troca de dois dos factores do produto. Isso significa que, em (3), podemos dispor os factores por uma ordem qualquer, para calcularmos a referida paridade. Então, (2) pode tomar este outro aspecto

$$D(\mathfrak{a}_1, \cdots, \mathfrak{a}_n) = \sum_{(j_1, \cdots, j_n)} P(i_1, \cdots, i_n) \cdot P(j_1, \cdots, j_n)\ a_{i_1 j_1} \cdots a_{i_n j_n}\,.$$

Em geral, há conveniência em fixar prèviamente $(i_1, i_2, \cdots, i_n)$.

Posto isto, estamos em condições de afirmar que, se a função determinante existe, ela não pode deixar de ser dada pela igualdade (2). A *univocidade* está provada, provada que seja a existência.

Quanto a esta última, vamos exactamente demonstrar que o 2.º membro de (2) tem as propriedades $D_1)$, $D_2)$ e $D_3)$. A propriedade $D_2)$ é imediata, porque, em cada parcela do 2.º membro de (2), figura uma componente, e uma só, de cada vector $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$. Se um dos vectores se multiplica por λ, todas as suas componentes aparecem multiplicadas por λ, e, assim, cada parcela de (2) aparece multiplicada por λ. A propriedade $D_3)$ também se verifica, pelo facto de ser, quando $\mathfrak{a}_i = \mathfrak{e}_i$, $a_{ik_i} = 0$, se $k_i \neq i$, $(i = 1, 2, \cdots, n)$, e $a_{ik_i} = 1$, se $k_i = i$. Deste

modo, é $D(\mathfrak{e}_1, \cdots, \mathfrak{e}_n) = P(1, 2, \cdots, n)\ 1 \cdots 1 = 1$. Resta a propriedade $D_1)$. Substituamos $\mathfrak{a}_i$ por $\mathfrak{a}_i + \mathfrak{a}_j$. Virá

$$\begin{aligned} D(\mathfrak{a}_i + \mathfrak{a}_j) &= \sum_{(k_1, \ldots, k_n)}^{n} P(k_1, \cdots, k_n)\ a_{1k_1} \cdots (a_{ik_i} + a_{jk_i}) \cdots a_{nk_n} = \\ &= \sum P(k_1, \cdots, k_n)\ a_{1k_1} \cdots a_{ik_i} \cdots a_{nk_n} + \\ &+ \sum P(k_1, \cdots, k_n)\ a_{1k_1} \cdots a_{i-1,k_{i-1}}\ a_{jk_i} \cdots a_{nk_n}\,. \end{aligned}$$

Deste último membro, o primeiro somatório é igual a $D(\mathfrak{a}_1, \cdots, \mathfrak{a}_n)$, pelo que, se o segundo somatório for nulo, fica provada a afirmação. Isto vai resultar de haver, nessse segundo somatório, parcelas iguais duas a duas, com mudança de sinal. À parcela $P(k_1, \cdots, k_i, \cdots, k_j, \cdots, k_n) \cdot a_{1k_1} \cdots a_{jk_i} \cdots a_{jk_j} \cdots a_{nk_n}$ corresponde, de facto, a parcela

$$P(k_1, \cdots, k_j, \cdots, k_i, \cdots, k_n)\ a_{1k_1} \cdots a_{jk_j} \cdots a_{jk_i} \cdots a_{nk_n}\,,$$

esta segunda relativa ao caso em que se dá a k_i o valor k_j e a k_j o valor k_i. Sendo $P(k_1, \cdots, k_i, \cdots, k_j, \cdots, k_n) = -P(k_1, \cdots, k_j, \cdots, k_i, \cdots, k_n)$, o resultado desejado fica estabelecido. Tem lugar o importante

TEOREMA 1: *Consideremos uma base de* $\mathfrak{M}_n$ *e tomemos, nessa base, os vectores* $\mathfrak{a}_i = \sum_{j=1}^{n} \mathfrak{e}_j a_{ij}$, $(i = 1, 2, \cdots, n)$. *Existe a função determinante* $D(\mathfrak{a}_1, \cdots, \mathfrak{a}_n)$, *que é única e tem a expressão*

$$D(\mathfrak{a}_1, \cdots, \mathfrak{a}_n) = \sum_{(h_1, \ldots, h_n)}^{n} P(h_1, \cdots, h_n)\ a_{1h_1}\ a_{2h_2} \cdots a_{nh_n}\,. \tag{4}$$

§ 2. Os quadros dos determinantes

1) **Quadros. Alguns tipos de quadros**—A expressão encontrada para D sugere se escreva o quadro

$$D = \begin{vmatrix} a_{11} & a_{12} & \cdots a_{1n} \\ a_{21} & a_{22} & \cdots a_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{n1} & a_{n2} & \cdots a_{nn} \end{vmatrix}, \tag{1}$$

onde se consideram *linhas* e *colunas* do determinante, de modo análogo ao que aconteceu no caso das matrizes. O número n chama-se *ordem*

do determinante. Os elementos $a_{11}, a_{22}, \cdots, a_{nn}$ formam a *diagonal principal* de D e os elementos $a_{n1}, a_{n-2,2}, \cdots a_{1n}$ formam a *segunda diagonal.*

Neste número, vamos referir alguns tipos especiais de quadros, dando o valor dos mesmos, por meio de considerações particulares.

1.º EXEMPLO: Façamos a hipótese de se ter $a_{ih} = 0$, sempre que $i > h$. Significa isto que são nulos todos os elementos abaixo da 1.ª diagonal. O determinante diz-se *triangular*. Na formula (4) do número anterior, qualquer termo que contenha a_{nh_n} é nulo, salvo se contiver a_{nn}. Depois, nos termos que ficam, são nulos todos aqueles que contenham $a_{n-1,h_{n-1}}$, salvo se $h_{n-1} = n-1$. O raciocínio prossegue, chegando a concluir-se que, neste exemplo, se tem $D = P(1,2,\cdots,n)\, a_{11}\, a_{22} \cdots a_{nn} = a_{11}\, a_{22} \cdots a_{nn}$.

2.º EXEMPLO: Na hipótese de se ter $a_{ih} = 0$, sempre que $h > i$, o resultado é o mesmo. O determinante, chamado ainda triangular, reduz-se ao produto dos elementos da sua primeira diagonal.

3.º EXEMPLO: Tomemos agora um quadro com o aspecto

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1r} & 0 & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2r} & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{r1} & a_{r2} & \cdots & a_{rr} & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & b_{11} & b_{12} & \cdots & b_{1s} \\ 0 & 0 & \cdots & 0 & b_{21} & b_{22} & \cdots & b_{2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & b_{s1} & b_{s2} & \cdots & b_{ss} \end{vmatrix},$$

no qual $r + s = n$. Se imaginarmos os b_{hl} como constantes e os a_{ij} como variáveis, podemos conceber $\Delta = \Phi(\mathfrak{a}_1, \cdots, \mathfrak{a}_r)$ como uma função dos vectores $\mathfrak{a}_1, \cdots, \mathfrak{a}_r$, num espaço a r dimensões, desde que se tomem para componentes dos $\mathfrak{a}_i$ os valores $a_{i1}, \cdots, a_{ir}$, numa certa base $\mathfrak{e}_1, \cdots, \mathfrak{e}_r$. Verifica-se que Φ goza das propriedades D_1) e D_2), de sorte que será

$$\Delta = \Phi(\mathfrak{e}_1, \cdots, \mathfrak{e}_r) \cdot \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & a_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ a_{r1} & a_{r2} & \cdots & a_{rr} \end{vmatrix},$$

onde $\Phi(\mathfrak{e}_1, \cdots, \mathfrak{e}_r)$ resulta de Δ fazendo todos os a_{ij} iguais a zero, salvo os da 1.ª diagonal, que se põem iguais a $u \in \mathfrak{R}$.

Em seguida, $\Phi(\mathfrak{e}_1, \cdots, \mathfrak{e}_r)$ pode imaginar-se como uma função $\Psi(\mathfrak{b}_1, \cdots, \mathfrak{b}_s)$, dos vectores $\mathfrak{b}_1, \cdots, \mathfrak{b}_s$, num espaço a s dimensões, desde que se tomem para componentes dos $\mathfrak{b}_j$ os elementos $b_{j1}, \cdots, b_{js}$, numa certa base $\mathfrak{h}_1, \cdots, \mathfrak{h}_s$. Pela mesma razão de acima, será

$$\Psi(\mathfrak{b}_1, \cdots, \mathfrak{b}_s) = \Phi(\mathfrak{e}_1, \cdots, \mathfrak{e}_r) = \Psi(\mathfrak{h}_1, \cdots, \mathfrak{h}_s) \cdot \begin{vmatrix} b_{11} & \cdots & b_{1s} \\ \cdots & \cdots & \cdots \\ b_{s1} & \cdots & b_{ss} \end{vmatrix},$$

onde $\Psi(\mathfrak{h}_1, \cdots, \mathfrak{h}_s)$ resulta de $\Psi(\mathfrak{b}_1, \cdots, \mathfrak{b}_s)$ fazendo todos os b_{kl} iguais a zero, salvo os da 1.ª diagonal, que se põem iguais a $u \in \mathfrak{R}$. Visto ser $\Psi(\mathfrak{h}_1, \cdots, \mathfrak{h}_s) = u$, chega-se a

$$\Delta = \begin{vmatrix} a_{11} & \cdots & a_{1r} \\ \cdots & \cdots & \cdots \\ a_{r1} & \cdots & a_{rr} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & \cdots & b_{1s} \\ \cdots & \cdots & \cdots \\ b_{s1} & \cdots & b_{ss} \end{vmatrix}.$$

2) **Produto de determinantes** — Como uma questão que se segue imediatamente às que se trataram no número anterior, propomo-nos agora indicar uma regra para se efectuar o produto de dois quadros da mesma ordem n. A este respeito, vamos estabelecer a igualdade

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & \cdots & b_{1n} \\ \cdots & \cdots & \cdots \\ b_{n1} & \cdots & b_{nn} \end{vmatrix} = \begin{vmatrix} \sum_{j=1}^{n} a_{1j}\, b_{j1} & \cdots & \sum_{j=1}^{n} a_{1j}\, b_{jn} \\ \cdots & \cdots & \cdots \\ \sum_{j=1}^{n} a_{nj} b_{j1} & \cdots & \sum_{j=1}^{n} a_{nj} b_{jn} \end{vmatrix}.$$

Para isso, ponhamos

$$(1) \qquad \mathfrak{c}_i = \mathfrak{b}_1\, a_{i1} + \cdots + \mathfrak{b}_n\, a_{in}, \quad (i = 1, 2, \cdots, n),$$

de sorte que

$$D(\mathfrak{c}_1, \cdots, \mathfrak{c}_n) = \sum_{(h_1, \cdots, h_n)} D(\mathfrak{b}_{h_1}, \cdots, \mathfrak{b}_{h_n})\, a_{1h_1} \cdots a_{nh_n} =$$

$$= \sum_{(h_1, \cdots, h_n)} P(h_1, \cdots, h_n)\, D(\mathfrak{b}_1, \cdots, \mathfrak{b}_n)\, a_{1h_1} \cdots a_{nh_n} =$$

$$= D(\mathfrak{b}_1, \cdots, \mathfrak{b}_n) \sum_{(h_1, \cdots, h_n)} P(h_1, \cdots h_n)\, a_{1h_1} \cdots a_{nh_n} =$$

$$= D(\mathfrak{b}_1, \cdots, \mathfrak{b}_n) \cdot \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}.$$

Se imaginarmos os $\mathfrak{b}_j$ escolhidos prèviamente pelas relações

$$\mathfrak{b}_j = \mathfrak{e}_1 b_{j1} + \cdots + \mathfrak{e}_n b_{jn}, \tag{2}$$

nas quais $\mathfrak{e}_1, \cdots, \mathfrak{e}_n$ formam a base de $\mathfrak{M}_n$, tomada *a priori* sob a condição $D(\mathfrak{e}_1, \cdots, \mathfrak{e}_n) = u$, vemos que

$$D(\mathfrak{b}_1, \cdots, \mathfrak{b}_n) = \sum_{(j_1, \cdots, j_n)} D(\mathfrak{e}_{j_1}, \cdots, \mathfrak{e}_{j_n}) b_{1j_1} \cdots b_{nj_n} =$$

$$= \sum_{(j_1, \cdots, j_n)} P(j_1, \cdots, j_n) D(\mathfrak{e}_1, \cdots, \mathfrak{e}_n) b_{1j_1} \cdots b_{nj_n} = \begin{vmatrix} b_{11} \cdots b_{1n} \\ \cdots\cdots\cdots \\ b_{n1} \cdots b_{nn} \end{vmatrix},$$

de sorte que

$$D(\mathfrak{c}_1, \cdots, \mathfrak{c}_n) = \begin{vmatrix} a_{11} \cdots a_{1n} \\ \cdots\cdots\cdots \\ a_{n1} \cdots a_{nn} \end{vmatrix} \cdot \begin{vmatrix} b_{11} \cdots b_{1n} \\ \cdots\cdots\cdots \\ b_{n1} \cdots b_{nn} \end{vmatrix}. \tag{3}$$

Por outro lado, porém, as componentes dos $\mathfrak{c}_i$, tendo em conta (1) e (2), são

$$c_{i1} = \sum_{j=1}^{n} a_{ij} b_{j1}, \cdots, c_{in} = \sum_{j=1}^{n} a_{ij} b_{jn},$$

pelo que, escrevendo, em vez do 1.º membro de (3) o respectivo quadro, fica estabelecida a igualdade desejada. Podemos enunciar o chamado *teorema da multiplicação de determinantes*:

TEOREMA 1: *Obtem-se o produto de dois determinantes de ordem* n, *escrevendo um determinante de ordem* n, *cujo elemento* c_{ih}, *do cruzamento da linha de ordem* i, *com a coluna de ordem* h, *é a soma dos produtos dos elementos da linha de ordem* i, *do 1.º factor, pelos elementos da coluna de ordem* h, *do 2.º factor, tomados aos pares, sucessivamente.*

Voltemos de novo ao quadro (1), de (IX, 2, 1), que pode representar-se abreviadamente por $|a_{ih}|$, com i índice de linha e h índice de coluna. Na multiplicidade $\mathfrak{M}_n$, consideremos, depois, os vectores coluna do quadro, a saber:

$$\mathfrak{a}'_i = |a_{1i}, a_{2i}, \cdots, a_{ni}|, \qquad (i = 1, 2, \cdots, n).$$

O quadro, cujo valor é conhecido, é função dos $\mathfrak{a}'_i$, tendo-se

$$\Theta(\mathfrak{a}'_i, \cdots, \mathfrak{a}'_n) = |a_{ih}| = D(\mathfrak{a}_1, \cdots, \mathfrak{a}_n).$$

Vamos ver que Θ goza das propriedades D_1), D_2) e D_3), o que nos permitirá escrever

$$\Theta(\mathfrak{a}'_1, \cdots, \mathfrak{a}'_n) = D(\mathfrak{a}'_1, \cdots, \mathfrak{a}'_n) = \begin{vmatrix} a_{11} a_{21} \cdots a_{n1} \\ a_{12} a_{22} \cdots a_{n2} \\ \cdots\cdots\cdots \\ a_{1n} a_{2n} \cdots a_{nn} \end{vmatrix}$$

e enunciar o seguinte

TEOREMA 2 — *O valor dum determinante não se altera quando se mudam as linhas em colunas e as colunas em linhas (rotação espacial de 180º à volta da 1.ª diagonal).* A propriedade D_2) é consequência imediata da igualdade (4), de (IX, 1, 2), pois que cada termo do respectivo somatório tem um e um só elemento de cada coluna. A propriedade D_3) é válida, porque, se fizermos $\mathfrak{a}'_i = \mathfrak{e}_i$, $(i = 1, 2, \cdots, n)$, o quadro em estudo é exactamente o quadro correspondente a $D(\mathfrak{e}_1, \cdots, \mathfrak{e}_n)$. Quanto à propriedade D_1), imaginemos que se substitui o quadro por este outro

$$\begin{vmatrix} a_{11} \cdots a_{1,i-1} \; a_{1i} + a_{1k} \cdots a_{1n} \\ a_{21} \cdots a_{2,i-1} \; a_{2i} + a_{2k} \cdots a_{2n} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n1} \cdots a_{n,i-1} \; a_{ni} + a_{nk} \cdots a_{nn} \end{vmatrix}, \tag{4}$$

isto é, que se considera o quadro obtido do quadro 1, de (IX, 2, 1), por substituição de $\mathfrak{a}'_i$ por $\mathfrak{a}'_i + \mathfrak{a}'_k$. Verifica-se imediatamente que é

$$\Theta(\mathfrak{a}'_1, \cdots, \mathfrak{a}'_i + \mathfrak{a}'_k, \cdots, \mathfrak{a}'_n) = \Theta(\mathfrak{a}'_1, \cdots, \mathfrak{a}'_n) \cdot D(\mathfrak{e}_1, \cdots, \mathfrak{e}_{k-1}, \mathfrak{e}_k + \mathfrak{e}_i, \cdots, \mathfrak{e}_n),$$

onde, é claro, este último determinante é um quadro no qual todas as linhas, à excepção da linha de ordem k, apenas têm o elemento diagonal igual a $u \in \mathfrak{R}$, enquanto que os restantes elementos são nulos. Na linha de ordem k são iguais a u o elemento diagonal e o elemento da coluna de ordem i.

Efectuando, de facto, o produto indicado no 2.º membro da última igualdade escrita, tendo em conta a regra de multiplicação de determinantes, encontra-se o determinante (4). Mas, como $D(\mathfrak{e}_1, \cdots, \mathfrak{e}_{k-1}, \mathfrak{e}_k + \mathfrak{e}_i, \cdots, \mathfrak{e}_n) = 1$, obtém-se ainda $\Theta(\mathfrak{a}'_1, \cdots, \mathfrak{a}'_{i-1}, \mathfrak{a}'_i + \mathfrak{a}'_k, \cdots, \mathfrak{a}'_n) = \Theta(\mathfrak{a}'_1, \cdots, \mathfrak{a}'_n)$, como se deseja.

OBSERVAÇÃO — Os resultados acabados de encontrar permitem-nos dar outra regra para o produto de determinantes, diferente da regra

contida no teorema 1, esta última assim designada: *regra de multiplicação de linhas por colunas.*

Na verdade, se substituirmos o 2.º factor do produto pelo determinante obtido dele por troca de linhas com colunas, o novo determinante é igual ao anterior. A multiplicação, feita em seguida pela regra efectivamente demonstrada, leva a concluir-se: a multiplicação de dois determinantes pode efectuar-se de *linha por linha.*

Há, anàlogamente, regras de multiplição de colunas por linhas e de colunas por colunas.

Citemos agora outros exemplos de determinantes que convém conhecer.

DETERMINANTE HEMI-SIMÉTRICO — Um determinante $D=|a_{ik}|$ diz-se *hemi-simétrico*, se o quadro correspondente satisfizer às condições $a_{ih}=-a_{ih}$, se $h\neq i$, e $a_{ii}=0$, $(i,h=1,2,\cdots,n)$. Trocando, num tal determinante, as linhas com as colunas, obtém-se outro determinante D', igual a D, que também resulta de D por mudança de sinal de todas as linhas. Supondo D de ordem ímpar, tem-ee $D'=(-1)^n D=-D=D$, o que leva à seguinte proposição:

TEOREMA 3 (JACOBI) — *Se $\mathfrak{K}$ não tem a característica 2, um determinante hemi-simétrico de ordem ímpar, com elementos de $\mathfrak{K}$, é nulo.* Acrescentemos que esta proposição é geral.

