MONOGRAFIAS DE MATEMÁTICA N.° 23

INTRODUÇÃO À ÁLGEBRA

(2ª EDIÇÃO)

ARON SIMIS

INSTITUTO DE MATEMÁTICA PURA E APLICADA

RIO DE JANEIRO

1977

DEPARTAMENTO DE INFORMAÇÃO CIENTÍFICA (DIC)

MONOGRAFIAS DE MATEMÁTICA

1) Alberto Azevedo & Renzo Piccinini - Introdução à Teoria dos Grupos
2) Nathan M. Santos - Vetores e Matrizes (esgotado)
3) Manfredo P. Carmo - Introdução à Geometria Diferencial Global
4) Jacob Palis Jr. - Sistemas Dinâmicos
5) João Pitombeira de Carvalho - Introdução à Álgebra Linear (esgotado)
6) Pedro J. Fernandez - Introdução à Teoria das Probabilidades
7) R.C. Robinson - Lectures on Hamiltonian Systems
8) Manfredo P. do Carmo - Notas de Geometria Riemanniana
9) Chain S. Hönig - Análise Funcional e o Problema de Sturn-Liouville
10) Welington de Melo - Estabilidade Estrutural em Variedades de Dimensão 2
11) Jaime Lesmes - Teoria das Distribuições e Equações Diferenciais
12) Clóvis Vilanova - Elementos da Teoria dos Grupos e da Teoria dos Anéis
13) Jean Claude Douai - Cohomologie des Groupes
14) H. Blaine Lawson Jr. - Lectures on Minimal Submanifolds, Vol.1
15) Elon L. Lima - Variedades Diferenciáveis
16) Pedro Mendes - Teoremas de Ω-estabilidade e Estabilidade Estrutural em Variedades Abertas.
17) Herbert Amann - Lectures on Some Fixed Point Theorems
18) Exercícios de Matemática - IMPA
19) Djairo G. de Figueiredo - Números Irracionais e Transcendentes
20) C.E. Zeeman - Uma Introdução Informal à Topologia das Superfícies
21) Manfredo P. do Carmo - Notas de um curso de Grupos de Lie
22) A. Prestel - Lectures on Formally Real Fields
23) Aron Simis - Introdução à Álgebra.

INSTITUTO DE MATEMÁTICA PURA E APLICADA
Rua Luiz de Camões, 68
20.000 - Rio de Janeiro - RJ

Ao José Morgado,

a quem devo o início.

Justificativa

O presente texto partiu de notas preliminares destinadas a auxiliar os alunos do Curso de Introdução à Álgebra, (no IMPA, verão de 1975). Subsequentemente, tais notas se transformaram no Nº 23 da coleção Monografias de Matemática daquele Instituto e, como tal, têm servido aos estudantes.

Como dá-se comumente com textos deste nível, a monografia esgotou-se, deixando-me a escolha entre simplesmente imprimir mais exemplares na coleção de Monografia ou fazer o texto acessível a um público mais amplo. Optei pela segunda alternativa, no que oferece ótimo elemento de propaganda para a Álgebra nos meios menos ortodoxos, além de fornecer um desafio ao preconceito vigente de que Álgebra é formalismo simbólico.

É justamente este último aspecto que constitui novidade no texto. Pensei em oferecer matéria prima para trabalho, tendo sido a idéia (nociva, no meu entender) de "forma acabada" relegado a plano secundário. Daí, uma feição do manuscrito: rústico e por vezes, telegráfico. Uma tal feição exige, naturalmente, esforço intensivo por parte do leitor. A recompensa, contudo, é maior do que resultaria de uma leitura formalista e neuroticamente burilada.

Há dois tópicos fundamentais: elementos da teoria dos grupos e noções de corpos e suas extensões finitas. Deixei-me guiar guiar pela idéia de fornecer poucas definições e muitos exemplos; resultados que, ordinariamente, apareceriam sob forma de proposição ou teorema, aqui aparecem livremente na confecção dos próprios exemplos.

Ficaram de fora belíssimos exemplos de grupos cristalográficos, padrões decorativos e grupos de lacetes, por um lado, e da teoria clássica das equações (Cardan, Tartaglia, Newton), por outro lado. A serem incluidos no texto, acarretaria um aumento desproporcional.

No final do livro estão incluidos vários exercícios, alguns dos quais são reformulações de outros entremeados no texto. Além disso, há um apêndice onde são explicadas noções usadas correntemente no Curso, tais como a noção de relação de equivalência, de relação de ordem, etc.

Aron Simis

Outono de 1977

ÍNDICE

1. Introdução à Teoria dos Grupos

1.1. Primeiros exemplos.

A natureza é pródiga em sistemas que guardam entre si, por diferentes que sejam, certos atributos comuns. A fim de expressar o que há de comum entre tais sistemas, é conveniente estabelecer alguma linguagem matemática mediante a qual possa-se abstrair certas propriedades "mínimas" que permanecem válidas qualquer que seja o sistema particular em questão. Chega-se então à ideia de estrutura (ou conjunto estruturado) em Matemática. Nesta parte de Curso lida-se com um exemplo de tal estrutura: o de grupo.

Antes, porém, convém descrever alguns exemplos com os quais possamos, sempre que necessário, experimentar.

(A) Números inteiros.

Pelo conjunto $\mathbb{Z}$ dos números inteiros entenderemos a reunião do conjunto $\mathbb{N}$ dos naturais (incluindo 0) e seus negativos. Assim, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

Pode-se protestar, argumentando-se que não se disse aí absolutamente nada que tenha significado matemático. O protesto é válido. Podemos amenizar um pouco este impasse, com a seguinte proposta conciliatória: suponhamos que é dado o conjunto $\mathbb{N}$ dos números naturais (incluindo 0) juntamente com a operação $+$ e a relação $\leq$ de ordem "usuais". Então, podemos construir o conjunto $\mathbb{Z}$ dos inteiros e munir-lo de uma operação $+$ e de uma relação de ordem $\leq$, de tal modo

que $\mathbb{N} \subset \mathbb{Z}$ e $+$ e $\leq$, restringidas a $\mathbb{N}$, coincidem com as relações $+$ e $\leq$ usuais definidas em $\mathbb{N}$.

Mais precisamente, postulemos a existência de um conjunto $\mathbb{N}$ com pelo menos dois elementos, de uma operação $+ : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ e de uma relação de ordem $\leq$ em $\mathbb{N}$ sujeitos às seguintes exigências:

($\mathbb{N}$.1) A relação de ordem $\leq$ é boa; quer dizer, todo subconjunto S de $\mathbb{N}$, tal que $S \neq \emptyset$, contém um elemento a tal que $a \leq b$ para todo $b \in S$.

($\mathbb{N}$.2) A operação $+$ é

(i) Comutativa: $a + b = b + a$

(ii) Associativa: $(a+b) + c = a + (b+c)$

(iii) Cancelativa: $a + b = a + c \Rightarrow b = c$

($\mathbb{N}$.3) Compatibilidade de $+$ e $\leq$: $a \leq b \Rightarrow a + c \leq b + c$ para todo $c \in \mathbb{N}$.

($\mathbb{N}$.4) Para todo $a, b \in \mathbb{N}$ tais que $a \leq b$, existe $c \in \mathbb{N}$ tal que $a + c = b$ (c é chamado a diferença entre b e a).

Observação: É possível mostrar que uma tal estrutura é, num certo sentido, única. Contudo, não nos ocuparemos disto aqui.

Em seguida, daremos uma receita rápida de como construir $\mathbb{Z}$ a partir dos dados acima. Os detalhes deverão ser preenchidos ao menos uma vez na vida.

Considera-se o produto cartesiano $\mathbb{N}\times\mathbb{N} = \{(m,n) \mid m,n \in \mathbb{N}\}$ e nele se define a seguinte relação de equivalência $\sim$:

$$(m,n) \sim (m',n') \quad \text{se e só se} \quad m+n' = m'+n$$

(onde + é a operação de "soma" em $\mathbb{N}$). Em seguida, considera-se o conjunto quociente $\mathbb{Z} = \mathbb{N}\times\mathbb{N}/\sim$ por esta relação de equivalência. Em $\mathbb{Z}$, definimos uma operação + decretando:

$$\underset{\text{operação em definição}}{(m,n) + (m',n')} \quad = \quad \underset{\text{operação dada em } \mathbb{N}}{(m+m' \, , \, n+n')}$$

Verifica-se que a definição é boa (isto é, não depende dos representantes escolhidos das classes da equivalência $\sim$). Definimos também uma relação de ordem em $\mathbb{Z}$:

$$\underset{\text{ordem em definição}}{(m,n) \leq (m',n')} \quad \text{se e só se} \quad \underset{\text{ordem em } \mathbb{N}}{m+n' \leq m'+n}$$

Verifica-se igualmente tratar-se de uma relação de ordem.

Seja $0 \in \mathbb{N}$ o menor elemento de $\mathbb{N}$ (isto é, $0 \leq m$ para todo $m \in \mathbb{N}$). É fácil ver que $m + 0 = m$ para todo $m \in \mathbb{N}$. Por outro lado, todo elemento de $\mathbb{Z}$ é de uma das duas formas $(m,0)$ ou $(0,m)$, com $m \in \mathbb{N}$ (sugestão: dado um elemento (p,q) considere-se, separadamente, os casos em que $p \leq q$ e $q \leq p$).

Finalmente, vê-se facilmente que a aplicação $\varphi: \mathbb{N} \to \mathbb{Z}$, definida por $\varphi(m) = (m,0)$ é injetora, o que permite identificar $\mathbb{N}$ com o subconjunto $\{(m,0) \mid m \in \mathbb{N}\}$ de $\mathbb{Z}$. Chamando $-\mathbb{N}$ ao conjunto $\{(0,m) \mid m \in \mathbb{N}\} \subset \mathbb{Z}$, tem-se $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$ mediante a identificação acima. É claro que $\mathbb{N} \cap (-\mathbb{N}) = \{0\}$. Daí, expressão usual (usada acima) de que $\mathbb{Z}$ é o conjunto dos naturais e seus "negativos".

Quais as vantagens (ou desvantagens) de $\mathbb{Z}$ em relação a $\mathbb{N}$? Do ponto de vista estritamente da economia, $\mathbb{Z}$ parece maior e mais

complexo. Este ponto é, contudo, simplista e pode ser razoavelmente refutado com o argumento de que $\mathbb{N}$ e $\mathbb{Z}$ têm a mesma potência (ou cardinal), isto é, podem ser colocados em bijeção, e além do mais, $\mathbb{Z}$ é facilmente descrito a partir de $\mathbb{N}$.

Vantagens de $\mathbb{Z}$: preenche todos os requisitos que $\mathbb{N}$ preenche (com a exceção óbvia de ($\mathbb{N}$.1)),com um favor adicional, a saber, pode-se dispensar em ($\mathbb{N}$.4) a exigência de que $(m,n) \leq (m',n')$ a fim de que exista a diferença entre (m',n') e (m,n); o leitor poderá verificar este fato pessoalmente e dele se convencer. Em particular, a diferença $(0,0) - (m,n)$ sempre existe, qualquer que seja $(m,n) \in \mathbb{Z}$. Tal elemento será designado por $-(m,n)$. Se $a \in \mathbb{Z}$ designa um elemento de $\mathbb{Z}$ (abandonando a notação (,), de resto pedante), então $-a$ é chamado <u>inverso</u> (aditivo) de a.

Isolemos esta propriedade:

(I) Para todo $a \in \mathbb{Z}$, existe um elemento (designado por) $-a \in \mathbb{Z}$ tal que $a + (-a) = 0$.

Isolemos outra propriedade, que já deveria ter sido verificada mais acima (e é imediata):

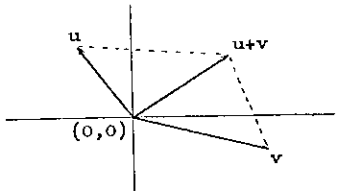
(N) Para todo $a \in \mathbb{Z}$, tem-se $a + 0 = a$.

Convém isolar tais propriedades por se apresentarem amiúde em outros exemplos. Elas se incluirão entre o conjunto de propriedades mínimas (ou axiomas) a serem exigidas na definição formal de um grupo.

<u>Observação</u>: Propriedades especiais dos números inteiros (que não decorrem dos axiomas de grupo) serão revistas nos exercícios.

(B) Vetores (Álgebra Linear)

Os vetores do plano (aplicados na origem (0,0)) podem ser somados pela regra usual do paralelogramo:



Visto de outra maneira, temos uma operação de adição em $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ que consiste em adicionar as coordenadas de mesmo nome:

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

Aqui, o sinal + no segundo membro designa a operação de adição usual de números reais, induzida pela operação + de números racionais (por passagem ao limite: cortes de Dedekind) a qual, por sua vez se define a partir da operação + em $\mathbb{Z}$ acima definida.

É fácil verificar que $\mathbb{R}$ e, consequentemente, $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, munidos das operações + assim definidas satisfazem as propriedades (I) e (N) acima descritas para $\mathbb{Z}$. Em ambos os casos, a operação + é comutativa e associativa.

A adição de vetores no plano estende-se facilmente ao caso de vetores no espaço a n dimensões, isto é, ao $\mathbb{R}^n$.

Observação: Neste curso somente será de interesse a operação de + em $\mathbb{R}^n = \mathbb{R} \times \ldots \times \mathbb{R}$. Num curso de Álgebra Linear, salienta-se uma outra operação: a de produto de um número real por um vetor.

(C) Simetrias de uma reta no plano.

Até agora, os exemplos foram todos comutativos, isto é, a operação + obedecia a lei de comutatividade: $a + b = b + a$, para todos os elementos a,b. Poderíamos acrescentar aos já vistos, os exemplos seguintes: os números racionais $\neq 0$, os números reais $\neq 0$, os números complexos $\neq 0$, respectivamente munidos da operação de produto usual.

Queremos agora dar um exemplo não comutativo. Para tal, somos forçados a abandonar a arena dos números propriamente e recorrer a uma situação mais geométrica.

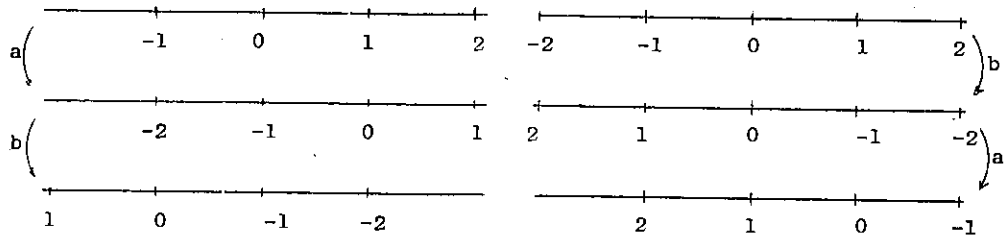
Consideremos uma reta ℓ no plano (por exemplo, o eixo das abcissas em $\mathbb{R}^2$) e consideremos as congruências de ℓ, isto é, os movimentos rígidos do plano que levam ℓ em si mesma. Tais congruências - designadas simetrias de ℓ - são de duas espécies: translação ao longo de ℓ de comprimento $r \in \mathbb{R}$ e rotação de π radianos em torno de um ponto de ℓ (evidentemente, rotações em torno de um mesmo ponto que diferem por um múltiplo de 2π, são consideradas idênticas).

