CENTRO DE ESTUDOS DE MATEMÁTICA

SÔBRE OS GRUPOS ABELIANOS

POR

ALMEIDA COSTA

FACULDADE DE CIÊNCIAS DO PÔRTO

1942

PUBLICAÇÕES DO

CENTRO DE ESTUDOS DE MATEMÁTICA

N.º 4

SUBSIDIADA PELO "INSTITUTO PARA A ALTA CULTURA"

ANAIS DA FACULDADE DE CIÊNCIAS DO PORTO

Fundados por F. GOMES TEIXEIRA
e continuados sob a direcção de A. MENDES CORRÊA

Extracto do tômo XXVII.

SÔBRE OS GRUPOS ABELIANOS

POR

A. ALMEIDA COSTA

Prof. ext. da Universidade do Pôrto

PÔRTO
Imprensa Portuguesa
108, Rua Formosa, 116

1942

SÔBRE OS GRUPOS ABELIANOS

POR

A. Almeida Costa

Prof. ext. da Universidade do Pôrto

Em tudo o que vai seguir-se, tratar-se-ão, apenas, grupos abelianos com um número finito de elementos geradores e com domínio operatório constituído por anel com elemento um. É nosso objectivo fazer um certo número de observações preliminares (secção *A*) e indagar de certos casos para os quais é possível indicar uma *base* com uma *ordem* ou *dimensionalidade* invariante (secções *B* e *C*). Na secção *D*, para comodidade do leitor, reproduz-se uma demonstração dum teorema fundamental. Finalmente, na secção *E*, verifica-se que uma noção de *produto directo*, dada por M. Wedderburn na memória «*On hypercomplex numbers*», publicada nos *Proceedings of the London Mathematical Society*, second series, volume 6, 1908, cai dentro da idéia de grupo abeliano com domínio operatório anular com elemento um.

Deve-se a W. Krull a noção de grupo com operadores, para o caso comutativo. Os resultados dêste autor, com a intervenção dêste novo conceito, foram publicados na memória insêrta na *Mathematische Zeitschrift*, Band 23, 1925, pág. 161, aob a designação «*Über verallgemeinerte endliche Abelsche Gruppe*». O. Schmidt introduziu a noção de operador num grupo qualquer, publicando a tal respeito um artigo naquela citada revista alemã (Band 29, 1929, pág. 34) intitulado «*Über unendliche Gruppen mit endlicher Kette*». Nos livros modernos, esta noção é hoje corrente. A êsse respeito podem consultar-se o nosso Curso sôbre «*Elementos da Teoria dos Grupos*» ou o livro «*Moderne Algebra* de B. L. van der Waerden. É cheio de ensinamentos o livro «*Lehrbuch der Gruppentheorie*», de H. Zassenhaus (Teubner, Berlin).

Dum modo geral, para o conteúdo dêste trabalho, o leitor poderá comparar o que aqui se escreve com a expo-

sição feita sôbre o assunto no tômo 2.º da obra citada de VAN DER WAERDEN ou com a do autor dada no livro «*Grupos abelianos e Aneis e ideais não comutativos*».

A

1) **O elemento um como operador** — Seja o grupo

$$\mathfrak{G} = \{\varepsilon, \alpha, \beta, \gamma, \ldots\},$$

onde ε é o elemento unidade, e seja o anel operatório

$$\mathfrak{S} = \{u, a, b, c, \ldots\},$$

no qual u é o elemento um. Como se sabe, têm lugar as relações

$$\begin{aligned} &\alpha^a \in \mathfrak{G}, \text{ (1)} \qquad (\alpha\beta)^a = \alpha^a . \beta^a , \\ &\alpha^{a+b} = \alpha^a . \alpha^b , \qquad \alpha^{ab} = (\alpha^a)^b . \end{aligned} \tag{1}$$

Delas se deduzem as igualdades

$$\varepsilon^a = \varepsilon, \quad (\alpha^{-1})^a = (\alpha^a)^{-1}, \quad \alpha^0 = \varepsilon, \quad \alpha^{-a} = (\alpha^a)^{-1} = (\alpha^{-1})^a .$$

Nada nos permite afirmar, porém, que o elemento u seja *operador unitário*, isto é que se tenha

$$\alpha^u = \alpha.$$

Escrevendo

$$\alpha = \alpha\ \alpha^{-u} . \alpha^u ,$$

cada elemento de $\mathfrak{G}$ se pode considerar como produto de dois, o primeiro dos quais, $\beta = \alpha\ \alpha^{-u}$, satisfaz a condição $\beta^a = \varepsilon$, qualquer que seja $a \in \mathfrak{S}$, e o segundo, $\gamma = \alpha^u$, admite u como operador unitário. O conjunto dos elementos β constitue um sub-grupo admissível $\mathfrak{G}'$, o conjunto dos γ um sub-grupo admissível $\mathfrak{G}''$, valendo a igualdade

$$\mathfrak{G} = \mathfrak{G}' \times \mathfrak{G}'',$$

em cujo segundo membro figura um produto directo.

(1) Com $\in$ significamos «pertence» ou «pertencente».

Suponhamos que $\mathfrak{G}$ é um *grupo finito* relativo a $\mathfrak{S}$. Isto significa que existem elementos $v_1, \ldots, v_n$ de $\mathfrak{G}$, tais que, para qualquer $v \in \mathfrak{G}$, se pode escrever

$$v = v_1^{a_1} \ldots v_n^{a_n} \qquad (a_i \in \mathfrak{G}),$$

salvo os elementos da forma

$$v' = v_1^{i_1} \ldots v_n^{i_n},$$

onde $i_1, \ldots, i_n$ pertencem ao anel dos números inteiros.

Procuremos, neste caso, o sub-grupo $\mathfrak{G}'$. Os seus elementos são de uma das formas

$$\begin{aligned} &v_1^{a_1} \ldots v_n^{a_n} . v_1^{-a_1 u} \ldots v_n^{-a_n u}, \\ &v_1^{i_1} \ldots v_n^{i_n} . v^{-i_1 u} \ldots v_n^{-i_n u}. \end{aligned} \tag{2}$$

Os primeiros são todos iguais a ε. Como, para i_1 igual a zero, é também $v_1^{i_1} = \varepsilon$, podemos dizer que $\mathfrak{G}'$ se compõe ùnicamente dos elementos com o aspecto (2).

O sub-grupo $\mathfrak{G}''$ compõe-se, então, dos elementos

$$\begin{aligned} &\alpha = v_1^{a_1 u} \ldots v_n^{a_n u} = v_1^{a_1} \ldots v_n^{a_n}, \\ &\beta = v_1^{i_1 u} \ldots v_n^{i_n u} = v_1^{b_1} \ldots v_n^{b_n}, \quad (b_i \in \mathfrak{S}), \end{aligned}$$

ou seja $\mathfrak{G}''$ compõe-se dos elementos da forma

$$v = v_1^{a_1} \ldots v_n^{a_n}, \tag{3}$$

para os quais u é sempre operador unitário.

Quando se diz, pois, que o grupo $\mathfrak{G}$ é formado por elementos do tipo (3), o carácter unitário do operador u tem de ser concebido. Os elementos $v_1, \ldots, v_n$ não têm a forma (3), não pertencendo a $\mathfrak{G}$. Os geradores são os elementos

$$v_1^u, \ldots, v_n^u,$$

que representaremos, de futuro, com $v_1, \ldots, v_n$.

Sempre que uma relação da forma

$$v_1^{a_1} \ldots v_n^{a_n} = \varepsilon$$

apenas tem lugar se $a_1 = \ldots = a_n = 0$, os elementos $v_1, \ldots, v_n$ dizem-se *independentes*. O seu número é a *ordem* ou *dimensionalidade* de $\mathfrak{G}$.

Se o grupo $\mathfrak{G}$ admitisse um segundo domínio operatório Ω, os raciocínios anteriores poderiam estender-se a um tal caso, mediante restrições simples. Tornava-se necessário, em primeiro lugar, que $\mathfrak{G}'$ e $\mathfrak{G}''$ fôssem admissíveis em face de Ω. Isso exigiria que se tivesse, por ex., para $\rho \in \Omega$,

$$(\alpha\,\alpha^{-u})^\rho = \alpha^\rho\,(\alpha^{-u})^\rho = \alpha^\rho\,(\alpha^\rho)^{-u}.$$

Esta circunstância seria, então, suposta, pois pôr-se-ia, dum modo geral,

$$(\alpha^a)^\rho = (\alpha^\rho)^a.$$

Como são de especial interêsse os grupos com uma dimensionalidade finita n, o grupo $\mathfrak{G}$, representando com $\mathfrak{S}\,v_i$ o conjunto dos elementos da forma v_i^a, poderia continuar a escrever-se

$$\mathfrak{G} = \mathfrak{S}\,v_1 \times \ldots \times \mathfrak{S}\,v_n,$$

se os sub-grupos $\mathfrak{S}\,v_i$ fôssem admissíveis em face de Ω. Isso exigiria, por ex.,

$$(v_i^a)^\rho = v_i^{a^\rho}.$$

Suporíamos que os elementos de Ω operavam também sôbre $\mathfrak{S}$ (à direita) e que teria lugar a relação

$$(\alpha^a)^\rho = \alpha^{a\rho}.$$

2) **Endomorfismos de $\mathfrak{G}$** — Um *endomorfismo* Θ é uma homomorfia operatória de $\mathfrak{G}$ sôbre si mesmo. É definido por uma matriz quadrada, pondo

$$v_j^\Theta = V_j = \prod_{k=1}^{n} v_k^{a_{kj}}, \qquad (j = 1, 2, \ldots, n). \tag{4}$$

A matriz em causa é $A = (a_{kj})$.

Tem lugar a seguinte proposição: (1) *é condição necessária e suficiente para que (4) se torne num automorfismo, que A não seja um divisor nulo esquerdo no anel completo das matrizes quadradas com elementos de $\mathfrak{S}$ e que tenha um inverso direito.*

(1) Veja-se VAN DER WAERDEN, loc. cit., ou o nosso Curso sôbre *Grupos abelianos e Anéis e ideais não comutativos*. O raciocíni o do § 3.º é análogo ao empregado para estabelecer a proposição em referência

Em tal caso, de (4) tira-se

$$v_k = \prod_j V_j^{b'_{jk}}. \tag{5}$$

A matriz $B = (b_{kj})$ é a matriz inversa direita de A. Como as igualdades (5) são análogas a (4), conclui-se: *B não é divisor nulo esquerdo e tem inverso direito.* Designando êsse inverso com B', vem

$$B\,B' = U = \text{matriz unidade.}$$

Logo é

$$A\,B\,B' = A\,U = A = A\,B.\,B' = U\,B' = B'.$$

Tem-se, em resumo,

$$A\,B = B\,A = U.$$

A matriz dum automorfismo é, pois, uma matriz com inverso *(regular)*, e inversamente.

Daqui conclui-se que *A também não é divisor nulo direito e tem inverso esquerdo.* Inversamente, esta última conclusão leva às anteriores.

De facto, consideremos um grupo $\mathfrak{G}$ construído à custa dos símbolos $w_1^u, \ldots, w_n^u$, e ponhamos

$$w = w_1^{a_1} \ldots w_n^{a_n} \in \mathfrak{G}, \qquad (w^a)^b = w^{ba}. \tag{5'}$$

O endomorfismo

$$W_j = \prod_k w_k^{a_{jk}}$$

é um automorfismo, pois a proposição anterior, mediante as igualdades (5'), modifica-se precisamente substituindo «divisor nulo esquerdo» por «divisor nulo direito» e «inverso direito» por «inverso esquerdo». Dêste modo, existe uma matriz $B' = (b'_{jk})$ tal que $B'A = U_n$, sendo U_n a matriz unidade de grau n. É também $AB' = U_n$. E, sendo regular a matriz A, ela não pode ser divisor nulo esquerdo e tem inverso direito, como se deseja.

