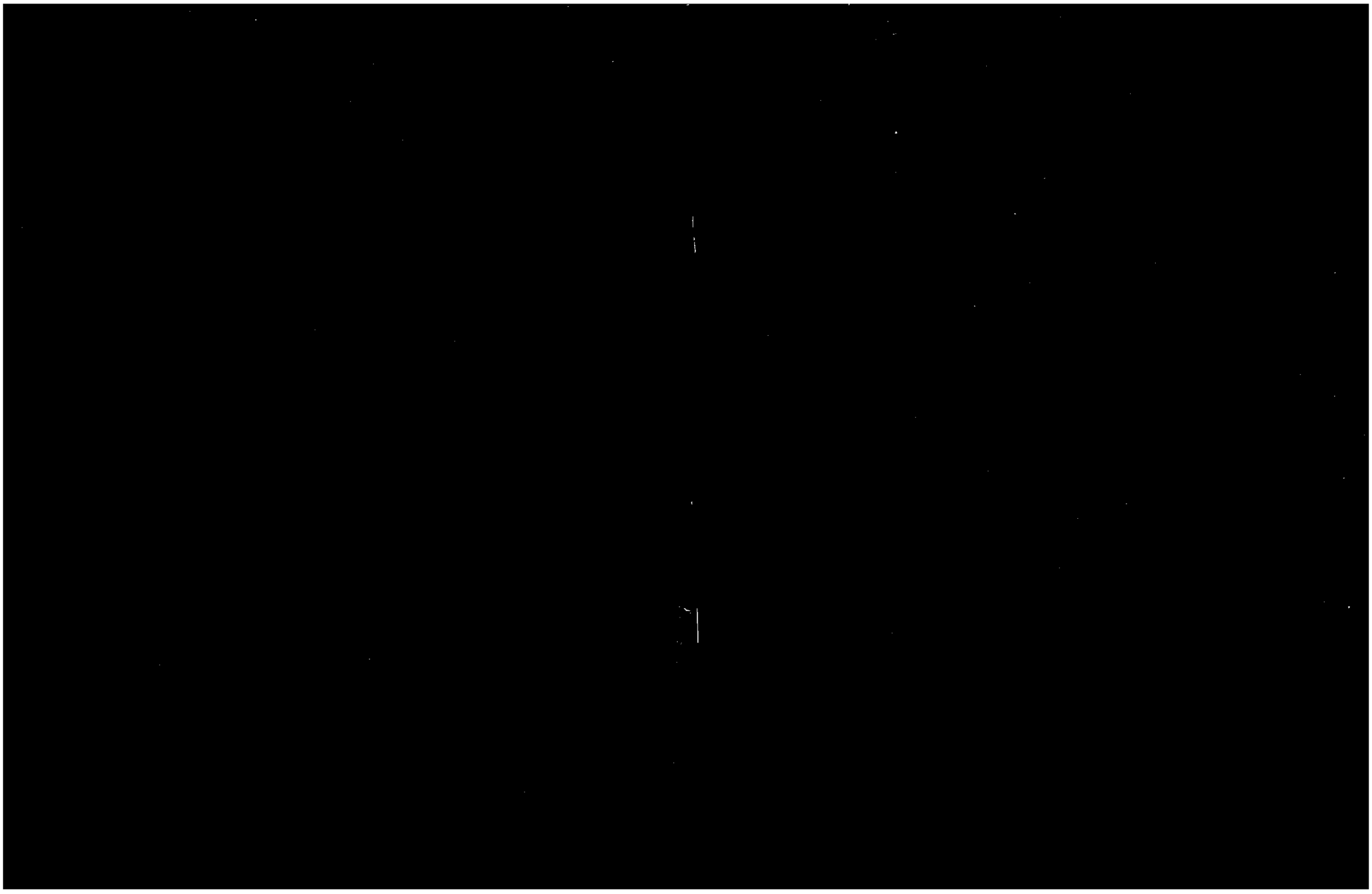

ÁLGEBRA MODERNA

1.º caderno

GRUPOS

Capítulo I

POSTULADOS, REGRAS DE CÁLCULO, SUB-GRUPOS

1) POSTULADOS -O conjunto não vazio $\mathcal{G} = \{a,b,c,...\}$ diz-se um grupo, se se verificam os quatro postulados a seguir. I) De $a,b \in \mathcal{G}$ deduz-se, por um processo determinado, um produto $a.b = ab = c \in \mathcal{G}$. II) Existe uma unidade direita, u, tal que $au = a$, qualquer que seja $a \in \mathcal{G}$. III) Existe um inverso direito, α, de cada $a \in \mathcal{G}$. Isto significa $a\alpha = u$. Escreveremos $\alpha = a^{-1}$. IV) Se $a,b,c \in \mathcal{G}$, vale a relação $ab = ac.c^{-1}b$.

2) CONSEQUÊNCIAS -O inverso direito dum elemento é também inverso esquerdo do mesmo elemento. Para o vêr, designemos com b um inverso direito de a^{-1}, de modo que $a^{-1}b = u$. Então é $a^{-1}a.a^{-1}b = a^{-1}a.u = a^{-1}a = a^{-1}b = u$. Assim, como se deseja, é, simultaneamente, $a^{-1}a = u$, $aa^{-1} = u$.

Uma unidade direita é também unidade esquerda. Tem-se, de facto, $bb^{-1}.bu = u.bu = ub = bu = b$.

A última consequência que queremos indicar nêste § é a que traduz a propriedade associativa: $a.bc = ab.c$. O quarto postulado dá, pondo $b = u$, e, depois, $a = u$,

$$a = ac.c^{-1}, \qquad b = c.c^{-1}b$$

Daqui se tira

$$a.bc = (ab.b^{-1}).bc = ab.c.$$

O 4.º postulado pode substituir-se introduzindo a propriedade associativa, pois $ac.c^{-1}b = (a c.c^{-1}) b = (a.c c^{-1})b = a b$.