DETERMINANTE SIMÉTRICO — Um determinante D diz-se *simétrico*, se o quadro correspondente verificar a condição $a_{ih}=a_{hi}$. Tanto os determinantes simétricos como os hemi-simétricos têm propriedades interessantes, que podem encontrar-se no livro de *Álgebra Superior* indicado na Bibliografia deste Capítulo.

3) **Sobre o cálculo dos determinantes** — Dado o determinante $D=|a_{ik}|$, $(i,k=1,2,\cdots,n)$, *um menor de D* é um determinante extraído de D e contendo $r<n$ linhas e colunas. O determinante formado pelos elementos das $n-r$ linhas e das $n-r$ colunas restantes diz-se *menor complementar* daquele menor. A *classe* dum menor é dada pela soma de todos os índices, tanto das linhas como das colunas, que figuram nos elementos da diagonal principal do menor. Se essa soma é par, o menor é de *classe par*; de contrário, é de *classe ímpar.*

Se D_r é um menor de D, com r linhas e r colunas, e D'_{n-r} é o seu menor complementar, o menor complementar de D'_{n-r} é D_r. Vê-se imediatamente que dois menores complementares um do outro pertencem à mesma classe.

Sejam s e s' as somas dos índices das diagonais principais de D_r e D'_{n-r}. Diz-se *complemento algébrico* de D_r a expressão $(-1)^s D'_{n-r}=(-1)^{s'} D'_{n-r}$. O complemento algébrico de D'_{n-r} é $(-1)^s D_r=(-1)^{s'} D_r$. Se se tem $r=1$, é, por exemplo, $D_r=D_1=|a_{ij}|=$ determinante do único elemento a_{ij}. O seu complemento algébrico é $(-1)^{i+j} D'_{n-1}$. Neste caso, poremos $(-1)^{i+j} D'_{n-1}=A_{ji}$.

Dadas estas definições, vamos indicar um processo de cálculo dum determinante, cómodo em certos casos, nos quais se evita, portanto, o emprego, quase sempre laborioso, da igualdade (4) de (IX, 1, 2).

Em face da referida igualdade, vê-se que um elemento a_{ij} do quadro D, posto em factor comum nas parcelas do desenvolvimento de D que o contenham, aparece multiplicado por uma soma cujas parcelas, à parte o sinal de cada uma delas, representam os termos do desenvolvimento do menor complementar de a_{ij}. Ora vamos verificar que a soma dos termos em que figura a_{ij} se pode escrever sob a forma $a_{ij}A_{ji}$. Um termo de A_{ji} tem o aspecto $T=(-1)^{i+j}(-1)^f a_{1h_1}\cdots a_{i-1,h_{i-1}}\,a_{i+1,h_{i+1}}\cdots a_{nh_n}$, onde f designa o número de inversões de $(h_1,\cdots,h_{i-1},h_{i+1},\cdots,h_n)$. Tem assim de verificar-se que a quantidade $(-1)^{i+j+f} a_{ij}a_{1h_1}\cdots a_{i-1,h_{i-1}}a_{i+1,h_{i+1}}\cdots a_{nh_n}$, que é, à parte o sinal, um termo do desenvolvimento de D, tem o sinal que lhe cabe nesse desenvolvimento. Tal sinal é dado, como resulta do que se disse em (IX, 1, 2), pela soma das inversões dos dois sistemas $(i,1,2,\cdots,i-1,i+1,\cdots,n)$ e $(j,h_1,h_2,\cdots,h_{i-1},h_{i+1},\cdots,h_n)$, soma que é $(i-1)+f+(j-1)$, precisamente da paridade de $i+j+f$.

O resultado que acabamos de mostrar permite-nos escrever o desenvolvimento de D, segundo os elementos da linha de ordem i, sob a forma

$$D=\sum_{j=1}^{n} a_{ij}A_{ji},\quad (i=1,2,\cdots,n),$$

ou, segundo os elementos da coluna de ordem j, sob a forma

$$D=\sum_{i=1}^{n} a_{ij}A_{ji}=\sum_{i=1}^{n} A_{ji}a_{ij},\quad (j=1,2,\cdots,n).$$

Diremos:

TEOREMA 1: *O valor dum determinante é a soma dos produtos dos elementos duma linha ou duma coluna pelos respectivos complementos algébricos.*

Sabemos que um determinante é nulo, se contiver dois vectores-linha ou dois vectores-coluna iguais. Então, tem-se

$$\sum_{j=1}^{n} a_{ij} A_{jk} = 0, \qquad \sum_{i=1}^{n} A_{ki} a_{ij} = 0,$$

sendo, na primeira igualdade, $k \neq i$ e $k, i = 1, 2, \cdots, n$; enquanto que, na segunda, $k \neq j$ e $k, j = 1, 2, \cdots, n$. É válido o

TEOREMA 2: *A soma dos produtos dos elementos duma linha (ou duma coluna) de* D *pelos complementos algébricos dos elementos correspondentes doutra linha (ou doutra coluna) é igual a zero.*

APLICAÇÃO: Estamos agora em condição de fazer o cálculo que vai indicar-se, do chamado determinante de VANDERMONDE. Tem o aspecto

$$D = \begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \cdots & \cdots & \cdots & & \cdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{vmatrix} = D_n.$$

Operações imediatas levam a

$$D_n = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & a_2 - a_1 & a_2^2 - a_2 a_1 & & a_2^{n-1} - a_2^{n-2} a_1 \\ \cdots & \cdots & \cdots & & \cdots \\ 1 & a_n - a_1 & a_n^2 - a_n a_1 & \cdots & a_n^{n-1} - a_n^{n-2} a_1 \end{vmatrix},$$

de modo que, fazendo o desenvolvimento segundo os elementos da primeira linha, encontramos

$$D_n = (a_2 - a_1)(a_3 - a_1) \cdots (a_n - a_1) \cdot \begin{vmatrix} 1 & a_2 & \cdots & a_2^{n-2} \\ 1 & a_3 & \cdots & a_3^{n-2} \\ \cdots & \cdots & & \cdots \\ 1 & a_n & \cdots & a_n^{n-2} \end{vmatrix} = \prod_{i \neq 1} (a_i - a_1) \cdot D_{n-1},$$

onde D_{n-1} é um determinante de VANDERMONDE de ordem $n-1$. Admitindo que, para D_{n-1}, se tem $D_{n-1} = \prod_{j>i} (a_j - a_i)$, $(i = 2, \cdots, n-1;\ j = 3, \cdots, n)$,

resultará $D_n = \prod_{j>i} (a_j - a_i)$, $(i = 1, 2, \cdots, n-1;\ j = 2, \cdots, n)$.

Obteve-se, pois, o valor de D_n por um método de indução, visto que, para $n = 2$, é $D_2 = \begin{vmatrix} 1 & a_1 \\ 1 & a_2 \end{vmatrix} = a_2 - a_1$.

§ 3. Determinantes, matrizes e equações lineares

1) **Sobre a característica duma matriz** — É útil definir a característica duma matriz rectangular por um processo diferente do que se utilizou em (VII, 2, 2). Para esse efeito, demonstraremos este

TEOREMA 1: *A característica* r *duma matriz* A *é igual a ordem do determinante de mais alta ordem, não nulo, que é possível extrair de* A. Em primeiro lugar, se pode extrair-se de A um determinante de ordem r não nulo, há r linhas em A formando uma sub-matriz de A, nas quais se encontram r colunas linearmente independentes. A característica da sub-matriz é r (igual ao número das suas linhas) e a característica da matriz A não pode ser inferior a r. Inversamente, se uma matriz tem uma característica r, há r linhas linearmente independentes formando uma sub-matriz de característica r. Essa sub-matriz conterá r colunas igualmente independentes. O determinante formado por essas r colunas é $\neq 0$. O teorema é agora imediato.

A busca da característica duma matriz pode ser muito facilitada por um teorema que vamos ainda estabelecer. Se a característica de A é o número r, todos os determinantes de ordem $r+1$ extraídos de A são nulos, como vimos. Basta, porém, considerar um único determinante A, de ordem r, não nulo, extraído de A, para se reconhecer, à custa dos determinantes de ordem $r+1$ extraídos de A, mas que admitem A como menor de 1.ª ordem, que r é a característica. Duma maneira precisa, tem-se:

TEOREMA 2: *Se* $\Delta \neq 0$ *é um determinante de ordem* r, *extraído de* A, *e se todos os determinantes de ordem* r+1, *extraídos de* A, *que têm* A *como menor, são nulos,* r *é a característica de* A. Como a característica se conserva em face das transformações simples, imagi-

nemos o determinante Δ contido r nas primeiras linhas e colunas de A. Será

$$A = \begin{bmatrix} \Delta_0 & a_{1,r+1} \cdots a_{1n} \\ \cdots\cdots\cdots & \cdots\cdots \\ a_{m1} \cdots a_{m,r+1} \cdots a_{mn} \end{bmatrix} = \begin{bmatrix} \Delta_0 & P \\ Q & R \end{bmatrix},$$

onde Δ_0 é a matríz formada pelos elementos de Δ e P, Q, R são matrizes rectangulares de significado imediato. Ora, em $\Delta_0 = \begin{bmatrix} a_{11} \cdots a_{1r} \\ \cdots\cdots \\ a_{r1} \cdots a_{rr} \end{bmatrix}$, as linhas são linearmente independentes, de sorte que r é a característica de Δ_0. Os elementos $a_{i1}, a_{i2}, \cdots a_{ir}$, com $i = r+1, \cdots, n$, exprimem-se linearmente nas r linhas de Δ_0. Assim, as transformações simples permitem reduzir A à forma $B = \begin{bmatrix} \Delta_0 & P \\ 0 & T \end{bmatrix}$, onde 0 é a matriz nula de $m-r$ linhas e de r colunas e T é uma nova matriz rectangular. Um determinante qualquer. de ordem $r+1$, extraído de A, que contenha Δ, tem o seu correspondente em B. Deste último determinante, a linha de ordem $r+1$ é uma combinação linear de $r+1$ linhas de A (na parte respectiva), entre as quais as r primeiras, de sorte que a propriedade do enunciado do teorema vale para a matriz B, isto é: todos os determinantes de ordem $r+1$, extraídos de B, dos quais o determinante $|\Delta_0|$, composto pelos elementos de Δ_0, é menor de 1.ª ordem, são nulos. Como os determinantes de ordem $r+1$, a considerar em B, são da forma

$$\begin{vmatrix} a_{11} \cdots a_{1r}\ a_{1j} \\ \cdots\cdots\cdots \\ a_{r1} \cdots a_{rr}\ a_{rj} \\ 0 \cdots 0 \quad b_{hj} \end{vmatrix} = \Delta \cdot b_{hj} = 0,$$

vê-se que $b_{hj} = 0$. Assim B tem o aspecto $B = \begin{bmatrix} \Delta_0 & P \\ 0 & 0 \end{bmatrix}$, donde se conclui que a característica de B é igual a r. O teorema está provado.

2) **Os determinantes e as equações lineares** — As soluções dos sistemas lineares, estudados em (VII, 3, 2) e em (VIII, 2, 1), podem encontrar-se de modo interessante, utilizando os determinantes. Como preparação para a resolução geral do problema, começaremos por este

1.º CASO (sistema CRAMER): Seja o sistema

$$\sum_{k=1}^{n} a_{ik} x_k = b_i, \quad (i = 1, 2, \cdots, n), \tag{1}$$

de tantas equações quantas as incógnitas. O sistema (1) diz-se um *sistema* CRAMER, se o determinante $|a_{ik}|$ for $\neq 0$. Nesse caso, a matriz simples do sistema tem a característica n, e o mesmo sucede, necessàriamente, à matriz ampliada. O sistema (1) é solúvel. Se $x_1, \cdots, x_n$ é uma solução, escrevamos

$$x_j \cdot |a_{ik}| = \begin{vmatrix} a_{11} \cdots (a_{1j} x_j) \cdots a_{1n} \\ a_{21} \cdots (a_{2j} x_j) \cdots a_{2n} \\ \cdots\cdots\cdots\cdots \\ a_{n1} \cdots (a_{nj} x_j) \cdots a_{nn} \end{vmatrix} =$$

$$= \begin{vmatrix} a_{11} \cdots a_{1,j-1} \sum_{s=1}^{n} a_{1s} x_s \cdots a_{1n} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n1} \cdots a_{n,j-1} \sum_{s=1}^{n} a_{ns} x_s \cdots a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} \cdots a_{1,j-1}\ b_1 \cdots a_{1n} \\ \cdots\cdots\cdots\cdots \\ a_{n1} \cdots a_{n,j-1}\ b_n \cdots a_{nn} \end{vmatrix}.$$

Tem-se então

$$x_j = \frac{\sum_{s=1}^{n} A_{js} b_s}{|a_{ik}|}. \tag{2}$$

Deste modo, as soluções de (1) não podem deixar de ter a forma (2). E como as soluções existem, elas serão dadas por (2). É válido este

TEOREMA 1: *O valor da incógnita* x_j, *num sistema* CRAMER *(1), é dado por um cociente, cujo denominador é o determinante* $|a_{jk}|$ *do sistema e cujo numerador é o determinante que resulta de* $|a_{ik}|$ *substituindo os elementos* a_{ij}, *da coluna de ordem* j, *pelos termos constantes* b_i.

Estamos agora em condições de passar ao

2.º CASO (caso geral): Suponhamos o sistema

$$\sum_{h=1}^{n} a_{ih} x_h = b_i, \quad (i = 1, 2, \cdots, m), \tag{3}$$

com m equações e n incógnitas. Se a característica do sistema é r, isto é, se as matrizes simples e ampliada do sistema têm a característica r, disponhamos as equações de (3), de modo a ter como primeiras r equações certas equações cujos coeficientes constituam r linhas independentes. Considerando, então, o sistema assim obtido como sendo formado já pelas primeiras r equações de (3), somos levados a

$$\sum_{h=1}^{n} a_{ih} x_h = b_i , \quad (i = 1, 2, \cdots, r), \tag{4}$$

que é um sistema equivalente a (3). Se, em seguida, colocarmos, em (4), em primeiro lugar, r incógnitas que tenham como coeficientes um quadro determinante $\neq 0$, chega-se a outro sistema, no qual, designadas as incógnitas por novos símbolos, os r primeiros símbolos correspondem às r primeiras incógnitas. Em resumo: suporemos já, em (4), que as r primeiras colunas da matriz do sistema são linearmente independentes. Dando a (4) o aspecto

$$\begin{aligned} &a_{11} x_1 + \cdots + a_{1r} x_r = b_1 - a_{1,r+1} x_{r+1} - \cdots - a_{1n} x_n , \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &a_{r1} x_1 + \cdots + a_{rr} x_r = b_r - a_{r,r+1} x_{r+1} - \cdots - a_{rn} x_n , \end{aligned} \tag{5}$$

podemos considerar este sistema nas condições do 1.º caso. Obtém-se

$$x_j = \frac{\begin{vmatrix} a_{11} \cdots a_{1,j-1}\, b_1 - \sum_{s=r+1}^{n} a_{1s} x_s \cdots a_{1r} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{r1} \cdots a_{r,j-1}\, b_r - \sum_{s=r+1}^{n} a_{rs} x_s \cdots a_{rr} \end{vmatrix}}{|a_{ik}|} .$$

Fazendo $|a_{ik}| = D$, é ainda

$$x_j = \frac{1}{D} \sum_{t=1}^{r} A_{jt} b_t - \frac{1}{D} \sum_{s=r+1}^{n} \left(\sum_{t=1}^{r} A_{jt} a_{ts} \right) x_s . \tag{6}$$

Dando aqui valores arbitrários aos x_s, obtêm-se todas as soluções de (5), e, portanto, do sistema dado (3). As equações de (3), que se escreveram em (4), dizem-se *equações principais de (3)*; e as incógnitas que figuram nos primeiros membros de (5) dizem-se, anàlogamente, *incógnitas principais de (3)*. Tem-se:

TEOREMA 2: *Se o sistema (3) é solúvel, as suas soluções são dadas por (6), supostas as* r *primeiras equações de (3) as equações principais e supostas as* r *primeiras incógnitas de (3) as incógnitas principais.*

Por virtude das suas numerosas aplicações, vamos tratar ainda um terceiro caso, que é, aliás, bastante particular.

3.º CASO (sistema de $n-1$ equações homogéneas com n incógnitas): Suporemos ainda que a característica do sistema é igual a $n-1$. As soluções constituirão uma multiplicidade vectorial a uma dimensão, que vamos determinar. O sistema tem o aspecto

$$\begin{aligned} &a_{11} x_1 + \cdots + a_{1n} x_n = 0 , \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &a_{n-1,1} x_1 + \cdots + a_{n-1,n} x_n = 0 , \end{aligned} \tag{7}$$

e a matriz do sistema é

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n-1,1} & a_{n-1,2} & \cdots & a_{n-1,n} \end{bmatrix} , \tag{8}$$

podendo dela tirar-se um determinante de ordem $n-1$ que é $\neq 0$. Designaremos por $D_1, D_2, \cdots, D_n$ os n determinantes de ordem $n-1$ extraídos de (8) por supressão sucessiva da 1.ª, 2.ª, ... colunas. Pode indicar-se a seguinte regra, para se encontrarem as soluções de (7). Consideram-se os determinantes

$$\begin{vmatrix} a_{j1} & a_{j2} & \cdots & a_{jn} \\ a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n-1,1} & a_{n-1,2} & \cdots & a_{n-1,n} \end{vmatrix} , \tag{9}$$

$(j = 1, 2, \cdots, n-1)$, que são todos nulos. Por desenvolvimento, segundo os elementos da 1.ª linha, obtêm-se as $n-1$ relações $\sum_{i=1}^{n} (-1)^{i+1} a_{ji} D_i = 0$, que, por comparação com (7), mostram ser $x_1 = D_1$, $x_2 = -D_2, \cdots, x_n = (-1)^{n+1} D_n$ uma das suas soluções. Daqui o

TEOREMA 3: *Dado o sistema (7), de característica* n - 1, *as soluções são proporcionais aos determinantes de ordem* n - 1 *extraídos de (8), afectados de sinais alternadamente* + *e* - , *e começando pelo determinante obtido por supressão da 1.ª coluna.*

§ 4. Transformações lineares

1) **Produto de matrizes** — Sejam $\mathfrak{N}_n(\mathfrak{e}_1, \cdots, \mathfrak{e}_n)$ e $\mathfrak{M}_m(\mathfrak{v}_1, \cdots, \mathfrak{v}_m)$ duas multiplicidades vectoriais, de ordens n e m, respectivamente, sobre o mesmo corpo $\mathfrak{K}$. Uma homomorfia operatória fica definida conhecidos os elementos U_j e $\mathfrak{M}_m$, correspondentes dos $\mathfrak{e}_j$. Poremos

$$U_j = \sum_{k=1}^{m} \mathfrak{v}_k a_{kj}, \qquad (j = 1, 2, \cdots, n).$$

Dado o elemento $\sum \mathfrak{e}_j a_j$ e $\mathfrak{N}_n$, o seu correspondente em $\mathfrak{M}_m$ é

$$\sum_{j=1}^{n} U_j a_j = \sum_{j,k} \mathfrak{v}_k a_{kj} a_j = \sum_{k=1}^{m} \mathfrak{v}_k b_k, \qquad (b_k = \sum_{j=1}^{n} a_{kj} a_j).$$

Vê-se que a homomorfia também pode considerar se definida pela matriz rectangular $A = (a_{kj})$, de m linhas e n colunas. Se considerarmos uma segunda homomorfia $\mathfrak{M}_m \sim \mathfrak{Q}_q(\mathfrak{w}_1, \cdots, \mathfrak{w}_q)$, definida pelas igualdades

$$\mathfrak{v}_k \to V_k = \sum_{s=1}^{q} \mathfrak{w}_s b_{sk}, \qquad (k = 1, 2, \cdots, m),$$

levanta-se a questão de procurar definir por uma matriz a homomorfia $\mathfrak{N}_n \sim \mathfrak{Q}_q$. Obtém-se sucessivamente:

$$\mathfrak{e}_j \to U_j \to \sum_{k=1}^{m} V_k a_{kj} = \sum_{k=1}^{m} \sum_{s=1}^{q} \mathfrak{w}_s b_{sk} a_{kj} = \sum_{s=1}^{q} \mathfrak{w}_s c_{sj},$$

com $c_{sj} = \sum_{k=1}^{m} b_{sk} a_{kj}$. A matriz C, de elementos c_{sj}, é a matriz procurada. C tem tantas linhas quantas as linhas de B e tantas colunas quantas as colunas de A. Escreveremos

$$C\begin{pmatrix} q \text{ linhas} \\ n \text{ colunas} \end{pmatrix} = B\begin{pmatrix} q \text{ linhas} \\ m \text{ colunas} \end{pmatrix} \cdot A\begin{pmatrix} m \text{ linhas} \\ n \text{ colunas} \end{pmatrix}$$

ou, mais simplesmente, $C = B \cdot A = BA$, e diremos que C é o *produto* de B por A.