Designemos por S o conjunto das simetrias de ℓ. Em S introduzimos uma operação que consiste em executar sucessivamente dois movimentos rígidos. O leitor certificar-se-á, intuitivamente ao menos, de que a aplicação sucessiva de duas simetrias conduz a outra simetria de ℓ, de maneira que tal processo define efetivamente uma operação em

S (por exemplo, todas as rotações em torno de pontos de ℓ são obtidas por translações ao longo de ℓ seguidas de uma rotação arbitrariamente escolhida mas fixa de uma vez por todas; a rigor, as simetrias de ℓ são aplicações lineares de $\mathbb{R}^2$ em $\mathbb{R}^2$, de tipo especial, e a operação de executá-las sucessivamente traduz-se pelo produto das matrizes que representam tais aplicações lineares numa base escolhida).

É evidente que a operação em S assim definida é associativa (a execução sucessiva de movimentos rígidos sempre o é). As propriedades (I) e (N) de $\mathbb{Z}$ permanecem válidas neste caso. Por exemplo, a simetria que desempenha o mesmo papel do 0 em $\mathbb{Z}$, é um rotação de 0 (ou 2π) radianos em torno de um ponto qualquer de ℓ.

Contudo, a operação <u>não é comutativa</u>. Com efeito, se a é uma translação de comprimento $r \neq 0$ e se b é uma rotação qualquer, então $a.b \neq b.a$ (onde . designa a operação em S).

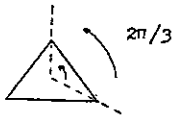


(D) <u>Simetrias espaciais do triângulo equilátero</u>.

Todos os exemplos descritos anteriormente tinham em comum a propriedade de que o conjunto em questão era infinito. O exemplo que ora consideraremos, além de ser não comutativo, é finito.

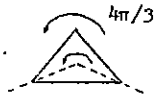
Seja t um triângulo equilátero, o qual suporemos centrado

na origem do espaço R^3. Consideramos, não somente as simetrias planas de t, mas também suas simetrias espaciais. São, ao todo, em número de seis (*) assim descritas:

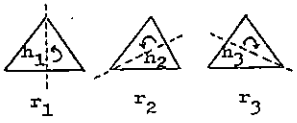


R_o: rotação plana de 0 radianos

R_1: rotação plana de $2\pi/3$ radianos no sentido contrário ao do relógio.



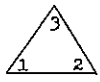
R_2: rotação plana de $4\pi/3$ radianos no sentido contrário ao do relógio.



r_i: rotação espacial de π radianos em torno da altura h_i, $i = 1, 2, 3$.

Seja G o conjunto dessas simetrias. Em G definimos a operação que consiste em executar duas simetrias sucessivamente. Verifica-se (ao cabo de no máximo 36 execuções !) que o resultado da execução sucessiva de duas simetrias é ainda uma simetria, de modo que temos uma operação em G.

Numerando os vértices, conforme a figura abaixo, visualizamos melhor a execução das simetrias interpretando-as como permutações entre os vértices.



(*) Identificamos as simetrias que diferem por uma rotação de 2π radianos.

Assim, R_1 traduz-se por

$$1 \to 2$$
$$2 \to 3$$
$$3 \to 1$$

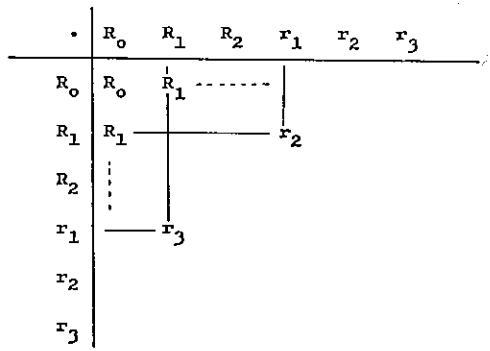
enquanto que r_1 traduz-se por

$$1 \to 2$$
$$2 \to 1$$
$$3 \to 3$$

Designando por . a operação de execução sucessiva de duas simetrias, tem-se que:

$$R_1 \cdot r_1: \quad 1 \to 1,\ 2 \to 3,\ 3 \to 2 \qquad \text{e} \qquad r_1 \cdot R_1: \quad 1 \to 3,\ 2 \to 2,\ 3 \to 1$$

Logo, $R_1 \cdot r_1 = r_2 \neq r_3 = r_1 \cdot R_1$, mostrando que a operação . não é comutativa. É um bom exercício efetuar todos os produtos de simetrias e dispo-los conforme a tabela:



A simetria que desempenha o mesmo papel de 0 ($0 \in \mathbb{Z}$) é, evidentemente, R_o. A fim de completar a tabela acima sem recorrer ao cálculo

efetivo dos 36 produtos, o leitor poderá usar alguns expedientes para poupar tempo. Por exemplo, a 1ª linha e a 1ª coluna são preenchidas automaticamente devido ao caráter privilegiado de R_0. Que outras peculiaridades podem contribuir para a tarefa de preencher a tabela ? É útil, pelo menos a posteriori, observar tais peculiaridades.

1.2. A noção abstrata de grupo. Subgrupos.

Nesta seção, reuniremos algumas propriedades comuns aos exemplos da seção 1.1 sob a forma de axiomas. Em todos os exemplos descritos, estávamos de posse de um conjunto G munido de uma operação (designada doravante por $.$) satisfazendo as seguintes condições:

(G.1) A operação $.$ é associativa, isto é, $a.(b.c) = (a.b).c$ para todos $a,b,c \in G$.

(G.2) Existe um elemento $e \in G$ tal que $a.e = e.a = a$ para todo $a \in G$.

(G.3) Para todo $a \in G$, existe $a' \in G$ tal que $a.a' = a'.a = e$.

Isto sugere a seguinte:

Definição - Um grupo é um conjunto G munido de uma operação satisfazendo às condições (G.1), (G.2), (G.3) (chamadas axiomas de grupo).

Se, além dos axiomas G.1, G.2 e G.3, o grupo satisfizer a propriedade adicional da comutatividade, dir-se-á que G é um grupo comutativo ou um grupo abeliano (em homenagem ao matemático norueguês Abel).

Note-se que os axiomas G.2 e G.3 nada dizem sobre a unicida-

de de e ou de a'. Contudo, segue-se a fortiori dos axiomas a unicidade de e e a'. Com efeito, podemos demonstrar a seguinte:

Proposição - Num grupo G, as equações $X.a = b$ e $a.Y = b$ admitem solução única.

Demonstração: Se x é uma solução da equação $X.a = b$, então $(x.a).a' = b.a'$, onde $a' \in G$ é tal que $a.a' = a'.a = e$. Pelo axioma G.1, resulta $x.(a.a') = b.a'$. Pelo axioma G.2, $x = x.e = x.(a.a') = b.a'$. Isto dá a pista de uma solução. Substituição direta de $b.a'$ na equação $X.a = b$ mostra que $b.a'$ é uma solução. Para verificar a unicidade, sejam x_1 e x_2 soluções de $X.a = b$. Então $x_1.a = x_2.a$. Daqui que

$$x_1 = x_1.e = x_1.(a.a') = (x_1.a).a'$$

$$= (x_2.a).a' = x_2.(a.a') = x_2.e = x_2 ,$$

pelos axiomas G.2, G.3 e G.1, respectivamente.

A prova para a equação $a.Y = b$ é análoga. C.Q.D.

Observe-se que a unicidade do elemento e é imediata e nada tem a ver com a proposição acima. Com efeito, se $e' \in G$ também satisfaz G.2, tem-se $e = e.e' = e'$. Por outro lado, a unicidade do elemento a' para cada $a \in G$ segue-se facilmente da proposição acima já que, em particular, a equação $X.a = e$ tem solução única.

Exercício: Mostre que os axiomas G.1, G.2 e G.3 são equivalentes (em conjunto) aos axiomas seguintes, aparentemente mais fracos:

(G.1)': = (G.1)

(G.2)': existe um elemento $e \in G$ tal que $a.e = a$ para todo $a \in G$.

(G.3)': para todo $a \in G$, existe $a' \in G$ tal que $a.a' = e$.

Exercício: Com os ensinamentos do exercício acima, preencha mais rapidamente a tabela da pág. 9.

Definição - O elemento $e \in G$ mencionado no axioma G.2 é chamado o elemento neutro ou a identidade do grupo G. O elemento a' do axioma G.3 é chamado o inverso de a.

Doravante, o inverso de um elemento $a \in G$ será designado por a^{-1}.

Especialmente importantes são os grupos finitos. Para tais grupos é comum e, por vezes, instrutivo, construir uma tabela de multiplicação. Procede-se exatamente como no exemplo (D) da seção 1.1. Enumeramos os elementos do grupo G, digamos, $e = a_1, \ldots, a_n$, e dispomo-los como se segue:

	e	a_2	a_3	$\cdots$	a_n
e	e	a_2	a_3	$\cdots$	a_n
a_2	a_2	a_2^2	$a_2 \cdot a_3$	$\cdots$	$a_2 \cdot a_n$
a_3	a_3	$a_3 \cdot a_2$	a_3^2	$\cdots$	$a_3 \cdot a_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		
a_n	a_n	$a_n \cdot a_2$	$a_n \cdot a_3$	$\cdots$	a_n^2

onde $a_i^2 = a_i \cdot a_i$, $i = 2, \ldots, n$.

Uma das principais vantagens de tal tabela é a de permitir comparar rapidamente dois grupos finitos a fim de determinar quão "distintos" tais grupos são (veja a seção 1.4, sobre a noção de grupos isomorfos). Por exemplo, consideremos os dois grupos G, H assim de

finidos:

G = {simetrias planas de um quadrado}

H = {simetrias espaciais de um retângulo não quadrado}.

Vê-se que $G = \{e, r_2, r_3, r_4\}$, onde e = rotação de 0 radianos, r_2 = rotação plana de $\pi/2$ radianos, r_3 = rotação plana de π radianos, r_4 = rotação plana de $3\pi/2$ radianos. Por outro lado, $H = \{e', r_2', r_3', r_4'\}$, onde r_2' = rotação plana de π radianos, r_3' = rotação (espacial) de π radianos em torno do eixo mediano horizontal do retângulo, r_4' = rotação (espacial) de π radianos em torno do eixo mediano vertical.

As tabelas de G e H obtém-se facilmente:

G

	e	r_2	r_3	r_4
e	e	r_2	r_3	r_4
r_2	r_2	r_3	r_4	e
r_3	r_3	r_4	e	r_2
r_4	r_4	e	r_2	r_3

H

	e'	r_2'	r_3'	r_4'
e'	e'	r_2'	r_3'	r_4'
r_2'	r_2'	e'	r_4'	r_3'
r_3'	r_3'	r_4'	e'	r_2'
r_4'	r_4'	r_3'	r_2'	e'

Uma diferença fundamental entre as duas tabelas é gritante: a diagonal de G contém além do elemento neutro e, o elemento r_3, ao passo que a de H contém somente o elemento neutro (esta propriedade independe da ordem em que foram dispostos os elementos para escrever-se a tabela).

Observemos as tabelas de G e H mais pormenorizadamente. O subconjunto $G_1 = \{e, r_3\}$ de G e os subconjuntos $H_1 = \{e', r_2'\}$, $H_2 = \{e', r_3'\}$, $H_3 = \{e', r_4'\}$ de H têm a propriedade particular de

que o produto de dois elementos do subconjunto é ainda um elemento desse subconjunto. Dizemos de tais subconjuntos que são fechados (ou estáveis) em relação à operação do grupo. É claro que todo grupo G admite pelo menos dois subconjuntos estáveis, a saber, $\{e\}$ e G. Estas considerações motivam a seguinte

Definição - Um subconjunto H de um grupo G é chamado um subgrupo de G se satisfaz as seguintes condições:

(SG 1) $H \neq \emptyset$

(SG 2) H é fechado em relação à operação de G, isto é, $a,b \in H \Rightarrow a.b \in H$

(SG 3) H é fechado em relação a inversos, isto é, se $a \in H$ então $a^{-1} \in H$.

Observemos que um subgrupo G é simplesmente um subconjunto estável de G que constitui "per se" um grupo relativamente à operação de G induzida em H.

Os subconjuntos G_1 e H_1, H_2, H_3 são subgrupos de G e H respectivamente. O conjunto dos números pares (incluindo 0) é um subgrupo de $\mathbb{Z}$; o conjunto dos ímpares não é um subgrupo de $\mathbb{Z}$.

Em geral, a condição (SG 3) é essencial para determinar se um dado subconjunto $H \subset G$ é um grupo com respeito à operação induzida. Assim, por exemplo, o conjunto $\mathbb{N} \subset \mathbb{Z}$ dos naturais satisfaz (SG 1) e (SG 2), mas não é um grupo com respeito à soma usual.

Contudo, pode-se provar a seguinte

Proposição - Seja G um grupo e $H \subset G$ um subconjunto finito. Se H satisfaz (SG 1) e (SG 2), então H é um subgrupo.

Demonstração: Seja $H = \{a_1, \ldots, a_n\}$, $n \geq 1$ (SG 1). Consideremos o conjunto $H_1 = \{a_1, a_1^2, a_1^3, \ldots\}$. Por (SG 2), temos que H_1 é um subconjunto de H. Logo H_1 é finito. Necessariamente, $a_1 = a_1^m$ para algum $m \geq 2$, logo $e = a_1^{-1}.a_1 = a_1^{-1}.a_1^m = (a_1^{-1}.a_1).a_1^{m-1} = a_1^{m-1}$. Se $m = 2$, tem-se $e = a_1$, logo $e \in H$. Se $m \geq 3$, $e = a_1^{m-1} = a_1.a_1^{m-2}$, logo $e \in H$ por (SG 2). Em qualquer caso, tem-se sempre $e \in H$.

Para mostrar que H satisfaz (SG 3), seja $a \in H$ um elemento qualquer de H. Consideremos os produtos $a.a_1, a.a_2, \ldots, a.a_n$. É claro que $a.a_i = a.a_j$ se e só se $i = j$. Por (SG 2), tais produtos pertencem a H. Como há n tais produtos, segue-se que $H = \{a.a_1, \ldots, a.a_n\}$.(*) Em particular, $a.a_i = e$ para algum i, logo $a_i = e.a_i = (a^{-1}.a).a_i = a^{-1}.(a.a_i) = a^{-1}.e = a^{-1}$. Isto é, $a^{-1} \in H$. C.Q.D.