3) O COCIENTE DE DOIS ELEMENTOS -Dados $a, b \in \mathcal{L}$, existem elementos x, y em $\mathcal{L}$ tais que

$$x a = b, \qquad a y = b. \tag{1}$$

De facto, tem-se

$$x = b a^{-1}, \qquad y = a^{-1} b.$$

Estas soluções são únicas. Se, por ex., $x a = x' a = b$, vê-se que

$$x a a^{-1} = x = x' a a^{-1} = x'.$$

Conclui-se daqui (tendo em conta que as equações $x a = a$, $a y = a$ são satisfeitas pondo $x = u$, $y = u$) que há uma só unidade direita, a qual é também a única unidade esquerda. De futuro, representaremos com u essa unidade, que se diz elemento um do grupo.

As equações $a y = u$, $x a = u$, que se resolvem com $y = a^{-1}$ e $x = a^{-1}$ mostram que há um só inverso direito, que é também o único inverso esquerdo.

Com a^{-1} representaremos, de futuro, êsse único inverso.

4) OUTRA FORMA DOS POSTULADOS -A solubilidade de (1), no grupo, pode constituir um postulado capaz de substituir II) e III), se o postulado IV) se substituir pela propriedade associativa. Consideremos, na verdade, a equação $a y = a$. Se u fôr uma solução, vamos ver que é uma unidade direita. Seja $c \in \mathcal{L}$. Por hipótese é $a u = a$. Então, se x é uma solução de $x a = c$, tem-se $x a . u = c u = x . a u = x a = c$, como se deseja. Em segundo lugar, consideremos a equação $bx = u$.

Se designarmos com β uma solução, êste elemento é um inverso direito de b, valendo $b \beta = u$.

