Á L G E B R A   M O D E R N A

2.º caderno

G R U P O S (continuação)

Capítulo II

HOMOMORFIAS

1) <u>DIVISORES NORMAIS OU SUB-GRUPOS INVARIANTES</u> - $\mathcal{G}$ e $\mathcal{J}$ serão sempre um grupo e um sub-grupo. $\mathcal{J}$ diz-se <u>divisor normal</u> ou <u>sub-grupo invariante</u>, se, para cada $a \in \mathcal{G}$, valer $a\mathcal{J} = \mathcal{J}a$. Esta mesma igualdade subsiste, se se utiliza outro elemento <u>b</u>, em vez de <u>a</u>, que pertença à classe $a\mathcal{J}$. Num grupo abeliano, todos os sub-grupos são divisores normais. Tôdo o sub-grupo de índice 2 é um divisor normal.

Se $\mathcal{J}$ é divisor normal de $\mathcal{G}$, é divisor normal de qualquer sub-grupo $\mathcal{L}$ de $\mathcal{G}$, compreendido entre $\mathcal{J}$ e $\mathcal{G}$.

Um grupo diz-se <u>simples</u> se os seus divisores normais se reduzem ao grupo unidade e ao próprio grupo.

2) <u>CENTRO DUM GRUPO</u> - Diz-se <u>centro</u> dum grupo o conjunto dos seus elementos que comutam com todos os elementos do grupo. O centro é um divisor normal abeliano.

3) <u>HOMOMORFIAS</u> -Duma maneira geral, chamaremos <u>domínio multiplicativo</u> um conjunto no qual se define um preceito de produto. Se $\mathcal{D}$ e $\overline{\mathcal{D}}$ fôrem dois domínios multiplicativos, distinguiremos entre <u>homomorfia</u> e <u>homomorfismo</u>, definindo aquele como uma correspondência entre elementos de $\mathcal{D}$ e de $\overline{\mathcal{D}}$, sob as condições seguintes: α)-a cada elemento de $\mathcal{D}$ corresponde um elemento bem determinado de $\overline{\mathcal{D}}$;
β)-ao produto de dois elementos de $\mathcal{D}$ corresponde o produto dos elementos correspondentes de $\overline{\mathcal{D}}$;
γ)-no geral, apenas uma parte de $\overline{\mathcal{D}}$ é utilizada como imagem dos elementos de $\mathcal{D}$.

Se a condição τ) é substituida pela seguinte: τ')-tôdo o conjunto $\overline{\mathfrak{M}}$ é utilizado como imagem, tem-se um homomorfismo. $\overline{\mathfrak{M}}$ será, então, uma imagem homomorfa de $\mathfrak{M}$, o que se representará com $\mathfrak{M}\sim\overline{\mathfrak{M}}$.

Numa homomorfia de $\mathfrak{M}$ sôbre $\overline{\mathfrak{M}}$, a parte $\overline{\mathfrak{M}}'$ de $\overline{\mathfrak{M}}$ utilizada como imagem determina um homomorfismo $\mathfrak{M}\sim\overline{\mathfrak{M}}'$.

Quando $\mathfrak{M}$ é um grupo, tôda a sua imagem homomorfa é igualmente um grupo. Ao elemento um do primeiro corresponde o elemento um do segundo, e a $a^{-1}\in\mathfrak{M}$ corresponderá $a'^{-1}\in\overline{\mathfrak{M}}$, se a' é o correspondente de a.

Tendo-se um homomorfismo de $\mathfrak{M}$ sôbre $\overline{\mathfrak{M}}$ e dêste sôbre $\mathfrak{M}^*$, pode definir-se um homomorfismo de $\mathfrak{M}$ sôbre $\mathfrak{M}^*$, por intermédio de $\overline{\mathfrak{M}}$. Assim, a relação de homomorfismo é transitiva. A referida relação é também reflexa, pois, podemos imaginar os elementos de $\mathfrak{M}$ como as suas próprias imagens.