Se o anel $\mathfrak{S}$ é comutativo, é indiferente pôr

$$(\alpha^a)^b = \alpha^{ab}, \quad (\alpha^a)^b = \alpha^{ba}. \tag{6}$$

O automorfismo (4) pode definir-se adoptando a segunda relação (6) e pondo

$$v_j^{\Theta} = V_j = \prod_{k=1}^{n} v_q^{b_{jk}}$$

onde $B = (b_{jk}) = \tilde{A}$ é a matriz transposta de A.

Conclui-se que, *num anel comutativo, se* A *não é divisor nulo esquerdo e tem inverso direito, a sua matriz transposta está nas mesmas condições,* pois não tem divisor nulo direito e tem inverso esquerdo.

Seja agora $\mathfrak{S}'$ um anel isomorfo-inverso de $\mathfrak{S}$. Se $a' \in \mathfrak{S}'$ é o correspondente de $a \in \mathfrak{S}$, ponhamos, para $\alpha \in \mathfrak{G}$,

$$\alpha^{a'} = \alpha^a .$$

Nesse caso deverá ter-se

$$(\alpha^a)^b = \alpha^{ab} = \alpha^{b'a'} = (\alpha^{a'})^{b'}.$$

O nosso grupo $\mathfrak{G}$ pode considerar-se, então, como um grupo finito relativo a $\mathfrak{S}'$, sob a condição de se pôr

$$(\alpha^{a'})^{b'} = \alpha^{b'a'}.$$

Supondo que (4) define um automorfismo, substituamos as relações (4) pelas seguintes:

$$v_j^{\Theta} = V_j = \prod_{k=1}^{n} v_k^{b'_{jk}}, \tag{7}$$

onde $B' = (b'_{jk})$ é a matriz transposta de $A' = (a'_{jk})$. Vê-se imediatamente que fica definido o mesmo automorfismo.

De facto, a um elemento $\prod_j v_j^{a_j} = \prod_j v_j^{a'_j}$ corresponde, por (4), um elemento

$$v = \prod_j V_j^{a_j} = \prod_k v_k^{\sum_j a_{kj} a_j},$$

e, por (7), um elemento

$$\prod_j V_j^{a'_j} = \prod_k v_k^{\sum_j a'_j b'_{jk}} = v.$$

Dêste modo, pode concluir-se: *se num anel completo de matrizes quadradas com elementos de* $\mathfrak{S}$, *uma matriz* A *não é divisor nulo esquerdo e tem um inverso direito, no anel completo de matrizes quadradas do anel* $\mathfrak{S}'$, *isomorfo-inverso de* $\mathfrak{S}$. *a matriz transposta,* $\tilde{A}' = B'$, *da matriz* A' *formada dos elementos correspondentes aos da matriz* A, *está nas mesmas condições, pois não é divisor nulo direito e tem inverso esquerdo.*

3) **Sôbre a ordem de** $\mathfrak{G}$ — Em face de raciocínios anteriores, levanta-se a questão de indagar se é um número bem determinado a ordem de $\mathfrak{G}$. Trata-se de saber se não será possível encontrar uma base independente, $V_1, \ldots, V_m$, com $m \neq n$.

Sempre que tal é possível, tem-se

$$V_j = \prod_{k=1}^{n} v_k^{a_{kj}}, \quad (j = 1, 2, \ldots, m),$$

deduzindo-se $b_j = 0$, da relação $\prod_{j=1}^{m} V_j^{b_j} = \varepsilon$. Então, a matriz $A = (a_{kj})$, de n linhas e m colunas, deverá ser tal que, multiplicada à direita por uma matriz qualquer não nula de m linhas, não possa levar a uma matriz nula. E, sendo assim, as relações $\sum_{j=1}^{m} a_{kj} b_j = 0$ levam necessàriamente aos valores $b_j = 0$, de sorte que uma relação $\prod V_j^{c_j} = \varepsilon$ dá sempre $c_j = 0$, isto é: os V_j são independentes.

Devendo ainda, por hipótese, poderem os v_k exprimir-se nos V_j, ter-se-á

$$v_k = \prod_{j=1}^{m} V_j^{b_{jk}}, \quad (k = 1, 2, \ldots, n),$$

e, portanto, designando com B a matriz (b_{jk}):

$$A \binom{n \text{ linhas}}{m \text{ colunas}} \times B \binom{m \text{ linhas}}{n \text{ colunas}} = U_n \binom{n \text{ linhas}}{n \text{ colunas}},$$

onde U_n é a matriz unidade.

Isto significa, embora não possamos designar B como matriz inversa de A, que deve existir, dada A, uma matriz B tal que $AB = U_n$. E, sendo assim, os v_k exprimem-se

nos V_j, pois, pondo $v'_k = \prod_{j=1}^{m} V_j^{b_{jk}}$, tem-se

$$v'_k = \prod_{j=1}^{m} \left(\prod_{l=1}^{n} v_l^{a_{lj}} \right)^{b_{jk}} = \prod_{l=1}^{n} v_l^{\sum_j a_{lj}\, b_{jk}} = v_k .$$

A matriz B tem as mesmas propriedades que A: da igualdade $BC = O$, conclui-se $C = O$; e a matriz A é tal que $BA = U_m$ é a matriz unidade de grau m. Também pode demonstrar-se que não existe matriz $D \neq O$ tal que $DA = O$. De facto, o produto DA tem m colunas, de sorte que $DA.B = D.AB = D$ tem sentido, dando $D = O$.

A questão aqui posta, no caso de ser comutativo o anel $\mathfrak{S}$, leva a um resultado interessante. Formemos, com efeito, os elementos das diagonais principais de $AB = U_n$ e de $BA = U_m$. Por um lado, a sua soma é nu; por outro, é mu. Como, porém, em face da sua forma, deverá ter-se $nu = mu$, conclui-se a existência de valores inteiros finitos q tais que $qu = 0$. O problema não pode pôr-se sempre que esta condição se não dá. A condição não é, todavia, suficiente, como resulta imediatamente do caso de $\mathfrak{S}$ ser um corpo.

Suponhamos, por ex., que $\mathfrak{S}$ é um *anel ideal principal*. Sabemos que dois ideais quaisquer não nulos não podem ter como elementos comuns apenas o elemento nulo. O que acabamos de dizer leva ao mesmo resultado.

Sejam u_1, u_2 dois elementos não nulos de $\mathfrak{S}$ e sejam $r, s \in \mathfrak{S}$ elementos quaisquer de $\mathfrak{S}$. $r u_1$, $s u_2$ e $r u_1 + s u_2$ são ideais em $\mathfrak{S}$. Se d é o elemento gerador do último ideal, existem elementos $a, b, \alpha, \beta \in \mathfrak{S}$ tais que

$$\begin{array}{ll} a\,d = u_1, & \alpha u_1 + \beta u_2 = d, \\ b\,d = u_2, & \alpha a + \beta b = u. \end{array}$$

Poderá imaginar-se que ru_1 e su_2 não têm elemento comum, salvo o elemento nulo, isto é que uma igualdade como $\vartheta u_1 + \varphi u_2 = 0$, $(\vartheta, \varphi \in \mathfrak{S})$, dá $\vartheta = \varphi = 0$? Se assim fôr, teremos uma base (u_1, u_2) para o módulo $ru_1 + su_2$, que admitirá igualmente a base d.

Se observarmos que deveria ser

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} (a\,b) = \begin{pmatrix} \alpha a & \alpha b \\ \beta a & \beta b \end{pmatrix} = \begin{pmatrix} u & o \\ o & u \end{pmatrix},$$

$$(a\,b) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = (a\alpha + b\beta) = (u),$$

chegávamos ao absurdo $u = o$.

4) **Regresso aos endomorfismos do § 2.°** — Vamos estudar neste § os endomorfismos anteriormente referidos, supondo que a imagem homomorfa de $\mathfrak{G}$ tem uma base finita $w_1, w_2, \ldots, w_m$, que pode ser diferente da base dos V_j. Nenhuma hipótese formularemos quanto ao valor de m, nem suporemos, mesmo, que os elementos base (como sucede quando se não faz menção expressa) são independentes.

O endomorfismo fica definido pelas relações

$$v_j^{\Theta} = V_j = \prod_{k=1}^{m} w_k^{a_{kj}}, \quad (j = 1, 2, \ldots, n),$$

tendo-se, aliás,

$$w_i = \prod_{l=1}^{n} v_l^{c_{li}}, \quad (i = 1, 2, \ldots, m). \tag{7'}$$

Uma primeira questão que se levanta consiste em ver como se transforma a matriz rectangular $A = (a_{kj})$ quando se faz uma mudança de base em $\mathfrak{G}$. Resolveremos a questão duma maneira absolutamente geral, imaginando que, simultâneamente, se substituem os elementos w_i por elementos equivalentes. Tal equivalência é a tradução das igualdades

$$w'_k = \prod_{s=1}^{m} w_s^{q_{sk}}, \quad (k = 1, 2, \ldots, m), \tag{8}$$

nas quais se supõe $Q = (q_{sk})$ uma matriz quadrada com inverso direito e esquerdo.

Pratiquemos, então, a mudança de base

$$v'_j = \prod_{k=1}^{n} v_k^{p_{kj}}, \quad (j = 1, 2, \ldots, n), \tag{8'}$$

ao lado de (8). Trata-se de procurar a matriz obtida exprimindo nos w'_i os homomorfos dos v'_j, que designaremos com V'_j. Ora é

$$V'_j = \prod_{k=1}^{n} V_k^{p_{kj}} = \prod_{k=1}^{n} \left(\prod_{l=1}^{m} w_l^{a_{lk}} \right)^{p_{kj}} = \prod_{l=1}^{m} w_l^{\sum_k a_{lk}\, p_{kj}} .$$

Por outro lado, tem-se

$$w_l = \prod_1^m w'^{r_{il}}_i ,$$

designando com $R=(r_{il})$ a matriz inversa de Q. Assim, é

$$V'_j = \prod_{i=1}^m w'^{t_{ij}}_i ,$$

onde $T=(t_{ij})$ é a matriz procurada, definida por

$$T = R\,A\,P = Q^{-1}\,A\,P.$$

O problema que acaba de resolver-se não pode confundir-se com a questão seguinte, de importância fundamental para os resultados posteriores: Dado um sub-grupo $\mathfrak{N}$ $(w_1, \ldots, w_m)$ de $\mathfrak{G}$ $(v_1, \ldots, v_n)$, definido por $(7')$, procurar a matriz que define o mesmo sub-grupo, supondo que se substituem as bases de $\mathfrak{G}$ e de $\mathfrak{N}$, mediante (8) e (8').

Devem, então, exprimir-se os w'_k nos v'_j. Tem-se, sucessivamente:

$$w'_k = \prod_{s=1}^m \left(\prod_{l=1}^n v_l^{c_{ls}} \right)^{q_{sk}} = \prod_{l=1}^n v_l^{\sum_s c_{ls}\, q_{sk}} ,$$

$$v_l = \prod_{j=1}^n v'^{s_{jl}}_j , \qquad S=(s_{jl}) = P^{-1},$$

$$w'_k = \prod_{j=1}^n v'^{\theta_{jk}}_j , \qquad \Theta = (\theta_{jk}) = P^{-1}\,C\,Q.$$

5) **Transformações simples de matrizes** — Dada a matriz rectangular $C=(c_{kj})$, de n linhas e m colunas, dizem-se *transformações simples* de C as transformações dos dois tipos seguintes: 1.° — troca das linhas de ordens k e j (ou das colunas); 2.° — adição à linha de ordem k, dos elementos correspondentes da linha de ordem j multiplicados, à esquerda, pelo elemento $a \in \mathfrak{S}$, e operação análoga (com multiplicação à direita) para as colunas.

