~~UNIVERSIDADE DE LISBOA~~

CURSO DE ÁLGEBRA ABSTRACTA

por
PELO

~~DR.~~ A. ALMEIDA COSTA,
Professor de matemática no Instituto Superior Técnico e na Faculdade de Ciência de Lisboa

~~VOL. I~~

LISBOA — 1954

Imprensa Portuguesa ★ Rua Formosa, 108-116 ★ Porto

PREFÁCIO

Em 1942, no Centro de Estudos Matemáticos *anexo à FACULDADE DE CIÊNCIAS DO PORTO, publicámos, para uso local, um pequeno volume intitulado «Elementos da Teoria dos Grupos», logo seguido de dois outros: «Grupos abelianos e Anéis e ideais não comutativos», também datado de 1942; e «Elementos da Teoria dos Anéis», em 1943.*

Esses tomos, dos quais se fez uma tiragem muito reduzida, esgotaram-se ràpidamente. A doutrina neles contida serve de base ao nosso livro «Hiper-complexos, I», de 1948, igualmente publicado na Colecção do referido Centro de Estudos Matemáticos.

Acedendo a solicitações de vários lados, começamos uma reimpressão, um tanto modificada, dos volumes esgotados. O texto agora apresentado é concebido nos termos precisos das lições feitas aos estudantes da UNIVERSIDADE DE LISBOA que se iniciam na matéria.

Por isso, este tomo 1.º contém uma parte dos fundamentos da Álgebra Moderna, tais como se encontram em todos os livros de índole semelhante. O seu conteúdo é bastante para a compreensão de uma grande parte da nossa obra «Hiper-complexos, I», atrás citada. Acerca dos assuntos versados nesta última, contamos poder

dar a lume, no começo de 1955, complementos importantes, reunidos sob a designação de «Hiper-complexos, II» (1).

Regressando à reimpressão agora iniciada, diremos ainda ser nossa intenção coligir num tomo 2.º aquela outra parte dos fundamentos julgada necessária, para que formem uma colecção independente os quatro livros designados ou a designar do modo seguinte: — Curso de Álgebra abstracta, *vol. I;* Curso de Álgebra abstracta, *vol. II;* Hiper-complexos, I; Hiper-complexos, II.

Lisboa, Setembro de 1954.

A. Almeida Costa.

---

(1) *Para se ter uma ideia da índole dos complementos anunciados, indicamos aqui os títulos dos Capítulos do livro respectivo: Cap. XIII* — Sobre sub-nilanéis; *Cap. XIV* — O radical de Jacobson; *Cap. XV* — Sobre ideais de contracção e aniquiladores na teoria geral dos módulos; *Cap. XVI* — Radical — G, Anti-radical, Ideal regular máximo dum anel; *Cap. XVII* — Anéis primitivos; *Cap. XVIII* — Somas sub-directas de anéis, Anéis semi-simples; *Cap. XIX* — Somas sub-directas de módulos, Módulos semi-simples, Sub-módulos — G; *Cap. XX* — Módulos e anéis com operadores, Anéis simples e Álgebras simples; *Cap. XXI* — Álgebras algébricas, Problema de Kurosch.

CAPÍTULO I

GRUPOS

§ 1 — Postulados, exemplos, regras de cálculo

1) **Postulados** — Tomemos um conjunto $\mathfrak{C} = \{a, b, c, \ldots\}$, de elementos $a, b, c, \ldots$. O conjunto supõe-se *não vazio*, isto é, supõe-se que contém, efectivamente, certos elementos. Diz-se que $\mathfrak{C}$ constitui um *grupo* $\mathfrak{G}$, se se verificam os quatro postulados a seguir.

1) Dados dois elementos a e b, quaisquer, pertencentes ao conjunto, existe um preceito de *multiplicação*, segundo o qual se deduz daqueles dois elementos um outro elemento c, que se chama *produto* de a por b. Em símbolos, escreveremos:

$$a, b \in \mathfrak{C}, \qquad a.b = ab \in \mathfrak{C},$$

significando com o sinal $\in$ que o elemento ou elementos que o precedem pertencem ao conjunto que o segue. O postulado pode enunciar-se dizendo simplesmente que o conjunto $\mathfrak{C}$ é *fechado* relativamente ao produto.

2) Existe uma *unidade direita* u. Isto significa que, para qualquer $a \in \mathfrak{C}$, tem lugar a igualdade $a.u = au = a$, $(u \in \mathfrak{C})$.

3) Existe um *inverso direito* de cada elemento. Isto significa que, para qualquer $a \in \mathfrak{C}$, pode determinar-se $a \in \mathfrak{C}$ tal que $au = u$.

4) O produto definido goza da propriedade associativa: $a\,b.c = a.b\,c$.

Vamos analisar imediatamente algumas consequências destes postulados.

TEOREMA 1: — *Um inverso direito dum elemento é inverso esquerdo do mesmo elemento.* Dado a, supõe-se $a\,\alpha = u$. Pretende-se provar que é também $\alpha\,a = u$. Seja α' um inverso direito de α. É $\alpha\,\alpha' = u$. Multiplicando ambos os membros, à esquerda, por $\alpha\,a$, obtemos: $\alpha\,a.\alpha\,\alpha' = \alpha\,a.u = \alpha\,a$, visto que u é unidade direita. Tendo em conta a propriedade associativa, é também $\alpha\,a.\alpha\,\alpha' = (\alpha\,a.\alpha)\,\alpha' = (\alpha.a\,\alpha)\,\alpha' = \alpha\,u.\alpha' = \alpha\,\alpha' = u$. Por consequência, como se deseja, $\alpha\,a.\alpha\,\alpha' = \alpha\,a = u$.

TEOREMA 2: — *Uma unidade direita é uma unidade esquerda.* Supõe-se que, dado qualquer $b \in \mathfrak{C}$, é $b\,u = b$. Pretende-se provar que é também $u\,b = b$. Representemos por β o inverso direito de b e escrevamos: $b\,\beta.b\,u = u.b\,u = u\,b.u = u\,b$. Depois, observemos que é também $b\,\beta.b\,u = b\,(\beta.b\,u) = b\,(\beta\,b.u) = b.\beta\,b = b\,u = b$. Segue-se $u\,b = b\,u = b$, como se afirmou.

TEOREMA 3: — *Dados quaisquer* $\mathrm{a, b, c} \in \mathfrak{C} = \mathfrak{G}$, *é válida a igualdade* $\mathrm{a\,b = a\,c.\gamma\,b}$, *se* γ *é um inverso direito de* c. A demonstração repousa sobre a propriedade associativa.

OBSERVAÇÃO: — No enunciado dos postulados, poderíamos substituir a propriedade associativa pela propriedade expressa no teorema 3. Vamos ver, com efeito, que, tendo em conta os três primeiros postulados e o referido teorema 3, resulta a propriedade associativa.

Em primeiro lugar, os teoremas 1 e 2 também se demonstram à face das novas hipóteses. Quanto ao teorema 1, tem-se: $\alpha\,a.\alpha\,\alpha' = \alpha\,\alpha' = u$, à face da propriedade admitida no teorema 3; e é, por outro lado, $\alpha\,a.\alpha\,\alpha' = \alpha\,a.u = \alpha\,a$, o que implica $\alpha\,a = u$. Relativamente ao teorema 2, vê-se que é $b\,\beta.b\,u = u.b\,u = u\,b$, assim como, pelo teorema 3, $b\,\beta.b\,u = \mathrm{b}\,u = b$. Resulta, assim, assim, $u\,b = b$.

Demonstrados os dois teoremas, utilizemos ainda a propriedade de hipótese do teorema 3, fazendo, sucessivamente, $b = u$ e $a = u$. Vem $a = a\,c.\gamma$ e $b = c.\gamma\,b$. Portanto, é $a.b\,c = (a\,b.\beta)\,b\,c = a\,b.c$. [Claramente que, sendo c qualquer, é indiferente pôr $a = a\,c.\gamma$ ou $a = a\,b.\beta$].

Continuando na análise das primeiras consequências dos postulados, provaremos agora este

TEOREMA 4: — *Dados* $\mathrm{a, b} \in \mathfrak{G}$, *as equações* $\mathrm{x\,a = b}$ *e* $\mathrm{a\,y = b}$, *em* x *e* y, *respectivamente, são solúveis em* $\mathfrak{G}$. Relativamente à primeira, multipliquemos ambos os membros, à direita, por α. Vem $x\,a.a = b\,a = x$, sendo, na verdade $b\,a.a = b$. Anàlogamente, uma solução de $a\,y = b$ é $y = a\,\mathrm{b}$.

Vamos ver que as soluções encontradas são únicas. Se, por ex., x e x' fossem duas soluções da primeira, resultaria $x\,a = x'a$, $x\,a.a = x'\,a.a = x = x'$. Anàlogamente se trataria a outra equação.

Consideremos as equações particulares $x\,a = a, a\,y = a$. Qualquer delas admite a solução u. Como a solução é única, haverá uma só unidade direita e uma só unidade esquerda. A igualdade das unidades leva-nos à existência de uma única unidade direita e esquerda, que será representada por u e designada por *elemento um* do grupo.

Do mesmo modo, o estudo das equações $x\,a = u, a\,y = u$ leva à conclusão de que há um só inverso direito, que é o único inverso esquerdo, de cada elemento $a \in \mathfrak{G}$. Representar-se-á por a^{-1} e designar-se-á por *inverso* de a.

Concluiremos este número, provando que os quatro postulados 1), 2), 3) e 4) são equivalentes aos três seguintes:

1′) o produto $a.b = a\,b$ é fechado em $\mathfrak{G}$;

2′) tem lugar a propriedade associativa; $a.b\,c = a\,b.c$;

3′) as equações $x\,a = b$, $a\,y = b$ são solúveis em $\mathfrak{G}$.

Vimos já que 1′), 2′) e 3′) se deduzem dos primeiros.

Resta-nos provar que, inversamente, os primeiros são consequências de 1′), 2′) e 3′).

Provemos a existência de unidade direita. Consideremos a equação $a\,y = a$ e chamemos u uma solução, a qual existe, por hipótese. Se, agora, $x\,a = c$ for uma equação cuja solução é x, temos $x\,a.u = c\,u = x.a\,u = x\,a = c$. A relação $c\,u = c$, por ser c arbitrário, justifica a afirmação.

Quanto à existência de inverso, tomemos a equação $a\,y = u$, onde u é a unidade direita, já conhecida. A equação é solúvel, pelo que existe o inverso direito α, de a.

2) **Semi-grupos e grupóides** — Em alguns autores, a definição de *semi-grupo* é dada nos termos seguintes: um conjunto não vazio $\mathfrak{C}$ diz-se um semi-grupo, se nele forem verificados os postulados 1′) e 2′), substituindo-se 3′) por este outro postulado 3″): as equações $x\,a = b$, $a\,y = b$ admitem, quando muito, uma solução no conjunto $\mathfrak{C}$.

Noutros autores, entende-se por semi-grupo um conjunto $\mathfrak{C}$ em que há um produto associativo. É esta a definição que utilizaremos.

Um *grupóide* é um semi-grupo com elemento um.

Tomemos um semi-grupo com a propriedade 3″). Nesse caso, das relações $x\,a = x'\,a$, $a\,y = a\,y'$, deduz-se, respectivamente, $x = x'$, $y = y'$. De facto, se for b o valor comum de $x\,a$ e $x'\,a$, a equação $x\,a = b$ é, então, solúvel. Como a solução é única, vem $x = x'$. O mesmo se diz de $a\,y = a\,y'$.

O facto de uma equação do tipo $x\,a = x'\,a$ levar à conclusão $x = x'$ exprime-se dizendo que é válida a *lei de corte*. Assim:

TEOREMA 5: — *Se, num semi-grupo, as equações* x a = b, a y = b *admitirem uma solução, quando muito, é válida no semi-grupo a lei de corte.* E também se tem

TEOREMA 6: — *Se, num semi-grupo finito, as equações* x a = b, a y = b *admitirem uma solução, quando muito, 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 $x\,a$ pertencem ao semi-grupo e são todos distintos. O número de elementos $x\,a$ é igual ao número de elementos x, pelo que a equação $x\,a = b$ é sempre solúvel. O mesmo se diz da equação $a\,y = b$.

No caso dos grupos finitos, podemos substituir o postulado 3′) por este outro 3‴): a lei de corte é válida, à direita e à esquerda. De facto, um conjunto com as propriedades 1′) e 2′) é um semi-grupo. Estamos, então, em presença dum semi-grupo finito, para o qual tem lugar a propriedade 3″), valendo, consequentemente, o teorema 6.

3) **A tabela do grupo finito** — A estrutura dum grupo finito fica completamente conhecida, logo que se tenha uma tabela na qual se possa encontrar o produto de dois quaisquer dos seus elementos. Consideremos, por ex., 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 dos dois elementos. Cada linha horizontal, como cada linha vertical, contém, dentro da tabela, todos os elementos do grupo e cada um deles uma só vez. O teorema 3 é traduzido na tabela de modo interessante, indicado no quadro que adiante se desenha. Por ele 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.

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, a observação seguinte: quaisquer que sejam as tabelas construídas, só a partir de 6 elementos se encontram grupos para os quais o produto não é comutativo ($ab \neq ba$).

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

4) **Exemplos. Grupos de transformações** – Um grupo $\mathfrak{G}$ diz-se *abeliano,* se, dados $a, b \in \mathfrak{G}$, for $ab = ba$. O grupo $\mathfrak{G} = \{-1, +1\}$, no qual o produto de dois elementos é o produto ordinário, é um grupo abeliano. O conjunto dos números racionais, excluído o zero, forma também um grupo abeliano, relativamente ao produto ordinário. É frequente, tratando-se de grupos abelianos, utilizar o sinal $+$ para significar o produto de dois elementos. Nesse caso, utilizaremos $\mathfrak{M}$, em vez de $\mathfrak{G}$, para representar o grupo, e diremos que $\mathfrak{M}$ é um *grupo abeliano aditivo* ou um *módulo*. Teremos, então,

$$a + b \in \mathfrak{M}, \qquad a + (b + c) = (a + b) + c,$$

para traduzirem os postulados 1′) e 2′). Quanto a 3′), só temos que escrever a equação $a + y = b$ e afirmar que ela é solúvel. A comutatividade da soma ficará expressa neste novo postulado 4′): $a + b = b + a$. Para harmonia da notação, convém utilizar o, em vez de u, e $(-a)$, em vez de a^{-1}. Assim, teremos: $a + o = a, a + (-a) = o$. Por simplicidade, escreveremos ainda $a - b$, em vez de $a + (-b)$.

O conjunto dos inteiros constitui um grupo abeliano, relativamente à soma como operação de produto. Se a operação de produto for a operação ordinária, o conjunto dos inteiros é um grupóide.

Tomemos um conjunto $\mathfrak{C}$, qualquer. Se, a cada $a \in \mathfrak{C}$ fizermos corresponder um elemento bem determinado $a' = \varphi(a) \in \mathfrak{C}$, diremos que se tem uma aplicação de $\mathfrak{C}$ *em* si. O elemento a' diz-se *imagem* de a. A função φ, acabada de definir, é *unívoca.* Ela diz-se *biunívoca,* se, tomado o conjunto $\mathfrak{C}' \subset \mathfrak{C}$ (leia-se $\mathfrak{C}'$ contido em $\mathfrak{C}$), formado pelas imagens a' dos elementos de $\mathfrak{C}$, cada a' é imagem dum único a. Por outras palavras: se for $a \neq b$, também $a' \neq b'$.

Pode dar-se o caso de ser $\mathfrak{C}' = \mathfrak{C}$. Diz-se, então, que φ é uma aplicação de $\mathfrak{C}$ *sobre* si. Esta última aplicação também pode ser unívoca ou biunívoca, tal como a anterior.

Uma aplicação biunívoca de $\mathfrak{C}$ sobre si chama-se uma *transformação* de $\mathfrak{C}$. Entre as transformações, há a *identidade,* que aplica cada elemento sobre si mesmo. A *transformação inversa* φ^{-1}, de φ, é definida pela igualdade $a = \varphi^{-1}(a')$, ou, melhor, $b = \varphi^{-1}(a)$, se for $a = \varphi(b)$.

Supondo φ e ψ duas transformações, definiremos *produto* $\psi\varphi$ como a transformação $a'' = \psi\varphi(a) = \psi(a')$. À transformação produto $\theta = \psi\varphi$ deve dar-se a forma $c = a'' = \theta(a)$.

Pelo que acabamos de ver, o símbolo $\psi\varphi$ deve entender-se como efectuando primeiramente φ, em seguida ψ. Se quisermos significar o contrário, devemos escrever

$$a' = (a)\psi, \qquad a'' = (a)\psi\varphi = (a')\varphi, \qquad c = a'' = (a)\theta.$$

O produto é associativo, pois que $\omega.\psi\varphi(a) = \omega(\psi(\varphi(a)))$, $\omega\psi.\varphi(a) = \omega(\psi(\varphi(a))) = \omega.\psi\varphi(a)$. Tem lugar este

TEOREMA 7: — *O conjunto das transformações dum conjunto* $\mathfrak{C}$ *forma um grupo.*

Se nos estendermos às aplicações de $\mathfrak{C}$ em si, obtém-se um conjunto que é um grupóide.

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

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

Estas transformações costumam designar-se por *permutações* de n elementos e o grupo que elas formam por *grupo simétrico de ordem* n. Representá-lo-emos pelo símbolo $\mathfrak{S}_n$.

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

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

vê-se que

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

Em geral, é $\psi\varphi \neq \varphi\psi$. O grupo simétrico, se $n \geqq 3$, não é abeliano.

A noção de transformação de $\mathfrak{C}$, quando este conjunto tem uma infinidade de elementos, pode conceber-se como uma extensão da ideia de permutação.

Outro exemplo importante de grupo de transformações é o que vamos tratar em seguida. Ele é fundamental em *Geometria no espaço*, designando-se ali por *grupo das rotações* à volta da origem das coordenadas.

Consideremos as equações

$$\begin{aligned} x_1 &= a\,x + b\,y + c\,z, \\ y_1 &= a'x + b'y + c'z, \\ z_1 &= a''x + b''y + c''z, \end{aligned} \tag{2}$$

onde os nove coeficientes $a, b, \ldots, a', \ldots$ verificam as relações

$$\begin{aligned} a^2 + b^2 + c^2 &= 1, & a\,a' + b\,b' + c\,c' &= 0, \\ a'^2 + b'^2 + c'^2 &= 1, & a\,a'' + b\,b'' + c\,c'' &= 0, \\ a''^2 + b''^2 + c''^2 &= 1, & a'\,a'' + b'\,b'' + c'\,c'' &= 0. \end{aligned} \tag{3}$$

Suporemos ainda que o determinante (1)

$$\Delta = \begin{vmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{vmatrix},$$

para o qual se tem

$$\Delta^2 = \begin{vmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{vmatrix} \cdot \begin{vmatrix} a & a' & a'' \\ b & b' & b'' \\ c & c' & c'' \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} = 1,$$

é igual à unidade. Então, mostraremos que o conjunto das transformações (2) é efectivamente um grupo. [Fala-se de transformações, pelo facto de haver correspondência biunívoca entre os sistemas de números x, y, z e os sistemas correspondentes x_1, y_1, z_1].

A transformação

$$x_1 = x, \qquad y_1 = y, \qquad z_1 = z,$$

como transformação idêntica, representará o elemento um do grupo. Para designarmos abreviadamente (3), utilizaremos o símbolo $A(a, b, \ldots, a', b', \ldots)$, no qual se põem em evidência, por uma ordem bem determinada, os coeficientes respectivos. Sendo $B(\alpha, \beta, \ldots, \alpha', \beta', \ldots)$ uma segunda transformação (2), vê-se que é $AB\ (r, s, t, r', s', \ldots)$ a transformação definida pelas relações

$$\begin{aligned} x_1 &= a\,(\alpha x + \beta y + \gamma z) + b\,(\alpha' x + \beta' y + \gamma' z) + \\ &\quad + c\,(\alpha'' x + \beta'' y + \gamma'' z), \\ y_1 &= a'\,(\alpha x + \beta y + \gamma z) + b'\,(\alpha' x + \beta' y + \gamma' z) + \end{aligned}$$

---

(1) Este exemplo pode ser deixado para mais tarde, depois de feita a teoria dos determinantes. Aqui apenas se exige, todavia, o conhecimento das operações com determinantes de 3.ª ordem.

$$+ c'(\alpha'' x + \beta'' y + \gamma'' z),$$
$$z_1 = a''(\alpha x + \beta y + \gamma z) + b''(\alpha' x + \beta' y + \gamma' z) +$$
$$+ c''(\alpha'' x + \beta'' x + \gamma'' z).$$

Tem-se

$$r = a\alpha + b\alpha' + c\alpha'', \qquad r' = a'\alpha + b'\alpha' + c'\alpha'',$$
$$s = a\beta + b\beta' + c\beta'', \qquad s' = a'\beta + b'\beta' + c'\beta'',$$
$$t = a\gamma + b\gamma' + c\gamma'', \qquad t' = a'\gamma + b'\gamma' + c'\gamma'',$$

$$r'' = a''\alpha + b''\alpha' + c''\alpha'',$$
$$s'' = a''\beta + b''\beta' + c''\beta'',$$
$$t'' = a''\gamma + b''\gamma' + c''\gamma''.$$

Os coeficientes $r, s, \ldots, r', s', \ldots$ verificam as relações impostas aos coeficientes $a, b, \ldots, a', b', \ldots$. Por isso, o produto de duas transformações é fechado. A transformação inversa de (2) é a seguinte:

$$\begin{aligned} x_1 &= (b'c'' - b''c')x + (b''c - bc'')y + (bc' - b'c)z, \\ y_1 &= (a''c' - a'c'')x + (ac'' - a''c)y + (a'c - ac')z, \\ z_1 &= (a'b'' - a''b')x + (a''b - ab'')y + (ab' - a'b)z. \end{aligned} \tag{4}$$

Ela escreve-se fàcilmente, atendendo à relação $\Delta = 1$ e resolvendo (2) em ordem a x, y, z, continuando, porém, a utilizar x_1, y_1, z_1 como variáveis dos primeiros membros e x, y, z como variáveis dos segundos. As condições (3) são satisfeitas, como vamos mostrar. Das referidas relações (3), as que têm segundos membros nulos dão fàcilmente as igualdades

$$\frac{a}{b'c'' - b''c'} = \frac{b}{a''c' - a'c''} = \frac{c}{a'b'' - a''b'},$$
$$\frac{a'}{b''c - bc''} = \frac{b'}{ac'' - a''c} = \frac{c'}{a''b - ab''},$$
$$\frac{a''}{bc' - b'c} = \frac{b''}{a'c - ac'} = \frac{c''}{ab' - a'b}.$$

Chamando ρ, ρ', ρ'', respectivamente, os valores comuns das fracções que figuram em cada uma das três linhas anteriores, tira-se, por ex.,

$$\begin{aligned} a &= \rho(b'c'' - b''c'), \\ b &= \rho(a''c' - a'c''), \qquad a^2 + b^2 + c^2 = \rho.\Delta = 1 = \rho. \\ c &= \rho(a'b'' - a''b'), \end{aligned}$$

Assim, tem-se $\rho = \rho' = \rho'' = 1$, podendo (4) escrever-se

$$\begin{aligned} x_1 &= ax + a'y + a''z, \\ y_1 &= bx + b'y + b''z, \\ z_1 &= cx + c'y + c''z. \end{aligned} \tag{4'}$$

Trata-se agora de ver que as igualdades (3) são equivalentes às seguintes:

$$\begin{aligned} a^2 + a'^2 + a''^2 &= 1, \qquad ab + a'b' + a''b'' = o, \\ b^2 + b'^2 + b''^2 &= 1, \qquad ac + a'c' + a''c'' = o, \\ c^2 + c'^2 + c''^2 &= 1, \qquad bc + b'c' + b''c'' = o. \end{aligned}$$

Se pusermos

$$\frac{a}{b'c'' - b''c'} = \frac{a'}{b''c - bc''} = \frac{a''}{bc' - b'c} = \frac{ab + a'b' + a''b''}{o},$$

vemos que é $ab + a'b' + a''b'' = o$. Se tivermos em conta a identidade

$$\begin{aligned} (a^2 + a'^2 + a''^2)(b^2 + b'^2 + b''^2) - (ab + a'b' + a''b'')^2 = \\ = (a'b'' - a''b')^2 + (a''b - ab'')^2 + (ab' - a'b)^2 = \\ = c^2 + c'^2 + c''^2, \end{aligned}$$

e, em seguida, a identidade análoga que leva a

$$(a^2 + a'^2 + a''^2)(c^2 + c'^2 + c''^2) = b^2 + b'^2 + b''^2,$$

tiramos, por produto desta com a anterior,

$$(a^2 + a'^2 + a'^2)^2 = 1, \quad \text{ou} \quad a^2 + a'^2 + a''^2 = 1,$$

pois se suporão reais os coeficientes de (2). As restantes igualdades provam-se de modo análogo. A condição $\Delta = 1$ é também verificada em (4'). Finalmente, pelo que respeita à propriedade associativa das transformações (2), não há necessidade de demonstração particular, para se reconhecer que tem lugar.

Como se afirmou, as igualdades (2) definem um grupo de transformações.

5) **A noção de isomorfismo e o teorema de Cayley** — Sejam $\mathfrak{G}$ um grupo e $\mathfrak{C}'$ um conjunto algebrizado com um produto. Se, dado $x \in \mathfrak{G}$, lhe corresponder um elemento determinado $x' \in \mathfrak{C}'$, de tal modo que todos os elementos de $\mathfrak{C}'$ sejam utilizados como imagem, e de tal modo ainda que, com $x \to x'$ (1), $y \to y'$, se tenha também $xy \to (xy)' = x'y'$, a correspondência $x \to x'$ diz-se um *homomorfismo*. Neste n.º interessa-nos o caso em que cada elemento x' é imagem dum único elemento x. A correspondência $x \to x'$ é, então, biunívoca, e chama-se um *isomorfismo*.

Mesmo no caso do homomorfismo, a imagem $\mathfrak{C}'$, de $\mathfrak{G}$, é um grupo $\mathfrak{G}'$. Adiante retomaremos este assunto. Aqui, observaremos apenas que o isomorfismo $\mathfrak{G} \simeq \mathfrak{C}'$, designado pelo símbolo $\simeq$, permite considerar dois grupos como *equivalentes*, sob o ponto de vista abstracto. Qualquer afirmação feita sobre os elementos não acentuados de $\mathfrak{G}$ pode repetir-se para os elementos acentuados de $\mathfrak{C}' = \mathfrak{G}'$. O teorema de CAYLEY é o seguinte:

TEOREMA 8: — *Qualquer grupo é isomorfo dum grupo de transformações (permutações).* Dado o grupo $\mathfrak{G}$, tomemos $a \in \mathfrak{G}$, fixo, e $x \in \mathfrak{G}$, arbitrário. A correspondência $x \to xa$ é uma permutação de $\mathfrak{G}$. Escreveremos $xa = xA_d$, de modo que a cada $a \in \mathfrak{G}$ se faz corresponder uma permutação A_d. Se for $a \neq b$ é $A_d \neq B_d$, como se verifica pondo $x = u$: $ua = a = uA_d$, $ub = b = uB_d \neq uA_d$. O produto ab define a permutação

$$x \to x.ab = (xa)b = (xA_d)B_d = x(A_dB_d).$$

Vê-se que ao produto ab corresponde o produto das permutações correspondentes, pelo que o teorema fica demonstrado.

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

Como caso particular, tem lugar o

COROLÁRIO 1: — *Todo o grupo finito com* n *elementos é isomorfo dum grupo de permutações pertencentes a* $\mathfrak{S}_n$.

Regressemos ao grupo $\mathfrak{G}$ e ao conjunto $\mathfrak{C}'$, assim como à correspondência $x \to x'$. Se tiver lugar a propriedade $xy \to (xy)' = y'x'$, a referida correspondência diz-se um *anti-homomorfismo*. No caso da biunivocidade, tem-se um *anti-isomorfismo* ou um *isomorfismo inverso*.

Tomemos $a \in \mathfrak{G}$ e a aplicação $x \to ax$, de $\mathfrak{G}$ sobre $\mathfrak{G}$. Escreveremos $ax = xA_e$. Então, é imediato que a correspondência $a \to A_e$ é um anti-isomorfismo. O conjunto dos A_e, tal como o dos A_d forma um grupo, dentro do grupo das transformações de $\mathfrak{G}$.

Representemos por $\mathfrak{G}_d$ e conjunto dos A_d, por $\mathfrak{G}_e$ o conjunto dos A_e e por $\tau(\mathfrak{G})$ o conjunto das transformações de $\mathfrak{G}$. Em virtude de se ter $xA_dB_e = (xA_d)B_e = (xa)B_e = b.xa = b\,x.a = (xB_e)A_d = xB_eA_d$, vê se que a transformação A_dB_e é a mesma que a transformação B_eA_d, precisamente pelo facto de as duas transformações levarem dum elemento $x \in \mathfrak{G}$ ao mesmo transformado $x' \in \mathfrak{G}$. A igualdade $A_dB_e = B_eA_d$ traduz-se dizendo que os elementos de $\mathfrak{G}_e$ fazem parte do *comutador* de $\mathfrak{G}_d$, dentro de $\tau(\mathfrak{G})$. Vamos ver, mais precisamente,

(1) Escrevendo-se $x \to x'$, significa-se que x' é a imagem de x.

que são *comutadores recíprocos,* isto é, por ex., que, dentro de $\tau(\mathfrak{G})$, qualquer transformação que comute com todas as transformações de $\mathfrak{G}_d$ pertence necessàriamente a $\mathfrak{G}_e$. Tomemos $\sigma \in \tau(\mathfrak{G})$ e suponhamos

$$x \to x\sigma; \qquad (x A_d)\sigma = (xa)\sigma = (x\sigma) A_d = (x\sigma)a.$$

Fazendo $x = u$, deverá ter-se

$$u \to u\sigma = b \in \mathfrak{G}, \quad (u A_d)\sigma = (ua)\sigma = a\sigma = (u\sigma)a = ba.$$

Assim, vê-se que

$$a \to a\sigma = ba = aB_e,$$

qualquer que seja $a \in \mathfrak{G}$. Por isso, tem-se $\sigma = B_e$, como se afirmou. Podemos fixar este

TEOREMA 9: — *Dado um grupo* $\mathfrak{G}$, *os grupos* $\mathfrak{G}_d$ *e* $\mathfrak{G}_e$, *contidos no grupo* $\tau(\mathfrak{G})$, *das transformações de* $\mathfrak{G}$, *são comutadores recíprocos dentro de* $\tau(\mathfrak{G})$.

6) **Regras de cálculo** — As regras de cálculo que vamos estudar dizem respeito a operações com mais de dois elementos. Por ex., o produto de três elementos a, b, c, dispostos pela ordem a, b, c, é, por definição, dado pela igualdade $abc = a\,b.c$. Neste caso particular, não poderia haver ambiguidade na interpretação do símbolo abc, pois que, a outra possível interpretação, como $a.bc$, levaria ao mesmo resultado.

Esta observação é geral, como vamos ver. Escrevamos, por definição, $a_1 a_2 \ldots a_n = a_1 \ldots a_{n-1}.a_n$. Se supusermos

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

provaremos, com efeito, que se tem

$$AB = a_1 a_2 \ldots a_p. \qquad (5)$$

Para $p = n+1$, ou seja $B = a_{n+1}$, tem-se $AB = a_1 \ldots a_n . a_{n+1} = a_1 \ldots a_{n+1} = a_1 \ldots a_p$. Admitamos que a igualdade (5) está provada para $p = n+k-1$. Demonstrá-la-emos para $p = n+k$. Ponhamos $B' = a_{n+1} \ldots a_{n+k-1}$. Tem-se $AB' = a_1 \ldots a_{n+k-1}$, por hipótese. Escrevamos, depois, $AB' . a_{n+k} = A . B' a_{n+k}$. Como $B' a_{n+k} = a_{n+1} \ldots a_{n+k-1} . a_{n+k} = a_{n+1} \ldots a_{n+k} = B$, vê-se que $AB' . a_{n+k} = AB$. Por outro lado, $AB' . a_{n+k} = a_1 \ldots a_{n+k-1} . a_{n+k} = a_1 \ldots a_{n+k}$; e, assim, $AB = a_1 \ldots a_{n+k}$, como se deseja.

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

$$a^m . a^n = a^{m+n}, \qquad (a^m)^n = a^{mn},$$

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

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

Vamos passar à potência nula e às potências de expoente negativo. Por definição, poremos $a^0 = u$. Quanto a a^{-n}, escreveremos, também por definição, $a^n . a^{-n} = u$. Vê-se que $a^{-n} = (a^n)^{-1}$. Mostraremos ainda que $a^{-n} = (a^{-1})^n$, servindo-nos novamente do método de indução. Temos $a^{-1} = (a^{-1})^1$, quando $n = 1$. Quando se toma $n+1$, vem $a^{n+1} . a^{-(n+1)} = u$, sendo também $a^{n+1} . (a^{-1})^{n+1} = a^1 a^n . (a^{-1})^n a^{-1} = a^1 . a^n (a^{-1})^n . a^{-1} = a^1 u a^{-1} = u$. Consequentemente, $(a^{-1})^{n+1}$ é igualmente inverso de a^{n+1}.

Para expoentes negativos, valem as igualdades

$$(a^n)^{-m} = a^{-nm}, \qquad a^n . a^{-m} = a^{n-m}.$$

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 for $n > m$, 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 $a^{-(m-n)} \cdot a^{-1} = (a^{-1})^{m-n+1} = a^{n-(m+1)}$, pelo que a afirmação fica efectivamente justificada. Claro que o caso $n=m$ leva a $a^n \cdot a^{-n} = a^{n-n} = a^0 = u$, não carecendo aqui de demonstração.

Passando aos grupos abelianos aditivos, há interesse em reproduzir as regras anteriores, utilizando as notações adequadas. Assim:

$$a_1 + \ldots + a_n = (a_1 + \ldots + a_{n-1}) + a_n; \qquad /-$$

de $A = a_1 + \ldots + a_n$, $B = a_{n+1} + \ldots + a_p$, $(p \geqq n+1)$, tira-se

$$A + B = a_1 + \ldots + a_p;$$

$na = a + \ldots + a$, onde a se repete n vezes;

$ma + na = (m+n)a$; $\quad n \cdot ma = mna$;

$Oa = o$ (o produto do número zero por um elemento do grupo dá o elemento nulo do grupo);

$na + (-n \cdot a) = o$; $\quad -n \cdot a = -na = n(-a)$;

$-m \cdot na = -nma$, $\quad na + (-ma) = (n-m)a$;

$-m \cdot (-na) = m(-(-na)) = mna$.

Aqui podemos juntar ainda a relação $n(a+b) = na + nb$.

Para terminarmos as regras de cálculo que temos em vista, vamos demonstrar que, no caso dos grupos abelianos, o produto é independente da ordem dos factores. Seja $i_1, i_2, \ldots, i_n$ uma nova disposição dos números $1, 2, \ldots, n$. Trata-se de provar que $a_1 \ldots a_n = a_{i_1} a_{i_2} \ldots a_{i_n}$. No caso de dois elementos, o teorema é imediato. Admitamos $i_k = n$. Se o teorema é verdadeiro para $n-1$ elementos, prová-lo-emos para n factores. Tem-se

$a_{i_1} a_{i_2} \ldots a_{i_{k-1}} \cdot a_{i_k} \cdot a_{i_{k+1}} \ldots a_{i_n} = a_{i_1} \ldots a_{i_{k-1}} \cdot a_n \cdot a_{i_{k+1}} \ldots$
$\ldots a_{i_n} = a_{i_1} \ldots a_{i_{k-1}} \cdot a_{i_{k+1}} \ldots a_{i_n} \cdot a_n = a_1 \ldots a_{n-1} \cdot a_n =$
$= a_1 \ldots a_n$. Passa-se da antepenúltima para a penúltima expressão pela hipótese da indução relativa a $n-1$.

§ 2 — Subgrupos, grupos cíclicos, complexos associados dum subgrupo

1) **Critério de subgrupo** — 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 três postulados 1'), 2') e 3'), do § 1. O postulado da associatividade é aqui uma consequência necessária, logo que tenha lugar 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 $xa = b$, $ay = b$ são solúveis em $\mathfrak{g}$. Como a solução de $xa = b$ é ba^{-1}, vamos provar o seguinte

TEOREMA 10: — *E 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 2) 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 3). Como o postulado 4) tem lugar, se tiver lugar o postulado 1), é este 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 $a^{-1}b \in \mathfrak{g}$].

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. O próprio grupo se pode considerar um subgrupo impróprio do grupo.

Um grupo é também semi-grupo. Se $\mathfrak{h}$ for um *sub-semi-grupo,* ou seja um semi-grupo contido no grupo, a hipótese de $\mathfrak{h}$ ser

finito implica que seja subgrupo. De facto, a propriedade 3'') é válida e o teorema 6 é aplicável.

2) **Subgrupo gerado por um conjunto de elementos** — Consideremos um conjunto de elementos $a, b, c, \ldots \in \mathfrak{G}$, conjunto que pode ser finito ou infinito. Diz-se *subgrupo gerado* por estes elementos o mais pequeno subgrupo que os contém.

Qualquer subgrupo que contém os elementos contém necessàriamente todos os elementos da forma

$$a^r \ldots b^s \ldots c^t \ldots a^{-r'} \ldots b^{-s'} \ldots c^{-t'} \ldots, \qquad (6)$$

em cada um dos quais o número de factores é finito. Vamos verificar que a totalidade dos elementos do tipo (6) constitui um subgrupo, ao qual pertencem a, b, c, ... Será, por isso, o subgrupo procurado. Claramente que a, b, c, ... entram no tipo (6), acontecendo o mesmo ao elemento um. O inverso dum elemento da forma (6) tem a forma (6) e o produto de dois elementos da forma (6) é ainda dessa forma. O critério de subgrupo é aplicável e a afirmação fica demonstrada.

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

$$\mathfrak{Z} = \{\ldots, a^{-r}, \ldots, u, a, \ldots, a^n, \ldots\}.$$

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 ex., 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 $a^{h-k} = a^k \cdot a^{-k} = u$. Conclúi-se, assim, que há potências de expoente $h - k > 0$ tais que $a^{h-k} = u$. Designemos por m o mais pequeno expoente tal que $a^m = u$. Mostraremos que o grupo cíclico se compõe dos m elementos seguintes:

$$\mathfrak{Z} = \{u, a, a^2, \ldots, a^{m-1}\}. \qquad (7)$$

Para isso, teremos de provar os dois factos seguintes: 1) que as potências de a, figurando em (7), são todas diferentes; 2) que qualquer outra potência de a é igual a uma daquelas. Se houvesse em (7) 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 (7) são, pois, todos distintos. Seja agora uma potência a^s, com $s \neq 0, 1, \ldots, m-1$. Podemos escrever sempre $s = mq + r$, onde $0 \leqq r < m$. 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 (7), como se afirmou.

Esclareçamos a igualdade $s = mq + r$. Se fosse $s = -1$, por ex., escreveríamos $-1 = m(-1) + (m-1)$; para $s = -2$, teríamos $-2 = m(-1) + (m-2)$, etc.. A divisão indicada tem, assim, sempre lugar, com $0 \leqq r < m$.

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

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 um grupo cíclico $\mathfrak{Z} = \{\ldots, a^{-n}, \ldots, a^0 = u, a, \ldots, a^n, \ldots\}$. Um subgrupo será da forma $\mathfrak{g} = \{\ldots, a^{-t}, \ldots, a^{-v}, \ldots, u, \ldots, a^{v'}, \ldots, a^{t'} \ldots\}$. Vamos provar o seguinte

TEOREMA 11: — *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 potência de expoente positivo, também pertencente a $\mathfrak{g}$, pondo $v' = cp + r$, com $0 \leqq r < p$, tem-se $a^{v'} = a^{cp+r} = (a^p)^c . a^r$. Se $r = 0$, $a^{v'}$ é uma potência 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 $a^{kp-n} = a^{kp} . a^{-n} = a^{kp}$, o subgrupo conteria o elemento $a^{kp} = a^{kp-n}$, no qual o expoente de a seria inferior a p, contra a hipótese.

Vê-se, como consequência, que a potência a^p, de menor expoente, do subgrupo cíclico finito, não pode ser tal que p seja primo com n, ordem do grupo, a não ser que o subgrupo seja impróprio. Se q, pelo contrário, for primo com n, o subgrupo cíclico gerado por a^q, que está contido no grupo, não podendo ser subgrupo próprio, será igual ao grupo. Deste modo, é válido este enunciado:

TEOREMA 12: — *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 2: — *A equação* $b^x = a^r$, *na incógnita* x, *é sempre solúvel.*

As considerações feitas levam a este outro

TEOREMA 13: — *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 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 supor* $\mathfrak{Z}$ *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.*

4) **Outras propriedades dos grupos cíclicos** — Consideremos 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 14: — *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, pois $a^{tm} = \gamma^m = u$, não podendo ter-se, com $m' < m$, $\gamma^{m'} = u$, visto que isso acarretaria $a^{tm'} = u$, com $tm' < tm$. Do mesmo modo se verifica ser a ordem de β igual a t. Feito isto, tomemos os produtos da forma $\beta^r \gamma^s$, com $(r = 1, 2, \ldots, \ldots, t;\ s = 1, 2, \ldots, m)$. 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 $\{\beta^0 = u, \beta, \ldots, \beta^{t-1}\}$, $\{\gamma^0 = u, \gamma, \ldots, \gamma^{m-1}\}$. 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 $r_1 \leqq t$, $s_1 \leqq m$ 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 $2tm$, vê-se que é $mr_1 + ts_1 = tm + 1$, 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, $a = bc$. Ora as ordens de b e c são, respectivamente, t e m. Se, com efeito,

a ordem de b, por ex., pudesse ser $t' < t$, ter-se-ia $(b\,c)^{t'm} = a^{t'm} = b^{t'm} . c^{t'm} = c^{t'm} = a^{t\,s_1 t'm} = u$, e a ordem do grupo (ordem de a) seria inferior a $t\,m$, contra a hipótese.

Vê-se, finalmente, que não pode haver duas potências a^p e a^q, diferentes das anteriores potências $a^{m\,r_1}$ e $a^{t\,s_1}$, das ordens t e m, respectivamente, e tais que $a^{p+q} = a$, raciocinando do modo seguinte: se fosse $a = a^p . a^q = a^{p+q} = a^{m\,r_1 + t\,s_1}$, com $a^{p\,t} = u$, $a^{q\,m} = u$, ter-se-ia $a^{p+q-(m\,r_1 + t\,s_1)} = u$, com $p + q = m\,r_1 + t\,s_1$. De facto, como a soma $p + q$ não chega a ser $2\,t\,m$ e como $m\,r_1 + t\,s_1 = t\,m + 1$, não há outra possibilidade. Por outro lado, é $p\,t = k\,t\,m$, $q\,m = k'\,t\,m$, com certos inteiros k e k'. Então, vem $p = k\,m$, $q = k'\,t$, e $k\,m + k'\,t = m\,r_1 + t\,s_1$, ou $m(k - r_1) = t(s_1 - k')$. Desta relação conclui-se $s_1 - k' = a\,m$, $k - r_1 = a\,t$, e, portanto,

$$a^p = a^{k\,m} = a^{r_1 m + a\,t\,m} = a^{r_1 m},$$
$$a^q = a^{k'\,t} = a^{s_1\,t - a\,m\,t} = a^{s_1 t},$$

como se queria demonstrar.

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

5) **Sobre o uso de certos sinais de equivalência** — Imaginemos um conjunto e uma operação de comparação dos seus elementos, que representaremos pelo símbolo $\lesssim$. Suponhamos que esta operação goza das propriedades seguintes: 1) $a \lesssim a$, (propriedade *reflexiva*); 2) se $a \lesssim b$, também $b \lesssim a$, (propriedade *simétrica*); 3) se $a \lesssim b$ e $b \lesssim c$, então $a \lesssim c$, (propriedade *transitiva*). A referida operação diz-se, em tal caso, uma *relação de equivalência*.

Obtém-se, por ex., uma relação de equivalência, considerando como equivalentes os triângulos semelhantes dum plano.

É válido o seguinte

TEOREMA 15: — *Se, num conjunto* $\mathfrak{C}$, *tivermos uma relação de equivalência, podemos dividir o conjunto em classes de elementos equivalentes, verificando as duas propriedades I e II, a saber:* I) *um elemento do conjunto pertence a uma das classes;* II) *duas classes não têm elemento comum.* [Neste enunciado, como no exemplo referido, dois elementos tais que $a \lesssim b$ dizem-se *equivalentes*]. Demonstremos o teorema. Visto que $a \lesssim a$, 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 a for equivalente a b, $(b \lesssim a)$, então $a \in C_b$. Dado outro elemento $d \in C_a$, das relações $a \lesssim d$, $b \lesssim a$, concluímos $b \lesssim d$, ou seja $d \in C_b$. A classe C_a estará contida em C_b, e esta estará contida naquela. As duas classes não são distintas. O teorema fica provado.

6) **Complexos associados dum subgrupo** — Sejam $\mathbf{G}$ (1) um grupo e $\mathfrak{g}$ um subgrupo. É fácil de demonstrar que a seguinte relação é uma relação de equivalência: $a \lesssim b$, se for $b \in a\,\mathfrak{g}$.

Demonstremos, por ex., a propriedade simétrica. Admitamos que se tem $a \lesssim b$; precisamos provar que é $b \lesssim a$, ou seja que $a \in b\,\mathfrak{g}$. Na verdade, supondo $b = a\,g$, com $g \in \mathfrak{g}$, é também $a = b\,g^{-1}$, com $g^{-1} \in \mathfrak{g}$.

A referida relação de equivalência permite dividir o grupo $\mathbf{G}$ em classes de equivalentes, isto é, permite que se escreva

$$\mathbf{G} = \{\mathfrak{g}, a\,\mathfrak{g}, b\,\mathfrak{g}, \ldots\}.$$

---

(1) Dificuldades técnicas obrigam-nos a substituir, por vezes, as letras góticas, por letras latinas correspondentes, de tipo diferente do que é utilizado no texto. Assim: G ou $\mathfrak{G}$, C ou $\mathfrak{C}$, H ou $\mathfrak{H}$, etc., têm neste livro o mesmo significado.

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

Se o grupo 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 G sob a forma

$$G = \{\mathfrak{g}, \mathfrak{g}a, \mathfrak{g}b, \dots\}.$$

É evidente que, no geral, as classes direitas são distintas das classes esquerdas com o mesmo representante: $\mathfrak{g}a \neq a\mathfrak{g}$. É fácil, porém, passar dumas a outras. Por ex.: $(a\mathfrak{g})^{-1} = \mathfrak{g}^{-1}a^{-1} = \mathfrak{g}a^{-1}$, pois $\mathfrak{g}^{-1} = \mathfrak{g}$. Significa isto que, de cada classe esquerda, se obtém, pelo processo indicado, uma e uma só classe direita. E as classes esquerdas distintas correspondem classes direitas distintas, pois que, inversamente, se passa das direitas para as esquerdas.

Dividido G em classes esquerdas, por ex., cada classe contém, como sabemos, os diferentes elementos do grupo que são equivalentes a qualquer elemento da classe. Supondo $a \leqslant b$, é indiferente tomar a ou b como representante da classe. Como critério de equivalência de a e b podemos tomar a condição $a^{-1}b \in \mathfrak{g}$. Para a divisão em classes direitas, a relação $a \leqslant b$ exprime-se pondo $ba^{-1} \in \mathfrak{g}$.

Também se escreve $b \equiv a \pmod{\mathfrak{g}}_e$, sob a forma de *congruência,* para significar que b é equivalente a a, numa decomposição em classes esquerdas associadas de $\mathfrak{g}$. Significado análogo tem a congruência $b \equiv a \pmod{\mathfrak{g}}_d$, relativa a classes direitas.

No caso dos grupos finitos, o número de classes 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 16: — *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 3: — *Nos grupos finitos, a ordem dum subgrupo é um divisor da ordem do grupo.* Em particular:

COROLÁRIO 4: — *Nos grupos finitos, a ordem de qualquer elemento é um divisor da ordem do grupo.*

Em correlação com os raciocínios anteriores, provaremos ainda um certo número de proposições.

TEOREMA 17: — *Se* a *e* b *são dois elementos comutáveis dum grupo* 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 da ordem de ab. Se essa ordem pudesse ser $h < pq$, ter-se-ia $a^h . b^h = u$ 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. Vamos provar a seguinte proposição:

TEOREMA 18: — *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 4, teorema 14, satisfazem ao enunciado. Provaremos mais este

ADITAMENTO AO TEOREMA 18: — *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 t 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.

Duma maneira geral, num grupo qualquer, um elemento a de ordem $N = p_1^{r_1} p_2^{r_2} \dots p_s^{r_s}$ é sempre o produto de s elementos comutáveis que são potências de a e cujas ordens são, respectivamente, $p_1^{r_1}, \dots, p_s^{r_s}$.

§ 3 — Divisores normais, homomorfismos, grupo factor, teorema da homomorfia

1) **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 $a \in \mathfrak{G}$, for $a\,\mathfrak{g} = \mathfrak{g}\,a$. 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 ex., 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 pertencerá 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 $\mathfrak{G}$.

Regressemos a $\mathfrak{G}$ e a um subgrupo qualquer $\mathfrak{g}$. Consideremos a congruência $x \equiv y \pmod{\mathfrak{g}}_e$ e procuremos uma condição necessária e suficiente a que deva satisfazer $\mathfrak{g}$, a fim de que, supondo $x \equiv y \pmod{\mathfrak{g}}_e$, $x' \equiv y' \pmod{\mathfrak{g}}_e$, se tenha também $xx' \equiv yy' \pmod{\mathfrak{g}}_e$. Das condições $y \in x\,\mathfrak{g}, y' \in x'\,\mathfrak{g}$ deverá resultar $yy' \in (xx')\,\mathfrak{g}$, ou seja $(x\,\mathfrak{g})(x'\,\mathfrak{g}) \subseteq (xx')\,\mathfrak{g}$ (1), 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 àquela. Assim, uma condição necessária e suficiente, para que $\mathfrak{g}$ permita o produto de congruências indicado, é a seguinte:

$$\mathfrak{g}\,x' \subseteq x'\,\mathfrak{g}, \qquad (x' \in \mathfrak{G}). \tag{8}$$

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 (8). Podemos enunciar o

TEOREMA 19: — *É condição necessária e suficiente, para que $\mathfrak{H}$ seja um invariante, que se tenha, quaisquer que sejam $\mathfrak{x}, \mathfrak{x}' \in \mathfrak{G}$, $(\mathfrak{x}\,\mathfrak{H})(\mathfrak{x}'\,\mathfrak{H}) \subseteq (\mathfrak{x}\,\mathfrak{x}')\,\mathfrak{H}$. Mais precisamente: que se tenha $(\mathfrak{x}\,\mathfrak{H})(\mathfrak{x}'\,\mathfrak{H}) = (\mathfrak{x}\,\mathfrak{x}')\,\mathfrak{H}$.* 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.

2) **Homomorfismos e isomorfismos** — No § 1, n.º 5, referimo-nos já a estas duas noções. Dum modo geral, sejam $\mathfrak{A}$ e $\mathfrak{A}'$ dois conjuntos algebrizados com uma noção de produto *(espaços algébricos).* Se, dado $a \in \mathfrak{A}$, lhe fizermos corresponder $a' \in \mathfrak{A}'$, de modo unívoco, de tal sorte que, sendo também $b \to b'$, se tenha $ab \to (ab)' = a'b'$, a correspondência definida diz-se uma *homomorfia.* Uma homomorfia chama-se um *homomorfismo,* quando todo o espaço algébrico $\mathfrak{A}'$ é utilizado como imagem.

(1) O sinal $\subseteq$ significa inclusão, ou seja, «contido em».

Utilizaremos o simbolismo $\mathfrak{A} \sim \mathfrak{A}'$, para significar que os dois espaços se correspondem por homomorfismo.

Quando há correspondência biunívoca numa homomorfia, tem-se uma *isomorfia*. Já dissemos anteriormente que um homomorfismo com biunivocidade se diz um *isomorfismo*. Também indicámos o simbolismo $\mathfrak{A} \simeq \mathfrak{A}'$ para significar isomorfismo.

Supondo $\mathfrak{A}'$ e $\mathfrak{A}$ um mesmo espaço, uma homomorfia chama-se um *endomorfismo*.

Fizemos já esta afirmação:

TEOREMA 20: — *Considerado o homomorfismo* $\mathfrak{G} \sim \mathfrak{G}'$, *se* $\mathfrak{G}$ *é grupo,* $\mathfrak{G}'$ *é grupo.* Demonstremos, por ex., a solubilidade da equação $a'x' = b'$. Se a e b tiverem a' e b', respectivamente, como correspondentes, a equação $ax = b$ é solúvel, por hipótese. Chamando x' o correspondente de x, vê-se que $(ax)' = b' = a'x'$, como se deseja.

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

COROLÁRIO 5: — *Se* η *é um endomorfismo de* $\mathfrak{G}$, *então* $\mathfrak{G}\eta$ *é um subgrupo de* $\mathfrak{G}$.

Um endomorfismo dum espaço algébrico $\mathfrak{A}$ aplica $\mathfrak{A}$ numa parte $\overline{\mathfrak{A}}$, de $\mathfrak{A}$. A aplicação $\mathfrak{A} \to \overline{\mathfrak{A}}$ é um homomorfismo. Se este homomorfismo for um isomorfismo, diz-se um *meromorfismo*. Quando $\overline{\mathfrak{A}} = \mathfrak{A}$, o meromorfismo designa-se por *automorfismo*.

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

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

TEOREMA 21: — *Se um grupo* $\mathfrak{G}$ *possui um meromorfismo autêntico* $\mathfrak{G} \simeq \mathfrak{G}\sigma$, *o grupo admite a sucessão infinita de subgrupos* $\mathfrak{G} \supset \mathfrak{G}\sigma \supset \mathfrak{G}\sigma^2 \supset \ldots$, *sem sinal* $=$ *entre quaisquer termos da mesma sucessão.* 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 6: — *Num grupo finito não pode haver um meromorfismo autêntico.*

3) **Automorfismos dum grupo. Elementos conjugados** — Os automorfismos dum espaço algébrico $\mathfrak{A}$ 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, por serem realizadas as três condições seguintes: I) todo o elemento de $\mathfrak{G}$ é uma imagem; II) se $x \neq y$, é $x' \neq y'$; III) tem-se $xy \to (xy)' = x'y'$. Para se obter $axa^{-1} = d$, basta pôr $x = a^{-1}da$. Supondo $x \neq y$, se pudesse ser $axa^{-1} = aya^{-1}$, deduzíamos imediatamente $x = y$, contra a hipótese. Finalmente, tomemos xy. O seu correspondente é $a(xy)a^{-1} = axa^{-1}.aya^{-1} = x'y'$. As condições I) a III) são efectivamente realizadas.