Usando a proposição acima, torna-se bastante cômodo determinar todos os subgrupos de um grupo finito olhando-se a tabela do grupo em questão.

Exercício: Determine todos os subgrupos do grupo das simetrias espaciais de um triângulo equilátero.

Exercício: Determine todos os subgrupos do grupo $\mathbb{Z}$ dos números inteiros. (Sugestão: use o algoritmo de divisão em $\mathbb{Z}$, o qual afirma que dados inteiros m, a $(a > 0)$, existem inteiros n, r tais que $m = n.a + r$, com $0 \leq r < a$; vide Exercício 4.(e) no final do livro).

(*) Princípio das "gavetas e encaixes".

1.3. Um manancial inesgotável: grupos de permutações.

Retomemos, por instantes, o grupo G das simetrias do triângulo equilátero. Vimos que uma maneira cômoda de trabalhar com G consistia em enumerar os vértices do triângulo e escrever as simetrias sob a forma geral:

$$\begin{matrix} 1 & \to & i_1 \\ 1 & \to & i_2 \\ 1 & \to & i_3 \end{matrix}$$

onde $i_1, i_2, i_3 \in \{1, 2, 3\}$ e $i_1 \neq i_2 \neq i_3 \neq i_1$. Em outras palavras, uma tal simetria pode ser interpretada como uma permutação do conjunto $\{1,2,3\}$. Isto sugere que, em geral, o conjunto das permutações de um conjunto finito $\{a_1, \ldots, a_n\}$ ou, simplesmente, de $\{1, \ldots, n\}$, forme um grupo mediante a operação de execução sucessiva (ou "composição") de permutações.

Na verdade, assim é. Mais geralmente, seja E um conjunto qualquer e seja S_E o conjunto de todas as aplicações $f: E \to E$ bijetoras. Então S_E é um grupo mediante a operação de composição de aplicações. O inverso de $f \in S_E$ no sentido da teoria dos grupos é precisamente a aplicação inversa f^{-1} no sentido das aplicações (isto motiva, em parte, a notação a^{-1} para o inverso de um elemento a de um grupo abstrato). O elemento neutro de S_E é, como se verifica imediatamente, a aplicação identidade I_E.

Em particular, se $E = \{1, \ldots, n\}$ $(n \in N)$, escrevemos S_n em vez de S_E. S_n é designado o grupo das permutações de n objetos (ou símbolos). A notação usual para um elemento de S_n

é

$$\begin{pmatrix} 1 & 2 & & n \\ i(1) & i(2) & \dots & i(n) \end{pmatrix} \quad \text{ou} \quad \begin{pmatrix} 1 & 2 & & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}.$$

Esta notação facilita, na prática, a operação de composição de permutações.

Outra designação para S_n é "grupo simétrico em n símbolos". Neste caso, deve-se ter algum cuidado, pois, enquanto que S_3 e o grupo G das simetrias do triângulo equilátero são essencialmente o mesmo grupo (veja seção 1.4, Exercício), S_4 e o grupo das simetrias do quadrado não têm sequer o mesmo número de elementos.

Exercício: Mostre que S_n tem $n! = 1.2. \dots .n$ elementos. Quantos elementos tem o grupo (das simetrias) do quadrado ?

Em geral, calcular com elementos de S_n pode ser bastante complicado. Se $n = 1, 2, 3$, S_n é relativamente simples. Para $n \geq 4$, S_n tem pelo menos 24 elementos, o que torna as coisas mais penosas. De qualquer modo, existem algumas técnicas de caráter geral.

Primeiramente, podemos isolar algumas permutações de tipo especial, chamadas ciclos. Um r-ciclo em S_n é uma permutação $s \in S_n$ tal que existem elementos $a_1, \dots, a_r \in \{1, \dots, n\}$ satisfazendo as condições seguintes:

$$s(a_i) = a_{i+1} \quad , \quad i \leq 1 < r$$
$$s(a_r) = a_1$$
$$s(x) = x \quad \text{para todo} \quad x \notin \{a_1, \dots, a_n\}.$$

Assim, um ciclo está especificado quando se seleciona um subconjunto

de $\{1, \ldots, n\}$ (eventualmente $\emptyset$) e uma ordenação para os elementos deste subconjunto. Ora, para cada r tal que $1 \leq r \leq n$, $\{1, \ldots, n\}$ admite $n!/r!(n-r)!$ subconjuntos com r elementos. Cada um desses subconjuntos de r elementos com $r \geq 2$ dá origem a $(r-1)!$ r-ciclos distintos (isto é, distintos como permutações). Resulta que S_n tem $n!/r(n-r)!$ r-ciclos distintos, sempre que $r \geq 2$.

É um bom exercício calcular este número em casos particulares. Por exemplo, todos os elementos de S_n, $n \leq 3$, são ciclos (exercício: descreva-os!). Se $n \geq 4$, S_n admite ao menos uma permutação que não é ciclo, a saber:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots & n \\ 2 & 1 & 4 & 3 & 5 & \ldots & n \end{pmatrix} .$$

Como existe uma bijeção entre o conjunto dos r-ciclos em S_n e o conjunto dos subconjuntos ordenados de $\{1, \ldots, n\}$ com r elementos, podemos designar um r-ciclo pelo símbolo $(a_1\ a_2\ \ldots\ a_r)$, onde $\{a_1, \ldots, a_r\}$ é o conjunto de elementos de $\{1, \ldots, n\}$ correspondente. Vê-se que a permutação acima é produto dos ciclos (12) e (34).

Dois ciclos $(a_1 \ldots a_r)$ e $(b_1 \ldots b_t)$ são ditos <u>disjuntos</u> se os conjuntos $\{a_1, \ldots, a_r\}$ e $\{b_1, \ldots, b_t\}$ têm interseção vazia. O interesse central dos ciclos é a seguinte

<u>Proposição</u> - Todo elemento de S_n pode-se escrever como produto de ciclos disjuntos.

<u>Demonstração</u>: Seja $s \in S_n$. Se $a \in \{1, \ldots, n\}$, escrevemos $s^m(a)$

para designar $s(s(\ldots s(a)))$ (m vezes). Consideremos todos os ciclos da forma $(a, s(a), s^2(a), \ldots, s^{r-2}(a))$, com a percorrendo $\{1, \ldots, n\}$ e r o menor inteiro positivo (atenção: r depende de a) tal que $S^r(a) = a$. (Exercício: prove a existência de um tal r). Tais ciclos, ditos ciclos da permutação s, são os candidatos naturais para a proposição. Infelizmente, dois quaisquer destes ciclos não são necessariamente disjuntos. Para remediar esta situação, introduzimos a seguinte relação de equivalência no conjunto $\{1, \ldots, n\}$:

$a \sim b$ se e só se $b = s^i(a)$ para algum inteiro i.

É fácil verificar que $\sim$ é realmente uma relação de equivalência. Se $\bar{a}$ designa a classe de a nesta equivalência e se $\{1,\ldots,n\}/\sim$ é designado por Q, tomamos o conjunto $\{(a, s(a), \ldots, s^{r-1}(a)) \mid \bar{a} \in Q\}$ de ciclos, disjuntos desta feita. Afirmamos, agora, que s é igual ao produto de todos os ciclos que são membros deste conjunto. Com efeito, se s' designa tal produto, é claro que tem-se $s(a) = s'(a)$ para todo $a \in \{1, \ldots, n\}$. Em outras palavras, pela definição de igualdade de aplicações, $s = s'$. C.Q.D.

Corolário - Todo elemento de S_n é um produto de 2-ciclos.

Demonstração: Basta observar que todo e qualquer ciclo $(a_1 \ldots a_r)$ é igual ao produto $(a_1a_2)(a_1a_3) \ldots (a_1a_r)$ e usar a proposição anterior.

Um 2-ciclo é também chamado uma transposição. Uma permutação $s \in S_n$ é dita par (respectivamente, ímpar) se for produto de um número par (respectivamente, ímpar) de transposições. Mostra-se que esta definição é boa, isto é, se s é escrita como algum produto de um número par de transposições então outra qualquer representa

ção de s como produto de transposições admite sempre um número par de transposições.

É claro que a permutação idêntica é par e que o produto de duas permutações pares é par. Segue-se (veja a Proposição na seção 1.1 que dá um critério de subgrupo finito) que o conjunto A_n das permutações pares é um subgrupo de S_n. Ora, o produto de uma permutação par por uma ímpar é uma permutação ímpar; como S_n tem pelo menos uma permutação ímpar se $n \geq 2$, a saber, o ciclo (12), segue-se que S_n tem tantas permutações pares como ímpares se $n \geq 2$. Em outras palavras, A_n tem $n!/2$ elementos se $n \geq 2$. A_n é chamado o grupo alternado em n símbolos e é importante na teoria das equações.

1.4. Isomorfismos de grupos. Teorema de Cayley.

Já vimos, anteriormente, que dois grupos finitos podem ter comportamentos distintos ainda que possuam o mesmo número de elementos. Precisamos de uma noção mais sutil do que a de "número de elementos" para decidir se dois grupos são essencialmente iguais, isto é, se têm tabelas de multiplicação iguais (caso finito).

A matéria prima é o conceito de homomorfismo: trata-se de uma aplicação $f: G \to H$, onde G e H são grupos, satisfazendo a condição:

$$f(a.b) = f(a) \,.\, f(b).$$

(Designamos o produto em G e o produto em H pelo mesmo símbolo

$\circ$; não há confusão séria nesta ambiguidade).

A primeira observação é que se $f: G \to H$ é um homomorfismo, então $f(e)$ é o elemento neutro de H, onde e é o elemento neutro de G.

Exemplo: Seja $\{1,-1\} \subset \mathbb{Q}$ o subgrupo multiplicativo dos racionais constituído por 1 e -1. Seja $\psi: S_n \to \{1,-1\}$ a aplicação que associa 1 a uma permutação par e -1, a uma ímpar. Então ψ é um homomorfismo.

Seja $f: G \to H$ um homomorfismo. Se a aplicação f é injetora (respectivamente, sobrejetora, bijetora), f é dito um monomorfismo (respectivamente, epimorfismo, isomorfismo).

Definição - Dois grupos G e H são isomorfos se existe um isomorfismo $f: G \to H$.

Exercício: Mostre que o grupo G das simetrias planas do quadrado e o grupo H das simetrias (espaciais) de um retângulo não quadrado não são isomorfos.

Exercício: Mostre que S_3 e o grupo das simetrias (espaciais) do triângulo equilátero são isomorfos.

Para ilustrar o fato de que um mesmo grupo pode aparecer sob formas aparentemente distintas, consideremos o conjunto G constituído pelas seguintes funções de $\mathbb{R}\setminus\{0,1\}$ (reta real menos 0 e 1) em $\mathbb{R}\setminus\{0,1\}$:

$$I: x \longmapsto x$$

$$f_1: x \longmapsto \frac{1}{x} \qquad F_2: x \longmapsto \frac{1}{1-x}$$

$$f_2: x \longmapsto 1-x$$

$$f_3: x \longmapsto \frac{x}{x-1} \qquad F_2: x \longmapsto \frac{x-1}{x}$$

Mediante a composição usual de funções, G constitui um subgrupo do grupo de todas as bijeções de $\mathbf{R}\setminus\{0,1\}$ em si mesmo (leitor: verifique esta afirmação).

Consideremos a seguinte aplicação $\varphi: G \to S_3$:

$$\varphi(I) = I \quad , \quad \varphi(f_i) = r_i \quad , \quad i = 1, 2, 3$$
$$\varphi(F_j) = R_j \quad , \quad j = 1, 2$$

É claro que φ é bijetora. Deixamos ao leitor o cuidado de verificar que φ é um homomorfismo (alguma medida de economia em vista?). Logo, φ é um isomorfismo, isto é, o grupo acima é essencialmente o grupo simétrico S_3.

Toda a importância teórica dos grupos de permutações S_n reside no seguinte resultado, devido ao matemático inglês A. Cayley (século XIX):

Teorema (Cayley) - Seja G um grupo finito. Então G é isomorfo a um subgrupo de S_n para algum n.

Demonstração: Suponhamos que G tem n elementos. Mostraremos que G é isomorfo a um subgrupo de S_n ou, o que é o mesmo, a um subgrupo de S_G = grupo das bijeções de G em G. Definamos $\varphi: G \to S_G$ da seguinte maneira:

$$\varphi(a) = f_a \ ,$$

onde $f_a: G \to G$ é tal que $f_a(x) = a.x$ para todo $x \in G$. Precisamos, primeiramente, verificar que f_a é uma bijeção. Ora, como a operação de grupo é cancelativa, segue-se que f_a é injetora; mas f_a é também sobrejetora; mas f_a é também sobrejetora como se vê facil

mente. Assim, temos com efeito $f_a \in S_G$.

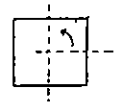
Verifiquemos que φ é um homomorfismo (recordamos que a operação de S_G é a composição usual de funções). Temos que verificar que $f_{a.b} = f_a.f_b$ para dois elementos $a,b \in G$ quaisquer; mas, isto decorre imediatamente da definição de f_a e da associatividade do produto em G.

Resta verificar que φ é injetora, do que decorrerá então que G é isomorfo ao subgrupo $\varphi(G) \subset S_G$, onde $\varphi(G) = \{\varphi(a) \mid a \in G\}$ (Exercício: verifique que $\varphi(G)$ é efetivamente subgrupo de S_G). Suponhamos então que se tenha $\varphi(a) = \varphi(b)$, isto é, que $f_a = f_b$. Segue-se que $a.x = b.x$ para todo $x \in G$. Em particular, com $x = e$, obtemos $a = b$. C.Q.D.

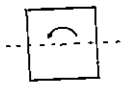
A vantagem do teorema de Cayley é que permite transplantar questões sobre um dado grupo finito G para questões sobre permutações de n objetos. Na prática, porém, tal procedimento pode oferecer desvantagens, principalmente se G tem muitos elementos. Para ilustrar esta situação, consideremos o seguinte

Exemplo: D_4 = grupo das simetrias espaciais do quadrado. As simetrias são em número de 8, como segue.

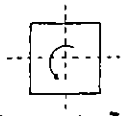
I = rotação de 0 rad^s.



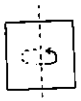
R_1 = rotação plana de $\pi/2$ rad^s.



R_2 = rotação plana de π rad^s.



R_3 = rotação plana de $3\pi/2$ rad^s.