Estas transformações modificam a matriz C, que tornam numa outra matriz rectangular D, igualmente com n linhas e m colunas. Elas correspondem a mudanças de base em $\mathfrak{G}$ ou à substituïção da base no sub-grupo $\mathfrak{N}$.

Designando com P_{kj} a matriz quadrada de grau n que resulta da matriz unidade U_n trocando as linhas de ordens k e j, o produto

$$P_{kj}\,C = D$$

dá a transformada D, de C, pela primeira transformação. Mas P_{kj} é a matriz que determina uma nova base para $\mathfrak{G}$:

$$v'_1 = v_1, \ldots, v'_k = v_j, \ldots, v'_j = v_k, \ldots, v'_n = v_n .$$

Como se quere definir o sub-grupo $\mathfrak{N}$, determinado por C, tomando em $\mathfrak{S}$ o sistema base dos v'_i, tem de substituir-se a matriz C pela matriz $P_{kj}^{-1}\,C = P_{kj}\,C = D$, resultado que justifica a afirmação feita.

As transformações do 1.° tipo relativas a colunas correspondem a mudanças de base como as seguintes:

$$w'_1 = w_1, \ldots, w'_k = w_j, \ldots, w'_j = w_k, \ldots, w'_m = w_m .$$

A matriz C torna-se, neste caso, na matriz

$$D = C\,P_{kj},$$

onde P_{kj} é de grau m.

Passemos às transformações do 2.° tipo. Se designarmos com $Q_{kj}\,(a)$ a matriz quadrada de ordem n que se obtém de U_n substituindo o elemento nulo da linha de ordem k e da coluna de ordem j pelo elemento a, vê-se imediatamente que é

$$D = Q_{kj}\,(a)\,C.$$

A mudança de base

$$v_1 = v'_1, \ldots, v_k = v'_k, \ldots, v_j = v'_j\,v'^{a}_k, \ldots, v_n = v'_n ,$$

leva a substituir C por

$$Q_{kj}^{-1}\,(-a)\,C = Q_{kj}\,(a)\,C = D,$$

pois $$Q_{kj}^{-1}\,(-a) = Q_{kj}\,(a).$$

Finalmente, a mudança de base

$$w_1 = w'_1, \ldots, w_k = w'_k\,w'^{a}_j, \ldots, w_j = w'_j, \ldots, w_m = w'_m ,$$

corresponde à transformação do 2.° tipo relativa a colunas.

B

6) **Caso em que $\mathfrak{S}$ tem algoritmo de divisão** — Em tôda esta secção, o anel $\mathfrak{S}$, além de admitir elemento u, supõe-se sem divisores nulos e ter algorítmo de divisão. Para cada $a \in \mathfrak{S}$, pode fixar-se um valor absoluto inteiro, não negativo, $|a|$, de modo que, dados dois elementos quaisquer a e b, existam uma divisão direita e uma divisão esquerda:

$$\begin{cases} b = q\,a + r, \\ |r| < |a|, \end{cases} \qquad \begin{cases} b = a\,q' + r', \\ |r'| < |a|. \end{cases}$$

Demonstra-se então, fàcilmente, que um ideal direito ou esquerdo de $\mathfrak{S}$ é sempre um ideal principal direito (ou esquerdo) (1).

Sob o ponto de vista assinalado no final do § 4.°, seja $\mathfrak{N}(w_1, \ldots, w_m)$ um sub-grupo de $\mathfrak{G}$. As transformações simples de matrizes do § 5.° definem, como se viu, mudanças de base em $\mathfrak{G}$ e $\mathfrak{N}$.

Representemos com C as transformadas sucessivas duma matriz C. Se considerarmos o elemento de C que tem um valor absoluto mínimo, as transformações simples podem ter ou não ter a possibilidade de fazer substituir os elementos de C por outros, entre os quais se encontra um com um valor absoluto inferior ao mínimo anterior. O raciocínio prossegue-se até encontrar nas matrizes sucessivas uma que contenha um elemento com a propriedade do mínimo possível, em face das transformações simples. Em seguida, coloca-se tal elemento como c_{11}.

Posto isto, todos os elementos da primeira coluna de C são divididos, à direita, por c_{11}, e os da primeira linha são divididos, à esquerda, igualmente por c_{11}. Se, por ex., c_{12} não admitisse a divisão à esquerda, ter-se-ia $c_{12} = c_{11}\,q + r$, com $|r| < |c_{11}|$, sendo $r \neq 0$. Bastaria agora, utilizando o 2.° tipo de transformações simples, subtrair dos elementos da segunda coluna os elementos da primeira multiplicados à direita por q, para se encontrar um elemento r na matriz C de valor absoluto inferior a $|c_{11}|$, o que é contra a hipótese.

(1) *Grupos abelianos e Aneis*, etc., pág. 70, Cap. V.

A matriz C é, pois, da forma

$$C = \begin{pmatrix} c_{11} & k\,c_{11} & \ldots & f\,c_{11} \\ k'c_{11} & c_{22} & \ldots & c_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ f'c_{11} & c_{n2} & \ldots & c_{nm} \end{pmatrix}. \qquad (8'')$$

Por meio de operações simples do 2.° tipo, podemos reduzir C à forma

$$C = \begin{pmatrix} c_{11} & o & \ldots & o \\ \vdots & & C' & \\ o & & & \end{pmatrix}. \qquad (8''')$$

Os elementos da matriz C' são todos divididos por c_{11}, pois, se o não fôssem, bastaria juntar à primeira coluna uma coluna contendo um elemento c_{ik} não dividido por c_{11} para depois se poder aplicar o raciocínio anterior a c_{11} e c_{ik}.

Em seguida opera-se com C' como se operou com C. As operações a efectuar para reduzir C' a uma forma análoga à de C são operações que se devem executar, certamente, sôbre a matriz C. Mas elas *não alteram* os elementos da 1.ª linha e da 1.ª coluna de C, onde o único elemento não nulo continuará a ser c_{11}.

Chega-se, assim, a encontrar a transformada de C sob a forma

$$P\,C\,Q = D = \begin{pmatrix} |c_{11} & o & \ldots & o & \ldots & o| \\ o & c_{22} & \ldots & o & \ldots & o \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ o & o & \ldots & c_{rr} & \ldots & o \\ \ldots & \ldots & \ldots & \ldots & \ldots & . \\ |o & o & \ldots & o & \ldots & o| \end{pmatrix}, \qquad (9)$$

onde P e Q são matrizes invertíveis e onde pode ter-se $r = m$ ou $r = n$.

Os elementos c_{ii}, designados por *divisores elementares*, são divididos pelos seus anteriores.

Os raciocínios acabados de fazer permitem substituir as igualdades (7'), que definem o sub-grupo $\mathfrak{N}$, pelos seguintes:

$$w'_i = v'_i e_{ii}, \quad (i = 1, 2, \ldots, r), \qquad (10)$$

$$w'_j = \varepsilon, \quad (j = r+1, \ldots . m), \quad c_{i+1,\,i+1} \equiv 0\,(c_{ii}).$$

7) **Sôbre a questão da dimensionalidade** — A questão da ordem de $\mathfrak{G}$ é dominada pelo importante teorema seguinte: *Dado* $\mathfrak{G}$, *de ordem* n, *qualquer sub-grupo* $\mathfrak{N}$ *pode considerar-se como tendo uma ordem igual ou inferior a* n.

Sem dúvida que não é evidente ser $\mathfrak{N}$ um grupo finito. Consideremos o caso em que $\mathfrak{G} = \mathfrak{S} v$ se exprime na base do único elemento v. Se $v^a \neq \varepsilon$ pertence a $\mathfrak{N}$, o conjunto dos elementos de $\mathfrak{S}$, tais como a, que dão elementos de $\mathfrak{N}$, constituem um ideal direito, r, de $\mathfrak{S}$. Dado um segundo elemento $v^b \in \mathfrak{N}$, seja g o elemento gerador de r. Então é $a = gr$, $b = gs$, em que $r, s \in \mathfrak{S}$. Os nossos dois elementos escrevem-se

$$v^a = (v^g)^r, \qquad v^b = (v^g)^s.$$

Vê-se, assim, que o elemento $v^g \in \mathfrak{N}$ constitui uma base para $\mathfrak{N}$.

Continuando a seguir VAN DER WAERDEN (loc. cit.), admitamos a validade do teorema para o caso de $\mathfrak{G}$ ser um grupo de ordem n-1. Vamos provar que vale para a ordem n.

Se o sub-grupo $\mathfrak{N}$ tem elementos que se exprimem ùnicamente em n-1 dos elementos base v_i (nos n-1 primeiros, por ex.), o teorema está demonstrado. Se há elementos de $\mathfrak{N}$ que careçam dos n elementos v_i para a sua expressão, tomemos um dêsses elementos

$$\alpha = v_1^{a_1} \ldots v_n^{a_n} \neq \varepsilon,$$

com $a_n \neq 0$. Então os elementos $a_n \in \mathfrak{S}$, que figuram nas expressões de elementos de $\mathfrak{N}$, constituem um ideal direito de $\mathfrak{S}$. Designemos com g o seu elemento gerador. Existe, em $\mathfrak{N}$, um elemento da forma

$$\beta = v_1^{b_1} \ldots v_{n-1}^{b_{n-1}} v_n^g.$$

Dado, então, um elemento qualquer $\alpha \in \mathfrak{N}$, vê-se que existe um elemento $x \in \mathfrak{S}$ tal que $\Lambda = \alpha \beta^{-x}$ se exprime em $v_1, \ldots, v_{n-1}$:

$$\Lambda = \alpha \beta^{-x} = v_1^{c_1} \ldots v_{n-1}^{c_{n-1}}.$$

Mas $\Lambda \in \mathfrak{N}$. A totalidade dos elementos de $\mathfrak{N}$ que se exprimem em $v_1, \ldots, v_{n-1}$ constitui um sub-grupo que

pode, por hipótese, exprimir-se igualmente numa base $(w_1, \ldots, w_{m-1})$, com $m \leqq n$. Relativamente aos restantes elementos de $\mathfrak{N}$, a sua forma é

$$\alpha = \Lambda \beta^x,$$

pelo que basta tomar como elemento de ordem $m \leqq n$, para a base de $\mathfrak{N}$, precisamente $w_m = \beta$.

A independência de $w_1, \ldots, w_m$ resulta imediatamente. Se fôsse

$$w_1^{a_1} \ldots w_{m-1}^{a_{m-1}} w_m^b = \varepsilon,$$

teria de ser $b \neq 0$, pois, por hipótese, entre os $m-1$ primeiros w_i não há dependência. Então, substituindo na relação anterior os w_i pelas suas expressões nos $v_1 \ldots, v_{n-1}$, e $w_m = \beta$ pela sua expressão dada acima, obter-se-ia $g b = 0$, e, portanto, $g = 0$, o que é absurdo.

Pôsto isto, imaginemos que os w_i das igualdades (7′) são independentes. Nesse caso, nas relações (10), ter-se-á, necessàriamente, $r = m$, pois que o processo de redução a (9) mostra que a tôda a relação entre os w_i corresponde uma relação entre os w'_i, e reciprocamente.