Anàlogamente, distinguiremos entre isomorfia e isomorfismo, definindo aquela sob as condições seguintes: α)-condições α) e β) da homomorfia; β)-os elementos de $\overline{\mathfrak{M}}$ que são utilizados como imagem são-no apenas uma vez. No isomorfismo, utiliza-se tôdo o conjunto $\overline{\mathfrak{M}}$ como imagem, sob as condições da isomorfia.

A relação de isomorfismo é reflexa, simétrica e transitiva.

Consideremos o caso dum grupo. A isomorfia dum grupo sôbre si mesmo diz-se meromorfia. O isomorfismo dum grupo sôbre si mesmo diz-se automorfismo.

Façamos uma observação. Tomemos um grupo cíclico infinito gerado por a e consideremos a correspondência $a^r \longrightarrow a^{2r}$, que define uma meromorfia. Por meio dela fica determinado um isomorfismo entre o grupo e um sub-grupo. Diz-se meromorfismo um tal isomorfismo.

TEOREMA:-Se um grupo possui um meromorfismo autêntico $\mathcal{G}\cong\sigma\mathcal{G}$, o grupo admite a sucessão infinita de sub-grupos

$$\mathcal{G}\supset\sigma\mathcal{G}\supset\sigma^2\mathcal{G}\supset\ldots,$$

sem existência de sinal = . Com o símbolo $\sigma\mathcal{G}$ significamos, é claro, o resultado da aplicação da operação do meromorfismo aos elementos de $\mathcal{G}$. Por hipótese é $\mathcal{G}\supset\sigma\mathcal{G}$. Então é, necessàriamente, $\sigma\mathcal{G}\supset\sigma^2\mathcal{G}$, porque, sendo $\mathcal{G}\cong\sigma\mathcal{G}$, aos elementos $\sigma\mathcal{G}$, pertencentes a $\mathcal{G}$, corresponderão os elementos $\sigma^2\mathcal{G}$, de $\sigma\mathcal{G}$, que não podem abranger a totalidade dêste último, visto que esta corresponde a $\mathcal{G}$.

Corolário:- Num grupo finito não pode haver um meromorfismo autêntico.

Um homomorfismo do domínio $\mathfrak{M}$ sôbre si mesmo, diz-se um endomorfismo.

4) GRUPOS COM OPERADORES -A noção de grupo com operadores é devida a W.Krull e O.Schmidt. Tomemos $\mathcal{G}=\{u,a,b,\ldots\}$ e consideremos o conjunto de símbolos $\mathfrak{L}=\{\ominus,\Phi,\ldots\}$ realizando as condições seguintes: 1ª)-com a e $\ominus$ define-se um produto $\ominus a\in\mathcal{G}$; 2ª)-tem lugar a igualdade $\ominus(ab)=\ominus a.\ominus b$; diz-se que o grupo $\mathcal{G}$ admite os operadores do domínio operatório $\mathfrak{L}$.

No caso dum grupo abeliano, a condição segunda reveste-se do aspecto habitual duma propriedade distributiva: $\ominus(a+b)=\ominus a+\ominus b$. Os números inteiros, por ex., constituem um domínio operatório de qualquer módulo.

Em tôdos os casos, a transformação $a\longrightarrow\ominus a$, definida por $\ominus$, é um endomorfismo do grupo. Os teoremas da teoria geral dos grupos, nos quais intervêm as noções de sub-grupo e de divisor normal, podem transportar-se aos grupos com operadores, mediante as restricções seguintes: α)-como sub-grupos apenas se consideram os sub-grupos admissíveis γ, ou seja aqueles que, com a, contêm Θa, qualquer que seja $\Theta \in \mathcal{L}$; β)-como divisores normais apenas se consideram, nas mesmas condições, os divisores normais admissíveis.