Estes automorfismos dizem-se *internos*. É válido o seguinte

TEOREMA 22: — *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

$y^{-1}.yay^{-1}.y=a$. Agora conclui-se $aY^{-1}X=(aY^{-1})X=$ $=(y^{-1}ay)X=x.y^{-1}ay.x^{-1}=xy^{-1}.a.(xy^{-1})^{-1}$, 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 23: — *O subgrupo* $J_{\mathfrak{G}}$, *de* $A_{\mathfrak{G}}$, *é um invariante.* Conforme as considerações feitas no § 3, n.º 1, 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 $a\Theta X\Theta^{-1}=(x(a\Theta)x^{-1})\Theta^{-1}=x\Theta^{-1}.$ $.a\Theta\Theta^{-1}.x^{-1}\Theta^{-1}$. Claramente que é $x^{-1}\Theta^{-1}=(x\Theta^{-1})^{-1}$. Assim, $a\Theta X\Theta^{-1}=(x\Theta^{-1})a(x\Theta^{-1})^{-1}$, e a proposição fica estabelecida.

Se $a\in\mathfrak{G}$ for um elemento fixo, chamam-se conjugados de a todos os elementos da forma xax^{-1}, em que x percorre $\mathfrak{G}$. Definamos, dentro de $\mathfrak{G}$, a seguinte relação, que é, como pode verificar-se, uma relação de equivalência: $a\backsim b$, se b for conjugado de a. Por meio dela, divide-se o grupo em classes de equivalentes, que aqui são classes de elementos conjugados. É válido este

TEOREMA 24: — *Os elementos da mesma classe 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 $(yay^{-1})^n=$ $=yay^{-1}.yay^{-1}\ldots yay^{-1}=ya^ny^{-1}=yuy^{-1}=u$. Se pudesse ser $(yay^{-1})^m=u$, viria $ya^my^{-1}=u$, ou $a^m=u$, o que não tem lugar.

A caracterização dum invariante pela condição $y'\mathfrak{H}y'^{-1}\subseteq\mathfrak{H}$ 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.*

4) **Algumas propriedades dos subgrupos 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 todavia lugar a seguinte proposição:

TEOREMA 25: — *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 $\mathfrak{h}\mathfrak{g}=\mathfrak{g}\mathfrak{h}$ é 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 $a\mathfrak{P}a^{-1}=$ $=a\mathfrak{H}\mathfrak{H}'a^{-1}=a\mathfrak{H}a^{-1}.a\mathfrak{H}'a^{-1}\subseteq\mathfrak{H}\mathfrak{H}'=\mathfrak{P}$, 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. [O símbolo $\cap$, que deve ler-se *intersecção,* colocado entre dois conjuntos $\mathfrak{C}$ e $\mathfrak{C}'$, leva a $\mathfrak{C}\cap\mathfrak{C}'$, a interpretar como o conjunto dos elementos que pertencem simultâneamente a $\mathfrak{C}$ e a $\mathfrak{C}'$]. Tendo-se $a\mathfrak{D}a^{-1}\subseteq a\mathrm{H}a^{-1}\subseteq\mathrm{H}$, e, anàlogamente, $a\mathfrak{D}a^{-1}\subseteq a\mathrm{H}'a^{-1}\subseteq\mathrm{H}'$, vê-se que $a\mathfrak{D}a^{-1}\subseteq$ $\subseteq\mathrm{H}\cap\mathrm{H}'=\mathfrak{D}$, o que justifica a afirmação.

Provaremos agora este

TEOREMA 26: — *Se* $\mathfrak{g}$ *é um subgrupo e* H *um invariante, a intersecção* $\mathfrak{g}\cap\mathrm{H}$ *é um invariante em* $\mathfrak{g}$. Temos de estabelecer a relação de inclusão $a(\mathfrak{g}\cap\mathrm{H})a^{-1}\subseteq\mathfrak{g}\cap\mathrm{H}$, $(a\in\mathfrak{g})$. Se observarmos que $a\mathfrak{g}a^{-1}\subseteq\mathfrak{g}$, $a(\mathfrak{g}\cap\mathrm{H})a^{-1}\subseteq\mathfrak{g}$, $a\mathrm{H}a^{-1}\subseteq\mathrm{H}$, $a(\mathfrak{g}\cap$

$\cap \mathrm{H})\, a^{-1} \subseteq \mathrm{H}$, concluímos, como se deseja, $a\,(\mathfrak{g} \cap \mathrm{H})\, a^{-1} \subseteq \subseteq \mathfrak{g} \cap \mathrm{H}$.

Como última afirmação deste número, temos o seguinte

TEOREMA 27: — *Se dois invariantes* H *e* 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, começamos por definir o *comutador* de dois elementos. Dados $a, b \in \mathrm{G}$, o seu comutador é o elemento $(a\,b)\,(b\,a)^{-1} = a\,b\,a^{-1}\,b^{-1}$. Feito isto, seja $a \in \mathrm{H}$ e $a' \in \mathrm{H}'$. O comutador $(a\,a')\,(a'\,a)^{-1} = a\,a'\,a^{-1}\,a'^{-1}$ pode escrever-se de duas maneiras diferentes: sob a forma $a\,a'\,a^{-1}.a'^{-1}$, vê-se que pertence a H', por ser o produto de dois elementos de H'; sob a forma $a.a'\,a^{-1}\,a'^{-1}$, vê-se que pertence a H, por ser o produto de dois elementos de H. Será, assim, $a\,a'\,(a'\,a)^{-1} = u$, ou seja $a\,a' = a'\,a$. Os elementos a e a' comutam, como se afirmou.

5) **O grupo factor** — Vimos, no final n.º 1 deste §, 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 $a\,b\,\mathfrak{g}$), que $\mathfrak{g}$ fosse um invariante.

Quando $\mathfrak{g}$ é um invariante, há, assim, um preceito de multiplicação no conjunto

$$\{\mathfrak{g}, a\,\mathfrak{g}, b\,\mathfrak{g}, \ldots\}. \qquad (9)$$

À face desse preceito, 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 G.

O grupo (9) diz-se *grupo factor,* ou *grupo cociente,* de G segundo $\mathfrak{g}$. Substituindo $\mathfrak{g}$ por H, representaremos o grupo cociente por G/H.

Existe um homomorfismo $\mathrm{G} \sim \mathrm{G}/\mathrm{H}$, fazendo corresponder a cada elemento de G a classe a que o elemento pertence.

Claramente que, sendo H um invariante, o grupo (9) pode também escrever-se

$$\{\mathrm{H}, \mathrm{H}\,a, \mathrm{H}\,b, \ldots\}, \qquad (\mathrm{H} = \mathfrak{g}).$$

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 G que esse subgrupo contém, forma um subgrupo de G, que tem em G o mesmo índice que o subgrupo do grupo cociente tem neste último.

Sejam N o número de elementos de G e n a ordem de H. Então, $N/n = r$ é o índice de H em G, e também a ordem do grupo cociente G/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 G que aquele subgrupo contém é sn, de modo que o índice do subgrupo de 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 G pode fazer-se assim: sejam a e b dois elementos individualizados, pertencentes, respectivamente, às classes $a\,\mathrm{H}$ e $b\,\mathrm{H}$, as quais fazem parte do subgrupo do grupo cociente. Nesse caso, também $b^{-1}\,\mathrm{H}$ pertence a esse subgrupo, o mesmo se dizendo de $a\,\mathrm{H}\,.\,b^{-1}\,\mathrm{H} = a\,b^{-1}\,\mathrm{H}$, o que mostra ser $a\,b^{-1}$ um elemento individualizado. O critério de subgrupo é válido e a demonstração está feita.

Também, sob a hipótese dum grupo finito, tem lugar o interessante resultado seguinte: *dado um grupo finito* G, *se* s *é o expoente mínimo do elemento* $\mathrm{a} \in \mathrm{G}$ *tal que* a^{s} *figura num divisor* normal H, *então* s *é divisor da ordem do grupo cociente* G/H. Consideremos, com efeito, o seguinte conjunto de elementos de G/H: $\mathfrak{C} = \{\mathrm{H}, \mathrm{H}\,a, \ldots, \mathrm{H}\,a^{s-1}\}$. Os diferentes elementos são distintos, pois que $\mathrm{H}\,a^h = \mathrm{H}\,a^k$, com $h \neq k$, levaria a $\mathrm{H}\,a^{k-h} = \mathrm{H}$, com $s > k - h > 0$ (suposto $k > h$), donde se concluiria ser $a^{k-h} \in \mathrm{H}$, 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 G/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: $a'-a\in\mathfrak{N}$. Esta condição pode escrever-se $a'\equiv a \pmod{\mathfrak{N}}$ ou, mais simplesmente, $a'\equiv a\,(\mathfrak{N})$.

Se, por ex., J é o grupo cíclico dos números inteiros, o subgrupo (m), gerado por um número positivo qualquer m, leva ao grupo diferença $J-(m)$, cujos elementos, em número de m, são (m), $1+(m)$, ..., $m-1+(m)$. Dois números inteiros a e b são *côngruos módulo* (m), se a sua diferença for um múltiplo de m, o que se designará simplesmente por $a\equiv b\,(m)$.

O grupo diferença é aqui não apenas abeliano, mas também cíclico. Todos os seus elementos são gerados por $1+(m)$. E pode afirmar-se que todo o grupo cíclico de ordem m é isomorfo do grupo diferença $J-(m)$.

6) **O teorema da homomorfia** — Vamos demonstrar o teorema a seguir, conhecido sob o nome de *teorema da homomorfia:*

TEOREMA 28: — *Se* G *é um grupo e* $\mathrm{G}/\mathrm{H}=\overline{\mathrm{G}}$ *é um grupo cociente, tem lugar o homomorfismo* $\mathrm{G}\sim\overline{\mathrm{G}}=\mathrm{G}/\mathrm{H}$; *recìprocamente, se* $\mathrm{G}\sim\overline{\mathrm{G}}$, *então* $\overline{\mathrm{G}}$, *a menos de isomorfismo, é um grupo cociente.* A 2.ª parte do teorema significa que $\overline{\mathrm{G}}$ é isomorfo dum certo grupo factor: $\overline{\mathrm{G}}\simeq\mathrm{G}/\mathrm{H}$.

A 1.ª parte do teorema foi demonstrada no número anterior. Seja agora $\overline{\mathrm{G}}$ uma imagem homomorfa de G e tomemos o elemento um $=\bar{u}\in\overline{\mathrm{G}}$. Consideremos o conjunto de elementos

$$u, a, b, \ldots \in \mathrm{G} \to \bar{u}, \tag{10}$$

isto é, aqueles elementos de G que têm o elemento um de $\overline{\mathrm{G}}$ como correspondente. Vamos ver que o conjunto (10) forma um subgrupo invariante. Se $a\to\bar{u}$, $b\to\bar{u}$, também $a^{-1}\to\bar{u}$ e

$ba^{-1}\to\bar{u}$. Em (10), com a e b, encontramos ba^{-1}. Resta provar o carácter de invariante do subgrupo (10), a que chamaremos H. Tomemos $x\mathrm{H}$, $(x\in\mathrm{G})$. Os elementos de $x\mathrm{H}$ têm todos o mesmo correspondente $\bar{x}\in\overline{\mathrm{G}}$. Inversamente, se um elemento $y\in\mathrm{G}$ tem $\bar{x}$ como correspondente, como x^{-1} tem $\bar{x}^{-1}$ como correspondente, o elemento $x^{-1}y$, de correspondente $\bar{u}$, pertencerá a H. Da relação $x^{-1}y\in\mathrm{H}$, deduz-se $y\in x\mathrm{H}$. Deste modo $x\mathrm{H}$ representa a totalidade dos elementos de G que têm $\bar{x}$ como correspondente. Demonstra-se anàlogamente que essa totalidade é $\mathrm{H}x$, de sorte que $x\mathrm{H}=\mathrm{H}x$, qualquer que seja $x\in\mathrm{G}$. H é, efectivamente, um invariante.

Verifica-se, deste modo, que a cada classe de G/H corresponde um elemento bem determinado de $\overline{\mathrm{G}}$. 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 isomorfismo. Ora tomemos duas classes distintas $x\mathrm{H}$ e $y\mathrm{H}$. Não pode ter-se $\bar{x}=\bar{y}$, pois que, de contrário, seria $x^{-1}y\to\bar{u}$ e isto acarretaria $x^{-1}y\in\mathrm{H}$, ou seja a igualdades das classes, contra a hipótese. A afirmação relativa ao produto é imediata. O teorema da homomorfia está demonstrado.

7) **Algumas aplicações** — Dado o grupo G, tomemos $a\in\mathrm{G}$. O conjunto dos elementos de 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 $(a)=\mathfrak{h}$, gerado por a. Para cada $x\in\mathfrak{g}$ é $x\mathfrak{h}=\mathfrak{h}x$, pelo que:

TEOREMA 29: — *O grupo cíclico gerado por* a *é subgrupo invariante do normalizador de* a.

Sejam agora os complexos associados de $\mathfrak{g}$ em G. Pode utilizar-se a forma de escrita

$$\mathrm{G}=\mathfrak{g}\cup b_1\mathfrak{g}\cup b_2\mathfrak{g}\cup\ldots, \tag{11}$$

em substituição de outra já utilizada no § 2, n.º 6, para significar que $\mathbf{G}$ é o conjunto das classes associadas de $\mathfrak{g}$ que são diferentes e se imaginam de representantes $u, b_1, b_2, \ldots$.

Façamos uma observação. Na teoria dos conjuntos, o símbolo $\cup$, que deve ler-se *união,* colocado entre dois ou vários conjuntos $\mathfrak{C}$, $\mathfrak{C}'$, $\mathfrak{C}''$, ... leva a $\mathfrak{C} \cup \mathfrak{C}' \cup \mathfrak{C}'' \cup \ldots$, a interpretar como o conjunto dos elementos que pertencem, pelo menos, a um dos conjuntos. Em (11), excepcionalmente, os diferentes conjuntos da união não têm elementos comuns (ou são *disjuntos*).

Posto isto, determinemos 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

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

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 $a = b_i^{-1} b_j \,.\, a \,.\, b_j^{-1} b_i = b_i^{-1} b_j \,.\, a \,.\, (b_i^{-1} b_j)^{-1}$, ou seja $a \,.\, b_i^{-1} b_j = b_i^{-1} b_j \,.\, a$. 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 30: — *Há uma correspondência biunívoca completa entre os conjugados dum elemento* a ∈ $\mathbf{G}$ *e os complexos associados do normalizador de* a.

Se $\mathbf{G}$ 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 lugar o

COROLÁRIO 7: — *Num grupo finito, o número de conjugados dum elemento é um divisor de ordem do grupo.*

Passemos à noção de *normalizador dum subgrupo* $\mathfrak{g}$. Consideram-se em $\mathbf{G}$ 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 $\mathfrak{g}$. Vê-se que $\mathfrak{h}$ contém o próprio subgrupo $\mathfrak{g}$, o qual é invariante de $\mathfrak{h}$. Escrevendo $\mathbf{G}$ sob a forma

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

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 $a \mathfrak{g} a^{-1}$, $(a \in \mathbf{G})$. De facto, tem-se $b_i g \,.\, \mathfrak{g} \,.\, g^{-1} b_i^{-1} = b_i (g \mathfrak{g} g^{-1}) b_i^{-1} = b_i \mathfrak{g} b_i^{-1}$. Como no caso do normalizador dum elemento, também aqui complexos diferentes levam a subgrupos conjugados diferentes, e, além disso, os complexos levam a todos os subgrupos conjugados de $\mathfrak{g}$. Podemos dizer:

TEOREMA 31: — *Há uma correspondência biunívoca completa entre os subgrupos conjugados dum subgrupo* $\mathfrak{g}$ *e os complexos associados do normalizador do subgrupo.*

Dentro deste número das aplicações, trataremos ainda a noção de *grupo comutador*. Da definição de comutador de dois elementos, dada no n.º 4 deste §, 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 $\mathbf{G}$, o subgrupo de $\mathbf{G}$ gerado pelos comutadores.

TEOREMA 32: — *O grupo comutador é um invariante do grupo dado.* Seja $x \in \mathbf{G}$. Podemos escrever, sucessivamente:

$$\begin{gathered} x \,.\, a\, b\, (b\, a)^{-1} \,.\, x^{-1} = x\, a\, b\, a^{-1} b^{-1} x^{-1} = \\ = x\, a\, b \,.\, (a \,.\, x\, b)^{-1} (a \,.\, x\, b) \,.\, (x\, b \,.\, a)^{-1} = \\ = x\, a\, b\, b^{-1} x^{-1} a^{-1} \,.\, (a \,.\, x\, b) \,.\, (x\, b \,.\, a)^{-1} = \\ = [x\, a \,.\, (a\, x)^{-1}] \,.\, [(a \,.\, x\, b) \,.\, (x\, b \,.\, a)^{-1}] \,. \end{gathered}$$

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, concluímos que o conjugado dum comutador pertence ao grupo comutador. Seja agora o produto de dois comutadores. Vê-se que $x[(a\,b)(b\,a)^{-1}.(c\,d)(d\,c)^{-1}]\,x^{-1} = x[(a\,b)(b\,a)^{-1}]\,x^{-1}.$ $.x[(c\,d)(d\,c)^{-1}]\,x^{-1}$, 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 goza da propriedade de conter os conjugados dos seus elementos. É um invariante.

TEOREMA 33: — *O grupo cociente* $\mathbf{G}/\mathbb{C}$ *é abeliano.* Na verdade, tem-se $x\,\mathbb{C}\,.\,y\,\mathbb{C} = (x\,y)\,\mathbb{C}$, $y\,\mathbb{C}\,.\,x\,\mathbb{C} = (y\,x)\,\mathbb{C}$. Representando por c o comutador de x e y, é $(x\,y)(y\,x)^{-1} = c \in \mathbb{C}$, ou seja $x\,y \in \mathbb{C}(y\,x)$, o que mostra serem idênticas as classes $\mathbb{C}(x\,y)$ e $\mathbb{C}(y\,x)$, e, portanto, as classes $(x\,y)\,\mathbb{C}$ e $(y\,x)\,\mathbb{C}$. O produto $x\,\mathbb{C}\,.\,y\,\mathbb{C}$ é comutativo, como afirma o teorema.

O grupo comutador tem uma definição curiosa, que assenta neste

TEOREMA 34: — *O grupo comutador está contido em todo o invariante cujo grupo cociente seja abeliano.* Seja $\mathfrak{D}$ um invariante nas condições do enunciado. Dados $a, b \in \mathbf{G}$, tem-se $a\,\mathfrak{D}\,.\,b\,\mathfrak{D} = b\,\mathfrak{D}\,.\,a\,\mathfrak{D}$. Trata-se de provar que $\mathfrak{D}$ contém o comutador $(a\,b)(b\,a)^{-1}$. De facto, sendo $(a\,b)\,\mathfrak{D} = \mathfrak{D}\,(b\,a)$, existe $c \in \mathfrak{D}$ tal que $a\,b = c\,.\,b\,a$, o que leva a $c = a\,b\,(b\,a)^{-1} \in \mathfrak{D}$, como se deseja. É válida, pois, esta definição: *o grupo comutador é intersecção de todos os invariantes de* $\mathbf{G}$ *aos quais correspondem grupos cocientes abelianos.*

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

TEOREMA 35: — *A derivada segunda de* $\mathbf{G}$ *é um invariante de* $\mathbf{G}$.

Para fazermos a demonstração, comecemos por uma nota muito simples. Se c é o comutador de a e b, o comutador de $x\,a\,x^{-1}$ e $x\,b\,x^{-1}$ é $x\,c\,x^{-1}$. Nessas condições, se pomos $\mathbf{G}'' = \{u, C_1, C_2, \ldots\}$, imaginemos ser $C_i = c_1\,c_2\,(c_2\,c_1)^{-1}$. Será também $x\,C_i\,x^{-1}$ o comutador de $x\,c_1\,x^{-1}$ e $x\,c_2\,x^{-1}$. Ora, como estes dois últimos elementos pertencem a $\mathbf{G}'$, o seu comutador pertencerá a $\mathbf{G}''$. Se C_i for um produto de dois comutadores, encontra-se anàlogamente $x\,C_i\,x^{-1} \in \mathbf{G}''$, por ser o produto de dois elementos de $\mathbf{G}''$. O teorema é agora imediato.

Acabaremos este número, citando um invariante abeliano dum grupo que tem importância. É o *centro* do grupo, conjunto dos elementos de $\mathbf{G}$ que comutam com todos os elementos de $\mathbf{G}$. 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 $\mathbf{G}$ pertence ao centro, se, e só se, a totalidade dos seus conjugados se reduz ao próprio elemento.

§ 4 — O grupo simétrico

1) **Representação cíclica das permutações de n elementos** — Definimos o grupo simétrico $\mathfrak{S}_n$ no § 1, n.º 4. Consideremos os q elementos $i_1, i_2, \ldots, i_q$, dos n elementos $1, 2, \ldots, n$. Um ciclo $(i_1\,i_2 \ldots i_q)$ é a permutação

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

que muda i_1 em i_2, i_2 em i_3, etc., até i_q, que muda em i_1.

TEOREMA 36: — *Toda a permutação é um produto de ciclos.* Seja, com efeito,

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

Escrevamos o ciclo $(i_1 j_1 k_1 \ldots l_1)$, 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 $(i_r j_r \ldots p_r)$, 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 (j) significa a identidade; 2) um ciclo $(i_1 i_2 i_3 \ldots i_q)$ pode escrever-se ainda $(i_2 i_3 \ldots i_q i_1)$ ou $(i_3 i_4 \ldots i_q i_1 i_2)$, etc.; 3) na decomposição de uma permutação como produto de ciclos, é indiferente a ordem pelo 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 $1, 2, \ldots, n$, 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:

$$\mathfrak{S}_1: (1); \qquad \mathfrak{S}_2: (1), (12);$$
$$\mathfrak{S}_3: (1), (12), (13), (23), (123), (132).$$

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

TEOREMA 37: — *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 $(i_1 i_2 \ldots i_q) = (i_1 i_q)(i_1 i_{q-1}) \ldots (i_1 i_2)$, como se verifica imediatamente.

Quanto à segunda parte, utilizaremos as duas igualdades seguintes:

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

Na verdade, suponhamos $\varphi = (i_1 \ldots i_q)(j_1 \ldots j_r) \ldots (k_1 \ldots \ldots k_s)$ uma decomposição de φ em ciclos disjuntos e associemos a φ o número $N(\varphi) = (q-1) + (r-1) + \ldots + (s-1)$. Então, o número $N[(a\,b)\varphi]$, no caso de a e b pertencerem a um 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 $\varphi = (a\,b)(c\,d) \ldots (p\,q)$ um produto de m transposições, vê-se que tem lugar a relação

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

pois as transposições são as suas próprias inversas. Como, porém, $N(u) = 0$, existe uma relação $\pm 1 \pm 1 \pm \ldots \pm 1 + + N(\varphi) = 0$, onde os algarismos 1 estão escritos m vezes. A paridade de m é, assim, a do número bem determinado $N(\varphi)$. O teorema está completamente demonstrado. Dele resulta este

COROLÁRIO 8: — *O grupo $\mathfrak{S}_n$ é gerado pelas transposições* $(12), (13), \ldots, (1\,n)$. Basta ter em conta a igualdade $(i\,j) = (1\,j)(1\,i)(1\,j), (i \neq 1)$, para o reconhecer.

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

COROLÁRIO 9: — *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.*

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

TEOREMA 38: — *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 2 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 $(i\,j\,k)$, e o teorema fica provado. Podemos precisar e dizer:

TEOREMA 39: — *O grupo* $\mathfrak{A}_n$ *é gerado pelos ciclos* (1 2 3), (1 2 4), ..., (1 2 n). O grupo $\mathfrak{A}_3$, por ex., 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. Têm 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 do 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 considerarmos a permutação

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

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

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

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

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

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

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

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

$$q\geqq r\geqq\dots\geqq s,\qquad q+r+\dots+s=n.$$

Tais decomposições 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 este

TEOREMA 40: — *O número de partições de* n *é igual ao número de classes conjugadas do grupo simétrico* $\mathfrak{S}_n$. Claramente que a toda a partição correspondem decomposições em ciclos correspondentes. Pode verificar-se ainda que se tem $p(2)=2, p(3)=3$, $p(4)=5$, etc.

Suponhamos $n>2$. Se uma permutação $\varphi \in \mathfrak{S}_n$ for diferentes da permutação unidade, a decomposição em ciclos leva necessàriamente a $q>1$. Por ex., 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 $\psi(3)\neq 3$, 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 41: — *O centro de* $\mathfrak{S}_n$, *sob a hipótese* $n>2$, *reduz-se ao grupo unidade. Para* $n\leqq 2$, *o centro é o próprio grupo* $\mathfrak{S}_n$.

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

TEOREMA 42: — *O grupo alterno* $\mathfrak{A}_n$, *se for* $n>4$, *é um grupo simples.* Utilizaremos na demonstração o

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 (123), sabemos já que a afirmação é válida. O mesmo se diz, supondo $(132)\in\mathfrak{N}$. De resto, é $(132)^2=(123)$. Para o caso $n>3$, comecemos por admitir $(12k)\in\mathfrak{N}$. Então, $(1k2)=(12k)^2\in\mathfrak{N}$. E, pondo $\rho=(12)(kt),(k,t\neq 1,2)$, vê-se que $\rho.(1k2).\rho^{-1}=(12t)\in\mathfrak{N}$, qualquer que seja t. Tem-se $\mathfrak{N}=\mathfrak{A}_n$. Em seguida, posta a hipótese $(1ik)\in\mathfrak{N}$, com $i,k\neq 2$, basta escrever $\tau=(1k)(i2)$, para se reconhecer que $\tau.(1ik).\tau^{-1}=(1k2)\in\mathfrak{N}$. Finalmente, supondo $(ijk)\in\mathfrak{N}$, com $i,j,k\neq 1$, definindo σ pela relação $\sigma=(ik)(j1)$, encontra-se $\sigma.(ijk).\sigma^{-1}=(1ik)$. 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 $\mathfrak{N}$, e que deixe fixos o maior número possível de elementos. Essa permutação não pode ser decomposta em ciclos com elementos em número diferente, pois, se fosse $\sigma=(t_1\dots t_p).(m_1\dots m_q)\dots$, com $p>q$, a permutação σ^q conservaria todos os elementos

que σ deixa invariantes, e, além destes, ainda os elementos $m_1,\dots,m_q$. 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

$$\sigma=(ik)(tm)\dots(pn),\qquad \sigma=(ikp)\dots(tmn),$$
$$\sigma=(iktm)\dots(prsn),\qquad \sigma=(iktm\dots n)\dots.$$

Em qualquer dos casos, haveria dois elementos, t e m, pertencentes ao mesmo ciclo e diferentes dos elementos i, k, n. A permutação $\sigma'=(ikn).\sigma.(ikn)^{-1}$, 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 $\sigma=(ij)(kt)$, $\sigma=(ijk)$. A última relação, em face do lema 1, dará $\mathfrak{N}=\mathfrak{A}_n$. Se for válida a primeira relação, como se tem $n>4$, ponhamos $\sigma'=(ktm).\sigma.(ktm)^{-1}=(ij)(tm)$. Vê-se que $\sigma'\in\mathfrak{N}$, tendo-se também $\sigma\sigma'=(ktm)\in\mathfrak{N}$. Ainda pelo lema, será $\mathfrak{N}=\mathfrak{A}_n$. A demonstração está feita.

Quando $n=4$, a demonstração anterior falha, precisamente porque, ao escrever-se $\sigma=(ij)(kt)\in\mathfrak{N}$, não pode passar-se à permutação $\sigma'=(ij)(tm)$, por ser m um quinto elemento.

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 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: $\mathfrak{B} = \{(1); (12).(34); (13).(24); (14).(23)\}$. Neste subgrupo, a permutação idêntica e cada um dos seus elementos formam por sua vez, um subgrupo cíclico de 2.ª ordem, que é divisor normal do grupo de KLEIN. A cadeia de invariantes $\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset \mathfrak{B} \supset \{(1); (12)(34)\} \supset (1)$ também não permite a inserção de qualquer subgrupo que venha a ser invariante no elemento da cadeia que o precede.

§ 5 — Grupos transitivos e intransitivos. Grupos primitivos e imprimitivos

1) **Grupos transitivos e intransitivos** — Sejam $\mathfrak{C} = \{a, b, c, \ldots, x, y, \ldots\}$ um conjunto qualquer e $\mathfrak{G} = \{\varepsilon, \alpha, \ldots, \lambda, \ldots, \rho, \sigma, \tau, \ldots, \xi, \eta, \zeta, \ldots\}$ um grupo de transformações de $\mathfrak{C}$. $\mathfrak{G}$ diz-se *transitivo sobre* $\mathfrak{C}$, se, dados $x, y \in \mathfrak{C}$ arbitrários, existir $\rho \in \mathfrak{G}$ tal que $x\rho = y$.

TEOREMA 43: — *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* $\sigma \in \mathfrak{G}$ *por forma a ter-se* $a\sigma = z$. 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, $a\xi = x$, $a\eta = y$, para certos ξ e η, vê-se que $a = x\xi^{-1}$ e $a\eta = x\xi^{-1}\eta = y$. O elemento $\sigma = \xi^{-1}\eta \in \mathfrak{G}$ é tal que $x\sigma = y$. 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 $\lambda \in \mathfrak{G}$ verificando a igualdade $b = a\lambda$. 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 intransitivo e fixemos um elemento a. Além da identidade ε, 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 44: — *Há uma correspondência biunívoca completa entre as classes associadas de* $\mathfrak{G}_a$ *e os elementos de* $\mathfrak{C}$. De facto, todos os elementos duma classe $\mathfrak{G}_a\sigma$ transformam a no mesmo elemento $a\sigma$; e, assim, a cada classe corresponde um elemento de $\mathfrak{C}$. Se for $\mathfrak{G}_a\sigma \neq \mathfrak{G}_a\rho$, é $a\sigma \neq a\rho$, pois que a igualdade $a\sigma = a\rho$ daria $a = a\rho\sigma^{-1}$ ou seja $\rho\sigma^{-1} \in \mathfrak{G}_a$; 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 45: — *Há correspondência biunívoca completa entre os elementos de* $\mathfrak{G}_a$ *e os elementos de* $\mathfrak{G}_b$. Suponhamos $b = a\tau$. Então, $\tau^{-1}\mathfrak{G}_a\tau$ é um subgrupo conjugado de $\mathfrak{G}_a$ que conserva b. Inversamente, se $b\sigma = b$, então $a\tau\sigma = a\tau$, ou $a = a\tau\sigma\tau^{-1}$ Será $\tau\sigma\tau^{-1} \in \mathfrak{G}_a$ e $\sigma \in \tau^{-1}\mathfrak{G}_a\tau$. O teorema fica provado, precisamente pelo facto de ser $\mathfrak{G}_b = \tau^{-1}\mathfrak{G}_a\tau$.

COROLÁRIO 10: — *Se* $\mathbf{G}$ *é um grupo finito de transformações, de* $\mathfrak{C}$, *todos os subgrupos* $\mathbf{G}_a$ *contêm o mesmo número de elementos. Se* $\mathfrak{C}$ *é finito, o número de classes associadas de* $\mathbf{G}_a$ *é igual ao número de elementos de* $\mathfrak{C}$. *Se* $\mathbf{G}$ *e* $\mathfrak{C}$ *são finitos, o número de elementos de* $\mathfrak{C}$ *é um divisor da ordem de* $\mathbf{G}$.

2) **Grupos primitivos e imprimitivos** — Admitamos que $\mathbf{G}$ é transitivo sobre $\mathfrak{C}$. $\mathbf{G}$ diz-se *imprimitivo*, se for possível decompor $\mathfrak{C}$ sob a forma $\mathfrak{C} = \{\mathfrak{C}_1, \mathfrak{C}_2, \ldots\}$, 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) dados $\mathfrak{C}_i$ e $\mathfrak{C}_j$ arbitrários existe um $\sigma \in \mathbf{G}$ tal que $\mathfrak{C}_i\sigma = \mathfrak{C}_j$; 4) qualquer $\lambda \in \mathbf{G}$ transforma um $\mathfrak{C}_k$ noutro subconjunto $\mathfrak{C}_i$;

TEOREMA 46: — *É condição necessária e suficiente, para que o grupo* $\mathfrak{G}$, *transitivo sobre* $\mathfrak{C}$, *seja imprimitivo, que exista um certo* $\mathfrak{C}_k$ *tal que, para cada* $\mathfrak{C}_q$, *possa determinar-se* $\sigma \in \mathfrak{G}$ *por forma a ter-se* $\mathfrak{C}_k \sigma = \mathfrak{C}_q$. Da definição resulta imediatamente que a condição é necessária. O domínio de imprimitividade $\mathfrak{C}_k$ é qualquer. Para se ver que é suficiente, tomemos $\mathfrak{C}_i$ e $\mathfrak{C}_j$ arbitràriamente. Por ser, fixado $\mathfrak{C}_k$, $\mathfrak{C}_k \xi = \mathfrak{C}_i$, $\mathfrak{C}_k \eta = \mathfrak{C}_j$, para certos ξ e η, vê-se que $\sigma = \xi^{-1}\eta$ é tal que $\mathfrak{C}_i \sigma = \mathfrak{C}_j$. O teorema está provado.

Se $\mathfrak{G}$ não é imprimitivo, diz-se *primitivo*. Os conjuntos $\mathfrak{C}_i$, 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 47: — *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 44.

Uma proposição análoga à do teorema 45 é também válida aqui. O mesmo se diz do corolário 10. Observemos 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 48: — *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, assim, como se afirma no teorema, $\mathfrak{G}_a \subset \mathfrak{H} \subset \mathfrak{G}$.

Inversamente, dado $\mathfrak{H}$ nas condições indicadas, escrevamos $\mathfrak{G} = \mathfrak{H} \cup \mathfrak{H}\rho \cup \mathfrak{H}\sigma \cup \ldots$, $\mathfrak{H} = \mathfrak{G}_a \cup \mathfrak{G}_a\alpha \cup \mathfrak{G}_a\beta \cup \ldots$, e, portanto, $\mathfrak{G} = (\mathfrak{G}_a \cup \mathfrak{G}_a\alpha \cup \ldots) \cup (\mathfrak{G}_a\rho \cup \mathfrak{G}_a\alpha\rho \cup \ldots) \cup \ldots$. 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 ex., cada classe associada da decomposição $\mathfrak{H} = \mathfrak{G}_a \cup \mathfrak{G}_a\alpha \cup \ldots$ vai dar um só elemento de $\mathfrak{C}_1$.

O teorema 44 garante que o processo indicado leva a todos os elementos de $\mathfrak{C}$ e a cada um deles uma só vez. Os $\mathfrak{C}_i$ são, pois, disjuntos. Do facto de ser $\mathfrak{G} \supset \mathfrak{H}$, resulta existirem dois conjuntos $\mathfrak{C}_i$, pelo menos. E, por ser $\mathfrak{H} \supset \mathfrak{G}_a$, cada $\mathfrak{C}_i$ tem mais do que um elemento. Finalmente, dados os conjuntos $a\mathfrak{H}\rho$ e $a\mathfrak{H}\sigma$, a transformação $\rho^{-1}\sigma$ faz passar do primeiro ao segundo.

Feita 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.

Pelo contrário, o grupo simétrico $\mathfrak{S}_n$ é primitivo sobre o conjunto $\mathfrak{C}$ dos n números a que respeita. De facto, é transitivo.

Suponhamos, em seguida, que era possível decompor-se em domínios de imprimitividade. Excluído o caso $n=2$, para o qual a primitividade é banal, imaginemos $n \geqq 3$. Então, $\mathfrak{C}$ poderia tomar, pôr ex., a forma $\mathfrak{C}=\{\{j,\ldots,k\},\ldots,\{i,\ldots\}\}$. A permutação que mudasse $j,\ldots,k$ em $j,\ldots,i$ não transformaria entre si os domínios de decomposição de $\mathfrak{S}_n$, contra a hipótese.

BIBLIOGRAFIA

A redacção deste Capítulo assenta nas exposições que, na parte respectiva, se encontram em:

A. SPEISER — *Die Theorie der Gruppen von endlicher Ordnung*, 2.ª edição, Berlim, Springer, 1927.

B. L. VAN DER WAERDEN — *Moderne Algebra*, tomo 1.º, Berlim, Springer, 1930.

H. ZASSENHAUS — *Lehrbuch der Gruppentheorie*, Berlim, Teubner, 1937.

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

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

Para uma discussão dos fundamentos, pode ver-se ainda:

J. MORGADO — *Álgebra Moderna*, 1 — Grupos, 30 páginas, Porto, Junta de Investigação Matemática, 1945.

CAPÍTULO II

ANÉIS

§ 1 — Postulados, exemplos, regras de cálculo

1) **Postulados** — Tomemos um conjunto não vazio $\mathfrak{C}=\{a,b,c,\ldots\}$ e suponhamos que esse conjunto é um sistema de elementos com *dupla composição*, ou seja, é um sistema no qual, dados dois elementos $a,b \in \mathfrak{C}$, existe um preceito de *soma*, que leva a $a+b=c$, e um preceito de *produto*, que leva a $a.b=ab=d$, com $c,d \in \mathfrak{C}$. Diz-se que $\mathfrak{C}$ constitui um *anel* $\mathfrak{A}$, se se verificam os dois sistemas de postulados a seguir.

1.º Sistema:

I) $\mathfrak{C}$ é *fechado* relativamente à soma;
II) é válida a *lei associativa:* $(a+b)+c=a+(b+c)$;
III) é válida a *lei comutativa:* $a+b=b+a$;
IV) a equação $a+x=b$ é solúvel em $\mathfrak{C}$.

2.º Sistema:

V) $\mathfrak{C}$ é *fechado* relativamente ao produto;
VI) é válida a *lei associativa*: $ab.c=a.bc$;
VII) é válida a *lei distributiva esquerda:* $a(b+c)=ab+ac$;
VIII) é válida a *lei distributiva direita*: $(a+b)c=ac+bc$.

O primeiro sistema de postulados mostra que o anel $\mathfrak{A}$, pelo que respeita à soma, forma um grupo *abeliano*, chamado *grupo aditivo do anel*. Quanto ao produto, $\mathfrak{A}$ é semi-grupo. Neste sentido, tem-se o *semi-grupo multiplicativo do anel*.

Se tiver lugar

$$\text{VIII}') \quad a\,b = b\,a,$$

o anel diz-se *comutativo*.

No conjunto $\mathfrak{A}$, tomado como módulo, cada inteiro n determina um endomorfismo $a \to n\,a$. O número inteiro 1 define o endomorfismo identidade e o inteiro zero define o *endomorfismo nulo*, assim denominado pelo facto de todos os elementos de $\mathfrak{A}$ serem aplicados sobre o zero de $\mathfrak{A}$.

Veremos que há anéis com um número finito de elementos. Pode suceder, portanto, independentemente do número de elementos do anel, que haja números inteiros não nulos que determinem em $\mathfrak{A}$ o endomorfismo nulo. Se m e n estão nessas condições, também o estão $m - n$ e $m\,n$. O primeiro facto garante que o conjunto de tais inteiros constitui um submódulo do módulo $\mathfrak{Z}$ dos inteiros, pelo que será gerado por um inteiro $q \geqq o$. Este número q diz-se *característica* do anel. Na hipótese $q > o$ ele representa a ordem máxima dos elementos de $\mathfrak{A}$. Quando for $q = o$, a ordem máxima é infinita. É por isso que, na hipótese $q = o$, tanto se diz que a *característica é zero* como que essa *característica é infinita*.

Vamos analisar imediatamente algumas consequências dos postulados. Deixaremos de parte, é claro, aquelas que resultam utilizando ùnicamente a operação de soma, as quais foram já detalhadas no Cap. anterior, § 1, n.º 6.

Também aqui a propriedade associativa do produto nos leva, como nos Grupos, a pôr

$$A\,B = a_1 \ldots a_p, \quad \text{com} \quad \begin{cases} A = a_1 \ldots a_n, \\ B = a_{n+1} \ldots a_p, \end{cases} \quad (p \geqq n+1),$$

desde que se defina produto de n elementos pela igualdade $a_1 \ldots a_n = a_1 \ldots a_{n-1}.a_n$.

Passemos ao estudo das propriedades distributivas, as quais não têm semelhantes na Teoria dos Grupos. Fácil é de concluir, por indução, que se tem

$$a\,(b_1 + \ldots + b_n) = a\,b_1 + \ldots + a\,b_n, \qquad (b_1 + \ldots + b_n)\,a = b_1\,a + \ldots + b_n\,a.$$

Da combinação das duas leis distributivas e do facto de $\mathfrak{A}$ ser um grupo abeliano aditivo, resulta a relação

$$(a_1 + \ldots + a_n)\,(b_1 + \ldots + b_m) = \sum_{i,k} a_i\,b_k,$$

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 $a\,(b - c) = a\,d$. Trata-se de demonstrar que é $a\,d = a\,b - a\,c$. Ora isso é imediato, visto que $a\,d + a\,c = a\,(c + d) = a\,b$. Assim, é válida a igualdade $a\,(b - c) = a\,b - a\,c$. No caso particular de ser $c = b$, vem $a\,(b - b) = a\,b - a\,b = o$, pelo que $a.o = o$. Daqui este

TEOREMA 1: — *O produto dum elemento qualquer pelo elemento nulo (ou deste por um elemento qualquer) leva ao elemento nulo.*

Este teorema sugere imediatamente que se indague acerca da sua inversão. Consideremos, por ex., um conjunto de elementos da forma (a, b), onde a e b são números reais quaisquer, e definamos, nesse conjunto, os preceitos de soma e de produto segundo as regras

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

O conjunto em questão é um anel, cujo elemento nulo é (o, o). Ora, se considerarmos o produto $(a, o).(o, b) = (o, o)$, vê-se que

se obtém o elemento nulo por um produto de dois elementos, nenhum dos quais é nulo. A inversa do teorema 1 não é, pois, verdadeira.

Dado, em $\mathfrak{A}$, um elemento $a \neq o$, se $b \neq o$ é tal que $ab = o$, diz-se que b é um *divisor de zero à direita* e a um *divisor de zero à esquerda*. Podemos incluir o elemento nulo nos divisores de zero, dizendo: se $a \neq o$ e b for tal que $ab = o$, b é um divisor de zero à direita; se $a \neq o$ e b for tal que $ba = o$, b é um divisor de zero à esquerda.

Consideraremos como compatíveis os diferentes postulados dos anéis (comutativos, ou não), pelo facto de eles terem lugar no anel dos números inteiros.

Além do anel dos inteiros, podemos indicar, como exemplo, o anel dos números racionais, o dos números reais e o dos números complexos.

2) **Anéis de divisão. Domínios de integridade** — Chama-se *anel de divisão, quase-corpo* ou *corpoíde*, todo o anel no qual é válido ainda este novo sistema de postulados:

3.º Sistema:

IX) existe elemento diferente do elemento nulo;
X) as equações $xa = b$, $ay = b$, quando $a \neq o$, são solúveis no anel, qualquer que seja b.

A restrição introduzida com $a \neq o$, no último postulado, é exigida pela compatibilidade de IX e X. Se pudesse ser $a = o$, então a solução de $xa = b$, com b qualquer, levaria a $xa = o = b$, pelo que não haveria elemento $\neq o$.

Um anel de divisão diz-se um *corpo* (DEDEKIND), se tiver ainda lugar

X′) $ab = ba$.

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 postulados a seguir:

3.º Sistema:

IX″) existe elemento diferente do elemento nulo;
X″) $ab = ba$;
XI″) se a equação $ax = b$, com $a \neq o$, é solúvel, a solução é única.

Hoje também se consideram *domínios de integridade não comutativos*, assim definidos: são anéis para os quais se tem o

3.º Sistema de postulados:

IX‴) existe elemento diferente do elemento nulo;
X‴) se as equações $xa = b$, e $ay = b$, com $a \neq o$, são solúveis, as respectivas soluções são únicas.

Se não for dito o contrário, nós entenderemos sempre que um domínio de integridade é comutativo ($ab = ba$).

Estudemos algumas propriedades dos anéis de divisão. Em primeiro lugar, existe *elemento um* $= u$, satisfazendo às relações $au = ua = a$, com a arbitrário. Para o ver, tomemos a equação $ay = a$, $(a \neq o)$, e designemos por u' uma solução. O elemento u' satisfaz a $bu' = b$, qualquer que seja b, porque, se for $xa = b$, tem-se $x.au' = xa.u' = bu' = xa = b$. Por isso, u' é uma unidade direita, Existe, anàlogamente, uma unidade esquerda u''. Em seguida, de $u''u' = u'' = u'$, chega-se à existência de $u = u' = u''$, único elemento um.

Prova-se, agora, a existência de inverso a^{-1}, dum elemento qualquer $a \neq o$. Pondo $ay = u$, a solução a desta equação é, de facto, um inverso direito de a. Mas, como $a \neq o$, designemos

por a' o seu inverso direito: $a\,a' = u$. Tem-se $a\,a = u$, $a\,a\,a = u$, $a\,a\,a\,a' = a\,a' = a\,a = u$, o que mostra ser a inverso esquerdo de a. Escreveremos $a = a^{-1}$. Este inverso é único (veja-se, adiante, o n.º 3).

Pode concluir-se daqui que um anel de divisão não tem divisores de zero: se um produto de dois elementos é nulo, um dos factores é nulo. De facto, se $a\,b = o$, tem-se, se $a \neq o$, $a^{-1}\,a\,b = b = o$; e, se $b \neq o$, $a\,b\,b^{-1} = a = o$.

Tem lugar, portanto, este

TEOREMA 2: — *Num anel de divisão existe elemento um, todo o elemento* a ≠ o *tem inverso e não há divisores de zero, salvo o elemento nulo.*

COROLÁRIO 1: — *Os elementos não nulos dum anel de divisão formam um grupo relativamente ao produto. A inversa é verdadeira.*

Quanto à inversa, observemos que, da hipótese de os elementos não nulos dum anel formarem grupo com respeito ao produto, resultam imediatamente os postulados IX) e X). Em particular, o elemento nulo (zero) é solução das equações $x\,a = o$, $a\,y = o$, se $a \neq o$.

Também no caso dos domínios de integridade não há divisores de zero, além de zero. Se $a\,b = o$, com $a \neq o$, como é $a\,.\,o = o$, segue-se $b = o$. Inversamente, um anel comutativo, cujos elementos diferentes de zero não podem ser divisores de zero, é um domínio de integridade. Na verdade, se a equação $a\,x = b$, com $a \neq o$, é solúvel, não pode ter-se $a\,x = a\,x' = b$, $(x' \neq x)$, visto que, de contrário, seria $a\,(x' - x) = o$, com $x' - x \neq o$. A *lei de corte* tem lugar, quando o elemento cortado é $\neq o$.

Os elementos diferentes de zero dum domínio de integridade formam um semi-grupo, e esta propriedade é característica, como acabamos de verificar. É válido este

TEOREMA 3: — *É condição necessária e suficiente, para que um anel* $\mathfrak{A}$, *com elementos diferentes de zero, seja um domínio de integridade, que não existam divisores de zero, salvo zero.* Também se tem:

TEOREMA 3′: — *É condição necessária e suficiente, para que um anel* $\mathfrak{A}$, *com elementos diferentes de zero, seja um domínio de integridade não comutativo, que não existam divisores de zero, salvo zero.* A demonstração segue nos moldes do caso comutativo.

Comparando os raciocínios aqui feitos com os do n.º 2, § 1, Cap. I, vemos que, num domínio de integridade não comutativo, se realizam as condições seguintes: 1) o conjunto dos seus elementos, tal como para um anel qualquer, formam, relativamente ao produto, um semi-grupo; 2) os seus elementos diferentes de zero constituem um sub-semi-grupo daquele semi-grupo; 3) neste sub-semi-grupo tem lugar a propriedade 3″) do n.º 2, § 1, Cap. I, a qual é equivalente à lei de corte. A actual condição 3) é já arrastada, porém, pela actual condição 2).

TEOREMA 4: — *Um domínio de integridade não comutativo, com um número finito de elementos, é um anel de divisão.* Esta afirmação é consequência da 2.ª parte do corolário 1, pois, que, todo o semi-grupo com um número finito de elementos e com a propriedade 3″) do n.º 2, § 1, Cap. I, é um grupo. Ela perde o seu significado, como veremos mais tarde, em virtude dum teorema devido a WEDDERBURN.

Os números racionais ou os números reais constituem corpos. O conjunto dos inteiros é um domínio de integridade.

Embora tenhamos dado já um exemplo de anel comutativo que não é domínio de integridade, vamos citar aqui segundo exemplo. Consideremos o conjunto das funções contínuas no intervalo $(-\pi, +\pi)$. Trata-se, de facto, dum anel comutativo. Ele não é domínio de integridade, pois que as duas funções

$$f(x) = \begin{cases} x, & \text{no intervalo } (0, \pi), \\ 0, & \text{» » } (-\pi, 0), \end{cases}$$

$$g(x) = \begin{cases} 0, & \text{no intervalo } (0, \pi), \\ x, & \text{» » } (-\pi, 0), \end{cases}$$

ambas diferentes de zero e contínuas no intervalo em causa, dão $f(x).g(x)=0$.

Achamos interessante indicar ainda neste momento como pode construir-se um corpo de 4 elementos: o, u, a, b. Veremos que se tem necessàriamente $b=u+a=a+u$, de sorte que o corpo se comporá de o, u, a, $u+a$. 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 o, u, $-u$, $2u$ são distintos. Nessas circunstâncias, a tabela do grupo multiplicativo (com $a=-u$, $b=2u$) daria

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

,

donde se tirava, por ex., $2u.(-u)=-2u=u$, que seria falso, por hipótese. A segunda hipótese, sempre sob a condição de *existir* o corpo de 4 elementos, mostraria que esses elementos seriam o, u, $2u$, a. O elemento $a+u$ não poderia ser igual a nenhum daqueles, visto que: $a+u=o$ daria $a=-u=2u$; $a+u=u$ daria $a=o$; $a+u=2u$ daria $a=u$; e, de $a+u=a$, concluiríamos $u=o$. Será necessàriamente $-u=u$, $2u=o$. Então, $2a=2b=o$ e a tabela da soma toma o aspecto

	o	u	a	b
o	o	u	a	b
u	u	o	b	a
a	a	b	o	u
b	b	a	u	o

.

Construídas as tabelas *únicas* dos grupos aditivos e multiplicativos, verificam-se, em seguida, os postulados dos corpos. O corpo tem a característica dois.

3) **O elemento um e o inverso dum elemento** — Dos postulados enunciados para os anéis, não se conclui que existe 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 produto se introduzem pelas regras $(a,b)+(c,d)=(a+c,b+d)$; $(a,b).(c,d)=(o,o)$. 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, $a\,(u_d-u'_d)=o$. 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. Das relações $u_e\,u_d=u_e=u_d$ conclui-se, então, que essas unidades são iguais. E, suposta u'_d outra unidade direita, também deveria ser $u'_d=u_e$, pelo que se pode dar este enunciado:

TEOREMA 5: — *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 mesma ordem de ideias é interessante esta afirmação:

TEOREMA 6: — *A existência de uma* única *unidade esquerda* u_e *implica que* u_e *seja unidade bilateral (elemento um).* De facto, tomemos a e b quaisquer. Escrevendo $(a\,u_e-a+u_e)\,b=a\,b-a\,b+b=b$, conclui-se $a\,u_e-a+u_e=u_e$, ou $a\,u_e=a$, como se deseja.

Quando ao inverso dum elemento, fazem-se considerações análogas. No anel dos números pares, como no outro exemplo neste 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 $a_d'^{-1}$ é um segundo inverso direito, da igualdade $a\,a_d^{-1} = a\,a_d'^{-1}$ deduz-se $a(a_d^{-1} - a_d'^{-1}) = o$, mas não pode concluir-se $a_d^{-1} = a_d'^{-1}$, 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. Será $a_d^{-1} = a_e^{-1}\,a.a_d^{-1} = a_e^{-1}.\,a\,a_d^{-1} = a_e^{-1}$. Suposto $a_d'^{-1}$ outro inverso direito, também deveria ter-se $a_d'^{-1} = a_e^{-1}$, pelo que é válido este enunciado:

TEOREMA 7: — *Se um elemento* a *dum anel tem inverso direito e esquerdo, esses inversos são iguais. Há, então, um só inverso direito e esquerdo, que se diz* inverso *de* a *e se representa por* a^{-1}.

Claramente que um divisor de zero não pode ter inverso. Se designarmos por *unidades* os elementos dum anel com inverso, 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 8: — *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 a e a_1 dois inversos direitos distintos de a. Façamos $\beta_1 = a_1 a - u$. Vê-se que $\beta_1 \neq o$, $a\beta_1 = o$, $\beta_1 a_1 = o$. Em seguida, ponhamos $a_2 = a_1 + \beta_1$. Também a_2 é um inverso direito de a, a partir do qual construiremos $\beta_2 = a_2 a - u \neq o$, com $a\beta_2 = o$, $\beta_2 a_2 = o$. Duma maneira geral, chegados a a_n, faremos $\beta_n = a_n a - u$ e verificaremos ser $\beta_n \neq o$, $a\beta_n = o$, $\beta_n a_n = o$. Depois prosseguiremos com $a_{n+1} = a_n + \beta_n$, etc.. Se provarmos que os β_i são todos distintos, ficará construída uma infinidade de inversos direitos distintos de a, a saber: $a_1 + \beta_i$, $(i = 1, 2, \ldots, n, \ldots)$.