Se os w_i são dependentes, não podemos ter (10) com $r = m$. E isso porque, se tivéssemos, como entre os w'_i existiriam relações de dependência, por ex.

$$w_1'^{a_1} \ldots w_m'^{a_m} = \varepsilon,$$

teríamos também

$$v_1'^{c_{11} a_1} \ldots v_m'^{c_{mm} a_m} = \varepsilon,$$

pelo que os v'_i não seriam independentes.

Imaginemos, agora, que o sub-grupo $\mathfrak{N}$ é o próprio grupo $\mathfrak{G}$, com outro modo de representação. Pregunta-se: pode ser $m > n$, sendo os w_i independentes? Colocada a matriz C sob a forma

$$C = \begin{pmatrix} c_{11} & 0 & \ldots & 0 & \ldots & 0 \\ 0 & c_{22} & \ldots & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & c_{mn} & \ldots & 0 \end{pmatrix},$$

vê-se que apenas n dos w'_i são independentes, pois os restantes são iguais a ε. Ora a existência de dependência entre os w'_i leva à existência de dependência entre os w_i.

A pregunta formulada responde-se pela negativa.

Mas surge uma segunda pregunta: pode ser $m < n$? Bastaria considerar $\mathfrak{N}$ como grupo e $\mathfrak{G}$ como sub-grupo, para se vêr que a resposta deve ser negativa. Directamente, é-se levado à matriz

$$C = \begin{pmatrix} c_{11} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & c_{mm} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}.$$

Como os primeiros membros de (10) são suficientes para exprimir os elementos de $\mathfrak{G}$, também $v'^{c_{11}}_1, \dots, v'^{c_{mm}}_m$ o são, de modo que a expressão de v'_{m+1}, por ex., levaria a uma dependência entre os v'_i, o que arrastaria dependência entre os v_i, contra a hipótese.

Em resumo: *a dimensionalidade dum grupo abeliano finito com respeito a um anel com algoritmo de divisão é um número bem determinado, se uma tal dimensionalidade existe.*

c

8) **Caso em que $\mathfrak{S}$ é um anel ideal principal** — Às transformações simples de matrizes, juntaremos, neste caso, um terceiro tipo. Sejam a e b dois elementos de $\mathfrak{S}$ e designemos com d o seu máximo divisor comum. Têm lugar as relações

$$\begin{matrix} a = a' d, \\ b = b' d, \end{matrix} \qquad r a + s b = d,$$

onde tôdas as letras escritas representam elementos de $\mathfrak{S}$.

Da última relação tira-se

$$r a' d + s b' d = d,$$

e, sendo $d \neq 0$,

$$r a' + s b' = u.$$

A matriz

$$\pi = \begin{pmatrix} r & s \\ -b' & a' \end{pmatrix}$$

é invertível em $\mathfrak{S}$. Dum modo geral, num domínio de integridade, vale o teorema seguinte: *é condição necessária e suficiente para que uma matriz seja invertível, que o seu determinante seja uma unidade* (1).

Tomemos a matriz A e a sua adjunta A_a. Valem as igualdades

$$A A_a = A_a A = |A| U_n,$$

onde $|A|$ é o determinante da matriz A e U_n é a matriz unidade. Se $|A| = a$ é uma unidade, pode escrever-se

$$A \,.\, a^{-1} A_a = a^{-1} A_a \,.\, A = U_n,$$

o que mostra ser suficiente a condição enunciada.

Inversamente, se $A B = U_n$, tem-se $|A|\,|B| = u$, pelo que $|A|$ é uma unidade.

Uma matriz de determinante unidade permite, assim, passar duma base independente dum grupo finito $\mathfrak{G}$ a uma segunda base nas mesmas condições.

Justificada dêste modo a invertibilidade da matriz π, vê-se imediatamente que a sua inversa é

$$\pi^{-1} = \begin{pmatrix} a' & -s \\ b' & r \end{pmatrix}.$$

Seja $\mathfrak{G}(v_1, \dots, v_n)$ um grupo relativo a $\mathfrak{S}$. Efectuemos a transformação seguinte:

$$\begin{cases} v'_1 = v_1, \dots, v'_{i-1} = v_{i-1}, v'_{i+1} = v_{i+1}, \dots, \\ \qquad v'_{j-1} = v_{j-1}, v'_{j+1} = v_{j+1}, \dots, v'_n = v_n, \\ v'_i = v_i^{a'} v_j^{b'}, \\ v'_j = v_i^{-s} v_j^{r}, \end{cases} \tag{11}$$

à qual corresponde a matriz

(1) Veja-se, para outros pormenores, por ex., pág. 55, Cap. IV, do nosso Curso sôbre *Grupos abelianos e Anéis e ideais não comutativos*.

$$S_{ij}\,(a,b)=\begin{vmatrix} u & o & \dots & o & \dots & o & \dots & o \\ o & u & \dots & o & \dots & o & \dots & o \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ o & o & \dots & a' & \dots & -s & \dots & o \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ o & o & \dots & b' & \dots & r & \dots & o \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ o & o & \dots & o & \dots & o & \dots & u \end{vmatrix},$$

onde a' e $-s$ pertencem à linha de ordem i, e b' e r à linha de ordem j. As colunas de ordem i e j contêm, respectivamente, a', b' e $-s$, r.

O teorema de LAPLACE dá-nos (1)

$$|\,S_{ij}\,(a,b)\,|=\begin{vmatrix} a' & \dots & -s \\ \dots & \dots & \dots \\ b' & \dots & r \end{vmatrix}\cdot\begin{vmatrix} u & \dots & o \\ \dots & \dots & \dots \\ o & \dots & u \end{vmatrix}=$$

$$=a'r+(-1)^{j-i+1}s\,.\,(-1)^{j-i-1}b'=a'r+b's=u,$$

de sorte que S_{ij} é invertível. E tem-se

$$S_{ij}^{-1}(a,b)=\begin{pmatrix} \dots & \dots & \dots & \dots & \dots \\ \dots & r & \dots & s & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & -b' & \dots & a' & \dots \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix},$$

matriz que resulta da substituïção dos vértices do quadrado $a', -s, b', r$, de S_{ij}.

Os elementos $(v'_1, \dots, v'_n)$ do grupo $\mathfrak{S}$ são independentes, como sabemos. Nessas condições, consideremos o sub-grupo $\mathfrak{N}\,(w_1, \dots, w_m)$ definido por uma matriz rectangular C. Quando se toma a base dos v'_i para $\mathfrak{S}$, a matriz C é substituída por

$$D=S_{ij}^{-1}C.$$

Se supusermos que os elementos a e b em causa são os elementos seguintes da matriz C:

$$c_{ik}=a, \quad c_{jk}=b,$$

(1) *Grupos abelianos e Anéis*, etc., pág. 54, Cap. IV.

vê-se imediatamente que os elementos d_{ik} e d_{jk} de D são

$$d_{ik}=d, \quad d_{jk}=0.$$

Em resumo: a transformação simples (11) permite substituir os elementos a, b não nulos, duma mesma coluna duma matriz, pelos elementos d, 0, onde d é o *m. d. c.* de a e b. Os restantes elementos de C, salvo os das linhas i e j, são conservados.

Procede-se anàlogamente com uma transformação que substitua dois dos elementos da base de $\mathfrak{N}$. Far-se-á

$$w'_i=w_i^r\,w_j^s, \quad w'_j=w'_i{}^{-b'}\,w_j^{a'}, \qquad (12)$$

mantendo para os outros w'_k as relações $w_k=w_k$.

Então, a matriz (1)

$$T_{ij}\,(a,b)=\begin{pmatrix} \dots & \dots & \dots & \dots & \dots \\ \dots & r & \dots & -b' & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & s & \dots & a' & \dots \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix},$$

a interpretar anàlogamente a $S_{ij}\,(a,b)$, tem a inversa

$$T_{ij}^{-1}\,(a,b)=\begin{pmatrix} \dots & \dots & \dots & \dots & \dots \\ \dots & a' & \dots & b' & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & -s & \dots & r & \dots \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix}.$$

A matriz C é substituída pela matriz

$$D=C\,T_{ij}.$$

Se supusermos $\quad c_{ki}=a, \quad c_{kj}=b, \quad$ é

$$d_{ki}=d. \quad d_{kj}=0.$$

Em resumo: a transformação simples (12) permite substituir os elementos a e b não nulos duma mesma linha

(1) Algumas das notações empregadas neste trabalho são tiradas de A. A. ALBERT, *Modern Higher Algebra*, University Press, Chicago, 1936.

pelos elementos d, 0, sendo d o *m. d. c.* de a e b. Os restantes elementos de C, salvo os das colunas i e j, são conservados.

9) **Redução duma matriz à forma (9)** — À custa dos *3* tipos de transformação simples, trata-se de provar que é possível ainda a redução de C à forma (9). As matrizes sucessivas, transformadas de C, continuarão a representar-se com C, sem perigo de confusão.

Sabemos, com efeito, que, dado um elemento de $\mathfrak{S}$, é possível decompô-lo num produto de elementos primos de $\mathfrak{S}$, decomposição que é única, desde que se ressalvem, nos factores, os elementos que são unidades de $\mathfrak{S}$. Consideremos, então, o elemento de C que contém um número mínimo de factores na sua decomposição. As transformações simples podem ter ou não ter a possibilidade de fazer substituir os elementos de C por outros, entre os quais se encontre com um número de factores de decomposição inferior ao mínimo anterior. O raciocínio prossegue-se até encontrar nas matrizes sucessivas uma que contenha um elemento com a propriedade do mínimo possível, em face das transformações simples. Em seguida, coloca-se tal elemento como c_{11}.

Pôsto isto, todos os elementos da primeira coluna e da primeira linha são divididos por c_{11}. Se, realmente, c_{12}, por ex., o não fôsse, designando com d o *m. d. c.* de c_{11} e c_{12}, seria

$$c_{11} = a'\,d, \qquad c_{12} = b'\,d,$$

com $a', b' \in \mathfrak{S}$. Ora a' não poderia ser uma unidade de $\mathfrak{S}$, pois, de contrário, tinha-se $a'^{-1}\,c_{11} = d$, $c_{12} = b'\,a'^{-1}\,c_{11}$, e, conseqüentemente, c_{11} dividiria c_{12}, contra a hipótese. Mas, então, uma operação simples poderia substituir c_{11}, c_{12} por d, 0, e encontrar-se-ia um elemento d com menos factores primos de decomposição do que c_{11}, o que é contrário à propriedade atribuída a c_{11}. A matriz C é, pois, da forma (8″), podendo, por operações do 2.° tipo, reduzir-se a (8‴). E as considerações continuam como no § 6.°.

10) — **A questão da dimensionalidade** — O importante teorema do começo do § 7.° é válido aqui.

Suponhamos que o grupo $\mathfrak{G}\ (v_1, \ldots, v_n)$ é um grupo habitual com n geradores (o anel $\mathfrak{S}$ é o anel dos números inteiros). Se $\mathfrak{N}\ (w_1, \ldots, w_m)$ é um sub-grupo para o qual

$$w_k = \prod_i v_i^{c_{ik}}, \qquad (k = 1, 2, \ldots, m),$$

trata-se de construir, efectivamente, uma base independente para $\mathfrak{N}$.