Visto que $a \longrightarrow \Theta a$ é um endomorfismo, tem-se imediatamente:

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

No caso dos módulos escrever-se-á

$$\Theta 0 = 0, \qquad \Theta(-a) = -\Theta a.$$

5) GRUPOIDES -Dado um domínio multiplicativo $\mathfrak{M}$, consideraremos indiferente dizer "endomorfismo de $\mathfrak{M}$" ou "operador de $\mathfrak{M}$". Estudemos o conjunto dos operadores de $\mathfrak{M}$. Nêsse conjunto há elemento um, o qual define precisamente a correspondência $a \longrightarrow a$, onde $a \in \mathfrak{M}$. Se Θ e Φ são dois operadores, define-se um produto $\Theta\Phi$, pondo $\Theta\Phi a = \Theta(\Phi a)$. Esta definição é legítima, pelo facto de definir um endomorfismo, como o mostram as igualdades seguintes:

$$\Theta\Phi(ab) = \Theta(\Phi(ab)) = \Theta(\Phi a \cdot \Phi b) = \Theta\Phi a \cdot \Theta\Phi b.$$

A propriedade associativa tem lugar, pois

$$(\Theta\Phi \cdot \Psi)\, a = \Theta\Phi(\Psi a) = \Theta(\Phi(\Psi a))$$

$$(\Theta \cdot \Phi\Psi)\, a = \Theta(\Phi\Psi a) = \Theta(\Phi(\Psi a))$$

Designando, então, por grupoide um conjunto de elementos no qual existe um preceito de produto associativo e elemento um, podemos enunciar o seguinte

TEOREMA:-Os operadores dum domínio multiplicativo constituem um grupoide.

Seja Q um conjunto de operadores de $\mathfrak{M}$. Diz-se prolongamento de Q, e representa-se com $\{Q\}$, o conjunto dos operadores de $\mathfrak{M}$ formado pelo operador um, 1, e pelos produtos, repetidos ou não, dos elementos de Q entre si e pelo operador 1. É claro que $\{Q\}$ é um grupoide. É o menor grupoide que contém 1 e Q.

6) AUTOMORFISMOS DUM GRUPO -Os automorfismos dum grupo $\mathcal{G}$ constituem um grupo $A_{\mathcal{G}}$, que é sub-grupo do grupo de transformações de $\mathcal{G}$.

Sejam $a \in \mathcal{G}$ um elemento fixo e x um elemento variável (qualquer). Consideremos em $\mathcal{G}$ a correspondência $x \longrightarrow x' = a\,x\,a^{-1}$. Fàcilmente se vê que ela define um automorfismo. Tais automorfismos dizem-se internos; os outros dizem-se externos.

No caso dos grupos abelianos, tôdos os automorfismos internos se reduzem à transformacão idêntica.

Tem lugar o

TEOREMA:-Os automorfismos internos dum grupo constituem um grupo $J_{\mathcal{G}}$. Designemos com X o automorfismo interno definido pelo elemento $x \in \mathcal{G}$. X é um operador, para o qual, se $a \in \mathcal{G}$,

$$Xa = x\,a\,x^{-1}.$$

Se Y é um segundo automorfismo interno, tem-se $Ya = y\,a\,y^{-1}$. Definindo Y^{-1} pela igualdade $Y^{-1}a = y^{-1}a\,y$, vê-se que

$$XY^{-1}a = X(Y^{-1}a) = x(y^{-1}a\,y)\,x^{-1} = x\,y^{-1}a(x\,y^{-1})^{-1}$$

define um automorfismo interno. O teorema está demonstrado.

A cada elemento $x \in \mathcal{G}$ corresponde um automorfismo interno e ao produto de dois elementos corresponde o produto dos automorfismos correspondentes, pois

$$x\,y\,a(xy)^{-1} = x\,y\,a\,y^{-1}\,x^{-1} = XY\,a.$$

O elemento x', correspondente de x, num automorfismo interno, diz-se conjugado de x. A totalidade dos conjugados de a é dada por $y\,a\,y^{-1}$, onde y percorre o grupo. Se no grupo $\mathcal{G}$ se considera a correspondência $a \rightarrow y\,a\,y^{-1}$ define-se uma relação de equivalência. O grupo $\mathcal{G}$ pode decompôr-se, assim, em classes de elementos conjugados, sem elemento comum. Entre essas classes há algumas compostas por um único elemento. A condição necessária e suficiente para que z constitua, por si só, uma classe, é que z pertença ao centro do grupo.