Ora, sendo $\beta_{n+1} = a_{n+1}a - u = (a_n + \beta_n)a - u = a_n a + \beta_n a - u = \beta_n + \beta_n a = \beta_n(u + a)$, conclui-se a sucessão de igualdades

$$\beta_{n+1} = \beta_n(u + a) = \beta_{n-1}(u + a)^2 = \ldots = \beta_1(u + a)^n,$$

das quais se tira

$$\beta_k = \beta_i(u + a)^l, \qquad (k > i;\ k = l + i).$$

O facto de u e a serem comutáveis permite a aplicação da fórmula do binómio, o que dará

$$\beta_k = \beta_i\left[u + l\,a + \binom{l}{2}a^2 + \ldots + l\,a^{l-1} + a^l\right],$$

$$\beta_k - \beta_i = l\,\beta_i a + \binom{l}{2}\beta_i a^2 + \ldots + l\,\beta_i a^{l-1} + \beta_i a^l.$$

Multiplicando ambos os membros desta última igualdade, à direita, por a_i^l, encontra-se $(\beta_k - \beta_i)\,a_i^l = \beta_i a^l a_i^l = \beta_i$, pois $\binom{l}{r}\beta_i a^r a_i^l = \binom{l}{r}\beta_i a^r a_i^r a_i^{l-r} = \binom{l}{r}\beta_i a_i^{l-r} = o$, por ser $\beta_i a_i = o$. Não pode ter-se $\beta_k - \beta_i = o$, e o teorema fica demonstrado.

4) **Outras regras de cálculo** — Quando os factores dum produto são iguais, define-se

$$a^n = a \ldots a, \text{ (com } n \text{ factores)},$$

e é-se levado às igualdades

$$a^n.a^m = a^{n+m}, \qquad (a^n)^m = a^{n\,m},$$

que se demonstram como as regras análogas para os Grupos.

Se o anel tem elemento um e a tem inverso, podemos estender as regras de cálculo anteriores às potências de expoente nulo e negativo. Põe-se, então,

$$a^o = u, \qquad a^{-n} = (a^{-1})^n,$$

verificando-se, em seguida, estas igualdades

$$a^{-n}=(a_n^{\wedge})^{-1}, \quad a^n.a^{-m}=a^{n-m}, \quad (a^n)^{-m}=a^{-nm}.$$

Uma regra que não tem equivalente na teoria dos Grupos é expressa nas igualdades seguintes:

$$n\,.\,ab=na\,.\,b=a\,.\,nb$$

que se demonstram por indução. O «produto» $n\,.\,ab$ representa-se simplesmente por nab.

Consideremos agora o elemento $-nab$. É $nab-nab=o$. Mas $-na\,.\,b+na\,.\,b=-na\,.\,b+nab=(-na+na)\,b=o$, pelo que $-nab=-na\,.\,b$. Também se vê que $-nab=a\,.\,(-nb)$, convindo, assim, fixar as regras

$$-nab=-na\,.\,b=a\,.\,(-nb).$$

Tomemos ainda uma expressão do tipo $-n\,.\,ab$. Vimos, nas regras de cálculo relativas a grupos abelianos aditivos, que é $-n\,.\,ab=-nab$. É assim que se tem

$$-n\,.\,ab=-nab=-na\,.\,b=a\,.\,(-nb)=n(-a)\,.\,b=$$
$$=a\,.\,n(-b)=(-n\,.\,a)\,b=a\,.\,(-n\,.\,b).$$

Para terminar este número, façamos 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.

5) **Sobre as aplicações dum grupo em si próprio** — No que vai seguir-se, representaremos um grupo pela letra $\mathfrak{M}$ e utilizaremos o sinal $+$ como sinal da operação do grupo, embora $\mathfrak{M}$ não seja geralmente comutativo. Estudaremos o conjunto $\tau(\mathfrak{M})$ das aplicações de $\mathfrak{M}$ em si, isto é, das correspondências que levam dum elemento de $\mathfrak{M}$ a um elemento de $\mathfrak{M}$. Se $A, B, C, \ldots$ forem essas aplicações e $x \in \mathfrak{M}$, a correspondência $x \to xA$ repre-

senta a aplicação em causa. Se, qualquer que seja x, for $xA=xB$, poremos $A=B$. Assim, nos raciocínios a seguir, $A, B, C, \ldots$ serão supostas distintas.

Em $\tau(\mathfrak{M})$, definiremos uma *soma* $A+B$, escrevendo

$$x(A+B)=xA+xB;$$

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

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

Verifica-se imediatamente o seguinte

TEOREMA 9: — *O conjunto* $\tau(\mathfrak{M})$ *é grupo ~~abeliano~~ relativamente à soma.* De facto: 1) $A+B \in \tau(\mathfrak{M})$; 2) existe elemento um, que representaremos por 0 (zero), e que é a aplicação por meio da qual a todo o elemento $x \in \mathfrak{M}$ se faz corresponder $\emptyset \in \mathfrak{M}$: $x0=o=$ identidade de $\mathfrak{M}$; 3) existe aplicação inversa $-A$, de cada aplicação A, como se deduz pondo $x(-A)=-xA$; 4) é válida a propriedade associativa $(A+B)+C=A+(B+C)$. E também se tem:

TEOREMA 10: — *O conjunto* $\tau(\mathfrak{M})$ *é um grupóide relativamente à operação de produto.* De facto: 1′) $AB \in \tau(\mathfrak{M})$; 2′) é válida a propriedade associativa: $(AB)C=A(BC)$; 3(IV)) existe elemento um, que é a transformação idêntica.

Nas relações que envolvem soma e produto tem lugar a igualdade

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

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

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

que se entende por aplicação de A a uma soma de dois elementos.

Restrinjamos, porém, o conjunto $\tau(\mathfrak{M})$, tomando neste conjunto apenas o subconjunto $\mathfrak{E}(\mathfrak{M})$ dos endomorfismos de $\mathfrak{M}$, definidos, como sabemos, por meio de igualdades da forma

$$(x+y)A = xA + yA.$$

Fàcilmente se verifica que este conjunto $\mathfrak{E}(\mathfrak{M})$ é fechado relativamente à soma e ao produto. Então, no conjunto $\mathfrak{E}(\mathfrak{M})$, já é válida a igualdade

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

pois que $x(B+C)A = (xB + xC)A = xBA + xCA = x(BA + CA)$. Tal como anteriormente, porém, continua a ser $A+B \neq B+A$.

Finalmente, suponhamos que o grupo $\mathfrak{M}$ é um grupo comutativo. No conjunto dos endomorfismos $\mathfrak{E}(\mathfrak{M})$ já se tem $A+B = B+A$, podendo enunciar-se este importante

Teorema 11: — *O conjunto* $\mathfrak{E}(\mathfrak{M})$ *dos endomorfismos dum grupo abeliano* $\mathfrak{M}$ *é um anel.* Claramente que a aplicação zero é um endomorfismo e que, supondo A um endomorfismo, $-A$ é igualmente um endomorfismo.

§ 2 — Subanéis, anéis ampliados, ideais, homomorfismos, anéis cocientes

1) **Critério de subanel** — Dum modo geral, dado um conjunto $\mathfrak{C}$, onde se verificam determinadas regras, que levam a uma certa designação para $\mathfrak{C}$, diz-se subconjunto de $\mathfrak{C}$, com a mesma designação, um conjunto $\mathfrak{C}'$, de elementos de $\mathfrak{C}$, no qual se verificam as regras em referência. Quando $\mathfrak{C}'$ não contém todos os elementos de $\mathfrak{C}$, o subconjunto diz-se *próprio* ou *autêntico.*

Teorema 12: — $\mathfrak{A}'$ *é um subanel do anel* $\mathfrak{A}$, *se, com* a *e* b, *contiver* a — b *e* a b; $\mathfrak{D}'$ *é um subanel de divisão do anel de divisão* $\mathfrak{D}$, *se, com* a *e* b, *contiver* a — b, *assim como* b a^{-1}, *quando* a $\neq o$; $\mathfrak{A}'$ *é um subdomínio de integridade do domínio de integridade* $\mathfrak{A}$, *(comutativo ou não), se for subanel e contiver, pelo menos, dois elementos.* Tratemos, por ex., o caso dos subanéis de divisão. A hipótese $a - b$ e $\mathfrak{D}'$ garante ser $\mathfrak{D}'$ um grupo abeliano. Como se admite a existência dum elemento $a \neq o$, o postulado IX) é verificado. Então, os elementos não nulos de $\mathfrak{D}'$ satisfazem o critério de subgrupo, pelo que, em $\mathfrak{D}'$, o produto desses elementos é fechado. A inclusão do zero não altera esse facto. Resulta daí que $\mathfrak{D}'$ é um subanel cujos elementos não nulos formam um subgrupo. Portanto, $\mathfrak{D}'$ 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 o e u.

Tratando-se de corpos, introduz-se a designação de *corpo primo* para todo aquele que não tem subcorpo próprio. A intersecção de todos os subcorpos dum corpo é um corpo primo.

Seja $\mathfrak{K}$ um corpo e tomemos u e $\mathfrak{K}$. 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 do n.º 2, § 1, o qual era $2u = o$. O conjunto dos elementos distintos mu é um domínio de integridade.

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 $\mathfrak{C}'$ um conjunto algebrizado

com uma soma e um produto. Se, dado $x \in \mathfrak{A}$, lhe corresponder um elemento determinado $x' \in \mathfrak{C}'$, de tal modo que todos os elementos de $\mathfrak{C}'$ sejam utilizados como imagem, e de tal modo ainda que, com $x \to x', y \to y'$ se tenha também $x+y \to (x+y)' = x'+y', xy \to (xy)' = x'y'$, a correspondência $x \to x'$ diz-se um *homomorfismo*. Se cada elemento x' é imagem dum único elemento x, a correspondência $x \to x'$ é biunívoca e diz-se um *isomorfismo*.

Mesmo caso do homomorfismo, a imagem $\mathfrak{C}'$, de $\mathfrak{A}$, é um anel $\mathfrak{A}'$. Adiante retomaremos este assunto.

Com as notações $\mathfrak{A} \sim \mathfrak{A}'$ e $\mathfrak{A} \simeq \mathfrak{A}'$, tal como no caso dos Grupos, significaremos, respectivamente, homomorfismo anular e isomorfismo anular.

Posto isto, consideremos um anel $\mathfrak{A}$ e tomemos $a \in \mathfrak{A}$, fixo, e $x \in \mathfrak{A}$, arbitrário. A correspondência $x \to xa$ faz uma aplicação de $\mathfrak{A}$ em si, que é um endomorfismo do grupo abeliano aditivo de $\mathfrak{A}$. Escreveremos $xa = xE_a^{(d)}$, de sorte que $E_a^{(d)}$ é o *endomorfismo definido pela multiplicação, à direita, por* a. A correspondência $x \to ax = xE_a^{(e)}$ 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 $x(a+b) = xa + xb = xE_a^{(d)} + E_b^{(d)} = x(E_a^{(d)} + E_b^{(d)})$, 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 $x(ab) = (xa)b = xE_a^{(d)}E_b^{(d)}$, deduz-se

$$ab \to E_{ab}^{(a)} = E_a^{(d)}E_b^{(d)}.$$

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 $\mathfrak{E}(\mathfrak{A})$, dos endomorfismos do grupo abeliano aditivo de $\mathfrak{A}$. Se existir elemento $u \in \mathfrak{A}$, então, suposto $a \neq b$, é $u \to ua = a = uE_a^{(d)}$, $u \to ub = b = uE_b^{(d)}$, de sorte que $E_a^{(d)} \neq E_b^{(d)}$. Tem lugar o teorema a seguir, que corresponde ao teorema de CAYLEY do n.º 5, § 1, Cap. I:

TEOREMA 13: — *Um anel com elemento um é isomorfo dum subanel do anel dos endomorfismos do seu grupo abeliano aditivo.*

A noção de *anti-homomorfismo* anular é definida pelas leis

$$a \to a', b \to b', \; a+b \to (a+b)' = a'+b', \; ab \to (ab)' = b'a' .$$

No caso de biunivocidade, tem-se um *anti-isomorfismo* ou um *isomorfismo inverso*. A correspondência $a \to E_a^{(e)}$, atrás definida, é um anti homomorfismo. Se existe $u \in \mathfrak{A}$, é um anti-isomorfismo. O conjunto dos $E_a^{(e)}$ é um subanel $\mathfrak{A}_e$, de $\mathfrak{E}(\mathfrak{A})$.

É válido este

TEOREMA 14: — *Dado anel* $\mathfrak{A}$, *com elemento um, os subanéis* $\mathfrak{A}_d$ *e* $\mathfrak{A}_e$ *são comutadores recíprocos dentro de* $\mathfrak{E}(\mathfrak{A})$. Em virtude de se ter $axb = ax.b = a.xb = xE_a^{(e)}E_b^{(d)} = xE_b^{(d)}E_a^{(e)}$, vê-se que, efectivamente, é $E_a^{(e)}E_b^{(d)} = E_b^{(d)}E_a^{(e)}$. Inversamente, suponhamos, por ex., $\sigma \in \mathfrak{E}(\mathfrak{A})$ tal que $(xE_b^{(d)})\sigma = (x\sigma)E_b^{(d)}$. Então, fazendo $x = u$ e pondo $u\sigma = c$, vê-se que $(uE_b^{(d)})\sigma = (ub)\sigma = b\sigma = (u\sigma)E_b^{(d)} = cb$. Significa isto que a correspondência $b \to b\sigma$ é definida por $b \to cb = bE_c^{(e)} = b\sigma$, de sorte que $\sigma = E_c^{(e)}$, como se deseja.

3) **Anéis ampliados** — Dado um anel $\mathfrak{A}$, se o anel $\mathfrak{A}'$ contém $\mathfrak{A}$, diz-se uma *ampliação* ou *extensão* de $\mathfrak{A}$. É importante a seguinte proposição:

TEOREMA 15: — *Seja* $\mathfrak{C}$ *um conjunto de anéis* $\mathfrak{A}_\alpha$, *em número finito ou infinito, e suponhamos que o conjunto goza da propriedade de haver sempre um anel do conjunto que contém dois anéis quaisquer dados do mesmo; então, o conjunto unido (união)* $\mathfrak{U}$, *dos* $\mathfrak{A}_\alpha$ (1),

(1) $|\mathfrak{A}_\alpha|_{\alpha \in A}$ é o símbolo pelo qual se representa uma família ou conjunto de conjuntos $\mathfrak{A}_\alpha$. O índice variável α percorre os elementos dum conjunto A, existindo uma correspondência biunívoca completa entre ás $\mathfrak{A}_\alpha$ e os elementos de A.

é um anel. A respectiva demonstração faz-se verificando em $\mathfrak{A}$ os postulados dos anéis. Sejam, por ex., a, b, e $\mathfrak{A}$. Se for $a \in \mathfrak{A}_\alpha$, $b \in \mathfrak{A}_\beta$, existe $\mathfrak{A}_\gamma$ 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 $\{\mathfrak{A}_\alpha\}_{\alpha \in A}$, 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 I) é verificado em $\mathfrak{A}$. Se quiséssemos provar a propriedade associativa $ab.c = a.bc$, 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.

No caso particular de os $\mathfrak{A}_\alpha$ serem corpos $\mathfrak{K}_\alpha$, o conjunto unido $\mathfrak{A}$ é ainda um corpo. Na *Teoria dos Corpos* esta observação é muito útil. Também convém notar que não foi feita a hipótese inicial de os diferentes $\mathfrak{A}_\alpha$ serem subanéis dum mesmo anel. Construído o anel $\mathfrak{A}$, este é ampliação de qualquer $\mathfrak{A}_\alpha$.

No número anterior, verificámos ser $\mathfrak{E}(\mathfrak{A})$, em geral, uma extensão de $\mathfrak{A}_d$ e de $\mathfrak{A}_e$. Eis agora um teorema de muito interesse:

TEOREMA 16: — *Um anel* $\mathfrak{A}_o$, *sem elemento um, pode «mergulhar-se» sempre num anel* $\mathfrak{A}$, *com elemento um.* O enunciado significa, duma maneira precisa, que, dado $\mathfrak{A}_o$, podemos construir uma ampliação $\mathfrak{A}$, contendo uma parte $\mathfrak{A}'_o$, isomorfa de $\mathfrak{A}_o$. Sob o ponto de vista abstracto, é legítima a substituição de $\mathfrak{A}'_o$ por $\mathfrak{A}_o$, dentro de $\mathfrak{A}$, pois que, tendo lugar a correspondência biunívoca $a_o \to a'_o$, $(a'_o \in \mathfrak{A}'_o)$, qualquer relação entre elementos acentuados se transfere para elementos não acentuados, e reciprocamente. Por outro lado, nas relações, dentro de $\mathfrak{A}$, em que intervenham elementos de $\mathfrak{A}'_o$ e elementos não pertencente a $\mathfrak{A}'_o$, a substituição de a'_o por a_o é meramente formal.

Passemos ao teorema. Seja $a_o \in \mathfrak{A}_o$. O anel $\mathfrak{A}$ será constituído pelos elementos $[m, a_o]$, onde m é inteiro, e onde, suposto

$b_o \in \mathfrak{A}_o$ e n inteiro, os preceitos de soma e de produto são definidos pelas igualdades

$$[m, a_o] + [n, b_o] = [m+n, a_o + b_o],$$
$$[m, a_o] \,.\, [n, b_o] = [mn, mb_o + na_o + a_o b_o].$$

De facto, em $\mathfrak{A}$ são verificados os postulados dos anéis, como é fácil de reconhecer. O elemento $[1, o]$ é o elemento um de $\mathfrak{A}$. E, por via da correspondência $a_o \to [o, a_o]$ determina-se a parte $\mathfrak{A}'_o$, de $\mathfrak{A}$, isomorfa de $\mathfrak{A}_o$.

O teorema 13 do número anterior pode agora revestir-se do aspecto preciso do teorema de CAYLEY:

TEOREMA 17: — *Todo o anel é isomorfo dum anel de endomorfismos.*

No estudo das relações entre $\mathfrak{A}_o$ 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, $(r > o)$, tal que $a^r = o$. Claramente que, se a_o for nilpotente em $\mathfrak{A}_o$, ele é nilpotente em $\mathfrak{A}$. Vamos ver que, inversamente, supondo $a \in \mathfrak{A}$ tal que $a^t = o$, é $a \in \mathfrak{A}_o$. De facto, escrevamos $a = [m, a_o]$. Como se tem $a^t = [m^t, b_o] = [o, o]$, deverá ser $m^t = o$, $m = o$, e, portanto, $a = [o, a_o] = a_o$. Tem-se:

TEOREMA 18: — *Na extensão de* $\mathfrak{A}_o$ *para* $\mathfrak{A}$, *há conservação dos elementos nilpotentes.*

4) **Ideais** — Um subconjunto $\mathfrak{r}$, de $\mathfrak{A}$, diz-se um *ideal direito* do anel $\mathfrak{A}$, se forem verificadas as duas condições seguintes: 1) $\mathfrak{r}$ contém, com a e b, o elemento $a - b$; 2) $\mathfrak{r}$ contém, com a, todos os produtos ar, com $r \in \mathfrak{A}$.

Um *ideal esquerdo* é, de $\mathfrak{A}$, satisfaz a 1) e à condição seguinte 2'): é contém, com a, todos os produtos sa, com $s \in \mathfrak{A}$.

Um *ideal bilateral,* ou, mais simplesmente, um *ideal,* é um subconjunto $\mathfrak{a}$, de $\mathfrak{A}$, que é simultâneamente ideal direito e esquerdo.

Vamos dar exemplos de ideais. Diz-se *ideal principal esquerdo gerado por* a o conjunto $(a)_e$ dos elementos $s\,a + n\,a$, onde $s \in \mathfrak{A}$ e n é inteiro. O *ideal principal direito gerado por* a é o conjunto $(a)_d$ dos elementos $a\,r + n\,a, (r \in \mathfrak{A})$, e o *ideal geral por* a é o conjunto (a) dos elementos $s\,a + a\,r + \Sigma\, p\,a\,q + n\,a$, 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 $a_1, a_2, \ldots, a_p$ são os elementos geradores, têm-se os conjuntos

$$\begin{array}{l} \{ s_1\,a_1 + \ldots + s_p\,a_p + n_1\,a_1 + \ldots + n_p\,a_p \}, \\ \{ a_1\,r_1 + \ldots + a_p\,r_p + n_1\,a_1 + \ldots + n_p\,a_p \} \end{array}$$

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 $s_1 = \ldots = s_p = o, n_2 = \ldots = n_p = 0, n_1 = 1$, 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

$$\begin{array}{l} (a_1, \ldots, a_p)_e = \{ \Sigma\, s_i\,a_i + \Sigma\, n_i\,a_i \}, \\ (a_1, \ldots, a_p)_d = \{ \Sigma\, a_i\,r_i + \Sigma\, n_i\,a_i \}, \\ (a_1, \ldots, a_p) = \{ \Sigma\, s_i\,a_i + \Sigma\, a_i\,r_i + \Sigma\, p\,a_i\,q + \Sigma\, n_i\,a_i \}. \end{array}$$

A última igualdade define o ideal bilateral gerado por $a_1, \ldots, a_p$.

Em todos os casos, os ideais em questão são os ideais mínimos que contêm $a_1, \ldots, a_p$. Se tomarmos, por ex., um ideal esquerdo que contenha $a_1, \ldots, a_p$, esse ideal conterá $s_1\,a_1, \ldots, s_p\,a_p$, conterá a soma $s_1\,a_1 + \ldots + s_p\,a_p$, assim como $n_1\,a_1 + \ldots + n_p\,a_p$ e a soma $\Sigma\, s_i\,a_i + \Sigma\, n_i\,a_i$.

O ideal esquerdo gerado por $a_1, \ldots, a_p$ 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 ex., que eles geram, é o conjunto dos somatórios finitos da forma $\Sigma\, a_i\,r_i + \Sigma\, n_i\,a_i$, 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* $= (o)$, 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 $a_1, \ldots, a_p$ é simplesmente o conjunto dos elementos da forma $a_1\,t_1 + \ldots + a_p\,t_p, (t_i \in \mathfrak{A})$, pois que $a_1\,r_1 + \ldots + a_p\,r_p + n_1\,a_1 + \ldots + n_p\,a_p = a_1\,(r_1 + n_1\,u) + \ldots + a_p\,(r_p + n_p\,u) = a_1\,t_1 + \ldots + a_p\,t_p$.

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 $n.2 + m.3 = n.2 + m.(2+1) = n'.2 + m'$. 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 $\{a\,r\}$ e $\{s\,a\}$ representam, repectivamente, 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 tam-

bém 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 $\Sigma\, b\, b' \in \mathfrak{A}$, obtidos por somatório finito, quando $b \in \mathfrak{m}$ e $b' \in \mathfrak{m}'$. 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 ex., as seguintes regras de cálculo:

$$\mathfrak{C}.(\mathfrak{r},\mathfrak{r}') = (\mathfrak{C}\mathfrak{r}, \mathfrak{C}\mathfrak{r}'), \qquad \mathfrak{C}.\mathfrak{r}\mathfrak{r}' = \mathfrak{C}\mathfrak{r}.\mathfrak{r}'.$$

O produto $\mathfrak{e}\,\mathfrak{r}$ é um ideal bilateral e a soma $(\mathfrak{r}, \mathfrak{A}\mathfrak{r})$ é o *ideal bilateral gerado por* $\mathfrak{r}$. Anàlogamente, $(\mathfrak{e}, \mathfrak{e}\mathfrak{A})$ é o *ideal bilateral gerado por* $\mathfrak{e}$.

O *cociente* $(\mathfrak{r}:\mathfrak{C})$, do ideal direito $\mathfrak{r}$ pelo conjunto $\mathfrak{C}$, define-se como o conjunto dos elementos $t \in \mathfrak{A}$ tais que $\mathfrak{C}t \subseteq \mathfrak{r}$. É um ideal direito. O cociente $(\mathfrak{r}:\mathfrak{A})$ é um ideal bilateral.

5) **Subanel gerado por um conjunto de elementos** — Consideremos um conjunto $\mathfrak{Q} = \{a, b, c, \ldots, t, \ldots\}$ de elementos dum anel $\mathfrak{A}$, conjunto que pode ser finito ou infinito. Diz-se *subanel gerado* por $\mathfrak{Q}$ o mais pequeno subanel que contém $\mathfrak{Q}$. Qualquer subanel que contenha $\mathfrak{Q}$ contém necessàriamente todos os elementos da forma $\Sigma \pm a\, b \ldots t$, 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 $\mathfrak{Q}$, muitas vezes representado por $[\mathfrak{Q}]$.

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:

$$C(C(\mathfrak{Q})) \supseteq \mathfrak{Q}, \qquad C(C(C(\mathfrak{Q}))) = C(\mathfrak{Q}).$$

Podemos agora ligar às ideias do n.º 2 deste § as diferentes noções de ideal. Se representarmos por 1 o endomorfismo idêntico de $\mathfrak{A}$, vê-se que, no anel $\mathfrak{E}(\mathfrak{A})$, nos endomorfismos de $\mathfrak{A}$, o subanel gerado por 1 e $\mathfrak{A}_d$, que aqui podemos designar por $\mathfrak{E}(1, \mathfrak{A}_d)$, é o conjunto de elementos da forma $\Sigma \pm 1\, E_r^{(d)} \ldots E_s^{(d)}$, e que o subanel gerado por $1, \mathfrak{A}_d$ e $\mathfrak{A}_e$, representado por $\mathfrak{E}(1, \mathfrak{A}_d, \mathfrak{A}_e)$, é o conjunto de elementos da forma $\Sigma \pm 1\, E_r^{(d)} \ldots E_s^{(d)} E_t^{(e)} \ldots E_v^{(e)}$. Então, tem-se:

$$(a)_d = a\,\mathfrak{E}(1, \mathfrak{A}_d), \qquad (a) = a\,\mathfrak{E}(1, \mathfrak{A}_d, \mathfrak{A}_e),$$

subentendendo, é claro, que um símbolo da forma $a\,\mathfrak{B}$, onde $\mathfrak{B} \subseteq \mathfrak{E}(\mathfrak{A})$, representa o conjunto de elementos de aspecto $a\,S$, com $S \in \mathfrak{B}$.

6) **Homomorfismos e isomorfismos** — No n.º 2 deste § referimo-nos já a estas duas noções. Dum modo geral, sejam $\mathfrak{B}$ e $\mathfrak{B}'$ dois conjuntos algebrizados com uma noção de soma e uma noção de produto. Se, dado $b \in \mathfrak{B}$ lhe fizermos corresponder $b' \in \mathfrak{B}'$, de modo unívoco, de tal sorte que, sendo também $a \to a'$, se tenha $a + b \to (a+b)' = a' + b'$, $ab \to (ab)' = a'b'$, $(a \in \mathfrak{B},\ a' \in \mathfrak{B}')$, a correspondência definida diz-se uma *homomorfia*. Uma homomorfia chama-se um *homomorfismo*, quando todo o espaço algébrico $\mathfrak{B}'$ é utilizado como imagem. Empregaremos o simbolismo $\mathfrak{B} \sim \mathfrak{B}'$, para significar que os dois espaços se correspondem por homomorfismo. Quando há correspondência biunívoca num homomorfismo, diz-se que se tem um *isomorfismo* e escreve-se $\mathfrak{B} \simeq \mathfrak{B}'$.

Fizemos já esta afirmação:

TEOREMA 19: — *Considerado o homomorfismo* $\mathfrak{A} \sim \mathfrak{A}'$, *se* $\mathfrak{A}$ *é anel,* $\mathfrak{A}'$ *é anel.* A demonstração não oferece qualquer dificul-

dade. Na correspondência homomorfa em causa, são correspondentes os elementos zero, assim como os elementos um, se $\mathfrak{A}$ tem elemento um. Pode, todavia, existir elemento um em $\mathfrak{A}'$, sem que o haja 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 e $\mathfrak{r}$ como submódulo. É, assim, $(a+\mathfrak{r})+(b+\mathfrak{r})=a+b+\mathfrak{r}$. 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 1.º 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'' e $\mathfrak{a}$, é também $ab=cd+ca''+a'd+a'a''=cd+a'''$, com a''' e $\mathfrak{a}$. 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 e $\mathfrak{A}$ fizermos corresponder a classe $a+\mathfrak{a}$, o homomorfismo $\mathfrak{A}\sim\mathfrak{A}/\mathfrak{a}$, que reconhecemos na Teoria dos Grupos, é homomorfismo no sentido anular, que lhe atribuímos neste número. Pondo $a+\mathfrak{a}=\bar{a}$, vê-se que $a\to\bar{a}, b\to\overline{b}, ab\to\bar{a}+\overline{b}=\bar{a}+\overline{b}, ab\to\bar{a}\,\overline{b}=\bar{a}\,\overline{b}$. Tem lugar o teorema a seguir, conhecido sob o nome de *teorema da homomorfia para Anéis:*

TEOREMA 20: — *Se* $\mathfrak{A}$ *é um anel e* $\mathfrak{A}/\mathfrak{a}=\overline{\mathfrak{A}}$ *é um anel diferença, tem lugar o homomorfismo* $\mathfrak{A}\sim\overline{\mathfrak{A}}=\mathfrak{A}/\mathfrak{a}$; *recìproca-*

mente, se $\mathfrak{A}\sim\overline{\mathfrak{A}}$, *então* $\overline{\mathfrak{A}}$, *a menos de isomorfismo, é um anel diferença.* A 2.ª parte do teorema significa que $\overline{\mathfrak{A}}$ é isomorfo, no sentido anular, dum certo anel diferença: $\overline{\mathfrak{A}}\simeq\mathfrak{A}/\mathfrak{a}$. A 1.ª parte foi já demonstrada.

Seja agora $\overline{\mathfrak{A}}$ imagem homomorfa de $\mathfrak{A}$ e tomemos o submódulo $\mathfrak{a}$, de $\mathfrak{A}$, determinado no sentido da Teoria dos Grupos, tal que $\overline{\mathfrak{A}}\simeq\mathfrak{a}/\mathfrak{a}$. Trata-se de ver que $\mathfrak{a}$ é um ideal bilateral e que o isomorfismo anterior também faz corresponder ao produto $\bar{a}\,\overline{b}$ o produto $(a+\mathfrak{a})(b+\mathfrak{a})$, das classes correspondentes.

De facto, $\mathfrak{a}$ é caracterizado por conter todos os elementos que, no homomorfismo $\mathfrak{A}\sim\overline{\mathfrak{A}}$, têm zero como correspondente. Então, se a e $\mathfrak{a}$, também ar, sa e $\mathfrak{a}$, porque, sendo, naquele homomorfismo, $a\to\bar{a}, r\to\overline{r}$, etc., é igualmente

$$\begin{aligned} ar&\to\bar{a}\,\overline{r}=\overline{o}\,.\,\overline{r}=\overline{o},\\ sa&\to\overline{s}\,\bar{a}=\overline{s}\,.\,\overline{o}=\overline{o},\end{aligned}\qquad(\overline{o}=\text{zero de }\overline{\mathfrak{A}}).$$

Assim, $\mathfrak{a}$ é ideal bilateral. Na correspondência biunívoca, conhecida da Teoria dos Grupos, entre $\overline{\mathfrak{A}}$ e $\mathfrak{A}/\mathfrak{a}$, tem-se também $\bar{a}\,\overline{b}=(a+\mathfrak{a})(b+\mathfrak{a})$, em virtude do seguinte: dado $\bar{a}$, passa-se a $a+\mathfrak{a}$, procurando a e $\mathfrak{A}$ tal que, no homomorfismo $\mathfrak{A}\sim\overline{\mathfrak{A}}$, seja $a\to\bar{a}$; então, supondo $b\to\overline{b}$, como se tem $ab\to\bar{a}\,\overline{b}$, passa-se de $\bar{a}\,\overline{b}$ a $ab+\mathfrak{a}=(a+\mathfrak{a})(b+\mathfrak{a})$. O teorema da homomorfia está completamente provado.

O ideal bilateral $\mathfrak{a}$, acabado de determinar, diz-se *núcleo* do homomorfismo $\mathfrak{A}\sim\overline{\mathfrak{A}}$.

6) **Relações de congruência** — Suponhamos que, num anel $\mathfrak{A}$, é dada uma relação de equivalência $a\leqslant b$, segundo a qual: 1) de $a\leqslant b, c\leqslant d$, deduz-se $a+c\leqslant b+d$; 2) de $a\leqslant b, c\leqslant d$ deduz-se $ac\leqslant bd$; então, a relação de equivalência diz-se uma *relação de congruência.*

Por ex., se $\mathfrak{a}$ for um ideal bilateral, a equivalência de classes, definida por meio de $\mathfrak{a}$, [$a\leqslant b$, se b e $a+\mathfrak{a}$], é uma congruência. As classes associadas $a+\mathfrak{a}$ dizem-se também *classes residuais,* e, de acordo com notações e designações anteriores,

escreve-se $b \equiv a\,(\mathfrak{a})$, para significar que b e a são *côngruos módulo* $\mathfrak{a}$. Para completa justificação deste modo de escrever, vamos provar este

TEOREMA 21: — *Toda a relação de congruência num anel* $\mathfrak{A}$ *é uma relação de equivalência definida por um ideal bilateral* $\mathfrak{a}$. Como a relação de congruência é de equivalência, consideremos, em $\mathfrak{A}$, a classe A_o dos equivalentes a zero. Se for $o \leqslant a_o$, como é $-a_o \leqslant -a_o$, da condição 1), de congruência, tira-se $-a_o \leqslant o$; e, da condição 2), conclui-se $o \leqslant a_o r$, $o \leqslant a_o s$, se $o \leqslant a_o$. Por isso, $A_o = \mathfrak{a}$ é um ideal bilateral. A demonstração do teorema resultará, provando-se agora os dois factos seguintes: 1.° — todos os elementos de $a + \mathfrak{a}$ estão contidos numa classe de equivalência A; 2.° — toda a classe de equivalência A está contida numa classe $a + \mathfrak{a}$.

O 1.° facto é imediato: se $a \in A$, é $a + \mathfrak{a} \subseteq A$, como se conclui pela condição 1). Quanto ao 2.° facto, consideremos A e suponhamos $a \in A$. Vamos ver que, tendo-se $b \in A$, é também $b \equiv a + \mathfrak{a}$. Das relações $a \leqslant b$, $-a \leqslant -a$, tira-se, sempre por 1), $o \leqslant b - a$, pelo que $b - a \in \mathfrak{a}$, como se deseja.

7) **Anéis cocientes** — Neste § é essencial supor-se que $\mathfrak{A}$ é um anel comutativo.

Ponhamos de parte, em $\mathfrak{A}$, um conjunto $\mathfrak{M}$ de elementos que não são divisores de zero. Admitamos mais que $\mathfrak{M}$ é fechado relativamente ao produto definido em $\mathfrak{A}$. No que vai seguir-se serão utilizados símbolos do tipo (a, b), nos quais se compreenderá sempre ser $a \in \mathfrak{A}$, $b \in \mathfrak{M}$.

Tomemos o conjunto $\mathfrak{C}$ dos símbolos (a, b) e introduzamos no conjunto a relação de equivalência seguinte: $(a, b) \leqslant (c, d)$, quando $a\,d = b\,c$. 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

$$\begin{aligned} [a, b] + [c, d] &= [a\,d + b\,c,\ b\,d], \\ [a, b] \,.\, [c, d] &= [a\,c,\ b\,d]. \end{aligned} \qquad (1)$$

A coerência destas definições exige: 1.° — que os resultados da soma e do produto sejam classes de $\mathfrak{S}$; 2.° — 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 ex., $[a, b] = [a', b']$, ou seja $a\,b' = b\,a'$. Então, $[a', b'] + [c, d] = [a'\,d + b'\,c,\ b'\,d]$, tornando-se necessário provar que é $[a\,d + b\,c,\ b\,d] = [a'\,d + b'\,c,\ b'\,d]$, ou seja que se tem $(a\,d + b\,c)\,b'\,d = b\,d\,(a'\,d + b'\,c)$. 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 detalhemos a verificação dos postulados.

O elemento zero é $[o, c]$, 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 ex., resulta deste modo: se $[a\,c, c] = O = [o, c]$, então $a\,c\,c = c.o = o$, o que exige $a = o$. Podemos dizer:

TEOREMA 22: — *Suponhamos* $\mathfrak{A}$ *um anel comutativo e* $\mathfrak{M}$ *um conjunto de elementos de* $\mathfrak{A}$ *que não são divisores de zero e 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»*.

Se, em particular, $\mathfrak{A}$ for um domínio de integridade e tomarmos para $\mathfrak{M}$ todos os elementos de $\mathfrak{A}$, salvo zero, podemos mostrar que $\mathfrak{S}$ é um corpo. Na verdade, seja $[a, b] \in \mathfrak{S} = \mathfrak{K}$. Se supomos $a \neq o$, é $[a, b] \neq o$. Tem sentido escrever $[b, a]$ e é $[a, b].[b, a] = [a\,b, a\,b] = [b, b] =$ elemento um de $\mathfrak{K}$. Todos os elementos não nulos de $\mathfrak{K}$ têm inverso, pelo que $\mathfrak{K}$ é um corpo. Logo:

TEOREMA 23: — *Todo o domínio de integridade se pode «mergulhar» num corpo.*

Em correlação com os raciocínios acabados de expor, demonstraremos aqui este

TEOREMA 24: — *Todo o semi-grupo comutativo se pode mergulhar num grupo abeliano.* Dado o semi-grupo $\mathfrak{T} = \{a, b, c, \ldots\}$, basta considerar o conjunto $\mathfrak{C}_0$ de símbolos (a, b) e definir em $\mathfrak{C}_0$ a relação de equivalência seguinte: $(a, b) \simeq (c, d)$, se, e só se, $ad = bc$. Então, com efeito, o conjunto $\mathfrak{C}$, das classes correspondentes, algebrizado pelo produto

$$[a, b].[c, d] = [ac, bd]$$

passa a ser um grupo abeliano contendo uma parte isomorfa de $\mathfrak{T}$. A cada $b \in \mathfrak{T}$, devemos fazer corresponder $[ab, a] \in \mathfrak{C}$. Também podemos observar que se resolve a equação $[a, b].[x, y] = [c, d]$, pondo $[x, y] = [bc, ad]$.

§ 3 — Anéis de polinómios

1) **Definição geral** — Estreitamente ligada com a teoria das ampliações dum anel, e muito especialmente com o caso 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:

$$\begin{vmatrix} a_{00} & a_{01} & a_{02} & \ldots \\ a_{10} & a_{11} & a_{12} & \ldots \\ a_{20} & a_{21} & a_{22} & \ldots \\ \ldots\ldots & \ldots\ldots & & \end{vmatrix} \qquad (2)$$

Suporemos que há apenas um número finito de elementos $a_{\lambda\mu}$ diferentes do elemento zero de $\mathfrak{A}$.

Definamos, no conjunto dos quadros, um preceito de soma e outro de produto, pondo:

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 $a_{\lambda\mu}$;

para o produto: $c_{\lambda\mu} = \Sigma a_{mp} b_{qr}$, estendendo o somatório a m, p, q, r, tais 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 para os quais $M + N$ e $Q + R$ tenham valores máximos, todos os $c_{\lambda\mu}$, tais que $\lambda + \mu$ exceda em uma unidade, pelo menos, a soma daqueles dois máximos, são nulos. O conjunto dos quadros (2) 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

$$\begin{vmatrix} a_{00} & o & o & \ldots \\ o & o & o & \ldots \\ \ldots\ldots & \ldots\ldots & & \end{vmatrix}, \qquad (3)$$

os quais, por soma e produto, dão ainda elementos da mesma forma. Substituindo, em $\mathfrak{B}$, estes elementos (3) 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:

$$\begin{vmatrix} o & o & \ldots \\ a_{10} & o & \ldots \\ o & o & \ldots \\ \ldots\ldots & & \end{vmatrix} = a_{10}\, x, \qquad \begin{vmatrix} o & a_{01} & o & \ldots \\ o & o & o & \ldots \\ \ldots\ldots & & & \end{vmatrix} = a_{01}\, y,$$

$$\begin{vmatrix} o & o & o & \ldots \\ o & a_{11} & o & \ldots \\ o & o & o & \ldots \\ \ldots\ldots & & & \end{vmatrix} = a_{11}\, xy, \qquad \begin{vmatrix} a_{00} & a_{01} & o & \ldots \\ a_{10} & a_{11} & o & \ldots \\ o & o & o & \ldots \\ \ldots\ldots & & & \end{vmatrix} = a_{00} + a_{10}\, x + a_{01}\, y + a_{11}\, xy,$$

conforme regras que fàcilmente se reconhecem. A nova representação é coerente, pois que a operação de soma expressa pelo sinal $+$, que ela introduz, é a mesma que a que foi prèviamente introduzida em $\mathfrak{B}'$. Utilizaremos, assim, a notação

$$\sum_{i,j=o}^{\infty} a_{ij}\, x^i\, y^j, \qquad (a_{ij} \in \mathfrak{A}), \tag{4}$$

onde apenas um número finito de «coeficientes» a_{ij} se supõem diferentes de zero.

A regra de produto leva aqui à igualdade

$$\sum_{m,p=o}^{\infty} a_{mp}\, x^m y^p \,.\, \sum_{q,r=o}^{\infty} b_{qr}\, x^q y^r = \sum_{\lambda,\mu=o}^{\infty} c_{\lambda\mu}\, x^\lambda y^\mu,$$

com $m+q=\lambda$, $p+r=\mu$, como acima se viu.

Conclui-se deste modo que o uso dos símbolos (4), à semelhança do que se passa na Álgebra clássica, implica a comutabilidade das «indeterminadas» x e y, assim como a comutabilidade destas com os elementos a_{ij}.

A justificação do vocábulo «indeterminadas», com que se designaram x e 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 uma equação do tipo

$$\sum_{h=o}^{\infty} a_h\, x^h = o, \quad \text{ou} \quad \sum_{h=o}^{\infty} a_h\, y^h = o,$$

salvo no caso banal de todos os a_h serem nulos. É o que se exprime 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

$$\sum_{h,j=o}^{\infty} a_{hj}\, x^h\, y^j = \sum_{h,j=o}^{\infty} b_{hj}\, x^h\, y^j,$$

a 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 (4)

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 (4), mas de todos os elementos da forma (4). Ele representa uma ampliação autêntica de $\mathfrak{A}$, suposto $\mathfrak{A} \neq (o)$.

O que acabamos de dizer para x e y diz-se para n indeterminadas quaisquer, $x_1, x_2, \ldots, x_n$. O anel ampliado correspondente representa-se por $\mathfrak{A}[x_1, x_2, \ldots, x_n]$ e os elementos do mesmo têm a representação unívoca

$$\sum_{k_1,\ldots,k_n=o}^{\infty} a_{k_1\ldots k_n}\, x_1^{k_1} \ldots x_n^{k_n}, \tag{5}$$

onde há apenas um número finito de coeficientes $a_{k_1\ldots k_n}$ que são diferentes de zero e $\mathfrak{A}$.

2) **Construção de $\mathfrak{A}[x_1, \ldots, x_n]$ por adjunções sucessivas** — O anel $\mathfrak{A}[x_1, \ldots, x_n]$ pode, como vamos ver, construir-se por adjunções anulares transcendentes sucessivas, pondo

$$\mathfrak{A}_1 = \mathfrak{A}[x_1],\ \mathfrak{A}_2 = \mathfrak{A}_1[x_2],\ \ldots,\ \mathfrak{A}_n = \mathfrak{A}_{n-1}[x_n].$$

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

$$P_n = \sum_{k_n=o}^{\infty} A_{k_n} x_n^{k_n},$$

com

$$A_{k_n} = \sum_{k_1,\ldots,k_{n-1}=o}^{\infty} a^{k_n}_{k_1\ldots k_{n-1}}\, x_1^{k_1} \ldots x_{n-1}^{k-1},$$

ou seja da forma

$$P_n = \sum_{k_n=o}^{\infty} \Big[\sum_{k_1,\ldots,k_{n-1}=o}^{\infty} a^{k_n}_{k_1\ldots k_{n-1}}\, x_1^{k_1} \ldots x_{n-1}^{k_{n-1}} \Big] x_n^{k_n} =$$

$$= \sum_{k_n} \Big[\sum_{k_1,\ldots,k_{n-1}} a_{k_1\ldots k_n} x_1^{k_1} \ldots x_{n-1}^{k_{n-1}} \Big] x_n^{k_n}, \tag{6}$$

pondo $a_{k_1 \dots k_n} = a^{k_n}_{k_1 \dots k_{n-1}}$. Ora há uma correspondência biunívoca completa entre os elementos (6) e os elementos de $\mathfrak{A}[x_1, \dots, x_n]$. A identidade dos anéis construídos deve ser entendida precisamente no sentido do isomorfismo anular: $\mathfrak{A}[x_1, \dots, x_n] \simeq \mathfrak{A}_n$.

É ainda ao 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 for alterada.

3) **Algumas propriedades dos polinómios** — Suponhamos uma única indeterminada x. É válido o seguinte

TEOREMA 25: — *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 $\overline{|a_0\ a_1 \dots a_n \dots}$, ponhamos $\overline{|a_0\ a_1 \dots a_n \dots} \cdot \overline{|b_0\ b_1 \dots b_n \dots} = o$. Se a_p e b_q forem, respectivamente, os últimos elementos de $\mathfrak{A}$ que não são nulos nos dois factores, o produto $\overline{|c_0\ c_1 \dots c_r \dots}$ desses factores contém o elemento

$$c_{p+q} = a_{p+q} b_o + \dots + a_p b_q + \dots + a_o b_{p+q} = a_p b_q \neq o ,$$

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 $P(y) = a_0 + a_1 y + \dots + a_n y^n$, no qual se põe em evidência o último coeficiente $a_n \neq o$. O número n diz-se *grau* de $P(y)$.

No que vai seguir-se, tratando-se com polinómios de uma 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 26: — *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 $\mathfrak{A}_1, \dots, \mathfrak{A}_n$ são sucessivamente construídos a partir de domínios de integridade, segue-se que $\mathfrak{A}_n = \mathfrak{A}[x_1, \dots, x_n]$ é um domínio de integridade não comutativo, se $\mathfrak{A}$ for um domínio de integridade não comutativo.

No caso dos polinómios de muitas indeterminadas, o *grau* avalia-se como habitualmente. O polinómio nulo tem sempre, porém, o grau $-\infty$.

Um polinómio diz-se *homogéneo,* quando todos os seus termos são do mesmo grau. Um polinómio qualquer é sempre uma soma de polinómios homogéneos. Tem-se:

TEOREMA 27: — *O produto de dois polinómios homogéneos de graus* m *e* n *é um polinómio homogéneo do grau* m + n, *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 $\neq o$. 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 26 é válido para os polinómios de* $\mathfrak{A}[x_1, \dots, x_n]$.

Quando o anel inicial 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 $(a_o x_1)^{-1}$, por ex., não existe em $\mathfrak{A}_n$, pois

$$\frac{u}{a_o x_1} = \sum_{k_1, \dots, k_n = o}^{\infty} a_{k_1 \dots k_n} x_1^{k_1} \dots x_n^{k_n} .$$

levaria a

$$u = \sum_{k_1, \ldots, k_n = o} a_o\, a_{k_1 \ldots k_n}\, x_1^{k_1+1} \ldots x_n^{k_n},$$

igualdade que é impossível, pelo facto de não haver no 2.º membro termo que não contenha x_1.

4) **Os polinómios 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 $m \leqq n$, 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 ainda as *divisões à direita e à esquerda,* no sentido que vai precisar-se para uma divisão à direita. Ponhamos

$$P(x) = a_o x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n,$$
$$D(x) = b_o x^m + b_1 x^{m-1} + \ldots + b_{m-1} x + b_m.$$

Por hipótese, é $a_o \neq o$ e existe b_o^{-1}. Provaremos ser possível, e duma só maneira, escrever

$$P(x) = Q_d(x) \,.\, D(x) + R_d(x), \qquad (7)$$

onde $R_d(x)$ é um polinómio de grau inferior a m.

Admitamos a possibilidade de (7). Uma segunda possibilidade levaria a $P(x) = Q'_d(x) \,.\, D(x) + R'_d(x)$, deduzindo-se $o = (Q_d(x) - Q'_d(x)) \,.\, D(x) + (R_d(x) - R'_d(x))$, ou seja $(Q'_d(x) - Q_d(x)) \,.\, D(x) = R_d(x) - R'_d(x)$. Sendo $Q'_d(x) \neq Q_d(x)$, o grau do 1.º membro da última igualdade 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 (7). Tem-se

$$P(x) - a_o\, b_o^{-1} x^{n-m} D(x) = P_{n-1}(x), \qquad (8)$$

onde o polinómio do 2.º membro é, quando muito, do grau $n-1$. Se $n-1 \geqq m$ e se, por ex., o coeficiente do termo do grau $n-1$ de P_{n-1} é c_{n-1}, a diferença

$$P_{n-1}(x) - c_{n-1}\, b_o^{-1} x^{n-m-1} D(x) = P_{n-2}(x) \qquad (8')$$

é, quando muito, do grau $n-2$. O processo continua até se chegar a $P(x) - (a_o\, b_o^{-1} x^{n-m} + c_{n-1}\, b_o^{-1} x^{n-m-1} + \ldots + d) \,.\, D(x) = R_d(x)$, onde $R_d(x)$ é o segundo membro da última igualdade a escrever, análoga a (8) e (8'), a qual é obtida logo que o grau respectivo seja $< m$, Será $Q_d(x) = a_o\, b_o^{-1} x^{n-m} + \ldots + d$, podendo ter-se $d = o$.

Na divisão à esquerda, a igualdade (7) é substituída por

$$P(x) = D(x) \,.\, Q_e(x) + R_e(x).$$

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

$$x^n - b^n = (x^{n-1} + b\, x^{n-2} + \ldots + b^{n-2} x + b^{n-1})(x - b),$$
$$x^n - b^n = (x - b)(x^{n-1} + b\, x^{n-2} + \ldots + b^{n-2} x + b^{n-1}).$$

Tem-se, então,

$$P(x) = a_o x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a^n,$$
$$R_d(x) = a_o b^n + a_1 b^{n-1} + \ldots + a_{n-1} b + a^n,$$

como se vê efectuando a diferença

$$P(x) - R_d(x) = a_o (x^n - b^n) + a_1 (x^{n-1} - b^{n-1}) + \ldots + a^{n-1}(x - b) = (a_o x^{n-1} + \ldots)(x - b).$$

Vê-se anàlogamente que é

$$R_e(x) = b^n a_o + a_1 b^{n-1} + \ldots + b\, a_{n-1} + a_n.$$

Convém fazer uma observação. Se $D(x)$ se reduzir a $b_m = b_o$ (sempre sob a hipótese de existir b_o^{-1}), o resto de qual-

quer das divisões é zero. O respectivo grau será $-\infty < 0$, sendo zero o grau de $D(x)$. E podemos dizer:

TEOREMA 28: — *Supondo* $\mathfrak{D}$ *um anel de divisão, há sempre algoritmo de divisão em* $\mathfrak{D}[x]$.

No número próximo daremos certos pormenores relativos ao caso em que $\mathfrak{D} = \mathfrak{K}$ é um corpo. Evidentemente que, então, como em geral, sempre que $\mathfrak{A}$ é comutativo, não se distinguem a divisão à direita e à esquerda.

5) **O algoritmo de divisão em** $\mathfrak{K}[x]$ — Como dissemos já, trata-se neste número do algoritmo de divisão em $\mathfrak{K}[x]$, suposto $\mathfrak{K}$ um corpo. Na verdade, vamos reencontrar o resultado anterior por um método diferente, que lembra o algoritmo de divisão da teoria dos inteiros.

Se forem $P, Q \in \mathfrak{K}[x]$, diz-se que Q é *divisor* ou *está contido* em P, e que este último é *múltiplo* de Q ou que *contém* Q, se existir $D \in \mathfrak{K}[x]$ tal que $P = QD$. O domínio de integridade $\mathfrak{K}[x]$ contém elemento um, que é $u \in \mathfrak{K}$. Esse elemento é divisor de todos os polinómios; e existe um elemento, o elemento nulo, que é divisível por todos os polinómios. [A divisão por zero, mesmo no caso de ser $P(x) = o$, não se considera]. Um polinómio é sempre divisível por si mesmo.

Um elemento $E \in \mathfrak{K}[x]$ diz-se uma *unidade,* conforme designação já introduzida no n.º 3 do § 1, se tiver inverso E^{-1}. De $EE^{-1} = u$, conclui-se ser E um divisor de u. Inversamente, um divisor de u, é uma unidade. O inverso duma unidade é uma unidade.

Um elemento Q diz-se *associado* de P, se for $P = QE$. Então é também $Q = PE^{-1}$, pelo que a noção de elementos associados é recíproca.

Diz-se que Q é um divisor *autêntico* de P, se for $P = QR$, sem que R seja uma unidade. Neste caso, P não pode ser divisor de Q.

Um elemento P 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 autênticos que não sejam unidades.

Se uma unidade se decompõe num produto, os diferentes factores são unidades. A definição dada de elemento primo diz, então, que as unidades são elementos primos. Em geral, porém, não se consideram como tal e designam-se simplesmente por unidades.

Posto isto, vamos dar uma noção de *valor absoluto* em $\mathfrak{K}[x]$. Se for $P \in \mathfrak{K}[x]$, representaremos pelo símbolo $|P|$ o seu valor absoluto. Então, tomemos um inteiro fixo $v > 1$ e introduzamos as definições seguintes: 1) $|P| = 0$, se $P = o$; 2) $|P| = v^n$, se n é o grau do polinómio $P \neq o$. Com estas definições, prova-se:

$$|P| = 0, \text{ se } P = o; \quad |P| \geqq 1, \text{ se } P \neq o;$$
$$|P \pm Q| \leqq |P| + |Q|; \quad |PQ| = |P| . |Q|.$$

Para o elemento $u \in \mathfrak{K}$, tem-se $P = Pu$, de sorte que $|u| = 1$. Duma maneira geral, tendo em conta que $EE^{-1} = u$, é válido o

TEOREMA 29: — *É condição necessária e suficiente, para que um elemento de* $\mathfrak{K}[x]$ *seja uma unidade, que ele pertença a* $\mathfrak{K}$. É claro que neste enunciado se ressalva o elemento zero.

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 $\neq o$ 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.* Utilizaremos mais tarde estas noções.