Se nos w_k há um, pelo menos, que contém v_n na sua expressão, consideremos o ideal gerado pelos c_{nk}, isto é, determinemos o *m. d. c.* φ destas quantidades. Existe uma relação do tipo

$$c_{n1}\,b_1 + c_{n2}\,b_2 + \ldots + c_{nm}\,b_m = \varphi,$$

que se pode determinar, por ex., do modo sucessivo seguinte:

$$\begin{aligned} &c_{n1}\,\delta_1 + c_{n2}\,\delta_2 = \varphi_2,\\ &\varphi_2\,\varphi_2 + c_{n3}\,\delta_3 = \varphi_3,\\ &\ldots\ldots\ldots\ldots\ldots\ldots,\\ &\varphi_{m-1}\,\varphi_{m-1} + c_{nm}\,\delta_m = \varphi, \end{aligned}$$

onde $\varphi_2, \varphi_3, \ldots$ são, respectivamente, os *m. d. c.* de (c_{n1}, c_{n2}), $(\varphi_2, c_{n3}), \ldots, (\varphi_{m-1}, c_{nm})$, e os restantes coeficientes são números inteiros. Calculados, assim, $b_1, \ldots, b_m$, ponhamos

$$l_1 = \prod_1^m w_i^{b_i} = v_n^{\varphi} \prod_1^{n-1} v_i^{c_i},$$

e, em seguida,

$$w_1 = l_1^{\tau_1}\,w'_1,\ w_2 = l_1^{\tau_2}\,w'_2, \ldots, w_m = l_1^{\tau_m}\,w'_m,$$

onde os $w'_1, \ldots, w'_m$ não contêm v_n nas suas expressões.

Se nos w'_j figura v_{n-1} (poderíamos dizer que o mais alto v_i seria, por ex., v_r), praticando com os w'_j como se fêz com os w_i, chega a pôr-se

$$w'_1 = l_2^{\tau'_1}\,w''_1, \ldots, w'_m = l_2^{\tau'_m}\,w''_m,$$

onde l_2 é um produto dos w'_i (e, conseqüentemente, dos w_i), e onde os w''_i não contêm v_n e v_{n-1} nas suas expressões. E dá-se a circunstância de l_1 e l_2 serem independentes, pois uma relação $l_1^a\,l_2^b = \varepsilon$ levaria a $a\,\varphi = 0$, e, visto que $\varphi \neq 0$, a $a = 0$. Em seguida, de $l_2^b = \varepsilon$, tirar-se-ia $\varphi\,b = 0$, onde φ é o *m. d. c.* dos expoentes de v_{n-1} nos w'_j, e, portanto, tinha-se $b = 0$, como se deseja.

O raciocínio prossegue-se até chegar a

$$w_1^{(r)}, \ldots, w_m^{(r)},$$

tais que, escrevendo

$$w_1^{(r)} = l_{r+1}^{\tau_1^{(r)}} w_1^{(r+1)}, \ldots, w_m^{(r)} = l_{r+1}^{\tau_m^{(r)}} w_m^{(r+1)},$$

todos os $w_i^{(r+1)}$ sejam iguais a ε. Então os $w_i^{(r)}$ são tais que, achando o *m. d. c.* dos coeficientes do v_k de maior índice que nêles figura, se chega a um l_{r+1} no qual se exprimem todos os $w_i^{(r)}$.

A base procurada compõe-se de $(l_1, l_2, \ldots, l_{r+1})$.

A questão da dimensionalidade investiga-se como no § 7.°. Se os w_i das igualdades (7′) são independentes, nas relações (10) será, necessàriamente, $r = m$. Se são dependentes, não pode ter-se $r = m$.

Supondo $\mathfrak{N} = \mathfrak{G}$, também não pode ter-se $m > n$, supondo os w_i independentes. A hipótese $m < n$ é igualmente de excluir, como se vê trocando os papéis de $\mathfrak{N}$ e de $\mathfrak{G}$.

Em resumo: *a dimensionalidade dum grupo abeliano finito com respeito a um anel ideal principal é um número bem determinado, se uma tal dimensionalidade existe.*

Poderia ainda imaginar-se, no caso $\mathfrak{N} = \mathfrak{G}$, que seria possível $m = n$, com os w_i dependentes. Tal hipótese é ainda de excluir, pois ela levaria a $r < m$ elementos w_i', capazes de constituïrem uma base independente de $\mathfrak{G}$.

D

11) **O teorema fundamental** — Quando a base do grupo $\mathfrak{G}$, tratado nas secções *B* e *C*, não é independente, e nada se sabe, portanto, àcêrca da dimensionalidade de $\mathfrak{G}$, tem lugar o teorema fundamental: *o grupo $\mathfrak{G}$ é um produto directo de grupos cíclicos, cada um dos quais com um elemento base que pode tornar-se ε para elementos não nulos do anel $\mathfrak{S}$.*

A demonstração a seguir é extraída do livro várias vezes referido de VAN DER WAERDEN.

12) **Caso de um elemento gerador** — Consideremos, num grupo $\mathfrak{G}$ com um número finito de elementos, o grupo cíclico $\mathfrak{g}$ gerado por um elemento a, de ordem N:

$$\mathfrak{g} = \{ \varepsilon, a, a^2, \ldots, a^{N-1} \}.$$

Trata-se dum grupo relativo ao anel dos números inteiros, que é um anel dos dois tipos aqui em causa. Não é possível encontrar em $\mathfrak{g}$ uma base que não se torne ε para elementos não nulos do anel.

Duma maneira geral, seja $\mathfrak{G}$ um grupo relativo a $\mathfrak{S}$ do tipo $\mathfrak{G} = \mathfrak{S}\, g$, com o único gerador g. Os elementos de $\mathfrak{S}$ que satisfazem a $g^\omega = \varepsilon$ constituem um ideal esquerdo de $\mathfrak{S}$, tendo em vista a definição (5′) da secção *A*. De facto, de $g^a = \varepsilon$, $g^b = \varepsilon$, tira-se $g^{a-b} = \varepsilon$, e, de $g^a = \varepsilon$, tira-se, $g^{sa} = (g^a)^s = \varepsilon$, quaisquer que sejam $a, b, s \in \mathfrak{S}$.

Se a cada elemento $a \in \mathfrak{S}$ associarmos, em $\mathfrak{G}$, o elemento g^a, define-se um homomorfismo operatório, como se conclui das relações:

$$a + b \to g^{a+b} = g^a \cdot g^b,$$
$$s\,a \to g^{sa} = (g^a)^s.$$

Então, o grupo $\mathfrak{G}$ verifica a relação

$$\mathfrak{G} \cong \mathfrak{S}/\mathfrak{n},$$

onde $\mathfrak{n}$ é o ideal de $\mathfrak{S}$ que verifica $g^\omega = \varepsilon$. Existe, de resto, um elemento gerador, a, de $\mathfrak{n}$, que suporemos diferente do elemento nulo: $\mathfrak{n} = (a)$.

Quando $\mathfrak{S}$ é anel ideal principal, uma ulterior decomposição de $\mathfrak{G}$, num produto directo de grupos cíclicos, obtém-se fàcilmente, como vamos vêr.

Sabemos que não é possível encontrar uma base para $\mathfrak{G}$ que não se anule para elementos não nulos de $\mathfrak{S}$, se $a \neq 0$. Interessa, conseqüentemente, vêr se é possível decompor $\mathfrak{G}$, por forma que os ideais que tornam ε a base de cada factor tenham uma geração simples. É o que sucede se tais ideais forem gerados por elementos primos ou por potências de tais elementos. Assim, propomo-nos demonstrar o teorema seguinte: *o grupo cíclico $\mathfrak{G}$ é um produto directo de grupos cíclicos, cada um dos quais se torna ε por meio duma potência dum elemento primo. O produto das diferentes potências dá, precisamente, o elemento* a, *gerador de* $\mathfrak{n}$.

Se a é um elemento primo ou uma potência dum elemento primo, o teorema está demonstrado. No caso contrário, pode escrever-se $a = b\,c$, onde b e c são elementos de $\mathfrak{S}$ que têm factores primos não comuns. Ponhamos, então,

$$g_1 = g^b\,, \quad g_2 = g^c\,,$$

e consideremos os grupos cíclicos $\mathfrak{G}_1 = \mathfrak{S}g_1$, $\mathfrak{G}_2 = \mathfrak{S}g_2$. Vamos demonstrar que os ideais que tornam ε as bases g_1 e g_2 são, respectivamente, (c) e (b).

Sem dúvida que c torna g_1 igual a ε, de sorte que o ideal (c') verificando $g_1^x = \varepsilon$ satisfaz a $(c') \subseteq (c)$ (1). Anàlogamente se encontra $(b') \subseteq (b)$, sendo (b') o ideal solução de $g_2^x = \varepsilon$. Como o produto $c'\,b'$ verifica $g_1^x = g_2^x = \varepsilon$, verificará também $g^x = \varepsilon$, pois pode escrever-se

$$r\,b + s\,c = u, \; g = g^u = g^{r\,b + s\,c} = g_1^r \cdot g_2^s, \quad (r, s \in \mathfrak{S}),$$

visto que o máximo divisor comum de b e c é u. Será, assim, $c'\,b' = a\,t$, com $t \in \mathfrak{S}$. E tira-se

$$c'\,f = c, \quad b'\,p = b, \quad c'\,b'\,f\,p = c\,b = a = a\,t\,f\,p,$$

onde $f, p \in \mathfrak{S}$. A relação $t\,f\,p = u$ mostra que t, f, p são unidades de $\mathfrak{S}$, e que, portanto,

$$c' = c\,f^{-1}, \quad b' = b\,p^{-1},$$

donde se conclui, como se deseja,

$$(c') = (c), \quad (b') = (b).$$

Pôsto êste resultado, observemos o seguinte: o produto dum elemento de $\mathfrak{G}_1$ por um elemento de $\mathfrak{G}_2$ é um elemento de $\mathfrak{G}$, e, inversamente, todo o elemento de $\mathfrak{G}$ se pode considerar produto dum elemento de $\mathfrak{G}_1$ por um elemento de $\mathfrak{G}_2$, como o mostra a relação $g = g_1^r \cdot g_2^s$. Se, por outro lado, a intersecção de $\mathfrak{G}_1$ com $\mathfrak{G}_2$ fôr ε, poderá escrever-se

$$\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2\,.$$

(1) Com $\subseteq$ significa-se «inclusão».

Ora, se i fôr um elemento da intersecção, tem-se

$$i^b = i^c = \varepsilon, \quad i^{rb+sc} = i^u = i = \varepsilon.$$

Procedendo com $\mathfrak{G}_1$ e $\mathfrak{G}_2$ como se fêz com $\mathfrak{G}$, chega a estabelecer-se o teorema enunciado.

A decomposição de a em factores primos, pondo de parte elementos unidade, é unívoca. A um elemento unidade, de resto, teríamos de fazer corresponder, na decomposição de $\mathfrak{G}$, uma parcela igual a ε.

É igualmente unívoca a decomposição de $\mathfrak{G}$. Êsse facto resulta do seguinte: *dois produtos de potências de elementos primos que não contenham factor comum,* pela circunstância de terem um *m. d. c.* igual a u, *não podem tornar* ε *um mesmo elemento diferente de* ε.

Na verdade, suponhamos

$$\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2 \times \ldots = \mathfrak{G}'_1 \times \mathfrak{G}_2 \times \ldots,$$

duas decomposições de $\mathfrak{G}$, e designemos com $p_1^{\rho_1}$, $p_2^{\rho_2}, \ldots$, $p_1'^{\rho'_1}$, $p_2'^{\rho'_2}, \ldots$, as potências de elementos primos que tornam ε, respectivamente, os elementos de $\mathfrak{G}_1, \ldots, \mathfrak{G}'_1 \ldots$. O produto $P = p_1'^{\rho'_1} p_2'^{\rho'_2} \ldots$ torna ε todos os elementos de $\mathfrak{G}$, e, conseqüentemente, os elementos de $\mathfrak{G}_1$. Isso significa que (p_{11}^{ρ}) contém P. Êste processo demonstra não apenas que os p_i e os p'_i são idênticos, mas ainda que se tem $\rho_i = \rho'_i$, pois, por construção, os p_i são diferentes entre si, o mesmo sucedendo com os p'_i. A nota supra mostra, por fim, que é $\mathfrak{G}_i = \mathfrak{G}'_i$.