2) **O grupo linear** — Em correlação com a doutrina do número anterior, tomemos uma multiplicidade vectorial $\mathfrak{M}_n$ e a submultiplicidade $\mathfrak{M}_m (m \lessgtr n)$. A homomorfia operatória $\mathfrak{M}_n \sim \mathfrak{M}_m$ passa a ser um endomorfismo operatório Θ, de $\mathfrak{M}_n$, segundo o qual se tem a correspondência

$$(1) \qquad \mathfrak{e}_j \to \mathfrak{e}_j \Theta = U_j = \sum_{h=1}^{n} \mathfrak{e}_h a_{hj}, \qquad (j = 1, 2, \cdots, n).$$

A matriz $A = (a_{hj})$ é agora quadrada. Levanta-se o problema de se saber em que condições o endomorfismo é um automorfismo. Quere-se, então, que todos os elementos de $\mathfrak{M}_n$ sejam utilizados como imagens e que haja reciprocidade entre os vectores $\mathfrak{x}$ e $\mathfrak{M}_n$ e as suas imagens. Designando por $\mathfrak{x}'$ o correspondente ou transformado de $\mathfrak{x}$, visto que $\mathfrak{x}'$ se exprime nos U_j, podemos dizer:

TEOREMA 1: *É condição necessária e suficiente, para que o endomorfismo seja um automorfismo, que os elementos* U_j *sejam linearmente independentes.* Vamos dar outra forma a este enunciado. Dizer que os U_j são linearmente independentes é dizer que as equações $\sum_{j=1}^{n} a_{kj} \mu_j = 0$, que já encontrámos em (VII, 1, 3), apenas são satisfeitas por valores todos nulos atribuídos aos μ_j. Assim, vale este

TEOREMA 2: *É condição necessária e suficiente, para que o endomorfismo definido em (1) seja um automorfismo, que o determinante* $|a_{hj}|$, *da matriz quadrada do endomorfismo seja* $\neq 0$. Então, os U_j constituem uma base para $\mathfrak{M}_n$ e neles se exprimem todos os vectores. Em particular, tem-se

$$(2) \qquad \mathfrak{e}_j = \sum_{k=1}^{n} U_k b_{kj}, \qquad (j = 1, 2, \cdots, n).$$

Os $\mathfrak{e}_j$ são agora os correspondentes dos U_j no endomorfismo definido pela matriz $B = (b_{kj})$. Esta matriz encontra-se nas mesmas condições que a matriz $A = (a_{kj})$. Será igualmente $|b_{kj}| \neq 0$.

Substituamos, em (2), os U_k pelas suas expressões nos $\mathfrak{e}_j$. Vem

$$\mathfrak{e}_j = \sum_{k=1}^{n} \sum_{m=1}^{n} \mathfrak{e}_m a_{mk} b_{kj} = \sum_{m=1}^{n} \mathfrak{e}_m \left(\sum_{k=1}^{n} a_{mk} b_{kj} \right),$$

o que nos leva a

$$\sum_{k=1}^{n} a_{mk} b_{kj} = \delta_{mj}, \qquad \delta_{mj} = \begin{cases} 0, & \text{se } m \neq j, \\ u, & \text{se } m = j, \end{cases} \qquad (u \in \mathfrak{K}).$$

A matriz $(\delta_{mj}) = U_n$ tem o aspecto

$$U_n = \begin{bmatrix} u & 0 & \cdots & 0 \\ 0 & u & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & u \end{bmatrix}$$

e recebe o nome de *matriz unidade*. Para qualquer matriz quadrada C, de ordem n, tem-se $C U_n = U_n C = C$.

As matrizes A e B, em questão, satisfazem à igualdade $AB = U_n$. É evidente que os papéis de A e de B são recíprocos e que, por isso, substituindo (2) em (1), se chega a $BA = U_n$. Duas matrizes, como A e B, tais que $AB = BA = U_n$ dizem-se *inversas* uma da outra. Pode escrever-se $B = A^{-1}$, ou $A = B^{-1}$. É válido este

TEOREMA 3: *É condição necessária e suficiente, para que um endomorfismo seja um automorfismo, que a matriz do endomorfismo tenha inversa.*

COROLÁRIO: *São equivalentes estas duas afirmações: 1) o determinante da matriz* A, *representado por* $|A|$, *é* $\neq 0$; *2) a matriz* A *tem inversa* A^{-1}.

Na verdade, basta afirmar que a matriz A tem inversa direita A_d^{-1}, pois que, sendo $A A_d^{-1} = U_n$, imediatamente se verifica que é $|A A_d^{-1}| = |U_n| = u = |A| \cdot |A_d^{-1}|$, o que implica $|A| \neq 0$.

Eis ainda uma outra caracterização dos automorfismos:

TEOREMA 4: *É necessário e basta, para que* A *defina um automorfismo, que um produto* $AC = 0$ (= *matriz nula*) *implique* $C = 0$.

A condição é *necessária*: Se A define um automorfismo, existe uma matriz inversa esquerda B, de A. Então, $BA = U_n$, de sorte que, de $AC = 0$, se tira $B \cdot AC = 0$. Ora o produto de matrizes, como resulta da sua definição, é *associativo*, e, assim, tem-se $B \cdot AC = BA \cdot C = U_n C = C = 0$, como se deseja.

A condição é *suficiente*: Suponhamos que a matriz A é tal que

$AC = 0$ implica $C = 0$. Queremos provar que A define um automorfismo. Da demonstração do teorema 2 resulta, com efeito, que, se a hipótese

$$A \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = 0 \text{ implica } \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = 0,$$

onde os b_j estão dispostos em matriz com uma só coluna, então A define um automorfismo. O teorema está provado.

O conjunto das matrizes quadradas que definem automorfismos forma um grupo, à face da operação de produto. Aos automorfismos dá-se o nome de *transformações lineares*. O produto de duas transformações lineares é uma transformação linear. À face do produto, as transformações lineares formam um grupo, que se diz *grupo linear*.

O problema da transformação de coordenadas, tratado em (VIII, 1, 3), faz intervir ùnicamente matrizes quadradas $P = (p_{hj})$ que são invertíveis.

Utilizando o simbolismo das matrizes, podemos resolver fàcilmente as equações (1) do citado lugar (VIII, 1, 3), esclarecendo deste modo a observação que então foi feita. Tem-se, com efeito,

$$\begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix} = P \begin{bmatrix} \eta_1 \\ \vdots \\ \eta_n \end{bmatrix}, \text{ e, portanto, } \begin{bmatrix} \eta_1 \\ \vdots \\ \eta_n \end{bmatrix} = P^{-1} \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix}.$$

O mesmo se diz das equações (3), ainda de (VIII, 1, 3).

3) **O módulo finito das matrizes** — Como já dissemos, o produto de matrizes tem sentido, quando o número de colunas do 1.º factor é igual ao número de linhas do segundo.

Dadas duas matrizes $A = (a_{ik}), B = (b_{ik})$, em que o número de linhas e de colunas de cada uma delas é igual ao número correspondente da outra, define-se a sua *soma* como a matriz de elementos $c_{ik} = a_{ik} + b_{ik}$. Com esta definição, vê-se que as matrizes rectangulares em causa formam um grupo abeliano aditivo. Quando o produto é executável, tem-se

$$A \cdot BC = AB \cdot C, \quad A(B+C) = AB + AC, \quad (B+C)A = BA + CA.$$

Entretanto, para que o produto de duas matrizes seja uma matriz do mesmo tipo do dos factores, torna-se necessário supor que apenas se trata com matrizes quadradas. Quanto a estas, pode afirmar-se: *as*

matrizes quadradas de ordem n *formam um anel,* chamado *anel completo de matrizes* e representado por $\mathfrak{K}_n$, suposto $\mathfrak{K}$ o corpo a que pertencem os elementos das referidas matrizes.

Nesse anel, segundo a terminologia indicada em (VI, 2, 3), as unidades são as matrizes com inverso, as quais formam grupo, como se disse.

Seja $A \in \mathfrak{K}_n$. Podemos aplicar a A os elementos $a \in \mathfrak{K}$, conforme a regra

$$A\,a = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \cdot a = \begin{bmatrix} a_{11}\,a & \cdots & a_{1n}\,a \\ \cdots & \cdots & \cdots \\ a_{n1}\,a & \cdots & a_{nn}\,a \end{bmatrix},$$

À face desta definição, conclui-se que $\mathfrak{K}_n$ *é um módulo finito direito relativamente a* $\mathfrak{K}$ (ou esquerdo, pois que $\mathfrak{K}$ é comutativo). Como *matrizes-base,* podemos tomar as matrizes $E_{ij}, (i, j = 1, 2, \cdots, n)$, assim definidas: todos os seus elementos são nulos, salvo o do cruzamento da linha de ordem i com a coluna de ordem k, que é igual a u. A matriz $A = (a_{ik})$ tem a seguinte expressão nos E_{ij}: $A = \sum_{i,j=1}^{n} E_{ij}\,a_{ij}$.

A independência linear dos E_{ij} é, de resto, imediata.

4) **Dois problemas sobre homomorfias** — Na homomorfia $\mathfrak{N}_n \sim \mathfrak{M}_m$, representada em (IX, 4, 1) pela matriz A, levanta-se este problema: *determinar a matriz* A' *que a define, supondo que se fazem mudanças de base, tanto em* $\mathfrak{N}_n$ *como em* $\mathfrak{M}_m$. A nova base de $\mathfrak{N}_n$ será $E_1, \cdots, E_n$, a qual, em notação matricial, se pode fixar, pondo $[E_1 \cdots E_n] = [e_1 \cdots e_n] \cdot P$, onde P é a matriz invertível correspondente à mudança de base. Anàlogamente, em $\mathfrak{M}_m$, tem-se $[V_1 \cdots V_m] = [v_1 \cdots v_m] \cdot Q$, onde Q é invertível e de ordem m. Quanto à matriz A, foi ela introduzida do modo seguinte: $e_j \to U_j = \sum v_k\,a_{kj}$, $(k = 1, 2, \cdots, m;\ j = 1, 2, \cdots, n)$. Para encontrármos a matriz A' que define a mesma homomorfia, temos de exprimir os transformados dos E_j nos V_k. Representemos esses transformados por E'_j. Será, em notação de matrizes,

$$[E'_1 \cdots E'_n] = [U_1 \cdots U_n]\,P, \text{ com } [U_1 \cdots U_n] = [v_1 \cdots v_m]\,A,$$

o que leva a $[E'_1 \cdots E_n] = [v_1 \cdots v_m]\,A\,P$. Observando, em seguida, que se tem $[v_1 \cdots v_m] = [V_1 \cdots V_m]\,Q^{-1}$, chega-se a

$$[E'_1 \cdots E'_n] = [V_1 \cdots V_m]\,Q^{-1}\,A\,P.$$

Daqui se conclui que a matriz A é substituida por $A' = Q^{-1}\,A\,P$. O problema está resolvido.

O segundo problema é o seguinte: *suponhamos que temos uma base* $(e_1, \cdots, e_n)$, em $\mathfrak{M}_n$, *e que se considera um automorfismo definido por uma matriz* A; *pregunta-se qual é a matriz* A' *que define o mesmo automorfismo, se se muda de base?* Escrevamos a nova base sob a forma $[E_1 \cdots E_n] = [e_1 \cdots e_n]\,P$. O automorfismo faz corresponder aos e_j os vectores $U_j = \sum e_h\,a_{hj}$, $(h, j = 1, 2, \cdots, n)$. Para se encontrar A', vê-se que devemos procurar os transformados dos E_i e exprimir esses transformados nos próprios E_i. Se os transformados dos E_i se representam por E'_i, tem-se $[E'_1 \cdots E_n] = [U_1 \cdots U_n]\,P = [e_1 \cdots e_n]\,AP = [E_1 \cdots E_n]\,P^{-1}AP$. Vê-se, assim, que é $A' = P^{-1}AP$.

BIBLIOGRAFIA

E. Sperner, *Einführung in die analytische Geometrie und Algebra*, erster Teil, Göttingen, 1948.

J. Vicente Gonçalves, *Álgebra superior*, 2.º vol., Lisboa, 1950.

A. Adrian Albert, *Modern Higher Algebra*, Chicago, 1936.

A. Almeida Costa, *Grupos abelianos e Anéis e Ideais não comutativos*, Porto, 1942.

B. van der Waerden, *Moderne Algebra*, zweiter Teil, 1931.

CAPÍTULO X

Espaço projectivo

§ 1. Definição geral. Subespaços

1) **Definição geral** — Partamos do espaço linear ou *espaço afim* $\mathfrak{R}_n$, estudado no Capítulo VIII. O nosso primeiro objectivo consiste em dar uma representação dos pontos de $\mathfrak{R}_n$ por um modo diferente do que se usou no referido Capítulo. Num referencial $O_0(e_1, \cdots, e_n)$ fixado, um ponto $P \in \mathfrak{R}_n$ foi representado por n elementos $x_i \in \mathfrak{K}$, onde $\mathfrak{K}$ é um corpo qualquer. Poremos aqui $P = (x_1, \cdots, x_n)$ para significar esse facto.

Estabeleçamos agora uma correspondência biunívoca completa entre os sistemas de n elementos x_i e os sistemas de $n+1$ elementos $\xi_j \in \mathfrak{K}, (j = 0, 1, \cdots, n)$, nos termos que vamos indicar. Escrevamos

$$x_i = \frac{\xi_i}{\xi_0}, \quad (i = 1, 2, \cdots, n), \quad \text{com } \xi_0 \neq 0.$$

Claramente que, se os elementos ξ_j são dados, os elementos x_i ficam bem determinados. A inversa não é, porém, válida. Designemos por $\xi'_j, (j = 0, 1, \cdots, n)$, com $\xi'_0 \neq 0$, um segundo sistema de elementos de $\mathfrak{K}$ tais que $x_i = \xi'_i/\xi'_0$. Das igualdades $\xi_i/\xi_0 = \xi'_i/\xi'_0$, deduzimos

$$\xi'_i = \frac{\xi'_0}{\xi_0}\xi_i, \text{ ou seja } \xi'_i = \lambda\xi_i, \ (i = 0, 1, \cdots, n),$$

desde que se ponha $\xi'_0/\xi_0 = \lambda$.

Se não distinguirmos os sistemas proporcionais de $n+1$ elementos ξ_i, sempre sob a hipótese $\xi_0 \neq 0$, chegamos, de facto, a uma correspondência biunívoca completa entre os pontos $P \in \mathfrak{R}_n$ e os sistemas da forma $[\xi_0, \xi_1, \cdots, \xi_n]$. Aos elementos ξ_i damos, então, o nome de *coordenadas homogéneas* dos pontos de $\mathfrak{R}_n$.

Vamos estender esta representação. Introduziremos pontos novos, e, na verdade, pontos que receberão o nome de *pontos impróprios*, considerando um sistema $[\xi_0, \xi_1, \cdots, \xi_n]$, com $\xi_0 = 0$, como coordenadas homogéneas dum tal ponto, o qual também se representa, à semelhança do que aconteceu com os pontos de $\mathfrak{R}_n$, também chamados *pontos próprios*, por qualquer outro sistema de $n+1$ elementos proporcionais áqueles. Nesta convenção, que leva aos pontos impróprios, não se considera o sistema $[0, 0, \cdots, 0]$, ao qual se não atribui qualquer significado.

Diz-se *espaço projectivo a* n *dimensões*, e representa-se por $\mathfrak{P}_n$, a totalidade dos pontos próprios e impróprios, nos termos que acabam de ser indicados. Costuma dizer-se que *o espaço projectivo se obtem juntando ao espaço afim o conjunto dos pontos impróprios.*

2) **Os subespaços do espaço projectivo** — À semelhança do que aconteceu em $\mathfrak{R}_n$, vamos introduzir em $\mathfrak{P}_n$ a noção de subespaço linear, que designaremos geralmente por *subespaço projectivo*.

Se partirmos dum subespaço linear de $\mathfrak{R}_n$, definido por um sistema não homogéneo em $x_1, \cdots, x_n$ da forma

$$(1) \qquad \begin{aligned} &a_{10} + a_{11}x_1 + \cdots + a_{1n}x_n = 0, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &a_{m0} + a_{m1}x_1 + \cdots + a_{mn}x_n = 0, \end{aligned}$$

é claro que, recorrendo ás coordenadas homogéneas $[\xi_0, \cdots, \xi_n]$ dos pontos de $\mathfrak{R}_n$, o referido subespaço ficará igualmente definido pelo sistema homogéneo nos ξ_i, obtido do anterior pondo $x_i = \xi_i/\xi_0$, suposto que apenas se consideram as soluções do sistema transformado para as quais $\xi_0 \neq 0$. Em vez de (1), temos, assim

$$(2) \qquad \begin{aligned} &a_{10}\xi_0 + a_{11}\xi_1 + \cdots + a_{1n}\xi_n = 0, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &a_{m0}\xi_0 + a_{m1}\xi_1 + \cdots + a_{mn}\xi_n = 0. \end{aligned}$$

Toda a solução de (2), com $\xi_0 \neq 0$, leva a uma solução de (1), pondo $x_i = \xi_i/\xi_0$, e, reciprocamente, qualquer solução de (1) leva a uma

solução de (2), escolhendo $\xi_0 \neq 0$ e pondo $\xi_i = x_i \xi_0$. As soluções de (2) em questão não constituem ainda um subespaço projectivo, precisamente pelo facto de poder haver outras com $\xi_0 = 0$. Excluída de (2) a solução $[0, \cdots, 0]$ e consideradas *todas* as outras, define-se num subespaço projectivo de $\mathfrak{P}_n$.

DISCUSSÃO DOS SISTEMAS (1) E (2): Comecemos por supôr que (1) é solúvel, de sorte que, como vimos em (VIII, 2, 1), são as mesmas as características das duas matrizes

$$\begin{bmatrix} a_{10} & a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m0} & a_{m1} & \cdots & a_{mn} \end{bmatrix}, \qquad \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}.$$

Se $n - r$ é a característica comum ou característica do sistema (1), este sistema representa um subespaço linear de dimensão r. Diremos, então, que o sistema (2) representa igualmente um *subespaço projectivo de dimensão* r. Esta definição será mantida, de futuro, sem qualquer excepção.

O número $n - r$ é também a característica do sistema (2). O valor de r pode imaginar-se, por isso, obtido a partir do sistema (2), pondo $r = (n+1) - (n-r) - 1$.