M_1 = rotação do π rd^s em torno de uma mediana

M_2 = rotação de π rd^s em torno da outra mediana

D_1,D_2 = rotações de π rd^s em torno das diagonais, respectivamente

Pelo teorema de Cayley, sabemos que D_4 é isomorfo a um subgrupo de S_8. Mas, S_8 é bastante abusivo já que possui $8! = 40.320$ elementos ... . Será que é possível ter-se um isomorfismo de D_4 com um subgrupo de S_n, com $n < 8$? A resposta é afirmativa e na verdade, podemos escolher $n = 4$.

Deixamos a demonstração detalhada e rigorosa a cargo do leitor; a idéia em si é a mesma usada no caso das simetrias do triângulo equilátero. A saber, enumeramos os vértices do quadrado de 1 a 4. Cada simetria pode então ser "representada" por uma permutação de 4 símbolos. Esta "representação" fornece a aplicação procurada, que é automaticamente injetora. O único trabalho é verificar que se tra-

ta de um homomorfismo.

Exercício: Verifique que a aplicação $D_4 \to S_4$ explicada acima é um homomorfismo. Seja D_n o grupo das simetrias espaciais de um polígono regular de n lados; generalize o exemplo anterior para D_n.

Exercício: Seja $s = (1\ 2\ 3\ 4) \in S_4$. Mostre que $\{s^n \mid n \in \mathbb{Z}\}$ é um subgrupo de S_4 com 4 elementos e que tal subgrupo é isomorfo ao grupo das rotações planas do quadrado.

Exercício: Verifique que o conjunto das raízes complexas da equação $x^n - 1 = 0$ constitui um grupo mediante a multiplicação usual de números complexos. Descreva explicitamente os elementos desse grupo (em termos da aplicação exponencial e^z ou das funções cos e sen).

1.5. Grupos cíclicos. Geradores de um grupo. Aplicação às regras de casamento nas sociedades primitivas.

Até agora, não demos um algoritmo efetivo de construção dos subgrupos de um grupo. Dado um grupo finito "concreto" (por exemplo, o grupo das simetrias espaciais de um polígono regular), pode-se pensar em usar o computador. Em geral, porém, necessitamos de algumas técnicas teóricas que permitam construir subgrupos.

Surge então, naturalmente, a seguinte pergunta: dado um

grupo G e um subconjunto S de G, qual é o menor(*) subgrupo H de G que contém os elementos de S? Evidentemente, o primeiro caso a considerar é o caso em que $S = \{a\}$ é constituído por um único elemento. (O caso $S = \emptyset$ admite $H = \{e\}$ como solução do problema).

Primeiro, é evidente que se existe um tal subgrupo H de G, então H deve conter os produtos $a \ldots a$, isto é, H deve conter todas as pontências do elemento a:

$$\{\ldots, a^{-n}, \ldots, a^{-1}, a^{o} = e, a^{1}, \ldots, a^{n}, \ldots\}.$$

Chamemos $\langle a \rangle$ este conjunto. Por outro lado, verifica-se imediatamente que $\langle a \rangle$ já constitui um subgrupo de G. Pela condição do problema, concluímos que dá-se a igualdade $H = \langle a \rangle$. Assim, o menor subgrupo de um grupo G que contém o elemento $a \in G$ é o subgrupo $\langle a \rangle$ das potências de a. Dizemos que $\langle a \rangle$ é <u>gerado por</u> a.

Salta aos olhos a semelhança entre os subgrupos $\langle a \rangle$ e $\langle b \rangle$, onde a, b são dois elementos quaisquer de um grupo G. Na verdade, existem essencialmente dois tais grupos, conforme indica a proposição seguinte:

<u>Proposição</u> - Se $\langle a \rangle$ é um grupo gerado por um elemento a, então ou $\langle a \rangle$ é isomorfo ao grupo dos inteiros $\mathbb{Z}$ ou $\langle a \rangle$ é isomorfo ao grupo das rotações planas (isto é, simetrias planas) de um polígono regular de n lados, para algum $n \geq 1$.

<u>Demonstração</u>: Temos, por definição, $\langle a \rangle = \{\ldots, a^{-1}, e, a, \ldots\}$. Há

(*) Menor aqui refere-se à relação $\subset$ de inclusão de conjuntos. Em outras palavras, H é tal que está contido em todo subgrupo de G que contém os elementos de S.

dois casos a considerar:

(i) Não existem números inteiros distintos m_1, m_2 tais que se verifique $a^{m_1} = a^{m_2}$.

Definamos uma função $\varphi: \mathbb{Z} \to \langle a \rangle$ da seguinte maneira:

$$\varphi(m) = a^m \quad , \quad \text{para todo} \quad m \in \mathbb{Z}.$$

Por definição de $\langle a \rangle$, a^m é a forma geral de um elemento de $\langle a \rangle$. Isto acarreta ser φ sobrejetora. Por outro lado, φ é também injetora pela condição (i) em consideração. Para concluir que φ é um isomorfismo e que, portanto, $\langle a \rangle$ e $\mathbb{Z}$ são grupos isomorfos, basta demonstrar que φ é um homomorfismo.

Queremos, então, mostrar que $\varphi(m+n) = \varphi(m) + \varphi(n)$ para todos $m,n \in \mathbb{Z}$; em outras palavras, queremos verificar a regra dos expoentes inteiros num grupo:

$$a^m.a^n = a^{m+n} \quad , \quad \text{todos} \quad m,n \in \mathbb{Z}.$$

Verifiquemos a validade desta regra.

Para $m = 0$ ou $n = 0$, a igualdade é obviamente verificada. Suponhamos $m > 0$, $n > 0$. Neste caso, por definição, $a^m \cdot a^n = (\underbrace{a \cdot \ldots \cdot a}_{m \text{ vezes}}) \cdot (\underbrace{a \cdot \ldots \cdot a}_{n \text{ vezes}}) = \underbrace{a \cdot \ldots \cdot a}_{m+n \text{ vezes}}$, usando a associatividade da operação de grupo (*).

Suponhamos $m < 0$, $n < 0$. Neste caso, temos por definição:

(*) Observemos que $\underbrace{a \cdot \ldots \cdot a}_{m \text{ vezes}}$ está definido sem ambiguidade em virtude da associatividade e por um emprego simples do princípio de indução finita (veja Lista de Exercícios, Exerc. 4(c)).

$$a^m = (a^{-1})^{-m} = a^{-1} \cdot \ldots \cdot a^{-1} \quad (-m \text{ vezes})$$

$$a^n = (a^{-1})^{-n} = a^{-1} \cdot \ldots \cdot a^{-1} \quad (-n \text{ vezes})$$

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

A demonstração reduz-se ao caso anterior com o elemento $b = a^{-1}$.

Finalmente, o caso em que, digamos, $m > 0$ e $n < 0$ com $m > -n$. Neste caso, $a^m = a^{m+n-n} = a^{m+n}.a^{-n}$ pelo primeiro caso, já que $m+n > 0$ e $-n > 0$. Logo, resulta

$$a^{m+n} = a^m.a^n,$$

multiplicando a igualdade $a^m = a^{m+n}.a^{-n}$ à direita por a^{-1} $-n$ vezes.

Observação: A demonstração acima envolve, se verificada cuidadosamente, um argumento de indução finita. O leitor pode tentar uma demonstração mais elegante e econômica usando o princípio de indução finita.

(ii) Existem inteiros distintos m_1, m_2 tais que $a^{m_1} = a^{m_2}$.

Pela regra dos expoentes (observemos que tal regra é sempre válida, a demonstração dada acima não usou a condição (i) para o elemento a):

$$a^{m_1-m_2} = a^{m_1}.a^{-m_2} = a^{m_2-m_2} = a^0 = e$$

Supondo, digamos, $m_1 > m_2$, concluimos assim que existe um inteiro positivo m tal que $a^m = e$. Como o conjunto dos inteiros positivos é um subconjunto de $\mathbb{N}$, existe um menor inteiro positivo r tal que $a^r = e$.

Afirmamos que vale a igualdade $\langle a \rangle = \{e, a, \ldots, a^{r-1}\}$.

Com efeito, seja a^m um elemento qualquer de $\langle a \rangle$. Pelo algoritmo euclideano de divisão (veja Lista de Exercícios, Exercício 4(e)), existem inteiros q e s tais que

$$m = rq + s \quad , \quad 0 \leq s < r.$$

Novamente pela regra dos expoentes, obtemos:

$$a^m = a^{rq+s} = a^{rq}.a^s = \begin{cases} \underbrace{(a^r \cdot \ldots \cdot a^r)}_{q \text{ vezes}} \cdot a^s = (a^r)^q.a^s & , \text{ se } q > 0 \\ a^0 \cdot a^s = a^s & , \text{ se } q = 0 \\ \underbrace{a^{-r} \cdot \ldots \cdot a^{-r}}_{-q \text{ vezes}} \cdot a^s = ((a^{-1})^r)^{-q}.a^s & , \text{ se } q < 0. \end{cases}$$

Nos dois primeiros casos, obtemos imediatamente $a^m = a^s$. No terceiro caso, é fácil ver que $(a^{-1})^r = e$ vale ; com efeito, de $a.a^{-1} = e$ resulta $(a.a^{-1}) \cdot (a.a^{-1}) \ldots (a.a^{-1}) = (a.a^{-1})^r = e^r = e$ e, como $a.a^{-1} = a^{-1}.a$, resulta enfim que $a^r.(a^{-1})^r = e$, logo, $(a^{-1})^r = (a^r)^{-1} = e^{-1} = e$. Assim, $a^m = a^s$ também no terceiro caso.

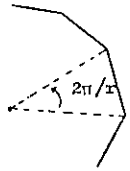
Desta maneira, vemos que $a^m \in \{e, a, \ldots, a^{r-1}\}$ para todo $m \in \mathbb{Z}$. Donde segue que $\langle a \rangle = \{e, a, \ldots, a^{r-1}\}$.

Finalmente, é claro que os elementos $e, a, \ldots, a^{r-1}$ são distintos. Com efeito, se $a^s = a^t$, com $0 \leq s < t \leq r-1$, então $a^{t-s} = e$, onde $0 < t-s < r$. Isto contradiz a definição do inteiro r.

Definamos uma aplicação $p: \langle a \rangle \to C_r$, onde C_r é o grupo das simetrias planas de um polígono regular de r lados:

$$\varphi(a^n) = R_1^n \ ,$$

onde $0 \leq n < r$ e R_1 = rotação plana de $2\pi/r$ radianos.



polígono regular de
r = lados

Aqui, como sempre, $R_1^n = R_1 \circ \ldots \circ R_1$ (n vezes). Como a regra de expoentes foi estabelecida anteriormente para um grupo abstrato, resulta ser válida em C_r também. Logo, φ é um homomorfismo. Por outro lado, φ é sobrejetora; com efeito, toda simetria plana do polígono é uma rotação de um múltiplo inteiro de $2\pi/r$, isto é, é da forma R_1^n, com n inteiro (positivo ou nulo).

Finalmente, do fato que r é o menor inteiro positivo tal que R_1^r = identidade, segue-se que φ é injetora. Logo $\langle a \rangle$ e C_r são isomorfos. C.Q.D.

Grupos gerados por um elemento aparecem tão comumente que convém dar-lhes nome.

Definição - Um grupo $\langle a \rangle$ é chamado um grupo cíclico infinito se $\langle a \rangle$ for isomorfo a $\mathbb{Z}$; se $\langle a \rangle$ for isomorfo ao grupo C_n das simetrias planas de um polígono regular de n lados, $\langle a \rangle$ será chamado grupo cíclico finito de ordem n.

As duas possibilidades são, em virtude da última proposição, mutuamente exclusivas. A menos de isomorfismo, existe um único grupo cíclico de ordem n ($n = 1, 2, \ldots, \infty$).

Uma propriedade fundamental dos grupos cíclicos é que eles

são abelianos (duas potências de um mesmo elemento sempre comutam entre si!). Além disso, servem de blocos fundamentais para a construção de grupos abelianos de uma certa classe.

Voltemos, entrementes, ao nosso problema original que consistia em construir o menor subgrupo contendo um certo subconjunto. Assim, seja G um grupo, $E \subset G$ um subconjunto de G. Se E reduz-se a um único elemento a, a solução é o grupo cíclico (a) gerado por a. Em geral, resolvemos o problema da seguinte maneira: existe pelo menos um subgrupo de G contendo E, a saber, o próprio G. Assim, existe um ou mais subgrupos de G contendo E. Se estamos procurando algo suficientemente pequeno ainda contendo E, é natural considerar a interseção

$H = \bigcap H_i$, onde H_i percorre o conjunto de todos os subgrupos de G contendo E.

Na verdade, temos o seguinte resultado:

Proposição - Seja G um grupo e seja $E \subset G$ um subconjunto qualquer de G. Então o menor subgrupo de G contendo E existe e é dado por $H = \bigcap H_i$, onde H_i percorre o conjunto de todos os subgrupos de G contendo E. Explicitamente, se $E \neq \emptyset$, um elemento de H é da forma $b_1 \cdot \ldots \cdot b_r$, onde b_i é um elemento de E ou o inverso de um elemento de E.

Demonstração: Mostremos que $H = \bigcap H_i$ é um subgrupo de G. É claro que $H \neq \emptyset$ pois o elemento neutro de G pertence a cada H_i. Em seguida, sejam $a,b \in H$, então $a,b \in H_i$ para todo i,

(já que H_i é subgrupo de G). Segue-se que $a.b \in H$. Finalmente, se $a \in H$ então $a^{-1} \in H_i$ para todo i, logo $a^{-1} \in H$.

Ora, como H é um subgrupo de G e contém o subconjunto E, segue-se que H contém o menor subgrupo de G contendo E. Mas, este último é um dos H_i, logo deve coincidir com H.

Finalmente, o subconjunto

$$H' = \{b_1 \circ \ldots \circ b_r \mid b_j \in E \text{ ou } b_j^{-1} \in E\} \subset G$$

é um subgrupo de G (se $E \neq \emptyset$) como se vê facilmente. Ora, $E \subset H'$. Logo, $H = H'$. C.Q.D.

Definição - Se G é um grupo e $E \subset G$ um subconjunto, o subgrupo de G gerado por E é o menor subgrupo de G contendo E. Notação: $\langle E \rangle$. Diz-se também que E é um sistema de geradores de $\langle E \rangle$.

Exemplos: (a) Um subgrupo de G é um grupo cíclico se e só se for gerado por um conjunto constituído de um único elemento de G.

(b) O subgrupo $\{1,-1\}$ do grupo dos racionais $\neq 0$ (multiplicativamente) é gerado por $\{-1\}$. Na verdade, existe essencialmente um só grupo com dois elementos, cuja tabela é necessariamente da forma seguinte:

	e	a
e	e	a
a	a	e

Um grupo com dois elementos é necessariamente cíclico.

(c) Existe um único grupo de três elementos, a menos de isomorfismo. A tabela é a seguinte:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

(Leitor: verifique a afirmação acima como exercício).
Logo, tal grupo é cíclico.