13) **Caso geral** — Passemos ao caso em que há mais do que um elemento gerador de $\mathfrak{G}$. Para um grupo abeliano finito ordinário com uma base de dois elementos α e β, de ordens N e P, respectivamente, podemos pôr

$$\mathfrak{G} = (\alpha)\,(\beta),$$

onde (α) é o grupo dos elementos α^m, e (β) o dos elementos β^n, com m e n inteiros quaisquer. O menor múltiplo comum de N e P torna ε todos os elementos de $\mathfrak{G}$. Não é possível encontrar uma base cujos elementos se não tornem ε para elementos não nulos do anel dos números inteiros.

Dum modo geral, suponhamos que há n elementos geradores $x_1, x_2, \ldots, x_n$ de $\mathfrak{G}$, de sorte que cada elemento de $\mathfrak{G}$ é da forma

$$x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}, \qquad (a_i \in \mathfrak{S}).$$

É da comparação de $\mathfrak{G}$ a um grupo abeliano com respeito a $\mathfrak{S}$ em que haja uma base de n elementos independentes que vai resultar a nossa demonstração, aplicável aos dois tipos de anéis em causa.

Sejam $u_1, \ldots, u_n$ n elementos como símbolos — base dum grupo abeliano $\mathfrak{G}'$ relativo a $\mathfrak{S}$. Dado o elemento $\Pi u_i^{a_i} \in \mathfrak{G}'$, façamos-lhe corresponder o elemento $\Pi x_i^{a_i} \in \mathfrak{G}$.

Tal correspondência é um homomorfismo operatório, tendo-se

$$\mathfrak{G} \cong \mathfrak{G}' / \mathfrak{N}',$$

onde $\mathfrak{N}'$ é o divisor normal de $\mathfrak{G}'$ que tem como correspondente em $\mathfrak{G}$ o elemento ε. Visto que $\mathfrak{N}'$ é um sub-grupo de $\mathfrak{G}'$, é possível encontrar bases $(V_1, \ldots, V_m)$, em $\mathfrak{N}'$, e $(U_1, \ldots, U_n)$, em $\mathfrak{G}'$, com $m \leqq n$, tais que

$$V_i = U_i^{b_i}, \quad b_{i+1} \equiv 0\,(b_i), \quad (i = 1, 2, \ldots, m).$$

Se designarmos com $\varphi_1, \varphi_2, \ldots, \varphi_n$ os elementos de $\mathfrak{G}$ que correspondem aos elementos $U_i \in \mathfrak{G}$, fácil é de vêr que os φ_i são geradores de $\mathfrak{G}$. Dado $\Pi x_i^{a_i}$ como correspondente de $\Pi u_i^{a_i} = \Pi U_i^{a_i}$, vê-se que se tem, com efeito, $\Pi x_i^{a_i} = \Pi \varphi_i^{a_i}$.

Importante é observar-se agora que, diferentemente do que sucede com os $\mathfrak{S} x_i$, os sub-grupos cíclicos $\mathfrak{S} \varphi_i$ não têm elementos comuns. Imaginemos a relação

$$\Pi \varphi_i^{c_i} = \varepsilon, \qquad (c_i \in \mathfrak{S}). \tag{13}$$

Então será

$$\prod_{i=1}^{n} U_i^{c_i} = \prod_{j=1}^{m} V_j^{t_j},$$

pois que o elemento representado no primeiro membro pertence ao sub-grupo $\mathfrak{N}'$. Nestas condições, tem lugar a igualdade

$$\prod_{i=1}^{n} U_i^{c_i} = \prod_{j=1}^{m} U_j^{t_j b_j},$$

de sorte que será, necessàriamente, dada a independência dos U_i,

$$c_1 = t_1 b_1, \ldots, c_m = t_m b_m, \; c_{m+1} = \ldots = c_n = 0.$$

Tem-se, dêste modo,

$$\varphi_i^{c_i} = \varphi_i^{t_i b_i} = (\varphi_i^{b_i})^{t_i} = \varepsilon,$$

pois $\varphi_i^{t_i b_i}$ corresponde, no homomorfismo $\mathfrak{G}' \sim \mathfrak{G}$, ao elemento $U_i^{t_i b_i} = V_i^{t_i} \in \mathfrak{N}'$. Tôda a relação da forma (13) só pode ter lugar quando cada um dos factores é igual a ε. Desta maneira, o produto directo de grupos cíclicos.

$$\mathfrak{G} = \prod_{1}^{n} \mathfrak{S} \varphi_i = \prod_{1}^{n} (\varphi_i) \tag{14}$$

representa $\mathfrak{G}$, como se enunciou no § 11.º. Cada sub-grupo (φ_i) é tornado ε por um ideal (b_i), valendo as relações

$$\begin{aligned} b_{i+1} &\equiv 0\,(b_i), \quad (i = 1, 2, \ldots, m \leqq n), \\ b_j &= (0), \quad (j = m+1, \ldots, n). \end{aligned} \tag{15}$$

É claro que no produto directo deverão pôr-se de parte os grupos cíclicos para os quais o ideal $(b_i) = \mathfrak{S}$. É o que sucede, por ex., quando, no caso comutativo, b_i é uma unidade. De resto, em ambos os casos, tem de existir inverso de b_i, sempre que $(b_i) = \mathfrak{S}$.

14) **Decomposição ulterior e teorema da univocidade para o caso dum anel ideal principal** — No caso comutativo, uma vez encontrados os grupos cíclicos $\mathfrak{S} \varphi_i$, vale, para cada um dêstes, o raciocínio feito no § 12.º. Cada grupo (φ_i) decompõe-se num produto directo de novos grupos cíclicos, e cada um dêstes últimos torna-se ε por meio dum ideal gerado por uma potência dum elemento primo p. O mesmo elemento primo pode comparecer em vários dos grupos (φ_i), de modo que, associando os grupos cíclicos da decomposição dos (φ_i) que correspondem ao mesmo elemento p, obtém-se

$$\mathfrak{G} = \mathfrak{H} \times \Pi \mathfrak{G}_p,$$

onde II é estendido a p, e onde $\mathfrak{O}$ é o produto dos grupos (φ_i) para os quais $(b_i) = (0)$.

Um teorema demonstrado no § 12.° garante que os grupos $\mathfrak{G}_p$ são *univocamente definidos*, mas não pode fazer-se uma afirmação semelhante relativamente ao grupo $\mathfrak{O}$. Todavia, o primeiro teorema da isomorfia (1) dá

$$\mathfrak{G} / II\,\mathfrak{G}_p \cong \mathfrak{O} / \mathfrak{O} \cap II\,\mathfrak{G}_p \cong \mathfrak{O} \text{ (2)}.$$

de sorte que, pondo de parte isomorfias, $\mathfrak{O}$ é também determinado (insistiremos adiante sôbre estas afirmações).

Sob as condições (15), os ideais (b_i) são, ainda, univocamente definidos, como vamos vêr. Suponhamos que em (14) figuram q grupos cíclicos não iguais a ε. Os ideais (b_i), em número de q, são, indiferentemente, definidos pelos elementos b_i ou por outros que defiram dêles por factores que sejam unidades de $\mathfrak{S}$. A univocidade que vamos demonstrar reduz-se, pois, a provar que a decomposição dos b_i em factores primos, pondo de parte unidades, pode fazer-se em face do grupo $\mathfrak{G}$.

Seja a potência p^ρ do elemento primo p. Se ela entra como factor em b_k, as igualdades $b_{i+1} = t\,b_i$ mostram que entra igualmente em factor nos b_i com índice superior a k. Por conseqüência, sabendo, para cada potência p^ρ, o número l dos b_i em que ela entra como factor, sabemos também quais são êsses b_i. Ora a determinação de l faz-se como vai vêr-se.

Lema 1.° — *Dado o grupo* $(\varphi_i)^{p^{\rho-1}} \overline{\supset} (\varphi_i)^{p^\rho}$, *se* p^ρ *é factor de* $\mathrm{b_i}$, *não pode ter lugar o sinal* $=$. Que o grupo $(\varphi_i)^{p^{\rho-1}}$ contém o grupo $(\varphi_i)^{p^\rho}$, vê-se imediatamente escrevendo $(\varphi_i)^{p^\rho} = (\varphi_i{}^p)^{p^{\rho-1}}$. Se fôssem iguais os dois grupos, existiria um elemento $k \in \mathfrak{S}$ tal que $\varphi_i{}^{p^{\rho-1}} = \varphi_i{}^{p^\rho k}$, e, portanto, ter-se-ia sucessivamente

$$p^{\rho-1} - p^\rho k = t\,b_i = t\,p^\rho\,a\,,$$

$$p^{\rho-1} = p^\rho\,(k + ta), \qquad (t, a \in \mathfrak{S}).$$

Ora a última igualdade é absurda.

(1) Veja-se o nosso Curso sôbre *Elementos de Teoria dos Grupos*, Cap. II, pág. 76.

(2) Com o sinal $\cap$ significa-se «intersecção» ou «parte comum».

Lema 2.° — *Se* p^ρ *não entra em* $\mathrm{b_i}$, *é* $(\varphi_i)^{p^{\rho-1}} = (\varphi_i)^{p^\rho}$. De facto, b_i tem então uma das formas

$$b_i = p^{\rho-k}\,a\,, \qquad b_i = p^{\rho-k}\,,$$

onde $k \leqq \rho$. O grupo $\Delta = (\varphi_i)^{p^{\rho-1}} / (\varphi_i)^{p^\rho}$ compõe-se dos elementos

$$(\varphi_i)^{p^\rho} = \varepsilon', \quad \varphi_i^{p^{\rho-1}}(\varphi_i)^{p^\rho}, \quad \varphi_i^{p^{\rho-1}\circ}(\varphi_i)^{p^\rho}, \ldots,$$

o que nos mostra tratar-se do grupo cíclico gerado por $H_i = \varphi_i^{p^{\rho-1}}(\varphi_i)^{p^\rho}$. Se b_i tem a primeira forma considerada, o elemento $a \in \mathfrak{S}$, que se supõe não conter o factor p, verifica $H_i^a = \varepsilon'$. Mas a não pode pertencer ao ideal (p), que é um ideal satisfazendo a $H_i^x = \varepsilon'$. Isso significa que o ideal solução desta última equação é um ideal $(r) \supset (p)$. Como, porém, o ideal (p) é um ideal primo sem divisor, tem-se $(r) = \mathfrak{S}$. Então, sendo

$$\Delta \cong \mathfrak{S} / \mathfrak{S} \cong \text{ grupo composto do elemento unidade,}$$

o grupo Δ contém ùnicamente o elemento ε', sendo, como se deseja, $(\varphi_i)^{p^{\rho-1}} = (\varphi_i)^{p^\rho}$. Para a outra forma de b_i a conclusão é a mesma.