5) SEMI-GRUPOS -Se num conjunto não vazio $\mathcal{L}$ existe um produto associativo e se as equações (1) admitem, quando muito, uma solução no conjunto, êste diz-se um semi-grupo. Nêste caso, das relações $a x = a x'$, $y a = y' a$ tira-se $x = x'$, $y = y'$.

Um semi-grupo com um número finito de elementos é um grupo. Se, com efeito, $a \in \mathcal{L}$ é fixo e x percorre $\mathcal{L}$, os elementos ax são tôdos distintos.

O número de elementos ax é igual ao número de elementos x, pelo que a equação $a x = b$ será sempre solúvel. O mesmo se diz da equação $y a = b$.

6) GRUPOS FINITOS -No caso dos conjuntos finitos, podemos enunciar os postulados como segue: I) existe um produto; II) o produto é associativo; III) as relações $ax = ax'$, $ya = y'$ arrastam, respectivamente, $x = x'$, $y = y'$.

De facto, um tal conjunto é um semi-grupo finito.

7) GRUPOS ABELIANOS -Diz-se abeliano ou comutativo um grupo para o qual é $a.b = b.a$. Não se distinguem, então, as multiplicações à direita e à esquerda. É costume empregar o sinal + para representar o produto e designar o grupo como grupo abeliano aditivo ou módulo. O elemento um indica-se com 0 (leia zero) e o inverso de a com $-a$. Escreve-se assim:

$$(a + b) + c = a + (b + c), \qquad a + o = a,$$

$$a + (-a) = a - a = 0.$$

A solução de $a + x = b$ que é $x = b + (-a)$ escreve-se sob a forma $x = b - a$, de modo que se tem $a + (b - a) = b$.

8) A TABELA DO GRUPO -Um grupo finito considera-se conhecido logo que se tenha uma tabela na qual se possa encontrar o produto de dois quaisquer dos seus elementos. Ex:

	u	a
u	u	a
a	a	u

;

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

A construção das linhas horizontais e verticais da tabela obedece a regras que traduzem precisamente o enunciado dos quatro postulados do § 1. Relativamente ao quarto postulado, confronte-se com o que sugere o quadro.

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

Pode verificar-se que tôdas as tabelas possíveis com grupos até 5 elementos levam a grupos abelianos.

Só a partir de 6 elementos se constroem grupos não abelianos.

9) GRUPO DE TRANSFORMAÇÕES -Definamos uma transformação. Consideremos as n equações

$$y_i = f_i(x_1,\ldots,x_n), \qquad (i = 1, 2, \ldots, n), \qquad (2)$$

que permitem passar dum sistema de valôres x_i para

um sistema de valôres y_i (imagem daquele). Diz-se que se tem uma transformação T, se a imagem y_i é bem determinada, e se, inversamente, existe um campo determinado dos y_i, tal que cada sistema de valôres destas variáveis pertencentes ao campo é sempre imagem dum único elemento do campo correspondente dos x_i.

O produto T'T de duas transformações como (2) define-se do modo a seguir. Por comodidade, utilizaremos uma única letra x, ou y, ou z, para significar um sistema de n quantidades x_i, ou y_i, ou z_i.

Então, dado x no seu campo, a transformação T far-lhe-á corresponder $y = T(x)$; em seguida, a transformação T' dará $z = T'(y) = T'(T(x))$. Escreveremos $z = T'T(x)$ para definição do produto das duas transformações. É bom frisar que o símbolo T'T significa que se efectua primeiramente T, depois T'. Se se utilizasse o símbolo TT' com tal significado, conviria escrever $z = (x)TT'$.

Vamos supôr que as relações (2) dão uma imagem do campo dos xx sôbre si mesmo, de modo que os yy são os xx num arranjo diferente, o mesmo se dizendo dos zz definidos por $z = T'(y)$.

No tipo das transformações (2) entra a transformação unidade (ou idêntica) $y = x$.