TEOREMA:-Os elementos da mesma classe possuem a mesma ordem. Se a ordem de a é n, tem-se $a^n = u$. Então, sendo $(y a y^{-1})^n = y\,a^n\,y^{-1}$, vê-se que $(y\,a\,y^{-1})^n = u$, qualquer que seja y. E não pode haver uma potência $m < n$ nas mesmas condições, visto que, da relação $(y\,a\,y^{-1})^m = y\,a^m\,y^{-1} = u$, se tiraria $a^m = u$.

Numa correspondência homomorfa de dois grupos, a cada sub-grupo dum deles corresponde um sub-grupo do outro. É assim que a um sub-grupo $\mathcal{Y}$ de $\mathcal{G}$ corresponde um sub-grupo conjugado $a\,\mathcal{Y}\,a^{-1}$, qualquer que seja a. Se $\mathcal{Y}$ é um divisor normal, tira-se, de $a\,\mathcal{Y} = \mathcal{Y}\,a$, a relação $a\,\mathcal{Y}\,a^{-1} = \mathcal{Y}$. Podemos enunciar o

TEOREMA:-Um divisor normal é idêntico com todos os seus sub-grupos conjugados, e reciprocamente. Para se demonstrar a inversa, basta notar que, de $a\,\mathcal{Y}\,a^{-1} = \mathcal{Y}$, se tira imediatamente $a\,\mathcal{Y} = \mathcal{Y}\,a$.

Um divisor normal é, pois, um sub-grupo invariante em face dos automorfismos internos.

O divisor normal pode ainda caracterizar-se pela propriedade de ser um sub-grupo que, com cada elemento, contém tôdos os seus conjugados. Na verdade, dado o sub-grupo $\mathcal{Y}$, se, qualquer que seja y, se tem $y\,\mathcal{Y}\,y^{-1} \subseteq \mathcal{Y}$, então, substituindo y por y^{-1}, vem também $y^{-1}\,\mathcal{Y}\,y \subseteq \mathcal{Y}$. Ora, da primeira relação, tira-se $\mathcal{Y} \subseteq y^{-1}\,\mathcal{Y}\,y$, o que leva a $\mathcal{Y} = y^{-1}\,\mathcal{Y}\,y$ ou $\mathcal{Y}\,y = y\,\mathcal{Y}$, como se deseja.

7) PROPRIEDADES DOS DIVISORES NORMAIS -É válido o seguinte

TEOREMA:-O produto dum sub-grupo $\mathcal{Y}$ por um divisor normal $\mathcal{N}$ dum grupo dado é um novo sub-grupo do grupo. Por produto entende-se aqui o conjunto de elementos do grupo que se obtem multiplicando cada elemento de $\mathcal{Y}$ por cada elemento de $\mathcal{N}$. A demonstração é imediata.

TEOREMA:-O produto de dois divisores normais, $\mathcal{N}$ e $\mathcal{N}'$, dum grupo, é um divisor normal do grupo. Se $\mathcal{C}$ designa êsse produto, vamos verificar, com efeito, que, qualquer que seja a, se tem $a\,\mathcal{C}\,a^{-1} \subseteq \mathcal{C}$. Representemos com c um elemento de $\mathcal{C}$. Será $c = nn'$, com $n \in \mathcal{N}$, $n' \in \mathcal{N}'$. Então

$$a\,c\,a^{-1} = a\,n\,n'a^{-1} = a\,n\,a^{-1}\,a\,n'a^{-1}$$

Daqui se conclui o teorema.