(d) O grupo G das rotações planas do quadrado é um grupo cíclico, gerado, por exemplo, pela rotação de $\pi/2$ radianos.

(e) O grupo das simetrias espaciais de um retângulo não quadrado é gerado pelo subconjunto $\{r_2', r_3'\}$ constituído de uma rotação plana de (π radianos) e de uma espacial em torno de uma mediana. Os subconjuntos $\{r_2', r_4'\}$, $\{r_3', r_4'\}$ são sistemas de geradores alternativos do grupo. Como este grupo não é isomorfo ao grupo do exemplo (d), ele não pode ser gerado por um único elemento, o que, de resto, se verifica diretamente.

Exercício: Determine um sistema de geradores do grupo D_3 das simetrias do triângulo equilátero.

Exercício: Se $\varphi: G \to H$ é um isomorfismo e $E \subset G$ é um sistema de geradores de G, então $\varphi(E)$ é um sistema de geradores de H, onde $\varphi(E) = \{\varphi(g) \mid g \in E\}$. Analise a validade deste resultado se φ for apenas um homomorfismo e se φ for um epimorfismo (os

dois casos separadamente).

Observação: É evidente que todo grupo admite ao menos um sistema de geradores, a saber, o conjunto de todos os elementos do grupo. Em outras palavras, se G é um grupo e H, um subgrupo de G, então $H = \langle H \rangle$. Contudo, o que é de algum interesse é determinar sistemas de geradores mínimos num certo sentido. Por exemplo, no grupo das simetrias do retângulo não quadrado, sistemas mínimos de geradores têm exatamente dois elementos.

Pode-se descrever um grupo exibindo um sistema de geradores e as "equações" não triviais que os elementos de tal sistema satisfazem. Por exemplo, um grupo cíclico finito de ordem n é descrito da seguinte maneira:

$$G = \langle a : a^n = e \rangle.$$

O grupo das simetrias do retângulo não quadrado:

$$H = \langle a,b : ab = ba \ , \ a^2 = e \ , \ b^2 = e \rangle.$$

O grupo das simetrias do triângulo equilátero:

$$D_3 = \langle a,b : a^3 = e \ , \ b^2 = e \ , \ ba = a^{-1} b \rangle.$$

É um bom exercício verificar que, não só o número de elementos nos sistemas de geradores acima é menor possível, como também o número de "equações" é menor possível.

Exercício: Mostre que o grupo D_3 pode ser descrito pelos seguintes sistemas de geradores e "equações":

$$D_3 = \langle a;b : a^2 = e \ , \ b^2 = e \ , \ (ab)^3 = e \rangle.$$

(Isto mostra que a representação de um grupo por meio de sistemas de geradores e "equações" mínimais não é unicamente determinada).

É um divertimento instrutivo "inventar" grupos prescrevendo sistemas de geradores e "equações"; ao fazê-lo, o leitor deve procurar escrever "equações" independentes num certo sentido (isto é , equações mínimas) e tentar comparar com exemplos concretos de grupos.

Passemos, entrementes, a uma aplicação da teoria dos grupos de permutações e da noção de sistema de geradores a um problema de antropologia que consiste em deslindar a possibilidade de casamento entre dois descendentes de ancestrais comuns, dentro das leis rígidas de casamento das sociedades primitivas. O aspecto antropológico propriamente dito pode ser encontrado no livro "Les structures élémentaires de la parenté", de C.Levi-Strauss (Presses Universitaires de France, 1949). A formulação matemática do problema, conforme exibimos a seguir, é devida a André Weil (Institute for Advanced Study, Princeton, N.J., EE.UU.) e aparece como apêndice ao citado livro.

As regras de casamento em certas sociedades primitivas são regidas pelos seguintes axiomas (ou leis):

1. Cada membro da sociedade pertence a um e um só tipo (de casamento). A sociedade tem um número finito de tipos.
2. Um homem e uma mulher podem casar-se se e só se pertencem a um mesmo tipo.
3. O tipo de um membro da sociedade é unicamente determinado pelo seu sexo e pelo tipo dos pais (Observação: o pai e a mãe pertencem necessariamente ao mesmo tipo, mas não o filho ou a filha).
4. Dois rapazes (ou duas moças) cujos pais pertencem a tipos diferen

tes a tipos distintos.

5. Um homem e sua irmã pertencem a tipos distintos (isto é, incesto fraterno é proibido).
6. Se um homem e uma mulher são parentes, a possibilidade ou impossibilidade de se casarem dependem apenas da relação de parentesco (e não do tipo a que pertence o homem).
7. Dados dois membros da sociedade, é permitido a alguns de seus descendentes contrair casamento.

Vamos, entrementes, traduzir matematicamente os axiomas acima. Pelo axioma 1, a sociedade admite um conjunto finito $T = \{t_1, \ldots, t_n\}$ de tipos e tal conjunto constitui uma partição do conjunto dos membros da sociedade. Axioma 2 significa que um homem e uma mulher pertencentes a tipos t_i, t_j, respectivamente, tais que $t_i \neq t_j$, não podem casar-se. Evidentemente, esta não é uma formulação matemática por causa de termo "não poder casar-se". Na verdade, o axioma 2 interessar-nos-á na medida em que homem e mulher têm grau de parentesco; neste caso, teremos fórmulas "de passagem" de um a outro. Uma tal fórmula aplicada a um tipo t_i dá um certo tipo t_j. O "poder casar-se" é traduzido pela propriedade de que tal fórmula aplicada a t_i, para todo $t_i \in T$, fornece o próprio t_i.

Como traduzir o axioma 3 ? Dado um casal de pais de um tipo (necessariamente comum) t, o tipo de um filho (homem) é uma função de t somente, digamos, $t \to m(t)$. Analogamente, o tipo de uma filha é função de t somente; seja $t \to f(t)$. Assim, matematicamente:

Axioma 3 (bis). Existem duas aplicações $m: T \to T$ e $f: T \to T$.

O axioma 4 significa que se $t_i \neq t_j$ (isto é, se $i \neq j$) então $m(t_i) \neq m(t_j)$ e $f(t_i) \neq f(t_j)$. Em outras palavras:

Axioma 4 (bis). As aplicações m e f são injetoras, logo, são permutações do conjunto T (porque T é finito).

Fórmulas de passagem I: se um homem é do tipo t, ambos pais pertencem ao tipo $m^{-1}(t)$ e sua irmã pertence ao tipo $f(m^{-1}(t)) = (f \circ m^{-1})(t)$, onde $\circ$ denota o produto de permutações. Da mesma forma, se uma mulher é do tipo t, seu irmão é do tipo $(m \circ f^{-1})(t)$.

O axioma 5 traduz-se facilmente por:

Axioma 5 (bis). Para todo t, $m(t) \neq f(t)$. Ou ainda, pelas fórmulas de passagem I, $(f \circ m^{-1})(t) \neq t$ para todo $t \in T$.

O axioma 6 é o mais delicado. Para fixar idéias comecemos pelo caso em que homem e mulher são primos (do 1º grau). Neste caso, existem quatro possíveis relações de parentesco:

(a) (b) (c) (d)

Os diagramas acima, usados pelos antropólogos, são interpretados de acordo com a seguinte lista de símbolos:

△ : homem

○ : mulher

= : casamento

| : descendente

⌐¬ : par de filhos (o símbolo ⌐¬ aparece em conjunto com |)

Se t é o tipo do homem, o tipo de sua prima no caso (a) de parentesco é $f(m(m^{-1}(m^{-1}(t))))$, ao passo que no caso (d) é $f(m(f^{-1}(m^{-1}(t))))$. Podemos dizer que as permutações $f \circ m \circ m^{-2}$ e $f \circ m \circ f^{-1} \circ m^{-1}$ exprimem, respectivamente, o parentesco em questão. No caso de parentesco deste tipo, isto é, primos de 1º grau, o axioma 6 traduz-se por:

Axioma 6 (bis)(caso (d)). $f(m(f^{-1}(m^{-1}(t)))) = t$ para todo $t \in T$

ou $f(m(f^{-1}(m^{-1}(t)))) \neq t$ para todo $t \in T$.

Isto é, ou $f \circ m \circ f^{-1} \circ m^{-1}$ é a permutação idêntica ou não deixa invariante nenhum elemento de T.

Se o parentesco é mais complicado, as expressões que o traduzem são permutações da forma $g_1 \circ \ldots \circ g_r$, onde $g_i \in \{m,f\}$ ou $g_i^{-1} \in \{m,f\}$. Cada uma dessa permutações, por sua vez, indica um parentesco. Então o axioma 6 fica satisfeito se exigirmos o seguinte:

Axioma 6 (bis). Todo elemento do subgrupo $\langle m,f \rangle$ de S_T gerado por m e f é a permutação idêntica ou não deixa invariante nenhum elemento de T.

Finalmente, para traduzir o axioma 7, observemos que ele implica que dados tipos t, t', tem-se que descendentes respectivos pertencem a tipos $(g_1 \circ \ldots \circ g_r)(t)$ e $(h_1 \circ \ldots \circ h_s)(t')$ iguais. Logo,

$t' = (h_s^{-1} \circ \ldots \circ h_1^{-1} \circ g_1 \circ \ldots \circ g_r)(t)$. Aqui, como acima, $g_i \in \langle m,f \rangle$ e $h_j \in \langle m,f \rangle$.

Reciprocamente, o leitor mostrará que dados indivíduos de tipos t, t' respectivamente, se existir $h \in \langle m,f \rangle$ tal que

$t' = h(t)$ então alguns descendentes dos indivíduos podem casar-se. Assim:

Axioma 7 (bis). O subgrupo $G = \langle m,f \rangle$ opera <u>transitivamente</u> sobre T, isto é, dados $t,t' \in T$ quaisquer, existe $h \in G$ tal que $t' = h(t)$.

Concluindo, temos o resultado fundamental:

<u>Proposição</u> - Os axiomas (leis de casamento) são preservados se e só se m, f geram um subgrupo G de S_T tal que:

(i) todo elemento de G diferente de I não fixa nenhum elemento de T

(ii) para todos $t,t' \in T$ existe $h \in G$ tal que $t' = h(t)$.

<u>Observação</u>: Tais subgrupos de S_T são chamados "regulares" e é fácil ver que possuem o mesmo número de elementos que T.

<u>Exemplo</u>: Todas as possibilidades para uma sociedade com 4 tipos de casamento.

Trata-se de determinar todos os subgrupos regulares de S_4 com 4 elementos. A menos de isomorfismo, temos apenas dois grupos de ordem 4: o grupo cíclico de ordem 4 e o grupo de Klein. É suficiente, portanto, considerar apenas um exemplo de cada um desses grupos, ou melhor, um modelo abstrato dos mesmos.

Um grupo cíclico de ordem 4 é da forma $G = \{e,a,a^2,a^3\}$. É fácil ver que a e a^3 são os únicos geradores (cíclicos) de G, logo têm papel simétrico. Basta, então, tomarmos a. Do ponto de vista do problema do casamento, interessa-nos conjuntos de geradores

constituídos de dois elementos. Temos, então, as seguintes possibilidades:

(1) $m = a$, $f = a^2$

(2) $m = a^2$, $f = a$

(3) $m = a$, $f = a^3$

(4) $m = a$, $f = e$

(5) $m = e$, $f = a$ (sociedade de Taran)

Para fixar idéias, podemos tomar $a = (1\ 2\ 3\ 4) \in S_4$. Por exemplo, o caso (1) obedece então às seguintes leis de tipo:

Pais	filho	filha
t_1	t_2	t_3
t_2	t_3	t_4
t_3	t_4	t_1
t_4	t_1	t_2

A sociedade de Taran (caso (5)) obedece às leis seguintes:

Pais	filho	filha
t_1	t_1	t_2
t_2	t_2	t_3
t_3	t_3	t_4
t_4	t_4	t_1

Considerando o grupo de Klein, vê-se que há essencialmente uma possibilidade (exercício); todas as outras diferem apenas por uma reordenação dos tipos. A sociedade de Kariera (Oceania) obedece a tal esquema:

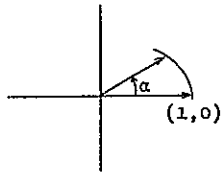
Pais	filho	filha
t_1	t_2	t_3
t_2	t_1	t_4
t_3	t_4	t_1
t_4	t_3	t_2

2. Noções sobre Grupos Clássicos

2.1. O grupo das rotações planas.

Intuitivamente, sabemos o que significa efetuar uma rotação no plano usual $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ em torno do eixo perpendicular ao plano e passando pela origem $(0,0)$. Do ponto de vista da álgebra linear, podemos expressar tal rotação por meio de certas matrizes.

Com efeito, uma rotação de ângulo $\alpha \in \mathbb{R}$, transforma o ponto de coordenadas $(1,0)$ (isto é, gira o vetor unitário $\vec{e}_1$) no ponto de coordenadas $(\cos \alpha, \text{sen } \alpha)$ (isto é, até coincidir com o vetor $(\cos \alpha)\vec{e}_1 + (\text{sen } \alpha)\vec{e}_2$).