Resolvendo (2) em ordem aos xx, o que é possível por hipótese, encontra-se

$$x_i = \varphi_i(y_1,\ldots,y_n), \qquad (i = 1, 2, \ldots, n). \qquad (3)$$

A transformação (3) diz-se inversa de (2), quando se escreve

$$y_i = \varphi_i(x_1,\ldots,x_n),$$

a fim de (2) e (3) se aplicarem ao mesmo sistema de elementos. Se tivermos em conta as igualdades

$$y_i = f_i\left[\varphi_1(y),\ldots,\varphi_n(y)\right], \qquad x_i = \varphi_i\left[f_1(x),\ldots,f_n(x)\right],$$

e designarmos com T^{-1} a transformação inversa de T, vê-se que é $TT^{-1}(x) = T^{-1}T(x) = x$.

No conjunto das possíveis transformações (2) figuram, assim, a transformação unidade, o produto de duas transformações e a inversa duma transformação.

O 4.º postulado da teoria dos grupos é verificado, pois, se S e V forem outras transformações, é $TS.S^{-1}V(x) = TV(x)$.

O conjunto das transformações (2), sob a restrição imposta de transformar o campo dos xx nêsse mesmo campo, constitui um grupo de transformações. Em particular, ficamos sabendo que as transformações gosam da propriedade associativa.

Imaginemos um conjunto de transformações gosando das duas propriedades seguintes: 1ª - contém a transformação inversa de cada transformação que lhe pertence; 2ª - contém o produto de duas das suas transformações; tal conjunto constitui um grupo.

Um exemplo importante de grupo de transformações é constituido pelo grupo das substituições de n letras, também designado grupo simétrico $\mathfrak{S}_n$.

10) REGRAS DE CÁLCULO - Do produto $a_1\ a_2$ de dois elementos, passa-se ao produto $a_1\ a_2\ a_3 = a_1\ a_2 . a_3$ de 3 elementos; e, duma maneira geral, do produto de n-1 elementos, passa-se ao produto de n elementos por meio da igualdade

$$a_1\ a_2 \dots a_n = a_1 \dots a_{n-1} . a_n .$$

Dados $A = a_1 \dots a_n$, $B = a_{n+1} \dots a_p$, $(p \geqslant n+2)$ é

$$AB = a_1\ a_2 \dots a_p .$$

A potência n de a define-se pela igualdade

$$a^n = a \dots a \quad \text{(com a repetido n vezes)}.$$

É válida a relação $a^n . a^m = a^{n+m}$.

Por indução, demonstra-se a igualdade $(a^n)^m = a^{nm}$.

A extensão das regras de cálculo às potências de expoente nulo e negativo faz-se como vai ver-se.

Para o expoente zero, põe-se $a^0 = u$; e, para um expoente negativo, escreve-se, por definição,

$$a^n . a^{-n} = u,$$

igualdade que é válida para n=1, conforme convenção anterior.

São fàcilmente demonstráveis as relações

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

usando o método de indução.

No caso de grupos aditivos têm lugar as igualdades

$$a_1 + a_2 + \dots + a_n = (a_1 + \dots + a_{n-1}) + a_n ;$$

$$A + B = a_1 + \dots + a_p , \text{ com } \begin{cases} A = a_1 + \dots + a_n , \\ B = a_{n+1} + \dots + a_p ; \end{cases} \quad (p \geqslant n+2)$$

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

$na + ma = (n+m)a$; $m.na = mna$;

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

$n\,a + (-n.a) = 0$; $-n.a = n\,(-a) = -n\,a$;

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

$-m.(-n\,a) = m\,n\,a$.

11) CRITÉRIO DE SUB-GRUPO -Se uma parte, $\mathcal{Y}$, dum grupo $\mathcal{G}$, forma grupo, diz-se que $\mathcal{Y}$ é sub-grupo de $\mathcal{G}$.