TEOREMA:-A intersecção de dois divisores normais é um divisor normal. A demonstração é imediata.

TEOREMA:-Dados o sub-grupo $\mathcal{Y}$ e o divisor normal $\mathcal{N}$, a intersecção de $\mathcal{Y}$ com $\mathcal{N}$ é um divisor normal de $\mathcal{Y}$. Em primeiro lugar, trata-se dum sub-grupo do grupo dado e também de cada um dos sub-grupos $\mathcal{Y}$ e $\mathcal{N}$. Designando-o com $\mathcal{D}$, seja $a \in \mathcal{Y}$. Visto que $a\,\mathcal{N}\,a^{-1} \subseteq \mathcal{N}$, será $a\,\mathcal{D}\,a^{-1} \subseteq \mathcal{N}$. Por outro lado, $a\,\mathcal{D}\,a^{-1} \subseteq \mathcal{D}$, de sorte que $a\mathcal{D}a^{-1} \subseteq \mathcal{D}$, q.e.d.

Terminaremos êste § com a demonstração do seguinte

TEOREMA:-Se dois divisores normais, $\mathcal{N}$ e $\mathcal{N}'$, têm apenas u como elemento comum, os elementos de cada um dêles comutam com tôdos os elementos do outro. Por hipótese é $a \in \mathcal{N}$, $a' \in \mathcal{N}'$. Trata-se de demonstrar que $a\,a' = a'a$. Ora $a'a\,a'^{-1} \in \mathcal{N}$, $a'a^{-1}a'^{-1} \in \mathcal{N}$, $a'a^{-1}a'^{-1}.a \in \mathcal{N}$. Escrevendo $a'a^{-1}a'^{-1}.a = a'.a^{-1}a'^{-1}a$, vê-se que êste elemento pertence a $\mathcal{N}'$. Será, pois, $a'a^{-1}a'^{-1}a = u$, e $a'^{-1}a^{-1} = a^{-1}a'^{-1}$, ou $a\,a' = a'a$, q.e.d..

8) NORMALIZADOR DUM ELEMENTO -Seja $a \in \mathcal{G}$ e consideremos o conjunto dos elementos de $\mathcal{G}$ que comutam com a. Tal conjunto diz-se normalizador de a. É um sub-grupo $\mathcal{Y}$. Como as potências de a comutam com a, o normalizador contém o grupo cíclico $\mathcal{Z}$ gerado por a. Para cada $x \in \mathcal{Y}$, vale $x\mathcal{Z} = \mathcal{Z}x$, o que mostra ser $\mathcal{Z}$ um divisor normal de $\mathcal{Y}$.

Sejam agora os complexos associados de $\mathcal{Y}$ em $\mathcal{G}$: $\mathcal{Y}$, $b_1\mathcal{Y}$, $b_2\mathcal{Y}$, ... Determinemos os conjugados de a, servindo-nos da expressão $y\,a\,y^{-1}$, mas fazendo coincidir y sucessivamente com cada complexo $b_i\mathcal{Y}$. Tem-se $b_i\mathcal{Y}.a.\mathcal{Y}^{-1}b_i^{-1} = b_i\,a\,b_i^{-1}$, resultado que mostra poder determinar-se uma correspondência entre os complexos e os conjugados de a. Esta correspondência é biunívoca, pois, se pudesse ser $b_i\,a\,b_i^{-1} = b_j\,a\,b_j^{-1}$, ter-se-ia

$$a.b_i^{-1}b_j = b_i^{-1}b_j.a.$$

Daqui concluia-se que $b_i^{-1}b_j$ pertenceria ao normalizador e não seriam diferentes as classes $b_i\mathcal{Y}$ e $b_j\mathcal{Y}$, contra o que se supõe.