TEOREMA 30: — *Dados* P *e* $D \neq o$; *existe sempre a possibilidade de se escrever* $P = DQ$, *com* $|R| < |D|$, *e, de facto, uma*

única possibilidade. Consideremos o conjunto dos polinómios $\Delta = P - D\,T$, onde T é um polinómio arbitrário. Nesse conjunto há elementos de valor absoluto mínimo. Se, para $T = Q$, se obtém um tal elemento $R = P - D\,Q$, o grau r, de R, é necessàriamente inferior ao grau m, de D. Se pudesse ser $r \geqq m$, representando por d_r e c_m os coeficientes dos termos de mais alto grau dos polinómios R e D, o elemento $\frac{d_r}{c_m} x^{r-m}$ daria

$$R - \frac{d_r}{c_m} x^{r-m} \,.\, D = P - D\,(Q + \frac{d_r}{c_m} x^{r-m}).$$

O polinómio do 2.º membro é da forma $P - D\,T$, tendo um grau inferior ao grau de R. Conclui-se, pois, $r < m$, ou seja $|R| < |D|$, e a decomposição aludida no teorema fica demonstrada.

Quanto à univocidade da mesma decomposição, imaginemos que era possível ter-se

$$\begin{cases} P = D\,Q + R, \\ |R| < |D|, \end{cases} \qquad \begin{cases} P = D\,Q' + R', \\ |R'| < |D|. \end{cases}$$

Concluir-se-ia $D\,(Q - Q') = R' - R$, de sorte que D dividiria a diferença $R' - R$. Se fosse $R' \neq R$, seria $|D| \leqq |R' - R|$. Como, por outro lado, o grau duma diferença é, quando muito, o grau do mais alto dos graus dos respectivos polinómios, seria também $|R' - R| < |D|$, que é uma conclusão a contradizer a anterior. Será, assim, $R' = R$, e, consequentemente $Q' = Q$.

OBSERVAÇÃO: — Pode observar-se que o algoritmo de divisão aqui introduzido é, na verdade, o mesmo que o do número anterior. Em particular, se $D = E$ é uma unidade, tem-se $P = D.D^{-1}P + o$, com $|o| = 0 < |D| = 1$.

A teoria do *máximo divisor comum* (m. d. c.) é agora muito fácil de fazer. Dados dois elementos não simultâneamente nulos

P, S e $\mathfrak{R}[x]$, diz-se m. d. c. daqueles dois polinómios um polinómio D, satisfazendo às três igualdades seguintes:

$$P = D\,Q, \qquad S = D\,Q', \qquad P\,R + S\,T = D, \tag{9}$$

para certos Q, Q', R, T e $\mathfrak{R}[x]$. Se um tal elemento D existe, ele divide os dois elementos P e S e goza da propriedade de ser divisível por todo o divisor comum de P e S. Note-se desde já que, determinado D por forma a verificar (9), também $D\,E$ verifica relações análogas a (9). Por isso, no que vai seguir-se, exigir-se-á que D seja normado. Provaremos, então, que as 3 condições (9) determinam D univocamente.

Sirvamo-nos do *algoritmo de Euclides,* pondo sucessivamente, se $S \neq o$ é um polinómio de valor absoluto não superior ao de $P \neq o$,

$$\begin{aligned} P &= S\,Q_1 + R_1, & |R_1| &< |S|, \\ S &= R_1\,Q_2 + R_2, & |R_2| &< |R_1|, \\ R_1 &= R_2\,Q_3 + R_3, & |R_3| &< |R_2|, \\ &\cdots\cdots\cdots\cdots & &\cdots\cdots\cdots \end{aligned}$$

$$\begin{aligned} R_{s-3} &= R_{s-2}\,Q_{s-1} + R_{s-1}, & |R_{s-1}| &< |R_{s-2}|, \\ R_{s-2} &= R_{s-1}\,Q_s, \end{aligned}$$

até se chegar a um resto $R_s = o$. Esse facto realizar-se-á necessàriamente, pois o valor absoluto dos restos vai decrescendo constantemente. Vamos ver, em seguida, que o último divisor R_{s-1} satisfaz às condições (9). Em primeiro lugar, R_{s-1} divide $R_{s-2}, R_{s-3}, \ldots, R_1, S, P$. Depois, para se chegar a $P\,R + S\,T = D$, basta notar a sucessão seguinte:

$$P - S\,Q_1 = R_1,$$

$$S = (P - S\,Q_1)\,Q_2 + R_2, \quad \text{ou} \quad -P\,Q_2 + S\,(Q_1\,Q_2 + u) = R_2,$$

$$P - S\,Q_1 = (-P\,Q_2 + S\,Q_1\,Q_2 + S)\,Q_3 + R_3$$

ou

$$P\,(u + Q_2\,Q_3) - S\,(Q_1 + Q_1\,Q_2\,Q_3 + Q_3) = R_3,$$

etc.. Chega-se, finalmente, a uma igualdade que contém P, S, R_{s-1} e que é do tipo desejado.

Se, agora, D e D_1 forem dois elementos normados satisfazendo a (9), de (9) e de $P = D_1 Q_1$, $S = D_1 Q'_1$, $P R_1 + S T_1 = D_1$, tira-se

$$\mathrm{D}(Q R_1 + Q' T_1) = D_1, \qquad D_1(Q_1 R + Q'_1 T) = D,$$

e, consequentemente,

$$|D| \gtrless |D_1|, \quad |D_1| \gtrless |D|, \quad |D| = |D_1|,$$
$$|Q R_1 + Q' T_1| = |Q_1 R + Q'_1 T|.$$

Assim, será $D = D_1 E$, onde $E \in \mathfrak{R}$. Sob a condição de D e D_1 serem normados, é $D = D_1$.

Quando um dos polinómios P ou S é nulo, por ex., $S = o$, o m. d. c. é o polinómio P.

Para significar que D é máximo divisor comum de P e S, escreve-se frequentemente $D = (P, S)$. É válido este interessante

TEOREMA 31: — *O máximo divisor comum* $\mathrm{D} = (\mathrm{P}, \mathrm{S})$, *suposto normado, é o elemento normado de valor absoluto mínimo entre os polinómios da forma* $\mathrm{P}\tau + \mathrm{S}\tau^*$, *onde* $\tau, \tau^* \in \mathfrak{R}[\mathrm{x}]$. Se P ou S é nulo, o teorema é imediato. O m. d. c. será PE, suposto normado. Vamos admitir P e S diferentes de zero. Tomemos, então, R e T, no lugar de τ e τ^*, de modo a satisfazer à condição de mínimo em causa, e ponhamos $D = PR + ST$. Isto é possível, pelo facto de existirem sempre elementos normados da forma em questão: se $S \neq o$ e Sa for normado, basta tomar $Sa = P.o + S.a$. O elemento D, acabado de obter, é divisor de P, como vamos provar. Em primeiro lugar, um polinómio normado bP, com $b \in \mathfrak{R}$, entra na expressão geral $P\tau + S\tau^*$. Por esse facto, o grau de D não é superior ao grau de P. Se, agora, D não dividisse P, seria $P = D Q_1 + R_1$, com $|R_1| < |D|$. Então, supondo $k R_1$ normado, ter-se-ia $k R_1 = k P - k D Q_1 = k P - k(PR + ST) Q_1 = P(k - k R Q_1) + S(-k T Q_1)$. Sob esta forma, tinha-se um elemento normado $k R_1$, de valor absoluto $|k R_1| = |R_1| < |D|$, dentro da expressão geral $P\tau + S\tau^*$, o que é absurdo. De mesmo modo se demonstraria que D divide S. O teorema fica provado.

§ 4 — Sobre a Teoria dos Corpos

1) **Estrutura dos corpos primos** — A teoria geral dos corpos ficará para mais tarde. Neste § limitamo-nos a ligeiras indicações de uso muito corrente.

Dado um corpo $\mathfrak{K}$, consideremos o seu corpo primo $\mathfrak{P}$. Dissemos já, (§ 2, n.º 1), que, em $\mathfrak{P}$, estão todos os elementos do domínio de integridade $\mathfrak{I}_o = \{mu\}$, onde m percorre os inteiros. $\mathfrak{P}$ contém igualmente o corpo cociente $\mathfrak{D}$, de $\mathfrak{I}_o$, de sorte que é necessàriamente $\mathfrak{P} = \mathfrak{D}$. Duas hipóteses se sugerem: a correspondência $\mathfrak{I} \sim \mathfrak{I}_o$, onde $\mathfrak{I}$ é o anel dos inteiros, ou é um homomorfismo ou um isomorfismo. No primeiro caso, há elementos $m \neq 0$ para os quais $mu = o$, elementos que constituem um ideal de $\mathfrak{I}$. E tem-se $\mathfrak{I}_o \simeq \mathfrak{I}/\mathfrak{a}$, se $\mathfrak{a}$ é esse ideal. Como $\mathfrak{a}$ é um grupo cíclico, designemos por p o menor elemento positivo que contém, de sorte que $\mathfrak{a} = (p)$. Se q e q' são dois inteiros positivos inferiores a p, o produto qq' não pode ser dividido por p, visto que, se o fosse, tinha-se $qq'u = kpu = o = qu.q'u$, o que daria uma das igualdades $qu = o$, $q'u = o$, pelo menos, contra o facto de ser p o gerador de $\mathfrak{a}$. Isto significa que p é um número primo. O anel diferença $\mathfrak{I}/(p)$ é um corpo de p elementos, como passamos a demonstrar. Tendo-se $\mathfrak{I}/(p) = \{(p), 1 + (p), \ldots, p - 1 + (p)\}$, provaremos que todos os elementos têm inverso. Seja $o < m < p$. Os produtos mm', onde $m' = 1, 2, \ldots, p - 1$, divididos por p, dão todos restos diferentes, pois, se pudesse ter-se, com $m'_1 \neq m'_2$,

$$mm'_1 = h_1 p + r_1, \qquad mm'_2 = h_2 p + r_1,$$

ter-se-ia também $m(m'_1 - m'_2) = (h_1 - h_2) p$, e p dividiria $m'_1 - m'_2$, o que é absurdo. Como p não entra num produto

mm', nenhum resto é nulo. Os restos são $1, 2, \ldots, p-1$, pelo que, sendo, por ex., $mm'' = hp+1$, os elementos $m+(p)$ e $m''+(p)$ são inversos, como se deseja. Do isomorfismo $\mathfrak{J}_0 \simeq \mathfrak{J}/\mathfrak{a}$, segue-se que o domínio de integridade $\mathfrak{J}_0$ é o corpo primo procurado. Quanto ao número p, trata-se da característica de $\mathfrak{K}$, no sentido geral definido no n.º 1 do § 1.

Passemos à 2.ª hipótese. Nesse caso tem-se $\mathfrak{J} \simeq \mathfrak{J}_0$, pelo que $\mathfrak{P}$ será isomorfo do corpo cociente de $\mathfrak{J}$, ou seja do corpo dos números racionais. É válido o

TEOREMA 32: — *Um corpo primo ou é isomorfo do corpo dos números racionais ou do corpo* $\mathfrak{J}(p)$, *onde* $\mathfrak{J}$ *é o anel dos inteiros e* p *é um número primo.*

Pode observar-se que as considerações que precederam o teorema anterior também provam ser zero ou um número primo a característica de todo o domínio de integridade com elemento u.

A noção de característica permite deduzir um certo número de regras que representam algumas singularidades no comportamento das operações elementares dentro do domínio de integridade $\mathfrak{A}$ com elemento um. Assim:

1.ª — Se a característica é p, a igualdade $ma = na$, com $o \neq a \in \mathfrak{A}$, dá $m \equiv n\,(p)$, e recìprocamente.

2.ª — Se a característica é p, tem lugar a igualdade

$$(\sum_{i=1}^{n} a_i)^p = \sum_{i=1}^{n} a_i^p, \qquad (a_i \in \mathfrak{A}),$$

que se prova por indução. De facto, para dois elementos, tem-se

$$(a_1+a_2)^p = a_1^p + \binom{p}{1} a_1^{p-1} a_2 + \ldots + \binom{p}{r} a_1^{p-r} a_2^r + \ldots + a_2^p,$$

com $p(p-1)\ldots(p-r+1) = \binom{p}{r}.1.2\ldots r$. Como é $r < p$, o número primo p só pode entrar em factor em $\binom{p}{r}$, de modo

que, no desenvolvimento de $(a_1+a_2)^p$ todas as parcelas intermédias são nulas, tendo-se apenas $(a_1+a_2)^p = a_1^p + a_2^p$. A indução é agora imediata.

3.ª — Se a característica é p, também se têm as igualdades $(a-b)^p = a^p - b^p$ e $(a-b)^{p-1} = a^{p-1} + b\,a^{p-2} + \ldots + b^{p-2}a + b^{p-1}$: Esta última prova-se tendo em conta que

$$(a-b)(a^{p-1}+b\,a^{p-2}+\ldots+b^{p-2}a+b^{p-1}) = a^p + b\,a^{p-1} + \ldots + b^{p-1}a - b\,a^{p-1} - \ldots - b^{p-1}a - b^p = a^p - b^p = (a-b)^p.$$

2) **Sobre as extensões dum corpo** — Seja Ω um corpo, extensão dum corpo $\mathfrak{K}$. Dado um conjunto $\mathfrak{T}$, de elementos de Ω, há corpos, contidos em Ω, que contêm $\mathfrak{K}$ e $\mathfrak{T}$. A intersecção desses corpos é um corpo mínimo em tais condições. Representá-la-emos 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 lhe aplicar o teorema 15, do n.º 3, § 2, de sorte que $\mathfrak{K}(\mathfrak{T})$ é o conjunto unido 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 uma ideia no número seguinte.

3) **Sobre as extensões simples** — Um tipo de extensão abstracta de $\mathfrak{K}$, chamado *extensão transcendente,* resulta muito fàcilmente dos raciocínios feitos sobre anéis de polinómios e anéis 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 cociente de $\mathfrak{K}[x]$, obtém-se um corpo, que representaremos por $\mathfrak{K}(x)$ e que é uma extensão transcendente *simples* de $\mathfrak{K}$. A designação de «simples» vai-se buscar 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 $\mathfrak{K}(\Theta) = \mathfrak{K}$, que exigirá $\Theta \in \mathfrak{K}$.

Tomemos, de entre os elementos de $\mathfrak{K}(\Theta)$, aqueles que são da forma

$$\sum_{k=o}^{n} a_k \Theta^k = P(\Theta), \qquad (a_k \in \mathfrak{K}).$$

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 $\mathfrak{a} = (o)$, será $\mathfrak{A} \simeq \mathfrak{K}[x]$. Nesta hipótese, o corpo $\mathfrak{K}(\Theta)$, que se identifica sempre com o corpo cociente 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, $\mathfrak{a} \neq (o)$, imaginemos um polinómio $\varphi(x) \in \mathfrak{K}[x]$, não nulo, de grau mínimo, pertencente a $\mathfrak{a}$. Ter-se-á, então, $\varphi(\Theta) = o$. É fácil de ver que $\varphi(x)$ é um polinómio primo. Se $\varphi(x) = ax + b$ é do 1.º 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 $\varphi(\Theta) = \psi(\Theta) \cdot \pi(\Theta) = o$, resultaria $\psi(\Theta) = o$ ou $\pi(\Theta) = o$, contra a hipótese de $\varphi(x)$ ser um polinómio de grau mínimo de correspondente zero no homomorfismo $P(x) \to P(\Theta)$.

O núcleo, $\mathfrak{a}$ conterá o ideal principal $(\varphi(x))$. Vamos ver que é $\mathfrak{a} = (\varphi(x))$. Se $\psi(x)$, de grau igual ou superior ao de $\varphi(x)$, tiver zero como correspondente, escrevendo $\psi(x) = \varphi(x) \cdot q(x) + r(x)$, com $r(x)$ de grau inferior ao de $\varphi(x)$, vê-se que é $r(\Theta) = o$. O polinómio $r(x)$ será nulo e $\psi(x) = \psi(x) \cdot q(x)$, o que demonstra a afirmação. Fica estabelecido deste modo o isomorfismo $\mathfrak{A} \simeq \mathfrak{K}[x]/(\varphi(x))$, sem esquecer que é $\mathfrak{A} \subseteq \mathfrak{K}(\Theta)$. Provaremos em seguida que o anel diferença $\mathfrak{K}[x]/(\varphi(x))$ é um corpo, e que, por consequência, é $\mathfrak{A} = \mathfrak{K}(\Theta)$.

Se quisermos resolver a equação

$$\big(f(x) + (\varphi(x))\big) \cdot \big(Y(x) + (\varphi(x))\big) = \psi(x) + (\varphi(x)),$$

na qual $f(x)$ e $\psi(x)$ são dois polinómios dados, de grau inferior ao de $\varphi(x)$, e $f(x) \notin (\varphi(x))$, comecemos por observar ser

$$\text{m. d. c. } (f(x), \varphi(x)) = u,$$

de modo que existem polinómios $g(x)$ e $h(x)$ tais que $fg + \varphi h = u$. Será, então, $\psi = \psi fg + \psi \varphi h$, pelo que $\psi(x) + (\varphi(x)) = \psi fg + (\varphi(x))$. Bastará fazer $Y(x) = \psi(x) \cdot g(x)$ para resolver a equação em causa.

Neste caso, para o qual se provou ser

$$\mathfrak{A} = \mathfrak{K}(\Theta) \simeq \mathfrak{K}[x]/(\varphi(x)),$$

diz-se que $\mathfrak{K}(\Theta)$ é uma extensão algébrica simples de $\mathfrak{K}$. O grau n do polinómio $\varphi(x)$ diz-se *grau de* Θ *relativamente a* $\mathfrak{K}$. E como podemos supor sempre $\varphi(x)$ um polinómio normado, temos este

TEOREMA 33: — *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* $\varphi(x) = o$. Convém fazer algumas observações. Os elementos do

corpo são da forma $P(x)+(\varphi(x))$, onde $P(x)$ é de grau inferior ao de $\varphi(x)$. Sob forma desenvolvida, tem-se

$$P(x)+(\varphi(x))=a_0 x^r+\ldots+a_{r-1}x+a_r+(\varphi(x))=$$
$$=a_0(x+(\varphi(x)))^r+\ldots+a_{r-1}(x+(\varphi(x)))+a_r+(\varphi(x)).$$

Há, em particular, os elementos $a+(\varphi(x))=\bar{a}\in\mathfrak{K}[x]/(\varphi(x))$ formando um corpo isomorfo de $\mathfrak{K}$. Então, podemos escrever, por ex.,

$$a_0(x+(\varphi(x))^r=(a_0+(\varphi(x)))(x+(\varphi(x)))^r=$$
$$=a_0 x^r+(\varphi(x))=\bar{a}_0(x+(\varphi(x)))^r.$$

Pondo ainda $x+\varphi(x)=\Theta$ e substituindo $\bar{a}$ por a, os elementos de $\mathfrak{K}[x]/(\varphi(x))$ são, efectivamente, polinómios da forma

$$a_0\Theta^r+a_1\Theta^{r-1}+\ldots+a_{r-1}\Theta+a^r,\qquad (r<n),$$

sendo, aliás, $\varphi(\Theta)=o$.

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

Na elaboração deste Capítulo, subsidiámo-nos das publicações seguintes:

E. Steinitz — *Algebraische Theorie der Körper*, «Journal für die reine und angewandte Mathematik», Band 137, 1910;

B. L. van der Waerden — *Moderne Algebra*, tomo 1.º, Berlim, 1930;

H. Hasse — *Höhere Algebra*, «Lineare Gleichungen», 2.ª edição, Berlim, 1933;

A. Adrian Albert — *Modern Higher Algebra*, Chicago, 1936;

A. Almeida Costa — *Elementos da Teoria dos Anéis*, Porto, Centro de Estudos Matemáticos, 1943;

N. Jacobson — *The Theory of Rings*, New York, 1943;

A. Andrade Guimarães — *Números racionais*, «Boletim da Sociedade Portuguesa de Matemática», série A, vol. 1, n.º 1, Lisboa, 1947;

A. Almeida Costa — *Sistemas Hiper-complexos*, Porto, Centro de Estudos Matemáticos, 1948;

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;

N. Jacobson — *Lectures in Abstract Algebra*, New York, 1951;

J. Gaspar Teixeira — Álgebra, *Introdução à Teoria dos Anéis*, Lisboa, Junta de Investigação Matemática, 1953;

A. Almeida Costa — *On modules and rings with operators*, «Revista da Faculdade de Ciências de Lisboa», vol. IV, 1954.

CAPÍTULO III

ESPAÇO LINEAR

§ 1 — Dependência e independência linear

1) **Sobre os grupos com operadores** — A noção de *grupo com operadores* foi introduzida por W. KRULL (1), em 1925, para o caso dos grupos comutativos. A extensão a grupos quaisquer foi feita por O. SCHMIDT (2), em 1928.

Tomemos um grupo $\mathfrak{G} = \{u, a, b, \ldots\}$ e suponhamos dado um conjunto de símbolos $\Omega = \{\alpha, \beta, \ldots, \varphi, \psi, \theta, \ldots\}$ realizando as condições seguintes: 1.ª — um elemento a do grupo e um elemento $\theta \in \Omega$ definem uma espécie de produto $a\theta$, que é um elemento do grupo; 2.ª — o elemento θ é distributivo relativamente ao produto: $(ab)\theta = a\theta . b\theta$.

A aplicação $a \to a\theta$ é um endomorfismo de $\mathfrak{G}$. Pode acontecer que operadores diferentes determinem o mesmo endomorfismo. Quando, pelo contrário, a operadores distintos corresponderem endomorfismos distintos, podemos identificar os operadores com os endomorfismos.

No n.º 3, § 3, do Cap. I, dissemos o que devia entender-se por automorfismo dum grupo $\mathfrak{G}$ e definimos o grupo $A\mathfrak{G}$ desses

(1) W. KRULL, *Über verallgemeinerte endliche Abelsche Gruppen*, tomo 23 da «Mathematische Zeitschrift», 1925, pgs. 161 a 196.

(2) O. SCHMIDT, *Über unendliche Gruppen mit endlicher Kette*, tomo 29 da «Mathematische Zeitschrift», 1928, pgs. 34 a 41.

automorfismos. O conjunto $A\mathfrak{G}$ constitui um sistema de operadores.

Se o grupo $\mathfrak{G}$ for um módulo $\mathfrak{M}$, o anel $\mathfrak{E}(\mathfrak{M})$, dos seus endomorfismos, definido no n.º 5, § 1, Cap. II, contém todos os operadores distintos de $\mathfrak{M}$.

Os teoremas demonstrados no Cap. I, nos quais intervêm as noções de subgrupo e de invariante, podem transportar-se 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 $\mathfrak{g}$, tais que, para cada $c \in \mathfrak{g}$, é também $c\theta \in \mathfrak{g}$, com $\theta \in \Omega$ 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 $c\theta \in \mathfrak{H}$; 3) como homomorfismos, 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 $\mathfrak{G}'$, a correspondência $a \to a'$ obedece à lei seguinte: $a\theta \to (a\theta)' = a'\theta$, qualquer que seja $\theta \in \Omega$.

Exemplificando, podemos enunciar o teorema 25, do n.º 4, § 3, Cap. I, dizendo: o produto $\mathfrak{h}\mathfrak{g}$ é um subgrupo $-\Omega$, de $\mathfrak{G}$, suposto este um grupo $-\Omega$, se $\mathfrak{g}$ for um invariante $-\Omega$ e $\mathfrak{h}$ um subgrupo $-\Omega$.

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

É agora fácil de dar o enunciado do teorema da homomorfia, no caso dos grupos $-\Omega$. Diremos: se $\mathfrak{G}$ é um grupo $-\Omega$ e $\mathfrak{H}$ um invariante $-\Omega$, então $\mathfrak{G}/\mathfrak{H} = \overline{\mathfrak{G}}$ é um grupo cociente no sentido $-\Omega$, tendo lugar o seguinte homomorfismo $-\Omega$:

$\mathfrak{G} \sim \overline{\mathfrak{G}} = \mathfrak{G}/\mathfrak{H}$; reciprocamente, se $\mathfrak{G} \sim \overline{\mathfrak{G}}$ é um homomorfismo — Ω, segue-se que $\overline{\mathfrak{G}}$, a menos de isomorfismo — Ω, é um grupo cociente no sentido — Ω.

2) **Módulos com respeito a anéis** — Nas aplicações, encontra-se frequentemente o caso particular de um módulo $\mathfrak{M}$ ter um domínio operatório Ω que é um anel não comutativo $\mathfrak{S}$. Se pusermos

$$\mathfrak{M} = \{o, \ldots, x, y, \ldots, z, \ldots\}, \quad \mathfrak{S} = \{o, a, b, c, \ldots\},$$

será

$$x\,a \in \mathfrak{M}, \qquad (x+y)\,a = x\,a + y\,a, \tag{1}$$

conforme a definição geral do número anterior.

Dá-se aqui a circunstância de, no domínio operatório, haver soma e produto de operadores. Admitindo, ao lado de (1), as igualdades

$$x(a+b) = x\,a + x\,b, \qquad x(a\,b) = (x\,a)\,b, \tag{2}$$

$\mathfrak{M}$ diz-se um *módulo com respeito ao anel* $\mathfrak{S}$.

Quando o anel $\mathfrak{S}$ tem elemento um $= u$, se for $x\,u = x$, qualquer que seja $x \in \mathfrak{M}$, o elemento u diz-se *operador unitário* do módulo. Não sendo u operador unitário, escrevamos $x = x\,u + (x - x\,u)$. O conjunto dos elementos $x\,u$ é um submódulo — $\mathfrak{S}$, de $\mathfrak{M}$, pois que $(x\,u)\,a = x\,(u\,a) = x\,a = (x\,a)\,u$; e o conjunto dos elementos $x - x\,u$ é igualmente um submódulo — $\mathfrak{S}$. Pondo $\{x\,u\} = \mathfrak{M}'$, $\{x - x\,u\} = \mathfrak{M}''$, vê-se que $\mathfrak{M} = (\mathfrak{M}', \mathfrak{M}'')$, onde se utilizou o símbolo $(\mathfrak{M}', \mathfrak{M}'')$ para significar o grupo dos elementos obtidos quando se juntam aos elementos de $\mathfrak{M}'$ os elementos de $\mathfrak{M}''$. Trata-se duma soma de dois subgrupos (invariantes) que leva a um subgrupo (invariante), aqui igual ao grupo. Para $\mathfrak{M}'$, u é operador unitário. Em $\mathfrak{M}''$, qualquer elemento $a \in \mathfrak{S}$ define o endomorfismo nulo. Se $z \in \mathfrak{M}' \cap \mathfrak{M}''$, vê-se que $z = z\,u$, $z\,u = o$, de sorte que $z = o$.

Se tomarmos duas decomposições dum elemento $x \in \mathfrak{M}$, sob a forma $x = x' + x''$, $x = y' + y''$, com $x', y' \in \mathfrak{M}'$, $x'', y'' \in \mathfrak{M}''$, concluímos $x\,u = x'\,u = x'$, $x\,u = y'\,u = y' = x'$, $x'' = y''$. As duas decomposições são idênticas. Diz-se, então, que $\mathfrak{M}$ é *soma directa* de $\mathfrak{M}'$ e $\mathfrak{M}''$ e escreve-se $\mathfrak{M} = \mathfrak{M}' + \mathfrak{M}''$.

Num anel $\mathfrak{A}$, o grupo abeliano aditivo correspondente é módulo com respeito a $\mathfrak{A}$. Em geral, há diferentes elementos de $\mathfrak{A}$ que determinam o mesmo endomorfismo, [cfr. n.º 3, § 2, Cap. II]. Seja $s \in \mathfrak{A}$ um elemento que anule, por multiplicação à direita, todos os elementos de $\mathfrak{A}$. O conjunto dos elementos com a propriedade atribuída a s é um ideal bilateral $\mathfrak{a}$, de $\mathfrak{A}$. Tomada a classe $\bar{a} = a + \mathfrak{a}$ de $\mathfrak{A}/\mathfrak{a}$, todos os elementos da classe induzem em $\mathfrak{A}$ o mesmo endomorfismo. Em vez do domínio operatório $\mathfrak{A}$, podemos considerar o domínio operatório $\overline{\mathfrak{A}} = \mathfrak{A}/\mathfrak{a}$. Nesse caso, a operadores distintos correspondem endomorfismos distintos. Se o anel $\mathfrak{A}$ tem elemento um, o ideal bilateral $\mathfrak{a}$ é o ideal nulo e todos os elementos de $\mathfrak{A}$ induzem já endomorfismos distintos.

3) **Exemplo importante** — Dado um anel $\mathfrak{A}$ com elemento um, formemos os símbolos $(a_1, \ldots, a_n)$, nos quais figuram n elementos de $\mathfrak{A}$. O conjunto dos símbolos forma um módulo $\mathfrak{M}$, se pusermos

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n),$$

supostos igualmente os b_i pertencentes a $\mathfrak{A}$. Se, em seguida, definirmos a aplicação de $a \in \mathfrak{A}$ aos elementos de $\mathfrak{M}$ pela igualdade

$$(a_1, \ldots, a_n)\,a = (a_1\,a, \ldots, a_n\,a),$$

é muito fácil de verificar que se realizam as condições expressas nas igualdades (1) e (2). Isto significa que $\mathfrak{M}$ é módulo com respeito a $\mathfrak{A}$. Façamos, em particular,

$$e_1 = (u, o, \ldots, o), \quad e_2 = (o, u, o, \ldots), \ldots, \quad e_n = (o, \ldots, o, u).$$

Vê-se que é $(a_1, \ldots, a_n) = e_1 a_1 + e_2 a_2 + \ldots + e_n a_n$.

O elemento zero de $\mathfrak{M}$ é $(o, o, \ldots, o)$, ao qual pode dar-se a forma $(o, \ldots, o) = e_1 . o + \ldots + e_n . o$. Qualquer elemento de $\mathfrak{M}$ tem uma única representação à custa dos e_i. O facto de a condição $e_1 a_1 + \ldots + e_n a_n = 0$ implicar $a_1 = \ldots = a_n = o$ 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 $e_i a, (a \in \mathfrak{A})$, $\mathfrak{M}$ é também aqui soma directa dos sub-módulos — $\mathfrak{A}$ que são os $e_i \mathfrak{A}$, escrevendo-se $\mathfrak{M} = e_1 \mathfrak{A} + \ldots + e_n \mathfrak{A}$. E, se nos lembrarmos de que um grupo cíclico gerado por um elemento b dum grupo abeliano aditivo se pode escrever $\mathfrak{J} b$ (melhor, aqui, $b \mathfrak{J}$), em que $\mathfrak{J}$ é o anel dos inteiros, justifica-se a designação de grupo cíclico atribuída aos $e_i \mathfrak{A}$. $\mathfrak{M}$ aparece, pois, como uma soma directa de subgrupos cíclicos.

4) **Dependência e independência linear** — O objectivo essencial deste Capítulo é o estudo dos *módulos finitos com respeito a um corpo* $\mathfrak{K}$, fazendo-se desse estudo importantes aplicações algébricas e geométricas.

Seja, então, $\mathfrak{A} = \mathfrak{K}$ um corpo, e suponhamos $\mathfrak{M}$ um módulo com respeito a $\mathfrak{K}$. Os elementos de $\mathfrak{M}$ designar-se-ão por *vectores* e serão representados por $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots, \mathfrak{x}, \mathfrak{y}, \mathfrak{z}, \ldots$. $\mathfrak{M}$ receberá, em seguida, o nome de *multiplicidade vectorial linear*. Quanto aos elementos de $\mathfrak{K}$, representá-los-emos aqui por $a, b, c, \ldots$ e também $\lambda, \mu, \xi, \ldots$, afectados ou não de índices.

A multiplicidade linear diz-se *finita*, se existirem n elementos $\mathfrak{e}_1, \ldots, \mathfrak{e}_n \in \mathfrak{M}$ tais que, para cada $\mathfrak{x} \in \mathfrak{M}$, se tenha, duma maneira única,

$$\mathfrak{x} = \mathfrak{e}_1 \xi_1 + \ldots + \mathfrak{e}_n \xi_n . \qquad (2')$$

Em particular, o vector zero $= 0$, terá a forma $0 = \mathfrak{e}_1 . o + \ldots + \mathfrak{e}_n . o$, onde o é o elemento nulo de $\mathfrak{K}$. O facto de a relação

$$\mathfrak{e}_1 \lambda_1 + \ldots + \mathfrak{e}_n \lambda_n = 0$$

implicar $\lambda_1 = \ldots = \lambda_n = o$ exprime-se dizendo que os vectores $\mathfrak{e}_i$ são *linearmente independentes*. O número n diz-se *dimensão* da multiplicidade vectorial, facto que recordaremos escrevendo $\mathfrak{M} = \mathfrak{M}_n$.

Os vectores $\mathfrak{e}_j$ definem o que se chama uma *base* de $\mathfrak{M}_n$.

Imaginemos agora que, dados os vectores $\mathfrak{a}_1, \ldots, \mathfrak{a}_p$, existe uma relação

$$\mathfrak{a}_1 \mu_1 + \ldots + \mathfrak{a}_p \mu_p = 0, \qquad (3)$$

sem que os μ_j sejam todos nulos; diz-se que os $\mathfrak{a}_j$ são *linearmente dependentes*. Escrevendo

$$\mathfrak{a}_j = \mathfrak{e}_1 a_{1j} + \ldots + \mathfrak{e}_n a_{nj}, \qquad (a_{kj} \in \mathfrak{K}),$$

e substituindo em (3), 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

$$\sum_j a_{kj} . \mu_j = o, \qquad (k = 1, \ldots, n).$$

Estas igualdades traduzem, de outra maneira, a dependência linear dos $\mathfrak{a}_j$.

Um único vector $\mathfrak{a} \neq 0$ é sempre linearmente independente. Dados 2 vectores, se um deles for zero, há, entre eles, uma dependência linear.

Conhecidos $\mathfrak{a}_1, \ldots, \mathfrak{a}_p$, se outro vector $\mathfrak{a}$ puder exprimir-se sob a forma $\mathfrak{a} = \mathfrak{a}_1 \lambda_1 + \ldots + \mathfrak{a}_p \lambda_p$, diz-se que $\mathfrak{a}$ é uma *combinação linear* dos $\mathfrak{a}_j$. É conveniente fazermos ainda esta

OBSERVAÇÃO: — Das igualdades $\mathfrak{a}(\lambda + o) = \mathfrak{a}\lambda = \mathfrak{a} . \lambda + \mathfrak{a} . o$, tira-se $\mathfrak{a} . o = 0$, qualquer que seja $\mathfrak{a}$. Então, da relação $\mathfrak{a}(\lambda - \lambda) = 0$, deduz-se $\mathfrak{a}\lambda + \mathfrak{a}(-\lambda) = 0$, ou seja $\mathfrak{a}(-\lambda) = -\mathfrak{a}\lambda$. Quando é $\lambda \neq \mu$, é $\mathfrak{a}\lambda \neq \mathfrak{a}\mu$, qualquer que seja $\mathfrak{a} \neq 0$, visto que a igualdade $\mathfrak{a}\lambda = \mathfrak{a}\mu$ levaria a $\mathfrak{a}\lambda - \mathfrak{a}\mu = \mathfrak{a}(\lambda - \mu) =$

$=0$, o que implicaria $\lambda-\mu=o$, ou $\lambda=\mu$. Operadores distintos induzem aqui endomorfismos distintos. O elemento $u\,e\,\Re$ induz o endomorfismo idêntico.

TEOREMA 1: — *Se os vectores* $\mathfrak{a}_j$, $(j=1,2,\ldots,p)$, *são linearmente dependentes, um deles é combinação linear dos outros.* De facto, sendo $\mathfrak{a}_1\lambda_1+\ldots+\mathfrak{a}_p\lambda_p=0$, com $\lambda_1\neq o$, por ex., da equação anterior pode tirar-se

$$\mathfrak{a}_1=-\mathfrak{a}_2\frac{\lambda_2}{\lambda_1}-\ldots-\mathfrak{a}_p\frac{\lambda_p}{\lambda_1},$$

o que justifica a afirmação.

TEOREMA 2: — *Se os vectores* $\mathfrak{a}_1,\ldots,\mathfrak{a}_p$ *são linearmente independentes, mas* $\mathfrak{a}_1,\ldots,\mathfrak{a}_{p+1}$ *são dependentes, o vector* $\mathfrak{a}_{p+1}$ *é combinação linear dos restantes.* Escrevendo $\mathfrak{a}_1\lambda_1+\ldots+\mathfrak{a}_p\lambda_p+\mathfrak{a}_{p+1}\lambda_{p+1}=0$, não pode ter se $\lambda_{p+1}=o$, visto que, de contrário, existiria uma dependência linear entre os $\mathfrak{a}_i$. Então, deduz-se

$$\mathfrak{a}_{p+1}=-\mathfrak{a}_1\frac{\lambda_1}{\lambda_{p+1}}-\ldots-\mathfrak{a}_p\frac{\lambda_p}{\lambda_{p+1}},$$

como se deseja.

Tem grande interesse o reconhecimento do carácter de dependência ou independência dum certo número de vectores dados. Por comodidade de linguagem, chamamos *componentes* do vector $\mathfrak{x}$ os coeficientes ξ_i que figuram na igualdade (2'). Dar um vector será, então, dar as suas componentes nos $\mathfrak{e}_i$.

Posto isto, consideremos os m vectores $\mathfrak{a}_1,\ldots,\mathfrak{a}_m$ e formemos o quadro rectangular seguinte, em cujas linhas horizontais (chamadas *vectores-linhas,* ou, simplesmente, *linhas)* figuram as componentes dos diferentes vectores:

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}. \qquad (4)$$

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.* É válida este

TEOREMA 3: — *Entre os* m *vectores* $\mathfrak{a}_j$, *supostos não todos nulos, há sempre* $r\leqq m$ *vectores independentes, nos quais todos se exprimem.*

Visto que um vector não nulo é linearmente independente, existe um número máximo r, não nulo, de vectores linearmente independentes, entre os $\mathfrak{a}_j$. Pelo teorema 2, todos os vectores dados se exprimem nesses r vectores independentes. O teorema está provado.

É a busca do número r, acabado de referir, que nos vai ocupar nas considerações a seguir.

Partamos da matriz rectangular (4), que abreviadamente designaremos por $A=(a_{ik})$ $(i=1,2,\ldots,m;\ k=1,2,\ldots,n)$. 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 $b\,e\,\Re$, não nulo; 2.º) — adição, à linha de ordem k, dos elementos correspondentes da linha de ordem j, multiplicados por um elemento de $\Re$; 3.º) — multiplicação dos elementos duma coluna de A por um elemento $b\neq o$; 4.º) — adição, à coluna q, dos elementos correspondentes da coluna de ordem t, multiplicados por um elemento de $\Re$. Vamos provar o seguinte

TEOREMA 4: — *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 $\mathfrak{a}_{j_1},\ldots,\mathfrak{a}_{j_{r+1}}$, 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 ex., em vez de $\mathfrak{a}_{j_1}$, de uma relação

$$\mathfrak{a}_{j_1}\lambda_1+\ldots+\mathfrak{a}_{j_{r+1}}\lambda_{r+1}=0, \qquad (5)$$

deduz-se a relação

$$(a_{j_1}\, b)\,\frac{\lambda_1}{b} + \ldots + a_{j_{r+1}}\,\lambda_{r+1} = 0,$$

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 (5). Depois da transformação, se, por ex., $a_{j_{r+1}}$ passa a ser substituído por $a_{j_{r+1}} + a_i b$, vamos ver que tem lugar uma igualdade da forma

$$a_{j_1}\,\mu_1 + \ldots + (a_{j_{r+1}} + a_i b)\,\mu_{r+1} = 0, \qquad (6)$$

sem que todos os μ_h sejam nulos. Por um lado, com efeito, é

$$a_{j_1}\,\lambda_1 + \ldots + a_{j_{r+1}}\,\lambda_{r+1} = 0; \qquad (6')$$

por outro, a_i não é independente de r dos vectores $a_{j_1}, \ldots, a_{j_{r+1}}$, sendo, por ex.,

$$a_{j_1}\,\lambda'_1 + \ldots + a_{j_r}\,\lambda'_r + a_i\lambda = 0. \qquad (7)$$

Aqui, pode acontecer que os vectores $a_{j_1}, \ldots, a_{j_r}$ sejam dependentes, e, então, sê-lo-ão os vectores que figuram em (6); ou, de contrário, se aqueles r vectores forem independentes, será, em (7), $\lambda \neq o$, e, em (6'), $\lambda_{r+1} \neq o$, o que permite a combinação

$$a_{j_1}\left(\frac{\lambda_1}{\lambda_{r+1}} + \frac{\lambda'_1\, b}{\lambda}\right) + \ldots + a_{j_r}\left(\frac{\lambda_r}{\lambda_{r+1}} + \frac{\lambda'_r\, b}{\lambda}\right) + \\ + (a_{j_{r+1}} + a_i b) = 0,$$

na qual é diferente de zero (e igual a 1) o coeficiente de $a_{j_{r+1}} + a_i b$.

Quanto ao 3.º tipo, raciocinaremos do modo a seguir. Consideremos, por ex., $a_1, \ldots, a_{r+1}$, e exprimamos a sua dependência linear sob a forma

$$\sum_{i=1}^{r+1} a_{ik}\,\lambda_i = o, \qquad (k = 1, 2, \ldots, n). \qquad (8)$$

Se uma das colunas, a 1.ª por ex., se multiplica por $b \neq o$, devemos substituir a_{i1} por $a_{i1}\, b$, qualquer que seja i. Isso equivale simplesmente a multiplicar por $b \neq o$ a primeira equação (8), de sorte que se verificam as relações análogas a (8), relativas aos novos vectores da matriz transformada. Resta analisar o 4.º tipo. Se, por ex., se juntam aos elementos da 1.ª coluna os elementos da 2.ª multiplicados por b, os elementos a_{i1} aparecem substituídos por $a_{i1} + a_{i2}\, b$, e as equações (8), relativas à matriz transformada, são todas as mesmas que aquelas, salvo a primeira (para $k = 1$), que é substituída pela seguinte:

$$\sum_{i=1}^{r+1} (a_{i1} + a_{i2}\, b)\,\lambda_i = o.$$

Escrevendo esta relação sob a forma

$$\sum_{i=1}^{r+1} a_{i1}\,\lambda_i + \left(\sum_{i=1}^{r+1} a_{i2}\,\lambda_i\right) b = o,$$

vê-se que ela é efectivamente verificada, por serem nulas ambas as parcelas que figuram no seu 1.º membro.

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 (4) pela *matriz transposta,* que resulta mudando as linhas em colunas e as colunas em linhas, obtém-se

$$\begin{pmatrix} a_{11} & a_{21} & \ldots & a_{m1} \\ a_{12} & a_{22} & \ldots & a_{m2} \\ \ldots & \ldots & \ldots & \ldots \\ a_{1n} & a_{2n} & \ldots & a_{mn} \end{pmatrix}. \qquad (9)$$

Esta matriz rectangular, de n linhas e m colunas, sujeita a transformações simples, leva a transformadas para as 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 (4) as transformações do 3.º ou do 4.º tipo, e escrevendo, em seguida, as matrizes transpostas das transformadas de (4). E, inversamente, as transformações do 3.º ou do 4.º tipo, em (9), obtêm-se a partir das do 1.º ou do 2.º tipo, efectuadas sobre (4), pelo mesmo processo de cima. O número s, relativo às linhas de (9), é o número máximo de colunas de (4). As transformações simples não alteram s. Tem lugar este

TEOREMA 5: — *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 esquema a seguir, escrito para a troca das duas primeiras colunas:

$$(a_{i1}, a_{i2}) \to (a_{i1}, a_{i2} + a_{i1}) \to (a_{i1}, -a_{i2} - a_{i1}) \to (-a_{i2}, -a_{i2} - a_{i1}) \to (a_{i2}, -a_{i2} - a_{i1}) \to (a_{i2}, -a_{i1}) \to (a_{i2}, a_{i1}).$$

Por isso, as trocas de linhas ou de colunas não alteram r e s.

A determinação prática de r é fácil. Tomemos (4) 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 agora a 1.ª linha por a'^{-1}_{11}, vemos que é admissível supor $a'_{11} = u \in \mathfrak{R}$. Então, por transformações simples do 2.º e do 4.º tipo, chega-se a

$$\begin{pmatrix} u & o & o & \dots & o \\ o & a'_{22} & a'_{23} & \dots & a'_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ o & a'_{m2} & a'_{m3} & \dots & a'_{mn} \end{pmatrix}.$$

Não se dando a circunstância de serem nulos todos os a'_{ih}, por trocas de linhas e de colunas, a partir da 2.ª linha e da 2.ª coluna, chegamos a

$$\begin{pmatrix} u & o & o & \dots & o \\ o & u & o & \dots & o \\ o & o & a''_{33} & \dots & a''_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ o & o & a''_{m3} & \dots & a''_{mn} \end{pmatrix}.$$

O processo continua. Chega-se finalmente a uma matriz da forma

$$\begin{pmatrix} u & o & \dots & o & \dots & o \\ o & u & \dots & o & \dots & o \\ \dots & \dots & \dots & \dots & \dots & \dots \\ o & o & \dots & u & \dots & o \\ o & o & \dots & o & \dots & o \\ \dots & \dots & \dots & \dots & \dots & \dots \\ o & o & \dots & o & \dots & o \end{pmatrix}, \qquad (10)$$

em cuja primeira diagonal figura r vezes o elemento u. Sob o aspecto (10), reconhece-se mais que se tem $s = r$. Daqui o importante

TEOREMA 6: — *Dada uma matriz* (4), *o número máximo de linhas independentes é igual ao número máximo de colunas independentes.*

O referido número diz-se *característica* da matriz.

COROLÁRIO 1: — *Em* $\mathfrak{M}_n$ *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* $\mathfrak{M}_n$.

É muito útil nas aplicações um outro teorema que vamos passar a demonstrar. Imaginemos p vectores $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_p$ e consideremos $m > p$ combinações lineares desses vectores, a saber: $\mathfrak{b}_1, \ldots, \mathfrak{b}_m$. 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 $m - p$ 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 7: — *Se* $\mathfrak{a}_1, \ldots, \mathfrak{a}_p$ *são* p *vectores linearmente independentes, e se* $\mathfrak{b}_1, \ldots, \mathfrak{b}_m$, *com* $m > p$, *são combinações lineares dos* $\mathfrak{a}_i$, *há entre os* $\mathfrak{b}_j$ *uma dependência linear.*

Dois sistemas de vectores $(\mathfrak{x}_1, \ldots, \mathfrak{x}_m)$ e $(\mathfrak{y}_1, \ldots, \mathfrak{y}_p)$ dizem-se *equivalentes,* se os $\mathfrak{x}_i$ se podem exprimir nos $\mathfrak{y}_j$, e inversamente. A este respeito, tem lugar uma proposição importante, devida a STEINITZ, que é a seguinte:

TEOREMA 8: — *Se os vectores* $\mathfrak{y}_1, \ldots, \mathfrak{y}_p$ *são independentes e exprimíveis em* $\mathfrak{x}_1, \ldots, \mathfrak{x}_m$, *é possível substituir* p *destes últimos, por ex.* $\mathfrak{x}_{i_1}, \ldots, \mathfrak{x}_{i_p}$, *pelos* $\mathfrak{y}_j$, *de tal modo que o sistema* $(\mathfrak{y}_1, \ldots, \mathfrak{y}_p, \mathfrak{x}_{i_{p+1}}, \ldots, \mathfrak{x}_{i_m})$ *seja equivalente a* $(\mathfrak{x}_1, \ldots, \mathfrak{x}_m)$.

Admitindo $p = 1$, da relação $\mathfrak{y}_1 = \mathfrak{x}_1 \lambda_1 + \ldots + \mathfrak{x}_m \lambda_m$, supondo, por ex., $\lambda_1 \neq o$, deduz-se

$$\mathfrak{x}_1 = \mathfrak{y}_1 \frac{u}{\lambda_1} - \mathfrak{x}_2 \frac{\lambda_2}{\lambda_1} - \ldots - \mathfrak{x}_m \frac{\lambda_m}{\lambda_1}.$$

Então $(\mathfrak{y}_1, \mathfrak{x}_2, \ldots, \mathfrak{x}_m)$ é equivalente a $(\mathfrak{x}_1, \mathfrak{x}_2, \ldots, \mathfrak{x}_m)$. Admitindo agora $p = 2$, o vector $\mathfrak{y}_2$ exprime-se em $\mathfrak{y}_1, \mathfrak{x}_2, \ldots, \mathfrak{x}_m$, sob a forma

$$\mathfrak{y}_2 = \mathfrak{y}_1 \lambda + \mathfrak{x}_2 \mu_2 + \ldots + \mathfrak{x}_m \mu_m, \tag{11}$$

não podendo ser nulos todos os μ_i, dada a independência de $\mathfrak{y}_1$ e $\mathfrak{y}_2$. Se for $\mu_2 \neq o$, da igualdade anterior tiramos

$$\mathfrak{x}_2 = -\mathfrak{y}_1 \frac{\lambda}{\mu_2} + \mathfrak{y}_2 \frac{u}{\mu_2} - \ldots - \mathfrak{x}_m \frac{\mu_m}{\mu_2}.$$

pelo que os dois sistemas $(\mathfrak{y}_1, \mathfrak{x}_2, \ldots, \mathfrak{x}_m)$ e $(\mathfrak{y}_1, \mathfrak{y}_2, \mathfrak{x}_3, \ldots, \mathfrak{x}_m)$ são equivalentes. Como a equivalência em causa é transitiva, também $(\mathfrak{x}_1, \ldots, \mathfrak{x}_m)$ e $(\mathfrak{y}_1, \mathfrak{y}_2, \mathfrak{x}_3, \ldots, \mathfrak{x}_m)$ são equivalentes.

O processo continua. Logo que se tenham substituído $p - 1$ 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 (11), 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 $\mathfrak{x}_i$.

Do teorema 7 conclui-se que uma base de $\mathfrak{M}_n$ tem sempre n elementos. Se ela pudesse ter $m < n$ elementos, haveria uma relação de dependência entre $\mathfrak{e}_1, \ldots, \mathfrak{e}_n$; e, se pudesse ser $m > n$, a relação de dependência teria lugar entre os próprios vectores da base (pelo facto de eles se exprimirem nos $\mathfrak{e}_k$). À mesma conclusão leva o teorema de STEINITZ, como vamos ver.

COROLÁRIO 3: — *A dimensão* n *é um invariante.* [O significado a atribuir a esta afirmação é precisamente o que acabou de ser explicado]. De facto, se $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ formam uma base, haverá equivalência entre os $\mathfrak{a}_j$ e os vectores $\mathfrak{e}_1, \ldots, \mathfrak{e}_n$. O teorema de STEINITZ exige $m \geqq n$ e $n \geqq m$, o que acarreta $m = n$.

À teoria das equações lineares, de que adiante nos ocuparemos, interessa ainda uma outra redução da matriz (4), fazendo intervir ùnicamente transformações sobre linhas.

Seja r a característica de (4). Como há r colunas linearmente independentes, vamos começar por supor que essas colunas são as primeiras. As transformações simples sobre linhas permitem levar (4) à forma

$$\begin{pmatrix} u & a'_{12} & a'_{13} & \dots & a'_{1n} \\ o & a'_{22} & a'_{23} & \dots & a'_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ o & a'_{m2} & a'_{m3} & \dots & a'_{mn} \end{pmatrix}, \qquad (12)$$

visto que, na 1.ª coluna, não podem figurar elementos todos iguais a zero. Em (12) não pode, se for $r \geqq 2$, ter-se na 2.ª coluna $a'_{22} = \dots = a'_{m2} = 0$, visto que, de contrário, a 2.ª coluna seria uma combinação linear da primeira. Transformações simples sobre linhas fazem passar de (12) a

$$\begin{pmatrix} u & a'_{12} & a'_{13} & \dots & a'_{1n} \\ o & u & a''_{23} & \dots & a''_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ o & o & a''_{m3} & \dots & a''_{mn} \end{pmatrix},$$

e, em seguida, a

$$\begin{pmatrix} u & o & a''_{13} & \dots & a''_{1n} \\ o & u & a''_{23} & \dots & a''_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ o & o & a''_{m3} & \dots & a''_{mn} \end{pmatrix}.$$

O processo continua, até se chegar a obter nas r primeiras colunas elementos todos nulos, salvo os elementos diagonais. Virá

$$\begin{pmatrix} u & o & \dots & o & b_{1,r+1} & \dots & b_{1n} \\ o & u & \dots & o & b_{2,r+1} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ o & o & \dots & u & b_{r,r+1} & \dots & b_{rn} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ o & o & \dots & o & b_{m,r+1} & \dots & b_{mn} \end{pmatrix}.$$

Importante é verificar agora que são compostas de elementos nulos todas as linhas, a partir da de ordem $r+1$. Estudemos, por ex., os elementos $b_{r+1,r+1}, \dots, b_{m,r+1}$. Deverá ter-se $b_{r+1,r+1} = o \cdot b_{1,r+1} + o \cdot b_{2,r+1} + \dots + o \cdot b_{r,r+1} = \dots = b_{m,r+1} = o$. Todas as colunas têm apenas elementos nulos, a partir do elemento de ordem $r+1$.

Se as r primeiras colunas de (4) não forem independentes, e as colunas independentes estiverem localizadas doutro modo, o método é aplicável anàlogamente; apenas, no aspecto final, não apareçe o elemento u nas r primeiras colunas, mas sim noutras, deixando, por isso, de pertencer à primeira diagonal.