Lema 3.° — *O grupo* Δ *é um grupo simples, quando* $(\varphi_i)^{p^{\rho-1}} \supset (\varphi_i)^{p^\rho}$. — Na verdade, p^ρ entra, então, como factor, em b_i; o ideal que verifica $H_i^x = \varepsilon'$ é precisamente o ideal (p), pois $\Delta \neq$ grupo unidade; e Δ não pode ter um sub-grupo diferente de Δ e do grupo unidade, em virtude do que vai seguir-se. Dado um grupo $\mathfrak{G} = \mathfrak{S}\,\varphi$, para o qual $\varphi^\omega = \varepsilon$ é satisfeita pelo ideal (p), com p primo, se existir um sub-grupo $\mathfrak{N} = \mathfrak{S}\varphi^b$, com $\varphi^b \neq \varepsilon$, o grupo $\mathfrak{G}/\mathfrak{N}$ torna-se ε' para todos os elementos de $\mathfrak{S}$, porque b não pertence a (p), e, conseqüentemente, o ideal que torna ε' a base $\varphi.\mathfrak{N}$ de $\mathfrak{G}/\mathfrak{N}$, contendo (p) como sub-ideal, só pode ser $\mathfrak{S}$. Isto significa que é $\mathfrak{G}/\mathfrak{N} \cong (\varepsilon')$, e, portanto, que $\varphi \in \mathfrak{N}$, tendo-se $\mathfrak{N} = \mathfrak{G}$, *q. e. d.*

Lema 4.° — *O grupo* $\Phi = \mathfrak{G}^{p^{\rho-1}} / \mathfrak{G}^{p^\rho}$ *é um produto directo de grupos simples.* A simples definição do grupo Φ

mostra que, com efeito, é

$$\Phi = (\varphi_1)^{p^{\rho}-1}/(\varphi_1)^{p^{\rho}} \times \ldots \times (\varphi_q)^{p^{\rho}-1}/(\varphi_q)^{p^{\rho}}. \qquad (16)$$

Um elemento $(\varphi_1^{a_1} \ldots \varphi_q^{a_q})^{p^{\rho}-1}. \ \mathfrak{G}^{p^{\rho}} \in \Phi$ pode escrever-se sob a forma

$$\varphi_1^{p^{\rho}-1 a_1}. \ \mathfrak{G}^{p^{\rho}} \ldots \varphi_q^{p^{\rho}-1 a_q}. \ \mathfrak{G}^{p^{\rho}},$$

isto é, sob a forma dum produto de elementos dos grupos que figuram no segundo membro de (16), e inversamente. Dêste modo, Φ, pondo de parte os factores de (16) iguais ao grupo unidade, é um produto directo de grupos simples.

Conseqüências — O número l procurado é igual ao número de factores de (4) diferentes do grupo unidade, e, portanto, igual ao comprimento da série de composição do grupo Φ, sendo, assim, bem determinado, como se deseja.

Uma outra conseqüência é a que vai seguir-se. Visto que os (b_i) são conhecidos, os grupos $\mathfrak{S}\varphi_i$ são univocamente determinados, pondo de parte isomorfias, pois

$$\mathfrak{S}\varphi_i \cong \mathfrak{S}/(b_i).$$

Podemos vêr ainda que as potências $p_i^{\rho}i$, postas em causa por virtude da decomposição ulterior dos factores $\mathfrak{S}\varphi_i$, são bem determinadas. Imaginemos as duas decomposições

$$\mathfrak{G} = \mathfrak{A}_1 \times \ldots \times \mathfrak{A}_r \times \mathfrak{B}_1 \times \ldots \times \mathfrak{B}_s =$$
$$= \mathfrak{A}'_1 \times \ldots \times \mathfrak{A}'_{r'} \times \mathfrak{B}'_1 \times \ldots \times \mathfrak{B}'_{s'}, \qquad (17)$$

onde os $\mathfrak{A}_i$, $\mathfrak{A}'_i$ são os grupos cíclicos para os quais $g_i^{\alpha} = \varepsilon$, $g_i'^{\alpha} = \varepsilon$, são satisfeitas, respectivamente, por $(p_i^{\rho}i)$, $(p_i'^{\rho'}i)$, e $\mathfrak{B}_j$, $\mathfrak{B}'_j$ são os grupos cíclicos para os quais os ideais análogos são $(b_i) = (0)$.

Tomemos o sub-grupo $\mathfrak{H}$, de $\mathfrak{G}$, que é o produto directo dos $\mathfrak{A}_i$ relativos ao mesmo elemento primo p,

$$\mathfrak{H} = \mathfrak{A}_{i_1} \times \ldots \times \mathfrak{A}_{i_k}, \quad (k \leqq r). \qquad (18)$$

$\mathfrak{H}$ compõe-se de ε e dos elementos de $\mathfrak{G}$ para os quais é possível encontrar uma potência de p que os torne iguais

a ε. Que os elementos de (18) estão nessas condições, é imediato. Recìprocamente, seja $\alpha \in \mathfrak{G}$ um tal elemento. Pondo

$$\alpha = \alpha_1 \ldots \alpha_r. \ \beta_1 \ldots \beta_s, \quad (\alpha_i \in \mathfrak{A}_i, \ \beta_i \in \mathfrak{B}_i),$$

a relação $\alpha^{p^m} = \varepsilon$ dá

$$p^m = k_1 p_1^{\rho_1} = \ldots = k_r p_r^{\rho_r}, \quad \beta_1 = \ldots = \beta_s = \varepsilon,$$

e, portanto,

$$\alpha = \alpha_1 \ldots \alpha_r. \qquad (19)$$

Tem agora de ser, forçosamente,

$$p_1 = p_2 = \ldots = p_r = p,$$

o que significa que, em (19), só podem figurar α_i α_i relativos ao mesmo elemento primo, como se afirmou.

Escrevendo α com o aspecto indicado pela segunda decomposição (17), chega-se a concluir a igualdade dos p_i e dos p'_i, ao mesmo tempo que as igualdades

$$\mathfrak{H} = \mathfrak{A}_{i_1} \times \ldots \times \mathfrak{A}_{i_k} = \mathfrak{A}'_{j_1} \times \ldots \times \mathfrak{A}'_{j_l},$$
$$\mathfrak{G}' = \mathfrak{A}_1 \times \ldots \times \mathfrak{A}_r = \mathfrak{A}'_1 \times \ldots \times \mathfrak{A}'_{r'},$$

com os $\mathfrak{A}'_j$ análogos aos $\mathfrak{A}_i$.

A demonstração da propriedade em vista, quanto aos $p_i \neq 0$, reduz-se à sua demonstração para o grupo $\mathfrak{H}$. Daremos a êste a forma

$$\mathfrak{H} = \mathfrak{A}_1 \times \ldots \times \mathfrak{A}_s = \mathfrak{A}'_1 \times \ldots \times \mathfrak{A}'_t,$$

e suporemos que $p^{\sigma_1}, \ldots p^{\sigma'_1}, \ldots$ são as potências mínimas que tornam ε os diferentes grupos. Dispondo os σ_i e os σ'_i por ordem crescente, seja

$$\sigma_1 \leqq \sigma_2 \leqq \ldots \leqq \sigma_s,$$
$$\sigma'_1 \leqq \sigma'_2 \leqq \ldots \leqq \sigma'_t.$$

Pondo $b_i = p^{\sigma i}$, os resultados do § 14.º garantem que os $p^{\sigma i}$ são bem determinados e iguais aos $p^{\sigma' i}$, como se quere.

Havendo elementos $p_i = 0$ a considerar, ponhamos

$$\mathfrak{G} = \mathfrak{A} \times \mathfrak{B} = \mathfrak{A} \times \mathfrak{B}',$$

onde $\mathfrak{A}$ é o produto dos $\mathfrak{A}_i$, $\mathfrak{B}$ o dos $\mathfrak{B}_j$ e $\mathfrak{B}'$ o dos $\mathfrak{B}'_j$, da igualdade (17). Tem-se

$$\mathfrak{G}/\mathfrak{A} \cong \mathfrak{B}, \quad \mathfrak{G}/\mathfrak{A} \cong \mathfrak{B}',$$

$$\mathfrak{B} \cong \mathfrak{B}'.$$

Para o grupo $\mathfrak{B}$, os b_i são bem determinados e todos iguais a zero. O mesmo tem lugar para o grupo isomorfo $\mathfrak{B}'$. O número dos b_i é igual em ambos os casos, pois que êsse número representa a dimensionalidade de $\mathfrak{B}$ ou de $\mathfrak{B}'$.

E

15) **Considerações gerais** – Exemplos importantes de grupos abelianos com operadores são dados pelos anéis, quando cada elemento do anel se imagina operando sôbre os elementos do anel conforme a regra do produto de dois elementos. Os operadores aparecem, então, como coeficientes, podendo colocar-se à direita ou à esquerda. Suponhamos, por ex., que os elementos do anel $\mathfrak{S}$ operam à direita.

Se $a \in \mathfrak{S}$, tem-se, para cada $s \in \mathfrak{S}$,

$$as \in \mathfrak{S}, \quad (a+b)\,s = as + bs, \quad (b \in \mathfrak{S}),$$

como o exige a definição de operador.

Os sub-grupos admissíveis são os ideais direitos.

Se o anel tem elemento um, êste elemento constitui uma base de $\mathfrak{S}$, que passa a ser um módulo finito relativamente a $\mathfrak{S}$. Existe uma dimensionalidade de 1.ª ordem, pois que, se se supõe $us = 0$, tem-se

$$us = s = 0.$$

É freqüente terem de considerar-se anéis com elemento u, para os quais há n elementos e_i satisfazendo às condições

seguintes:

$$u = e_1 + e_2 + \ldots + e_n,$$
$$e_i^2 = e_i, \quad e_i\,e_k = 0, \quad (i \neq k).$$

O anel $\mathfrak{S}$ é, então, uma soma directa de ideais direitos (1):

$$\mathfrak{S} = e_1\mathfrak{S} + \ldots + e_n\mathfrak{S} = \mathfrak{r}_1 + \ldots + \mathfrak{r}_n, \ (\mathfrak{r}_i = e_i\,\mathfrak{S}). \quad (20)$$

Inversamente, se $\mathfrak{S}$ tem elemento u e é soma directa de n ideais direitos $\mathfrak{r}_i$, pondo

$$u = e_1 + \ldots + e_n, \quad (e_i \in \mathfrak{r}_i),$$

os elementos e_i verificam as condições

$$e_i^2 = e_i, \quad e_i\,e_k = 0, \quad (i \neq k).$$

Sob a forma (20), $\mathfrak{S}$ revela-se como um módulo relativo a $\mathfrak{S}$ e com n geradores $e_1, \ldots, e_n$. Êstes geradores não constituem, todavia, uma base independente. Basta notar que se tem

$$e_i^2 = e_i, \quad e_i\,(e_i - u) = 0.$$

$\mathfrak{S}$ é uma soma directa de grupos cíclicos, cada um dos quais com uma base que se anula para elementos não nulos de $\mathfrak{S}$, elementos que constituem um ideal direito. Uma propriedade dêste ideal direito resulta das considerações que vão seguir-se (2).

Dum modo geral, dado um anel $\mathfrak{S}$, seja e um elemento idempotente: $e^2 = e$. Se designarmos com $\mathfrak{A}$ o conjunto dos elementos s para os quais $se = 0$; com $\mathfrak{B}$ o dos elementos s para os quais $es = 0$; e, com $\mathfrak{J}$, o dos elementos satisfazendo a $es = se = 0$, vê-se que, para cada $s \in \mathfrak{S}$, se tem

$$s = e(s - se) + (s - es)\,e + (s - es - se + ese) + \\ + ese, \quad (21)$$

---

(1) *Grupos abelianos e Anéis*, etc., Cap. VIII, pags. 107.

(2) Compare com L. E. Dickson, *Algebras and their Arithmetics*, Chicago, University Press, 1923.

com $s - se \in \mathfrak{A}$, $s - es \in \mathfrak{B}$, $s - es - se + ese \in \mathfrak{J}$.