Analogamente, o ponto $(0,1)$ é transformado no ponto $(-\text{sen } \alpha, \cos \alpha)$. Assim, a rotação de ângulo α é a aplicação linear do plano representada, na base canônica $\vec{e}_1$, $\vec{e}_2$, pela matriz

$$\begin{pmatrix} \cos \alpha & -\text{sen } \alpha \\ \text{sen } \alpha & \cos \alpha \end{pmatrix}$$

O que acontece se multiplicarmos duas matrizes deste tipo? A multiplicação a que nos referimos é o produto usual de matrizes, o

qual corresponde, uma vez fixada uma base, à composição de aplicações (lineares). Assim dados $\alpha,\alpha' \in \mathbb{R}$, tem-se:

$$\begin{pmatrix} \cos\alpha & -\operatorname{sen}\alpha \\ \operatorname{sen}\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\alpha' & -\operatorname{sen}\alpha' \\ \operatorname{sen}\alpha' & \cos\alpha' \end{pmatrix} =$$

$$\begin{pmatrix} \cos\alpha\cos\alpha' - \operatorname{sen}\alpha\operatorname{sen}\alpha' & -(\cos\alpha\operatorname{sen}\alpha' + \operatorname{sen}\alpha\cos\alpha') \\ \operatorname{sen}\alpha\cos\alpha' + \cos\alpha\operatorname{sen}\alpha' & \cos\alpha\cos\alpha' - \operatorname{sen}\alpha\operatorname{sen}\alpha' \end{pmatrix}$$

$$= \begin{pmatrix} \cos(\alpha+\alpha') & -\operatorname{sen}(\alpha+\alpha') \\ \operatorname{sen}(\alpha+\alpha') & \cos(\alpha+\alpha') \end{pmatrix}$$

que é ainda uma matriz do mesmo tipo, correspondente à rotação de ângulo $\alpha+\alpha'$. Em particular, o produto de duas tais matrizes é comutativo e obtém-se

$$\begin{pmatrix} \cos\alpha & -\operatorname{sen}\alpha \\ \operatorname{sen}\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos(-\alpha) & -\operatorname{sen}(-\alpha) \\ \operatorname{sen}(-\alpha) & \cos(-\alpha) \end{pmatrix} = \begin{pmatrix} \cos 0 & -\operatorname{sen} 0 \\ \operatorname{sen} 0 & \cos 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Podemos recolher os pedaços na seguinte

Proposição - As rotações planas em torno da origem constituem um grupo abeliano G, a saber, o grupo multiplicativo das matrizes

$$\begin{pmatrix} \cos\alpha & -\operatorname{sen}\alpha \\ \operatorname{sen}\alpha & \cos\alpha \end{pmatrix}, \quad \text{com} \quad \alpha \in \mathbb{R}.$$

Além disso, existe um homomorfismo φ do grupo aditivo dos números reais sobre G, dado por

$$\varphi(\alpha) = \begin{pmatrix} \cos\alpha & -\operatorname{sen}\alpha \\ \operatorname{sen}\alpha & \cos\alpha \end{pmatrix} .$$

O subgrupo $2\pi\,\mathbb{Z} = \{2\pi m \mid m \in \mathbb{Z}\}$ de $\mathbb{R}$ é exatamente o subgrupo dos reais α tais que $\varphi(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Exercício: Mostre que os números complexos de módulo = 1 (isto é, os complexos $\alpha + \beta i$ tais que $\alpha^2 + \beta^2 = 1$) constituem um subgrupo multiplicativo dos complexos $\neq 0$ (chamamo-lo de o grupo do círculo). Verifique que o grupo do círculo é isomorfo ao grupo das rotações planas em torno da origem.

Observemos que o subgrupo $2\pi\,\mathbb{Z}$ de $\mathbb{R}$ define, de maneira natural, uma relação de equivalência em $\mathbb{R}$ de tal maneira que dois reais estão numa mesma classe desta equivalência se sua diferença é um múltiplo inteiro de 2π. Vê-se, assim, que do ponto de vista estritamente da teoria dos grupos, não há distinção possível entre as seguintes noções: classes de equivalência de números reais pela relação mencionada acima, números complexos de módulo 1, rotações planas em torno da origem, matrizes da forma

$$\begin{pmatrix} \cos\alpha & -\operatorname{sen}\alpha \\ \operatorname{sen}\alpha & \cos\alpha \end{pmatrix}, \quad \text{com } \alpha \text{ real.}$$

Em seguida, daremos mais uma noção "isomorfa" às quatro noções acima.

Definição - Uma matriz 2×2 real $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ chama-se ortogonal se as seguintes condições forem preenchidas:

$$p^2 + q^2 = r^2 + s^2 = 1 \quad , \quad pr + qs = 0.$$

Por exemplo, as matrizes $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ são ortogonais Mais geralmente, a matriz

$$\begin{pmatrix} \cos \alpha & -\operatorname{sen} \alpha \\ \operatorname{sen} \alpha & \cos \alpha \end{pmatrix}$$

de uma rotação é ortogonal, como se verifica facilmente. Nosso próximo objetivo é verificar que o conjunto das matrizes ortogonais constitui um grupo com respeito ao produto de matrizes e determinar qual subgrupo deste grupo identifica-se com o grupo G das matrizes de rotações.

Um pouco de notação: a "transposta" A^t de uma matriz $A = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ é a matriz $\begin{pmatrix} p & r \\ q & s \end{pmatrix}$, obtida a partir de A por intercâmbio entre linhas e colunas. Um cálculo direto mostra que a matriz $A = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ é ortogonal se e só se $A^t.A = I$, onde I é a matriz identidade. O fato de que as matrizes ortogonais formam um grupo relativamente ao produto usual de matrizes deriva, então, da seguinte

Proposição - O conjunto das matrizes 2×2 reais A tais que $A^t.A = I$ constitui um grupo relativamente ao produto usual de matrizes.

Demonstração: Se A e B são matrizes 2×2 reais, um cálculo direto mostra que vale a igualdade:

$$(A.B)^t = B^t.A^t.$$

Se, além disso, tem-se $A^t.A = I$ e $B^t.B = I$, então

$$(A.B)^t.(A.B) = (B^t.A^t).(A.B) = B^t.(A^t.A).B$$
$$= B^t.I.B = B^t.B = I.$$

Logo, no conjunto das matrizes em questão, o produto usual é um operação.

É claro que I é o elemento neutro desta operação.

Finalmente, a condição $A^t.A = I$ mostra que A admite A^t como inverso. C.Q.D.

Em seguida, para identificar o grupo das rotações com um subgrupo do grupo das matrizes ortogonais, somos levados a utilizar a noção de determinante de uma matriz. Lembremos que o determinante det(A) de uma matriz 2×2 real A é um número real e que a função det assim obtida satisfaz, entre outras, a propriedade de preservar o produto de matrizes, isto é, det(A.B) = det A . det B.

Chamemos de <u>especial</u> uma matriz A tal que det(A) = 1. Da condição $A^t.A = I$ e do fato que $\det(A^t) = \det(A)$ (leitor: verifique), resulta que para uma matriz ortogonal A tem-se uma e uma só das duas possibilidades: det(A) = 1 ou det(A) = -1.

<u>Proposição</u> - O subconjunto do grupo das matrizes ortogonais A tais que det(A) = 1 constitui um subgrupo. Precisamente, tal subgrupo coincide (isto é, é isomorfo de uma maneira natural) com o grupo das rotações em torno da origem.

<u>Demonstração:</u> Já observamos, anteriormente, que uma matriz de rotação $\begin{pmatrix} \cos\alpha & -\operatorname{sen}\alpha \\ \operatorname{sen}\alpha & \cos\alpha \end{pmatrix}$ é ortogonal. Como as matrizes de rotação e as matrizes ortogonais constituem, respectivamente, grupos re-

lativamente ao produto usual de matrizes, segue-se que o grupo das rotações é isomorfo (pela inclusão natural) a um subgrupo das matrizes ortogonais. Teremos demonstrado tudo se provarmos que uma matriz ortogonal $A = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ é da forma $\begin{pmatrix} \cos \alpha & -\operatorname{sen} \alpha \\ \operatorname{sen} \alpha & \cos \alpha \end{pmatrix}$ se e só se A é especial.

Primeiramente, $\det \begin{pmatrix} \cos \alpha & -\operatorname{sen} \alpha \\ \operatorname{sen} \alpha & \cos \alpha \end{pmatrix} = \cos^2 \alpha + \operatorname{sen}^2 \alpha = 1$, logo uma matriz de rotação é especial. Inversamente, suponhamos que A é especial. Como A é ortogonal, temos $0 \leq p^2 = 1 - q^2 \leq 1$, logo $|p| \leq 1$. Pelo comportamento da função cos, existe $\alpha \in \mathbb{R}$ tal que $p = \cos \alpha$. Da igualdade $q^2 = 1 - p^2$ deduzimos que $q = \pm \operatorname{sen} \alpha$. Usando as demais condições de ortogonalidade: $r^2 + s^2 = 1$ e $pr + qs = 0$, deduzimos que $s = \pm \cos \alpha$ e $r = \pm \operatorname{sen} \alpha$. Finalmente, entrando com a condição de especialidade: $\det A = \det \begin{pmatrix} p & q \\ r & s \end{pmatrix} = ps - rq = 1$, concluímos que $q = -\operatorname{sen} \alpha$, $s = \cos \alpha$, $r = \operatorname{sen} \alpha$. C.Q.D.

O grupo das matrizes ortogonais é chamado o <u>grupo ortogonal</u> (de grau 2); o subgrupo constituído pelas matrizes especiais é dito <u>grupo ortogonal especial</u> (de grau 2). Este último é, como acabamos de ver, exatamente o grupo das rotações em torno da origem (= grupo dos movimentos rígidos do plano que transformam o círculo em si mesmo). Notação: $\mathcal{O}(\mathbb{R}^2)$, $S\mathcal{O}(\mathbb{R}^2)$.

Os grupos acima são, num certo sentido, "contínuos". Em particular, são grupos infinitos. Seus elementos são simetrias do círculo centrado na origem; da mesma forma que a circunferência é o caso limite dos polígonos regulares de n lados, à medida que $n \to +\infty$, também $\mathcal{O}(\mathbb{R}^2)$ e $S\mathcal{O}(\mathbb{R}^2)$ podem ser vistos como "caso limite" dos grupos de simetrias de polígonos regulares de n lados, quando

$n \to \infty$. Precisamente, temos a seguinte

Proposição - Se G é um subgrupo finito do grupo ortogonal $\mathcal{O}(\mathbb{R}^2)$, então ou G é isomorfo ao grupo cíclico C_n, para algum $n \geq 1$, ou G é isomorfo ao grupo das simetrias de um polígono regular de n lados, para algum $n \geq 1$ (N.B.: este último grupo, designado por D_n, é chamado também grupo diédrico de grau n).

Demonstração: Necessitamos do seguinte

Lema - Designemos por $\mathbb{R}/2\pi\mathbb{Z}$ o conjunto quociente de $\mathbb{R}$ pela relação de equivalência $\sim$ definida por: $\alpha \sim \beta$ se e só se $\alpha-\beta = 2\pi k$, algum $k \in \mathbb{Z}$. Seja $\iota: \mathbb{R} \to \mathbb{R}/2\pi\mathbb{Z}$ a aplicação quociente canônica. Então:

(1) $\mathbb{R}/2\pi\mathbb{Z}$ admite uma única estrutura de grupo tal que $\iota: \mathbb{R} \to \mathbb{R}/2\pi\mathbb{Z}$ seja um homomorfismo.

(2) Seja $\varphi: \mathbb{R} \to S\mathcal{O}(\mathbb{R}^2)$ definida conforme a Proposição da pag. 43 A (única) aplicação $\bar{\varphi}: \mathbb{R}/2\pi\mathbb{Z} \to S\mathcal{O}(\mathbb{R}^2)$ tal que $\bar{\varphi}.\iota = \varphi$ é um isomorfismo de grupos, desde que $\mathbb{R}/2\pi\mathbb{Z}$ seja munido da estrutura de grupo da parte (1).

Demonstração (de Lema): (1) Se $\iota: \mathbb{R} \to \mathbb{R}/2\pi\mathbb{Z}$ é um homomorfismo para uma estrutura de grupo em $\mathbb{R}/2\pi\mathbb{Z}$ (com operação que será designada por $\dot{+}$), deve-se ter $\iota(r+r') = \iota(r) \dot{+} \iota(r')$ para todos $r,r' \in \mathbb{R}$. Como todo elemento x de $\mathbb{R}/2\pi\mathbb{Z}$ é da forma $\iota(r)$ para algum $r \in \mathbb{R}$, resulta que a única operação possível em $\mathbb{R}/2\pi\mathbb{Z}$ tal que ι seja um homomorfismo é:

$$x+y = \iota(r) \dot{+} \iota(r') = \iota(r+r').$$

Resta verificar se $\dot{+}$, assim prescrita, é realmente uma operação bem definida, isto é, se não depende da escolha dos reais r,r' tais que $x = \iota(r)$ e $y = \iota(r')$. Para tal, suponhamos que $s,s' \in \mathbb{R}$ também são tais que $x = \iota(s)$, $y = \iota(s')$. Então, pela definição da aplicação quociente ι, tem-se $r-s = 2\pi k$, $r'-s' = 2\pi k'$ para certos $k,k' \in \mathbb{Z}$. Segue-se que $r+s - (r'+s') = 2(k+k')\pi$, logo $\iota(r+s) = \iota(r'+s')$ novamente pela definição de ι. Isto mostra que $\dot{+}$ independe dos representantes escolhidos. As demais verificações de que $\mathbb{R}/2\pi\mathbb{Z}$ é um grupo com a operação $\dot{+}$ são mera rotina. É claro também que $\iota: \mathbb{R} \to \mathbb{R}/2\pi\mathbb{Z}$ vem a ser, automaticamente, um homomorfismo.

(2) Lembremos que existe uma e uma só aplicação $\bar{\varphi}: \mathbb{R}/2\pi\mathbb{Z} \to SO(\mathbb{R}^2)$ tal que $\bar{\varphi} \circ \iota = \varphi$, a saber, $\bar{\varphi}(\iota(r)) = \varphi(r)$ (verifica-se que $\bar{\varphi}$ está bem definida). Ora,

$$\bar{\varphi}(\iota(r) \dot{+} \iota(r')) = \bar{\varphi}(\iota(r+r') = \varphi(r+r') = \varphi(r) + \varphi(r')$$
$$= \bar{\varphi}(\iota(r)) + \bar{\varphi}(\iota(r')).$$

Isto significa que $\bar{\varphi}$ é um homomorfismo. Da condição $\bar{\varphi} \circ \iota = \varphi$ resulta, facilmente, que $\bar{\varphi}$ é sobrejetor. Finalmente, se $\bar{\varphi}(\iota(r)) = 0$ então $\varphi(r) = 0$, logo $r \in 2\pi\mathbb{Z}$ (vide Proposição à pag. 43). Conseqüentemente, $\iota(r)$ é o elemento neutro de $\mathbb{R}/2\pi\mathbb{Z}$, o que mostra a injetividade de $\bar{\varphi}$. Conclusão: $\bar{\varphi}$ é um isomorfismo.

C.Q.D. para o Lema.

Voltemos à demonstração da Proposição. Designemos por $\theta: SO(\mathbb{R}^2) \to \mathbb{R}/2\pi\mathbb{Z}$ o homomorfismo inverso de $\bar{\varphi}$, que existe em virtude de $\bar{\varphi}$ ser um isomorfismo pelo Lema. Consideremos o subgrupo $H = G \cap SO(\mathbb{R}^2)$ de G; os elementos de H são precisamente as rotações que figuram em G.

Se $H = \{I\}$, mas $G \neq \{I\}$, tem-se necessariamente que G é cíclico gerado por uma matriz ortogonal não especial. Com efeito, designemos por reflexão uma matriz ortogonal não especial, isto é, ortogonal com determinante $= -1$. Como $\det(A.B) = \det A \,.\, \det B$, segue-se que o produto de duas reflexões é uma rotação. Ora, suponhamos que existem reflexões $S,T \in G$ tais que $S \neq T$. Neste caso $S.T \in G$ é uma rotação, logo $S.T \in H$. Mas $H = \{I\}$ por hipótese. Logo, $S.T = I$, isto é, $S = T^{-1} = T$ (em virtude de $T^2 = I$)$^{(*)}$; contradição. Logo, G admite uma única reflexão, isto é, G é cíclico de ordem 2.