Em (2), o valor de $n - r$ pode ir desde 0 até $n + 1$. Quando se tem $n - r = 0$, todos os coeficientes a_{ij} são nulos ($i = 1, 2, \cdots m$; $j = 0, 1, 2, \cdots, n$); o sistema (2) é satisfeito por todos os pontos de $\mathfrak{P}_n$, dizendo-se, assim, que (2) representa todo o espaço projectivo. A fórmula escrita dá $r = (n+1) - 0 - 1 = n$. Se supõe $n - r = 1$, é $r = n - 1$; obtém-se o que se chama um *hiperplano* de $\mathfrak{P}_n$. Se fôr $n - r = n - 2$, é $r = 2$; obtém-se um *plano projectivo*. Para $n - r = n - 1$, define-se uma *recta projectiva*. Ao caso $n - r = n$, ou $r = 0$, estudado em detalhe em (IX, 3, 2), correspondem para (2) soluções proporcionais, que levam a um único ponto. Um *ponto*, próprio ou impróprio, constitui um subespaço projectivo de *dimensão zero*. Finalmente, não exceptuaremos $n - r = n + 1$, relativa ao caso em que o sistema (2) tem a única solução $(0, 0, \cdots, 0)$. O sistema (1) não é solúvel e o sistema (2) não define qualquer ponto de $\mathfrak{P}_n$. Diremos que (2) representa o *subespaço vazio*, ao qual atribuiremos a dimensão $r = (n+1) - (n+1) - 1 = -1$.

Um hiperplano pode representar-se sempre por uma única equação homogénea nos $\xi\xi$, com os coeficientes não todos nulos. Em particular, a equação $\xi_0 = 0$ representa um hiperplano que contém todos os pontos impróprios de $\mathfrak{P}_n$. Assim: *os pontos impróprios de* $\mathfrak{P}_n$ *constituem um subespaço de dimensão* $n - 1$. Existe uma proposição geral nos termos seguintes:

TEOREMA: *Se um espaço projectivo de dimensão* r *tem pontos próprios, os pontos impróprios do subespaço constituem um subespaço projectivo de dimensão* $r - 1$. Em primeiro lugar, os pontos impróprios dum subespaço projectivo de dimensão r, definido pelo sistema (2), formam um subespaço porque, ou todas as soluções de (2) levam a pontos impróprios e a afirmação é válida, ou, de contrário, o subespaço (2) tem pontos próprios e a totalidade dos seus pontos impróprios obtem-se juntando ao sistema (2) a equação $\xi_0 = 0$. Neste último caso, temos de considerar o sistema

$$(3) \qquad \begin{aligned} &\sum a_{ik} \xi_k = 0, \qquad (i = 1, 2, \cdots, m; \quad k = 1, 2, \cdots, n), \\ &\xi_0 = 0, \end{aligned}$$

cuja matriz é

$$(4) \qquad \begin{bmatrix} a_{10} & a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m0} & a_{m1} & \cdots & a_{mn} \\ 1 & 0 & \cdots & 0 \end{bmatrix}.$$

Para acharmos a dimensão do subespaço (3), temos que determinar a característica de (4). Como o numero de linhas aumentou de uma unidade, em relação à matriz de (2), de característica $n - r$, a característica de (4) só pode ser $n - r$ ou $n - r + 1$. Se se desse a 1.ª hipótese, a nova equação $\xi_0 = 0$ não seria distinta das equações de (2). Para todas as soluções de (2) se teria $\xi_0 = 0$, contra a hipótese de o subespaço definido por (2) conter pontos próprios. A característica de (4) é $n - r + 1$ e a dimensão do subespaço definido por (3) é $x = (n+1) - (n - r + 1) - 1 = r - 1$, como afirma o teorema.

Um plano projectivo, com pontos próprios, tem uma só recta imprópria; uma recta projectiva, com pontos próprios, tem um único ponto impróprio; e um ponto próprio tem um espaço vazio de pontos impróprios.

3) **Outro modo de caracterizar os pontos impróprios dum subespaço projectivo** — A determinação dos pontos impróprios do subespaço (2) do número anterior pode fazer-se por uma via diferente.

Com efeito, o sistema (3) desse número é equivalente a este outro:

$$(1)\qquad \begin{aligned} &a_{11}\,\xi_1 + a_{12}\,\xi_2 + \cdots + a_{1n}\,\xi_n = 0\,,\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ &a_{m1}\,\xi_1 + a_{m2}\,\xi_2 + \cdots + a_{mn}\,\xi_n = 0\,,\\ &\xi_0 = 0\,, \end{aligned}$$

o qual nos sugere o estudo do sistema

$$(2)\qquad \begin{aligned} &a_{11}\,x_1 + a_{12}\,x_2 + \cdots + a_{1n}\,x_n = 0\,,\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ &a_{m1}\,x_1 + a_{m2}\,x_2 + \cdots + a_{mn}\,x_n = 0\,. \end{aligned}$$

Vê-se que, dada uma solução $(x_1, \cdots, x_n)$ deste último, se juntarmos a esta solução o elemento zero e escrevermos $(0, x_1, \cdots, x_n)$, obtemos uma solução de (1). Reciprocamente, uma solução de (1) à qual se tira o elemento zero é uma solução de (2).

Desde que o subespaço (2) do número anterior tem pontos próprios, a característica $n - r$ do sistema correspondente é a característica do sistema (1) do mesmo número e também a característica do sistema (2) acima escrito. Ora este último representa uma multiplicidade vectorial de dimensão r, como vimos em (VII, 3, 2). Daqui, este resultado:

TEOREMA 1: *Tomado $\mathfrak{P}_n$, aos pontos impróprios dum subspaço projectivo, de dimensão* r, *que tem pontos próprios, associa-se em $\mathfrak{M}_n$, de modo unívoco, uma submultiplicidade vectorial $\mathfrak{M}_r$, de dimensão* r.

Posto isto, usaremos a notação seguinte: se L é um subespaço de $\mathfrak{P}_n$, L' será o conjunto dos seus pontos próprios, L'' o subespaço dos pontos impróprios de L e $\mathfrak{L}$ a submultiplicidade vectorial associada a L, nos termos do teorema acabado de demonstrar.

Tomemos, então, dois subespaços projectivos L_1 e L_2, de $\mathfrak{P}_n$. Diremos que L_1 e L_2 são paralelos, quando, supondo L'_1 e L'_2 não vazios, estes dois conjuntos de pontos próprios (que formam sempre subespaços lineares do espaço afim $\mathfrak{R}$) definem subespaços paralelos de $\mathfrak{R}_n$. Isso exige que, das multiplicidades vectoriais $\mathfrak{L}_1$ e $\mathfrak{L}_2$, uma delas esteja contida na outra.

Suponhamos $\mathfrak{L}_1 \subseteq \mathfrak{L}_2$. Tem-se também, como resulta da ligação entre os sistemas (1) e (2), $L''_1 \subseteq L''_2$ (e recíprocamente). Assim:

TEOREMA 2: *É condição necessária e suficiente, para que dois subespaços de $\mathfrak{P}_n$, com pontos próprios, sejam paralelos, que o subespaço dos pontos impróprios dum deles esteja contido no outro.*

COROLÁRIO: *É condição necessária e suficiente, para que dois subespaços de $\mathfrak{P}_n$, com pontos próprios e com a mesma dimensão, sejam paralelos, que sejam idênticos os subespaços dos seus pontos impróprios.* Em particular: *duas rectas de $\mathfrak{P}_n$, com pontos próprios, são paralelas, se e só se têem o mesmo ponto impróprio; e dois planos de $\mathfrak{P}_n$, com pontos próprios, são paralelos, se e só se têm a mesma recta imprópria.*

4) **Intersecção e união de subespaços de $\mathfrak{P}_n$** — Já vimos que, por exemplo, aos pontos impróprios dum subespaço de dimensão r, com pontos próprios, podiamos associar uma submultiplicidade vectorial de dimensão r. Esta associação reveste-se de carácter geral, como vamos reconhecer, analisando o modo como introduzimos os pontos do espaço projectivo. Se $P = [\xi_0, \xi_1, \cdots, \xi_n] \in \mathfrak{P}_n$, o ponto P é também definido por qualquer sistema da forma $[\lambda\xi_0, \lambda\xi_1, \cdots, \lambda\xi_n]$, com $\lambda \neq 0$. Significa isto que cada ponto $P \in \mathfrak{P}_n$ é definido por uma submultiplicidade vectorial de dimensão 1, da multiplicidade $\mathfrak{M}_{n+1}$. Qualquer vector dessa submultiplicidade, diz-se *vector de coordenadas de* P.

Se se tratar dum subespaço projectivo de equações

$$(1)\qquad \begin{aligned} &a_{10}\,\xi_0 + a_{11}\,\xi_1 + \cdots + a_{1n}\,\xi_n = 0\,,\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ &a_{m0}\,\xi_0 + a_{m1}\,\xi_1 + \cdots + a_{mn}\,\xi_n = 0\,, \end{aligned}$$

procuremos determinar o conjunto dos vectores de coordenadas dos pontos deste subespaço. Supondo $n - r$ a característica de (1), o sistema (1) representa uma submultiplicidade vectorial de dimensão $(n+1) - (n-r) = r + 1$. Podemos mesmo dizer:

TEOREMA 1: *Dado um subespaço* L, *de dimensão* r, *no espaço $\mathfrak{P}_n$, associa-se-lhe, duma maneira unívoca, uma submultiplicidade vectorial $\mathfrak{L}$, de dimensão* r + 1, *em $\mathfrak{M}_{n+1}$; reciprocamente, cada $\mathfrak{L}$ está associada a um subespaço* L, *bem determinado.* A correspondência biunívoca entre L e $\mathfrak{L}$, aludida no teorema, vai permitir-nos resolver, duma maneira simples, alguns problemas relativos a subespaços de $\mathfrak{P}_n$.

Se L_1 e L_2 são dois subespaços, vamos ver que os pontos comuns aos dois subespaços constituem um novo subespaço. Designemos por $\mathfrak{L}_1$ e $\mathfrak{L}_2$ as submultiplicidades vectoriais associadas. A sua intersecção $\mathfrak{D} = \mathfrak{L}_1 \cap \mathfrak{L}_2$ está associada a um subespaço D, que é a *intersecção dos dois subespaços* L_1 e L_2, como vamos provar. Se um ponto pertence a L_1 e a L_2, qualquer vector de coordenadas do ponto pertence

às duas submultiplicidades correspondentes, portanto pertence a $\mathfrak{D}$. Reciprocamente, um vector de $\mathfrak{D}$ é vector associado dum ponto que pertence simultâneamente a L_1 e a L_2.

De modo análogo poderiamos tratar a intersecção duma família de subespaços.

Passemos em seguida à noção de *união de subespaços* de $\mathfrak{P}_n$. Dados L_1 e L_2, chamamos subespaço união dos dois subespaços o mais pequeno subespaço que os contém. Esse subespaço existe, porque, havendo subespaços de $\mathfrak{P}_n$ que contêm L_1 e L_2, como, por exemplo, o próprio $\mathfrak{P}_n$, a intersecção de todos esses subespaços preenche a definição dada para a união.

Um processo para a encontrar é também obtido pelo uso das submultiplicidades associadas $\mathfrak{L}_1$ e $\mathfrak{L}_2$. Formemos, com efeito, a submultiplicidade soma $\mathfrak{S} = (\mathfrak{L}_1, \mathfrak{L}_2)$, isto é, a submultiplicidade gerada por $\mathfrak{L}_1$ e $\mathfrak{L}_2$. A submultiplicidade $\mathfrak{S}$ está associada a um subespaço S, que é o subespaço união, como passamos a demonstrar. Em primeiro lugar, o subespaço S contém L_1 e L_2. Reciprocamente, qualquer subespaço que contenha L_1 e L_2 é tal que a submultiplicidade associada correspondente contém $\mathfrak{L}_1$ e $\mathfrak{L}_2$, e, portanto, contém $\mathfrak{S}$. Assim, o subespaço de que se partiu contém S, que é, pois, a união procurada.

Relativamente às dimensões de L_1, L_2, D e S, vamos demonstrar um teorema análogo àquele que demonstrámos em (VII, 3, 1) para submultiplicidades vectoriais. Designemos com r_1 e r_2 as dimensões de L_1 e de L_2, respectivamente, por d a dimensão de D e por s a de S. Passando às submultiplicidades vectoriais correspondentes, de dimensões r_1+1, r_2+1, $d+1$ e $s+1$, o teorema 2 daquele lugar leva-nos a $(r_1+1)+(r_2+1)=(d+1)+(s+1)$, donde deduzimos $r_1+r_2=d+s$, que é a relação desejada.

Se a intersecção D fôr vazia, tem-se $\mathfrak{D}=(0)$ e $d=-1$. Então, é $\mathfrak{S}=\mathfrak{L}_1+\mathfrak{L}_2$ uma soma directa, vê-se que se tem $(r_1+1)+(r_2+1)=s+1$, consequentemente $r_1+r_2=s-1$, exactamente obtida da relação geral anterior com $d=-1$.

APLICAÇÕES: Imaginemos que se tem $r_1+r_2 \gtrless n$. Virá $d=r_1+r_2-s$, consequentemente, tendo em conta ser $s \gtrless n$, $d \gtrless r_1+r_2-n \gtrless 0$. Daqui se conclui que, *se dois subespaços têm dimensões cuja soma é igual ou maior que* n, *a sua intersecção nunca é vazia.*

No espaço a 3 dimensões, dois planos têm sempre, pelo menos, uma recta comum; e uma recta e um plano têm sempre, pelo menos, um ponto comum. Consideremos ainda o caso de duas rectas estarem no mesmo plano. Será $r_1=1$, $r_2=1$, $s \gtrless 2$, consequentemente,

$d=r_1+r_2-s \gtrless 0$. A intersecção das duas rectas é um ponto, pelo menos.

5) **Dependência e independência de pontos** — Desde que a cada ponto de $\mathfrak{P}_n$ se associa de modo biunívoco uma submultiplicidade a uma dimensão de $\mathfrak{M}_{n+1}$, falaremos de *pontos dependentes* ou *independentes*, conformem forem dependentes ou independentes os vectores de qualquer sistema de vectores associados aos diferentes pontos. Reconhece-se imediatamente, com efeito, que, sendo $P_1, P_2, \cdots, P_t$ pontos de $\mathfrak{P}_n$ e $\mathfrak{x}_1, \mathfrak{x}_2, \cdots \mathfrak{x}_t$ um sistema de vectores associados, a dependência ou independência dos $\mathfrak{x}_j$ é a mesma que a dependência ou independência dos vectores $\mathfrak{x}_1\lambda_1, \mathfrak{x}_2\lambda_2, \cdots, \mathfrak{x}_t\lambda_t$, quaisquer que sejam os λ_j fixados, contando que nenhum deles seja nulo.

A associação dos espaços projectivos às submultiplicidades vectoriais permite pôr certos problemas para os pontos e dar-lhes soluções simples. Seja, por exemplo, construir o mais pequeno subespaço de $\mathfrak{P}_n$ que contenha os pontos $Q_1, \cdots, Q_t$. Se $\mathfrak{x}_1, \cdots, \mathfrak{x}_t$ forem vectores de coordenadas daqueles pontos, é claro que a submultiplicidade vectorial $\mathfrak{L}$ construida sobre os $\mathfrak{x}_j$ leva a definir um subespaço L, que é necessàriamente o subespaço procurado. Supondo que há apenas $r \gtrless t$ pontos independentes, $\mathfrak{L}$ terá a dimensão r e L a dimensão $r-1$. Fixaremos este

TEOREMA: *Dados os pontos* $Q_1, \cdots, Q_t$, *o subespaço projectivo de dimensão mínima que contém aqueles pontos (também chamado subespaço união dos pontos, de harmonia com a nomenclatura introduzida no número anterior) tem a dimensão* $r-1$, *suposto que* r *dos pontos em causa são independentes.*

Dois pontos dependentes são coincidentes; três pontos dependentes estão numa recta ou são coincidentes; quatro pontos dependentes estão num plano, podendo pertencer à mesma recta ou ser coincidentes, etc.. Num subespaço de dimensão, r, há $r+1$ pontos independentes, não podendo haver um número maior. Em $\mathfrak{P}_n$, há $n+1$ pontos independentes, nunca mais.

A noção de dependência e independência de pontos permite se interpretem igualdades como a seguinte: $Q=\sum_{i=1}^{t} Q_i\lambda_i$. Significa-se, com isto, que qualquer vector associado a Q é combinação linear dos vectores de qualquer sistema de vectores associados aos Q_i.

§ 2. Princípio de dualidade: espaço dual dum espaço projectivo

1) **Princípio de dualidade** – Consideremos o espaço projectivo $\mathfrak{P}_n$. Neste espaço, definimos já o subespaço vazio, de dimensão -1; os subespaços formados por um único ponto, que são de dimensão zero; as rectas, com a dimensão 1; os planos, com a dimensão 2; e assim sucessivamente, até aos hiperplanos, de dimensão $n-1$, e ao espaço inteiro, de dimensão n.

Com o símbolo $\mathfrak{R}$ significaremos a totalidade dos subespaços de $\mathfrak{P}_n$. A intersecção de dois subespaços L_1 e L_2 foi já representada por $L_1 \cap L_2$; utilizaremos o simbolismo $L_1 \cup L_2$, para designar o subespaço união dos dois subespaços. $\mathfrak{R}$ é, assim, um sistema algébrico com as duas operações $\cap$ e $\cup$. Estas duas operações estão condicionadas pelas leis seguintes: $R_1)$ $L_1 \cap L_2 = L_2 \cap L_1$, $L_1 \cup L_2 = L_2 \cup L_1$; $R_2)$ $L_1 \cap (L_2 \cap L_3) = (L_1 \cap L_2) \cap L_3$, $L_1 \cup (L_2 \cup L_3) = (L_1 \cup L_2) \cup L_3$; $R_3)$ $L_1 \cap (L_2 \cup L_1) = L_1$, $L_1 \cup (L_2 \cap L_1) = L_1$. A lei $R_1)$ diz-se *lei comutativa*; $R_2)$ é a *lei associativa*; e $R_3)$ recebe o nome de *lei de absorpção*.

Chama-se um *reticulado* um sistema algébrico com duas operações sujeitas às três leis referidas. $\mathfrak{R}$ é, pois, um reticulado.

O sistema das 3 leis mantem-se invariante (fica sob a mesma forma) se trocarmos entre si os sinais $\cap$ e $\cup$. Conclui-se daqui a afirmação seguinte, que constitui o

PRINCÍPIO DE DUALIDADE DO ESPAÇO PROJECTIVO: *Se, tomados certos subespaços de $\mathfrak{P}_n$, ligados entre si pelas operações $\cap$ e $\cup$, pudermos deduzir, por via de $R_1)$, $R_2)$ e $R_3)$, certos resultados para os referidos subespaços, então, também se podem deduzir doutros subespaços de $\mathfrak{P}_n$, ligados entre si pelas operações indicadas, mas com troca dos respectivos sinais, os resultados que se obtêm dos resultados anteriores fazendo neles a substituição dos espaços e procedendo à mesma troca de operações.*

Se a justificação deste princípio reside precisamente, como já se subentendeu, no facto de $R_1)$, $R_2)$ e $R_3)$ gozarem da propriedade de invariância em face da troca dos sinais $\cap$ e $\cup$, a sua aplicação exige que existam em $\mathfrak{P}_n$ subespaços que possam ligar-se pela referida

troca, quando existem subespaços ligados pelos sinais. A noção de *espaço dual de* $\mathfrak{P}_n$ levar-nos-á a concluir uma tal existência.