Como a propriedade associativa é uma propriedade necessária em $\mathcal{Y}$, vê-se que $\mathcal{Y}$ é sub-grupo quando verifica as condições: 1ª- com a e b, contém ab; 2ª- com a e b, contém a solução única das equações $ax = b$, $ya = b$. Estas duas condições são, porém superabundantes. Vê-se imediatamente que basta a seguinte: $\mathcal{Y}$ é sub-grupo, se, com a e b, contém a solução única de $xa = b$. Como essa solução é ba^{-1}, podemos dizer ainda: $\mathcal{Y}$ é sub-grupo, se, com a e b, contém ba^{-1} ou (ab^{-1}).

Quando $\mathcal{Y}$ é uma parte de $\mathcal{G}$, diz-se sub-grupo próprio ou autêntico. O elemento u constitui, por si só, um sub-grupo de $\mathcal{G}$. É o grupo unidade.

No caso de grupos finitos, o critério de sub-grupo pode enunciar-se assim: $\mathcal{Y}$ é sub-grupo, se, com a e b, contém ab. Então, com efeito, $\mathcal{Y}$ é um semi-grupo finito.

São sub-grupos do grupo simétrico $\mathcal{G}_n$ tôdos os grupos simétricos $\mathcal{G}_r$, com $r \leqslant n$. O conjunto de tôdas as substituições pares de $\mathcal{G}_n$ constitui o grupo alterno $\mathcal{A}_n$.

12) INTERSECÇÃO DE SUB-GRUPOS -Dado um sub-grupo de $\mathcal{G}$, que pode ser o próprio grupo, consideremos alguns dos seus elementos a,b,c,..., em número finito ou infinito. Os referidos elementos podem pertencer ou não a outros sub-grupos. É nosso objectivo procurar os elementos comuns a tôdos os sub-grupos que contêem os elementos em questão e verificar que êsses elementos comuns constituem um sub-grupo mínimo $\mathcal{J}$. A intersecção $\mathcal{J}$ contém, certamente, tôdos os

elementos da forma $a^{r_1} \ldots b^{s_1} \ldots a^{-r'_1} \ldots b^{-s'_1} \ldots$, aos quais correspondem inversos da forma $\ldots b^{s'_1} \ldots \ldots a^{r'_1} \ldots b^{-s_1} \ldots a^{-r_1}$. Êstes elementos são constituidos pelo produto dum número finito de factores que são potências de a,b,c,... . Êles constituem um sub-grupo $\mathcal{J}$, que contém os elementos a,b,c,..., pertencendo $\mathcal{J}$ a tôdo o sub-grupo que contenha a,b,c,... . Será, assim, $\mathcal{J} = \mathcal{J}$ um sub-grupo mínimo, q. e. d.

$\mathcal{J}$ diz-se grupo gerado pelos elementos a,b,c,...

13) GRUPOS CÍCLICOS -Tomemos $a \in \mathcal{G}$. O sub-grupo gerado por a diz-se um grupo cíclico. Pode suceder que tôdas as potências de a sejam distintas ou que haja algumas iguais. Nêste último caso o grupo cíclico é finito, podendo os seus elementos representar-se pelas n potências seguintes de a.

$$a^0 = u,\quad a^1 = a,\quad a^2,\ \ldots,\ a^{n-1} \qquad (4)$$

Sejam p e q dois números inteiros tais que $p > q$ e para os quais $a^p = a^q$. Então é $a^{p-q} = u$, com $p - q > 0$. Se designarmos com n o menor número positivo para o qual $a^n = u$, n satisfaz às condições do enunciado. Para o vêr, prova-se serem distintas tôdas as potências (4), e mostra-se que, qualquer que seja o inteiro s, existe sempre um inteiro k, satisfazendo a $0 \leqslant k < n$, para o qual $a^k = a^s$.

O número positivo n diz-se ordem de a. Se o grupo cíclico tem uma infinidade de elementos, a é de ordem infinita.