O caso interessante é quando $H \neq \{I\}$. Neste caso, agimos da seguinte maneira: dada uma rotação $R \in SO(\mathbb{R}^2)$, designamos por $\theta(R)$ o único representante da classe $\theta(R) \in \mathbb{R}/2\pi\mathbb{Z}$ contido no intervalo real $[0,2\pi)$. Seja então $R \in H$ tal que $R \neq I$ e tal que $\theta(R)$ seja menor possível entre as rotações de G.

Nossa intenção é mostrar que H é o grupo cíclico $\langle R \rangle$ gerado por R. Para tal, seja $T \in H$ qualquer. Então, podemos escolher um $m \in \mathbb{N}$ tal que

$$m.\theta(R) \leq \theta(T) < (m+1).\theta(R)$$

(N.B. Para escrever isto usamos a propriedade arquimedeana dos reais e a boa ordenação dos naturais). Em outras palavras, temos:

$$0 \leq \theta(T) - m.\theta(R) < \theta(R).$$

Em particular, $\theta(T) - m.\theta(R) \in [0,2\pi)$. Por outro lado,

---

(*) Por cálculo direto, a matriz de uma reflexão é igual a sua transposta.

$$\iota(\tilde{\theta}(T) - m.\tilde{\theta}(R)) = \iota(\tilde{\theta}(T)) - m.\iota(\tilde{\theta}(R))$$
$$= \theta(T) - m.\theta(R)$$
$$= \theta(T \circ R^{-m}).$$

Mas, $T \circ R^{-m} \in H$ pois $R \in H$ e $T \in H$. Ora, acabamos de ver que $\tilde{\theta}(T \circ R^{-m}) = \tilde{\theta}(T) - m.\tilde{\theta}(R) < \tilde{\theta}(R)$. Necessariamente, em virtude da escolha de R, $T \circ R^{-m} = I$. Isto é, $T = R^m$. Isto mostra que $T \in \langle R \rangle$, logo $H = \langle R \rangle$.

Temos dois casos a considerar:

(i) $H = G$. Neste caso, G é cíclico.

(ii) $H \neq G$. Neste caso, G contém ao menos uma reflexão S. Consideremos os elementos $S, S \cdot R, \ldots, S \cdot R^{n-1} \in G$, onde n é o número de elementos de H. Tais elementos são distintos entre sí. Como S é reflexão e R rotação, cada $S \cdot R^i$ é uma reflexão (usar determinantes!). Assim, G tem pelo menos estas n reflexões. Seja, agora, T uma reflexão qualquer em G. Então $S \circ T$ é uma rotação, isto é, $S \circ T = R^i$, para algum $0 \leq i \leq n-1$. Logo, $T = S \cdot R^i$. Concluímos que $G = \{I, R, \ldots, R^{n-1}, S, S \cdot R, \ldots, S \cdot R^{n-1}\}$. Por outro lado, G é gerado por R e S com as seguintes relações:
$R^n = I$, $S^2 = I$, $(R \cdot S)^2 = I$ (ou $R \cdot S = S \cdot R^{-1}$). Mas esta é precisamente a descrição do grupo das simetrias do polígono regular de n lados, por meio de geradores e relações. C.Q.D.

Exercício: Seja $H \subset G$ o grupo de rotações de G, como acima. Se R é tal que $H = \langle R \rangle$, mostre que $\tilde{\theta}(R) = 2\pi/n$, onde n = número de elementos de H.

Sugestão: mostre que $R^n = I$ e aplique θ a ambos os membros desta igualdade.

2.2. O grupo linear geral.

Os grupos $\mathcal{O}(\mathbb{R}^2)$ e $S\mathcal{O}(\mathbb{R}^2)$ têm em comum a peculiaridade de serem subgrupos de um mesmo grupo de matrizes, a saber, o grupo da matrizes 2×2 $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ tais que $ps - rq \neq 0$.

Definição - O grupo das matrizes $n\times n$ reais A tais que $\det A \neq 0$ é chamado o grupo linear geral (de grau n).

Notação: $GL(\mathbb{R}^n)$ ou $GL(n, \mathbb{R})$.

É preciso verificar que $GL(\mathbb{R}^n)$ é realmente um grupo com respeito, bem entendido, à multiplicação usual de matrizes quadradas. Primeiramente, como o determinante é uma função do conjunto de todas as matrizes $n\times n$ reais em $\mathbb{R}$ que preserva o produto, segue-se facilmente que $GL(\mathbb{R}^n)$ é fechado relativamente ao produto de matrizes. Em seguida, $I = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$ é evidentemente elemento neutro para o produto. Finalmente, se A é tal que $\det A \neq 0$, então a regra de Cramer (para determinar soluções de sistemas de n equações lineares a n incógnitas) mostra que a aplicação linear associada a A admite inversa, logo a matriz A admite inversa A^{-1}.

Definindo a transposta A^t de uma matriz $n\times n$ real A analogamente ao caso em que $n = 2$ (§2.1), obtemos os grupos ortogonal e ortogonal especial (de grau n). Assim:

$$\mathcal{O}(\mathbb{R}^n) = \mathcal{O}(n, \mathbb{R}) = \{A \in GL(\mathbb{R}^n) \mid A^t.A = I\}$$

$$S\mathcal{O}(\mathbb{R}^n) = S\mathcal{O}(n, \mathbb{R}) = \{A \in GL(\mathbb{R}^n) \mid A^t.A = I \text{ e } \det A = 1\}.$$

Outro subgrupo importante do grupo linear geral é o grupo

linear especial:

$$SL(\mathbb{R}^n) \doteq SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) \mid \det A = 1\}.$$

É imediato que $SL(n, \mathbb{R})$ é um subgrupo de $GL(n, \mathbb{R})$. Evidentemente, tem-se $SO(n, \mathbb{R}) = SL(n, \mathbb{R}) \cap O(n, \mathbb{R})$.

Os subgrupos de $GL(n, \mathbb{R})$ são chamados "grupos clássicos". Tais grupos têm sido bastante estudados, tendo inspirado tais estudos uma parte importante da teoria dos grupos: a teoria da representação (linear) de grupos.

Exemplo: Todo grupo finito é isomorfo a um subgrupo de $GL(n, \mathbb{R})$, para algum $n \geq 1$.

Para tal basta provar que, para todo $n \geq 1$, S_n é isomorfo a um subgrupo de $GL(n, \mathbb{R})$; o resto segue-se do teorema de Cayley (§1.4, p.22). Definamos uma aplicação $\varphi: S_n \to GL(n, \mathbb{R})$ da seguinte maneira: dada uma permutação

$$s = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \in S_n \quad ,$$

$\varphi(s)$ é a matriz $n \times n$ tal que, para todo $t = 1, 2, \ldots, n$, a t-ésima linha de $\varphi(s)$ é toda constituída de zeros exceto na i_t-ésima posição, onde aparece 1.

Por exemplo, se $n = 3$ e $s = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$, então

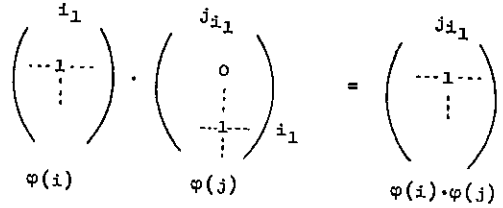
$$\varphi(s) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} .$$

É fácil verificar que $\varphi(s)$ é uma matriz contendo exatamente um elemento $\neq 0$ em cada linha e em cada coluna, e tal elemento é sempre $=1$. Segue-se disso que $\varphi(s)$ é sempre um elemento de $GL(n, \mathbb{R})$ (com determinante $= \pm 1$).

A verificação de que φ é um homomorfismo é um pouco mais delicada. Sejam

$$i = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \quad e \quad j = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$$

duas permutações. Queremos mostrar que $\varphi(i) \circ \varphi(j) = \varphi(i \cdot j)$ e para isto olhemos para uma linha genérica das matrizes em questão. Não se perde em generalidade ao considerar apenas a 1ª linha. Por definição, $\varphi(i)$ contém 1 na i_1-ésima posição (isto é, na i_1-ésima coluna). Seja $(i \cdot j)_1$ a posição onde 1 aparece na 1ª linha da matriz $\varphi(i) \cdot \varphi(j)$. Como é obtido tal elemento? Pela "multiplicação" da 1ª linha da matriz $\varphi(i)$ pela coluna de $\varphi(j)$ tal que admita 1 na i_1-ésima posição (isto é, no encontro com a i_1-ésima linha). Ora, por definição de φ, tal coluna é necessariamente a j_{i_1}-ésima coluna de $\varphi(j)$. Assim, o 1 que figura na 1ª linha da matriz $\varphi(i) \cdot \varphi(j)$ pertence à j_{i_1}-ésima coluna de $\varphi(i) \cdot \varphi(j)$. Por outro lado, por definição de φ, a matriz $\varphi(i \cdot j)$ admite 1 na j_{i_1}-ésima coluna (e 1ª linha) já que mediante a permutação composta $i \cdot j$, 1 é mandado em $j_{i_1} = i(j(1))$. Resulta que a posição de 1 nas 1as linhas das duas matrizes $\varphi(i) \cdot \varphi(j)$ e $\varphi(i \cdot j)$ é a mesma.



Isto mostra (repetindo o argumento para cada linha) que $\varphi(i)\cdot\varphi(j) = \varphi(i\cdot j)$.

Exercício: Seja

$$i = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \in S_n .$$

Então, tem-se, interpretando

$$\begin{pmatrix} 1 \\ \vdots \\ n \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} i_1 \\ \vdots \\ i_n \end{pmatrix}$$

como vetores colunas:

$$\varphi(i) \begin{pmatrix} 1 \\ 2 \\ \vdots \\ n \end{pmatrix} = \begin{pmatrix} i_1 \\ i_2 \\ \vdots \\ i_n \end{pmatrix} .$$

Deduza que φ é injetora e conclua que φ é bijetora sobre o conjunto das matrizes de $GL(\mathbf{R}^n)$ que contém 1 em cada linha e em cada coluna exatamente uma vez e 0 nas demais posições.

Desta maneira, todo grupo finito é, a menos de isomorfismos, um subgrupo de $GL(n, \mathbf{R})$ para algum $n \geq 1$.

Retornemos ao caso $n = 2$. $GL(2, \mathbb{R})$ e alguns de seus subgrupos são de grande importância na teoria das superfícies de Riemann (um capítulo das funções analíticas de variáveis complexas) bem como, mais particularmente, na teoria das chamadas formas modulares.

Consideremos o grupo especial $SL(2, \mathbb{R})$. Lembremos que uma matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{R})$ é tal que $ad - bc = 1$. Interpretadas como aplicações lineares do plano em si mesmo, tais matrizes expressam apenas propriedades "lineares" do plano. Propriedades geométricas mais sutis ficam, assim, escondidas a um observador menos avisado. Vamos verificar que, usando o conceito de isomorfismo de grupos, $SL(2, \mathbb{R})$ pode ser interpretado como um grupo de funções do plano de Argand em si mesmo que preservam, entre outras coisas, a medida de ângulos.

No que se segue, $\mathbb{C}$ é o conjunto dos números complexos com as operações usuais $+$ e $\cdot$; z designará um complexo qualquer e, sempre que for necessário, escreveremos z na forma $x + iy$, com $x, y \in \mathbb{R}$ e $i^2 = -1$. $\mathbb{R}$ será sempre considerado como contido naturalmente em $\mathbb{C}$ e isto significa que tal inclusão é dada pela injeção natural $x \mapsto x + i \cdot 0$, a qual preserva adição e multiplicação.

Proposição - Seja G o conjunto das funções de $\mathbb{C}$ em $\mathbb{C}$ definidas por $z \mapsto \frac{az + b}{cz + d}$, para alguns $a, b, c, d \in \mathbb{R}$ tais que $ad - bc = 1$. Então,

(1) G é um grupo relativamente à composição usual de funções e existe um homomorfismo sobrejetor $\varphi: SL(2, \mathbb{R}) \to G$;

(2) o conjunto das matrizes $A \in SL(2, \mathbb{R})$ tais que $\varphi(A) =$ aplicação identidade de $\mathbb{C}$ em $\mathbb{C}$ é o subgrupo constituído pelos

elementos $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ e $\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$. Tal subgrupo determina uma relação de equivalência $\sim$ em $SL(2,\mathbb{R})$ tal que $SL(2,\mathbb{R})/\sim$ admite uma estrutura natural de grupo isomorfo a G.

Demonstração: (1) Sejam $z \to \frac{az+b}{cz+d}$ e $z \to \frac{a_1z+b_1}{c_1z+d_1}$ duas funções de $\mathbb{C}$ em $\mathbb{C}$ tais que $a,b,c,d,a_1,b_1,c_1,d_1 \in \mathbb{R}$ e $ad-bc = 1$, $a_1d_1 - b_1c_1 = 1$. Por composição, obtemos:

$$z \to \frac{a_1(\frac{az+b}{cz+d}) + b_1}{c_1(\frac{az+b}{cz+d}) + d_1} = \frac{(aa_1+cb_1)z + ba_1 + db_1}{(ac_1+cd_1)z + bc_1 + dd_1},$$

onde $(aa_1+cb_1)(bc_1+dd_1) - (ba_1+db_1)(ac_1+cd_1) =$

$$= ad(a_1d_1-b_1c_1) - bc(a_1d_1-b_1c_1) =$$

$$= (ad-bc)(a_1d_1-b_1c_1) = 1\cdot 1 = 1.$$

Logo, G é fechado relativamente à composição de funções. A aplicação identidade $z \mapsto z$ de $\mathbb{C}$ pertence a G (com $a=d=1$, $b=c=0$), logo é elemento neutro de G. Enfim, a função $z \mapsto \frac{az+b}{cz+d}$ tal que $ad-bc = 1$ admite por inversa a função $z \mapsto \frac{dz-b}{-cz+a}$, o que se verifica por um cálculo direto de composição de funções. A inversa é também um elemento de G já que $da-(-b)(-c) = ad-bc = 1$.

Definimos $\varphi: SL(2,\mathbb{R}) \to G$ da maneira mais óbvia possível:

$$\varphi\begin{pmatrix}a & b\\ c & d\end{pmatrix} = (z \mapsto \frac{az+b}{cz+d}).$$

É evidente que φ é sobrejetora. Além disso, φ é um homomorfismo, o que se vê pelo produto usual de matrizes e o cálculo de composição de funções feito acima.