2) **Espaço dual de** $\mathfrak{P}_n$ – Tomemos um hiperplano de $\mathfrak{P}_n$, de equação

$$u_0\xi_0 + u_1\xi_1 + \cdots + u_n\xi_n = 0 .$$

Este hiperplano representa a totalidade dos pontos de $\mathfrak{P}_n$, de coordenadas $[\xi_0, \xi_1, \cdots, \xi_n]$, que verificam equação. Não há, porém, uma única maneira de escrever a equação do hiperplano. Com efeito, suponhamos que $v_0\xi_0 + v_1\xi_1 + \cdots + v_n\xi_n = 0$ representa o mesmo hiperplano. Então, as duas equações não são distintas. A matriz $\begin{bmatrix} u_0 & u_1 \cdots u_n \\ v_0 & v_1 \cdots v_n \end{bmatrix}$ tem a característica 1, e os elementos $v_i \in \mathfrak{K}$ são proporcionais aos elementos u_i. Neste sentido, é necessário e basta, para que dois sistemas de $n+1$ elementos da forma $\{u_0, u_1, \cdots, u_n\}$ representem o mesmo hiperplano, que os referidos sistemas sejam proporcionais.

Vamos construir um espaço projectivo $\mathfrak{P}_n^*$, no qual os pontos têm por coordenadas os elementos u_i, que caracterizam os hiperplanos de $\mathfrak{P}_n$. Diremos, assim, que ao hiperplano, de dimensão $n-1$, em $\mathfrak{P}_n$, corresponde o ponto, de dimensão zero, em $\mathfrak{P}_n^*$. A soma das duas dimensões é $(n-1)+0 = n-1$.

Consideremos, em seguida, um subespaço L, de $\mathfrak{P}_n$, de dimensão r, representado por um sistema do tipo

$$(1) \qquad \begin{aligned} &a_{10}\xi_0 + a_{11}\xi_1 + \cdots + a_{1n}\xi_n = 0 , \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &a_{m0}\xi_0 + a_{m1}\xi_1 + \cdots + a_{mn}\xi_n = 0 , \end{aligned}$$

de característica $n-r$. Os pontos do referido subespaço estão, pois, em $n-r$ hiperplanos (independentes), cada um dos quais definido por um sistema de $n+1$ elementos a_{ik}. Estes sistemas de $n+1$ elementos, em número de $n-r$, definem uma submultiplicidade vectorial de dimensão $n-r$. Se construirmos todos os vectores dessa submultiplicidade, encontramos todos os hiperplanos que contêm o subespaço de dimensão r de que partimos. A mesma submultiplicidade está, porém, associada em $\mathfrak{P}_n^*$ a um subespaço projectivo de dimensão $n-r-1$. Diremos que ao subespaço, de dimensão r, em $\mathfrak{P}_n$, corresponde um subespaço L^*, de dimensão $n-r-1$, em $\mathfrak{P}_n^*$. A soma das duas dimensões é ainda $r+(n-r-1) = n-1$.

O espaço $\mathfrak{P}_n^*$ recebe o nome de *espaço projectivo dual de* $\mathfrak{P}_n$.

Tomemos dois subespaços L_1 e L_2, de $\mathfrak{P}_n$, de dimensões, respectivamente, r_1 e r_2. Se for $L_1 \supseteq L_2$, o sistema que define L_2 pode obter-se juntando certas equações ao sistema que define L_1, equações que são independentes das equações de L_1, se $L_1 \supset L_2$. Daqui resulta que, para os subespaços correspondentes L_1^* e L_2^*, se tem $L_1^* \subseteq L_2^*$. Quanto às suas dimensões, que são $n - r_1 - 1$ e $n - r_2 - 1$, respectivamente, vê-se que, de harmonia com a inclusão escrita, vale a desigualdade $n - r_1 - 1 \geqslant n - r_2 - 1$, pois que é $r_1 \leqslant r_2$.

Imaginemos agora que L_1 e L_2 são quaisquer. É muito fácil de reconhecer a validade das duas igualdades seguintes:

$$(L_1 \cap L_2)^* = L_1^* \cup L_2^*, \qquad (L_1 \cup L_2)^* = L_1^* \cap L_2^*.$$

Conclui-se daqui que, havendo em $\mathfrak{P}_n$ subespaços relacionados entre si, de certa maneira, pelas operações $\cap$ e $\cup$, há em $\mathfrak{P}_n^*$ subespaços que estão nas relações obtidas das anteriores por troca dos sinais $\cap$ e $\cup$. Ora $\mathfrak{P}_n^*$ aparece-nos como um espaço projectivo construido pelo mesmo processo que levou a $\mathfrak{P}_n$. Abstraindo da passagem de $\mathfrak{P}_n$ a $\mathfrak{P}_n^*$, quer dizer, passando a considerar os sistemas $\{u_0, u_1, \cdots, u_n\}$ como representando agora pontos $[u_0, u_1, \cdots, u_n]$ de $\mathfrak{P}_n$, define se em $\mathfrak{P}_n$, partindo dum subespaço L, um subespaço $\overline{L} \subseteq \mathfrak{P}_n$. As relações entre os subespaços L^* são as mesmas que entre os subespaços $\overline{L}$. Portanto, como afirmámos no final do número anterior, se há em $\mathfrak{P}_n$ subespaços projectivos relacionados entre si, de certo modo, pelas operações $\cap$ e $\cup$, também há subespaços em condições de se poder aplicar o princípio de dualidade.

Embora, pelos raciocínios já feitos, saibamos determinar as equações de $\overline{L}$, conhecidas as equações de L, vamos insistir nessa determinação. Partamos de $L \subseteq \mathfrak{P}_n$, de dimensão r, ao qual corresponde a submultiplicidade vectorial $\mathfrak{L}$, de dimensão $r+1$, de $\mathfrak{M}_{n+1}$, e de equações (1). Conforme vimos em (VII, 3, 1), as equações de $\mathfrak{L}$, suposta definida por uma base $\mathfrak{b}_1, \cdots, \mathfrak{b}_{r+1}$, podem ser também escritas sob a forma

$$(2) \qquad \mathfrak{a}_i \cdot \mathfrak{x} = 0; \quad [i = 1, 2, \cdots, (n+1) - (r+1) = n - r],$$

onde os vectores $\mathfrak{a}_i$, determinados como se indicou naquele lugar, têem componentes que são, por exemplo, dadas pelos coeficientes de $n - r$ das equações (1). Vem assim $\mathfrak{a}_i \cdot \mathfrak{b}_j = 0, (i = 1, \cdots, n - r; j = 1, \cdots, r+1)$. Ora as equações de $\overline{\mathrm{L}}$ (ou de L*) são precisamente as seguintes:

$$\mathfrak{b}_j \cdot \mathfrak{x} = 0, \quad (j = 1, 2, \cdots, r+1).$$

3) **Coordenadas pluckerianas** — Quando nos não referimos a $\mathfrak{P}_n^*$, mas únicamente a $\mathfrak{P}_n$, é habitual utilizar a terminologia a que nos vamos referir.

Escrevendo a equação dum hiperplano $u_0\xi_0 + u_1\xi_1 + \cdots + u_n\xi_n = 0$, os elementos $\{u_0, u_1, \cdots, u_n\}$ chamam-se *coordenadas pluckerianas* do hiperplano. E quando se trata do subespaço L, de dimensão r, e de equações $\mathfrak{a}_i \cdot \mathfrak{x} = 0$, satisfeitas pelos vectores $\mathfrak{b}_j$, base da multiplicidade vectorial $\mathfrak{L}$, relativa a L, é costume dizer-se que os $\mathfrak{a}_i$ constituem uma base duma *paveia* ou *estrela* de ordem $n - r - 1$ de hiperplanos. Pertencem à paveia todos os hiperplanos cujas coordenadas pluckerianas são obtidas construindo a submultiplicidade vectorial gerada pelos $\mathfrak{a}_i$. O subespaço L, de dimensão r, é o *núcleo* da paveia.

Finalmente, observemos que se fala na dependência ou independência de hiperplanos, como aliás se deu a entender já ao analisar o sistema (1) do número anterior, na medida em que se fala da dependência ou independência dos «vectores» definidos pelas suas coordenadas pluckerianas.

§ 3. Coordenadas projectivas generalizadas

1) **Definição** — Consideremos o espaço projectivo $\mathfrak{P}_n$ e um subespaço L, de dimensão r. Sabemos que se podem encontrar, em L, $r+1$ pontos independentes $A_0, A_1, \cdots A_r$, os quais serão fixados por vectores de coordenadas correspondentes, $\mathfrak{a}_0, \cdots, \mathfrak{a}_r$. Se Q for um ponto qualquer de L e $\mathfrak{x}$ um vector de coordenadas de Q, tem-se

$$(1) \qquad \mathfrak{x}\lambda = \mathfrak{a}_0\eta_0 + \mathfrak{a}_1\eta_1 + \cdots + \mathfrak{a}_r\eta_r, \quad (\lambda \neq 0).$$

Os elementos η_i, embora tenhamos fixado os A_j e os $\mathfrak{a}_j$, não são determinados. E se dermos toda a liberdade possivel à escolha dos A_j e dos $\mathfrak{a}_j$ (ou, até, apenas, á escolha destes últimos), podem os η_i tomar valores quaisquer.

Para dar interese à nova definição dos pontos de L, têem de ser feitas limitações convenientes. Nesse sentido, fixam-se os pontos A_j, que passam então a designar-se por *pontos fundamentais*, e, quanto aos $\mathfrak{a}_j$, apenas serão permitidas as escolhas a que nos vamos referir.

Seja E um novo ponto de L, que não dependa de quaisquer r pontos, de entre os $r+1$ pontos fundamentais. Então, escolhido E, que se diz *ponto unidade*, apenas permitiremos aqueles sistemas de $\mathfrak{a}_j$

tais que seja possivel encontrar um vector e de coordenadas de E, por forma que se tenha

$$e\mu = a_0 + a_1 + \cdots + a_r . \tag{2}$$

A existência de tais a_j não é difícil de estabelecer. Imaginemos, com efeito, que se escreve $e\rho = \overline{a}_0\rho_0 + \cdots + \overline{a}_r\rho_r$, onde os $\overline{a}_j$ são vectores de coordenadas dos A_j. Basta pôr, em seguida, $a_0 = \overline{a}_0\rho_0, \cdots, a_r = \overline{a}_r\rho_r$, para se chegar a uma igualdade do tipo (2).

Se, agora, com duas escolhas de vectores de coordenadas, for, de

$$e\lambda = a_0 + \cdots + a_r, \qquad e\mu = \overline{a}_0 + \cdots + \overline{a}_r,$$

vamos ver que, então, as coordenadas x_i e ζ_i, dum mesmo ponto Q, determinadas conforme o preceito indicado em (1), são proporcionais. Comecemos por observar que, sendo $\overline{a}_0 = a_0\lambda_0, \cdots, \overline{a}_r = a_r\lambda_r$, da relação

$$a_0\frac{u}{\lambda} + \cdots + a_r\frac{u}{\lambda} = a_0\frac{\lambda_0}{\mu} + \cdots + a_r\frac{\lambda_r}{\mu},$$

se conclui ser $\lambda_0 = \cdots = \lambda_r = \mu/\lambda$. Então, pondo

$$\mathfrak{x}\rho = a_0 x_0 + \cdots + a_r x_r, \qquad \mathfrak{x}\sigma = \overline{a}_0\zeta_0 + \cdots + \overline{a}_r\zeta_r,$$

tem-se $\mathfrak{x}\sigma = a_0\frac{\mu}{\lambda}\zeta_0 + \cdots + a_r\frac{\mu}{\lambda}\zeta_r$, de sorte que

$$\frac{x_0}{\rho} = \frac{\mu}{\lambda}\frac{\zeta_0}{\sigma}, \cdots, \frac{x_r}{\rho} = \frac{\mu}{\lambda}\frac{\zeta_r}{\sigma}; \text{ ou seja } x_i = \tau\zeta_i,$$

com $(i = 0, 1, \cdots, r)$ e $\tau = \frac{\mu}{\lambda}\cdot\frac{\rho}{\sigma}$. A afirmação feita está provada.

O conjunto dos pontos A_j e do ponto E constitui um *sistema de coordenadas projectivas de* L, que será designado por $(A_0, A_1, \cdots, A_r/E)$, ou, mais abreviadamente ainda, por (A_i/E). As coordenadas x_i de cada ponto $Q \in L$, determinadas de harmonia com o método acabado de indicar, chamam-se *coordenadas projectivas generalizadas do ponto*.

O conjunto dos pontos A_j diz-se *simplex fundamental*. Os diferentes A_j constituem os *vertices* do simplex e os subespaços de dimensão $r-1$, definidos por cada sistema de r pontos A_j, tomam o nome de *lados* do simplex. No caso de se ter $r+1=3$, o simplex designa-se por *triângulo fundamental*, enquanto que, sendo $r+1=4$, se obtém um *tetraedro fundamental*.

O ponto E recebe a designação de ponto unidade, pelo facto de as suas coordenadas generalizadas serem $|1, 1, \cdots, 1|$, ou qualquer sistema de elementos iguais.

Consideremos, por exemplo, o lado S_i do simplex que não contém o ponto A_i. Para cada ponto desse lado, um vector de coordenadas correspondente é definido pela igualdade $\mathfrak{x}\lambda = a_0 x_0 + \cdots + a_{i-1}x_{i-1} + a_{i+1}x_{i+1} + \cdots + a_r x_r$. Significa isto que, para os pontos de S_i é $x_i = 0$, ou seja, que a equação do lado S_i, no sistema de coordenadas projectivas generalizadas em causa é $x_i = 0$.

É interessante observar que as coordenadas projectivas $[\xi_0, \xi_1, \cdots, \xi_n]$, introduzidas nos dois §§ anteriores, às quais podemos chamar *coordenadas naturais*, podem ser também interpretadas como coordenadas generalizadas. Para o verificarmos, comecemos por notar que um sistema de coordenadas generalizadas em $\mathfrak{P}_n$ exige se tomem $n+1$ pontos independentes para vértices dum simplex. Se esses pontos forem

$$A_j = [\delta_{0j}, \delta_{1j}, \cdots, \delta_{nj}], \quad (j = 0, 1, \cdots, n+1), \quad \delta_{ij} = \begin{cases} 0, \text{ se } i \neq j, \\ 1, \text{ se } i = j, \end{cases}$$

e o ponto fundamental for $E[1, 1, \cdots, 1]$, então, tomando para cada um dos pontos o vector de coordenadas definido pelas próprias coordenadas indicadas para cada um deles, verifica-se ser válida a igualdade $e = a_0 + a_1 + \cdots + a_n$, enquanto que, tomando um ponto $P = [\xi_0, \xi_1, \cdots, \xi_n]$, se tem, para o vector $\mathfrak{x}$ correspondente, de componentes ξ_i, $\mathfrak{x} = a_0\xi_0 + a_1\xi_1 + \cdots + a_n\xi_n$. As coordenadas generalizadas de P são agora, efectivamente, os elementos ξ_i, ou qualquer sistema de elementos proporcionais a estes.

2) **Matrizes e coordenadas generalizadas** — A igualdade $\mathfrak{x}\lambda = a_0 x_0 + \cdots + a_n x_n$, relativa a um sistema (A_i/E), introduzido em $\mathfrak{P}_n$, vai ser interpretada em notação matricial. Ela mostra que, se designarmos, num sistema fundamental $e_0, e_1, \cdots, e_n$, as componentes de cada vector a_i, por $(a_{0i}, a_{1i}, \cdots, a_{ni})$, se tem

$$\begin{aligned} \lambda\xi_0 &= a_{00}x_0 + a_{01}x_1 + \cdots + a_{0n}x_n, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ \lambda\xi_n &= a_{n0}x_0 + a_{n1}x_1 + \cdots + a_{nn}x_n, \end{aligned}$$

de sorte que, em termos de matrizes, se pode escrever

$$(1) \qquad \lambda \begin{bmatrix} \xi_0 \\ \vdots \\ \xi_n \end{bmatrix} = \begin{bmatrix} a_{00} & a_{01} \cdots a_{0n} \\ \cdots\cdots\cdots \\ a_{n0} & a_{n1} \cdots a_{nn} \end{bmatrix} \cdot \begin{bmatrix} \eta_0 \\ \vdots \\ \eta_n \end{bmatrix}.$$

Designando abreviadamente por $[\xi]$ a matriz de uma coluna do 1.º membro e por $[\eta]$ a matriz análoga do segundo, teremos, em vez de (1),

$$\lambda [\xi] = A \cdot [\eta],$$

onde $A = (a_{ij})$, $(i, j = 0, 1, \cdots, n)$. Como os vectores a_i são linearmente independentes, o determinante $|a_{ij}| = |A|$, como se viu em (IX, 1, 1), é diferente de zero. Daí resulta que a matriz A, nos termos indicados em (IX, 4, 2), é uma matriz invertível. Por meio do par de fórmulas

$$(2) \qquad \begin{aligned} \lambda [\xi] &= A \cdot [\eta], \\ [\eta] &= \lambda A^{-1} \cdot [\xi], \end{aligned}$$

ligamos entre si as coordenadas naturais dos pontos de $\mathfrak{P}_n$ e as coordenadas generalizadas dos mesmos pontos relativas a um sistema (A_i / E). Daremos o enunciado a seguir, que resume os resultados obtidos:

TEOREMA: *Dado o espaço projectivo $\mathfrak{P}_n$, a todo o sistema de coordenadas projectivas generalizadas se associa uma matriz invertível, determinada a menos dum factor constante. Recìprocamente, conhecida uma matriz invertível, ela associa-se sempre a um sistema de coordenadas projectivas generalizadas.*

3) **Coordenadas generalizadas dum hiperplano** — Sabemos que a equação dum hiperplano, em coordenadas naturais, é da forma $u_0 \xi_0 + u_1 \xi_1 + \cdots + u_n \xi_n = 0$. Sob forma matricial, pode escrever-se

$$(1) \qquad [u_0 u_1 \cdots u_n] \begin{bmatrix} \xi_0 \\ \xi_1 \\ \vdots \\ \xi_n \end{bmatrix} = 0.$$

O primeiro membro é o produto duma matriz de uma linha por uma matriz de uma coluna. Se mudarmos de coordenadas, conforme se indicou nas fórmulas (2) do número anterior, a equação (1) reveste-se do aspecto

$$(2) \qquad \lambda^{-1} [u_0 u_1 \cdots u_n] A [\eta] = 0.$$

Utilizando a abreviatura $[u]$ para significar a matriz $[u_0 u_1 \cdots u_n]$, escreveremos, em vez de (2), $\lambda^{-1} [u] A [\eta] = 0$. Pondo ainda $[v_0 v_1 \cdots v_n] = \lambda^{-1} [u] A$, é $[v][\eta] = 0$, se $[v] = [v_0 v_1 \cdots v_n]$. A equação do hiperplano (1), nas coordenadas η_i, é, assim, $v_0 \eta_0 + v_1 \eta_1 + \cdots + v_n \eta_n = 0$, ou, em forma matricial desenvolvida,

$$[v_0 v_1 \cdots v_n] \begin{bmatrix} \eta_0 \\ \eta_1 \\ \vdots \\ \eta_n \end{bmatrix} = 0.$$

Escrevendo simultâneamente as fórmulas de transformação para as coordenadas dos pontos e dos hiperplanos temos o conjunto das igualdades seguintes:

$$(3) \qquad \begin{aligned} \lambda [\xi] &= A [\eta], \\ [v] &= \lambda^{-1} [u] A. \end{aligned}$$

4) **Representação dos subespaços de $\mathfrak{P}_n$** — Um subespaço de dimensão r, de $\mathfrak{P}_n$, é representado por um sistema linear nos ξ_i, da forma

$$\sum_{k=0}^{n} b_{ik} \xi_k = 0, \qquad (i = 1, 2, \cdots, m).$$

É um sistema de característica $n - r$. Introduzindo a matriz $B = (b_{ik})$, as equações anteriores condensam-se na equação única

$$(1) \qquad B \cdot [\xi] = 0.$$

Mudando de coordenadas, obtemos, em vez de (1), esta outra equação

$$\lambda^{-1} B A [\eta] = 0, \text{ ou } C[\eta] = 0, \text{ se } C = AB.$$

A dimensão do subespaço que era r. quando avaliada no sistema das coordenadas naturais, é ainda r no novo sistema de coordenadas. De facto, a nova dimensão é dada tendo em conta a característica da matriz BA. Ora não é difícil de provar que, tratando-se do produto duma matriz de característica $n - r$ por uma matriz invertível, o valor da característica do produto continua a ser $n - r$.