Façamos ainda duas observações. A primeira diz-nos que o número de elementos conjugados de a (no caso de $\mathcal{G}$ ser finito) é igual ao índice do normalizador de a. A segunda dá uma propriedade do número de elementos de cada classe de elementos conjugados em que se decompõe um grupo. Se a é um representante duma tal classe, o número dos seus elementos, como índice do normalizador de a, é um divisor da ordem do grupo. Pode enunciar-se o

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

9) GRUPO FACTOR -Os complexos associados dum sub-grupo $\mathcal{Y}$, dum grupo $\mathcal{G}$, se $\mathcal{Y}$ é divisor normal, constituem um grupo, no sentido que vamos vêr. Em primeiro lugar, consideremos o conjunto em que cada elemento é um complexo associado dum sub-grupo; trata-se, em seguida, de dar nêsse conjunto um preceito de produto com o qual venham a verificar-se os postulados da teoria dos grupos. Se a e b pertencem a $\mathcal{G}$ e $\mathcal{Y}$ é um sub-grupo, os complexos $a\mathcal{Y}$ e $b\mathcal{Y}$, no caso de se multiplicarem tôdos os elementos do primeiro por tôdos os elementos do segundo, não levam, no geral, a elementos do grupo pertencentes ao mesmo complexo associado. É suficiente para que isso suceda, que $\mathcal{Y}$ seja um divisor normal. Nêsse caso, é válida a regra $a\mathcal{Y}.b\mathcal{Y} = ab.\mathcal{Y}$, como imediatamente se verifica. Assim, no conjunto

$$\mathcal{L} = \{\mathcal{Y}, a\mathcal{Y}, b\mathcal{Y}, \ldots\}$$

existe um preceito de produto. A validade da propriedade associativa resulta da suá validade em $\mathcal{G}$. Por último, as equações $a\mathcal{Y}.x\mathcal{Y} = b\mathcal{Y}$ e $y\mathcal{Y}.a\mathcal{Y} = b\mathcal{Y}$ têm as soluções $a^{-1}b\mathcal{Y}$, $b\,a^{-1}\mathcal{Y}$, respectivamente. O grupo constituido por $\mathcal{L}$ diz-se grupo factor de $\mathcal{G}$ segundo $\mathcal{Y}$, e representa-se com $\mathcal{G}/\mathcal{Y}$. O elemento um do grupo factor é $\mathcal{Y}$, e o inverso de $a\mathcal{Y}$ é $a^{-1}\mathcal{Y}$. É imediato que o grupo factor é uma imagem homomorfa do grupo dado.

Seja $\mathcal{G}$ um grupo finito de ordem N. Se o seu divisor normal $\mathcal{N}$ é de ordem n, o grupo factor é de ordem N/n. Se considerarmos no grupo factor um sub-grupo de índice r, a totalidade dos elementos de $\mathcal{G}$ que nele entram constitui um sub-grupo de $\mathcal{G}$ com o mesmo índice r. Demonstraremos ainda o seguinte

TEOREMA:-Dado um grupo $\mathcal{G}$, se s é a mais baixa potência do elemento $a \in \mathcal{G}$ que figura num divisor normal $\mathcal{N}$, s é divisor da ordem do grupo factor $\mathcal{G}|\mathcal{N}$. Consideremos, com efeito, o conjunto de elementos de $\mathcal{G}|\mathcal{N}$:

$$\mathcal{L} = \{\mathcal{N}, \ \mathcal{N}a, \ldots, \ \mathcal{N}a^{s-1}\}.$$

Êstes elementos são todos diferentes e constituem um grupo de ordem s. Como $\mathcal{L}$ é sub-grupo de $\mathcal{G}|\mathcal{N}$, resulta o teorema.

10) O GRUPO COMUTADOR -Dados $a, b \in \mathcal{G}$, o seu comutador, c, é definido por $c = ab(ba)^{-1} = a b a^{-1} b^{-1}$. Quando o comutador é u os elementos comutam. Esta condição é necessária à comutatibilidade.