TEOREMA 9: — *Uma matriz da forma* (4), *com a característica* r, *pode, por meio de transformações simples sobre linhas, reduzir-se a uma forma análoga à seguinte:*

$$\begin{vmatrix} u & o & \dots & o & b_{1,r+1} & \dots & b_{1n} \\ o & u & \dots & o & b_{2,r+1} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ o & o & \dots & u & b_{r,r+1} & \dots & b_{rn} \\ o & o & \dots & o & o & \dots & o \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ o & o & \dots & o & o & \dots & o \end{vmatrix}.$$

A localização das colunas em que figura o elemento u *pode ser diferente da que se indica.*

5) **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 $\neq (o)$ e admitamos que $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ constituem vectores independentes da submultiplicidade, em número máximo. O número r é bem determinado. A submultiplicidade compõe-se dos elementos da forma

$\mathfrak{a}_1 \lambda_1 + \ldots + \mathfrak{a}_r \lambda_r$, e apenas desses elementos. Diz-se que r é a *dimensão da submultiplicidade,* a qual será designada por $\mathfrak{M}_r$. Os vectores $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ formam uma base de $\mathfrak{M}_r$, não podendo haver uma base com menos de r elementos. À face do teorema de STEINITZ do número anterior, pode dar-se o seguinte enunciado:

TEOREMA 10: — *Se* $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ *são vectores constituindo uma base da submultiplicidade* $\mathfrak{M}_r$, *dada a base* $\mathfrak{e}_1, \ldots, \mathfrak{e}_n$, *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 $\mathfrak{e}_j$ 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. É válido o

TEOREMA 11: — *Entre os números* r', r'', d, s *existe a relação* $r' + r'' = d + s$. Para fazermos a demonstração, tomemos uma base $\mathfrak{a}_1, \ldots, \mathfrak{a}_d$, de $\mathfrak{D}$, e completemo-la com $\mathfrak{b}_1, \ldots, \mathfrak{b}_{r'-d}$, de modo a formar uma base de $\mathfrak{M}_{r'}$, e completemo-la com $\mathfrak{c}_1, \ldots, \mathfrak{c}_{r''-d}$, de modo a formar uma base de $\mathfrak{M}_{r''}$. O conjunto dos $\mathfrak{a}_i, \mathfrak{b}_j, \mathfrak{c}_h$ constitui uma base de $\mathfrak{S}$, como passamos a provar. Que eles permitem exprimir qualquer vector de $\mathfrak{S}$ é imediato. Basta, assim, verificar a sua independência. Imaginemos uma relação

$$\sum_{i=1}^{d} \mathfrak{a}_i \lambda_i + \sum_{j=1}^{r'-d} \mathfrak{b}_j \mu_j + \sum_{k=1}^{r''-d} \mathfrak{c}_k \nu_k = 0.$$

Deduz-se dela

$$\Sigma \mathfrak{a}_i \lambda_i + \Sigma \mathfrak{b}_j \mu_j = -\Sigma \mathfrak{c}_k \nu_k,$$

de modo que o elemento de $\mathfrak{M}_n$ representado por qualquer dos membros da igualdade anterior pertence simultâneamente a $\mathfrak{M}_{r''}$ e a $\mathfrak{M}_{r'}$, ou seja a $\mathfrak{D}$. Mas, escrevendo então, com certos ρ_i,

$$\Sigma \mathfrak{a}_i \rho_i = -\Sigma \mathfrak{c}_k \nu_k \qquad \text{ou} \qquad \Sigma \mathfrak{a}_i \rho_i + \Sigma \mathfrak{c}_k \nu_k = 0,$$

vê-se que os ν_k (assim como os ρ_i) são nulos. Resulta deste modo

$$\Sigma \mathfrak{a}_i \lambda_i + \Sigma \mathfrak{b}_j \mu_j = 0,$$

e, portanto, também $\lambda_i = o$, $\mu_j = o$, 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.

6) **Espaço linear** — Passamos agora a introduzir uma noção nova: a noção de *ponto*. Fá-lo-emos à custa dos postulados seguintes:

I) existem pontos $A, B, C, \ldots, X, \ldots$;
II) dois pontos A e B definem um vector $\overrightarrow{AB} = \mathfrak{a} \in \mathfrak{M}_n$;
III) dados um ponto A e um vector $\mathfrak{a}$, existe um ponto B tal que $\overrightarrow{AB} = \mathfrak{a}$;
IV) três pontos A, B, C satisfazem à relação $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$.

Chamaremos *espaço linear* a n dimensões, e representá-lo-emos pelo símbolo $\mathfrak{R}_n$, um conjunto de pontos e vectores que seja, relativamente aos vectores, uma multiplicidade vectorial a n dimensões, e que, relativamente aos pontos, verifique os postulados I) a IV).

Devemos dizer que, na definição anterior, há postulados supérfluos. Nós vamos mostrar, por ex., 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 $\mathfrak{a}$ tal que $\mathfrak{a}=\vec{AB}$; em seguida, a partir de B, o vector $\mathfrak{b}$ tal que $\mathfrak{b}=\vec{BC}$; finalmente, a partir de C, o vector $\mathfrak{c}$ tal que $\mathfrak{c}=\vec{CD}$. Tem-se

$$\mathfrak{a}+\mathfrak{b}=\vec{AB}+\vec{BC}=\vec{AC},$$

$$(\mathfrak{a}+\mathfrak{b})+\mathfrak{c}=\vec{AC}+\vec{CD}=\vec{AD}.$$

Por outro lado, é

$$\mathfrak{b}+\mathfrak{c}=\vec{BC}+\vec{CD}=\vec{BD},$$

$$\mathfrak{a}+(\mathfrak{b}+\mathfrak{c})=\vec{AB}+\vec{BD}=\vec{AD}=(\mathfrak{a}+\mathfrak{b})+\mathfrak{c},$$

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 $\mathfrak{a}=\vec{AB}$, $\mathfrak{b}=\vec{AC}$. A equação escrever-se-á $\vec{AB}+\mathfrak{x}=\vec{AC}$, que é satisfeita pondo $\mathfrak{x}=\vec{BC}$.

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 12: — *Todos os pontos de* $\mathfrak{R}_n$ *são obtidos a partir de qualquer ponto* $O_o \in \mathfrak{R}_n$, *construindo a partir de* O_o *todos os vectores* $\mathfrak{x} \in \mathfrak{M}_n$.

A demonstração é agora imediata.

Chamaremos *referencial* de $\mathfrak{R}_n$ um sistema $O_o(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$, formado pelo ponto $O_o \in \mathfrak{R}_n$, escolhido prèviamente de modo arbitrário, e por n vectores de $\mathfrak{M}_n$, linearmente independentes, aplicados a partir de O_o. Então, se X for um ponto de $\mathfrak{R}_n$, tem-se

$$\vec{O_oX}=\mathfrak{e}_1\xi_1+\ldots+\mathfrak{e}_n\xi_n.$$

Os elementos $\xi_i \in \Re$ dizem-se *coordenadas* do ponto X. Em particular, as coordenadas de O_o são $(o, o, \ldots, o)$, pois que $\vec{O_oO_o}=O$, como se conclui de $\vec{AO_o}+\vec{O_oO_o}=\vec{AO_o}$.

Tomemos dois pontos P e Q, de coordenadas $(\lambda_1, \ldots, \lambda_n)$ e $(\mu_1, \ldots, \mu_n)$, respectivamente. Tem-se

$$\vec{O_oP}=\mathfrak{e}_1\lambda_1+\ldots+\mathfrak{e}_n\lambda_n, \quad \vec{O_oQ}=\mathfrak{e}_1\mu_1+\ldots+\mathfrak{e}_n\mu_n,$$

e também $\vec{O_oP}+\vec{PQ}=\vec{O_oQ}$, ou seja

$$\sum_{i=1}^{n}\mathfrak{e}_i\lambda_i+\vec{PQ}=\sum_{i=1}^{n}\mathfrak{e}_i\mu_i.$$

Deduz-se daqui

$$\vec{PQ}=\sum_{i=1}^{n}\mathfrak{e}_i(\mu_i-\lambda_i),$$

igualdade que permite determinar as componentes dum vector, definido por 2 pontos, desde que se conheçam as coordenadas dos pontos.

Se, a partir dum ponto O_o', construirmos os vectores de $\mathfrak{M}_h$, definimos um espaço linear $\mathfrak{R}_h$, considerando a totalidade dos pontos assim obtidos, bem como a submultiplicidade $\mathfrak{M}_h$. A dimensão de $\mathfrak{R}_h$ é a dimensão de $\mathfrak{M}_h$.

Dois espaços lineares $\mathfrak{R}_h$ e $\mathfrak{R}_m$ dizem-se *paralelos,* se uma das multiplicidades vectoriais correspondentes está 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 13: — *Dois subespaços lineares paralelos ou não têm ponto comum ou um deles está contido no outro.* Para se encontrarem dois espaços paralelos sem ponto comum, basta

1) $O_0(\underbrace{x_1, \ldots, x_t}_{x_t}) = R_t$; depois, como $R_t \neq R_n$, tomar um ponto $O_0' \notin R_t$ e construir, a partir desse ponto, o espaço $R_k = O_0'(x_1, \ldots, x_k)$

tomar, por ex.,[1] $O_0(e_1, e_2)$, em seguida tomar um ponto O' tal que $\overrightarrow{O_0 O'} \notin e_1 \lambda_1 + e_2 \lambda_2$, e, finalmente, considerar $O'(e_1)$. Este espaço a uma dimensão é paralelo ao espaço a duas dimensões $O_0(e_1, e_2)$, não havendo ponto comum aos dois espaços.

Tomemos $p+1$ pontos de $\mathfrak{R}_n$, a saber: $O_0, O_1, \ldots, O_p$. Pode acontecer que os vectores $\overrightarrow{O_0 O_1}, \ldots, \overrightarrow{O_0 O_p}$ sejam linearmente independentes. Então, os $p+1$ pontos não pertencem a um subespaço linear de dimensão inferior a p. Podemos dizer:

TEOREMA 14: — *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.*

§ 2 — Equações Lineares

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. É dado o sistema

$$\begin{gathered} a_{i1} x_1 + a_{i2} x_2 + \ldots + a_{in} x_n = b_i, \\ (i = 1, 2, \ldots, m), \qquad (a_{ij}, b_i \in \mathfrak{K}), \end{gathered} \tag{13}$$

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 (13), como um ponto de $\mathfrak{R}_n$, cujas coordenadas são aqueles valores, num referencial prèviamente fixado. Introduzindo ainda os vectores

$$\mathfrak{a}_h = \{a_{1h}, a_{2h}, \ldots, a_{mh}\}, \qquad \mathfrak{b} = \{b_1, \ldots, b_m\},$$

o sistema (13) pode escrever-se abreviadamente

$$\mathfrak{a}_1 x_1 + \mathfrak{a}_2 x_2 + \ldots + \mathfrak{a}_n x_n = \mathfrak{b}. \tag{14}$$

Sob a forma (14), reconhece-se que é condição necessária e suficiente, para que (13) tenha soluções, que a multiplicidade vectorial construída sobre $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, ou gerada por $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, contenha o vector $\mathfrak{b}$. Claro que essa multiplicidade é a mesma que é gerada por aqueles $\mathfrak{a}_j$, de entre os $\mathfrak{a}_n$, que são linearmente independentes. E estes últimos são em número igual ao número máximo de colunas (ou de linhas) independentes da matriz

$$\begin{pmatrix} a_{11} & a_{12} & \ldots a_{1n} \\ a_{21} & a_{22} & \ldots a_{2n} \\ \ldots\ldots\ldots\ldots \\ a_{m1} & a_{m2} & \ldots a_{mn} \end{pmatrix}, \tag{15}$$

chamada *matriz simples* do sistema (13). Como para a existência de solução é necessário e basta que $\mathfrak{b}$ se exprima nos $\mathfrak{a}_j$, segue-se que o número máximo de colunas independentes da matriz

$$\begin{pmatrix} a_{11} & a_{12} & \ldots a_{1n} & b_1 \\ \ldots\ldots\ldots\ldots\ldots \\ a_{m1} & a_{m2} & \ldots a_{mn} & b_m \end{pmatrix},$$

chamada *matriz ampliada* do sistema (13), deve ser o mesmo que o de (15). Tem lugar o seguinte

TEOREMA 15: — *É condição necessária e suficiente, para que o sistema* (13), *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.*

2) **Os sistemas homogéneos** — Quando o vector $\mathfrak{b}$, de (14), é o vector nulo, o sistema correspondente (13) diz-se *homogéneo*. O teorema 15 é sempre verificado neste caso, de sorte que o sistema

$$a_{i1} x_1 + \ldots + a_{in} x_n = o, \tag{16}$$

$(i = 1, 2, \ldots, m)$, tem sempre soluções em $\mathfrak{K}$. Uma solução evidente é o ponto $(o, o, \ldots, o)$. É aqui cómoda a linguagem

a seguir. Um sistema de soluções de (16) diz-se um vector de $\mathfrak{M}_n$ (mais precisamente: os valores atribuídos aos x_k são as componentes dum vector de $\mathfrak{M}_n$, numa certa base prèviamente fixada). Então, é imediato este

TEOREMA 16: — *Os vectores-soluções de* (16) *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 (13) dizem-se equivalentes, se tiverem as mesmas soluções.

Se efectuarmos na matriz do sistema (16) (matriz simples) transformações dos tipos 1.º e 2.º, a matriz modifica-se, podendo fazer-se corresponder à transformada um sistema linear com o mesmo aspecto (16). Então, é válido este

TEOREMA 17: — *Os sistemas da forma* (16), *que correspondem às matrizes obtidas da matriz de* (16) *por transformações simples envolvendo apenas linhas, são equivalentes ao sistema* (16). A demonstração, que é extremamente fácil, é deixada ao cuidado do leitor.

Posto isto, imaginemos que é r a característica da matriz de (16) e que as primeiras r colunas são linearmente independentes. As transformações simples que envolvem linhas podem levar a matriz à forma referida no teorema 9, n.º 4, § 1. O sistema (16) ficará equivalente ao seguinte:

$$\begin{aligned} &x_1 + b_{1,r+1}\,x_{r+1} + \ldots + b_{1n}\,x_n = o,\\ &x_2 + b_{2,r+1}\,x_{r+1} + \ldots + b_{2n}\,x_n = o,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ &x_r + b_{r,r+1}\,x_{r+1} + \ldots + b_{rn}\,x_n = o. \end{aligned} \tag{17}$$

É agora fácil de encontrar a base que estamos procurando. É a base da multiplicidade solução de (17). Como há soluções, há certos valores $a_{r+1}, \ldots, a_n$, que podem ser atribuídos aos

$x_{r+1}, \ldots, x_n$, resultando daí os valores correspondentes a atribuir aos $x_1, \ldots, x_r$. De facto, (17) revela podermos dar valores quaisquer aos $x_{r+1}, \ldots, x_n$, resultando deles os valores correspondentes dos $x_1, \ldots, x_r$. Em suma: se pusermos $x_{r+1} = a_{r+1}, \ldots, x_n = a_n$, a solução ξ, de (17), ou de (16), é

$$\begin{aligned} \xi = &- e_1\,(b_{1,r+1}\,a_{r+1} + \ldots + b_{1n}\,a_n) -\\ &- e_2\,(b_{2,r+1}\,a_{r+1} + \ldots + b_{2n}\,a_n) -\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ &- e_r\,(b_{r,r+1}\,a_{r+1} + \ldots + b_{rn}\,a_n) +\\ &+ e_{r+1}\,a_{r+1} + \ldots + e_n\,a_n. \end{aligned} \tag{18}$$

Para o caso particular $a_{r+1} = 1$, $a_{r+2} = \ldots = a_n = o$, tem-se

$$\xi_1 = - e_1\,b_{1,r+1} - e_2\,b_{2,r+1} - \ldots - e_r b_{r,r+1} + e_{r+1}; \tag{18'}$$

para o caso particular $a_{r+2} = 1$, $a_{r+1} = a_{r+3} = \ldots = a_n = o$, tem-se

$$\begin{aligned} \xi_2 = &- e_1\,b_{1,r+2} - e_2\,b_{2,r+2} - \ldots\\ &\ldots - e_r\,b_{r,r+2} + e_{r+2};\ \text{etc.,} \end{aligned} \tag{18'}$$

até

$$\xi_{n-r} = - e_1\,b_{1n} - e_2\,b_{2n} - \ldots - e_r\,b_{rn} + e_n. \tag{18'}$$

Então, (18) pode tomar o aspecto

$$\xi = \xi_1\,a_{r+1} + \xi_2\,a_{r+2} + \ldots + \xi_{n-r}\,a_n. \tag{19}$$

Os vectores $\xi_1, \ldots, \xi_{n-r}$ são linearmente independentes, como se conclui das suas próprias expressões, nas quais figuram, respectivamente, $e_{r+1}, \ldots, e_n$. Em (19) tem-se a totalidade de soluções de (16), o que, repetimos, deve entender-se no sentido seguinte: fixada a base $e_1, \ldots, e_n$, na qual $\xi_1, \ldots, \xi_{n-r}$ têm as expressões (18'), os valores a atribuir aos x_h, em cada

solução, são as componentes do vector $\mathfrak{x}$, definido por (19), com os α_j arbitrários em $\mathfrak{K}$. Tem lugar o

TEOREMA 18: — *Um sistema da forma* (16), *de característica* r *(característica da matriz do sistema) representa uma multiplicidade vectorial de dimensão* n — r. Este teorema tem o seguinte recíproco:

TEOREMA 19: — *Toda a submultiplicidade vectorial de* $\mathfrak{M}_n$, *de dimensão* n — r, *pode ser representada por um sistema homogéneo da forma* (16), *de característica* r. Se a representação for efectivamente possível, o sistema (16) tem de conter, pelo menos, r equações. Vamos encontrar exactamente r equações que dão a representação. Suponhamos $\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-r}$ uma base da multiplicidade dada $\mathfrak{M}_{n-r}$ e consideremos o sistema a seguir, de $n-r$ equações homogéneas:

$$\mathfrak{a}_1 . \mathfrak{x} = o, \quad \ldots, \quad \mathfrak{a}_{n-r} . \mathfrak{x} = o, \tag{20}$$

onde $\mathfrak{a}_i . \mathfrak{x}$ é uma abreviatura de $a_{i1} x_1 + \ldots + a_{in} x_n$ e os a_{ik}, $(k = 1, 2, \ldots, n)$, são as componentes de $\mathfrak{a}_i$. O sistema (20) tem a característica $n-r$ e representa uma multiplicidade vectorial de ordem r. Se $\mathfrak{b}_1, \ldots, \mathfrak{b}_r$ for uma base dessa multiplicidade, as equações

$$\mathfrak{b}_1 . \mathfrak{x} = o, \quad \ldots, \quad \mathfrak{b}_r . \mathfrak{x} = o, \tag{21}$$

formam um sistema de característica r, que representa uma multiplicidade de ordem $n-r$. Mas, tendo-se, por virtude de (20), $\mathfrak{a}_1 . \mathfrak{b}_j = o, \ldots, \mathfrak{a}_{n-r} . \mathfrak{b}_j$ [1] $= o$, $(j = 1, 2, \ldots, r)$, vê-se que (21) é satisfeito pondo $\mathfrak{x} = \mathfrak{a}_1, \ldots, \mathfrak{a}_{n-r}$. Então, (21) representa a multiplicidade de que se partiu.

3) **Os sistemas não homogéneos** — Regressemos ao sistema (13), cujas soluções já designámos por pontos de $\mathfrak{R}_n$,

(1) Duma maneira geral, $\mathfrak{a} . \mathfrak{b}$ é a abreviatura de $a_1 b_1 + \ldots + a_n b_n$, supostos os a_i as componentes de $\mathfrak{a}$ e os b_j as componentes de $\mathfrak{b}$.

prèviamente fixado um referencial $O_o(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$. Se $P(x_1, \ldots, x_n)$ e $Q(y_1, \ldots, y_n)$ são dois pontos-soluções, o vector $\overrightarrow{PQ} = \mathfrak{z}$, de componentes $y_1 - x_1, \ldots, y_n - x_n$, verifica o sistema homogéneo correspondente (16). Inversamente, se $\mathfrak{z}$ é solução de (16), tomando o ponto P, solução de (13), e pondo $\overrightarrow{PQ} = \mathfrak{z}$, por via da igualdade $\overrightarrow{O_oP} + \overrightarrow{PQ} = \overrightarrow{O_oQ}$, ou $\overrightarrow{PQ} = \overrightarrow{O_oQ} - \overrightarrow{O_oP}$, determina-se um ponto-solução de (13). Podemos dar este enunciado:

TEOREMA 20: — *A totalidade dos pontos-soluções de* (13) *constitui um espaço linear com* n — r *dimensões, se* r *for a característica do sistema.* Neste enunciado, entende-se por característica do sistema o número r, que é característica comum da matriz simples e da matriz ampliada.

O teorema 20 tem o seguinte recíproco:

TEOREMA 21: — *Todo o subespaço linear de* $\mathfrak{R}_n$, *de dimensão* n — r, *pode ser representado por um sistema não homogéneo, da forma* (13), *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

$$a_{i1} x_1 + \ldots + a_{in} x_n = o, \quad (i = 1, 2, \ldots, m).$$

Se designarmos por $\xi_1, \ldots, \xi_n$ as coordenadas do ponto conhecido do subespaço, ponhamos

$$a_{i1} \xi_1 + \ldots + a_{in} \xi_n = b_i, \quad (i = 1, 2, \ldots, m),$$

e escrevamos o sistema não homogéneo

$$a_{i1} x_1 + \ldots + a_{in} x_n = b_i, \quad (i = 1, 2, \ldots, m).$$

Este sistema é solúvel e representa, no referencial de que se partiu, o subespaço linear dado.

OBSERVAÇÃO IMPORTANTE: — O sistema (13) 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 de Ω, de modo que (13) 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 que tem lugar este

TEOREMA 22: — *Se* Ω *é um corpo e* $\mathfrak{K} \subseteq \Omega$ *um subcorpo, dado um sistema* (13), *com coeficientes em* $\mathfrak{K}$, *a solubilidade do sistema, em* Ω, *implica a sua solubilidade em* $\mathfrak{K}$.

§ 3 — **Determinantes**

1) **Definição** — Em estreita correlação com a teoria do espaço linear e das equações lineares que desenvolvemos nos dois §§ anteriores, encontra-se a teoria dos determinantes, de que nos vamos ocupar.

Dada a multiplicidade $\mathfrak{M}_n$, numa certa base $e_1, \ldots, e_n$, chama-se *determinante* uma função de n vectores $a_1, \ldots, a_n$, representada por $D(a_1, \ldots, a_n)$, que satisfaz às três condições seguintes:

I) $D(a_1, \ldots, a_n)$ não se altera, quando o vector a_i se substitui por $a_i + a_h$, $(h \neq i)$;

II) $D(a_1, \ldots, a_n)$ vem multiplicado por λ, se um dos vectores a_i se substitui por $a_i \lambda$;

III) $D(e_1, \ldots, e_n) = u \in \mathfrak{K}$.

Mostrar que existe uma tal função D, que ela é única e reconhecer algumas das suas propriedades fundamentais, é o objectivo essencial deste §.

2) **Propriedades dos determinantes** — A fim de simplificarmos a escrita, adoptaremos as convenções a seguir.

Partindo dum certo determinante $D(a_1, \ldots, a_n)$, 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, $D(a_1, \ldots, a_n) = D$, e suponhamos a_i igual a zero. Em virtude de II), é $D(a_i \lambda) = D\lambda$; mas, por outro lado, se $a_i = 0$, é $a_i \lambda = 0$, e, portanto, $D(a_i \lambda) = D$. Conclui-se $D\lambda = D$, ou $D(\lambda - u) = o$, qualquer que seja $\lambda \in \mathfrak{K}$. Fazendo $\lambda = o$, vem $D = o$, pelo que

TEOREMA 23: — *Se, no determinante* $D(a_1, \ldots, a_n)$, *um dos vectores é nulo, o determinante é igual a zero.*

Voltemos a D. Em virtude de I) e II) tem-se

$$D(a_i + a_k) = D, \quad D(a_i \lambda) = D\lambda, \quad (i \neq k).$$

Daqui se conclui

$$D(a_k \lambda_k) = D\lambda_k = D(a_i + a_k \lambda_k, a_k \lambda_k), \quad (i \neq k),$$

$$D(a_i + a_k \lambda_k, a_k \lambda_k) = D(a_i + a_k \lambda_k, a_k)\lambda_k = D\lambda_k,$$

de sorte que

$$D(a_i + a_k \lambda_k) = D, \quad (i \neq k).$$

Repetindo o processo, chega-se ao seguinte

TEOREMA 24: — *O determinante* D *não muda de valor, se um dos vectores* a_i *se substituir por* $a_i + \Sigma a_k \lambda_k$, *suposto o somatório não estendido ao índice* i.

COROLÁRIO 4: — *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, $a_1\lambda_1 + \ldots + a_n\lambda_n = 0$, e imaginemos, por ex., $\lambda_n \neq o$. Ter-se-á

$$a_n = -a_1\frac{\lambda_1}{\lambda_n} - \ldots - a_{n-1}\frac{\lambda_{n-1}}{\lambda_n},$$

e também, pelo teorema anterior,

$$D\left(a_n + a_1\frac{\lambda_1}{\lambda_n} + \ldots + a_{n-1}\frac{\lambda_{n-1}}{\lambda_n}\right) = D\,(a_n = 0) = o,$$

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

$$D = D\,(a_i, a_k) \to D\,(a_i, a_k + a_i) = D \to$$
$$\to D\,(a_i, -a_k - a_i) = -D \to D\,(-a_k, -a_k - a_i) = -D \to$$
$$\to D\,(a_k, -a_k - a_i) = D \to D\,(a_k, -a_i) = D \to$$
$$\to D\,(a_k, a_i) = -D.$$

Conclui-se:

TEOREMA 25: — *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 4:

COROLÁRIO 5: — *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

$$D(a + b, a_2, \ldots, a_n) = D(a, a_2, \ldots, a_n) + D(b, a_2, \ldots, a_n),$$

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 $a_2, \ldots, a_n$ são linearmente dependentes, a igualdade é válida, pelo facto de todos os 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

$$a = c\lambda + a_2\lambda_2 + \ldots + a_n\lambda_n,$$
$$b = c\mu + a_2\mu_2 + \ldots + a_n\mu_n,$$

e, portanto,

$$D(a, a_2, \ldots, a_n) = D(c\lambda, a_2, \ldots, a_n) = D(c, a_2, \ldots, a_n)\lambda,$$
$$D(b, a_2, \ldots, a_n) = D(c, a_2, \ldots, a_n)\mu,$$
$$D(a + b, a_2, \ldots, a_n) = D(c, a_2, \ldots, a_n)(\lambda + \mu),$$

que levam imediatamente à igualdade em questão.

Uma repetição do raciocínio permite o enunciado seguinte, conhecido sob o nome de *teorema da adição.*

TEOREMA 26: — *Supondo* $\xi_i = \sum_{h_i=1}^{n} a_{ih_i}\lambda_{ih_i}$, $(i = 1, 2, \ldots, n)$, *tem-se* $D(\xi_1, \ldots, \xi_n) = D(\sum a_{1h_1}\lambda_{1h_1}, \xi_2, \ldots, \xi_n) = \sum_{h_1=1}^{n} D(a_{1h_1}, \xi_2, \ldots, \xi_n)\lambda_{1h_1} = \ldots = \sum_{h_1,\ldots,h_n=1}^{n} D(a_{1h_1}, \ldots, a_{nh_n})\lambda_{1h_1}\ldots\lambda_{nh_n}$. (22)

Claramente que não há necessidade de se admitir haver nas expressões de todos os ξ_i o mesmo número de parcelas. Alguns dos coeficientes λ_{ih_i} podem ser nulos.

COROLÁRIO 6: — *Admitindo que é* $D(a_1, \ldots, a_n) = 0$, *é também* $D(\xi_1, \ldots, \xi_n) = 0$, *se os* ξ_i *se exprimem nos* a_j. Na verdade, nas igualdades (22), os vectores a_{ih_i} são os mesmos para os diferentes ξ_i. No último somatório dessas igualdades figura o

determinante $D(\mathfrak{a}_{1h_1}, \ldots, \mathfrak{a}_{nh_n})$. O primeiro dos índices dos vectores $\mathfrak{a}$ pode suprimir-se, o que levará a

$$D(\mathfrak{x}_1, \ldots, \mathfrak{x}_n) = \sum_{h_1, \ldots, h_n = 1}^{n} D(\mathfrak{a}_{h_1}, \ldots, \mathfrak{a}_{h_n}) \lambda_{1h_1} \ldots \lambda_{nh_n}. \qquad (22')$$

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 $(h_1, \ldots, h_n)$ contém todos os números $1, 2, \ldots, n$. Então o determinante $D(\mathfrak{a}_{h_1}, \ldots, \mathfrak{a}_{h_n})$ é nulo, por ser, à parte o sinal, igual ao determinante $D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$. Todas as parcelas de (22′) são nulas e o primeiro membro da mesma igualdade é nulo, como afirma o corolário.

É agora que intervém a condição III) da definição de determinante, para nos levar a uma conclusão importante, a saber:

TEOREMA 27: — *Supostos* $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ *linearmente independentes, é* $D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \neq 0$. Se pudesse ter-se $D = o$, como os $\mathfrak{a}_i$ constituem uma base de $\mathfrak{M}_n$, seria $D(\mathfrak{x}_1, \ldots, \mathfrak{x}_n) = o$, quaisquer que fossem os $\mathfrak{x}_i$, em particular ter-se-ia $D(\mathfrak{e}_1, \ldots, \mathfrak{e}_n) = o$, contra a condição III).

OBSERVAÇÕES: — Como consequência das considerações feitas, é de observar o que vai a seguir-se. Se fosse definida uma função $\Phi(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ com as propriedades I) e II), atribuídas a D, e com a propriedade III′): $\Phi(\mathfrak{e}_1, \ldots, \mathfrak{e}_n) = o$; então a função Φ seria nula, quaisquer que fossem os $\mathfrak{a}_j$. Em geral, porém, uma função Φ, com as propriedades I) e II), será da forma

$$\Phi(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) = \Phi(\mathfrak{e}_1, \ldots, \mathfrak{e}_n) . D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n),$$

pois que, sendo $\Phi(\mathfrak{e}_1, \ldots, \mathfrak{e}_n) \neq o$, é

$$\frac{\Phi(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)}{\Phi(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)}$$

uma função com as propriedades I), II) e III).

3) **A existência e univocidade do determinante** — Do teorema da adição, pondo $\mathfrak{a}_j = \mathfrak{e}_1 a_{j1} + \ldots + \mathfrak{e}_n a_{jn}$, $(j = 1, 2, \ldots, \ldots, n)$, resulta

$$D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) = \sum_{h_1, \ldots, h_n = 1}^{n} D(\mathfrak{e}_{h_1}, \ldots, \mathfrak{e}_{h_n}) a_{1h_1} \ldots a_{nh_n}.$$

Como o somatório se pode estender apenas às «permutações» (1) dos números $1, 2, \ldots, n$, [pelo facto de as outras parcelas serem nulas], a igualdade anterior será escrita sob a forma

$$D = \sum_{(h_1, \ldots, h_n)}^{n} D(\mathfrak{e}_{h_1}, \ldots, \mathfrak{e}_{h_n}) a_{1h_1} \ldots a_{nh_n}, \qquad (23)$$

onde o símbolo $(h_1, \ldots, h_n)$ lembra precisamente aquela circunstância. Examinemos, em seguida, o determinante $D(\mathfrak{e}_{h_1}, \ldots, \ldots, \mathfrak{e}_{h_n})$, para o compararmos com o determinante $D(\mathfrak{e}_1, \ldots, \ldots, \mathfrak{e}_n)$. O valor deles pode diferir apenas no sinal. Decomponhamos a permutação

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ h_1 & h_2 & \ldots & h_n \end{pmatrix} \qquad (24)$$

em transposições. Se a cada transposição (ij) fizermos corresponder uma troca dos vectores $\mathfrak{e}_i$ e $\mathfrak{e}_j$, num determinante em que $\mathfrak{e}_1, \ldots, \mathfrak{e}_n$ se encontram numa ordem qualquer, vemos que, partindo do determinante $D(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$, e efectuando, sucessivamente, as trocas indicadas pelas transposições que figuram como factores na decomposição de (24), pela ordem pela qual se devem considerar esses mesmos factores na referida decomposição, se chega precisamente a

$$D(\mathfrak{e}_{h_1}, \ldots, \mathfrak{e}_{h_n}) = \pm D(\mathfrak{e}_1, \ldots, \mathfrak{e}_n),$$

(1) Muitas vezes, empregaremos a palavra «permutação» dos números 1, 2, ..., n para significar simplesmente uma nova disposição daqueles números.

conforme for par ou ímpar o número de transposições em causa. A igualdade (23) reduz-se, desta forma, a

$$D(a_1, \ldots, a_n) = \sum_{(h_1, \ldots, h_n)} P(h_1, \ldots, h_n)\, a_{1h_1} \ldots a_{nh_n}, \quad (25)$$

onde $P(h_1, \ldots, h_n) = \pm 1$ indica a paridade da permutação (24), também chamada paridade de $(h_1, \ldots, h_n)$.

Um processo para a determinação de $P(h_1, \ldots, h_n)$ é o que vai indicar-se. Suponhamos que, em $(h_1, \ldots, h_n)$, 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 $(h_1, \ldots, h_n)$. Depois, se houver m_2 inversões relativamente a 2, na nova permutação obtida, [número que é o mesmo que em $(h_1, \ldots, h_n)$], fazem-se m_2 trocas, a fim de se colocar 2 em segundo lugar. O processo continua, até se disporem todos os números na sua ordem natural, à custa de $m_1 + m_2 + \ldots + m_\rho$ trocas, tantas quantas as inversões em $(h_1, \ldots, h_n)$. Será precisamente

$$P(h_1, \ldots, h_n) = (-1)^{m_1 + m_2 + \ldots + m_\rho}.$$

Para que o leitor compreenda perfeitamente esta igualdade, vamos tomar um exemplo. A permutação (2 4 3 5 1), dos números 1, 2, 3, 4, 5, tem as inversões $5-1$, $3-1$, $4-1$, $2-1$, 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 $m_1 + m_2 + \ldots + m_\rho = 5$. Ora tem-se

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} = (15)\,(13)\,(14)\,(12)\,(34),$$

pelo que $P(2, 4, 3, 5, 1) = -1 = (-1)^5$.

OBSERVAÇÃO: — Ser-nos-á útil posteriormente uma observação que vamos fazer. Tomemos uma permutação $(i_1, i_2, \ldots, i_n)$

dos números $1, 2, \ldots, n$. Se trocarmos dois dos i_j, como isso equivale a multiplicar por mais uma transposição a permutação

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix},$$

segue-se que muda a paridade das inversões. Quando se escreve um produto

$$a_{i_1 j_1} a_{i_2 j_2} \ldots a_{i_n j_n}, \quad (25')$$

onde os i_k e os j_m vão de 1 a n, se somarmos 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 (25'), podemos dispor os factores por uma ordem qualquer, para calcularmos a referida paridade. Então, (25) pode tomar este outro aspecto

$$D(a_1, \ldots, a_n) = \sum_{(j_1, \ldots, j_n)}^{n} P(i_1, \ldots, i_n).P(j_1, \ldots, j_n)\, a_{i_1 j_1} \ldots a_{i_n j_n},$$

onde a permutação $(i_1, \ldots, i_n)$ se fixou prèviamente.

Posto isto, estamos em condições de afirmar que, se a função determinante existe, ela não pode deixar de ser dada pela igualdade (25). A *univocidade* está provada, provada que seja a *existência*.

Quanto a esta última, vamos exactamente demonstrar que o 2.º membro de (25) tem as propriedades I), II) e III).

A propriedade II) é imediata, porque, em cada parcela do 2.º membro de (25), figura uma componente, e uma só, de cada vector $a_1, \ldots, a_n$. Se um dos vectores se multiplica por λ, todas as suas componentes aparecem multiplicadas por λ, e, assim, cada parcela de (25) aparece multiplicada por λ. A propriedade III) também se verifica, pelo facto de ser $a_{ik_i} = o$, se $k_i \neq i$, $(i = 1, 2, \ldots, n)$, e $a_{ik_i} = 1$, se $k_i = i$. Deste modo

é $D(e_1, \ldots; e_n) = P(1, 2, \ldots, n)\, 1 \ldots 1 = 1$. Resta a propriedade I). Substituamos a_i por $a_i + a_j$. Virá

$$D(a_i + a_j) = \sum_{(k_1, \ldots, k_n)}^{n} P(k_1, \ldots, k_n)\, a_{1k_1} \ldots (a_{ik_i} + a_{jk_i}) \ldots a_{nk_n} = \Sigma P(k_1, \ldots, k_n)\, a_{1k_1} \ldots a_{ik_i} \ldots a_{nk_n} + \Sigma P(k_1, \ldots, k_n)\, a_{1k_1} \ldots a_{i-1,k_{i-1}}\, a_{jk_i} \ldots a_{nk_n}.$$

Deste último membro, o primeiro somatório é igual a $D(a_1, \ldots, a_n)$, pelo que, se o segundo for nulo, fica provada a afirmação. Isto vai resultar de haver no segundo somatório parcelas iguais duas a duas, com mudança de sinal. À parcela

$$P(k_1, \ldots, k_i, \ldots, k_j, \ldots, k_n)\, a_{1k_1} \ldots a_{jk_i} \ldots a_{jk_j} \ldots a_{nk_n}$$

corresponde, de facto, a parcela

$$P(k_1, \ldots, k_j, \ldots, k_i, \ldots, k_n)\, a_{1k_1} \ldots a_{jk_j} \ldots a_{jk_i} \ldots a_{nk_n},$$

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 $P(k_1, \ldots, k_i, \ldots, k_j, \ldots, k_n) = -P(k_1, \ldots, k_j, \ldots, k_i, \ldots, k_n)$, o resultado desejado fica estabelecido. Tem lugar o importante

TEOREMA 28: — *Consideremos uma base de* $\mathfrak{M}_n$ *e tomemos, nessa base, os vectores* $a_i = \sum_{j=1}^{n} e_j a_{ij}$, $(i = 1, 2, \ldots, n)$. *Existe a função determinante* $D(a_1, \ldots, a_n)$, *que é única e tem a expressão*

$$D(a_1, \ldots, a_n) = \sum_{(h_1, \ldots, h_n)}^{n} P(h_1, \ldots, h_n)\, a_{1h_1} a_{2h_2} \ldots a_{nh_n}. \quad (26)$$

4) **Os quadros dos determinantes** — A expressão encontrada para D sugere se escreva

$$D = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}, \quad (27)$$

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 $a_{11}, a_{22}, \ldots, a_{nn}$ formam a *diagonal principal* de D e os elementos $a_{n1}, a_{n-1,2}, \ldots, a_{1n}$ formam a *segunda diagonal*.

Neste número, utilizaremos os quadros com o aspecto (27), a fim de darmos alguns resultados de cálculo, muito úteis nas aplicações.

1.º EXEMPLO: — Façamos a hipótese de se ter $a_{ih} = o$, sempre que $i > h$. Significa isto que são nulos todos os elementos abaixo da primeira diagonal. O determinante diz-se *triangular*. Na fórmula (26), 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

$$D = P(1, 2, \ldots, n)\, a_{11}\, a_{22} \ldots a_{nn} = a_{11}\, a_{22} \ldots a_{nn}.$$

2.º EXEMPLO: — Na hipótese de se ter $a_{ih} = o$, 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

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1r} & o & o & \ldots & o \\ a_{21} & a_{22} & \ldots & a_{2r} & o & o & \ldots & o \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{r1} & a_{r2} & \ldots & a_{rr} & o & o & \ldots & o \\ o & o & \ldots & o & b_{11} & b_{12} & \ldots & b_{1s} \\ o & o & \ldots & o & b_{21} & b_{22} & \ldots & b_{2s} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ o & o & \ldots & o & b_{s1} & b_{s2} & \ldots & b_{ss} \end{vmatrix},$$

no qual $r + s = n$. Se imaginarmos os b_{hl} como constantes e os a_{ij} como variáveis, podemos conceber $\Delta = \Phi(a_1, \ldots, a_r)$

como uma função de vectores $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$, num espaço a r dimensões, desde que se tomem para componentes dos $\mathfrak{a}_i$ os números $a_{i1}, a_{i2}, \ldots, a_{ir}$, numa certa base $\mathfrak{e}_1, \ldots, \mathfrak{e}_r$. Verifica-se que Φ goza das propriedades I) e II), de sorte que será

$$\Delta = \Phi(\mathfrak{e}_1, \ldots, \mathfrak{e}_r) \cdot \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1r} \\ a_{21} & a_{22} & \ldots & a_{2r} \\ \ldots & \ldots & \ldots & \ldots \\ a_{r1} & a_{r2} & \ldots & a_{rr} \end{vmatrix},$$

onde $\Phi(\mathfrak{e}_1, \ldots, \mathfrak{e}_r)$ resulta de Δ fazendo todos os $a_{ij} = o$, salvo os da primeira diagonal, que se põem iguais a $u \in \mathfrak{R}$.

Em seguida, $\Phi(\mathfrak{e}_1, \ldots, \mathfrak{e}_r)$ pode imaginar-se como uma função $\Psi(\mathfrak{b}_1, \ldots, \mathfrak{b}_s)$, dos vectores $\mathfrak{b}_1, \ldots, \mathfrak{b}_s$, num espaço a s dimensões, desde que se tomem para componentes dos $\mathfrak{b}_j$ os números $b_{j1}, \ldots, b_{js}$, numa certa base $\mathfrak{h}_1, \ldots, \mathfrak{h}_s$. Pela mesma razão de acima, será

$$\Psi(\mathfrak{b}_1, \ldots, \mathfrak{b}_s) = \Phi(\mathfrak{e}_1, \ldots, \mathfrak{e}_r) =$$
$$= \Psi(\mathfrak{h}_1, \ldots, \mathfrak{h}_s) \cdot \begin{vmatrix} b_{11} & b_{12} & \ldots & b_{1s} \\ \ldots & \ldots & \ldots & \ldots \\ b_{s1} & b_{s2} & \ldots & b_{ss} \end{vmatrix},$$

onde $\Psi(\mathfrak{h}_1, \ldots, \mathfrak{h}_s)$ resulta de $\Psi(\mathfrak{b}_1, \ldots, \mathfrak{b}_s)$ fazendo todos os $b_{kl} = o$, salvo os da primeira diagonal, que se põem iguais a $u \in \mathfrak{R}$. Visto ser $\Psi(\mathfrak{h}_1, \ldots, \mathfrak{h}_s) = 1$, chega-se a

$$\Delta = \begin{vmatrix} a_{11} & \ldots & a_{1r} \\ \ldots & \ldots & \ldots \\ a_{r1} & \ldots & a_{rr} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & \ldots & b_{1s} \\ \ldots & \ldots & \ldots \\ b_{s1} & \ldots & b_{ss} \end{vmatrix}.$$

Como problema imediato, 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

$$\begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & b_{12} & \ldots & b_{1n} \\ b_{21} & b_{22} & \ldots & b_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ b_{n1} & b_{n2} & \ldots & b_{nn} \end{vmatrix} =$$

$$= \begin{vmatrix} \sum_{j=1}^{n} a_{1j} b_{j1} & \sum_{j=1}^{n} a_{1j} b_{j2} & \ldots & \sum_{j=1}^{n} a_{1j} b_{jn} \\ \sum_{j=1}^{n} a_{2j} b_{j1} & \sum_{j=1}^{n} a_{2j} b_{j2} & \ldots & \sum_{j=1}^{n} a_{2j} b_{jn} \\ \ldots & \ldots & \ldots & \ldots \\ \sum_{j=1}^{n} a_{nj} b_{j1} & \sum_{j=1}^{n} a_{nj} b_{j2} & \ldots & \sum_{j=1}^{n} a_{nj} b_{jn} \end{vmatrix}.$$

Para isso, ponhamos

$$\mathfrak{c}_i = \mathfrak{a}_1 a_{i1} + \ldots + \mathfrak{a}_n a_{in}, \quad (i = 1, 2, \ldots, n), \quad (28)$$

de sorte que

$$D(\mathfrak{c}_1, \ldots, \mathfrak{c}_n) = \sum_{(h_1, \ldots, h_n)} D(\mathfrak{a}_{h_1}, \ldots, \mathfrak{a}_{h_n}) a_{1h_1} \ldots$$
$$\ldots a_{nh_n} = \sum_{(h_1, \ldots, h_n)} D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) P(h_1, \ldots, h_n) a_{1h_1} \ldots$$
$$\ldots a_{nh_n} = D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \sum_{(h_1, \ldots, h_n)} P(h_1, \ldots, h_n) a_{1h_1} \ldots$$
$$\ldots a_{nh_n} = D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \cdot \begin{vmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{nn} \end{vmatrix}.$$

Se imaginarmos os $\mathfrak{a}_j$ escolhidos prèviamente pelas relações

$$\mathfrak{a}_j = \mathfrak{e}_1 b_{j1} + \ldots + \mathfrak{e}_n b_{jn}, \quad (29)$$

nas quais $\mathfrak{e}_1, \ldots, \mathfrak{e}_n$ formam a base de $\mathfrak{M}_n$, tomada *a priori* sob a condição $D(\mathfrak{e}_1, \ldots, \mathfrak{e}_n) = 1$, vemos que

$$D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) = \sum_{(j_1, \ldots, j_n)} D(\mathfrak{e}_{j_1}, \ldots, \mathfrak{e}_{j_n}) b_{1j_1} \ldots b_{nj_n} =$$
$$= \sum_{(j_1, \ldots, j_n)} P(j_1, \ldots, j_n) b_{1j_1} \ldots b_{nj_n} = \begin{vmatrix} b_{11} & \ldots & b_{1n} \\ \ldots & \ldots & \ldots \\ b_{1n} & \ldots & b_{nn} \end{vmatrix},$$

de sorte que

$$D(\mathfrak{c}_1, \ldots, \mathfrak{c}_n) = \begin{vmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{nn} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & \ldots & b_{1n} \\ \ldots & \ldots & \ldots \\ b_{n1} & \ldots & b_{nn} \end{vmatrix}. \quad (30)$$

Por outro lado, porém, as componentes dos ι_i, tendo em conta (28) e (29), são

$$c_{i1} = \sum_{j=1}^{n} a_{ij} b_{j1}, \quad \ldots, \quad c_{in} = \sum_{j=1}^{n} a_{ij} b_{jn},$$

pelo que, escrevendo em vez do 1.º membro de (30) o respectivo quadro, fica estabelecida a igualdade desejada. Podemos enunciar o chamado *teorema da multiplicação de determinantes:*

TEOREMA 29: — *Obtém-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 (27), 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 de (27), a saber:

$$\mathfrak{a}'_i = \{a_{1i}, a_{2i}, \ldots, a_{ni}\}, \qquad (i = 1, 2, \ldots, n).$$

O quadro, cujo valor é conhecido, é função dos $\mathfrak{a}'_i$, tendo-se

$$\Theta(\mathfrak{a}'_1, \ldots, \mathfrak{a}'_n) = |a_{ih}| = \Phi(\mathfrak{a}_1, \ldots, \mathfrak{a}_n).$$

Vamos ver que Θ goza das propriedades I), II) e III), o que nos permitirá escrever

$$\Theta(\mathfrak{a}'_1, \ldots, \mathfrak{a}'_n) = D(\mathfrak{a}'_1, \ldots, \mathfrak{a}'_n) = \begin{vmatrix} a_{11} & a_{21} & \ldots & a_{n1} \\ a_{12} & a_{22} & \ldots & a_{n2} \\ \ldots & \ldots & \ldots & \ldots \\ a_{1n} & a_{2n} & \ldots & a_{nn} \end{vmatrix}$$

e enunciar o seguinte

TEOREMA 30: — *O valor dum determinante não se altera quando se mudam as linhas em colunas e as colunas em linhas* [*rotação*

espacial de 180° à volta da primeira diagonal]. A propriedade II) é consequência imediata da igualdade (25), pois que cada termo do respectivo somatório tem um e um só elemento de cada coluna. A propriedade III) é válida, porque, se fizermos $\mathfrak{a}'_i = \mathfrak{e}_i$, $(i = 1, 2, \ldots, n)$, o quadro (27) é exactamente o quadro relativo a $\Phi(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$. Quanto à propriedade I), imaginemos que se substitui (27) pelo quadro

$$\begin{vmatrix} a_{11} & \ldots & a_{1,i-1} & a_{1i} + a_{1k} & \ldots & a_{1n} \\ a_{21} & \ldots & a_{2,i-1} & a_{2i} + a_{2k} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{n,i-1} & a_{ni} + a_{nk} & \ldots & a_{nn} \end{vmatrix}, \tag{31}$$

isto é, que se considera o quadro obtido por substituição de $\mathfrak{a}'_i$ por $\mathfrak{a}'_i + \mathfrak{a}'_k$. Verifica-se imediatamente que é

$$\Theta(\mathfrak{a}'_1, \ldots, \mathfrak{a}'_{i-1}, \mathfrak{a}'_i + \mathfrak{a}'_k, \ldots, \mathfrak{a}'_n) = \Theta(\mathfrak{a}'_1, \ldots, \mathfrak{a}'_n) \cdot D(\mathfrak{e}_1, \ldots, \mathfrak{e}_{k-1}, \mathfrak{e}_k + \mathfrak{e}_i, \ldots \mathfrak{e}_n), \tag{32}$$

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 $u \in \mathfrak{K}$, 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 de (32) pela regra de produto de determinantes, encontra-se o valor (31). Mas, como $D(\mathfrak{e}_1, \ldots, \mathfrak{e}_{k-1}, \mathfrak{e}_k + \mathfrak{e}_i, \ldots, \mathfrak{e}_n) = 1$, obtém-se ainda

$$\Theta(\mathfrak{a}'_1, \ldots, \mathfrak{a}'_{i-1}, \mathfrak{a}'_i + \mathfrak{a}'_k, \ldots, \mathfrak{a}'_n) = \Theta(\mathfrak{a}'_1, \ldots, \mathfrak{a}'_n),$$

como se deseja.

OBSERVAÇÃO: — Os resultados acabados de encontrar permitem-nos dar outras regras para o produto de determinantes, diferentes da regra contida no teorema 29, 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 multiplicação de colunas por linhas e de colunas por colunas.

Citemos agora outros exemplos que convém conhecer.

4.º EXEMPLO: — Um determinante D diz-se *hemi-simétrico,* se o quadro correspondente (27) satisfizer às condições $a_{ih} = -a_{hi}$, se $h \neq i$, e $a_{ii} = o$, $(i = 1, 2, \ldots, n)$. Trocando num tal determinante as linhas com as colunas, obtém-se outro determinante D', igual a D, que também resulta de D por mudança do sinal de todas as linhas. Supondo D de ordem ímpar, tem-se $D' = (-1)^n D = -D = D$, o que leva à seguinte proposição de JACOBI:

TEOREMA 31: — *Se $\mathfrak{K}$ não tem a característica 2, um determinante hemi-simétrico de ordem ímpar, com elementos de $\mathfrak{K}$, é nulo.* Acrescentemos que este resultado é geral.

5.º EXEMPLO: — Um determinante D diz-se *simétrico,* se o quadro correspondente (27) verificar a condição $a_{ih} = a_{hi}$. Propriedades interessantes dos determinantes simétricos e hemi-simétricos encontram-se nos livros dos Profs. J. VICENTE GONÇALVES e B. DE JESUS CARAÇA, citados na Bibliografia indicada no final do Capítulo.

5) **O desenvolvimento dum determinante segundo os elementos duma linha ou duma coluna** — Dado o determinante D, definido no quadro (27), um *menor* é um determinante extraído de D e contendo $r < n$ linhas e colunas. O determinante formado pelos elementos das $n - r$ linhas e 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 ex., $D_r = D_1 = |a_{ij}| =$ 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 (25).

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, 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 os termos em que figura a_{ij} se podem escrever sob a forma $a_{ij} A_{ji}$. Um termo de A_{ji} tem o aspecto

$$T = (-1)^{i+j} (-1)^f a_{1h_1} \ldots a_{i-1,h_{i-1}} a_{i+1,h_{i+1}} \ldots a_{nh_n},$$

onde f designa o número de inversões da «permutação» $(h_1, \ldots, h_{i-1}, h_{i+1}, \ldots, h_n)$ dos números $1, 2, \ldots, j-1, j+1, \ldots, n$. Tem assim de verificar-se que a quantidade

$$(-1)^{i+j+f} a_{ij} a_{1h_1} \ldots a_{i-1,h_{i-1}} a_{i+1,h_{i+1}} \ldots a_{nh_n},$$

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 da observação feita a seguir à fórmula (25), pela

soma das inversões das duas permutações $(i, 1, 2, \ldots, i-1, i+1, \ldots, n)$ e $(j, h_1, h_2, \ldots, h_{i-1}, h_{i+1}, \ldots, h_n)$, soma que é $(i-1)+f+(j-1)$, precisamente da paridade de $i+j+f$.