Inversamente, tomada uma equação material do tipo $C[\eta]=0$, onde C é uma matriz de característica $n-r$, podemos representar em coordenadas naturais o subespaço definido por aquela equação, servindo-nos uma vez mais da primeira equação (3) do número anterior, o que nos levará a $\lambda C A^{-1}[\xi]=0$, ou seja a $B[\xi]=0$, desde que se ponha $B=CA^{-1}$.

5) **Relação entre dois sistemas de coordenadas projectivas generalizadas** — Imaginemos agora dois sistemas (A_i/E) e (A'_i/E'), $(i=0,1,\cdots,n)$, de coordenadas projectivas, aos quais respeitam as coordenadas η_i e η'_i, respectivamente. O nosso objectivo é o de dar as relações que ligam os η_i aos η'_i. Servimo-nos, para isso, das coordenadas naturais como intermediárias. Temos

$$(1) \qquad \lambda[\xi]=A[\eta], \quad \lambda'[\xi]=A'[\eta'],$$

onde, na 2.ª igualdade figuram símbolos de significado idêntico aos que figuram na primeira. De (1) deduzimos, sucessivamente,

$$[\xi]=\lambda^{-1}A[\eta], \quad \lambda'\lambda^{-1}A[\eta]=A'[\eta'], \quad [\eta']=\rho A'^{-1}A[\eta],$$

onde $\rho=\lambda'\lambda^{-1}$. Claramente que a matriz $D=A'^{-1}A$ é uma matriz invertível, por ser o produto de duas matrizes invertíveis. As fórmulas de transformação de coordenadas ficam, assim, condensadas na igualdade

$$[\eta']=\rho D[\eta].$$

Inversamente, se for dada uma matriz invertível D, esta matriz é sempre matriz de transformação de coordenadas projectivas em coordenadas projectivas, pois que, se escrevermos $[\eta']=\rho D[\eta]$, podemos, em seguida, arbitrar λ e A, e, depois, por meio das relações $\rho=\lambda'\lambda^{-1}$, $D=A'^{-1}A$, determinar λ' e A'.

Também para as coordenadas generalizadas dum hiperplano se põe o mesmo problema de transformação. Trata-se de passar das coordenadas v_i para as coordenadas v'_i, relativas a (A'_i/E'). Temos, fazendo intervir os u_i,

$$[v]=\lambda^{-1}[u]A, \qquad [v']=\lambda'^{-1}[u]A',$$

de sorte que

$$[v']=\lambda'^{-1}\lambda\ [v]A^{-1}A'.$$

Às fórmulas (3), de (X, 3, 3), correspondem aqui as igualdades

$$[\eta']=\rho D[\eta], \qquad [v']=\rho^{-1}[v]D^{-1}.$$

Para as obtermos com o mesmo aspecto que têm as citadas fórmulas (3), escreveremos

$$\rho[\eta]=D^{-1}[\eta']$$
$$[v']=\rho^{-1}[v]D^{-1},$$

nas quais podemos ainda fazer $D^{-1}=F$. Os problemas que nos propunhamos tratar neste número ficam resolvidos.

BIBLIOGRAFIA

E. Sperner, *Einführung in die analytische Geometrie und Algebra*, zweiter Teil Göttingen, 1951.
G. Birkhoff, *Lattice theory*, New York, 1948.
H. Hermes, *Einführung in die Verbandstheorie*, Berlin, 1955.
B. L. van der Waerden, *Algebraische Geometrie*, Berlin, 1939.

CAPÍTULO XI

Espaço métrico

§ 1. Formas lineares. Formas bilineares. Formas quadráticas

1) **Formas lineares** – Dado o módulo direito $\mathfrak{M}=\{0,x,y,\cdots,x_1,y_1,z_1,\cdots\}$, sobre o anel de divisão $\mathfrak{D}=\{0,\alpha,\beta,\cdots,\alpha_1,\beta_1,\cdots,\xi,\eta,\cdots\}$, admitamos que se trata dum módulo unitário, nos termos indicados em (VII, 1, 1).

$\Phi(x)$ diz-se uma *forma linear em* x (ou sobre $\mathfrak{M}$), se forem satisfeitos os seguintes axiomas: $L_1)$ $\Phi(x)\in\mathfrak{D}$; $L_2)$ $\Phi(x\alpha)=\Phi(x)\cdot\alpha$; $L_3)$ $\Phi(x+y)=\Phi(x)+\Phi(y)$.

Supostas Φ_1 e Φ_2 duas formas lineares, define-se uma soma $\Phi_1+\Phi_2$, pondo $(\Phi_1+\Phi_2)(x)=\Phi_1(x)+\Phi_2(x)$. E também se introduzem formas lineares $(\alpha\Phi)$, por meio da igualdade $(\alpha\Phi)(x)=\alpha\cdot\Phi(x)$. Deste modo, o conjunto das formas lineares constitui um módulo esquerdo $\mathfrak{M}^*$, sobre $\mathfrak{D}$, como é fácil de verificar. A dependência e independência linear das formas lineares é estabelecida como para os módulos em geral, segundo se indicou em (VIII, 3, 1).

O módulo $\mathfrak{M}^*$ diz-se *espaço conjugado de* $\mathfrak{M}$, este último podendo receber a designação de *espaço vectorial sobre* $\mathfrak{D}$.

TEOREMA: *Se* $\Phi_1,\cdots,\Phi_t$ *forem formas lineares independentes, existem elementos* $x_1,\cdots,x_t\in\mathfrak{M}$ *tais que* $\Phi_i(x_j)=\delta_{ij}$, *com* $\delta_{ij}=u\in\mathfrak{D}$, *se* $j=i$, *e* $\delta_{ij}=0$, *se* $j\neq i$, $(i,j=1,2,\cdots,t)$. Por hipótese, existe y_1 tal que $\Phi_1(y_1)=\alpha\neq 0$. Então, é $\Phi_1(y_1\alpha^{-1})=u$. Pondo $y_1\alpha^{-1}=z_1$, tem-se $\Phi_1(z_1)=u$. Em seguida, façamos $y=x-z_1\Phi_1(x)$. Vê-se que

$\Phi_1(y)=0$. Todavia, existe y tal que $\Phi_2(y)\neq 0$, pois, de contrário, ter-se-ia $\Phi_2(x)-\Phi_2(z_1)\Phi_1(x)=0$, não havendo independência entre Φ_1 e Φ_2. Se, fazendo $y=y_2$, for $\Phi_2(y_2)=\beta\neq 0$, é $\Phi_2(y_2\beta^{-1})=u$, de sorte que, pondo $z_2=y_2\beta^{-1}$, vale $\Phi_1(z_1)=u$, $\Phi_1(z_2)=0$, $\Phi_2(z_2)=u$. E, pondo $x_1=z_1-z_2\Phi_2(z_1)$, $x_2=z_2$, é $\Phi_1(x_1)=u$, $\Phi_1(x_2)=0$, $\Phi_2(x_1)=0$, $\Phi_2(x_2)=u$. Duma maneira geral, admitamos que, para $r<t$, se construiram $y_1,y_2,\cdots,y_r$, sob as condições $\Phi_i(y_j)=\delta_{ij}$, $(i,j=1,2,\cdots,r)$; vamos construir $x_1,\cdots,x_{r+1}$, de modo a realizar as igualdades $\Phi_i(x_j)=\delta_{ij}$, $(i,j=1,\cdots,r+1)$. O teorema ficará provado.

Se pusermos $y=x-\sum_{i=1}^{r}y_i\Phi_i(x)$, verifica-se que $\Phi_j(y)=0$, para cada $j=1,2,\cdots,r$. Para um certo y é, porém, $\Phi_{r+1}(y)\neq 0$, visto que, de contrário, ter-se-ia a relação $\Phi_{r+1}(x)-\Phi_{r+1}(y_1)\Phi_1(x)-\cdots-\Phi_{r+1}(y_r)\Phi_r(x)=0$, qualquer que fosse x, e não haveria independência entre $\Phi_1,\cdots,\Phi_{r+1}$. Se, fazendo $y=z_{r+1}$, for $\Phi_{r+1}(z_{r+1})=\gamma\neq 0$, é $\Phi_{r+1}(z_{r+1}\gamma^{-1})=\Phi_{r+1}(y_{r+1})=u$, com $y_{r+1}=z_{r+1}\gamma^{-1}$. Por meio das igualdades

$$x_1=y_1-y_{r+1}\Phi_{r+1}(y_1),\ \cdots,\ x_r=y_r-y_{r+1}\Phi_{r+1}(y_r),\ x_{r+1}=y_{r+1}$$

ficam definidos os desejados $x_1,\cdots,x_{r+1}$.

COROLÁRIO: *Se* $\Phi(x)$ *for uma forma linear que se anula sempre que se anulam as formas* $\Phi_1,\cdots,\Phi_m$, *então* Φ *é uma combinação linear dos* Φ_i. Suponhamos que, nos Φ_i, são apenas linearmente independentes $\Phi_1,\cdots,\Phi_s$. Se Φ fosse independente destes últimos, poderíamos encontrar, à face do teorema anterior, um elemento x_{s+1} para o qual $\Phi(x_{s+1})\neq 0$, $\Phi_i(x_{s+1})=0$, contra a hipótese do enunciado.

2) **Dimensão do espaço conjugado** – O problema da dimensão de que nos vamos ocupar respeita ùnicamente ao caso em que $\mathfrak{M}$ se supõe finito, de dimensão m, por exemplo. Conforme o teorema do número anterior, suponhamos $\Psi_1,\cdots,\Psi_t$ formas lineares independentes e admitamos que $\Psi_i(x_j)=\delta_{ij}$, $(i,j=1,2,\cdots,t)$. Pondo $x_1\alpha_1+x_2\alpha_2+\cdots+x_t\alpha_t=0$, vê-se que $\Psi_i(x_1\alpha_1+\cdots+x_t\alpha_t)=\Psi_i(0)=0=\alpha_i$, de sorte que os x_j são independentes-$\mathfrak{D}$. Daqui resulta que a dimensão do espaço conjugado é, quando muito, igual à dimensão de $\mathfrak{M}$.

Ora, se $e_1,\cdots,e_n$ for uma base de $\mathfrak{M}$, uma forma linear Φ fica definida dando os valores de $\Phi(e_i)$, $(i=1,2,\cdots,n)$. Então, com

efeito, sendo $x = e_1\xi_1 + \cdots + e_n\xi_n$, é $\Phi(x) = \sum \Phi(e_i)\xi_i$. Nessas condições, tomemos $\Phi_i(e_j) = \delta_{ij}$, $(i, j = 1, 2, \cdots, n)$. Ficam definidas n funções lineares linearmente independentes, pois que, sendo $\beta_1\Phi_1 + \cdots + \beta_n\Phi_n = 0$, é $\sum_i \beta_i \Phi_i(e_j) = 0 = \beta_j$ Daqui este

TEOREMA: *Se o espaço vectorial direito $\mathfrak{M}$ sobre $\mathfrak{D}$, é finito, o seu espaço conjugado $\mathfrak{M}^*$ é igualmente finito e tem a mesma dimensão.*

3) **Formas bilineares** — Suponhamos agora que, ao lado do espaço vectorial $\mathfrak{M}$, se considera o espaço vectorial esquerdo $\mathfrak{M}' = \{0', x', y', \cdots\}$, sobre o mesmo anel de divisão $\mathfrak{D}$. Se a cada ponto $(x', x) \in \mathfrak{M}' \times \mathfrak{M}$ fizermos corresponder um elemento $f(x', x) \in \mathfrak{D}$, conforme a axiomática que vai seguir-se, chamaremos f uma *forma bilinear em* $(\mathfrak{x}', \mathfrak{x})$, *ou sobre* $\mathfrak{M}' \times \mathfrak{M}$: $B_1)$ $f(x', x + y) = f(x', x) + f(x', y)$; $B_2)$ $f(x' + y', x) = f(x', x) + f(y', x)$; $B_3)$ $f(x', x\alpha) = f(x', x)\alpha$; $B_4)$ $f(\alpha x', x) = \alpha f(x', x)$.

Um exemplo importante de forma bilinear é dado pondo $\mathfrak{M}' = \mathfrak{M}^*$ e escrevendo $f(\Phi, x) = \Phi(x)$. Então. com efeito, e por exemplo, tem-se $f(\Phi_1 + \Phi_2, x) = (\Phi_1 + \Phi_2)(x) = \Phi_1(x) + \Phi_2(x) = f(\Phi_1, x) + f(\Phi_2, x)$. De modo análogo se verificam os restantes axiomas.

As considerações que agora vamos passar a fazer, respeitarão ao caso em que $\mathfrak{D} = \mathfrak{K}$ é um corpo. Os respectivos coeficientes $\alpha \in \mathfrak{K}$ serão colocados à direita, em todos os casos. Àlem disso, faremos $\mathfrak{M}' = \mathfrak{M}$, de modo que as formas bilineares passarão a ser aplicações de $\mathfrak{M} \times \mathfrak{M}$ em $\mathfrak{K}$. Àlem disso, admitiremos que $\mathfrak{M}$ é módulo finito sobre $\mathfrak{K}$, de base $(\mathfrak{e}_1, \cdots, \mathfrak{e}_n)$, e representaremos os seus elementos por letras góticas minúsculas, de modo a colocarmo-nos exactamente nas condições do Capítulo VII, a propósito das multiplicidades vectoriais.

Então, para uma forma bilinear $P(\mathfrak{x}, \mathfrak{y})$, se $\mathfrak{x} = \sum \mathfrak{e}_i\xi_i$, $\mathfrak{y} = \sum \mathfrak{e}_i, \eta_i$, tem-se

$$P(\mathfrak{x}, \mathfrak{y}) = P\left(\sum_{i=1}^{n} \mathfrak{e}_i\xi_i, \sum_{j=1}^{n} \mathfrak{e}_j\eta_j\right) = \sum_{i,j} P(\mathfrak{e}_i, \mathfrak{e}_j)\xi_i\eta_j.$$

Fazendo $P(\mathfrak{e}_i, \mathfrak{e}_j) = \alpha_{ij} \in \mathfrak{K}$, concluimos que uma forma bilinear tem o aspecto

$$(1) \qquad P(\mathfrak{x}, \mathfrak{y}) = \sum_{i,j} \alpha_{ij}\xi_i\eta_j, \qquad (i, j = 1, 2, \cdots, n).$$

Reciprocamente: uma expressão como (1) é uma forma bilinear. Nessa expressão consideram-se os ξ_i e os η_j como *variáveis*, no sentido seguinte: o valor de $P(\mathfrak{x}, \mathfrak{y})$ é obtido substituindo os ξ_i e os η_j pelas ~~pelas~~ componentes dos vectores $\mathfrak{x}$ e $\mathfrak{y}$, componentes que podem ser, variando os vectores, quaisquer elementos do corpo $\mathfrak{K}$.

A forma bilinear (1) diz-se não *degenerada*, se só puder ter-se $P(\mathfrak{x}, \mathfrak{y}) = 0$, para qualquer $\mathfrak{y}$, quando for $\mathfrak{x} = 0$. Podemos também dizer que (1) é não degenerada, se só puder ser $\sum_j \left(\sum_i \alpha_{ij}\xi_i\right)\eta_j = 0$, para todos os η_j, se os ξ_i forem todos nulos. Isto equivale a afirmar que o sistema homogéneo

$$\sum_{i=1}^{n} \alpha_{ij}\xi_i = 0, \qquad (j = 1, 2, \cdots, n),$$

tem apenas a solução nula. Assim:

TEOREMA: *É condição necessária e suficiente, para que a forma bilinear (1) seja não degenerada, que o determinante $|\alpha_{ij}|$ seja $\neq 0$.*

A forma bilinear (1) diz-se *simétrica*, se tiver a propridade expressa pela igualdade seguinte: $P(\mathfrak{x}, \mathfrak{y}) = P(\mathfrak{y}, \mathfrak{x})$. É fácil de reconhecer que a condição de simetria é dada pelas igualdades $\alpha_{ij} = \alpha_{ji}$, para todos os valores de i e de j.

4) **Formas quadráticas** — Uma *forma quadrática* $Q(\mathfrak{x})$, no vector $\mathfrak{x}$, é uma expressão do tipo

$$(1) \qquad Q(\mathfrak{x}) = \sum_{i,k=1}^{n} \beta_{ik}\xi_i\xi_k, \qquad (\beta_{ik} \in \mathfrak{K}).$$

Os valores de $Q(\mathfrak{x})$ dependem do vector $\mathfrak{x}$, ou seja, dos valores atribuidos aos ξ_i, quando estas variáveis ξ_i têm $\mathfrak{K}$ como domínio de variação. Por simplicidade, se daí não resultar confusão, escreveremos Q, em vez de $Q(\mathfrak{x})$, para significar a forma quadrática.

Em Q, o coeficiente de $\xi_i\xi_k$ é $\beta_{ik} + \beta_{ki}$. Deste modo, se $\sum_{i,k} \gamma_{ik}\xi_i\xi_k$ fôr outra forma quadrática e se valerem as igualdades $\gamma_{ik} + \gamma_{ki} = \beta_{ik} + \beta_{ki}$, as duas formas quadráticas não são distintas. É habitual, o que não envolve perda de generalidade, quando se fala duma forma quadrática (1), admitir que se tem $\beta_{ik} = \beta_{ki}$. É o que faremos.

Imaginemos $\neq 2$ a característica de $\mathfrak{K}$. Dada a forma quadrática Q, vê-se que a forma bilinear $P(\mathfrak{x},\mathfrak{y}) = \sum \beta_{ik}\xi_i\eta_k$ é tal que $P(\mathfrak{x},\mathfrak{x}) = Q$. Outra forma bilinear $\sum \gamma_{ik}\xi_i\eta_k$ tal que $\gamma_{ik}+\gamma_{ki} = 2\beta_{ik}$ dá origem, pelo processo indicado, à mesma forma quadrática. Se se exigir, porém, que a forma bilinear seja simétrica, da condição $2\gamma_{ik} = 2\beta_{ik}$, conclui-se $\gamma_{ik} = \beta_{ik}$. Assim:

TEOREMA: *Se $\mathfrak{K}$ é um corpo de característica $\neq 2$, dada uma forma quadrática $Q(\mathfrak{x})$, com coeficientes em $\mathfrak{K}$, existe uma e uma só forma bilinear simétrica $P(\mathfrak{x},\mathfrak{y})$ tal que $P(\mathfrak{x},\mathfrak{x}) = Q(\mathfrak{x})$.* Podemos acrescentar que $P(\mathfrak{x},\mathfrak{y})$ é fácil de encontrar, desde que se conheça uma forma bilinear $P_0(\mathfrak{x},\mathfrak{y})$ originando Q. Basta pôr, então,

$$P(\mathfrak{x},\mathfrak{y}) = \frac{1}{2}[P_0(\mathfrak{x},\mathfrak{y}) + P_0(\mathfrak{y},\mathfrak{x})].$$

[Fez-se aqui $u = 1$ e escreveu-se 2 em vez de $2u$].