Diz-se grupo comutador, $\mathcal{L}$, dum grupo, o grupo gerado pelos comutadores. O grupo comutador é um divisor normal do grupo dado, como vamos vêr. Seja $x \in \mathcal{G}$. Podemos escrever sucessivamente:

$$x.ab(ba)^{-1}.x^{-1} = x\ a\ b\ a^{-1}\ b^{-1}\ x^{-1} =$$

$$= x a b.(a.xb)^{-1}.(a.xb).(xb.a)^{-1} = xabb^{-1}x^{-1}a^{-1}.(a.xb).(xb.a)^{-1} =$$

$$= \left(x a.(a x)^{-1}\right)\left((a.xb)(xb.a)^{-1}\right),$$

resultado que mostra que um conjugado do comutador $ab(ba)^{-1}$ pertence ao grupo comutador. A demonstração é a mesma se o comutador tiver a forma do inverso dum comutador dado. Quanto ao produto de dois comutadores, tem-se

$$x(ab)(ba)^{-1}.cd(dc)^{-1}x^{-1} = \left(x.ab(ba)^{-1}.x^{-1}\right)\left(x.cd(dc)^{-1}.x^{-1}\right)$$

Conclui-se, assim, que o conjugado dum elemento qualquer do grupo comutador pertence ao grupo comutador. Vale o

TEOREMA:-O grupo factor $\mathcal{G}|\mathcal{L}$ é abeliano. Para o demonstrar, dadas as igualdades $x\mathcal{L}.y\mathcal{L} = x\,y\,\mathcal{L}$, $y\mathcal{L}.x\mathcal{L} = y\,x\,\mathcal{L}$, tem de demonstrar-se ser $xy\mathcal{L} = yx\mathcal{L}$. Se designarmos com c o comutador de x e y, tem-se

$$y\,x\,\mathcal{L} = \mathcal{L}\,y\,x = \mathcal{L}\,c.y\,x = \mathcal{L}\,x\,y = x\,y\,\mathcal{L},$$

como se deseja. Vale também o

TEOREMA:-O grupo comutador está contido em todo o divisor normal cujo grupo factor seja abeliano. Seja $\mathcal{D}$ um divisor normal nessas condições. Se a e b são dois elementos do grupo dado, tem-se $a\mathcal{D}.b\mathcal{D} = b\mathcal{D}.a\mathcal{D}$. Ora tira-se daqui $ab\mathcal{D} = ba\mathcal{D} = \mathcal{D}ba$, pelo que existe um elemento $c \in \mathcal{D}$ tal que $ab = c.ba$. E sendo $c = ab(ba)^{-1}$, vê-se que c é um comutador.

Corolário:- O grupo comutador é intersecção de todos os divisores normais com grupo factor abeliano.

11) GRUPO FACTOR DOS GRUPOS ABELIANOS- No caso dos grupos abelianos, todo o sub-grupo é um divisor normal. Um grupo não abeliano com a mesma propriedade diz-se um grupo hamiltoniano. Nêstes casos, para todo o sub-grupo, há um grupo factor. Se $\mathcal{G}$ fôr o grupo e $\mathcal{M}$ o sub-grupo, poremos $a+\mathcal{M}$ como expressão dos elementos de $\mathcal{G}|\mathcal{M}$, quando $\mathcal{G}$ é abeliano.

Se dois elementos a e b são tais que a sua diferença pertence a $\mathfrak{M}$ eles geram o mesmo elemento do grupo factor. Dizem-se, então, elementos congruentes segundo o módulo $\mathfrak{M}$, o que se representa abreviadamente com

$$a \equiv b \pmod{\mathfrak{M}} \qquad \text{ou} \qquad a \equiv b\ (\mathfrak{M})$$

12) TEOREMA DA HOMOMORFIA -A correspondência homomorfa dum grupo $\mathfrak{G}'$ a outro grupo $\mathfrak{G}$, representada com $\mathfrak{G} \sim \mathfrak{G}'$, foi definida por propriedades simples. É possível aprofundar as consequências da definição e estabelecer resultados duma importância capital. Tomemos os elementos de $\mathfrak{G}$ que têm como correspondente o elemento um, u', de $\mathfrak{G}'$. Êsses elementos constituem um divisor normal $\mathfrak{N}$. Os complexos associados de $\mathfrak{N}$ são formados por elementos de $\mathfrak{G}$ que têm o mesmo correspondente em $\mathfrak{G}'$. E a dois complexos diferentes correspondem elementos diferentes. Podemos, por isso, formular o