O resultado que acabamos de demonstrar permite-nos escrever o desenvolvimento de D segundo os elementos da linha de ordem i, sob a forma

$$D = \sum_{j=1}^{n} a_{ij} A_{ji}, \qquad (i = 1, 2, \ldots, n),$$

ou, segundo os elementos da coluna de ordem j, sob a forma

$$D = \sum_{i=1}^{n} a_{ij} A_{ji} = \sum_{i=1}^{n} A_{ji} a_{ij}, \qquad (j = 1, 2, \ldots, n).$$

Diremos:

TEOREMA 32: — *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

$$\sum_{j=1}^{n} a_{ij} A_{jk} = o, \qquad (k \neq i; \quad k, i = 1, 2, \ldots, n),$$

$$\sum_{i=1}^{n} A_{ki} a_{ij} = o, \qquad (k \neq j; \quad k, j = 1, 2, \ldots, n).$$

É válido o

TEOREMA 33: — *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 condições de fazer o cálculo que vai indicar-se, do chamado determinante de VANDERMONDE. Tem o aspecto

$$D = \begin{vmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & a_n & a_n^2 & \ldots & a_n^{n-1} \end{vmatrix} = D_n.$$

Operações imediatas levam a

$$D_n = \begin{vmatrix} 1 & o & o & \ldots & o \\ 1 & a_2 - a_1 & a_2^2 - a_2 a_1 & \ldots & a_2^{n-1} - a_2^{n-2} a_1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & a_n - a_1 & a_n^2 - a_n a_1 & \ldots & a_n^{n-1} - a_n^{n-2} a_1 \end{vmatrix},$$

de modo que, fazendo o desenvolvimento segundo os elementos da primeira linha, encontramos

$$D_n = (a_2 - a_1)(a_3 - a_1) \ldots (a_n - a_1) \cdot \begin{vmatrix} 1 & a_2 & \ldots & a_2^{n-2} \\ 1 & a_3 & \ldots & a_3^{n-2} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & a_n & \ldots & a_n^{n-2} \end{vmatrix} =$$

$$= \prod_{i \neq 1} (a_i - a_1) \cdot D_{n-1},$$

onde D_{n-1} é um determinante de VANDERMONDE da ordem $n-1$. Admitindo que, para D_{n-1}, se tem

$$D_{n-1} = \prod_{j > i} (a_j - a_i), \qquad \begin{cases} i = 2, \ldots, n-1, \\ j = 3, \ldots n, \end{cases}$$

resultará

$$D_n = \prod_{j > i} (a_j - a_i), \qquad \begin{cases} i = 1, 2, \ldots, n-1; \\ j = 2, 3, \ldots, n. \end{cases}$$

Obteve-se, pois, o valor de D_n por um método de indução, visto que, para $n=2$, é

$$D_2=\begin{vmatrix}1 & a_1\\ 1 & a_2\end{vmatrix}=a_2-a_1.$$

6) **Os determinantes e as equações lineares** — As soluções dos sistemas lineares estudados no § 2 podem revestir-se dum aspecto interessante, utilizando os determinantes. É útil, para isso, definir a característica duma matriz por um processo diferente, contido no seguinte

TEOREMA 34: — *A característica* r *duma matriz* A *é igual à 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 submatriz de A, nas quais se encontram r colunas linearmente independentes. A característica da submatriz 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 submatriz de característica r. Essa submatriz conterá r colunas igualmente independentes. O determinante formado por essas r colunas é $\neq o$. 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 35: — *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, imaginemos o determinante Δ contido nas r primeiras linhas e colunas de A. Será

$$A=\begin{pmatrix}\Delta_o & \begin{matrix}a_{1,r+1} & \dots & a_{1n}\\ \dots & \dots & \dots\end{matrix}\\ \begin{matrix}a_{m1} & \dots & a_{m,r+1} & \dots & a_{mn}\end{matrix} & \end{pmatrix}=\begin{pmatrix}\Delta_o & P\\ Q & R\end{pmatrix},$$

onde Δ_o é a matriz formada pelos elementos de Δ e P, Q, R são matrizes rectangulares de significado imediato. Ora, em

$$\Delta_o=\begin{pmatrix}a_{11} & \dots & a_{1r}\\ \dots & \dots & \dots\\ a_{r1} & \dots & a_{rr}\end{pmatrix},$$

as linhas são linearmente independentes, de sorte que r é a característica de Δ_o. Os elementos $a_{i1}, a_{i2}, \dots, a_{ir}$, com $i=r+1, \dots, n$, exprimem-se linearmente nas r linhas de Δ_o. Assim, as transformações simples permitem reduzir A à forma

$$B=\begin{pmatrix}\Delta_o & P\\ O & T\end{pmatrix},$$

onde O é a matriz nula de $m-r$ linhas e $n-r$ 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, 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 Δ_o é menor de 1.ª ordem, são nulos. Como os determinantes de ordem $r+1$, a considerar em B, são da forma

$$\begin{vmatrix}a_{11} & \dots & a_{1r} & a_{1j}\\ \dots & \dots & \dots & \dots\\ a_{r1} & \dots & a_{rr} & a_{rj}\\ o & \dots & o & b_{hj}\end{vmatrix}=\Delta\,.\,b_{hj}=o,$$

vê-se que $b_{hj} = o$. Assim, B tem o aspecto

$$B = \begin{pmatrix} \Delta_o & P \\ O & O \end{pmatrix},$$

donde se conclui que a característica de B é igual a r. O teorema está provado.

Postas estas considerações, façamos a anunciada aplicação da teoria das determinantes à determinação das soluções dos sistemas lineares.

1.º Caso (sistema Cramer): — Seja o sistema

$$\sum_{k=1}^{n} a_{ik}\, x_k = b_i\,, \qquad (i = 1, 2, \ldots, n), \tag{33}$$

de tantas equações quantas as incógnitas. Diz-se sistema Cramer, se o determinante $|a_{ik}|$ for diferente de zero. Nesse caso, a matriz simples do sistema tem a característica n, e o mesmo sucede, necessàriamente, à matriz ampliada. O sistema (33) é solúvel. Se $x_1, \ldots, x_n$ é uma solução, escrevamos

$$x_j \,.\, |a_{ik}| = \begin{vmatrix} a_{11} \ldots a_{1j}\ x_j \ldots a_{1n} \\ a_{21} \ldots a_{2j}\ x_j \ldots a_{2n} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n1} \ldots a_{nj} x_j \ldots a_{nn} \end{vmatrix} =$$

$$= \begin{vmatrix} a_{11} \ldots a_{1,j-1} \sum_{s=1}^{n} a_{1s}\, x_s \ldots a_{1n} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1} \ldots a_{n,j-1} \sum_{s=1}^{n} a_{ns}\, x_s \ldots a_{nn} \end{vmatrix} =$$

$$= \begin{vmatrix} a_{11} \ldots a_{1,j-1}\, b_1 \ldots a_{1n} \\ a_{21} \ldots a_{2,j-1}\, b_2 \ldots a_{2n} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n1} \ldots a_{n,j-1}\, b_n \ldots a_{nn} \end{vmatrix}.$$

Tem-se, então,

$$x_j = \frac{\sum_{s=1}^{n} b_s\, A_{js}}{|a_{ik}|}\,. \tag{34}$$

Deste modo, as soluções de (33) não podem deixar de ter a forma (34). E, como as soluções existem, elas serão dadas por (34). É válido este

Teorema 36: — *O valor da incógnita* x_j, *num sistema* Cramer (33), *é dado por um cociente, cujo denominador é o determinante* $|a_{ih}|$ *do sistema e cujo numerador é o determinante que resulta de* $|a_{ih}|$ *substituindo os elementos* a_{ij}, *da coluna de ordem* j, *pelos termos constantes* b_i.

2.º Caso (caso geral): — Suponhamos agora o sistema

$$\sum_{h=1}^{n} a_{ih}\, x_h = b_i\,, \qquad (i = 1, 2, \ldots, m), \tag{35}$$

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 (35), de modo a ter, como primeiras r, certas equações cujos coeficientes constituam r linhas independentes. Considerando, então, o sistema assim obtido como sendo formado já pelas primeiras r equações de (35), somos levados a

$$\sum_{h=1}^{n} a_{ih}\, x_h = b_i\,, \qquad (i = 1, 2, \ldots, r), \tag{36}$$

que é um sistema equivalente a (35). Se, em seguida, colocarmos, em (36), em primeiro lugar, r incógnitas que tenham como coeficientes um quadro determinante diferente de zero, chega-se a outro sistema, no qual, designadas as incógnitas por novos símbolos, os r primeiros símbolos correspondem às primeiras r incógnitas. Em resumo: suporemos já, em (36),

que as r primeiras colunas da matriz do sistema são linearmente independentes.

Dando a (36) o aspecto

$$\begin{aligned} &a_{11}\,x_1+\ldots+a_{1r}\,x_r=b_1-a_{1,r+1}\,x_{r+1}-\ldots-a_{1n}\,x_n,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ &a_{r1}\,x_1+\ldots+a_{rr}\,x_r=b_r-a_{r,r+1}\,x_{r+1}-\ldots-a_{rn}\,x_n, \end{aligned} \tag{37}$$

podemos considerar este sistema nas condições do 1.º caso. Obtém-se

$$x_j=\frac{\begin{vmatrix} a_{11}\ldots a_{1,j-1}\;b_1-\sum\limits_{s=r+1}^{n}a_{1s}x_s\ldots a_{1r}\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ a_{r1}\ldots a_{r,j-1}\;b_r-\sum\limits_{s=r+1}^{n}a_{rs}x_s\ldots a_{rr}\end{vmatrix}}{|a_{ih}|}.$$

Fazendo $|a_{ih}|=D$, é ainda

$$x_j=\frac{1}{D}\sum_{t=1}^{r}b_t\,A_{jt}-\frac{1}{D}\sum_{s=r+1}^{n}\Big(\sum_{t=1}^{r}a_{ts}\,A_{jt}\Big)\,x_s\,. \tag{38}$$

Dando aqui valores arbitrários aos x_s, obtêm-se todas as soluções de (37), e, portanto, do sistema dado (35). As equações de (35), que se escreveram em (36), dizem-se *equações principais* de (35); e as incógnitas que figuram nos primeiros membros de (37) dizem-se, anàlogamente, *incógnitas principais* de (35). Tem-se:

TEOREMA 37: — *Se o sistema* (35) *é solúvel, as suas soluções são dadas por* (38), *supostas as* r *primeiras equações de* (35) *as equações principais e supostas as* r *primeiras incógnitas de* (35) *as incógnitas principais.*

3.º CASO (sistema de $n-1$ equações homogéneas com n incógnitas): — Vai interessar-nos aqui, por aparecer com frequência nas aplicações, a hipótese de a característica da matriz

do sistema ser igual a $n-1$. As soluções constituirão uma multiplicidade vectorial a uma dimensão, que vamos determinar. O sistema tem o aspecto

$$\begin{aligned} &a_{11}\,x_1\quad+\ldots+a_{1n}\,x_n\quad=o,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ &a_{n-1,1}\,x_1+\ldots+a_{n-1,n}\,x_n=o, \end{aligned} \tag{39}$$

e a matriz do sistema é

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n}\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ a_{n-1,1} & a_{n-1,2} & \ldots & a_{n-1,n}\end{pmatrix}, \tag{40}$$

podendo dela tirar-se um determinante de ordem $n-1$ que é $\neq o$. Designaremos por $D_1, D_2, \ldots, D_n$ os n determinantes de ordem $n-1$, extraídos de (40), por supressão da 1.ª, 2.ª, etc., colunas. Pode indicar-se a seguinte regra para se encontrarem as soluções de (39). Consideram-se os determinantes

$$\begin{vmatrix} a_{j1} & a_{j2} & \ldots & a_{jn}\\ a_{11} & a_{12} & \ldots & a_{1n}\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ a_{n-1,1} & a_{n-1,1} & \ldots & a_{n-1,n}\end{vmatrix}, \tag{41}$$

$(j=1, 2, \ldots, n-1)$, que são todos nulos. Por desenvolvimento, segundo os elementos da primeira linha, obtêm-se as $n-1$ equações

$$\sum_{i=1}^{n}(-1)^{i+1}a_{ji}\,D_i=o, \qquad /1$$

que, por comparação com (39), mostram ser $x_1=D_1$, $x_2=-D_2, \ldots, x_n=(-1)^{n+1}D_n$ uma das suas soluções. Daqui o

TEOREMA 38: — *Dado o sistema* (39), *de característica* $n-1$, *as soluções são proporcionais aos determinantes de ordem* $n-1$ *extraídos de* (40), *afectados de sinais alternadamente* $+$ *e* $-$, *e começando pelo determinante obtido por supressão da 1.ª coluna.*

§ 4 — Transformações lineares

1) **Definição geral**—Sejam $\mathfrak{M}_n(e_1,\ldots,e_n)$ e $\mathfrak{M}_m(v_1,\ldots,v_m)$ duas multiplicidades vectoriais, de ordens n e m, respectivamente, sobre o mesmo corpo $\mathfrak{K}$. Um homomorfismo operatório $\mathfrak{M}_n \sim \mathfrak{M}_m$ (ou uma homomorfia) fica definida conhecidos os elementos U_j (1) e $\mathfrak{M}_m$, correspondentes dos e_j. Poremos

$$U_j = \sum_{k=1}^{m} v_k\, a_{kj}\,, \qquad (j=1,2,\ldots,n).$$

Dado o elemento $\Sigma e_j\, a_j$ e $\mathfrak{M}_n$, o seu correspondente em $\mathfrak{M}_m$ é

$$\sum_{j=1}^{n} U_j a_j = \sum_{j,k} v_k\, a_{kj}\, a_j = \sum_{k=1}^{m} v_k\, b_k\,, \qquad (b_k = \sum_{j=1}^{n} a_{kj}\, a_j)\,.$$

Vê-se que o homomorfismo também pode considerar-se definido pela matriz rectangular $A=(a_{kj})$, de m linhas e n colunas. Se considerarmos um segundo homomorfismo (ou homomorfia) $\mathfrak{M}_m \sim \mathfrak{M}_q(w_1,\ldots,w_q)$, definido pelas igualdades

$$v_k \to V_k = \sum_{s=1}^{q} w_s\, b_{sk}\,, \qquad (k=1,2,\ldots,m),$$

levanta-se a questão de procurar definir por uma matriz o homomorfismo $\mathfrak{M}_n \sim \mathfrak{M}_q$. Obtém-se, sucessivamente,

$$e_j \to U_j \to \sum_{k=1}^{m} V_k\, a_{kj} = \sum_{k=1}^{m}\sum_{s=1}^{q} w_s\, b_{sk}\, a_{kj} = \sum_{s=1}^{q} w_s\, c_{sj}\,.$$

com

$$c_{sj} = \sum_{k=1}^{m} b_{sk}\, a_{kj}\,.$$

---

(1) Excepcionalmente, utilizaremos aqui também letras latinas maiúsculas para designarmos vectores.

A matriz C, de elementos c_{sj}, é a matriz procurada. Escreveremos

$$A=(a_{kj}),\quad (k=1,2,\ldots,m;\ j=1,2,\ldots,n),$$
$$B=(b_{sk}),\quad (k=1,2,\ldots,m;\ s=1,2,\ldots,q),$$
$$C=(c_{sj}),\quad (s=1,2,\ldots,q;\ j=1,2,\ldots,n).$$

A matriz C, que tem tantas linhas quantas as linhas de B e tantas colunas quantas as colunas de A, diz-se *produto* de B por A, escrevendo-se $C=B.A=BA$.

Em correlação com o emprego de matrizes, vamos tratar agora algumas questões importantes.

Suponhamos $\mathfrak{M}_m$ $(m \lessgtr n)$ um subespaço de $\mathfrak{M}_n$. O homomorfismo passa a ser um endomorfismo operatório Θ, de $\mathfrak{M}_n$, segundo o qual se tem a correspondência

$$e_j \to e_j\Theta = U_j = \sum_{h=1}^{n} e_h\, a_{hj}, \quad (j=1,2,\ldots,n). \qquad (42)$$

A matriz $A=(a_{hj})$ é agora quadrada. Levanta-se o problema de se saber em que condições o endomorfismo é um automorfismo. Quer-se, então, que todos os elementos de $\mathfrak{M}_n$ sejam utilizados como imagens e que haja reciprocidade entre os vectores $\mathfrak{x} \in \mathfrak{M}_n$ 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 39: — *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 uma relação

$$\sum_{j=1}^{n} U_j\, b_j = 0, \qquad (b_j \in \mathfrak{K}), \qquad (43)$$

implica $b_j = o$. Ora a relação pode escrever-se

$$\sum_{j=1}^{n} \left(\sum_{h=1}^{n} e_h \, a_{hj} \right) b_j = \sum_{h=1}^{n} e_h \left(\sum_{j=1}^{n} a_{hj} \, b_j \right) = 0.$$

Como, por hipótese, os e_k são linearmente independentes, tem-se

$$\sum_{j=1}^{n} a_{kj} \, b_j = o. \tag{44}$$

Portanto, escrever (43) é o mesmo que escrever (44). Assim, o endomorfismo será um automorfismo, se o sistema (44) apenas tiver a solução nula, o que equivale a dizer que o determinante $|a_{kj}|$ é $\neq o$. Daqui este

TEOREMA 40: — *É condição necessária e suficiente, para que o endomorfismo* (42) *seja um automorfismo, que o determinante* $|a_{kj}|$, *da matriz quadrada do endomorfismo seja* $\neq 0$. Nesse caso, os U_j constituem uma base para $\mathfrak{M}_n$ e neles se exprimem todos os vectores. Em particular, tem-se

$$e_j = \sum_{k=1}^{n} U_k \, b_{kj}, \qquad (j = 1, 2, \ldots, n). \tag{45}$$

Os 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 $|b_{kj}| \neq o$.

Substituamos, em (45), os U_k pelas suas expressões nos e_j. Vem

$$e_j = \sum_{k=1}^{n} \sum_{m=1}^{n} e_m \, a_{mk} \, b_{kj} = \sum_{m=1}^{n} e_m \left(\sum_{k=1}^{n} a_{mk} \, b_{kj} \right),$$

o que nos leva a

$$\sum_{h=1}^{n} a_{mh} \, b_{hj} = \delta_{mj}, \qquad \delta_{mj} = \begin{cases} o, \text{ se } m \neq j, \\ u, \text{ se } m = j. \end{cases}$$

A matriz $(\delta_{mj}) = U_n$ tem o aspecto

$$U_n = \begin{pmatrix} u & o & \ldots & o \\ o & u & \ldots & o \\ \ldots & \ldots & \ldots & \ldots \\ o & o & \ldots & u \end{pmatrix}, \qquad (u \in \mathfrak{R}),$$

e recebe o nome de *matriz unidade*. Qualquer matriz quadrada de ordem n, multiplicada à direita ou à esquerda por U_n, não fica alterada: $C\,U_n = U_n\,C = C$.

As matrizes A e B, em questão, satisfazem à igualdade $A\,B = U_n$. É evidente que os papéis de A e de B são recíprocos, e que podíamos substituir em (42) os e_h pelas suas expressões (45), o que nos levaria a $B\,A = U_n$.

Duas matrizes A e B tais que $A\,B = B\,A = U_n$ dizem-se *inversas* uma da outra. Pode escrever-se $B = A^{-1}$. E é válido este

TEOREMA 41: — *É condição necessária e suficiente, para que um endomorfismo seja um automorfismo, que a matriz do endomorfismo tenha inverso.*

COROLÁRIO 7: — *São equivalentes estas duas afirmações:* 1) *o determinante da matriz* A, *representado por* $|\mathrm{A}|$, *é* $\neq o$; 2) *a matriz* A *tem inverso* A^{-1}.

Na verdade, basta afirmar que a matriz A tem inverso direito A_d^{-1}, pois que, sendo $A\,A_d^{-1} = U_n$, imediatamente se verifica que é

$$|A\,A_d^{-1}| = |U_n| = u = |A| \,.\, |A_d^{-1}|,$$

o que implica $|A| \neq o$.

Eis ainda uma outra caracterização dos automorfismos:

TEOREMA 42: — *É necessário e basta, para que* A *defina um automorfismo, que um produto* $\mathrm{A\,C} = \mathrm{O}$ = *matriz nula implique* $\mathrm{C} = \mathrm{O}$.

A condição é *necessária:* — Se A define um automorfismo, existe um inverso esquerdo B, de A. Então, $BA = U_n$, e, de $AC = O$, tira-se $B.AC = O$. Ora o produto de matrizes, como resulta da sua definição, é *associativo,* e, assim, tem-se $B.AC = BA.C = U_n C = C = O$, como se deseja.

A condição é *suficiente:* — Suponhamos que a matriz A é tal que $AC = O$ implica $C = O$. Queremos provar que A define um automorfismo. Da demonstração do teorema 40 resulta, com efeito, que, se a hipótese

$$A\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = O, \qquad \text{implica} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = O,$$

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, chamado *grupo linear*. Aos automorfismos dá-se o nome de *transformações lineares*. Por via dum automorfismo, passa-se duma base de $\mathfrak{M}_n$ para uma segunda base. A matriz A é, nesse sentido, a matriz que define a *mudança da base*.

2) **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

$$A.BC = AB.C, \qquad A(B+C) = AB + AC,$$
$$(B+C)A = BA + CA.$$

Entretanto, para que o produto de duas matrizes seja uma matriz do mesmo tipo 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 $\mathfrak{R}_n$, suposto $\mathfrak{R}$ o corpo a que pertencem os elementos das referidas matrizes.

Nesse anel, as unidades são as matrizes com inverso, as quais formam o grupo linear, como já se assinalou.

Seja $A \in \mathfrak{R}_n$. Podemos aplicar a A os elementos $a \in \mathfrak{R}$, conforme a regra

$$Aa = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} . a = \begin{pmatrix} a_{11} & a & \dots & a_{1n} & a \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a & \dots & a_{nn} & a \end{pmatrix}.$$

À face desta definição, conclui-se que $\mathfrak{R}_n$ *é um módulo finito relativamente a* $\mathfrak{R}$. Como matrizes-base tomam-se as matrizes e_{ij}, $(i, j = 1, 2, \dots, n)$, 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}: $A = \sum_{i,k=1}^{n} e_{ik} a_{ik}$. A independência linear dos e_{ij} é, de resto, imediata.

3) **Dois problemas sobre homomorfismos** — No homomorfismo $\mathfrak{M}_n \sim \mathfrak{M}_m$, definido pela matriz A, levanta-se este problema: *determinar a matriz* A' *que o define, supondo que se fazem mudanças de base, tanto em* $\mathfrak{M}_n$ *como em* $\mathfrak{M}_m$. A nova base de $\mathfrak{M}_n$ será $E_1, \dots, E_n$, a qual, em notação matrical, se pode escrever

$$(E_1, \dots, E_n) = (e_1, \dots, e_n).P, \tag{46}$$

onde P é a matriz invertível que define a mudança de base. Anàlogamente, em $\mathfrak{M}_m$, tem-se

$$(V_1, \dots, V_m) = (v_1, \dots, v_m).Q,$$

onde Q é invertível e de ordem n. Quanto à matriz A, foi ela introduzida de modo seguinte:

$$\mathfrak{e}_j \to U_j = \sum_{k=1}^{m} \mathfrak{v}_k \, a_{kj}.$$

Para encontrarmos a matriz A', que define o mesmo homomorfismo, temos de exprimir os transformados dos E_j nos V_k. Representemos esses transformados por E'_j. Será, em notação de matrizes:

$$(E'_1, \ldots, E'_n) = (U_1, \ldots, U_n).P;$$

mas, como

$$(U_1, \ldots, U_n) = (\mathfrak{v}_1, \ldots, \mathfrak{v}_m)\, A,$$

é também

$$(E'_1, \ldots, E'_n) = (\mathfrak{v}_1, \ldots, \mathfrak{v}_m)\, AP.$$

Se agora observarmos que se tem

$$(V_1, \ldots, V_m)\, Q^{-1} = (\mathfrak{v}_1, \ldots, \mathfrak{v}_m),$$

vê-se que

$$(E'_1, \ldots, E'_n) = (V_1, \ldots, V_m)\, Q^{-1} AP.$$

Daqui se conclui que a matriz A é substituída por $A' = Q^{-1} AP$. O problema está resolvido.

O segundo problema é o seguinte: *suponhamos que temos uma base* $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$, *em* $\mathfrak{M}_n$, *e que se considera um automorfismo definido por uma matriz* A; *pergunta-se: qual é a matriz* A′ *que define o mesmo automorfismo, se se muda de base?*

Escrevamos a nova base sob a forma $(E_1, \ldots, E_n) = (\mathfrak{e}_1, \ldots, \mathfrak{e}_n)\, P$. O automorfismo faz corresponder aos $\mathfrak{e}_j$ os vectores

$$U_j = \sum_{h=1}^{n} \mathfrak{e}_h \, a_{hj}.$$

Para se encontrar A', vê-se que devemos procurar os transformados dos E_i e exprimir esses transformados nos próprios E_i. Ora, se o transformado de E_i é E'_i, tem-se

$$(E'_1, \ldots, E'_n) = (U_1, \ldots, U_n)\, P = (\mathfrak{e}_1, \ldots, \mathfrak{e}_n)\, AP = (E_1, \ldots, E_n)\, P^{-1} AP,$$

o que mostra ser $A' = P^{-1} AP$.

4) **Transformação de coordenadas** — Nos dois problemas do número anterior, foi posta em evidência uma questão de muito interesse, que consistiu em procurar as modificações introduzidas na expressão dum certo facto, quando se passa duma base a outra base. Em Geometria é fundamental saber efectuar *transformações de coordenadas,* em virtude de haver muitas vezes possibilidade de simplificar a representação de determinadas propriedades geométricas, quando se muda de referencial. Duma maneira precisa, vamos começar por ver como se transformam as componentes dum vector dado $\mathfrak{x} \in \mathfrak{M}_n$, ao passar-se duma base $\mathfrak{e}_1, \ldots, \mathfrak{e}_n$ a uma segunda base $E_1, \ldots, E_n$, por meio da relação (46). Depois, partindo dum referencial $O_o\,(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$, de $\mathfrak{R}_n$, trataremos questão análoga para as coordenadas dum ponto Q, que passará a ser referida a $O\,(E_1, \ldots, E_n)$.

Quanto aos vectores, se for

$$\mathfrak{x} = \sum_{i=1}^{n} \mathfrak{e}_i \xi_i, \qquad E_j = \sum_{h=i}^{n} \mathfrak{e}_h \, p_{hj},$$

vê-se que, pondo

$$\mathfrak{x} = \sum_{j=1}^{n} E_j \eta_j,$$

se tem sucessivamente:

$$\mathfrak{x} = \sum_{j=1}^{n} E_j \, \eta_j = \sum_{j,h} \mathfrak{e}_h \, p_{hj} \, \eta_j = \sum_{h} \mathfrak{e}_h \, (\sum_{j} p_{hj} \, \eta_j),$$

pelo que

$$\xi_h = \sum_{j=1}^{n} p_{hj}\,\eta_j . \tag{47}$$

Inversamente, se supusermos $P^{-1} = \Pi = (\pi_{ij})$ a matriz inversa de P, tem-se, por um processo análogo,

$$\eta_h = \sum_{j=1}^{n} \pi_{hj}\,\xi_j . \tag{48}$$

Também se chega a estas relações resolvendo em ordem aos η_h as equações (47). Sabemos, com efeito, que essa resolução é possível e que o resultado é único, pelo facto de ser $|P| \neq o$. As fórmulas (47) e (48) respondem à questão posta para os vectores. Podemos acrescentar que, dadas igualdades como (47), com $|p_{hj}| \neq o$, essas igualdades são sempre susceptíveis da interpretação geométrica que levou a escrevê-las.

Se imaginarmos o espaço $\mathfrak{R}_n$ e o referencial $O_o(e_1, \ldots, e_n)$, admitindo que é $\overrightarrow{O_o Q} = x = \Sigma e_i \xi_i$, $(i = 1, \ldots, n)$, as fórmulas (47) resolvem o que pode chamar-se o problema da *mudança da direcção dos eixos, com conservação da origem.* Por meio delas, ou das suas equivalentes (48), passa-se das coordenadas dum ponto Q, num referencial $O_o(e_1, \ldots, e_n)$, para as coordenadas do mesmo ponto noutro referencial com a mesma origem O_o, mas com eixos $(E_1, \ldots, E_n)$ diferentes.

Se há simples *mudança de origem,* passando-se de O_o a O'_o, mas conservando os eixos e_i, então, da relação

$$\overrightarrow{O_o Q} = \overrightarrow{O_o O'_o} + \overrightarrow{O'_o Q},$$

supondo que as coordenadas de O'_o em $O_o(e_1, \ldots, e_n)$, são $(\alpha_1, \ldots, \alpha_n)$, tira-se $\Sigma e_i \xi_i = \Sigma e_i \alpha_i + \Sigma e_i \xi'_i$, $(i = 1, 2, \ldots, n)$, ou seja

$$\xi'_i = \xi_i - \alpha_i , \qquad (i = 1, 2, \ldots, n). \tag{49}$$

Finalmente, pode haver mudança de origem e da direcção dos eixos. Os dois referenciais são $O_o(e_1, \ldots, e_n)$ e $O'_o(E_1, \ldots, E_n)$. A fixação do segundo referencial no primeiro faz-se à custa das igualdades

$$\overrightarrow{O_o O'_o} = \sum_{i=1}^{n} e_i \alpha_i , \qquad E_j = \sum_{i=1}^{n} e_i p_{ij} .$$

Então, dado o ponto Q, tem-se

$$\overrightarrow{O_o Q} = x = \sum_{i=1}^{n} e_i \xi_i , \qquad \overrightarrow{O_o O'_o} + \overrightarrow{O'_o Q} = \overrightarrow{O_o Q},$$

$$\overrightarrow{O'_o Q} = x' = \sum_{i=1}^{n} E_i \eta_i ,$$

e portanto,

$$\sum_{l=1}^{n} e_i \alpha_i + \sum_{i=1}^{n} E_i \eta_i = \sum_{i=1}^{n} e_i \xi_i ,$$

$$\sum_{i=1}^{n} e_i \alpha_i + \sum_{i,k=1}^{n} e_k p_{ki} \eta_i = \sum_{i=1}^{n} e_i \xi_i ,$$

ou seja

$$\xi_k = \alpha_k + \sum_{i=1}^{n} p_{ki} \eta_i . \tag{50}$$

Inversamente, se supusermos $P^{-1} = \Pi = (\pi_{ij})$ a matriz inversa de P, tem-se, por um processo análogo,

$$\eta_k = \beta_k + \sum_{i=1}^{n} \pi_{ki} \xi_i , \tag{51}$$

para o que bastaria ter em conta as relações

$$\overrightarrow{O'_o O_o} = \sum_{i=1}^{n} E_i \beta_i , \qquad e_j = \sum_{i=1}^{n} E_i \pi_{ij},$$

$$\overrightarrow{O'_o Q} = \sum_{i=1}^{n} E_i \eta_i , \qquad \overrightarrow{O'_o O_o} + \overrightarrow{O_o Q} = \overrightarrow{O'_o Q},$$

$$\overrightarrow{O_o Q} = \sum_{i=1}^{n} e_i \xi_i .$$

Também se chega às relações (51) resolvendo em ordem aos η_k as equações (50). Essa resolução é possível e o resultado é único. As fórmulas (50) e (51) respondem à questão posta para os pontos. Podemos acrescentar que, dadas igualdades como (50), com $|p_{kj}| \neq o$, essas igualdades são sempre susceptíveis da interpretação geométrica que levou a escrevê-las.

até aqui

BIBLIOGRAFIA

Este Capítulo foi redigido tendo principalmente em conta as obras seguintes:

H. WEYL — *Temps espace et matière*, Blanchard, Paris, 1922;

B. L. VAN DER WAERDEN — *Moderne Algebra*, tomo 2.º. Berlim, 1931;

A. ALMEIDA COSTA — *Grupos abelianos e Anéis e Ideais não comutativos*, Porto, Centro de Estudos Matemáticos, 1942;

B. DE JESUS CARAÇA — *Lições de Álgebra e Análise*, vol. 1, 2.ª edição, Lisboa, 1945;

ARNALDO MADUREIRA — *Álgebra superior e Geometria analítica*, tomo 1, Porto, 1948;

E. SPERNER — *Einführung in die analytische Geometrie und Algebra*, 1 Teil, Göttingen, 1948;

J. VICENTE GONÇALVES — *Álgebra superior*, 2.º vol., Lisboa, 1950.

Compete-nos esclarecer, entretanto, que foi o livro de E. SPERNER o que mais largamente se utilizou.

CAPÍTULO IV

ANÉIS DE IDEAIS PRINCIPAIS

§ 1 — O 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 $\mathfrak{S}$, com elemento um, diz-se que existe *algoritmo de divisão* em $\mathfrak{S}$, quando se realizarem as seguintes condições: 1.ª) — Dado um elemento a de $\mathfrak{S}$, é possível atribuir-lhe um valor absoluto inteiro $|a|$, não negativo; 2.ª) — dados dois elementos quaisquer $a \neq o$ e b, existem uma *divisão à direita* e uma *divisão à esquerda,* conforme as regras

$$\begin{cases} b = q\,a + r, \\ |r| < |a|, \end{cases} \qquad \begin{cases} b = a\,q' + r', \\ |r'| < |a|. \end{cases} \tag{1}$$

Quando o anel é comutativo, há coincidência das duas divisões. No Cap. II, § 3, n.º 5, estudamos o algoritmo de divisão em $\mathfrak{R}[x]$, nos moldes da definição actual. É um caso preciso para o qual foi estabelecida a univocidade do algoritmo.

TEOREMA 1: — *Um elemento não nulo dum anel* $\mathfrak{S}$ *com algoritmo de divisão não pode ter o valor absoluto igual a zero.* Se

$a \neq o$ e $|a| = 0$, a divisão $b = q\,a + r$, com $|r| < |a|$ será impossível. O único elemento cujo valor absoluto pode ser nulo é o elemento nulo.

TEOREMA 2: — *Num anel* $\mathfrak{S}$ *com algoritmo de divisão, um ideal direito* $\mathfrak{r}$ *é sempre um ideal principal direito.* Se $\mathfrak{r} = (o)$, o teorema é banal. Supondo $\mathfrak{r} \neq (o)$, designemos por $a \neq o$ um elemento de $\mathfrak{r}$ de valor absoluto mínimo. Se $b \in \mathfrak{r}$ é qualquer, o algoritmo de divisão permite escrever $b = a\,q' + r'$, com $|r'| < |a|$. Mas, sendo $r' = b - a\,q' \in \mathfrak{r}$, ter-se-á necessàriamente $r' = o$, $b = a\,q'$, $\mathfrak{r} = (a)_d$.

Existe um teorema análogo para os ideais esquerdos. Portanto:

TEOREMA 3: — *Se* $\mathfrak{S}$ *é um anel não comutativo com algoritmo de divisão, é um anel de ideais principais se tiver elemento um.*

3) **A teoria do máximo divisor comum** — Seja $\mathfrak{S}$ um anel de ideais principais não comutativo. Supondo $(a)_d$ e $(b)_d$ dois ideais direitos de $\mathfrak{S}$, o ideal direito soma é, por hipótese, gerado por um elemento d: $((a)_d, (b)_d) = (d)_d$. Tem-se

$$a = d\,q, \qquad b = d\,q', \qquad d = a\,r + b\,s, \tag{2}$$

onde $q, q', r, s \in \mathfrak{S}$. Comparando estas igualdades com as igualdades (9) do n.º 5, § 3, Cap. II, é natural designar d por *máximo divisor comum* (m. d. c.) *esquerdo* de a e b. O elemento d goza, com efeito, das 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.

Levanta-se desde já 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 $f\alpha = d$, $d\beta = f$, $(\alpha, \beta \in \mathfrak{S})$, e, consequentemente, $d\beta\alpha = f\alpha = d$, $f\alpha\beta = d\beta = f$, ou seja $d\,(\beta\alpha - u) = o$,

$f\,(\alpha\beta - u) = o$, supondo u o elemento um de $\mathfrak{S}$. Admitindo que $\mathfrak{S}$ não tem divisores de zero, concluir-se-á $\beta\alpha = \alpha\beta = u$. Daqui o

TEOREMA 4: — *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.*

Generalizando uma noção dada no referido n.º 5, § 3, Cap. II, diremos que dois elementos d e f, como os do teorema, são *associados esquerdos*. No § 1, n.º 3, do mesmo Cap. II, introduzimos 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 (2). Inversamente, se um elemento $g \in \mathfrak{S}$ goza das propriedades atribuídas ao m. d. c. esquerdo, tem-se $(g)_d \supseteq ((a)_d, (b)_d)$, em virtude da primeira; e, pela segunda, o próprio elemento d divida g à esquerda, o que levará a $g = d\,t$, $g \in (d)_d$ e $(g)_d \subseteq (d)_d$. Assim, é $(g)_d = (d)_d$ e g e d são associados. É válido o

TEOREMA 5: — *Se* $\mathfrak{S}$ *é um anel de ideais principais sem divisores de zero, o m. d. c. esquerdo de dois elementos* a, b ∈ $\mathfrak{S}$ *é bem determinado, sob a condição de não se distinguirem elementos associados esquerdos.*

A definição de *m. d. c. direito* de dois elementos é dada de modo análogo.

Quando o m. d. c. esquerdo de a e b for uma unidade, os elementos a e b dizem-se *primos entre si esquerdos*. Não há divisores comuns de a e b que não sejam unidades. Também se definem elementos *primos entre si direitos*. O ideal gerado pelo

m. d. c. de dois elementos primos é sempre o anel $\mathfrak{S}$ (ideal unidade).

4) O algoritmo de Euclides — Constitui um problema importante o da determinação de condições que caracterizem um anel $\mathfrak{S}$ 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 $\mathfrak{S}$, 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,* que encontrámos na teoria do m. d. c. em $\mathfrak{R}[x]$ e que se estende ao caso de que nos estamos ocupando. Escrevamos as igualdades

$$\begin{aligned} &a = b\,q_1 + r_1,\\ &b = r_1\,q_2 + r_2,\\ &\cdots\cdots\cdots\cdots \qquad (b \neq o),\\ &r_{s-3} = r_{s-2}\,q_{s-1} + r_{s-1},\\ &r_{s-2} = r_{s-1}\,q_s + o, \end{aligned}$$

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 (2). De facto, vê-se que r_{s-1} divide à esquerda, sucessivamente, $r_{s-2}, r_{s-3}, \ldots, b, a$; e que, inversamente, todo o elemento, dividindo à esquerda a e b, divide sucessivamente $r_1, r_2, \ldots, r_{s-1}$.

Pròpriamente, quanto à existência de algoritmo de divisão, orientados, de novo, pelo que se passa em $\mathfrak{R}[x]$, vamos responder pela afirmativa, se no anel não comutativo $\mathfrak{S}$, sem divisores de zero e com elemento um, pudermos introduzir uma noção de valor absoluto, nas condições seguintes: 1) $|a| = 0$, quando $a = o$, e apenas nesse caso; 2) $|a| > 0$, quando $a \neq o$, com $|a|$ inteiro; 3) $|a - a'| \gtrless$ maior dos valores absolutos

$(|a|, |a'|)$; 4) dos elementos $a + a', a - a'$, com a e a' não nulos, um deles tem valor absoluto $< |a|$; 5) $|a\,b| = |a| . |b|$.

Antes de fazermos a demonstração da existência, provaremos a univocidade do algoritmo. Suponhamos que são válidas as igualdades (1). Então, se pudesse ser ainda, por ex., $b = q_1 a + r_1$, ter-se-ia $(q - q_1)\,a = r_1 - r$. Com $r_1 \neq r$, viria $|r_1 - r| \geqslant |a|$; mas como, por outro lado, $|r_1 - r| \lessgtr$ maior dos valores absolutos $(|r_1|, |r|)$, seríamos levados a $|r_1 - r| < |a|$, em contradição com a conclusão anterior. Deverá ser, pois, $r_1 = r$, e, consequentemente $q_1 = q$.

Posto isto, dados $a \neq o$ e b, admitamos que é $b = o$. As igualdades $o = a . o + o$, $o = o . a + o$ são do tipo (1). Sendo $a, b \neq o$, tomemos, de entre os elementos da forma $b - t\,a$, em que $t \in \mathfrak{S}$, o elemento $b - q\,a = r$, de valor absoluto mínimo. Vamos ver que é $|r| < |a|$. Para a hipótese de se ter $r = o$, a afirmação é imediata. Mas, supondo $r \neq o$, se pudesse ser $|r| \geqslant |a|$, ter-se-ia

$$r \pm a = b - q\,a \pm a = b - (q \mp u)\,a,$$

em que um dos elementos $r \pm a$ seria de valor absoluto $< |r|$, o que é absurdo, pelo facto de tal elemento poder tomar a forma $b - t\,a$.

Fixemos o

TEOREMA 6: — *Num anel $\mathfrak{S}$ não comutativo, com elemento um e sem divisores de zero, mediante as condições 1) a 5), existe algoritmo unívoco de divisão.*

Finalmente, o estudo do m. d. c. em $\mathfrak{R}(x)$ sugere este outro

TEOREMA 7: — *O m. d. c. esquerdo* d, *de dois elementos* a *e* b, *dum anel $\mathfrak{S}$ nas condições do teorema anterior, é o elemento de valor absoluto mínimo de entre os elementos não nulos da forma* $\mathrm{a\,t} + \mathrm{b\,t'}$, $(\mathrm{t}, \mathrm{t'} \in \mathfrak{S})$. Na verdade, se r e s realizam o mínimo considerado, ponhamos $d = a\,r + b\,s$. Vamos ver que d é divisor esquerdo

de a e b. Se d não dividisse a, como é $d \neq o$, o elemento r_1 da igualdade $a = d\,q_1 + r_1$, com $|r_1| < |d|$, seria $\neq o$. Mas, tendo-se

$$r_1 = a - d\,q_1 = a - (a\,r + b\,s)\,q_1 = a\,(u - r\,q_1) + b\,(-s\,q_1),$$

encontraríamos em r_1 um elemento da forma $a\,t + b\,t'$, com $|r_1| < |d|$, o que seria absurdo. Do mesmo modo se demonstraria que d divide b.

5) **A teoria do menor múltiplo comum** — Sejam $(a)_d$ e $(b)_d$ dois ideais direitos do anel de ideais principais $\mathfrak{S}$. Pondo $(a)_d \cap (b)_d = (f)_d$, vê-se que é $f = a\,q, f = b\,q'$. O elemento f é *múltiplo esquerdo* de a e de b. Qualquer outro múltiplo esquerdo comum daqueles elementos, como g, por ex., levando a $g = a\,q_1$, $g = b\,q_2$, mostra ser $(g)_d \subseteq (f)_d$. Então é $g = f\,q_1$, 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 de b; 2.ª) qualquer múltiplo esquerdo de a e de b é múltiplo esquerdo de f. Em face disto, diz-se que f é o *menor múltiplo comum (m. m. c.) esquerdo* de a e b.

Levanta-se a questão de se 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 4 afirma-nos que se tem $h = f\varepsilon$, em que ε é unidade de $\mathfrak{S}$. 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 $h \in \mathfrak{S}$ goza das duas propriedades atribuídas 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 $f = h\,t$, $(f)_d \subseteq (h)_d$, e, consequentemente, a $(f)_d = (h)_d$. Logo:

TEOREMA 8: — *Se $\mathfrak{S}$ é um anel de ideais principais sem divisores de zero, o m. m. c. esquerdo (ou direito) de dois elementos* $a, b \in \mathfrak{S}$ *é bem determinado, sob a condição de não se distinguirem elementos associados esquerdos.*

§ 2 — O caso comutativo

1) **Considerações gerais** — Tomemos um domínio de integridade $\mathfrak{A}$ com elemento um. No n.º 5, § 3, Cap. II, ao estudarmos o domínio de integridade $\mathfrak{R}[x]$, introduzimos as noções de unidades, divisores, múltiplos, elementos associados, divisores autênticos e elementos primos, as quais podem transportar-se textualmente para $\mathfrak{A}$. A existência de elemento um é fundamental. Se, por ex., se tratar do domínio constituído pelos números pares, um elemento não é divisível 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 ex., 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 ímpar 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 $g/2^h \,.\, x = 1$, 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 $\mathfrak{N}$. Os elementos associados de $a \in \mathfrak{A}$ são da forma $\pm 2^n a = \pm 2^n g/2^h = \pm 2^{n'} g$, com $g > o$ e ímpar e n' qualquer. O elemento $8 = 2^3$, por ser uma unidade, pode ou não considerar-se primo. O elemento 6 não pode ser escrito sob a forma $6 = g/2^h \,.\, g'/2^{h'}$, pois que isso exigiria $g\,g' =$ número par, a não ser que se ponha $g = 3$, $g' = 1$, e

$$6 = 3\,.\,2 = \frac{3}{2^n} \cdot \frac{1}{2^{-(n+1)}} = \frac{3}{2^n} \cdot 2^{n+1}\,.$$

Isto significa que um dos factores de 6 é uma unidade, e que, portanto, 6 é um elemento primo. O elemento 9 não é primo: $9 = (3.2^n)\,.\,3/2^n$. Os elementos primos são todos aqueles que,

sob a forma reduzida, têm $g =$ número ímpar primo, e apenas esses.

Se $\mathfrak{K}$ é um corpo, todos os polinómios $ax+b \in \mathfrak{K}[x]$ são primos. Ainda em $\mathfrak{K}[x]$, estudemos as condições em que o elemento ax^2+bx+c, com $a \neq o$, é primo. Quando $c = o$, o elemento 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 elemento em causa, leva a $b^2-4ac = a^2(g-f)^2$. É, pois, necessário, 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 $ax^2+bx+c=a(x-f)(x-g)$.

Um domínio de integridade com elemento um diz-se um *domínio euclidiano,* quando forem satisfeitas as seguintes condições: 1.ª) — Existe a noção de valor absoluto $=|a|$, para cada $a \in \mathfrak{A}$, sendo $|a| \neq 0$, inteiro e positivo, se $a \neq o$; e $|a|=0$, se $a=o$; 2.ª) — Existe algoritmo de divisão no domínio de integridade, segundo o qual, dados $a \neq o$ e b qualquer, se podem determinar q e r, com $|r|<|a|$, satisfazendo a $b=aq+r$; 3.ª) — É $|ab|=|a| \cdot |b|$.

O domínio de integridade $\mathfrak{Z}$ dos inteiros é euclidiano. O mesmo se diz de $\mathfrak{K}[x]$, à face da noção de valor absoluto introduzida no n.º 5, § 3, Cap. II.

No n.º 3 suporemos $\mathfrak{A}$ um anel de ideais principais sem divisores de zero, como o são já $\mathfrak{Z}$ e $\mathfrak{K}[x]$. Lá indagaremos da possibilidade da decomposição dum elemento de $\mathfrak{A}$ em elementos primos, e, em seguida, do número de decomposições. No número próximo, porém, diremos algumas palavras sobre ideais, em correlação com uma teoria da divisibilidade a fazer depois, e, mesmo, em correlação com a divisibilidade a tratar no n.º 3.

2) **Ideais divisores e múltiplos de ideais. Ideais primos e ideais sem divisor.** O anel $\mathfrak{A}$, aqui em causa, será também 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 sinal $=$ não pode ter lugar, o divisor ou o múltiplo dizem-se *autênticos.*

Para se compreenderem bem estas definições, ~~suponhamos~~ consideremos o anel $\mathfrak{A}$ ~~com elemento um~~ e tomemos para ideais os dois ideais principais (a) e (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 b e a a divisão ordinária.

A relação $\mathfrak{b} \supseteq \mathfrak{a}$ (ou $\mathfrak{a} \subseteq \mathfrak{b}$) também pode escrever-se $\mathfrak{a} \equiv o(\mathfrak{b})$, no sentido das congruências: a diferença entre cada elemento de $\mathfrak{a}$ e o elemento nulo pertence a $\mathfrak{b}$.

Mesmo em relação a um elemento $a \in \mathfrak{a}$, podemos dizer que *o ideal é divisor do elemento:* $\mathfrak{a} \equiv o(a)$.

Um ideal $\mathfrak{p}$ diz-se *primo,* quando goza da propriedade seguinte: só pode dividir o produto de dois elementos $a, b \in \mathfrak{A}$, quando dividir, pelo menos, um dos elementos. A relação $ab \equiv o(\mathfrak{p})$ arrasta uma das relações $a \equiv o(\mathfrak{p})$, $b \equiv o(\mathfrak{p})$.

TEOREMA 9: — *Dados os ideais* $\mathfrak{a}$ *e* $\mathfrak{a}'$ *tais que* $\mathfrak{a}\mathfrak{a}' \subseteq \mathfrak{p}$, *com* $\mathfrak{a}$ não contido em $\mathfrak{p}$ (1), tem-se $\mathfrak{a}' \subseteq \mathfrak{p}$. Se pudesse ser $\mathfrak{a}'$ não contido em $\mathfrak{p}$, tomaríamos $a' \in \mathfrak{a}'$, com $a' \notin \mathfrak{p}$; depois, tomaríamos $a \in \mathfrak{a}$, com $a \notin \mathfrak{p}$. Ter-se-ia $aa' \in \mathfrak{p}$, sem que a ou a' pertencessem a $\mathfrak{p}$, contra a hipótese de $\mathfrak{p}$ ser primo.

Formemos agora o anel diferença $\mathfrak{A}/\mathfrak{p}$. Se se tiver $(a+\mathfrak{p})(b+\mathfrak{p}) = ab+\mathfrak{p}$, é $ab=\mathfrak{p}$, e, portanto, um dos ele-

(1) Dificuldades técnicas impedem o uso do sinal de «não contido». Duma maneira geral, se um determinado sinal tem um certo significado, o mesmo sinal com um traço obliquo «nega» esse significado.

mentos a ou b pertence a $\mathfrak{p}$, sendo $a+\mathfrak{p}=\bar{o}$ ou $b+\mathfrak{p}=\bar{o}$. Daqui este

TEOREMA 10: — *É condição necessária e suficiente, para que um ideal seja primo, que o respectivo anel diferença seja um domínio de integridade.* A demonstração da suficiência é imediata. Claramente, por outro lado, que se está supondo $\mathfrak{p}\neq\mathfrak{A}$, pelo que $\mathfrak{A}/\mathfrak{p}$ tem mais do que um elemento.

O ideal unidade $\mathfrak{A}$ satisfaz à definição de ideal primo e considera-se primo. Todavia, o teorema anterior não é, então, aplicável. O ideal nulo só é primo num domínio de integridade.

No anel $\mathfrak{A}$ dos números complexos $a+b\,i$, onde a e b são inteiros *(números inteiros de* GAUSS), o ideal $(1+i)$ é primo.

Um ideal $\mathfrak{a}$ diz-se *sem divisor,* se apenas tem como divisor autêntico o ideal unidade. É válido o

TEOREMA 11: — *É condição necessária e suficiente, para que, num anel $\mathfrak{A}$ com identidade, $\mathfrak{a}$ seja um ideal sem divisor, que o anel diferença $\mathfrak{A}/\mathfrak{a}$ seja um corpo.* Se $\mathfrak{a}$ é sem divisor, consideremos a equação $\bar{a}\,\bar{x}=\bar{b}$, onde $\bar{a}=a+\mathfrak{a}\neq\bar{o}$ e $\bar{b}=b+\mathfrak{a}$ é qualquer. O ideal gerado por $\mathfrak{a}$ e a é o próprio anel $\mathfrak{A}$. Assim, b pode tomar a forma $b=\alpha+a\,t$, com $\alpha\in\mathfrak{a}$, $t\in\mathfrak{A}$. Então, é $\bar{b}=\bar{\alpha}+\bar{a}\,\bar{t}=\bar{a}\,\bar{t}$, pelo que a equação é resolvida pondo $\bar{x}=\bar{t}$. Recìprocamente, se $\mathfrak{A}/\mathfrak{a}$ é um corpo, tomemos $\mathfrak{b}\supset\mathfrak{a}$. Vamos ver que o ideal $\mathfrak{b}$ é o ideal unidade. Seja $c\in\mathfrak{A}$ arbitrário e consideremos a equação $\bar{b}\,\bar{x}=\bar{c}$, com $\bar{b}\neq\bar{o}$ e $\bar{b}\in\mathfrak{b}$. Se $\bar{x}$ é a solução, os elementos b, c, x satisfazem à relação $c-b\,x\in\mathfrak{a}$, de sorte que $c\in\mathfrak{b}$, tendo-se $\mathfrak{A}\subseteq\mathfrak{b}$, ou seja $\mathfrak{b}=\mathfrak{A}$, como se deseja.

Todo o ideal sem divisor é primo. A inversa não é verdadeira, como vamos ver por um exemplo. Tomemos o anel $\mathfrak{I}[x]$ dos polinómios inteiros e demonstremos que os dois ideais (x) e $(2,x)$, são primos. Pode pôr-se

$$(2,x)=2\,\mathfrak{I}[x]+x\,\mathfrak{I}[x]=2f+x\,\mathfrak{I}[x],$$

onde f é inteiro. Relativamente ao anel diferença $\mathfrak{I}[x]/(2,x)$, tem-se a expressão seguinte para os seus elementos: $n+2k+x\,\mathfrak{I}[x]$, onde n e k são inteiros quaisquer. Só há dois elementos no anel diferença, a saber

$$2k+x\,\mathfrak{I}[x], \qquad (2n+1)+x\,\mathfrak{I}[x].$$

O primeiro é o elemento zero, o segundo o elemento um. O anel diferença é, assim, um domínio de integridade, e o ideal $(2,x)$ é primo.

No caso do ideal (x), os elementos de $\mathfrak{I}[x]/(x)$ são da forma $a_o+x\,\mathfrak{I}[x]$, onde a_o é um inteiro qualquer. As regras do produto reduzem-se às do produto dos números inteiros. O anel diferença é um domínio de integridade e (x) é primo. O ideal $(2,x)$ é um divisor autêntico do ideal (x).

Concluiremos este número com as definições de m. d. c. e m. m. c. de ideais. 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 designa-se por *m. d. c.* dos *dois 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.

De modo evidente, passa-se ao m. m. c. de $\mathfrak{a}$ e $\mathfrak{b}$. 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 $\mathfrak{a}\cap\mathfrak{b}$.

3) **A teoria da factorização** — Como já anunciamos, é essencial, neste número, supor $\mathfrak{A}$ um anel de ideais principais sem divisores de zero.

TEOREMA 12: — *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 $p=d\,k$. O elemento k não pode ser uma unidade, visto que isso acarretaria

$(p)=(d)$. Será d uma unidade, e, consequentemente, será $(d)=\mathfrak{A}$, o que demonstra o teorema.

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 $\bar{a}\,\bar{x}=\bar{b}$, se $\bar{a}\neq\bar{o}$, equivale à possibilidade da resolução da congruência $a\,x\equiv b\,(p)$ (1), suposto $a\notin(p)$. Ora, existindo elementos $r, r'\in\mathfrak{A}$ tais que $a\,r+p\,r'=u$, tem-se $a\,.\,r\,b+p\,.\,r'\,b=b$, obtendo-se para a congruência a solução $x=r\,b$.

Quando há algoritmo de divisão, o algoritmo de EUCLIDES leva fàcilmente à determinação de r. De facto, das igualdades

$$\begin{array}{ll} a=p\,q_1+r_1, & \ldots\ldots\ldots\ldots\ldots\ldots, \\ p=r_1\,q_2+r_2, & r_{s-3}=r_{s-2}\,q_{s-1}+r_{s-1}, \\ \ldots\ldots\ldots, & r_{s-2}=r_{s-1}\,q_s\,, \end{array}$$

com $r_{s-1}=u$, passa-se, sucessivamente, a partir da relação $r_{s-3}=r_{s-2}\,q_{s-1}+u$, à relação entre $(r_{s-4}, r_{s-3}, u), (r_{s-5}, r_{s-4}, u), \ldots, (p, r_1, u), (a, p, u)$, figurando sempre u sem qualquer coeficiente. A relação entre (a, p, u) será a relação desejada, pois se reveste da forma $a\,r+p\,s=u$.

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 13: — *Se for* $(a, b)=d$, é $(a\,c, b\,c)=d\,c$. De facto, supondo $a=d\,q, b=d\,q'$, $a\,r+b\,s=d$, tem-se $a\,c=d\,q\,c$, $b\,c=d\,q'\,c$, $a\,r\,c+b\,s\,c=d\,c$. O teorema está provado.

TEOREMA 14: — *Se um elemento* g *divide um produto* a b *e é primo com um dos factores, divide necessàriamente o outro fac-*

(1) Escreveu-se abreviadamente $a\equiv b\,(p)$, em vez de $a\equiv b\,((p))$.

tor. Por hipótese, é $a\,b=g\,q$, $(b, g)=u$. Então, será também $(a\,b, a\,g)=(g\,q, a\,g)=a$. O elemento g divide $g\,q$ e $g\,a$, pelo que dividirá o seu m. d. c., que é a.