Tomemos um sub-grupo dum grupo cíclico: $\ldots, a^{-t}, \ldots, a^{-p}, \ldots, a^0 = u, \ldots, a^{p'}, \ldots, a^{t'}, \ldots$. Vamos provar que é também um grupo cíclico. Designemos com a^p a menor potência de expoente positivo que figura no sub-grupo. Será $p \neq 0$, de contrário o sub-grupo se-

ria o grupo unidade. Se $a^{v'}$, com $v'>p$, é outro elemento do sub-grupo, pondo $v' = pc+r$, com $o \leqslant r < p$, tem-se $a^{v'} = (a^p)^c . a^r$. Se fôsse $r \neq o$, a pertenceria ao sub-grupo, contra o suposto. Para uma potência de expoente negativo, a conclusão é a mesma, como se vê recorrendo ao inverso. O sub-grupo em causa é, assim, gerado por a^p.

No caso dos grupos cíclicos finitos, p é um divisor da ordem n de a. Se assim não fôsse, n estaria entre dois múltiplos consecutivos de p: $(k-1)p < n < kp$. A diferença $kp - n$ seria inferior a p, e, sendo $a^{kp-n} = a^{kp}.a^{-n} = a^{kp}$, o sub-grupo contemia uma potência inferior a p. Portanto, a potência a^p, de menor expoente, dum sub-grupo dum grupo cíclico, não pode ser de expoente p primo com n. É muito simples demonstrar a seguinte proposição: se a ordem dum elemento a dum grupo é igual a n, a ordem do elemento a^p, em que p é primo com n, é também igual a n. O facto de ser então o grupo gerado por a^p idêntico ao grupo cíclico dado permite enunciar êste outro teorema: pondo $a^p = b$, tôda a equação $b^x = a^r$ é solúvel em x.

14) RELAÇÕES DE EQUIVALÊNCIA -Caracterizado um conjunto, suponhamos que uma certa propriedade, a qual põe em jôgo um par de elementos a, b, pode ser ou não verificada por êsse par. Quando a propriedade se verifica, escreveremos $a \longrightarrow b$. Se o sinal $\longrightarrow$ satisfaz a axiomática

$a \longrightarrow a$ (propriedade reflexa);

de $a \longrightarrow b$, tira-se $b \longrightarrow a$ (propriedade simétrica);

de $a \longrightarrow b$ e $b \longrightarrow c$, tira-se $a \longrightarrow c$ (propriedade transitiva);

diz-se que define uma relação de equivalência.

Num conjunto C em que há uma relação de equivalência, um elemento $a \in C$ e tôdos os equivalentes, tais como b, se $a \longrightarrow b$, constituem uma classe de equivalentes, C. Tôdo o elemento de C pertence sempre a uma classe, a qual pode ser constituida apenas por êsse elemento. Mas, se vários elementos a, b, ... pertencem a uma classe, esta é independente do elemento que serve para a definir: $C_a = C_b = \ldots$. Duas classes ou são estranhas, isto é, não têm elemento comum, ou têm um elemento comum. Nêste último caso são idênticas.

Uma relação de equivalência permite, pois, dividir um conjunto em classes de elementos estranhos. Inversamente, seja um conjunto C do 2º grau, no qual os seus elementos são conjuntos C', C", ... de elementos sem elemento comum; então, em C, definamos a relação $a \longrightarrow b$ considerando que $a \longrightarrow b$, se a e b pertencem ao mesmo conjunto C', ou C", etc. Vê-se que o sinal $\longrightarrow$ define em C uma relação de equivalência.