TEOREMA:-Se $\mathfrak{G}'$ é homomorfo de $\mathfrak{G}$, existe um divisor normal $\mathfrak{N}$, de $\mathfrak{G}$, tal que $\mathfrak{G}'$ é isomorfo do grupo factor $\mathfrak{G}|\mathfrak{N}$.

Do que acaba de dizer-se e do que se disse a propósito do grupo factor, resulta o

TEOREMA DA HOMOMORFIA:-Se um grupo $\bar{\mathfrak{G}}$ é uma imagem homomorfa dum grupo $\mathfrak{G}$, o grupo $\bar{\mathfrak{G}}$ é imagem isomorfa do grupo factor $\mathfrak{G}|\mathfrak{N}$, onde $\mathfrak{N}$ é divisor normal de $\mathfrak{G}$ que tem por imagem o elemento um, $\bar{u}$, de $\bar{\mathfrak{G}}$; e inversamente, por meio dum divisor normal $\mathfrak{N}$ de $\mathfrak{G}$, obtem-se uma imagem homomorfa de $\mathfrak{G}$ escrevendo o grupo factor $\mathfrak{G}|\mathfrak{N}$.

De futuro utilizaremos o símbolo $\cong$ para representar um isomorfismo.

Ao tratarmos dos automorfismos dum grupo, vimos que o grupo $J_{\mathfrak{G}}$ dos automorfismos internos era um sub-grupo do grupo $A_{\mathfrak{G}}$ de tôdos os automorfismos.

E vimos também que $J_{\mathfrak{G}}$ era uma imagem homomorfa do grupo $\mathfrak{G}$. Existe um divisor normal $\mathfrak{N}$ de $\mathfrak{G}$ tal que $\mathfrak{G}|\mathfrak{N} \cong J_{\mathfrak{G}}$. $\mathfrak{N}$ é o conjunto dos elementos de $\mathfrak{G}$ que definem o automorfismo idêntico. Se $z \in \mathfrak{N}$, é por consequência, $z\,a\,z^{-1} = a$, ou $z\,a = a\,z$. Isto significa que z pertence ao centro de $\mathfrak{G}$. Inversamente, um elemento do centro define o automorfismo idêntico. Logo, $\mathfrak{N}$ é o centro de $\mathfrak{G}$.

TEOREMA:-O grupo $J_{\mathfrak{G}}$ é divisor normal de $A_{\mathfrak{G}}$.

Representando com $\ominus$ o operador respeitante a um automorfismo qualquer, pretende provar-se que $\ominus X \ominus^{-1} \in J_{\mathfrak{G}}$, se $X \in A_{\mathfrak{G}}$. Suponhamos que $\ominus$ e $\ominus^{-1}$ determinam as seguintes correspondências entre elementos de $\mathfrak{G}$:

$$\ominus \begin{cases} a \to a' \\ b \to a \\ x \to x' \\ \text{------} \end{cases}, \qquad \ominus^{-1} \begin{cases} a' \to a \\ a \to b \\ x' \to x \\ \text{------} \end{cases};$$

então, $\ominus X \ominus^{-1}$ determina esta outra:

$$a \to \ominus\,(x\,b\,x^{-1}) = x'a\,x'^{-1},$$

que é um automorfismo interno, como se deseja.

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

A. SPEISER, citado no 1.º caderno;

B.L.van der WAERDEN, idem, idem;

H.ZASSENHAUS, Lehrbuch der Gruppentheorie, 1937, Teubner, Berlim;

A.ALMEIDA COSTA, citado no 1.º caderno.