A soma (21) é directa, como vamos demonstrar. Se

$$s = a' + b' + c' + d',$$

com $a' \in e\mathfrak{A}$, $b' \in \mathfrak{B}e$, $c' \in \mathfrak{J}$, $d' \in e\mathfrak{S}e$, tem-se

$$ese = ed'e, \quad d' = ete, \quad (t \in \mathfrak{S}),$$

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

Conclui-se agora que se tem

$$es = ea' + ese, \quad a' = er, \quad (r \in \mathfrak{A}).$$

Daqui resulta

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

O raciocínio é análogo quanto a b'. Finalmente,

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

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

Diz-se decomposição de PEIRCE a decomposição

$$\mathfrak{S} = e\mathfrak{A} + \mathfrak{B}e + \mathfrak{J} + e\mathfrak{S}e. \tag{22}$$

Pode, de resto, demonstrar-se que $\mathfrak{A}$ se compõe dos elementos da forma $s - se$, em que $s \in \mathfrak{S}$. Disse-se já, na verdade, que $s - se \in \mathfrak{A}$. Inversamente, se $x \in \mathfrak{A}$, é $xe = 0$, e, conseqüentemente, $x = x - xe$.

Uma afirmação análoga tem lugar para $\mathfrak{B}$.

Da igualdade (22), tira-se

$$\mathfrak{S}e = e\mathfrak{A}e \cup \mathfrak{B}e \cup \mathfrak{J}e \cup e\mathfrak{S}e\,(1) = \mathfrak{B}e + e\mathfrak{S}e,$$

(1) Com $\cup$ significa-se soma não directa.

e, portanto,

$$\mathfrak{S} = e\mathfrak{A} + \mathfrak{S}e + \mathfrak{J}.$$

Ora consideremos a soma directa $e\mathfrak{A} + \mathfrak{J}$. Por um lado, se x pertence a esta soma, tem-se $xe = 0$, pelo que $x \in \mathfrak{A}$. Por outro lado, se $x \in \mathfrak{A}$, a decomposição (21) dá (pois $xe = 0$)

$$x = e(x - xe) + (x - ex),$$

decompondo x numa soma de dois elementos, respectivamente pertencentes a $e\mathfrak{A}$ e $\mathfrak{J}$. Logo é

$$e\mathfrak{A} + \mathfrak{J} = \mathfrak{A},$$

$$\mathfrak{S} = \mathfrak{S}e + \mathfrak{A} = e\mathfrak{S} + \mathfrak{B}. \tag{23}$$

As decomposições (23) dizem-se, respectivamente, *decomposição esquerda* e *decomposição direita* de PEIRCE. Sob esta forma, aparece $\mathfrak{S}$ como soma de dois ideais esquerdos ou direitos.

Pode, assim, enunciar-se o teorema: *se* e *é idempotente, tem-se*

$$\mathfrak{S} = e\mathfrak{S} + \mathfrak{B},$$

como soma de dois ideais direitos, valendo,

$$\textit{para } x \in e\mathfrak{S}, \quad ex = x; \quad \textit{para } x' \in \mathfrak{B}, \quad ex' = 0.$$

No caso da decomposição (20), se $\mathfrak{B}_1$ é o ideal direito que anula e_1, vê-se que

$$\mathfrak{B}_1 \subseteq e_2\mathfrak{S} + \ldots + e_n\mathfrak{S}.$$

Inversamente, se $b_1 \in \mathfrak{B}_1$, pondo

$$b_1 = ub_1 = e_1b_1 + e_2b_1 + \ldots + e_nb_1,$$

vê-se que é

$$b_1 = e_2b_1 + \ldots + e_nb_1,$$

pelo que se terá

$$\mathfrak{B}_1 = e_2\mathfrak{S} + \ldots + e_n\mathfrak{S}.$$

16) **Anéis com n^2 matrizes unidades** — No que vai seguir-se, o anel $\mathfrak{S}$, além de possuir elemento u, contém n^2

elementos e_{ik} (matrizes unidades) verificando as relações seguintes:

1.ª) $e_{ik}\, e_{jl} = \delta_{kj}\, e_{il}$, $\begin{cases} \text{com } \delta_{kj} = 0, \text{ se } k \neq j, \\ \delta_{kj} = u, \text{ se } k = j; \end{cases}$

2.ª) $u = e_{11} + e_{22} + \ldots + e_{nn}$;

3.ª) $\mathfrak{S}\, e_k\, \mathfrak{S} = \mathfrak{S}, \quad (k = 1, 2, \ldots, n), \quad (e_k = e_{kk})$.

Ponhamos $\mathfrak{S}_{ij} = e_{ii}\, \mathfrak{S}\, e_{jj} = e_i\, \mathfrak{S}\, e_j$. Vê-se imediatamente que se tem

$$\mathfrak{S} = \sum_i e_i\, \mathfrak{S}, \quad e_i\, \mathfrak{S} = \sum_j e_i\, \mathfrak{S}\, e_j, \quad \mathfrak{S} = \sum_{i,j} \mathfrak{S}_{ij},$$

onde os somatórios se referem a somas directas. Os sub-anéis $\mathfrak{S}_{ij}$ verificam as igualdades

$$\mathfrak{S}_{ij}\, \mathfrak{S}_{kl} = \delta_{jk}\, \mathfrak{S}_{il}.$$

Os sub-anéis $\mathfrak{S}_{ii}$ admitem e_i como elemento um e nunca se reduzem ao único elemento nulo. As igualdades

$$\mathfrak{S}_{ij}\, \mathfrak{S}_{ji} = \mathfrak{S}_{ii}$$

mostram que os $\mathfrak{S}_{ij}$ também não podem reduzir-se a (0).

Seja $x_{11} \in \mathfrak{S}_{11}$. Façamos corresponder a x_{11} o elemento $a \in \mathfrak{S}$,

$$a = \sum_i e_{i1}\, x_{11}\, e_{1i}.$$

Esta correspondência é biunívoca. De facto, a x_{11} corresponde um elemento a bem determinado. Inversamente, a todo o elemento a da forma anterior, onde $x_{11} \in \mathfrak{S}_{11}$, corresponde um x_{11} bem determinado, pois

$$e_{11}\, a\, e_{11} = e_{11}\, x_{11}\, e_{11} = x_{11}.$$

O conjunto $\mathfrak{A}$ dos elementos a constitui um anel isomorfo de $\mathfrak{S}_{11}$:

$$x_{11} \to a = \sum_i e_{i1} x_{11}\, e_{1i}, \quad x_{11} + y_{11} \to \sum_i e_{i1}(x_{11} + y_{11})\, e_{1i} = a + b,$$

$$y_{11} \to b = \sum_i e_{i1}\, y_{11}\, e_{1i}, \quad x_{11}\, y_{11} \to \sum_i e_{i1}\, x_{11}\, y_{11}\, e_{1i} =$$

$$= \sum_i e_{i1}\, x_{11}\, e_{1i}\, e_{i1}\, y_{11}\, e_{i1} = \sum_i e_{i1}\, x_{11}\, e_{1i} \cdot \sum_i e_{i1}\, y_{11}\, e_{1i} = a\, b.$$

Em particular, ao elemento e_{11} corresponde

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

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

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

Um elemento $x \in \mathfrak{S}$ pode pôr-se sob a forma

$$x = \sum_{p,q} \chi_{pq}\, e_{pq}, \qquad \chi_{pq} = \sum_i e_{ip}\, x\, e_{qi},$$

pois

$$\sum_{p,q} \chi_{pq}\, e_{pq} = \sum_{p,q,i} e_{ip}\, x\, e_{qi}\, e_{pq} = \sum_{p,q} e_{pp}\, x\, e_{qq} = \sum_p e_{pp}\, x = x.$$

Os coeficientes χ_{pq} comutam com todos os e_{ij}:

$$\chi_{pq}\, e_{ij} = \sum_k e_{kp}\, x\, e_{qk}\, e_{ij} = e_{ip}\, x\, e_{qj} = e_{ij}\, e_{jp}\, x\, e_{qj} =$$

$$= e_{ij} \sum_k e_{kp}\, x\, e_{qk} = e_{ij}\, \chi_{pq}.$$

Mas, escrevendo

$$\chi_{pq} = \sum_i e_{i1} \cdot e_{1p}\, x\, e_{q1} \cdot e_{1i},$$

vê-se que $\chi_{pq} \in \mathfrak{A}$.

Isto significa que o anel $\mathfrak{S}$ se pode considerar como um módulo finito relativamente ao anel $\mathfrak{A}$.

A representação de cada elemento de $\mathfrak{S}$ é, então, única. De facto, vamos vêr que uma igualdade do tipo

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

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

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

$$e_{kl} \sum_p a_{pi}\, e_{pj} = e_{kl} \sum_p a'_{pi}\, e_{pj}, \qquad a_{li}\, e_{kj} = a'_{li}\, e_{kj}, \qquad a_{li}\, e_{kk} = a'_{li}\, e_{kk},$$

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

quaisquer que sejam l e i, como se deseja.

Atendendo a que se tem

$$\gamma_{pq}\, e_{pq} = \sum_i e_{ip}\, x\, e_{qi}\, e_{pq} = e_{pp}\, x\, e_{qq} \in \mathfrak{S}_{pq},$$

pode agora afirmar-se que é $\mathfrak{S}_{pq} = \mathfrak{A}\, e_{pq}$. Com WEDDERBURN, diz-se que $\mathfrak{S}$ é o produto directo de $\mathfrak{A}$ pelo sistema dos e_{ik}.

Procuremos ainda os elementos de $\mathfrak{S}$ que comutam com todos os e_{ik}. Se x é um tal elemento, vem

$$e_{ij}\, x = \sum_{p,q} e_{ij}\, \gamma_{pq}\, e_{pq} = \sum_{p,q} \gamma_{pq}\, e_{ij}\, e_{pq} = \sum_q \gamma_{jq}\, e_{iq},$$

$$x\, e_{ij} = \sum_{p,q} \gamma_{pq}\, e_{pq}\, e_{ij} = \sum_p \gamma_{pi}\, e_{pj},$$

$$\sum_q \gamma_{jq}\, e_{iq} = \sum_p \gamma_{pi}\, e_{pj},$$

o que leva a $q = j$, $p = i$, $\gamma_{jj} = \gamma_{ii}$, $\gamma_{jl} = 0$, $(j \neq l)$.

Por aqui se vê que x é da forma

$$x = \Sigma\, \gamma\, e_{ii} = \gamma, \text{ com } \gamma \in \mathfrak{A}.$$

Podemos enunciar o teorema seguinte: *sob as três condições indicadas, o anel* $\mathfrak{S}$ *é um módulo finito (produto directo de* WEDDERBURN*) com respeito aos elementos de* $\mathfrak{S}$ *que comutam com as matrizes unidades, as quais representam uma base correspondente de* $\mathfrak{S}$.

E podemos afirmar ser n^2 uma dimensionalidade de $\mathfrak{S}$ relativamente a $\mathfrak{A}$.

Casos importantes em que se realizam as três condições enunciadas no começo dêste § podem vêr-se na memória de E. NOETHER, «*Hyperkomplexe Grössen und Darstellungstheorie*», Band 29, da *Mathematische Zeitschrift*, 1929, ou num trabalho de E. ARTIN «*Zur Arithmetik der hyperkomplexen Systeme*», *Abhandlugen des mathematischen Seminars*, Hamburg, Band 5, 1927.

No nosso livro «*Grupos Abelianos e Anéis*, etc.», Cap. IX, págs. 128 e seguintes, e Cap. X, págs. 163 e seguintes, referimo-nos largamente ao conteúdo dos dois escritos que acabamos de referir.

Centro de Estudos de Matemática
da Faculdade de Ciências do Pôrto,
Junho de 1942.