15) COMPLEXOS ASSOCIADOS DUM SUB-GRUPO -Dados $\mathcal{G}$ e $\mathcal{g}$, seja $a \in \mathcal{G}$. Em $\mathcal{G}$ fica definida uma relação de equivalência, pondo $a \longrightarrow b$, se $b \in a\mathcal{g}$. Ao conjunto dos elementos $a\mathcal{g}$ chamamos complexo ou classe associada de $\mathcal{g}$. É, de resto, uma classe esquerda, para a distinguir duma classe, como $\mathcal{g}a$, que se diz direita. Por meio da relação de equivalência em causa, pode dividir-se um grupo em classes estranhas de elementos que são associados dum seu sub-grupo. Poremos, assim:

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

Se tivermos em conta a igualdade $(ab)^{-1} = b^{-1}a^{-1}$ e o facto de ser $\mathcal{g}^{-1} = \mathcal{g}$, vemos ser $(a\mathcal{g})^{-1} = \mathcal{g}a^{-1}$. Conclui-se que, a partir das classes esquerdas, se obtêm tôdas as classes direitas. Ao número de classes associadas, que pode ser finito ou infinito, chama-se índice do sub-grupo.

16) ORDEM DUM ELEMENTO -No caso dum grupo finito, a decomposição em classes do § anterior permite afirmar o seguinte

TEOREMA:-O número de elementos dum grupo, ou ordem do grupo, é dividido pela ordem e pelo índice dum sub-grupo.

Consideremos um elemento a de ordem p, pertencente a um grupo de ordem n. Tem-se $a^p = u$, $a^{pq} = a^n = (a^p)^q = u$. Para qualquer elemento a do grupo, vale a igualdade $a^n = u$.

TEOREMA:-Se p e q são dois números primos entre si e se a e b são elementos comutáveis do grupo, de ordem p e q, respectivamente, o produto ab é de ordem pq. Por hipótese, tem-se $a^p = u$, $b^q = u$, $(ab)^{pq} = u$. Por isso, pq pode ser a ordem de ab. Vejamos que essa ordem não pode ser $h < pq$. Se fôsse $a^h . b^h = u$, ou $a^h = b^{-h} = d$, d pertenceria aos dois grupos cíclicos gerados por a e b. A ordem de d, como divisor comum de p e q, seria 1, e tinha-se $d = u$, $a = u$. O número h seria múltiplo de p e também múltiplo de q, pelo menos igual a pq.

17) ALGUMAS PROPRIEDADES DOS GRUPOS CÍCLICOS

Consideremos um grupo cíclico de ordem $n = tm$, em que t e m são primos entre si, e seja a o elemento gerador. Vamos demonstrar o

TEOREMA:-a pode representar-se sempre, e duma maneira única, como produto de dois elementos do grupo cíclico, de ordem t e m, respectivamente. Ponhamos $a^t = \tau$, $a^m = \beta$. A ordem de τ é precisamente m, pois que $a^{tm} = \tau^m = u$, não podendo ter-se $\tau^{m'} = u$, com $m' < m$. Analogamente se demonstra ser t a ordem de β. Consideremos, então, os produtos $\beta^r \tau^s$, com $r = 1,2,\ldots,t$; $s = 1,2,\ldots m$. São em número de tm e tôdos diferentes, visto que a relação $\beta^r \tau^s = \beta^{r'} \tau^{s'}$, ou $\beta^{r-r'} = \tau^{s'-s} = d$, mostraria ser d um elemento dos grupos cíclicos gerados por β e τ, e, portanto, mostraria ser $d = u$, pelo facto de a ordem de d ter de dividir t e m. De $d = u$ resultaria em seguida, $r = r'$, $s = s'$.

Concluimos a existência de dois números inteiros $r_1 < t$, $s_1 < m$, tais que $\beta^{r_1} \tau^{s_1} = a^{m r_1 + t s_1} = a$. Não podendo a soma $mr + ts$ ser superior a $2tm$, vê-se que é $ts_1 + mr_1 = tm+1$, ou $ts_1 + m(r_1 - t) = 1$, o que incidentalmente no mostra o seguinte: dados dois números primos entre si, t e m, existem números inteiros s' e r' tais que $ts' + mr' = 1$.