COROLÁRIO 1: — *Se um elemento primo* p *divide um produto* a b, *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 de congruência $a\,x\equiv b\,(p)$, acima referida. Supondo x uma solução, uma segunda solução y, dando $a\,y\equiv b\,(p)$, leva a $a\,(y-x)\equiv o\,(p)$ ou $a\,(y-x)=f\,p$, $(f\in\mathfrak{A})$. Como $a\notin(p)$, será p primo com a, o que mostra ter-se $y-x=h\,p$, $(h\in\mathfrak{A})$, ou seja $y=x+p\,h$. Inversamente, qualquer que seja $h\in\mathfrak{A}$, $y=x+h\,p$ é solução da congruência, se o for x.

No caso do anel $\mathfrak{Z}$ dos inteiros, convém fazer algumas observações. Uma congruência $a\,x\equiv b\,(f)$ pode reduzir-se sempre ao caso em que $|b|<|f|$, bastando escrever, se $|b|\geqq|f|$, $b=h\,f+r$, com $|r|<|f|$. É, então, condição necessária e suficiente, para que a congruência seja solúvel, que existam inteiros x e y tais que $a\,x+f\,y=b$. A resolução desta equação 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 $x=\alpha+f\,h$, $y=\beta-a\,h$, onde h é um inteiro qualquer.

Entrando pròpriamente na teoria da factorização chegamos a provar a possibilidade de decompor cada elemento de $\mathfrak{A}$ em factores primos, à custa dum certo número de teoremas.

TEOREMA 15: — *Em* $\mathfrak{A}$, *é finita toda a sucessão de elementos* $a_1, a_2, \ldots$, *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 ex., $f \in (a_m)$, não pode haver, na sucessão dos a_i, um elemento de índice superior a m.

TEOREMA 16: — *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 17: — *Todo o elemento* $a \neq 0$ *pertencente a* $\mathfrak{A}$ *é um produto de factores primos.* Se a não fosse susceptível duma tal decomposição, poder-se-ia formar, em virtude do teorema 16, uma sucessão infinita de elementos $a_1, a_2, \ldots$, cada um dos quais seria um divisor autêntico do anterior, e todos eles tendo a mesma propriedade que a. O teorema 15 afirma-nos, por outro lado, que isso é impossível. A decomposição de a, a que alude o teorema, existe.

TEOREMA 18: — *A decomposição de* $a \in \mathfrak{A}$ *é unívoca.* Carecemos aqui duma observação. Consideremos o elemento primo p e uma unidade ε. Pode escrever-se $p = p\varepsilon.\varepsilon^{-1}$, 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. Tais decomposições considerar-se-ão idênticas. O teorema pressupõe, portanto, que os factores primos a considerar podem diferir uns dos outros por factores 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

$$a = p_1 p_2 \ldots p_s = p'_1 p'_2 \ldots p'_r, \qquad (3)$$

nas 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 unidade. O elemento primo p_1 divide o produto $p'_1 p'_2 \ldots p'_r$, pelo que dividirá p'_1 ou $p'_2 \ldots p'_r$. 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 $p_1 = p'_j$ (à parte unidades). Suponhamos $j = 1$. A igualdade (3) leva a $p_2 \ldots p_s = \varepsilon' p'_2 \ldots p'_r$, onde ε' é uma unidade. A repetição do raciocínio anterior leva a concluir 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 podem sintetizar-se neste

TEOREMA 19: — *Um anel de ideais principais comutativo, sem divisores de zero, é um domínio gaussiano.* E também:

TEOREMA 20: — *Um domínio euclidiano é um domínio gaussiano.*

4) **Aplicações** — O domínio dos inteiros de GAUSS tem as unidades ± 1 e $\pm i$. Se chamarmos *norma* de $\alpha = a + bi$ o número inteiro $N(\alpha) = a^2 + b^2$, vê-se imediatamente que é válida a igualdade $N(\alpha\beta) = N(\alpha).N(\beta)$. O elemento zero do domínio tem a norma igual a zero e é o único elemento nessas condições. Por isso, é necessário e basta, para que um produto seja nulo, que seja nulo um dos factores. Trata-se dum domínio de integridade.

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 elemento $\alpha - A\beta$ do domínio 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 dos inteiros de GAUSS, gozando, aliás, das mesmas propriedades. Então $N(\alpha - A\beta) = N(A' - A).N(\beta)$. Ora $N(A' - A) = (a' - a)^2 + (b' - b)^2 < 1$, e, portanto, $N(\alpha - A\beta) < N(\beta)$. Pondo $\alpha - A\beta = \gamma$, encontra-se, como se deseja, $\alpha = A\beta + \gamma$, $N(\gamma) < N(\beta)$. Basta, com efeito, tomar a norma dum elemento como valor absoluto do mesmo elemento. Podemos dizer:

TEOREMA 21: — *O anel dos números inteiros de* GAUSS *é um domínio euclidiano, portanto, um domínio gaussiano.*

No domínio $\mathfrak{Z}$ dos inteiros, a factorização indicado no § anterior é conhecida dos Elementos. As unidades são ± 1.

Num domínio gaussiano qualquer, tem-se:

TEOREMA 22: — *Se* $\mathfrak{A}$ *é um domínio gaussiano, um elemento indecomponível (ou que não é um produto de factores, a não ser que algum seja uma unidade) gera um ideal primo, um elemento decomponível gera um ideal que não é primo.* Se p é indecomponível e escrevemos $ab \equiv o(p)$, deve p figurar como factor em a ou b, e ser, portanto, $a \equiv o(p)$ ou $b \equiv o(p)$. Se p é decomponível, pondo $p = ab$, onde a e b são divisores autênticos de p, vê-se que $ab \equiv o(p)$, sem que se tenha $a \equiv o(p)$ ou $b \equiv o(p)$.

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 gera um ideal sem divisor. [Convém observar que o teorema 12 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 23: — *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, visto que um divisor comum de c e de a é necessàriamente uma unidade.

TEOREMA 24: — *O conjunto das classes de* $\mathfrak{A}/(a)$ *compostas de elementos primos com* a *constitui um grupo multiplicativo.* Na verdade: α) A classe que contém u pertence ao conjunto $\mathfrak{C}$, em causa; β) o produto de duas classes de $\mathfrak{C}$, visto que o produto de dois elementos primos com a é um elemento primo com a, é uma classe de $\mathfrak{C}$; γ) a propriedade associativa tem lugar em $\mathfrak{C}$; δ) 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 25: — *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 24, suposto $\mathfrak{A} = \mathfrak{Z}$ o anel dos inteiros. O anel diferença $\mathfrak{Z}/(a)$ 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 $\mathfrak{Z}/(p)$ é um corpo com p elementos. Das classes a que se refere o teorema 24 fazem parte todas as classes de $\mathfrak{Z}/(p)$, à excepção da

classe que contém o zero. Obtém-se $\Phi(p)=p-1$. Em particular, se $p=1$, é $\Phi(p)=0$. Quando a não é primo, suponhamos

$$a=\prod_{i=1}^{m} p_i^{r_i} \tag{4}$$

a sua decomposição em factores primos. Vamos ver que se tem

$$\Phi(a)=a\prod_{i=1}^{m}\left(1-\frac{1}{p_i}\right). \tag{4'}$$

Consideremos um grupo cíclico composto de a elementos. Se g for o elemento gerador, são igualmente geradores todos os elementos da forma g^t, em que t é primo com a, [Cfr., n.º 3, § 2, Cap. I]. 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

$$\mathfrak{G}=\{\varepsilon, g, \ldots, g^{p^\nu-1}\}, \quad (\varepsilon=g^{p^\nu}=\text{elemento um}),$$

se for g^k um elemento de ordem inferior a p^ν, ter-se-á $g^{kr}=\varepsilon$, com $r<p^\nu$ e inteiro. Mas, sendo $kr=p^\nu . n$, com n inteiro, 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 inteiro k leva a g^k, que não pode gerar $\mathfrak{G}$, pelo seguinte: se fosse $\mathfrak{G}=\{\varepsilon, g^k, g^{2k}, \ldots, g^{(p^\nu-1)k}\}$, com todas as potências distintas, o facto de se ter $k=pt$ levaria a $(g^{pt})^{p^\nu-1}=\varepsilon$, com $p^{\nu-1}<p^\nu-1$, o que é impossível. Deste modo, os elementos que não geram $\mathfrak{G}$ são $\varepsilon, g^p, g^{2p}, \ldots, g^{(p^{\nu-1}-1)p}$, 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 inteiros primos entre si, diferentes de 1, fácil é de ver que

$$\Phi(a)=\Phi(m)\,.\,\Phi(n). \tag{5}$$

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, aqui, no próprio grupo $\mathfrak{G}$. Como, inversamente, o produto de dois elementos 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

$$g^{km}=\varepsilon, \quad km=mnq, \quad k=nq, \quad g^k=(g^n)^q.$$

A igualdade (5) está demonstrada. Se a tem a decomposição (4), 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 (4') desejada. Diremos:

TEOREMA 26: — *Se o inteiro* a *é diferente de* 1, *o número de elementos primos com* a, *inferiores a* a, *é dado pela relação* (4'), *suposta* (4) *a decomposição de* a *em factores primos.*

É oportuno dar agora a seguinte proposição:

TEOREMA 27 (FERMAT): — *Se* p *é um inteiro primo e* a *é um inteiro 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 $\bar{a}=a+(p)\neq\bar{o}$, deste corpo, é válida a relação $\bar{a}^{p-1}=1+(p)=a^{p-1}+(p)$, que traduz precisamente a afirmação.

5) **Extensão da teoria da factorização** — Nos anéis de ideais principais sem divisores de zero, o problema da decomposição em factores primos teve a solução seguinte: um elemento é

sempre o produto de elementos primos bem determinados, contanto que não se distinga entre elementos primos associados.

Há outros domínios de integridade com elemento um, que não são anéis de ideais principais e nos quais o problema em causa tem a mesma solução. Tomemos, por ex., $\mathfrak{R}[x, y]$. Vamos ver que neste domínio é válida a teoria da factorização, pelo simples facto de ela ser válida em $\mathfrak{R}[x]$. Duma maneira geral, provaremos este

TEOREMA 28: — *Se* $\mathfrak{A}$ *é um domínio gaussiano,* $\mathfrak{A}[x]$ *é um domínio gaussiano.* A demonstração será feita um pouco mais adiante, depois de certos raciocínios que agora se seguem.

Tomemos, em $\mathfrak{A}$, dois (ou vários) elementos a e b, decompostos em factores primos, e consideremos, em seguida, o elemento produto dos factores comuns com o menor expoente. Esse elemento goza das duas propriedades características do m. d. c.. Pondo de parte unidades de $\mathfrak{A}$, ele é bem determinado.

A teoria do m. m. c. faz-se anàlogamente. Basta tomar, dadas as decomposições de a e b, o elemento formado pelo produto dos factores primos comuns e diferentes com o maior expoente.

Não existem, porém, teorias do m. d. c. e do m. m. c., no sentido dos ideais, precisamente pelo facto de não poder afirmar-se que todo o ideal seja principal.

Comecemos o estudo de $\mathfrak{A}[x]$, que nos propomos. Dado um elemento $P(x) \in \mathfrak{A}[x]$, pode escrever-se $P(x) = d \,.\, Q(x)$, onde d é o m. d. c. dos coeficientes de $P(x)$. $Q(x)$ é, então, um polinómio cujos coeficientes têm uma unidade (ou o elemento um) como m. d. c.. Os polinómios, como $Q(x)$, dizem-se *primitivos*. A decomposição anterior de $P(x)$, pondo de parte unidades de $\mathfrak{A}$, é bem determinada; mas é conveniente esclarecer que as unidades de $\mathfrak{A}$ e de $\mathfrak{A}[x]$ são as mesmas, pelo facto de um elemento não constante de $\mathfrak{A}[x]$ não poder ser uma unidade.

Os polinómios primitivos gozam dum certo número de propriedades, expressas nos teoremas que passamos a estabelecer.

TEOREMA 29: — *O produto de dois polinómios primitivos é um polinómio primitivo.* Se $R(x)$ e $S(x)$ são primitivos, seja d o m. d. c. dos coeficientes do produto $R(x)\ S(x)$: $R(x)\ S(x) = d\,Q(x)$. Supondo que d contém factores primos de $\mathfrak{A}$ não unidades, seja p um tal factor e sejam a_r e b_s os primeiros coeficientes de $R(x)$ e de $S(x)$, respectivamente, que não contêm p. O coeficiente do termo x^{r+s} do produto é da forma

$$a = a_o b_{r+s} + a_1 b_{r+s-1} + \ldots + a_r b_s + \\ + a_{r+1} b_{s-1} + \ldots + a_{r+s} b_o .$$

Todas as parcelas de a contêm p, salvo $a_r\, b_s$. Esta parcela, porém, contém igualmente p, porque a contém p. O teorema da univocidade da decomposição em $\mathfrak{A}$ garante que p será um factor de a_r ou de b_s, o que é absurdo. Assim, d é uma unidade e o teorema fica demonstrado.

TEOREMA 30: — *Se* $\mathfrak{K}$ *é o corpo cociente de* $\mathfrak{A}$, *cada polinómio* $f(x) \in \mathfrak{K}[x]$ *pode tomar a forma*

$$f(x) = \frac{P(x)}{a} = \frac{d}{a} Q(x), \qquad (6)$$

onde $P(x) \in \mathfrak{A}[x]$, $Q(x)$ *é um polinómio primitivo bem determinado em* $\mathfrak{A}[x]$ *e* $d/a \in \mathfrak{K}$ *é também bem determinado.* [O teorema põe de parte unidades de $\mathfrak{A}$]. Para dar a $f(x)$ a forma $\frac{P(x)}{a}$, basta ter em conta que os coeficientes de $f(x)$ têm a forma de cocientes de elementos de $\mathfrak{A}$. Pondo, depois, $P(x) = d\,.\,Q(x)$, tem-se um processo que leva a uma decomposição da forma anunciada. A representação é única, pois que, supondo $f(x) =$

$= d_1/a_1 \,.\, Q_1(x)$ um segundo modo de representação, tem-se sucessivamente:

$$\frac{d}{a} Q(x) = \frac{d_1}{a_1} Q_1(x), \qquad a_1 d\, Q(x) = a\, d_1 Q_1(x),$$
$$a_1 d = a\, d_1 \varepsilon, \qquad \varepsilon Q(x) = Q_1(x),$$

onde ε é uma unidade de $\mathfrak{A}$. O teorema está demonstrado.

TEOREMA 31: — *Um polinómio primitivo de* $\mathfrak{A}[x]$ *corresponde, conforme* (6), *a um elemento bem determinado de* $\mathfrak{K}[x]$, *pondo de parte unidades de* $\mathfrak{K}[x]$, *(elementos de* $\mathfrak{K}$*).* Dois polinómios $f(x)$ e $f_1(x)$, que levam ao mesmo $Q(x)$, dão

$$f(x) = \frac{d}{a} Q(x),$$

$$f_1(x) = \frac{d_1}{a_1} Q(x) = \frac{d_1 a}{a_1 d} \cdot \frac{d}{a} Q(x) = \frac{d_1 a}{a_1 d} f(x).$$

TEOREMA 32: — *A igualdade (6) faz corresponder o produto ao produto, e reciprocamente, ressalvando unidades de* $\mathfrak{K}[x]$. *Tem-se, com efeito,*

$$f(x) \,.\, f_1(x) = \frac{d}{a} Q(x) \,.\, \frac{d_1}{a_1} Q(x) = \frac{d\, d_1}{a\, a_1} Q(x) \,.\, Q_1(x),$$

sendo $Q\,Q_1$ um polinómio primitivo de $\mathfrak{A}[x]$. A parte recíproca resulta do teorema anterior.

TEOREMA 33: — *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 34: — *Os polinómios primitivos de* $\mathfrak{A}[x]$ *decompõem-se, de modo unívoco, em polinómios primitivos primos.* Dado, com efeito, o polinómio primitivo $Q(x)$ e $\mathfrak{A}[x]$, ele é sempre correspondente dum polinómio $f(x) = k\,Q(x)$ e $\mathfrak{K}[x]$, 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, deste modo,

$$f(x) = k\,Q(x) = a\,p_1(x) \ldots p_r(x) = a' q_1(x) \ldots q_r(x),$$

onde $k, a, a' \in \mathfrak{K}$. Ter-se-á também $\varepsilon k = a'$, onde ε é unidade de $\mathfrak{A}$, pelo que $Q(x) = \varepsilon\, q_1(x) \ldots q_r(x)$. Os polinómios $q_i(x)$ são primos. Outra decomposição de $Q(x)$ em elementos 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 do §.

Dado um polinómio $P(x)$ e $\mathfrak{A}[x]$, 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 $P(x) = d \,.\, Q(x)$ e decompondo d e $Q(x)$, de modo unívoco, em factores primos. Sendo dadas, então, duas decomposições $P(x) = d_1 \ldots d_r\, q_1(x) \ldots q_s(x) = d'_1 \ldots d'_{r'} q'_1(x) \ldots q'_{s'}(x)$, ter-se-ia, em primeiro lugar, $d_1 \ldots d_r = d'_1 \ldots d'_{r'}$, o que levaria à igualdade dos d_i e dos d'_j, e em segundo lugar, $q_1(x) \ldots q_s(x) = q'_1(x) \ldots q'_{s'}(x)$, 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* $P(x)$ e $\mathfrak{A}[x]$, *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 ex., um polinómio com coeficientes inteiros indecomponível tam-

bém se não decompõe quando os referidos coeficientes se supõem pertencer ao corpo dos números racionais.

Fixemos ainda esta proposição:

TEOREMA 35: — *Se* $\mathfrak{A}$ *é um domínio gaussiano,* $\mathfrak{A}[x_1, \ldots, x_n]$ *é um domínio gaussiano.*

6) **Sobre a irredutibilidade em** $\mathfrak{A}[x] - \mathfrak{A}$, como no número anterior, é um domínio gaussiano. O problema que vai ocupar-nos consiste em verificar condições em que um elemento $f(x)$ e $\in \mathfrak{A}[x]$ é decomponível ou não num *produto de polinómios*. Conforme dissemos, é válido este

TEOREMA 36: — *É necessário e basta, para que* $f(x) \in \mathfrak{A}[x]$ *seja um produto de polinómios, que* $f(x)$ *seja redutível em* $\mathbf{K}[x]$, *onde* $\mathfrak{K}$ *é o corpo cociente de* $\mathfrak{A}$.

Seja $a \in \mathfrak{A}$. O anel de polinómios $\mathfrak{A}[x]/(a)$ compõe-se de elementos da forma

$$a_o + a_1 x + \ldots + a_n x^n + a\,\mathfrak{A}[x].$$

Fazendo corresponder a cada um destes elementos um elemento

$$(a_o + a\mathfrak{A}) + (a_1 + a\mathfrak{A})\,x + \ldots + (a_n + a\mathfrak{A})\,x^n \in \mathfrak{A}/(a)[x],$$

a correspondência é um isomorfismo, como é fácil de ver. Os polinómios de última forma são *polinómios de* $\mathfrak{A}[x]$ *módulo* a. Dado $f(x) \in \mathfrak{A}[x]$, se o polinómio módulo a correspondente é do mesmo grau que $f(x)$ e irredutível, o polinómio $f(x)$ 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 $f(x) = (p-k)x + \ldots + (p-k)$, como $o < k < p$, $f(x)$ é redutível, se supusermos que $p-k$ não é unidade, visto que $p-k$ é factor de $f(x)$.

Em $\mathfrak{J}/(p)[x]$, aquele polinómio escrever-se-á ainda $(p-k)x + \ldots + (p-k)$ (1). Como $\mathfrak{J}/(p)$ é 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 $f(x) = (p x^3 + p q x^2 + 1)\ (x+2)$. O polinómio módulo p correspondente é $x+2$. Este polinómio é irredutível, mas não o é o polinómio $f(x)$. 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 corresponde ao facto de um polinómio ser irredutível em $\mathfrak{J}[x]$, mas ser redutível módulo p, embora conservando o grau. Tomemos $f(x) = x^4 + 2x^3 + 5x^2 + 3x + 3$. O polinómio módulo 2 é $x^4 + x^2 + x + 1 = (x+1)\ (x^3 + x^2 + 1)$. Se $f(x)$ 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 $f(x)$ 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 $\mathfrak{J}[x]$.

---

(1) É uma maneira abreviada de escrever $(p-k+(p))x + (p-k+(p))$.

Um critério importante de irredutibilidade é dado pelo seguinte

TEOREMA 37 (SCHÖNEMANN-EISENSTEIN): — *O polinómio* $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathfrak{A}[x]$ *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 *não côngruo de zero módulo* p, $a_i \equiv 0\,(p)$, $(i = 0, 1, 2, \ldots, n-1)$, a_0 *não côngruo de zero módulo* p^2. Suponhamos que podia pôr-se $f(x) = (b_0 + b_1 x + \ldots + b_r x^r) \cdot (c_0 + c_1 x + \ldots + c_s x^s)$, 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 simultâneamente estes dois últimos elementos. Suponhamos $c_0 \equiv o\,(p)$. Escrevendo

$$(b_0 + b_1 x + \ldots + b_r x^r)(c_0 + c_1 x + \ldots + c_s x^s) \equiv a_n x^n \,(p),$$

podemos eliminar c_0 na congruência. Se c_k for o primeiro dos coeficientes c_i que não é divisível por p, tem-se

$$(b_0 + b_1 x + \ldots + b_r x^r)(c_k x^k + \ldots + c_s x^s) \equiv a_n x^n \,(p).$$

O inteiro k satisfaz à dupla desigualdade $o < k \leqslant s$. No 1.º membro da congruência, o coeficiente de x^k é $c_k b_0$, 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 $f(x)$ num produto é, pois, absurda.

Um caso particular de irredutibilidade é o seguinte [suposto $\mathfrak{A} = \mathfrak{I}$]:

TEOREMA 38 (SCHÖNEMANN): — *O cociente*

$$\frac{x^{p^n} - u}{x^{p^{n-1}} - u} = x^{(p-1)p^{n-1}} + x^{(p-2)p^{n-1}} + \ldots + x^{2p^{n-1}} + x^{p^{n-1}} + u,$$

no qual p *é um elemento primo e* n *é um inteiro qualquer, é irredutível.* A demonstração repousa sobre a observação simples de que, dados $f(x) \in \mathfrak{A}[x]$ e $a \in \mathfrak{A}$, os dois polinómios $f(x)$ e $f(x+a)$ são simultâneamente decomponíveis ou indecomponíveis.

Mudando, então, x em $x+u$, tem-se

$$Q = \frac{(x+u)^{p^n} - u}{(x+u)^{p^{n-1}} - u} = \text{polinómio em } x \text{ que, para } x = o, \text{ se reduz a } pu.$$

Mas, sendo

$$(x+u)^{p^n} \equiv x^{p^n} + u\,(p), \quad (x+u)^{p^{n-1}} \equiv x^{p^{n-1}} + u\,(p),$$

pode escrever-se

$$Q = \frac{x^{p^n} + p\,\Phi(x)}{x^{p^{n-1}} + p\,\Psi(x)} = pu + a_1 x + \ldots + a_\sigma x^\sigma + p\,R(x)$$

onde $R(x)$, $\Phi(x)$ e $\Psi(x)$ pertencem a $\mathfrak{A}[x]$ e $\sigma = (p-1)p^{n-1}$. Da relação anterior tira-se, sucessivamente, suposto $T(x) \in \mathfrak{A}[x]$,

$$x^{p^n} + p\,\Phi(x) = (x^{p^{n-1}} + p\,\Psi(x))\,(pu + a_1 x + \ldots + a_\sigma x^\sigma) + p\,T(x), \quad x^{p^n} \equiv x^{p^{n-1}} \cdot (a_1 x + \ldots + a_\sigma x^\sigma)\ (\text{mod } p).$$

Daqui se conclui que é $u - a_\sigma \equiv o\,(p)$, e, portanto, a_σ não côngruo de zero módulo p, assim como $a_1, a_2, \ldots, a_{\sigma-1} \equiv o\,(p)$. O polinómio Q, para o qual é ainda $a_0 = pu$ não côngruo de zero módulo p^2, está precisamente nas condições exigidas pelo teorema SCHÖNEMANN-EISENSTEIN.

BIBLIOGRAFIA

São os seguintes os livros que há necessidade de indicar aqui:

B. L. VAN DER WAERDEN — *Moderne Algebra*, tomo 1.º, Berlim, 1930;

H. HASSE — *Höhere Algebra*, tomo I, 2.ª edição, Berlim, 1933;

H. HASSE — *Aufgabensammlung zur höheren Algebra*, Berlim, 1934;

A. ALMEIDA COSTA — *Elementos da Teoria dos Anéis*, Porto, Centro de Estudos Matemáticos, 1943.

CAPÍTULO V

IDEAIS COMUTATIVOS (TEORIA DE LASKER-NOETHER)

§ 1 — Ideais primários. Representações normadas. Ideais com uma base finita

1) **Indicações gerais** — Depois dos trabalhos de L. KRONECKER sobre sistemas modulares de polinómios, aos quais se seguiram resultados de J. KÖNIG e D. HILBERT, introduziu E. LASKER, em 1905, uma teoria de divisibilidade dos módulos de polinómios. Numa extensão das ideias de LASKER e de KRONECKER, pode dizer-se que a teoria dos ideais comutativos se reduz aos dois problemas seguintes: 1) estudo dos zeros dum ideal de polinómios dum domínio de integridade $\Re[x_1, \ldots, \ldots, x_n]$; 2) estudo das condições necessárias e suficientes para que um dado polinómio pertença a um dado ideal.

Com EMMY NOETHER, a solução dos problemas concretos que acabamos de referir é consequência duma teoria abstracta mais geral, que vai ocupar-nos neste Capítulo. Em todo ele, o símbolo $\mathfrak{A}$ representará um anel comutativo.

2) **Ideais primários** — Um ideal $\mathfrak{d}$, de $\mathfrak{A}$, diz-se *primário,* se goza da propriedade seguinte: a condição $a\,b \equiv o\ (\mathfrak{d})$, com a não côngruo de zero módulo $\mathfrak{d}$, arrasta a existência duma potência inteira $b^\rho \equiv o\ (\mathfrak{d})$. Os ideais primos representam casos particulares dos ideais primários.

Tomemos, no anel $\mathfrak{J}$ dos inteiros, o ideal (p^ρ), gerado pela potência ρ do número primo p. Se for $a\,b \equiv o\ (p^\rho)$, com a não côngruo de zero módulo p^ρ, vê-se que é $a\,b = h\,p^\rho$, sem que p^ρ entre em a inteiramente como factor. Nessas condições, p figura como factor em b, e, consequentemente, existe uma potência de b que contém p^ρ.

TEOREMA 1: — *É condição necessária e suficiente, para que* $\mathfrak{d}$ *seja um ideal primário, que todo o divisor de zero de* $\mathfrak{A}/\mathfrak{d}$ *seja um elemento nilpotente.* De facto, se $\mathfrak{d}$ é primário, suponhamos $\bar{a}\,\bar{b} = \bar{o}$, com $\bar{a} \neq \bar{o}$, $(\bar{a},\ \bar{b} \in \mathfrak{A}/\mathfrak{d})$. Se a e b são elementos de $\mathfrak{A}$ que têm $\bar{a}$ e $\bar{b}$ como correspondentes no homomorfismo $\mathfrak{A} \sim \mathfrak{A}/\mathfrak{d}$, vê-se que é $a\,b \equiv o\ (\mathfrak{d})$ e a não côngruo de zero módulo $\mathfrak{d}$. Por hipótese, tem-se $b^\rho \equiv o\ (\mathfrak{d})$, e, por consequência, $\bar{b}^\rho = \bar{o}$. Inversamente, seja $a\,b \equiv (\mathfrak{d})$, a não côngruo de zero módulo $\mathfrak{d}$. Como é $\bar{a}\,\bar{b} = \bar{o}$, a hipótese do teorema implica $\bar{b}^r = \bar{o}$, ou seja $b^r \in \mathfrak{d}$. O teorema está demonstrado.

No que vai seguir-se, daremos, sob a forma de teoremas, algumas propriedades dos ideais primários.

TEOREMA 2: — *O conjunto dos elementos* $a \in \mathfrak{A}$, *cujas potências pertencem a um ideal primário* $\mathfrak{d}$, *forma um ideal primo* $\mathfrak{p}$, *divisor de* $\mathfrak{d}$.

Em primeiro lugar, os referidos elementos constituem um ideal $\mathfrak{p}$, porque, suposto a tal que $a^\sigma \in \mathfrak{d}$, também $(t\,a)^\sigma = t^\sigma a^\sigma \in \mathfrak{d}$, $(t \in \mathfrak{A})$; e, se $a^\sigma \in \mathfrak{d}$, $b^\rho \in \mathfrak{d}$, também $(a-b)^{\rho+\sigma-1}$, como soma de elementos pertencentes a $\mathfrak{d}$, pertence a $\mathfrak{d}$. Em seguida, $\mathfrak{p}$ é primo, porque, se $a\,b \in \mathfrak{p}$, com $a \notin \mathfrak{p}$, tem-se $a^\tau b^\sigma \in \mathfrak{d}$, com $a^\sigma \notin \mathfrak{d}$; e, como $\mathfrak{d}$ é primário, ter-se-á $b^{\sigma\tau} \in \mathfrak{d}$, pelo que $b \in \mathfrak{p}$. Por último, tem-se $\mathfrak{p} \supseteq \mathfrak{d}$, pelo facto de $\mathfrak{d}$ ser composto de elementos cuja primeira potência pertence a $\mathfrak{d}$. O teorema ficou estabelecido.

$\mathfrak{p}$ diz-se *ideal primo associado a* $\mathfrak{d}$ e este último é *um ideal primário associado a* $\mathfrak{p}$.

COROLÁRIO 1: — *A condição* $a\,b \equiv o\ (\mathfrak{d})$, *com* a *não côngruo de zero módulo* $\mathfrak{d}$, *arrasta* $b \in \mathfrak{p}$.

COROLÁRIO 2: — *Dados os ideais* $\mathfrak{a}$ *e* $\mathfrak{a}'$ *tais que* $\mathfrak{a}\,\mathfrak{a}' \subseteq \mathfrak{s}$, *com* $\mathfrak{a}$ *não contido em* $\mathfrak{s}$, *tem-se* $\mathfrak{a}' \subseteq \mathfrak{p}$. Se pudesse ser $\mathfrak{a}'$ não contido em $\mathfrak{p}$, tomaríamos a' e $\mathfrak{a}'$, com $a' \notin \mathfrak{p}$, e, depois, tomaríamos $a \in \mathfrak{a}$, com $a \notin \mathfrak{s}$. Ter-se-ia $a\,a' \in \mathfrak{s}$, com $a \notin \mathfrak{s}$ e $a' \notin \mathfrak{p}$, contra a afirmação do corolário anterior.

As relações entre $\mathfrak{s}$ e $\mathfrak{p}$, expressas pelos resultados precedentes, são características de $\mathfrak{s}$ como ideal primário e de $\mathfrak{p}$ como ideal primo associado a $\mathfrak{s}$. Duma maneira precisa, é válido o seguinte

TEOREMA 3: — *Supondo* $\mathfrak{p} \supseteq \mathfrak{s}$ *e que* $a\,b \in \mathfrak{s}$, *com* $a \notin \mathfrak{s}$, *arrasta* $b \in \mathfrak{p}$; *além disso, que* $b \in \mathfrak{p}$ *arrasta* $b^\sigma \in \mathfrak{s}$, $\mathfrak{s}$ *é um ideal primário e* $\mathfrak{p}$ *é o ideal primo associado a* $\mathfrak{s}$. Em primeiro lugar, é imediato que $\mathfrak{s}$ é um ideal primário, pois $a\,b \equiv o\,(\mathfrak{s})$, com a não côngruo de zero módulo $\mathfrak{s}$, dá $b^\sigma \in \mathfrak{s}$. Seja, em seguida, $b \in \mathfrak{A}$ um elemento tal que $b^\sigma \in \mathfrak{s}$; pretende-se mostrar que $b \in \mathfrak{p}$, sem esquecer que, para todos os elementos de $\mathfrak{p}$, há uma potência pertencente a $\mathfrak{s}$. Supondo $b^\sigma \in \mathfrak{s}$, designemos por τ a mais pequena potência tal que $b^\tau \in \mathfrak{s}$. Se for $\tau = 1$, tem-se $b \in \mathfrak{s}$, e, portanto, $b \in \mathfrak{p}$, visto ser $\mathfrak{p} \supseteq \mathfrak{s}$. Escrevendo $b^\tau = b.b^{\tau-1}$, quando $\tau \neq 1$, pelo facto de se ter $b^{\tau-1} \notin \mathfrak{s}$, vale, por hipótese, como se deseja, $b \in \mathfrak{p}$.

É costume distinguir ainda entre *ideal primário forte* e *ideal primário fraco*, conforme $\mathfrak{s}$ contiver ou não uma potência de $\mathfrak{p}$. Se $\mathfrak{s}$ é forte, diz-se *expoente* de $\mathfrak{s}$ o mais pequeno inteiro ρ tal que $\mathfrak{p}^\rho \subseteq \mathfrak{s}$.

OBSERVAÇÃO: — A definição de ideal primo associado a um ideal primário entra na definição mais geral que vamos dar. Seja $\mathfrak{a}$ um ideal qualquer de $\mathfrak{A}$. Se considerarmos os elementos $x \in \mathfrak{A}$ para os quais existe um inteiro ρ (função de x) tal que $x^\rho \in \mathfrak{a}$, obtém-se um ideal de $\mathfrak{A}$, que se diz *radical* de $\mathfrak{a}$ e se representa pelo símbolo $\mathfrak{R}(\mathfrak{a})$. Claramente que é sempre $\mathfrak{R}(\mathfrak{a}) \supseteq \mathfrak{a}$. Neste sentido, vê-se que o ideal primo $\mathfrak{p}$, associado ao ideal primário $\mathfrak{s}$, é o radical $\mathfrak{R}(\mathfrak{s})$.

Tanto a noção de ideal primo como a de ideal primário são susceptíveis, em certos casos, de interpretação geométrica de grande interesse. Suponhamos $\mathfrak{K}$ o corpo dos números complexos e tomemos o domínio de integridade $\mathfrak{K}[x_1, \ldots, x_n]$. Se $P(x_1, \ldots, x_n)$ pertencer ao domínio e se os x_i se interpretam como coordenadas dum espaço $\mathfrak{R}_n$ a n dimensões, um ponto $(a_1, \ldots, a_n)$ desse espaço pertence à hiper-superfície $P(x_1, \ldots, x_n) = o$, se for $P(a_1, \ldots, a_n) = o$. Um conjunto $\mathfrak{C}$ de pontos de $\mathfrak{K}_n$ diz-se uma *multiplicidade algébrica irredutível,* se os pontos puderem ser definidos como intersecção dum certo número de hiper-superfícies, e se, satisfazendo todos os pontos a uma equação de tipo $P(x_1, \ldots, x_n) \,.\, Q(x_1, \ldots, x_n) = o$, pertencem os mesmos, necessàriamente, a uma das hiper-superfícies $P = o$ ou $Q = o$. Consideremos todas as hiper-superfícies que contêm todos os pontos de $\mathfrak{C}$ e as equações correspondentes. Os seus primeiros membros, como elementos de $\mathfrak{K}[x_1, \ldots, x_n]$, constituem um ideal. A irredutibilidade de $\mathfrak{C}$ mostra que esse ideal é primo. Um exemplo de multiplicidade irredutível é dado por um único ponto de $\mathfrak{R}_n$.

Posto isto, consideremos um ideal $\mathfrak{a}$ de $\mathfrak{K}[x_1, \ldots, x_n]$. Um ponto $(a_1, \ldots, a_n)$ diz-se um *zero do ideal,* se for um zero de todos os elementos do ideal. O problema da determinação dos zeros dum ideal, a que aludimos no n.º 1, tem grande importância, podendo dar-se a este respeito o enunciado a seguir, cuja demonstração diferimos para mais adiante.

TEOREMA 4: — *Uma multiplicidade algébrica irredutível* $\mathfrak{M}$ *determina, de modo unívoco, um ideal primo* $\mathfrak{p}$, *do qual são zeros todos os pontos de* $\mathfrak{M}$ *e apenas esses pontos; inversamente, um ideal primo* $\mathfrak{p}$, *de* $\mathfrak{K}[x_1, \ldots, x_n]$ *determina, pelo conjunto dos seus zeros, uma multiplicidade algébrica irredutível* $\mathfrak{M}$, *de pontos de* $\mathfrak{R}_n$, *não podendo haver um ideal* $\mathfrak{b} \supset \mathfrak{p}$ *do qual todos os pontos de* $\mathfrak{M}$ *sejam também zeros.*

Seja, de novo, um ideal arbitrário $\mathfrak{a}$, de $\mathfrak{K}[x_1, \ldots, x_n]$. Se $\mathfrak{M}$ for uma multiplicidade irredutível de zeros de $\mathfrak{a}$, poderemos formular duas hipóteses: ou $\mathfrak{M}$ é um subconjunto próprio duma outra multiplicidade irredutível de zeros de $\mathfrak{a}$

($\mathfrak{M}$ está, então, «mergulhada» noutra multiplicidade), ou esse facto não tem lugar. Se $\mathfrak{p}$ é o ideal primo definido por $\mathfrak{M}$, tem-se $\mathfrak{p} \supseteq \mathfrak{a}$. Se existe entre $\mathfrak{p}$ e $\mathfrak{a}$ outro ideal primo $\mathfrak{p}'$, a multiplicidade $\mathfrak{M}'$, que este define, contém $\mathfrak{M}$, que pode assim «mergulhar-se» em $\mathfrak{M}'$. Se não existe ideal $\mathfrak{p}'$, $\mathfrak{p}$ é um ideal primo mínimo divisor de $\mathfrak{a}$.

Quando $\mathfrak{a}$ é um ideal primário $\mathfrak{s}$, consideremos o ideal primo $\mathfrak{p}$ que lhe está associado. É $\mathfrak{p} \supseteq \mathfrak{s}$. Os zeros de $\mathfrak{p}$ são zeros de $\mathfrak{s}$, e a inversa é também verdadeira, como se verifica imediatamente. Assim: *os zeros dum ideal primário $\mathfrak{s}$ constituem uma multiplicidade irredutível, a qual define o ideal primo associado a $\mathfrak{s}$*. Essa multiplicidade não é «mergulhável», pois não existe ideal primo entre $\mathfrak{s}$ e $\mathfrak{p}$.

3) **Representações normadas dum ideal** — Um ideal $\mathfrak{a}$ diz-se *redutível,* se existirem dois ideais $\mathfrak{a}'$ e $\mathfrak{a}''$, divisores autênticos de $\mathfrak{a}$ e tais que $\mathfrak{a} = \mathfrak{a}' \cap \mathfrak{a}''$. Consideremos a intersecção dum número finito de ideais primários $\mathfrak{s}_i$, $(i = 1, 2, \ldots, r)$:

$$\mathfrak{a} = \mathfrak{s}_1 \cap \mathfrak{s}_2 \cap \ldots \cap \mathfrak{s}_r . \qquad (1)$$

Se um dos ideais $\mathfrak{s}_1$, por ex., contém a intersecção de todos os outros, é $\mathfrak{s}_1 \cap \ldots \cap \mathfrak{s}_r = \mathfrak{s}_2 \cap \ldots \cap \mathfrak{s}_r$. Escrita a igualdade (1), podemos supor eliminados, sucessivamente, todos os ideais gozando da propriedade que acaba de atribuir-se a $\mathfrak{s}_1$. Feito isso, chega-se a um resultado da forma (1). Suporemos, assim, que, em (1), se realizam já as condições indicadas. Nenhum dos ideais $\mathfrak{s}_j$ pode agora ser eliminado de (1), pelo que se diz *não simplificável* a representação correspondente de $\mathfrak{a}$. Isto não significa, todavia, que haja uma única representação não simplificável de $\mathfrak{a}$. Vamos demonstrar, com efeito, o seguinte

TEOREMA 5: — *A intersecção dum número finito de ideais primários $\mathfrak{s}_i$, com o mesmo ideal primo associado $\mathfrak{p}$, é um ideal primário associado a $\mathfrak{p}$.* Seja a decomposição (1) nas condições do enunciado. Quer-se mostrar que $\mathfrak{p}$ e $\mathfrak{a}$ estão nas relações

seguintes: 1) $\mathfrak{p} \supseteq \mathfrak{a}$; 2) a condição $ab \in \mathfrak{a}$, com $a \notin \mathfrak{a}$, arrasta $b \in \mathfrak{p}$; 3) a hipótese $b \in \mathfrak{p}$ implica $b^\sigma \in \mathfrak{a}$, para um certo σ. A relação $\mathfrak{p} \supseteq \mathfrak{a}$ é imediata, visto que $\mathfrak{p} \supseteq \mathfrak{s}_j$, para $j = 1, 2, \ldots, r$. Se $ab \in \mathfrak{a}$, é $ab \in \mathfrak{s}_j$, e, como $a \notin \mathfrak{a}$, há um ideal $\mathfrak{s}_h$, entre os $\mathfrak{s}_j$, que não contém a. Isso garante $b \in \mathfrak{p}$. Finalmente, se $b \in \mathfrak{p}$, tem-se $b^{\sigma_j} \in \mathfrak{s}_j$. Representando por σ o maior dos inteiros σ_j, tem-se $b^\sigma \in \mathfrak{s}_j$, qualquer que seja j. Logo é $b^\sigma \in \mathfrak{a}$, como se deseja.

Quando um ideal $\mathfrak{a}$ admite uma representação não simplificável (1), por meio de ideais primários $\mathfrak{s}_j$, cujos ideais primos associados $\mathfrak{p}_j$ são todos diferentes, diz-se que a representação de $\mathfrak{a}$ é *normada.*

Admitamos que $\mathfrak{a}$ é susceptível de ser representado por uma intersecção de ideais primários da forma (1). Os raciocínios que acabam de ser feitos mostram que $\mathfrak{a}$ é susceptível duma representação normada. Tem lugar, então, o seguinte

TEOREMA 6: — *Se $\mathfrak{a}$ admitir uma representação normada com mais do que uma componente $\mathfrak{s}_j$, $\mathfrak{a}$ não é primário.* Seja

$$\mathfrak{a} = \mathfrak{s}_1 \cap \ldots \cap \mathfrak{s}_r , \quad (r \geqq 2),$$

e suponhamos $\mathfrak{p}_j$ o ideal primo associado a $\mathfrak{s}_j$. Como os $\mathfrak{p}_j$ são todos diferentes, escolhamos um, de entre eles, $\mathfrak{p}_1$ por ex., que não contenha qualquer outro. Em seguida, tomemos, com $k = 2, 3, \ldots, r$, elementos $b_k^{k^\rho} \in \mathfrak{p}_k$ não pertencentes a $\mathfrak{p}_1$. Existe um inteiro σ tal que $b_k^\sigma \in \mathfrak{s}_k$, para todos os valores considerados de k. Por hipótese, é possível encontrar em $\mathfrak{s}_1$ um elemento $a_1 \notin \mathfrak{a}$, pois que, se todos os elementos de $\mathfrak{s}_1$ pertencessem a $\mathfrak{a}$, seria $\mathfrak{a} = \mathfrak{s}_1$, e o ideal $\mathfrak{s}_2$, por ex., conteria a intersecção dos demais ideais. O elemento $a_1 b_2^\sigma \ldots b_r^\sigma$, que pertence a $\mathfrak{s}_1, \mathfrak{s}_2, \ldots, \mathfrak{s}_r$, pertence a $\mathfrak{a}$, sem que a_1 pertença a $\mathfrak{a}$. Este último ideal não pode ser primário, pois que, pondo $b_2^\sigma \ldots b_r^\sigma = b$, vê-se que, em consequência de ser $a_1 b \in \mathfrak{a}$, $a_1 \notin \mathfrak{a}$, teria de ser $b^\rho \in \mathfrak{a}$, ao mesmo tempo que, pelo facto de se ter $\mathfrak{p}_1 \supseteq \mathfrak{s}_1 \supseteq \mathfrak{a}$, seria também $b^\rho \in \mathfrak{p}_1$. Isso daria $b_2^{\sigma\rho} \ldots b_r^{\sigma\rho} \in \mathfrak{p}_1$, e, portanto, uma potência $b_k^{\sigma\rho}$ pertenceria a $\mathfrak{p}_1$, o que mostraria

ser $b_k \in \mathfrak{p}_1$, contra a hipótese relativa à escolha de todos os b_k. A proposição está estabelecida.

Os ideais $\mathfrak{d}_j$ dizem-se, então, *componentes primárias* de $\mathfrak{a}$.

No caso do domínio de integridade $\mathfrak{R}[x_1, \ldots, x_n]$, é válido o seguinte

TEOREMA 7 (LASKER): — *Em* $\mathfrak{R}[x_1, \ldots, x_n]$, *todo o ideal* $\mathfrak{a}$ *tem uma representação normada, mediante um número finito de ideais primários.* A demonstração será feita adiante, como consequência duma proposição mais geral de E. NOETHER.

É muito simples provar este outro

TEOREMA 8: — *É condição necessária e suficiente, para que um ideal primo* $\mathfrak{p}$ *contenha um ideal* $\mathfrak{a}$, *susceptível duma representação normada, que* $\mathfrak{p}$ *contenha um ideal primo associado a uma das componentes primárias de* $\mathfrak{a}$. Na verdade, supondo $\mathfrak{a}$ com uma representação normada da forma (1), tem-se $\mathfrak{d}_1 \ldots \mathfrak{d}_r \subseteq \mathfrak{d}_1 \cap \ldots \cap \mathfrak{d}_r = \mathfrak{a}$, de modo que a hipótese $\mathfrak{p} \supseteq \mathfrak{a}$ implica que $\mathfrak{p}$ contenha um dos $\mathfrak{d}_i$. Então, $\mathfrak{p}$ contém igualmente o ideal primo associado a esse $\mathfrak{d}_i$, de sorte que a condição é necessária. A inversa é imediata.

Mediante o teorema de LASKER, no domínio $\mathfrak{R}[x_1, \ldots, x_n]$ o ideal $\mathfrak{a}$ é qualquer. Se, dado $\mathfrak{a}$, quisermos encontrar todos os seus ideais divisores, primos e mínimos, teremos de procurar os ideais primos $\mathfrak{p}_i$ associados às suas componentes primárias duma dada representação, abandonando aqueles $\mathfrak{p}_i$ que contenham outros dos $\mathfrak{p}_i$ como seus subideais autênticos. Cada ideal divisor, primo e mínimo, define uma multiplicidade «não mergulhável» de zeros de $\mathfrak{a}$, encontrando-se qualquer zero de $\mathfrak{a}$, conforme o teorema 8, numa dessas multiplicidades. Em resumo: se um ideal de $\mathfrak{R}[x_1, \ldots, x_n]$ é primário, os seus zeros constituem uma multiplicidade irredutível; se o não é, os seus zeros encontram-se totalmente num número finito de multiplicidades irredutíveis.

TEOREMA 9: — *O radical* $\mathfrak{R}(\mathfrak{a})$, *do ideal* $\mathfrak{a} \subseteq \mathfrak{R}[x_1, \ldots, x_n]$, *é dado pela intersecção dos ideais divisores de* $\mathfrak{a}$, *primos e mínimos.*

Prova-se imediatamente este teorema, tendo em conta a definição do radical $\mathfrak{R}(\mathfrak{a})$, dada na observação feita no n.º 2.

TEOREMA 10: — *No domínio* $\mathfrak{R}[\mathrm{x}_1, \ldots, \mathrm{x}_n]$, *os zeros dum ideal* $\mathfrak{a}$ *coincidem com os zeros do seu radical.* Um zero de $\mathfrak{R}(\mathfrak{a})$ é zero de $\mathfrak{a}$, por ser $\mathfrak{R}(\mathfrak{a}) \supseteq \mathfrak{a}$. Inversamente, seja $(a_1, \ldots, a_n)$ um zero de $\mathfrak{a}$. Se $P \in \mathfrak{R}(\mathfrak{a})$, tem-se $P^\sigma \in \mathfrak{a}$, e, portanto, $P^\sigma(a_1, \ldots, a_n) = o$, o que implica $P(a_1, \ldots, a_n) = o$. É fácil demonstrar agora o

TEOREMA 11 (teorema dos zeros de HILBERT): — *Se um polinómio* $\mathrm{P}(\mathrm{x}_1, \ldots, \mathrm{x}_n) \in \mathfrak{R}[\mathrm{x}_1, \ldots, \mathrm{x}_n]$ *admite todos os zeros do ideal* $\mathfrak{a}$, *há uma potência de* P *que pertence a* $\mathfrak{a}$. De facto, se P admite todos os zeros de $\mathfrak{a}$, admite os zeros das multiplicidades irredutíveis em que se decompõe a multiplicidade daqueles zeros, pelo que P pertence aos ideais divisores, primos e mínimos, de $\mathfrak{a}$, ou seja ao radical $\mathfrak{R}(\mathfrak{a})$.

4) **Ideais com uma base finita** — Dado $\mathfrak{A}$, diz-se que o seu ideal $\mathfrak{a}$ tem uma *base finita* $(a_1, \ldots, a_n)$, se for $\mathfrak{a} = (a_1, \ldots, a_n)$. Os elementos de $\mathfrak{a}$ são somas finitas da forma $\Sigma a_i s_i + \Sigma n_j a_j$, onde os s_i pertencem a $\mathfrak{A}$ e os n_j são inteiros.

Nos anéis de ideais principais, todo o ideal tem uma base finita, composta dum único elemento. Num corpo, os dois ideais que podem ser considerados (nulo e unidade) têm igualmente uma base finita. Dum modo geral, diz-se que, num anel $\mathfrak{A}$, é válida a *condição de base,* se todo o ideal tem uma base finita. Tem lugar esta proposição:

TEOREMA 12: — *Se a condição de base é válida no anel* $\mathfrak{A}$ *com elemento um, é igualmente válida em* $\mathfrak{A}[\mathrm{x}_1, \ldots, \mathrm{x}_n]$. Comecemos por considerar $\mathfrak{A}$ e $\mathfrak{A}[x]$. Se $\mathfrak{a}$ é um ideal de $\mathfrak{A}[x]$, não reduzido ao ideal nulo (para este o teorema é evidente), $\mathfrak{a}$ contém, efectivamente, polinómios em x, pois não pode reduzir-se a um ideal não nulo de $\mathfrak{A}$. Tomemos, então, o conjunto dos

polinómios de $\mathfrak{a}$, e, em seguida, o conjunto $\mathfrak{C}$ dos coeficientes das suas mais altas potências. Incidentalmente, figurarão entre tais polinómios elementos pertencentes a $\mathfrak{A}$, os quais contribuirão também para $\mathfrak{C}$. Juntando a $\mathfrak{C}$ o elemento nulo de $\mathfrak{A}$, obtém-se um ideal $\mathfrak{x}$, de $\mathfrak{A}$. De facto, sejam

$$\alpha = a x^n + \ldots, \qquad \beta = b x^m + \ldots$$

dois polinómios de $\mathfrak{a}$. Se $b = a$, a diferença $b - a \in \mathfrak{x}$. Se $b \neq a$, tem-se, supondo $n \geqq m$, $\alpha - \beta x^{n-m} = (a-b) x^n + \ldots$, e, portanto, $a - b \in \mathfrak{x}$. Se r é um elemento qualquer de $\mathfrak{A}$, ou é $r a = o$, e $r a \in \mathfrak{x}$, ou é $r a \neq o$, e $r a = r a x_1^n + \ldots \in \mathfrak{a}$, tendo-se $r a \in \mathfrak{x}$, como se deseja. Nestas condições, ponhamos $\mathfrak{x} = (a_1, \ldots, a_s)$. Visto que os a_j, pertencem a $\mathfrak{x}$, escrevamos

$$a_j = a_j x^{n_j} + \ldots \in \mathfrak{a}, \qquad (j = 1, 2, \ldots, s),$$

e designemos por n o maior dos n_j. O ideal $(a_1, \ldots, a_s)$ é um sub-ideal de $\mathfrak{a}$. Se um elemento $f(x) \in \mathfrak{a}$ é de grau $\sigma \geqq n$, e se o coeficiente da sua mais alta potência é $\Sigma a_j r_j$, o polinómio

$$g(x) = f(x) - \Sigma a_j r_j x^{\sigma - n_j} \in \mathfrak{a}$$

é de grau inferior a σ. O polinómio f aparece como a soma de dois polinómios de $\mathfrak{a}$, um deles pertencente ao ideal $(a_1, \ldots, a_s)$, o outro de grau inferior ao de f. Repetindo o processo sobre g, e continuando, chega-se a concluir que f é soma dum polinómio pertencente ao ideal $(a_1, \ldots, a_s)$ e de outro cujo grau é inferior a n. Por isso, vai interessar-nos a construção duma base para os polinómios de $\mathfrak{a}$ de grau inferior a n, visto que uma base de $\mathfrak{a}$ se obterá considerando simultâneamente os elementos de tal base e os elementos $a_1, \ldots, a_s$. Se existem em $\mathfrak{a}$ polinómios de grau $n-1$, os coeficientes de x^{n-1} e o elemento nulo de $\mathfrak{A}$ constituem um ideal $\mathfrak{x}'$, de $\mathfrak{A}$, sendo $\mathfrak{x}' = (b_1, \ldots, b_t)$. Os polinómios

$$\beta_i = b_i x^{n-1} + \ldots, \qquad (i = 1, 2, \ldots, t),$$

pertencem a $\mathfrak{a}$. Um polinómio $h(x) \in \mathfrak{a}$, de grau $n-1$, no qual o coeficiente da sua mais alta potência seja da forma $\Sigma b_i s_i$, é soma dum polinómio pertencente ao ideal $(\beta_1, \ldots, \beta_t)$ e de outro de grau $\leqq n-2$. Juntando à base $(\alpha_1, \ldots, \alpha_s)$, os elementos $(\beta_1, \ldots, \beta_t)$ obtém-se um ideal $(\alpha_1, \ldots, \alpha_s; \beta_1, \ldots, \beta_t)$, tal que todo o polinómio de $\mathfrak{a}$ é soma dum polinómio deste ideal e dum polinómio de grau $\leqq n-2$. Se há polinómios de grau $n-2$ em $\mathfrak{a}$, repete-se o raciocínio, que se prosseguirá, se for necessário, até encontrar uma base que leve ao ideal $(\alpha_1, \ldots, \alpha_s; \beta_1, \ldots, \beta_t; \ldots; \lambda_1, \ldots, \lambda_p)$, tal que todo o polinómio de $\mathfrak{a}$ seja uma soma dum polinómio deste ideal e dum elemento de $\mathfrak{A}$. Os elementos de $\mathfrak{A}$ nestas condições formam um ideal de $\mathfrak{A}$, que tem uma certa base, cujos elementos se juntarão à base dos $\alpha\alpha, \beta\beta, \ldots, \lambda\lambda$, para se obter, finalmente a base de $\mathfrak{a}$.