A forma quadrática Q tem a propriedade expressa na igualdade seguinte:

$$Q(\mathfrak{x}+\mathfrak{y}) = Q(\mathfrak{x}) + 2P(\mathfrak{x},\mathfrak{y}) + Q(\mathfrak{y}), \tag{2}$$

na qual $P(\mathfrak{x},\mathfrak{y})$ é a forma bilinear simétrica que origina a forma quadrática (para evitar certas dificuldades suporemos sempre $\neq 2$ a característica de $\mathfrak{K}$). De facto, partindo de (1), obtem-se

$$\sum_{i,k}\beta_{ik}(\xi_i+\eta_i)(\xi_k+\eta_k) = \sum_{i,k}\beta_{ik}\xi_i\xi_k + \sum_{i,k}\beta_{ik}\xi_i\eta_k + \sum_{i,k}\beta_{ik}\eta_i\xi_k + \sum_{i,k}\beta_{ik}\eta_i\eta_k.$$

Mas, pondo $\sum_{i,k}\beta_{ik}\eta_i\xi_k = \sum_{i,k}\beta_{ki}\xi_i\eta_k = \sum_{i,k}\beta_{ik}\xi_i\eta_k = P(\mathfrak{x},\mathfrak{y})$, reconhece-se que (3) é precisamente a igualdade (2). A forma bilinear simétrica $P(\mathfrak{x},\mathfrak{y})$, a que se refere o teorema e que figura em (2) chama-se *forma polar* da forma quadrática Q.

A forma Q diz-se *não degenerada*, se a sua forma polar fôr não degenerada. Se daí não resultar confusão, designaremos abreviadamente por P a forma polar de Q.

Suponhamos que o corpo $\mathfrak{K}$ é o corpo dos números reais. Então, a forma Q diz-se *definida positiva*, se tomar sempre valores positivos,

qualquer que seja $\mathfrak{x}\neq 0$. Só para $\mathfrak{x} = 0$ é $Q = 0$. Uma tal forma quadrática é sempre não degenerada, porque, se P fosse degenerada, seria $P(\mathfrak{x}_0,\mathfrak{y}) = 0$, para todo o vector $\mathfrak{y}$ e para um certo $\mathfrak{x}_0\neq 0$. Fazendo, depois, $\mathfrak{y} = \mathfrak{x}_0$, obter-se-ia $P(\mathfrak{x}_0,\mathfrak{x}_0) = Q(\mathfrak{x}_0) = 0$, com $\mathfrak{x}_0\neq 0$, o que seria contrário à definição de forma quadrática definida positiva.

5) **Outras propriedades das formas quadráticas** – A teoria das formas quadráticas é susceptível de aplicações importantes. Por isso, dar-lhe-emos um certo desenvolvimento, neste e noutros números.

Partamos da forma quadrática Q, dada na igualdade (1) do número anterior, e suponhamos que se efectua uma mudança de base no espaço vectorial $\mathfrak{M}_n$, pondo

$$[E_1 \cdots E_n] = [\mathfrak{e}_1 \cdots \mathfrak{e}_n]\cdot T, \tag{1}$$

onde $T = (t_{ik})$ é a matriz invertível (também chamada *não singular*) da transformação. Dado um vector $\mathfrak{x}\in\mathfrak{M}_n$, de componentes ξ_i na primeira base, as suas componentes na nova base são, como vimos em (VIII, 1, 3), dada pelas relações

$$\begin{bmatrix}\xi_1\\ \vdots\\ \xi_n\end{bmatrix} = T\cdot\begin{bmatrix}\eta_1\\ \vdots\\ \eta_n\end{bmatrix}, \quad \text{ou} \quad \begin{bmatrix}\eta_1\\ \vdots\\ \eta_n\end{bmatrix} = T^{-1}\cdot\begin{bmatrix}\xi_1\\ \vdots\\ \xi_n\end{bmatrix},$$

de sorte que, por substituição em Q, se obtem

$$Q(\mathfrak{x}) = \sum_{i,k}\beta_{ik}\left(\sum_l t_{il}\eta_l\right)\left(\sum_m t_{km}\eta_m\right) = \sum_{i,k,l,m}\beta_{ik}t_{il}t_{km}\eta_l\eta_m =$$
$$= \sum_{l,m}\gamma_{lm}\eta_l\eta_m, \quad \text{com} \quad \gamma_{lm} = \sum_{i,k}\beta_{ik}t_{il}t_{km}.$$

Utilizando a matriz $T' = (t'_{ik})$, transposta de T, vê-se que $\gamma_{lm} = \sum_{i,k} t'_{li}\beta_{ik}t_{km}$. Deste modo à matriz $B = (\beta_{ik})$, definida por intermédio dos coeficientes da forma quadrática Q, expressa na base inicial, fazemos corresponder, na nova base, a matriz $C = (\gamma_{ik}) = T'BT$. Tanto B como C são matrizes simétricas. Provaremos este

TEOREMA 1: *É possível efectuar uma mudança de base do tipo (1), de tal modo que a expressão de $Q(\mathfrak{x})$ na nova base tenha o aspecto seguinte:* $Q(\mathfrak{x}) = \sum_{i=1}^{n} c_i\eta_i^2$. Faremos a demonstração pelo método de

indução. Admitiremos que, sendo as variáveis ξ_i em número de $n-1$, o teorema é válido, e passamos a verificar a afirmação para a hipótese de n variáveis.

Dada a forma Q, pode dar-se o caso de serem nulos todos os coeficientes $\beta_{ii}, (i=1,2,\cdots,n)$. Se, então, fôr, por exemplo, $\beta_{12}\neq 0$ [um dos β_{ij}, com $i\neq j$, é necessàriamente $\neq 0$, doutro modo não existiria a forma quadrática], a mudança de base $E_1=\varepsilon_1+\varepsilon_2$, $E_2=\varepsilon_1-\varepsilon_2$, $E_i=\varepsilon_i$, $(i\neq 1,2)$, leva às igualdades $\xi_1=\zeta_1+\zeta_2$, $\xi_2=\zeta_1-\zeta_2$, $\xi_i=\zeta_i$, $(i\neq 1,2)$, nas quais designamos pelos ζ_j as novas componentes do vector $\mathfrak{x}$. A forma Q, nas novas variáveis, escreve-se $Q=\beta_{12}(\zeta_1+\zeta_2)(\zeta_1-\zeta_2)+\cdots+\beta_{21}(\zeta_1-\zeta_2)(\zeta_1+\zeta_2)+\cdots=2\beta_{12}\zeta_1^2-2\beta_{12}\zeta_2^2+\cdots$, não se dando já o caso de serem nulos todos os coeficientes dos diferentes termos em ζ_i^2, $(i=1,2,\cdots,n)$. Tais termos designam-se habitualmente por *termos quadrados*.

Regressemos, assim, à forma quadrática Q definida pela expressão (1) do número anterior, e suponhamos não nulo o coeficiente β_{11} do primeiro termo quadrado. Pode dar-se a Q o aspecto

$$Q=\beta_{11}\left(\xi_1+\frac{\beta_{12}}{\beta_{11}}\xi_2+\cdots+\frac{\beta_{1n}}{\beta_{11}}\xi_n\right)^2+\sum_{i,k=2}^{n}\gamma_{ik}\xi_i\xi_k,$$

desde que se ponha $\gamma_{ik}=\beta_{ik}-\frac{\beta_{1i}\beta_{1k}}{\beta_{11}}$. No subespaço de base $(\varepsilon_2,\cdots,\varepsilon_n)$, é possível, em virtude da hipótese de indução, fazer uma mudança de base do tipo $E_i=\sum\varepsilon_k t_{ki}$, $(i,k=2,\cdots,n)$, por forma que se tenha $\sum\gamma_{ik}\xi_i\xi_k=c_2\eta_2^2+\cdots+c_n\eta_n^2$. Será $|t_{ki}|\neq 0$. Se existir uma mudança de base para a qual valham as igualdades

$$(2)\qquad \xi_1+\frac{\beta_{12}}{\beta_{11}}\xi_2+\cdots+\frac{\beta_{1n}}{\beta_{11}}\xi_n=\eta_1,\qquad \xi_i=\sum_{k=2}^{n}t_{ik}\eta_k,$$

a forma quadrática Q vem a tomar, na verdade, o aspecto desejado: $\beta_{11}\eta_1^2+c_2\eta_2^2+\cdots+c_n\eta_n^2$. Ora, de (2), tira-se

$$\xi_1=\eta_1-\left(\frac{\beta_{12}}{\beta_{11}}\cdot\sum_{k=2}^{n}t_{2k}\eta_k+\cdots+\frac{\beta_{1n}}{\beta_{11}}\sum_{k=2}^{n}t_{nk}\eta_k\right),$$

de sorte que, pondo

$$(3)\qquad E_1=\varepsilon_1,\qquad E_i=-\varepsilon_1\left(\frac{\sum_{k=2}^{n}\beta_{1k}\,t_{ki}}{\beta_{11}}\right)+\varepsilon_2 t_{2i}+\cdots+\varepsilon_n t_{ni},$$

com $i=2,3,\cdots,n)$, os E_j, $(j=1,2,\cdots,n)$, formam uma base nas condições desejadas. O determinante da matriz dos coeficientes de (3) é, efectivamente, diferente de zero. O teorema está provado.

Diz-se que uma matriz tem a forma *diagonal*, se apenas são diferentes de zero alguns dos elementos da sua primeira diagonal. Se designarmos por A' a matriz transposta duma matriz A, a proposição acabada de estabelecer leva a este

COROLÁRIO 1: *Dada uma matriz quadrada simétrica* $B=(\beta_{ik})$, *existe uma matriz não singular* T *tal que* $T'BT=C$ *tem a forma diagonal.*

Ao escrever-se $Q(\mathfrak{x})=\sum_{i=1}^{n}c_i\eta_i^2$, podem alguns dos c_i ser nulos. De modo preciso, imaginemos que, na nova base dos E_j, se chegou a $Q(\mathfrak{x})=c_1\eta_1^2+\cdots+c_r\eta_r^2$. Os η_j, $(j=1,\cdots r)$, são formas lineares independentes nos ξ_i, e, além disso, tem-se o seguinte

TEOREMA 2: *O número* r *é um invariante.* De facto, utilizando a nova base, procuremos determinar os vectores $\mathfrak{a}$, de componentes α_i, tais que, qualquer que seja $\mathfrak{x}$, se tenha $Q(\mathfrak{x}+\mathfrak{a})=Q(\mathfrak{x})$. Se um vector $\mathfrak{a}$ tem nulas as componentes $\alpha_1,\cdots,\alpha_r$, esse vector satisfaz à exigência posta. Reciprocamente, se $\mathfrak{a}$ satisfaz à exigência em questão, é $\sum_{i=1}^{r}c_i(\eta_i+\alpha_i)^2-\sum_{i=1}^{r}c_i\eta_i^2=0$, quaisquer que sejam os η_i. Da igualdade anterior, tira-se $\sum_{i=1}^{r}c_i\alpha_i^2+2\sum_{i=1}^{r}c_i\eta_i\alpha_i=0$, para quaisquer η_i. Fazendo iguais a zero todos os η_i, vê-se ser $\sum_{i=1}^{r}c_i\alpha_i^2=0$, de sorte que deverá ter-se $2\sum_{i=1}^{r}c_i\eta_i\alpha_i=0$. Pondo $\eta_1=1$ e os demais η_i iguais a zero, vem $2c_1\alpha_1=0$, o que implica $\alpha_1=0$. Do mesmo modo se chega a $\alpha_2=\cdots=\alpha_r=0$. Conclui-se, portanto, que $Q(\mathfrak{x}+\mathfrak{a})=Q(\mathfrak{x})$ para todo o $\mathfrak{x}$ caracteriza os vectores da submultiplicidade de base $(E_{r+1},\cdots,E_n)$. Este subespaço de dimensão $n-r$, fixa o número $n-r$. O número r é, deste modo, um número determinado. Diz-se muitas vezes, chamando a $n-r$ a *nulidade* da forma quadrática, que r + nulidade de Q = dimensão da multiplicidade (ou do espaço).

Admitamos agora que $\mathfrak{K}$ é o corpo dos números reais. Se pusermos, para os $c_i > 0$, $\sqrt{c_i}\,\eta_i = \zeta_i$, e, para os $c_j < 0$, $\sqrt{-c_j}\,\eta_j = \zeta_j$, Q reveste-se dum aspecto ainda mais simples. Assim, se forem positivos os primeiros s coeficientes c_i e negativos os restantes, obtém-se $Q = \zeta_1^2 + \cdots + \zeta_s^2 - \zeta_{s+1}^2 - \cdots - \zeta_n^2$. Daqui o

COROLÁRIO 2: *É possível efectuar uma mudança de base do tipo (1), de tal modo que uma forma quadrática com coeficientes reais se reduza ao tipo* $\zeta_1^2 + \cdots + \zeta_s^2 - \zeta_{s+1}^2 - \cdots - \zeta_n^2$. Vamos precisar ainda os termos deste enunciado. Tem-se:

TEOREMA 2 (lei da inércia de SYLVESTER): *Se a forma quadrática* $Q(\mathfrak{x})$ *toma o aspecto indicado no corolário anterior, os dois números* r *e* s *são invariantes.* Temos apenas de provar que s é invariante. Suponhamos que era possível chegar, por duas mudanças de base distintas, a

$$Q(\mathfrak{x}) = \zeta_1^2 + \cdots + \zeta_s^2 - \zeta_{s+1}^2 - \cdots - \zeta_r^2, \tag{4}$$

$$Q(\mathfrak{x}) = \eta_1^2 + \cdots + \eta_t^2 - \eta_{t+1}^2 - \cdots - \eta_r^2. \tag{5}$$

Para a primeira mudança, ter-se-ia $[E_1 \cdots E_n] = [\mathfrak{e}_1 \cdots \mathfrak{e}_n]\,P$, enquanto que, para a segunda, seria $[V_1 \cdots V_n] = [\mathfrak{e}_1 \cdots \mathfrak{e}_n]\,T$. Resultaria daqui $[V_1 \cdots V_n] = [E_1 \cdots E_n]\,P^{-1}\,T = [E_1 \cdots E_n]\,R$, onde P, T, R são matrizes invertíveis. Vamos imaginar, pois, que passámos de (4) a (5) por uma mudança de base. Admitamos $t < s$. As equações $\zeta_{s+1} = \cdots = 0, \cdots, \zeta_r = 0$ determinam uma submultiplicidade vectorial $\mathfrak{M}'$, de $\mathfrak{M}_n$, cuja dimensão é $n - (r - s)$. Para todos os vectores de $\mathfrak{M}'$ é $Q(\mathfrak{x}) \geqq 0$. De modo análogo, tem-se $Q(\mathfrak{x}) < 0$, se $\mathfrak{x} \neq 0$ é um vector da submultiplicidade $\mathfrak{M}''$ definida por $\eta_1 = 0, \cdots, \eta_t = 0, \eta_{r+1} = 0, \cdots, \eta_n = 0$. A dimensão de $\mathfrak{M}''$ é $n - (t + n - r) = r - t$. Como se tem $r - t + n - (r - s) = n + s - t > n$, há vectores comuns a $\mathfrak{M}'$ e $\mathfrak{M}''$ não nulos. Para um tal vector, tem-se simultaneamente $Q(\mathfrak{x}) > 0, Q(\mathfrak{x}) < 0$, o que é uma contradição. Não pode ser $t < s$. De modo análogo se veria que não pode ser $s < t$. Logo é $s = t$, como se deseja.

As considerações precedentes levaram a avaliar do comportamento das formas quadráticas à face do grupo linear, tratado em (IX, 4, 2). Faremos adiante algumas limitações para as mudanças de base (ou de variáveis) postas em causa, afim de reconhecermos outras propriedades das formas quadráticas.

§ 2. Os fundamentos da Geometria métrica

1) **O espaço euclideano** — Construida nos Capítulos VII, VIII e IX a geometria linear ou afim, vamos passar a uma situação mais elevada em Geometria, situação em que é possível comparar vectores dirigidos segundo direcções diferentes. Limitar-nos-emos ao caso em que $\mathfrak{K}$ é o corpo dos números reais. Introduziremos, então, o seguinte

POSTULADO MÉTRICO FUNDAMENTAL: *A cada vector* $\mathfrak{x}$ *corresponde um número* $Q(\mathfrak{x}) = \sum_{i,k=1}^{n} g_{ik}\,\xi_i\,\xi_k$, *dado por uma forma quadrática definida positiva.* Um espaço linear, no qual é válido este postulado diz-se um *espaço métrico euclideano*, ou, mais simplesmente, um *espaço euclideano*. $Q(\mathfrak{x})$ diz-se *forma métrica.*

O valor de $\sqrt{Q(\mathfrak{x})}$ diz-se *norma* ou *comprimento* do vector $\mathfrak{x}$.

Consideremos as transformações lineares de $\mathfrak{M}_n$, nos termos em que foram definidas em (IX, 4, 2). Chamaremos *transformações métricas* aquelas que transformam cada vector $\mathfrak{x}$ num vector $\mathfrak{x}'$, de modo que se tenha $Q(\mathfrak{x}) = Q(\mathfrak{x}')$. Tomados os vectores $\mathfrak{x}$ e $\mathfrak{y}$, o valor $P(\mathfrak{x}, \mathfrak{y})$ da forma polar de Q recebe o nome de *produto escalar* dos dois vectores.

Seja φ um endomorfismo de $\mathfrak{M}_n$ sobre si e admitamos que $\mathfrak{a}\varphi = \mathfrak{a}'$, $\mathfrak{b}\varphi = \mathfrak{b}'$. Tem lugar a proposição que passamos a enunciar:

TEOREMA 1: *É condição necessária e suficiente, para que o endomorfismo* φ *seja uma transformação métrica, que, para qualquer par de vectores* $\mathfrak{a}$ *e* $\mathfrak{b}$, *se tenha* $P(\mathfrak{a}, \mathfrak{b}) = P(\mathfrak{a}', \mathfrak{b}')$. A condição é necessária: Se φ é uma transformação métrica, vale a igualdade $Q(\mathfrak{a} + \mathfrak{b}) = Q(\mathfrak{a}' + \mathfrak{b}')$, ou seja, em virtude da relação (2) de (XI, 1, 4),

$$Q(\mathfrak{a}) + 2\,P(\mathfrak{a}, \mathfrak{b}) + Q(\mathfrak{b}) = Q(\mathfrak{a}') + 2\,P(\mathfrak{a}', \mathfrak{b}') + Q(\mathfrak{b}').$$

Daqui se conclui $P(\mathfrak{a}, \mathfrak{b}) = P(\mathfrak{a}', \mathfrak{b}')$, como se afirma no teorema.

A condição é *suficiente*: Da hipótese $P(\mathfrak{a}, \mathfrak{b}) = P(\mathfrak{a}', \mathfrak{b}')$, concluimos $Q(\mathfrak{a}) = Q(\mathfrak{a}')$. O transformado dum vector diferente de zero é $\neq 0$. O núcleo do endomorfismo reduz-se ao vector zero. Trata-se dum automorfismo. O teorema está provado.

O *ângulo* θ de dois vectores $\mathfrak{a}$ e $\mathfrak{b}$, nenhum dos quais é nulo, é definido pela igualdade

$$\cos\theta = \frac{P(\mathfrak{a},\mathfrak{b})}{\sqrt{Q(\mathfrak{a})}\cdot\sqrt{Q(\mathfrak{b})}}.$$

Vamos mostrar que θ é um ângulo real, isto é, vamos ver que se tem $|\cos\theta| \gtrless 1$.