Pondo $\beta^{r_1} = a^{m r_1} = b$, $\tau^{s_1} = a^{t s_1} = c$, é $a = bc$. 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

$$(b\,c)^{t'm} = a^{t'm} = b^{t'm} . c^{t'm} = a^{t s_1 t' m} = u,$$

o que é absurdo, pelo facto de a ordem de a não ser inferior a tm. Vê-se, finalmente, que não pode haver duas potências a^p e a^q, diferentes das anteriores potências a^{mr_1} e a^{ts_1}, das ordens t e m, respectivamente, tais que $a^p . a^q = a$, raciocinando do modo seguinte. Se fôsse

$$a = a^p . a^q = a^{p+q} = a^{m r_1 + t s_1}, \quad a^{pt} = u, \quad a^{qm} = u,$$

ter-se-ia $a^{p+q-(m r_1 + t s_1)} = u$. Como a soma $p+q$ não chega a ser $2tm$ e $mr + ts = tm+1$, tem de ser $p+q = mr_1 + ts_1$. Sendo, por outro lado, $pt = ktm$, $qm = \varepsilon tm$, com k e ε inteiros, será $p = km$, $q = \varepsilon t$, $m(k - r_1) = t(s_1 - \varepsilon)$, e, portanto, $k = r_1 + \alpha t$, $\varepsilon = s_1 + \alpha m$, com α inteiro. E conclui-se

$$a^p = a^{km} = a^{r_1 tm + \alpha tm} = a^{r_1 m},$$

$$a^q = a^{et} = a^{s_1 t + \alpha tm} = a^{s_1 t}, \qquad \text{q.e.d.}$$

Dum modo geral, seja N a ordem dum grupo cíclico qualquer gerado por a. Pondo $N = p_1^{r_1} \ldots p_s^{r_s}$, onde $p_1, \ldots, p_s$ são números primos diferentes, vê-se que a é o produto de s elementos bem determinados do grupo cíclico, de ordens $p_1^{r_1}, \ldots, p_s^{r_s}$.

18) APLICAÇÃO A GRUPOS QUAISQUER - Num grupo $\mathcal{G}$ é válido o seguinte

TEOREMA: - Um elemento a de ordem tm, onde 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 do § anterior satisfazem ao enunciado. Vamos precisar, demonstrando que dois elementos, d e f, nas condições de b e c, são idênticos a êstes. Pondo $a = df$, $a^t = d^t f^t = f^t$, vê-se que f^t é uma potência de a. No grupo cíclico gerado por f, grupo que é da ordem m, por hipótese, o elemento f^t, cujo expoente é primo com m, gera o mesmo grupo que f. Portanto f é uma potência de f^t, ou ainda uma potência de a. De modo análogo se vê que d é também uma potência de a. Assim, a decomposição referida no teorema tem lugar no grupo cíclico gerado por a e apenas nêsse grupo. Por isso mesmo a decomposição é única.

Podemos enunciar a seguinte proposição geral:

TEOREMA: - Um elemento $a \in \mathcal{G}$, se fôr de ordem $N = p_1^{r_1} \ldots p_s^{r_s}$, é sempre o produto de s elementos comutáveis bem determinados do grupo, elementos que são potências de a e cujas ordens são, respectivamente, $p_1^{r_1}, \ldots, p_s^{r_s}$.

B I B L I O G R A F I A

A. SPEISER, Die theorie der Gruppen von endlicher Ordnung, 2ª edição, 1927, Springer, Berlim;

B. L. van der WAERDEN, Moderne Algebra, tomo 1º, 1930, Springer, Berlim;

SÉGUIER et POTRON, Théorie des groupes abstraits, 1938, fascículo XCI do "Mémorial des Sciences Mathématiques";

A. ALMEIDA COSTA, Elementos da teoria dos grupos, 1942, Centro de Estudos Matemáticos do Pôrto.