Demonstrado o teorema para $\mathfrak{A}[x]$ ou $\mathfrak{A}[x_1]$, passa-se a $\mathfrak{A}[x_1, x_2]$ e continua-se até $\mathfrak{A}[x_1, \ldots, x_n]$.

Como aplicação deste importante resultado, provaremos o

TEOREMA 13 (HILBERT): — *Dada uma sucessão infinita de formas de* n *variáveis* $x_1, x_2, \ldots, x_n$, *por ex.,* $F_1, F_2, F_3, \ldots$, *com coeficientes pertencentes a um corpo* $\mathfrak{K}$, *há sempre um sistema* $\Phi_1, \ldots, \Phi_m$, *de* m *formas, tomadas entre os* F_i, *tais que todos os* F_j *se exprimem do modo seguinte:* $F_j = A_1 \Phi_1 + \ldots + A_m \Phi_m$. *Os coeficientes* $A_1, \ldots, A_m$ *são formas construídas com coeficientes pertencentes ao referido corpo.* Consideremos o ideal de $\mathfrak{K}[x_1, \ldots, x_n]$ gerado pelos elementos $F_1, F_2, \ldots$. Nesse ideal há uma base finita. Se $\Phi'_1, \ldots, \Phi'_q$ forem os elementos dessa base, eles exprimem-se, no seu conjunto, num certo número de elementos $\Phi_1, \ldots, \Phi_m$, tomados entre os F_j, de sorte que os Φ constituem também uma base para o ideal. Os A_i são formas, por o serem os F_j.

§ 2 — Anéis noetherianos

1) **Definição e primeiras propriedades** — Tomemos o anel $\mathfrak{A}$. Diz-se que $\mathfrak{A}$ verifica a condição de *cadeia ascendente* ou de *cadeia divisora,* se, para um conjunto de ideais $\mathfrak{a}_i$ satisfazendo a

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \ldots .$$

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

Também se diz, conforme E. ARTIN, que se introduziu em $\mathfrak{A}$ uma *condição de máximo*. Isto significa que, num conjunto qualquer de ideais de $\mathfrak{A}$, há, pelo menos, um ideal máximo, isto é, um ideal que não está contido noutro ideal do conjunto. A equivalência das duas condições é imediata.

Os anéis com condição ascendente de cadeia designam-se por *anéis* — O (1) ou *anéis noetherianos.*

É extremamente importante a proposição seguir, que abreviadamente se exprime desta maneira: *o teorema* — O *é equivalente à condição de base de* HILBERT.

TEOREMA 14: — *É condição necessária e suficiente, para que* $\mathfrak{A}$ *seja um anel* — O, *que tenha lugar, em* $\mathfrak{A}$, *a condição de base.* A demonstração está incluída na do teorema 15, que é relativa a módulos — Ω.

Se $\mathfrak{M}$ é um módulo — Ω, a *condição ascendente para submódulos* — Ω, ou condição de máximo, introduz-se exactamente da mesma maneira que se fez para os ideais de $\mathfrak{A}$: É finita toda a cadeia de submódulos — Ω da forma $\mathfrak{N}_1 \subseteq \mathfrak{N}_2 \subseteq \mathfrak{N}_3 \subseteq \ldots$. Então, tem-se:

TEOREMA 15: — *É condição necessária e suficiente, para que valha em* $\mathfrak{M}$ *a condição de cadeia ascendente, que todo o submódulo* — Ω *tenha um número finito de geradores.* A condição é *necessária:* Se a condição de cadeia é válida, tomemos um submódulo $\mathfrak{N}$, de $\mathfrak{M}$. Supondo que $x_1 \in \mathfrak{N}$ não gera $\mathfrak{N}$, existe um segundo elemento $x_2 \in \mathfrak{N}$, não contido no submódulo (x_1), gerado por x_1. Então é $(x_1) \subset (x_1, x_2)$, se (x_1, x_2) representa o submódulo — Ω gerado por x_1 e x_2. Admitindo que é $\mathfrak{N} \neq (x_1, x_2)$, existe um elemento $x_3 \in \mathfrak{N}$ que não pertence a (x_1, x_2), podendo escrever-se $(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3)$. O raciocínio prossegue, chegando a obter-se $(x_1, \ldots, x_n) = \mathfrak{N}$, visto não poder existir uma cadeia infinita $(x_1) \subset (x_1, x_2) \subset \subset (x_1, x_2, x_3) \subset \ldots$.

A condição é *suficiente:* Admitindo que existe *condição de base para os submódulos,* isto é, que todo o submódulo tem um número finito de geradores, não pode haver cadeia infinita de submódulos — Ω, visto que o conjunto unido dos submódulos da cadeia constituiria um submódulo — Ω sem uma base finita. O teorema está, pois, demonstrado.

O facto de $\mathfrak{A}$ ser um anel-*O* leva a realizar-se a hipótese essencial do n.º 3 do § anterior, que se refere à representação normada dum ideal. Também outras noções e proposições dos n.os 2 e 3, do referido §, podem tornar-se aqui mais precisas.

TEOREMA 16: — *Num anel-*O, *todo o ideal primário é um ideal forte.*

Se $\mathfrak{d}$ é primário e b pertence ao ideal primo $\mathfrak{p}$ associado a $\mathfrak{d}$, existe um inteiro σ tal que $b^\sigma \in \mathfrak{d}$. O número σ admite um *mínimo* ρ, independente de b, como vamos ver. Admitamos, com efeito, que se tem $\mathfrak{p} = (a_1, \ldots, a_m)$ e que é $a_1^{s_1}, a_2^{s_2}, \ldots, \ldots, a_m^{s_m} \in \mathfrak{d}$. Pondo $s = \sum_{i=1}^{m} (s_i - 1) + 1$, o ideal $\mathfrak{p}^s$ é gerado por todos os produtos dos elementos a_i, $(i = 1, 2, \ldots, m)$, repetidos ou não, tais que a soma dos expoentes é igual a s. Se tomarmos um desses elementos geradores, não podem ser todos os expoentes dos seus a_i iguais ou inferiores a $s_i - 1$. Supondo que a_j figura com o expoente s_j, o elemento gerador correspondente pertence a $\mathfrak{d}$, de sorte que todos os geradores pertencerão a $\mathfrak{d}$ e será $\mathfrak{p}^s \subseteq \mathfrak{d}$. O mínimo ρ referido será $\leqq s$.

(1) Inicial da palavra alemã «*Obermenge*».

TEOREMA 17: — *Num anel* — O, *se* $\mathfrak{d}$ *é um ideal primário e* $\mathfrak{p}$ *é um ideal primo gozando das propriedades* $\mathfrak{p} \supseteq \mathfrak{d}$, $\mathfrak{p}^s \subseteq \mathfrak{d}$, $\mathfrak{p}$ *é o ideal primo associado a* $\mathfrak{d}$. Claro que $\mathfrak{p}$ pode ser o ideal primo em questão, visto que esse ideal tem as propriedades referidas. Em seguida, se $\mathfrak{q}$ fosse um ideal primo nas mesmas condições, ter-se-ia $\mathfrak{p}^s \subseteq \mathfrak{d} \subseteq \mathfrak{q}$, $\mathfrak{q}^{s'} \subseteq \mathfrak{d} \subseteq \mathfrak{p}$, de sorte que se concluiria $\mathfrak{p} \subseteq \mathfrak{q}$, $\mathfrak{q} \subseteq \mathfrak{p}$, ou seja $\mathfrak{p} = \mathfrak{q}$.

TEOREMA 18: — *Num anel* — O, *da condição* $\mathfrak{a}\,\mathfrak{a}' \subseteq \mathfrak{d}$, *supondo* $\mathfrak{d}$ *primário e* $\mathfrak{a}$ *não contido em* $\mathfrak{d}$, *tira-se* $\mathfrak{a}'^{\tau} \subseteq \mathfrak{d}$. Basta ter em conta, com efeito, que $\mathfrak{a}' \subseteq \mathfrak{p}$.

TEOREMA 19: — *Num anel* — O, *um ideal* $\mathfrak{a}$ *contém sempre um ideal produto dum certo número de ideais primos divisores de* $\mathfrak{a}$. Se $\mathfrak{a}$ é primo, o teorema é trivial. Se $\mathfrak{a}$ não é primo, existem elementos b, c, pertencentes ao anel, tais que $bc \in \mathfrak{a}$, com $b, c \notin \mathfrak{a}$. O ideal principal $(bc) = (b).(c)$ está contido em $\mathfrak{a}$. E tem-se $\mathfrak{b} = ((b), \mathfrak{a}) \supset \mathfrak{a}$, $\mathfrak{c} = ((c), \mathfrak{a}) \supset \mathfrak{a}$, $\mathfrak{b}\mathfrak{c} = ((bc), (b)\mathfrak{a}, \mathfrak{a}(c), \mathfrak{a}^2) \subseteq \mathfrak{a}$. Se o teorema enunciado é válido para $\mathfrak{b}$ e $\mathfrak{c}$, é válido para $\mathfrak{a}$. Admitir, pois, que o teorema não é válido para $\mathfrak{a}$ é admitir que não é válido para um divisor autêntico de $\mathfrak{a}$. E a repetição do raciocínio para $\mathfrak{b}$ ou $\mathfrak{c}$ e a continuação do processo levariam a contradizer a condição de cadeia ascendente. Assim, o teorema é válido para qualquer $\mathfrak{a}$.

2) **Redutibilidade dos ideais dum anel** — O — Demos no n.º 3 do § anterior a definição de ideal redutível. Um ideal diz-se *irredutível,* se não for redutível. Pode dar-se este enunciado:

TEOREMA 20: — *Todo o ideal* $\mathfrak{a}$ *dum anel* — O *é intersecção dum número finito de ideais irredutíveis.* Se $\mathfrak{a}$ é irredutível, o teorema é banal. Se $\mathfrak{a}$ é redutível, ponhamos $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$, com $\mathfrak{b} \supset \mathfrak{a}$, $\mathfrak{c} \supset \mathfrak{a}$. Se o teorema não fosse válido para $\mathfrak{a}$ não o seria para $\mathfrak{b}$ ou $\mathfrak{c}$, e um destes dois últimos ideais, pelo menos, seria redutível e permitiria continuar o processo, por forma a contradizer a condição de cadeia ascendente.

O notável resultado de E. NOETHER, segundo o qual todo o ideal dum anel — O tem uma representação normada, é agora consequência imediata desta proposição:

TEOREMA 21: — *Num anel* — O, *todo o ideal irredutível é primário.* Se o ideal irredutível $\mathfrak{a}$ não fosse primário, seria possível encontrar dois elementos f, g pertencentes ao anel $\mathfrak{A}$ (em causa), tais que $fg \in \mathfrak{a}$, com $f \notin \mathfrak{a}$ e $g^{\sigma} \notin \mathfrak{a}$, qualquer que fosse o inteiro σ. O ideal $(\mathfrak{a}, f)$, gerado por $\mathfrak{a}$ e f, seria um divisor autêntico de $\mathfrak{a}$, e o mesmo se diria do ideal $(\mathfrak{a}, \mathfrak{A}\, g^h)$, com h inteiro. Mas, sendo $\mathfrak{A}$ um anel — O, os ideais $\mathfrak{a} : g$, $\mathfrak{a} : g^2$, etc. que estão nas relações $\mathfrak{a} : g \subseteq \mathfrak{a} : g^2 \subseteq \ldots \subseteq \mathfrak{a} : g^h \subseteq \ldots$, constituem uma cadeia finita, dando, para um certo h, $\mathfrak{a} : g^h = \mathfrak{a} : g^{h+1}$. Vamos ver, então, que os dois divisores autênticos de $\mathfrak{a}$, há pouco referidos, teriam uma intersecção igual a $\mathfrak{a}$, contra a hipótese de $\mathfrak{a}$ ser irredutível. Um elemento d da intersecção teria simultâneamente as formas $d = a + r\, g^h = a' + s f + m f$, com $a, a' \in \mathfrak{a}$; $r, s \in \mathfrak{A}$; e m inteiro. Concluíam-se as relações

$$d\, g = a\, g + r\, g^{h+1} = a' g + s f g + m f g .$$

Como $fg \in \mathfrak{a}$, a última expressão pertence a $\mathfrak{a}$ e será $s' g + r\, g^{h+1} \in \mathfrak{a}$. O elemento $d\, g - a\, g = r\, g^{h+1}$ também pertence a $\mathfrak{a}$. A igualdade $\mathfrak{a} : g^h = \mathfrak{a} : g^{h+1}$ mostra que o elemento $r \in \mathfrak{a} : g^{h+1}$ pertence a $\mathfrak{a} : g^h$, pelo que $r\, g^h \in \mathfrak{a}$. O elemento d de que se partiu, tendo a forma $d = a + r\, g^h$ é, portanto, um elemento de $\mathfrak{a}$. O teorema está provado. E podemos fixar:

TEOREMA 22: — *Num anel-*O, *todo o ideal admite uma representação normada.*

Num corpo $\mathfrak{K}$ é válida a condição de base, que será, pois, válida no domínio de integridade $\mathfrak{K}[x_1, \ldots, x_n]$. Este domínio é um anel-O, e o teorema de LASKER do n.º 3, do § anterior, fica estabelecido.

A representação normada de E. NOETHER verifica dois teoremas de univocidade a que nos vamos referir. Antes de darmos os respectivos enunciados, é conveniente, porém, fazer duas observações de que carecemos para a sua demonstração.

OBSERVAÇÕES: — 1.ª) Se $\mathfrak{s}$ é um ideal primário e $\mathfrak{p}$ o ideal primo associado, sabemos que a condição $\mathfrak{b}\,\mathfrak{b}' \subseteq \mathfrak{s}$, com $\mathfrak{b}'$ não contido em $\mathfrak{p}$, arrasta $\mathfrak{b} \subseteq \mathfrak{s}$. Por consequência, é, então, $\mathfrak{s} : \mathfrak{b}' = \mathfrak{s}$, visto que, tendo-se $(\mathfrak{s} : \mathfrak{b}').\mathfrak{b}' \subseteq \mathfrak{s}$, se conclui $\mathfrak{s} : \mathfrak{b}' \subseteq \mathfrak{s}$.

2.ª) Da definição de cociente de ideais resulta a igualdade $(\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_s) : \mathfrak{a}' = (\mathfrak{a}_1 : \mathfrak{a}') \cap \ldots \cap (\mathfrak{a}_s : \mathfrak{a}')$, como pode ver-se do modo a seguir: Se $\alpha' \in \mathfrak{a}'$ e α é tal que $\alpha\alpha' \in \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_s$, tem-se $\alpha\alpha' \in \mathfrak{a}_i$, $(i = 1, 2, \ldots, s)$, e, portanto, $\alpha \in \mathfrak{a}_i : \mathfrak{a}'$. Inversamente, se $\alpha \in \mathfrak{a}_i : \mathfrak{a}'$, qualquer que seja i, tem-se $\alpha\alpha' \in \mathfrak{a}_i$, de sorte que $\beta = \alpha\alpha' \in \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_s$, e, portanto, $\alpha \in (\mathfrak{a}_1 \cap \ldots \ldots \cap \mathfrak{a}_s) : \mathfrak{a}'$.

TEOREMA 23 (1.º teorema da univocidade): — *Dadas duas decomposições normadas* $\mathfrak{a} = \mathfrak{s}_1 \cap \ldots \cap \mathfrak{s}_r$, $\mathfrak{a} = \mathfrak{s}'_1 \cap \ldots \cap \mathfrak{s}'_s$, *tem-se* $r = s$ *e os conjuntos dos ideais primos associados aos* $\mathfrak{s}_j$ *e aos* $\mathfrak{s}'_h$ *são os mesmos.* Designemos por $\mathfrak{p}'_i$ o ideal primo associado a $\mathfrak{s}'_i$, na segunda decomposição normada. Vamos provar que, para qualquer $\mathfrak{p}_j$, há um divisor entre os $\mathfrak{p}'_i$ e inversamente. Seja $\mathfrak{p}_r$, por ex., um ideal máximo entre os $\mathfrak{p}_j$ e suponhamos que não tem divisor entre os $\mathfrak{p}'_i$. Será $\mathfrak{s}'_i : \mathfrak{s}_r = \mathfrak{s}'_i$, $(i = 1, 2, \ldots, s)$, visto que $\mathfrak{s}_r$ não poderá estar contido em qualquer $\mathfrak{p}'_i$. E virá $\mathfrak{a} : \mathfrak{s}_r = (\mathfrak{s}_1 : \mathfrak{s}_r) \cap \ldots \cap (\mathfrak{s}_{r-1} : \mathfrak{s}_r) = (\mathfrak{s}'_1 : \mathfrak{s}_r) \cap \ldots \cap (\mathfrak{s}'_s : \mathfrak{s}_r) = \mathfrak{s}'_1 \cap \ldots \cap \mathfrak{s}'_s = \mathfrak{a}$. Como seria também $(\mathfrak{s}_j : \mathfrak{s}_r) = \mathfrak{s}_j$, $(j = 1, \ldots, r-1)$, ainda pela razão de se ter $\mathfrak{s}_r$ não contido em $\mathfrak{p}_j$, que resulta de ser normada a 1.ª representação de $\mathfrak{a}$ e de ser $\mathfrak{p}_r$ um máximo entre os $\mathfrak{p}_j$, valeriam as igualdades $\mathfrak{a} : \mathfrak{s}_r = \mathfrak{a} = \mathfrak{s}_1 \cap \ldots \cap \mathfrak{s}_{r-1}$, que mostrariam ser $\mathfrak{s}_r$ um ideal supérfluo na representação de $\mathfrak{a}$, contra a hipótese de a mesma ser normada.

O mesmo raciocínio prova que um máximo dos $\mathfrak{p}'_i$ está contido num dos $\mathfrak{p}_j$, de sorte que tem lugar a afirmação acima feita, no que toca aos máximos em questão. Se $\mathfrak{m}$ é agora um ideal máximo entre os $\mathfrak{p}_j$ e os $\mathfrak{p}'_i$, $\mathfrak{m}$ pertence tanto aos $\mathfrak{p}_j$ como

aos $\mathfrak{p}'_i$. Suponhamos, assim, $\mathfrak{p}_r = \mathfrak{p}'_s$. Se pomos $\mathfrak{s} = \mathfrak{s}_r \cap \mathfrak{s}'_s$, tem-se, pelo facto de ser $\mathfrak{s}_r : \mathfrak{s} = \mathfrak{s}'_s : \mathfrak{s} = \mathfrak{A}$,

$$\mathfrak{a}_1 = \mathfrak{a} : \mathfrak{s} = (\mathfrak{s}_1 : \mathfrak{s}) \cap \ldots \cap (\mathfrak{s}_{r-1} : \mathfrak{s}) = (\mathfrak{s}'_1 : \mathfrak{s}) \cap \ldots \cap (\mathfrak{s}'_{s-1} : \mathfrak{s}).$$

Um ideal primo divisor de $\mathfrak{s}$ conterá, necessàriamente, $\mathfrak{p}_r = \mathfrak{p}'_s$, de modo que não poderá ser nenhum dos restantes $\mathfrak{p}_j$ ou $\mathfrak{p}'_i$. Por isso, tem-se

$$\mathfrak{a}_1 = \mathfrak{s}_1 \cap \ldots \cap \mathfrak{s}_{r-1} = \mathfrak{s}'_1 \cap \ldots \cap \mathfrak{s}'_{s-1}.$$

Aplicando a $\mathfrak{a}_1$ as considerações que foram aplicadas a $\mathfrak{a}$ e prosseguindo, chega-se a concluir que, de facto, cada ideal $\mathfrak{p}_j$ figura entre os $\mathfrak{p}'_i$, e inversamente. Os números r e s serão iguais e o 1.º teorema da univocidade é válido.

TEOREMA 24 (2.º teorema da univocidade): — *Dadas duas decomposições normadas, como as do teorema anterior, os* $\mathfrak{s}_j$ *e os* $\mathfrak{s}'_i$ *podem ser ordenados por forma que* $\mathfrak{s}_i$ *e* $\mathfrak{s}'_i$ *estejam associados ao mesmo ideal primo* $\mathfrak{p}_i$, *tendo-se* $\mathfrak{s}_i = \mathfrak{s}'_i$, *sempre que* $\mathfrak{p}_i$ *é ideal primo mínimo divisor de* $\mathfrak{a}$. A afirmação relativa à ordem dos ideais das decomposições é trivial, à face do teorema anterior e da definição de representação normada. Admitindo, em seguida, que $\mathfrak{p}_1 = \mathfrak{p}'_1$ é ideal divisor mínimo de $\mathfrak{a}$, ponhamos

$$\mathfrak{a}' = \mathfrak{s}_2 \cap \ldots \cap \mathfrak{s}_r \cap \mathfrak{s}'_2 \cap \ldots \cap \mathfrak{s}'_r.$$

Não pode ter-se $\mathfrak{a}' \subseteq \mathfrak{p}_1$, pois que, de contrário, $\mathfrak{p}_1$ conteria um dos outros $\mathfrak{p}_i$ e não seria ideal divisor mínimo de $\mathfrak{a}$. Nessas condições, é $\mathfrak{s}_1 : \mathfrak{a}' = \mathfrak{s}_1$, $\mathfrak{s}'_1 : \mathfrak{a}' = \mathfrak{s}'_1$. E, como $\mathfrak{s}_2 : \mathfrak{a}' = \mathfrak{A}$, etc., vem $\mathfrak{a} : \mathfrak{a}' = \mathfrak{s}_1 = \mathfrak{s}'_1$, como se deseja.

Os ideais $\mathfrak{p}_i$ que, conforme o 1.º teorema da univocidade, se fazem corresponder a cada ideal $\mathfrak{a}$, dizem-se *ideais primos associados ao ideal* $\mathfrak{a}$. Se considerarmos, em particular, os $\mathfrak{p}_h$ que são divisores primos mínimos de $\mathfrak{a}$, chamaremos *componentes primárias isoladas de* $\mathfrak{a}$ os ideais $\mathfrak{s}_h$ de associados $\mathfrak{p}_h$.

Em complemento das considerações que seguiram o teorema 8, do n.º 3, do § 1, podemos afirmar que os zeros do ideal $\mathfrak{a}$, de $\mathfrak{K}[x_1, \ldots, x_n]$, estão contidos nas multiplicidades irredutíveis definidas pelas componentes primárias isoladas de $\mathfrak{a}$.

3). **Sobre as multiplicidades algébricas** — É interessante resumir neste momento as considerações geométricas do Capítulo, deixando-lhe, mesmo, um pouco mais de generalidade.

Seja $\mathfrak{K}$ um corpo qualquer e designemos por $\mathfrak{L}$ uma extensão de $\mathfrak{K}$. Chamaremos *pontos* do espaço $\mathfrak{R}_n$ um sistema de elementos $(\xi_1, \ldots, \xi_n)$, tais que $\xi_i \in \mathfrak{L}$. Os elementos ξ_i são as *coordenadas* do ponto. Um conjunto de pontos de $\mathfrak{R}_n$ diz-se uma *multiplicidade algébrica* $\mathfrak{M}$, se as coordenadas de todos os pontos do conjunto satisfizerem a um sistema de equações da forma

$$f_1(x_1, \ldots, x_n) = o, \qquad f_r(x_1, \ldots, x_n) = o,$$

onde $f_1, \ldots, f_r \in \mathfrak{K}[x_1, \ldots, x_n]$, e se todos os pontos em tais condições pertencerem ao conjunto. Todos os elementos do ideal $\mathfrak{a} = (f_1, \ldots, f_r)$ admitem os pontos de $\mathfrak{M}$ como seus zeros. Inversamente, um zero do ideal $\mathfrak{a}$ pertence a $\mathfrak{M}$, pois é zero de cada um dos f_i.

Visto que $\mathfrak{K}[x_1, \ldots, x_n]$ é um anel — O, podemos dizer que uma multiplicidade algébrica é sempre o conjunto de todos os pontos que são zeros dum ideal. Não podemos, evidentemente, afirmar que não possa a multiplicidade ser definida por outro sistema de equações e que não possa, pois, haver outros ideais cujos zeros constituam/um ideal, mas os zeros deste ideal definem geralmente um conjunto que contém aquele como subconjunto autêntico.

No caso de $\mathfrak{C}$ ser uma multiplicidade algébrica $\mathfrak{M}$, aquela totalidade de polinómios define o *ideal* $\mathfrak{a}_{\mathfrak{M}}$ *associado à multiplicidade,* ideal cujos zeros constituem, precisamente, o conjunto $\mathfrak{C}$.

Se os ideais $\mathfrak{a}$ e $\mathfrak{b}$ admitem as bases $(P_1, \ldots, P_r)$ e $(Q_1, \ldots, Q_s)$, respectivamente, o ideal $(\mathfrak{a}, \mathfrak{b})$ admite a base $(P_1, \ldots, P_r, Q_1, \ldots, Q_s)$. A multiplicidade definida pela soma $(\mathfrak{a}, \mathfrak{b})$ é, assim, constituída por todos os pontos de $\mathfrak{R}_n$ que pertencem

a multiplicidade. Qualquer que seja o conjunto $\mathfrak{L}$ dos pontos de $\mathfrak{R}_n$, a totalidade dos polinómios que admitem todos aqueles pontos como zeros constitui um ideal

simultâneamente às multiplicidades $\mathfrak{M}$ e $\mathfrak{N}$, respectivamente definidas por $\mathfrak{a}$ e $\mathfrak{b}$. O ideal $\mathfrak{a}\mathfrak{b}$ admite a base $(P_1 Q_1, \ldots, P_i Q_k, \ldots)$. Vamos ver que a multiplicidade correspondente é o conjunto unido (união) dos pontos de $\mathfrak{M}$ e de $\mathfrak{N}$. Os elementos base do produto definem uma multiplicidade que contém o conjunto unido. Inversamente, se um ponto não pertence ao conjunto unido, existem polinómios $P \in \mathfrak{a}$, $Q \in \mathfrak{b}$ que não admitem aquele ponto como zero, o qual não pode anular todos os P_j e todos os Q_k, e, portanto todos os $P_i Q_k$. O ponto não pertence à multiplicidade definida por $\mathfrak{a}\mathfrak{b}$.

Tomemos ainda o ideal $\mathfrak{a} \cap \mathfrak{b}$. Sendo $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$, a multiplicidade definida por este último ideal está contida no conjunto unido. Por outro lado, um ponto do conjunto unido, anulando todos os P_i (ou todos os Q_k), anula, em particular, todos os polinómios de $\mathfrak{a}$ que pertencem a $\mathfrak{b}$. Por aqui se vê, mais uma vez, que uma dada multiplicidade, definida pelos zeros dum certo ideal, constitui, geralmente, um conjunto de zeros doutro ideal.

Na terminologia aqui utilizada, uma multiplicidade algébrica $\mathfrak{M}$ é irredutível, se o ideal $\mathfrak{p}$ que lhe está associado é primo. Nesse caso, $\mathfrak{M}$ nunca é o conjunto unido de duas submultiplicidades autênticas, $\mathfrak{M}_1$ e $\mathfrak{M}_2$, pois que, se a estas últimas estão associados os ideais $\mathfrak{a}_1$ e $\mathfrak{a}_2$, poderíamos encontrar dois polinómios $P_1 \in \mathfrak{a}_1$, $P_2 \in \mathfrak{a}_2$, que não eram anulados por todos os pontos de $\mathfrak{M}$, e para os quais $P_1 P_2 \in \mathfrak{p}$, sendo $P_1 \notin \mathfrak{p}$, $P_2 \notin \mathfrak{p}$. Inversamente, se $\mathfrak{M}$ não é um conjunto de duas sub-multiplicidades algébricas autênticas, o ideal $\mathfrak{p}$ correspondente é primo, como vamos ver. Se existisse um produto PQ de dois polinómios que admitisse todos os pontos de $\mathfrak{M}$ como zeros, sem que P ou Q estivessem nessas condições, bastaria considerar $\mathfrak{M}_1$ como o conjunto dos pontos de $\mathfrak{M}$ que fossem zeros de P e $\mathfrak{M}_2$ como o conjunto dos pontos de $\mathfrak{M}$ que fossem zeros de Q, para se terem duas multiplicidades algébricas cujo conjunto unido daria $\mathfrak{M}$.

Do importante teorema 4, do n.º 2, do § 1, a primeira parte encontra-se completamente esclarecida. A demonstração da segunda parte pode fazer-se a partir do teorema dos zeros de

HILBERT (teor. 11, n.º 3, § 1), seguindo-se a via inversa da que se indicou no referido §, visto que ali se deu aquele teorema dos zeros depois do teorema 4. É dessa maneira que vamos proceder agora. O enunciado preciso de HILBERT é este:

TEOREMA 25: — *Sejam dadas* m *funções racionais inteiras homogéneas* $f_1, \ldots, f_m$, *de* n *variáveis* $x_1, \ldots, x_n$, *e sejam* $F_1 \ldots$, $F_k, \ldots$ *funções racionais inteiras homogéneas das mesmas variáveis, que se anulam para todos os zeros dos* f_i; *é possível determinar um inteiro* r *tal que o produto* $\Pi^{(r)}$, *de* r *quaisquer* F_j, *tem a forma* $\Pi^{(r)} = a_1 f_1 + \ldots + a_m f_m$, *onde* $a_1, \ldots, a_m$ *são funções racionais inteiras homogéneas dos* x_i. No caso dos F_j serem em número finito s, este teorema resulta fàcilmente do teorema dos zeros em causa, de que repetimos o enunciado: se o polinómio P se anula para todos os zeros do ideal $\mathfrak{a}$, tem-se $P^\sigma \in \mathfrak{a}$, para um valor conveniente do inteiro σ. Na verdade, ponhamos $\mathfrak{a} = (f_1, \ldots, f_m)$. Vale, por hipótese, para $j = 1, 2, \ldots s$, $F_j^{\sigma_j} \in \mathfrak{a}$. Se pomos $r = (\sigma_1 - 1) + \ldots + (\sigma_s - 1) + 1$, um produto qualquer de r funções F_j (diferentes ou não) é da forma $F_{i_1} \ldots F_{i_r}$. Se as diferentes funções $F_1, \ldots, F_s$, que no produto figuram (uma vez posto o mesmo como produto de potências dos F_j), tiverem expoentes todos inferiores a $\sigma_1, \ldots, \sigma_s$, o número de factores não pode ser r. Haverá, assim, para um dos F_j, um expoente, pelo menos, igual a σ_j, pelo que o produto pertencerá ao ideal.

Supondo, em seguida, que os F_j não são em número finito, o teorema de HILBERT, que tem no § anterior o n.º 13, permite determinar um sistema $\Phi_1, \ldots, \Phi_q$, de q formas, tomadas entre os F_j, tais que todos os F_j se exprimem do modo seguinte: $F_j = A_1 \Phi_1 + \ldots + A_q \Phi_q$. Então, como o teorema é válido para os Φ_k, é válido para os F_j. Quanto à restrição introduzida nos enunciados de HILBERT, exigindo que os coeficientes $a_1, \ldots, a_m$, $A_1, \ldots, A_q$ sejam homogéneos, resulta ela, como sabemos, de serem homogéneos tanto os F_j como os f_i.

Embora não houvesse necessidade de dar o enunciado do teorema 25, julgamos haver interesse em tê-lo feito. Passando pròpriamente ao teorema dos zeros, eis agora a demonstração, que deixa ainda um ponto em suspenso para o § seguinte.

Ponhamos $\mathfrak{a} = (f_1, \ldots, f_m)$ e consideremos o ideal

$$\mathfrak{a}_1 = (f_1, \ldots, f_m;\ u + x_{n+1} \cdot P) \in \mathfrak{K}[x_1, \ldots, x_{n+1}] = \mathfrak{K}_{(n+1)}.$$

Um zero do ideal $\mathfrak{a}_1$, como teria de anular P, daria $u = o$, o que é absurdo. *Admitamos* que o único ideal de $\mathfrak{K}_{(n+1)}$ que não tem qualquer zero é o ideal unidade. Será $\mathfrak{a}_1 = \mathfrak{K}_{(n+1)}$, resultando daqui a existência de elementos $A_1, \ldots, A_{m+1} \in \mathfrak{K}_{(n+1)}$ para os quais

$$u = A_1 f_1 + \ldots + A_m f_m + A_{m+1}(u + x_{n+1} P).$$

Substituindo a indeterminada x_{n+1} pela expressão $-u/P$, encontra-se

$$u = \sum_{i=1}^{m} A_i\left(x_1, \ldots, x_n, -\frac{u}{P}\right) f_i,$$

donde, por multiplicação de ambos os membros por uma potência conveniente de P: $P^\rho = \sum_{i=1}^{m} a_i f_i$, como se deseja.

Reduzida desta maneira a questão que nos tem preocupado, reservemos para o § próximo a análise da parte não demonstrada e voltemos ao teorema fundamental 4.

Sejam $\mathfrak{p}$ um ideal primo e $\mathfrak{M}$ a multiplicidade algébrica correspondente. Trata-se de ver que todo o polimónio P, que admite como zeros os pontos de $\mathfrak{M}$, pertence a $\mathfrak{p}$. Na verdade, sabemos que existe uma potência de P pertencente a $\mathfrak{p}$. Como $\mathfrak{p}$ é primo, conclui-se $P \in \mathfrak{p}$. Em suma, ficou estabelecida a importante proposição seguinte: *o ideal associado a uma multiplicidade irredutível é primo, e, inversamente, à multiplicidade dos zeros dum ideal primo está associado esse ideal primo.* Fixemos também:

TEOREMA 26: — *Os zeros dum ideal primário* $\mathfrak{z}$ *constituem uma multiplicidade irredutível, à qual está associado o ideal primo* $\mathfrak{p}$ *associado a* $\mathfrak{z}$.

TEOREMA 27: — *Dado um ideal* $\mathfrak{a}$, *uma multiplicidade algébrica irredutível de zeros de* $\mathfrak{a}$ *está sempre «mergulhada» numa das multiplicidades irredutíveis definidas pelas suas componentes primárias isoladas. Estas últimas correspondem às multiplicidades irredutíveis de zeros de* $\mathfrak{a}$ *que não são «mergulháveis».*

TEOREMA 28: — *A multiplicidade algébrica dos zeros de* $\mathfrak{a}$ *é o conjunto unido das suas submultiplicidades irredutíveis não «mergulháveis».*

Tendo em conta a definição de radical $\mathfrak{R}(\mathfrak{a})$, de $\mathfrak{a}$, pode ainda dizer-se:

TEOREMA 29: — *O ideal associado à multiplicidade dos zeros de* $\mathfrak{a}$ *é o radical* $\mathfrak{R}(\mathfrak{a})$.

É possível precisar ainda que, dado o radical $\mathfrak{R}(\mathfrak{a})$, existe um inteiro fixo ρ, apenas dependente de $\mathfrak{a}$, tal que, para cada $P \in \mathfrak{R}(\mathfrak{a})$, é $P^\rho \in \mathfrak{a}$. De facto, dado P, se $P^s \in \mathfrak{a}$, P^s pertence a todos os ideais primários que entram numa representação normada de $\mathfrak{a}$, e, portanto, pertence aos ideais primos associados correspondentes. Para cada um destes últimos ideais, existe um número σ, independente de P, tal que P^σ pertence ao ideal primário em causa. Se ρ é o maior dos números σ, tem-se $P^\rho \in \mathfrak{a}$, como se deseja.

§ 3 — Sobre a teoria da eliminação

1) **Posição do problema** — Na teoria da eliminação, trata-se de indagar da solubilidade dum sistema de equações algébricas com várias incógnitas e de dar processos para o cálculo das soluções. No caso particular das equações lineares, o problema foi resolvido completamente, no Cap. III, por um método especial, que aqui encontra aplicação. No que vai seguir-se, começaremos pelo caso mais simples de duas equações com uma única incógnita. Elevar-nos-emos depois até o caso geral.

Os coeficientes que figuram nas diferentes equações supõem-se pertencer a um dado corpo $\mathfrak{K}$. Quanto às soluções, podem as mesmas encontrar-se, não em $\mathfrak{K}$, mas em extensões de $\mathfrak{K}$. Na Teoria dos Corpos, a desenvolver noutro volume, falaremos da existência duma ampliação de $\mathfrak{K}$, qualquer que este seja, na qual uma equação polinomial, com coeficientes em $\mathfrak{K}$, tem sempre tantas soluções quantas indica o grau da equação. Se o corpo $\mathfrak{K}$ goza já da propriedade atribuída à referida ampliação, diz-se que $\mathfrak{K}$ é *algèbricamente fechado.*

2) **O método de Euler** — Tomemos as duas equações

$$P(x) = o, \qquad Q(x) = o, \tag{2}$$

nas quais

$$P(x) = a_o x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n ,$$
$$Q(x) = b_o x^m + b_1 x^{m-1} + \ldots + b_{m-1} x + b_m ,$$

com $a_o , b_o \neq o$. Podemos enunciar o seguinte

TEOREMA 30 (EULER): — *É condição necessária e suficiente, para que as duas equações* (2) *tenham* p *raízes comuns, que existam dois polinómios em* x, V *e* W, *de graus, respectivamente,* m — p *e* n — p, *tais que* $V(x) . P(x) = W(x) . Q(x)$. A condição é *necessária:* Representemos por $\alpha_1, \alpha_2, \ldots, \alpha_p$ as raízes comuns, que podem existir em $\mathfrak{K}$ ou numa ampliação conveniente desse corpo. Será

$$P(x) = a_o (x - \alpha_1) \ldots (x - \alpha_p) . P_1(x);$$
$$Q(x) = b_o (x - \alpha_1) \ldots (x - \alpha_p) . Q_1(x).$$

O grau de P_1 é $n - p$ e o de Q_1 é $m - p$. Como se tem $b_o P(x) Q_1(x) = a_o Q(x) P_1(x)$, vê-se que basta fazer $V(x) = b_o Q_1(x)$, $W(x) = a_o P_1(x)$, para se concluir a afirmação.

A condição é *suficiente:* Imaginemos que existem os polinómios V e W, tais que $V(x) P(x) = W(x) Q(x)$. Dividindo

V e W pelo seu m. d. c., obtêm-se os cocientes V' e W', sendo $V'(x)\,P(x) = W'(x)\,Q(x)$. Por aqui se vê que V' divide o 2.º membro; e, como é primo com W', dividirá necessàriamente $Q(x)$. Tem-se, assim, $Q(x) = V'\,S(x)$, e, portanto, $W'\,V'\,S(x) = V'\,P(x)$, ou seja $W'\,S(x) = P(x)$. Das relações simultâneas

$$P(x) = W'\,S(x), \qquad Q(x) = V'\,S(x),$$

conclui-se serem raízes comuns de $P(x)$ e de $Q(x)$ as raízes de $S(x)$. Ora o grau de $S(x)$ é fácil de avaliar. Suponhamos $n \geq m$. O grau de V' é, quando muito, $m-p$; e o grau de $S(x)$, por consequência, pelo menos igual a $m-(m-p)=p$. A proposição fica demonstrada.

O reconhecimento efectivo de soluções comuns às equações (2) vai ser feito, todavia, reconhecendo a existência de uma solução. Deverão existir V, do grau $m-1$, e W, do grau $n-1$, nas condições do teorema de EULER. Se pusermos

$$V = v_0\,x^{m-1} + v_1\,x^{m-2} + \ldots + v_{m-2}\,x + v_{m-1},$$
$$W = w_0\,x^{n-1} + w_1\,x^{n-2} + \ldots + w_{n-2}\,x + w_{n-1},$$

obtém-se a identidade

$$(a_0\,x^n + a_1\,x^{n-1} + \ldots + a_{n-1}\,x + a_n)\,.\,(v_0\,x^{m-1} + v_1 x^{m-2} + \ldots + v_{m-1}) = (b_0 x^m + b_1 x^{m-1} + \ldots + b_{m-1}\,x + b_m)\,.\,(w_0\,x^{n-1} + w_1 x^{n-2} + \ldots + w_{n-1}).$$

Efectuando os produtos em ambos os membros e igualando os coeficientes das mesmas potências de x, obtêm-se $m+n$ equações formando um sistema linear e homogéneo, a $m+n$ incógnitas. Estas últimas são os v_i e os w_j. A fim de que elas não tomem ùnicamente os valores zero, isto é, a fim de que existam,

de facto, os polinómios V e W, deverá ser nulo o determinante do referido sistema. Esse determinante, à parte uma questão de sinal, tem o aspecto seguinte:

$$\Delta = \begin{vmatrix} a_0 & a_1 & \ldots & a_{m-1} & a_m & a_{m+1} & \ldots & a_{n-1} & a_n & 0 & \ldots & 0 \\ 0 & a_0 & \ldots & a_{m-2} & a_{m-1} & a_m & \ldots & a_{n-2} & a_{n-1} & a_n & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & a_0 & a_1 & a_2 & \ldots & a_{n-m} & a_{n-m+1} & a_{n-m+2} & \ldots & a_n \\ b_0 & b_1 & \ldots & b_{m-1} & b_m & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ 0 & b_0 & \ldots & b_{m-2} & b_{m-1} & b_m & \ldots & 0 & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & b_0 & b_1 & b_2 & \ldots & b_m \end{vmatrix}.$$

Deste modo, a condição necessária e suficiente, para que o sistema (2) tenha solução, é expressa pela relação $\Delta = 0$. Δ diz-se *resultante* dos polinómios P e Q ou das equações $P=0$, $Q=0$.

Posto isto, consideremos as igualdades

$$\begin{aligned} x^{m-1}P(x) &= a_0\,x^{n+m-1} + a_1\,x^{n+m-2} + \ldots + \\ &\quad + a_{n-1}\,x^m + a_n\,x^{m-1}, \\ x^{m-2}P(x) &= a_0\,x^{n+m-2} + \ldots + \\ &\quad + a_{n-1}\,x^{m-1} + a_n\,x^{m-2}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ P(x) &= a_0\,x^n + \ldots + a_n, \\ x^{n-1}Q(x) &= b_0\,x^{n+m-1} + b_1\,x^{n+m-2} + \ldots + \\ &\quad + b_{m-1}\,x^n + b_m\,x^{n-1}, \\ x^{n-2}Q(x) &= b_0\,x^{n+m-2} + \ldots + \\ &\quad + b_{m-1}\,x^{n-1} + b_m\,x^{n-2}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ Q(x) &= b_0\,x^m + \ldots + b_m, \end{aligned}$$

e tomemos os complementos algébricos dos elementos da última coluna do determinante Δ. Multiplicando ambos os membros das igualdades anteriores, sucessivamente, por esses complementos algébricos e adicionando as resultados, obtém-se

$$A\,P(x) + B\,Q(x) = \Delta,$$

onde A e B são polinómios de $\mathfrak{K}[x]$, dos graus $m-1$ e $n-1$, respectivamente, quando muito. Assim, Δ pertence ao ideal gerado por P e Q: $\Delta \equiv o\,((P, Q))$. Se as equações (2) não têm raízes comuns, é $\Delta \neq o$, e, portanto,

$$\Delta^{-1} A\, P(x) + \Delta^{-1} B\, Q(x) = u \in \mathfrak{K},$$

conclusão que entra no teorema mais geral seguinte:

TEOREMA 31: — *Se o ideal* $\mathfrak{a} = (P_1, \ldots, P_m)$ *não tem zeros, é possível encontrar polinómios* $A_i \in \mathfrak{K}[x]$ *tais que* $\Sigma\, A_i\, P_i(x) = u$. Para fazermos a demonstração, estudemos um sistema da forma

$$P_1(x) = o, \quad \ldots, \quad P_m(x) = o, \tag{3}$$

isto é, procuremos igualmente condições necessárias e suficientes para a solubilidade do sistema.

Claramente que nos ocuparemos ùnicamente do caso em que o número de equações é efectivamente m, ou seja, não suporemos constante qualquer dos primeiros membros das equações (3).

Substituamos (3) pelo sistema seguinte

$$\begin{aligned} x^{r-r_1} P_1(x) = o, \quad \ldots, \quad x^{r-r_m} P_m(x) = o, \\ (x-u)^{r-r_1} P_1(x) = o, \quad \ldots, \quad (x-u)^{r-r_m} P_m(x) = o. \end{aligned} \tag{4}$$

Supõe-se aqui que r_i é o grau de P_i e que r é o maior dos graus dos diferentes P_i. É indiferente exprimir que (3) ou (4) têm raízes comuns. No que vai seguir-se, designaremos por $Q_1, \ldots, Q_q$ os primeiros membros de (4). Supondo $X_1, \ldots, X_q, Y_1, \ldots, Y_q$ um sistema de indeterminadas, consideremos o corpo $\mathfrak{K}(X_1, \ldots, X_q, Y_1, \ldots, Y_q) = \mathfrak{L}$ e os dois polinómios

$$\begin{aligned} S(x) &= X_1 Q_1 + \ldots + X_q Q_q, \\ T(x) &= Y_1 Q_1 + \ldots + Y_q Q_q, \end{aligned} \tag{5}$$

pertencentes a $\mathfrak{L}[x]$. Nenhum deles se reduz a uma constante. Se estes últimos polinómios têm um factor comum, tal factor

pertencerá necessàriamente a $\mathfrak{K}[x]$, e será um factor comum dos Q_j ou dos P_j. Inversamente, um factor comum destes últimos é factor comum de S e de T. Igualando a zero a resultante Δ dos polinómios (5), obtém-se uma condição necessária e suficiente para que as equações (3) tenham uma solução comum. Como Δ é um polinómio nos X, Y, com coeficientes de $\mathfrak{K}$, ordenando Δ segundo as potências daquelas indeterminadas, a condição $\Delta = o$ parte-se em f condições

$$\Delta_1 = o, \quad \ldots, \quad \Delta_f = o,$$

a que devem satisfazer os coeficientes de (3). E, tendo-se,

$$\Delta = A\, S(x) + B\, T(x), \qquad (A, B \in \mathfrak{L}[x]),$$

vê-se que é, sucessivamente,

$$\begin{aligned} &\Delta \in (Q_1, \ldots, Q_q) = \text{ideal de } \mathfrak{L}[x], \\ &\Delta \in (P_1, \ldots, P_m) = \text{ideal de } \mathfrak{L}[x], \\ &\Delta = \alpha_1 \Delta_1 + \ldots + \alpha_f \Delta_f = \beta_1 P_1 + \ldots + \beta_m P_m, \end{aligned}$$

onde os α_i pertencem a $\mathfrak{L}$ e os β_j pertencem a $\mathfrak{L}[x]$. Por consequência, ordenando a expressão $\Sigma\, \beta_h P_h$ segundo os X_i e os Y_j, conclui-se $(\Delta_1, \ldots, \Delta_f) \equiv o\ (P_1, \ldots, P_m)$, onde, agora, $(P_1, \ldots, P_m)$ é ideal de $\mathfrak{K}[x]$.

Se as equações (3) não têm soluções comuns, um dos Δ_h é uma constante não nula de $\mathfrak{K}$, e a relação

$$\Delta_h = a_1 P_1 + \ldots + a_m P_m, \qquad (a_i \in \mathfrak{K}[x]);$$

leva à igualdade desejada

$$\sum_{i=1}^{m} a_i \Delta_h^{-1} P_i = u \in \mathfrak{K}, \qquad (A_i = a_i \Delta_h^{-1}).$$

O conjunto dos Δ_h diz-se *sistema resultante* dos polinómios P_i.

3) **Os sistemas de equações algébricas com n incógnitas.** — O sistema mais geral que consideraremos é da forma

$$P_1(x_1, \ldots, x_n) = o, \quad \ldots, \quad P_m(x_1, \ldots, x_n) = o, \quad (6)$$

supostos os P_i pertencentes a $\mathfrak{R}[x_1, \ldots, x_n]$. Também, para um tal sistema, provaremos este

TEOREMA 32: — *Se o ideal* $\mathfrak{a} = (P_1, \ldots, P_m)$ *não tem zeros, é possível encontrar polinómios* $A_i \in \mathfrak{R}[x_1, \ldots, x_n]$ *tais que* $\sum_{i=1}^{m} A_i P_i(x_1, \ldots, x_n) = u$. Com a justificação deste enunciado completar-se-á a demonstração do teorema dos zeros de HILBERT, pois que o ponto deixado em suspenso fica completamente levantado.

Partamos de (6). Suponhamos que todas as equações contêem um termo de grau máximo com uma única variável, x_n, por ex.. A eliminação de x_n entre as equações (6) leva a um sistema

$$\Delta_1 = o, \quad \ldots, \quad \Delta_f = o, \quad (7)$$

no qual figuram $x_1, \ldots, x_{n-1}$. Estas quantidades interpretam-se como elementos indeterminados duma ampliação de $\mathfrak{R}$, que terão de satisfazer a (7), a fim de que o sistema proposto seja solúvel. Se as equações (6) não têm soluções comuns, o sistema (7) é impossível, de sorte que, numa demonstração por indução, podem encontrar-se, por hipótese, polinómios em $x_1, \ldots, x_{n-1}$, com coeficientes em $\mathfrak{R}$, tais que

$$\sum_{i=1}^{f} A_i \Delta_i = u \in \mathfrak{R}.$$

Como se tem

$$\Delta_i = \sum_{k=1}^{m} a_k P_k, \qquad (a_k \in \mathfrak{R}[x_1, \ldots, x_n]),$$

encontra-se ainda

$$\sum_{i,k} A_i a_k P_k = \sum_j B_j P_j = u,$$

como se deseja.

Resta ver a possibilidade de reduzir o caso geral de (6) ao caso em que todas as equações têm um termo de grau máximo com uma única variável. Façamos em (6) a mudança de variáveis

$$x_1 = X_1 x_1', \; x_2 = x_2' + X_2 x_1', \; \ldots, \; x_n = x_n' + X_n x_1', \quad (8)$$

onde $X_1, \ldots, X_n$ são indeterminadas. O polinómio P_1, por ex., transforma-se em

$$T_1(x_1', \ldots, x_n') = P_1(X_1 x_1', \ldots, x_n' + X_n x_1') \in \\ \in \mathfrak{R}(X_1, \ldots, X_n)[x_1', \ldots, x_n'],$$

no qual se encontra um termo apenas em x_1', proveniente da parte homogénea do mais alto grau de $P_1(x_1, \ldots, x_n)$, com um coeficiente fácil de determinar. Um termo $a x_1^{r_1} \ldots x_n^{r_n}$, de grau máximo, contribui, com efeito, para o citado coeficiente, com uma parte $a X_1^{r_1} \ldots X_n^{r_n}$. A expressão homogénea em referência contribui, pois, com uma expressão da sua própria forma, mas nas indeterminadas X_i, pelo que o termo em x_1' subsiste efectivamente. O sistema transformado de (6),

$$T_1 = o, \qquad \ldots, \qquad T_m = o,$$

é tal que pode escrever-se

$$\Sigma C_i T_i = u, \qquad (C_i \in \mathfrak{R}(X_1, \ldots, X_n)[x_1', \ldots, x_n'].$$

Regressando às variáveis x_j, os T_i reproduzem os P_i enquanto — que os C_i se tornam em polinómios ainda com coeficientes em $\mathfrak{R}(X_1, \ldots, X_n)$. Supondo que se obtém $\Sigma D_i P_i = u$, mul-

tiplicando ambos os membros por uma expressão conveniente nos X_i, tira-se

$$\Sigma F_i P_i = G, \qquad (G \in \Re(X_1 \ldots, X_n)).$$

Ordenando ambos os membros desta igualdade segundo as potências dos X_i, os coeficientes do 1.º membro são combinações lineares dos polinómios P_i, com coeficientes em $\Re$. Das igualdades dos coeficientes dos dois membros, visto que G não é idênticamente nulo, conclui-se

$$\Sigma \beta_i P_i = a \in \Re, \qquad (\beta_i \in \Re[x_1, \ldots, x_n])$$

ou seja, como se pretende,

$$\Sigma a^{-1} \beta_i P_i = u.$$

BIBLIOGRAFIA

D. Hilbert — *Gesammelte Abhandlungen*, tomo II;

B. L. van der Waerden — *Moderne Algebra*, tomo 2.º, 1931;

W. Krull — *Idealtheorie*, «Ergebnisse der Mathematik und ihrer Grenzgebiete», Berlim, 1935;

A. Almeida Costa — *Elementos da Teoria dos Anéis*, Porto, 1943;

Arnaldo Madureira — *Álgebra superior e Geometria analítica*, tomo 1, Porto, 1948;

J. Vicente Gonçalves — *Álgebra Superior*, 2.º vol., Lisboa, 1950;

A. Almeida Costa — *Para a história dos domínios multiplicativos associativos*, Actas do XXI Congresso da Associação Espanhola para o Progresso das Ciências, Málaga, 1951;

N. Jacobson — *Lectures in Abstract Algebra*, 1951.

ÍNDICE DE AUTORES E TERMOS

CORRECÇÕES

Página	*Linha*	*Onde se lê*	*Leia-se*
21	6	a_{n+h-1}	a_{n+k-1}
53	1	intransitivo	transitivo
60	17	*corpos*	*corpo—s*
65	3 * (1)	Quando	Quanto
76	7	*geral*	*gerado*
81	9 *	6)	7)
82	16 *	7)	8)
93	1 *	$P = DQ$	$P = DQ + R$
98	11	$\Im(p)$	$\Im/(p)$
101	6	$= \psi(x) . q(x)$	$= \varphi(x) . q(x)$
116	8	p vectores	p vectores independentes
116	13	$m + p$	m
149	16	n	m
173	4 *	$ab + \bar{o}$	$ab + \mathfrak{p} = \bar{o}$
173	4 *	$ab = \mathfrak{p}$	$ab \in \mathfrak{p}$

Em todo o livro, os sinais $\subset$ e $\supset$ significam, respectivamente, «contido» e «contendo», no sentido próprio. Os sinais $\subseteq$ e $\supseteq$ significam, simplesmente, «contido» e «contendo».

---

(1) O asterisco (*) indica que as linhas devem ser contadas a partir do fim da página.

ÍNDICE

CAPÍTULO II

ANÉIS

CAPÍTULO III

ESPAÇO LINEAR