Sendo λ e μ dois números reais, sabemos que

$$Q(\mathfrak{a}\lambda + \mathfrak{b}\mu) = \lambda^2 Q(\mathfrak{a}) + 2\lambda\mu P(\mathfrak{a},\mathfrak{b}) + \mu^2 Q(\mathfrak{b}) \gtrless 0,$$

quaisquer que sejam λ e μ. Tomando $\lambda > 0$, a desigualdade anterior implica $P^2(\mathfrak{a},\mathfrak{b}) - Q(\mathfrak{a})Q(\mathfrak{b}) \gtrless 0$, ou

$$P^2(\mathfrak{a},\mathfrak{b}) \gtrless Q(\mathfrak{a})\cdot Q(\mathfrak{b}), \tag{1}$$

esta última conhecida sob o nome de *desigualdade de* SCHWARZ. Quando o sinal $=$ tem aqui lugar, é $\cos\theta = \pm 1$, e os dois vectores dizem-se *paralelos*. Em todos os casos, resulta de (1) que se tem $|\cos\theta| \gtrless 1$. Na hipótese do paralelismo, obtem-se $Q(\mathfrak{a}\lambda+\mathfrak{b}\mu) = (\lambda\sqrt{Q(\mathfrak{a})} + \mu\sqrt{Q(\mathfrak{b})})^2$, pelo que, escolhendo λ e μ por forma que seja $\lambda\sqrt{Q(\mathfrak{a})} = -\mu\sqrt{Q(\mathfrak{b})}$, vem $Q(\mathfrak{a}\lambda + \mathfrak{b}\mu) = 0$. Conclui-se $\mathfrak{a}\lambda + \mathfrak{b}\mu = 0$, com $\lambda \neq 0$, $\mu \neq 0$. A hipótese do paralelismo arrasta que os dois vectores pertençam à mesma submultiplicidade vectorial a uma dimensão. A recíproca é válida.

Quando $\mathfrak{a}$ e $\mathfrak{b}$ são tais que $P(\mathfrak{a},\mathfrak{b}) = 0$, dizem-se *ortogonais*. O ângulo θ tem o valor $\pm\frac{\pi}{2}$. É válido este

TEOREMA 2: *Um sistema de vectores não nulos ortogonais dois a dois é composto de vectores independentes.* Se $\mathfrak{a}_1, \cdots, \mathfrak{a}_r$ são os vectores em questão, uma igualdade $\mathfrak{a}_1\lambda_1 + \mathfrak{a}_2\lambda_2 + \cdots + \mathfrak{a}_r\lambda_r = 0$, com os λ_i não todos nulos, daria $P(\mathfrak{a}_i, \mathfrak{a}_1\lambda_1 + \cdots + \mathfrak{a}_r\lambda_r) = 0 = P(\mathfrak{a}_i,\mathfrak{a}_1)\lambda_1 + \cdots + P(\mathfrak{a}_i,\mathfrak{a}_i)\lambda_i + \cdots + P(\mathfrak{a}_i,\mathfrak{a}_r)\lambda_r$, para cada $i = 1, 2, \cdots, r$. Como $P(\mathfrak{a}_i,\mathfrak{a}_i) = 0$, se $i \neq j$, e $P(\mathfrak{a}_i,\mathfrak{a}_i) \neq 0$, resulta $\lambda_i = 0$.

COROLÁRIO: *A multiplicidade vectorial associada a um espaço euclideano a* n *dimensões tem, quando muito,* n *vectores ortogonais dois a dois.*

2) **As bases ortonormadas** — Na multiplicidades vectorial $\mathfrak{M}_n$, associada ao espaço euclideano, um vector diz-se *normado* (ou *normalizado*), se a sua norma for igual á unidade. Provaremos o seguinte

TEOREMA 1: *Dada uma base* $(\mathfrak{e}_1, \cdots \mathfrak{e}_n)$, *de* $\mathfrak{M}_n$, *é sempre possivel obter uma base completa de vectores normados, ortogonais dois a dois (base ortonormada).* Comecemos por observar que, tendo-se, na base dada, $Q(\mathfrak{x}) = \sum g_{ik}\xi_i\xi_k$, é $Q(\mathfrak{e}_i) = g_{ii}, (i = 1, 2, \cdots, n)$. Por outro lado, como já várias vezes tivémos ocasião de aplicar, tem-se $Q(\mathfrak{x}\lambda) = \lambda^2 Q(\mathfrak{x})$. Então, se pusérmos $E_1 = \mathfrak{e}_1/\sqrt{Q(\mathfrak{e}_1)}$, é $Q(E_1) = 1$. Em seguida, escrevendo $E'_2 = E_1\alpha + \mathfrak{e}_2\beta$, o 2.º membro não pode ser nulo, a não ser que se tenha $\alpha = \beta = 0$, visto que, doutra forma, haveria uma relação de dependência entre $\mathfrak{e}_1$ e $\mathfrak{e}_2$. Determinando α e β pela condição $P(E_1, E'_2) = P(E_1, E_1)\alpha + P(E_1\cdot\mathfrak{e}_2)\beta = 0$, vê-se que pode sempre supôr-se $\beta = 1, \alpha = -P(E_1, \mathfrak{e}_2)$. Vem, então, $E'_2 = \mathfrak{e}_2 - E_1 P(E_1, \mathfrak{e}_2)$, e, depois, por normalização, $E_2 = E'_2/\sqrt{Q(E'_2)}$. Análogamente, pôr-se-á $E'_3 = E_1\alpha + E_2\beta + \mathfrak{e}_3\gamma$, com as condições $P(E_1, E'_3) = \alpha + P(E_1, \mathfrak{e}_3)\gamma = 0$, $P(E_2, E'_3) = \beta + P(E_2, \mathfrak{e}_3)\gamma = 0$, às quais podemos satisfazer, com $\gamma = 1$, $\alpha = -P(E_1, \mathfrak{e}_3)$, $\beta = -P(E_2, \mathfrak{e}_3)$. o que leva a $E'_3 = \mathfrak{e}_3 - E_1 P(E_1, \mathfrak{e}_3) - E_2 P(E_2, \mathfrak{e}_3)$, $E_3 = E'_3/\sqrt{Q(E'_3)}$. Prossegue-se deste modo, até

$$E'_n = \mathfrak{e}_n - \sum_{i=1}^{n-1} E_i P(E_i, \mathfrak{e}_n), \qquad E_n = \frac{E'_n}{\sqrt{Q(E'_n)}}.$$

O sistema $(E_1, \cdots, E_n)$ é o sistema orto-normado que se desejava. A matriz que faz passar da antiga à nova base é do tipo

$$\begin{bmatrix} a & b & d & \cdots & l \\ 0 & c & e & \cdots & m \\ 0 & 0 & f & \cdots & p \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & r \end{bmatrix} \tag{1}$$

O seu determinante é $\neq 0$, por serem diferentes de zero os elementos que figuram na primeira diagonal.

Escolhida a base ortonormada, a forma métrica $Q(\mathfrak{x})$, também chamada *forma quadrática fundamental*, toma o aspecto $Q(\mathfrak{x}) = \eta_1^2 + \eta_2^2 + \cdots + \eta_n^2$. O teorema demonstrado tem, então, este

COROLÁRIO 1: *Uma forma quadrática definida positiva nas variáveis* $\xi_i, (i = 1, 2, \cdots, n)$, *é sempre uma soma de* n *quadrados de formas lineares nas mesmas variáveis.* Podemos acrescentar um

ADITAMENTO: *As formas lineares* η_i, *nos* ξ_j, *são linearmente independentes.* Já em (XI, 1, 5), antes do enunciado do teorema 2,

fizemos afirmação semelhante. O facto resulta, por exemplo, tendo em conta que os η_i são as novas coordenadas. Também resulta directamente da circunstância de a matriz inversa da matriz (1) ser uma matriz do mesmo tipo, igualmente com elementos diferentes de zero na sua primeira diagonal.

Numa base ortonormada, a caracterização das transformações métricas é feita de modo interessante. Uma matriz diz-se *ortogonal*, quando, consideradas as suas colunas como vectores, esses vectores são normados e ortogonais dois a dois. Então, tem-se:

TEOREMA 2: *É condição necessária e suficiente, para que, numa base ortonormada, uma transformação linear seja uma transformação métrica, que a respectiva matriz seja ortogonal.* Seja A uma matriz relativa a uma transformação métrica. Para os vectores-base $(\varepsilon_1, \cdots, \varepsilon_n)$, os respectivos transformados são dados por

$$\varepsilon'_i = \sum_{k=1}^{n} \varepsilon_k a_{ki}, \quad \text{ou} \quad [\varepsilon'_1 \cdots \varepsilon'_n] = [\varepsilon_1 \cdots \varepsilon_n] A .$$

Mas, sendo $Q(\varepsilon'_i) = P(\varepsilon'_i, \varepsilon'_i) = Q(\varepsilon_i) = 1 = P\left(\sum \varepsilon_k a_{ki}, \sum \varepsilon_j a_{ji}\right) =$

$$= \sum_{k,j} P(\varepsilon_k, \varepsilon_j)\, a_{ki} a_{ji} = \sum_k a_{ki}^2, \quad \text{e} \quad P(\varepsilon'_i, \varepsilon'_l) = \sum_{k,j} P(\varepsilon_k, \varepsilon_j)\, a_{ki}\, a_{jl} =$$

$= \sum_k a_{ki} a_{kl} = P(\varepsilon_i, \varepsilon_l) = 0$, se $i \neq l$, conclui-se imediatamente que a condição do enunciado é necessária. Para se vêr que é suficiente, tomemos A ortogonal. Então $A'A = U_n =$ matriz unidade e $|A| \neq 0$, pelo que A define uma transformação linear. Ela é métrica, pelo facto de conservar a norma e os produtos escalares dos vectores-base.

Em virtude de se ter $A'A = U_n$, resulta também, como vimos em (IX, 4, 2), que $A\,A' = (A')'A' = U_n$. A transformação definida por A' é igualmente ortogonal. Daqui este

COROLÁRIO 2: *Se uma matriz é ortogonal, as linhas satisfazem a ligações análogas às das colunas.*

O subgrupo do grupo linear formado pelas transformações métricas diz-se *grupo euclideano.*

3) **O problema dos eixos principais** — Continuemos a tratar um espaço euclideano com uma base ortonormada para $\mathfrak{M}_n$. Dada uma

forma quadrática qualquer, vamos analisar o seu comportamento em face do grupo ortogonal. Nesse sentido, fixaremos aqui o importante

TEOREMA 1: *É possível, dada a forma quadrática* $B = \sum \beta_{ij} \xi_i \xi_j$, $(i, j = 1, 2, \cdots, n)$, *encontrar uma mudança de eixos levando da base ortogonal a uma base ortogonal, de tal modo que* B *fique reduzida ao tipo* $B(\mathfrak{x}) = \lambda_1 \eta_1^2 + \lambda_2 \eta_2^2 + \cdots + \lambda_n \eta_n^2$. A demonstração, que pode fazer-se por métodos puramente algébricos, vai ser dada admitindo o resultado seguinte, da Análise Matemática: Se a forma quadrática $\sum \beta_{ik} \xi_i \xi_k$ toma valores nos pontos $(\xi_1, \cdots, \xi_n)$ que satisfazem à igualdade $\xi_1^2 + \cdots + \xi_n^2 = 1$, há um desses pontos em que ela tem um máximo absoluto. E também nos será útil esta outra observação: Se a forma quadrática $a x^2 + 2 b x y + c y^2$ toma valores nos pontos (x, y) que satisfazem à igualdade $x^2 + y^2 = 1$ e é máxima para $x = 0$, $y = 1$, então, é $b = 0$.

Seja agora E_1 o vector normado correspondente ao máximo de B. Se fizermos uma mudança de eixos ortogonais, de modo que E_1 seja o primeiro dos novos eixos, a forma quadrática passa a ter o aspecto $B(\mathfrak{x}) = \sum \gamma_{ik} \eta_i \eta_k$ e toma o valor máximo absoluto quando $\eta_1 = 1$, $\eta_2 = \eta_3 = \cdots = \eta_n = 0$. Em particular, se anularmos todas as variáveis em $B(\mathfrak{x})$, salvo, por exemplo, η_1 e η_2, a forma quadrática correspondente de duas variáveis é máxima para $\eta_1 = 1$, $\eta_2 = 0$, o que implica $\gamma_{21} = \gamma_{12} = 0$. Qualquer γ_{1i} é nulo. $B(\mathfrak{x})$ é, assim, do tipo $B(\mathfrak{x}) = \gamma_{11} \eta_1^2 + \sum_{i,k=2}^{n} \gamma_{ik} \eta_i \eta_k$. O coeficiente $\gamma_{11} = \lambda_1$ é o máximo absoluto de $B(\mathfrak{x})$, nas condições indicadas. A forma quadrática $B(\mathfrak{x}) - \gamma_{11} \eta_1^2 = \sum_{i,k=2}^{n} \gamma_{ik} \eta_i \eta_k$ de $n-1$ variáveis, que podemos imaginar referida à base $(E'_2, \cdots, E'_n)$, composta pelos últimos $n-1$ novos eixos, vai ser estudada nos mesmos moldes, sem esquecer, todavia, que a submultiplicidade construida sobre $(E'_2, \cdots, E'_n)$ é ortogonal a E_1. Então, o novo vector E_2, de máximo de $B(\mathfrak{x}) - \gamma_{11} \eta_1^2$, é, efectivamente ortogonal a E_1. O processo leva à demonstração do teorema.

Uma vez conhecida a base $(E_1, \cdots, E_n)$ para a qual $B(\mathfrak{x}) = \lambda_1 \eta_1^2 + \cdots + \lambda_n \eta_n^2$, a matriz inicial B passou a ser uma matriz C definindo um endomorfismo operatório Γ (que podemos designar também por *aplicação linear*). Os eixos E_i dizem-se *eixos principais* da forma quadrática. Em virtude de a aplicação linear Γ, definida

por C, levar à correspondência $E_i \to E_i\Gamma = E'_i = E_i\lambda_i$, isto é, em virtude de se ter $[E'_1 \cdots E'_n] = [E_1 \cdots E_n]\,C = [(E_1\lambda_1)\cdots(E_n\lambda_n)]$, justificam-se as considerações que passamos a fazer.

Sempre que o transformado $\mathfrak{x}'$, dum vector $\mathfrak{x}$, por uma aplicação linear definida por uma matriz C, for tal que $\mathfrak{x}' = \mathfrak{x}\lambda\,(= C\mathfrak{x})$, o vector $\mathfrak{x}$ diz-se um *vector próprio* da matriz e λ diz-se o *valor próprio* ou valor característico correspondente. O teorema enunciado pode revestir-se deste outro aspecto:

TEOREMA 1': *Dada a matriz simétrica* $B = (\beta_{ik})$, *há* n *vectores próprios ortogonais para a transformação linear que ela define.* Este facto permite encontrar uma equação que dá todos os coeficientes λ_i do teorema 1, pois que, para E_1, por exemplo, sendo $E_1\lambda_1 = CE_1 = E_1\Gamma$, a propriedade de o vector E_1 ser característico é independente dos eixos, podendo escrever-se as equações

$$\begin{aligned} &\beta_{11}\xi_1 + \beta_{12}\xi_2 + \cdots + \beta_{1n}\xi_n = \xi_1\lambda_1\,,\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ &\beta_{n1}\xi_1 + \beta_{n2}\xi_2 + \cdots + \beta_{nn}\xi_n = \xi_n\lambda_1\,. \end{aligned}$$

A existência de soluções não nulas nos ξ_i para este sistema homogéneo implica que λ_1 seja raiz da equação

$$\Delta(\lambda) = \begin{vmatrix} \beta_{11}-\lambda & \beta_{12} & \cdots & \beta_{1n}\\ \beta_{21} & \beta_{22}-\lambda & \cdots & \beta_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ \beta_{n1} & \beta_{n2} & \cdots & \beta_{nn}-\lambda \end{vmatrix} = 0\,,$$

chamada *equação secular* ou *equação característica*. O que se disse de λ_1, diz-se de qualquer λ_i, pelo que todos os λ_i, $(i = 1, 2, \cdots, n)$, são raízes da equação secular.

Dos teoremas 1 deste número e do anterior resultam dois corolários.

COROLÁRIO 1: *As raízes da equação secular são reais.*

COROLÁRIO 2: *Dadas duas formas quadráticas* $Q(\mathfrak{x}) = \sum g_{ik}\xi_i\xi_k$ *e* $B(\mathfrak{x}) = \sum \beta_{ik}\xi_i\xi_k$, $(i, k = 1, 2, \cdots, n)$, *a primeira das quais definida positiva, a outra qualquer, há sempre uma base ortonormada para a qual se tem* $Q(\mathfrak{x}) = \sum \eta_i^2$, $B(\mathfrak{x}) = \sum \lambda_i\eta_i^2$, $(i = 1, 2, \cdots, n)$.

Regressemos à equação característica, para darmos ideia de como pode ser discutida. O endomorfismo definido por B, não é, geralmente, uma transformação linear. Tem-se, em geral, $|\beta_{ik}| = 0$, o que significa haver raízes nulas da equação. Os resultados da discussão são os seguintes:

1.° — Se o determinante $|\beta_{ik}|$ ou descriminante da forma quadrática for nulo, a matriz B aplica a multiplicidade $\mathfrak{M}_n$ numa submultiplicidade própria.

2.° — Se a submultiplicidade própria é de ordem $n-k$, existe um menor do descriminante com $n-k$ linhas e $n-k$ colunas (menor de ordem k), que é $\neq 0$, sendo nulos os menores de ordem inferior a k.

3.° — Se há n raízes distintas da equação $\Delta(\lambda) = 0$, haverá n eixos principais isolados e apenas n.

4.° — A existência de uma raiz dupla arrasta a existência de uma infinidade de eixos principais paralelos a uma submultiplicidade a duas dimensões, etc..

5.° — A uma raiz múltipla λ, de ordem k, corresponde uma infinidade de direcções principais paralelas à submultiplicidade definida pelas equações

$$(\alpha)\begin{cases} (\beta_{11}-\lambda)\xi_1 + \beta_{12}\xi_2 + \cdots + \beta_{1n}\xi_n = 0\,,\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ \beta_{n1}\xi_1 + \beta_{n2}\xi_2 + \cdots + (\beta_{nn}-\lambda)\xi_n = 0\,, \end{cases}$$

das quais apenas $n-k$ são distintas.

BIBLIOGRAFIA

N. BOURBAKI, *Algèbre*, Chapitre II, *Algèbre linéaire*, Paris, 1955.

N. JACOBSON, *On the theory of primitive rings*, «Annals of Mathematics», vol. 48, 1947, págs. 8 a 21.

A. ALMEIDA COSTA, *Anéis associativos não comutativos*, Lisboa, 1955.

G. BIRKHOFF e S. MACLANE, *A survey of Modern Algebra*, New York, 1944.

H. WEYL, *Temps, espace et matière*, Blanchard, Paris, 1922.

A. ALMEIDA COSTA, *Notas de Cálculo vectorial*, Porto, 1931.

A. MADUREIRA E SOUSA, *Lições de Álgebra Superior e Geometria Analítica*, tomo 1, Porto, 1948.

E. SPERNER, *Einführung in die analytische Geometrie und Algebra*, zweiter Teil, Göttingen, 1948.

ÍNDICE GERAL

CAPÍTULO I

Conjuntos

CAPÍTULO II

Grupoides e Semi-grupos. Primeiros teoremas sobre grupos

CAPÍTULO III

Grupos

CAPÍTULO IV

Grupos com operadores

CAPÍTULO V

Generalidades sobre aneis e ideais. Números racionais. Corpos ordenados. Números reais

CAPÍTULO VI

Anéis primos e semi-primos. Anéis de ideais principais. Anéis de polinómios. Corpos

CAPÍTULO VII

Grupos abelianos: Multiplicidades vectoriais. Equações lineares homogéneas

CAPÍTULO VIII

Espaços lineares. Equações lineares não homogéneas. Módulos sobre anéis de divisão

CAPÍTULO IX

Determinantes. Transformações lineares

CAPÍTULO X

Espaço projectivo

CAPÍTULO XI

Espaço métrico

ÍNDICE DE NOMES E DE TERMOS