(2) Suponhamos que $\varphi\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ = aplicação identidade. Então $\frac{az+b}{cz+d} = z$ para todo $z \in \mathbb{C}$, logo obtemos $cz^2 + (d-a)z - b = 0$ para todo $z \in \mathbb{C}$, $z \neq -\frac{d}{c}$. Como a equação escrita tem (no máximo) duas raízes, segue-se necessariamente que $b = c = 0$ e $a = d$. Por outro lado, $ad - bc = 1$ pois $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{R})$. Resulta, enfim, que $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ou $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. É claro que estas duas matrizes constituem um subgrupo de $SL(2, \mathbb{R})$. Tal subgrupo determina a seguinte a relação de equivalência em $SL(2, \mathbb{R})$ (cf. o caso de $\mathbb{R}$ e seu subgrupo $2\pi\mathbb{Z}$):
$A \sim B$ se e só se $B = A \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = A$ ou $B = A \cdot \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -A$. Tal relação é bastante suave, tudo o que faz é identificar (isto é, colocar numa mesma classe) matrizes com suas simétricas aditivas. Se $A \in SL(2, \mathbb{R})$, $\tilde{A}$ designará sua classe de equivalência (constituída somente por A e $-A$).

Definimos um produto em $SL(2, \mathbb{R})/\sim$:

$$\tilde{A}.\tilde{B} = \widetilde{A.B}.$$

Deixamos ao leitor a verificação de que a definição é boa, isto é, independe dos representantes das classes (a verificação é aqui imediata). O elemento neutro de $SL(2, \mathbb{R})/\sim$ é $\tilde{I}$; o inverso de $\tilde{A}$ é $\widetilde{A^{-1}}$.

Exatamente como no caso de $\mathbb{R}/2\pi\mathbb{Z}$ e do grupo das rotações, aqui também o homomorfismo sobrejetor $\varphi: SL(2, \mathbb{R}) \to G$ induz, naturalmente, um homomorfismo sobrejetor $\tilde{\varphi}: SL(2, \mathbb{R})/\sim \to G$.

Para concluir, verifiquemos que $\tilde{\varphi}$ é injetor. Como $\tilde{\varphi}$ é um homomorfismo, basta ver que se $\tilde{\varphi}(\tilde{A})$ = aplicação identidade, en-

tão $\tilde{A} = \tilde{I}$. Ora, por definição, $\tilde{\varphi}(\tilde{A}) = \varphi(A)$. Como vimos acima, $\varphi(A)$ é a aplicação identidade de $\mathbb{C}$ se e só se $A = I$ ou $A = -I$, isto é, se $\tilde{A} = \tilde{I}$. C.Q.D.

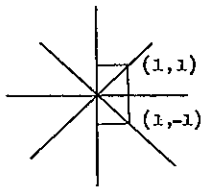
Observações: (1) A técnica acima usada, bem como no caso de $\mathbb{R}$ e $2\pi\mathbb{Z}$, de passar ao conjunto quociente, muní-lo em seguida de uma estrutura (natural) de grupo e, finalmente, obter um certo isomorfismo a partir de um homomorfismo sobrejetor, é bastante geral como veremos no Capítulo 3.

(2) As funções $z \mapsto \frac{az+b}{cz+d}$ são funções de $\mathbb{C}$ em $\mathbb{C}$ no sentido geral que demos no início do curso. Contudo, elas têm por domínio de definição, em geral, $\mathbb{C}$ menos um número complexo. Assim, se $c \neq 0$, a função está definida apenas no complementar $\mathbb{C} \setminus \{-\frac{d}{c}\}$. Por exemplo, a função $z \mapsto -\frac{1}{z}$ não está definida em 0.

O grupo quociente $SL(2, \mathbb{R})/\sim$ é chamado o grupo linear projetivo especial (de grau 2). O grupo das aplicações $z \mapsto \frac{az+b}{cz+d}$, $ad - bc = 1$, é chamado grupo das transformações fracionárias lineares (reais).

Acabamos de mostrar que os grupos acima são isomorfos. O grupo linear projetivo especial é designado comumente por $PSL(2, \mathbb{R})$. As propriedades das transformações fracionárias lineares relativas à estrutura do grupo dessas transformações são válidas em $PSL(2, \mathbb{R})$, pelo isomorfismo obtido. Contudo, o comportamento geométrico de uma transformação fracionária $z \mapsto \frac{az+b}{cz+d}$ é inteiramente diferente do da matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ quando ambas são consideradas como funções do plano $\mathbb{R}^2$ em si mesmo ($\mathbb{C}$ é identificado com $\mathbb{R}^2$ mediante a aplicação natural $x+iy \mapsto (x,y)$).

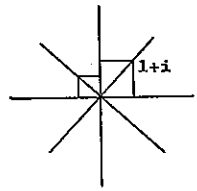
Por exemplo, a matriz $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ aplicada ao vetor coluna $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ dá como resultado o vetor $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$, enquanto que a transformação fracionária $z \to -\frac{1}{z}$ transforma o complexo $1+i$ no complexo $-\frac{1}{2}+\frac{1}{2}i$.



ação de $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

como aplicação linear usual, isto é, rotação de $-\frac{\pi}{2}$ radianos.

Atenção: 0 é o único ponto fixo da aplicação.



ação de $z \to -\frac{1}{z}$

como aplicação do plano em si mesmo. Atenção: i e -i são pontos fixos de $z \mapsto -\frac{1}{z}$.

A seguir, oferecemos sem demonstração alguns fatos importantes sobre transformações fracionárias.

1. Toda transformação fracionária linear $\neq$ identidade tem no máximo dois pontos fixos e pelo menos um ponto fixo. (Isto é imediato por consideração da equação $\frac{az+b}{cz+d} = z$, isto é, da equação $cz^2 + (d-a)z - b = 0$). De acordo com tais pontos fixos, a transformação pode ser:

(E) Elítica, quando admite um par de complexos conjugados z e $\bar{z}$ como pontos fixos, onde $Im(z) > 0$. Este caso tem lugar se e só se $c \neq 0$, $a \neq d$ e $b \neq 0$ ou $c \neq 0$, $a = d$ e $bc < 0$.

Por exemplo, $z \mapsto -\frac{1}{z}$ é elítica.

(H) Hiperbólica, quando admite dois pontos fixos distintos sobre o

eixo real. Este caso tem lugar se e só se $b = 0$, $a \neq d$ e $c \neq 0$ ou $bc > 0$ e $a = d$.

Por exemplo, $z \mapsto \frac{z}{z+1}$. Uma transformação $z \mapsto \frac{az+b}{cz+d}$ com $b \neq 0$, se é hiperbólica, deve satisfazer à condição $|a| > 1$, ou, equivalentemente, à condição $|a+d| > 2$.

(P) <u>Parabólica</u>, quando admite apenas um ponto fixo, necessariamente sobre o eixo real. Tal acontece se e só se $c = 0$ ou $c \neq 0$, $b = 0$ e $a = d$ (equivalentemente, se $c \neq 0$ e $|a+d| = 2$).

Por exemplo, $z \mapsto z+b$ é parabólica.

2. Dada uma transformação $z \mapsto \frac{az+b}{cz+d}$, com $c \neq 0$ ela escreve-se na forma canônica $z \mapsto \frac{a}{c} + \frac{(bc-ad)/c^2}{z+d/c} = \frac{a}{c} - \frac{1}{c^2}\,\frac{1}{z+d/c}$, logo é composta de uma transformação elítica $(z \mapsto -1/(z+d/c))$, de uma homotetia de razão $1/c^2$ (que é uma transformação fracionária linear do tipo que vimos considerando apenas no caso em que $c = 1$ ou $c = -1$) e de uma transformação parabólica $(z \mapsto z + a/c)$.

3. A fim de libertarmo-nos do "inconveniente" de que as transformações fracionárias lineares não estão definidas em todos os pontos de $\mathbb{C}$ e de que, consequentemente, a composição de tais funções exige que excluamos, de cada vez, um número finito de pontos de $\mathbb{C}$, utilizamos o seguinte estratagema: consideramos um novo conjunto, $\bar{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, onde $\{\infty\}$ é um conjunto constituído por um único elemento ∞ (a notação ∞ é sugestiva, mas ∞ não tem significado intrinseco qualquer). Dada uma transformação $T: z \mapsto \frac{az+b}{cz+d}$, com $c \neq 0$, ela está definida para todo $z \in \mathbb{C}$ exceto para $z = -\frac{d}{c}$ (N.B. não há indeterminação possível em virtude da condição $ad-bc \neq 0$). Defi-

nimos: $T(-\frac{d}{c}) = \infty$. Por outro lado, se $T_1(z) = \frac{a\frac{1}{z}+b}{c\frac{1}{z}+d} = \frac{dz+c}{bz+a}$, definimos $T(\infty) = T_1(0)$. Desta maneira, T se estende a uma função $\bar{T}$ de $\bar{\mathbb{C}}$ em $\bar{\mathbb{C}}$ (domínio de definição: todo $\bar{\mathbb{C}}$) e podemos compor as funções $\bar{T}$ à vontade.

Podemos identificar $\bar{\mathbb{C}}$ com a esfera $x_1^2 + x_2^2 + x_3^2 = 1$ (em $\mathbb{R}^3$) pela projeção estereográfica, isto é, pelo processo de confecção de mapas. Assim, as transformações fracionárias são funções genuínas da esfera em si mesmo.

Tal procedimento está ligado à teoria das superfícies de Riemann mencionada mais acima.

3. Grupos Quocientes. Teoremas de isomorfismos

Uma questão que se põe naturalmente é a de formar novos grupos a partir de um grupo dado G. Em seções anteriores consideramos a noção de subgrupo gerado por um subconjunto $S \subset G$; esta é uma maneira importante de formar grupos a partir de G pois dá uma ideia da estrutura interna de G. Mas, caminhemos um pouco mais.

Seja H um subgrupo de G. Como podemos formar novos grupos a partir de G e H de maneira a contribuir para nosso conhecimento da estrutura de G ?

A resposta a esta pergunta é um capítulo longo e sofisticado da teoria dos grupos, envolvendo aspectos delicados das "extensões de grupos" e "cohomologia de grupos".

Aqui, seremos um pouco menos ambiciosos. Nossa intenção é tratar o caso em que o subgrupo H tem propriedade de invariância especiais; estas propriedades serão automaticamente satisfeitas se G for abeliano.

A fim de fundamentar o procedimento geral, passemos em revista alguns exemplos:

(1) Seja $G = \mathbb{R}$, com a adição usual. Seja $H = 2\pi\mathbb{Z} = \{2\pi k \mid k \in \mathbb{Z}\}$.

Conforme vimos no §2.1, $2\pi\mathbb{Z}$ determina uma relação de equivalência $\sim$ em $\mathbb{R}$ tal que $a \sim b$ se e só se $b = a + 2\pi k$, para algum $k \in \mathbb{Z}$. Ainda vimos lá que o conjunto quociente $\mathbb{R}/\sim$ pode ser munido de uma estrutura de grupo, pondo $\tilde{a} + \tilde{b} = \widetilde{a+b}$. Isto define realmente

uma operação em $\mathbf{R}/\sim$ já que, se $a_1 = a + 2\pi k$ e $b_1 = b + 2\pi t$, então $a_1+b_1 = (a + 2\pi k) + (b + 2\pi t) = (a+b) + (2\pi k + 2\pi t)$. A questão reduziu-se a poder comutar os elementos $2\pi k$ e b, tudo mais corre suavemente.

(2) $G = SL(2, \mathbf{R})$, $H = \{I,-I\}$. A relação de equivalência determinada por H é completamente análoga ao caso anterior. Com efeito, dissemos no §2.2 que $A \sim B$ se $B = A.I = A$ ou $B = A.(-I) = -A$. Definimos $\tilde{A}.\tilde{B} = \widetilde{A.B}$, o que é permissível pois se $\tilde{A}_1 = \tilde{A}$ e $\tilde{B}_1 = \tilde{B}$, então $A_1 = A.I$ ou $A_1 = A.(-I)$ e $B_1 = B.I$ ou $B_1 = B.(-I)$; logo, $A_1B_1 = A.I.B.I = AB.I$ ou $A_1B_1 = A.(-I).B.I = A.B.(-I)I$ ou, etc.

Em qualquer caso, foi usado o fato de que B comuta com os elementos de H.

(3) $G = S_3$, $H = \{(1), (123), (132)\}$. Como nos casos anteriores, H determina a relação de equivalência seguinte:

$i,j \in S_3$, $i \sim h$ se $j = i.h$, para algum $h \in H$.

Vejamos se $\tilde{i}.\tilde{j} = \widetilde{i.j}$ define uma operação no quociente $S_3/\sim$. Verificaremos apenas um caso, deixando os restantes ao leitor. Por exemplo, $i = (12)$ e $j = (13)$. Os elementos equivalentes a (12) são:

$$(12) = (12)(1) \quad , \quad (13) = (12)(123) \quad e \quad (23) = (12)(132),$$

enquanto que aqueles equivalentes a (13) são:

$$(13) = (13)(1) \quad , \quad (23) = (13)(123) \quad e \quad (12) = (13)(132).$$

Assim, para verificar se $\widetilde{(12)}.\widetilde{(13)}$ está bem definido precisamos verificar ao todo 9 produtos (na verdade, só 6 tais produtos requerem cuidado). Verificaremos um caso típico, deixando os demais como exercício para o leitor. Sejam,então, $i_1 = (13)$ e $j_1 = (12)$. Tem-se:

$$i_1.j_1 = (13).(12) = (12)(123).(13)(132)$$
$$= (12).(123)(13).(132) = (12).(13)(132).(132)$$
$$= (12)(13).(132)^2 = i.j.(123).$$

Logo $\widetilde{i_1.j_1} = \widetilde{i.j}$, como queríamos verificar. Observemos que, desta feita, G não é abeliano e tampouco (123) comuta com (13). O que valeu é que dados $h \in H$ e $i \in G$, existe $h_1 \in H$ tal que $h.i = i.h_1$.

Com olhos voltados para os exemplos acima, consideremos agora o caso geral. Seja, assim G um grupo e H, um subgrupo de G. Tem-se:

Proposição - Seja $\sim$ a relação de equivalência em G determinada por H, isto é: $x \sim y$ se e só se $y = xh$ para algum $h \in H$. A classe de um elemento $x \in G$ é designada por $\tilde{x}$. A expressão $\tilde{x}.\tilde{y} = \widetilde{xy}$ define uma operação no conjunto quociente $G/\sim$ se e somente se a condição seguinte tiver lugar.

(*) Para todo $y \in G$ e para todo $h \in H$, tem-se $y^{-1}hy \in H$.

Demonstração: Suponhamos (*) válida; quer-se mostrar que se $\tilde{x}_1 = \tilde{x}$ e $\tilde{y}_1 = \tilde{y}$, então $\widetilde{x_1y_1} = \widetilde{xy}$. Por definição, existem $h,h' \in H$ tais que $x_1 = xh$ e $y_1 = yh'$. Logo, $x_1y_1 = xh.yh'$. A condição (*) diz-nos que existe $h_1 \in H$ tal que $hy = yh_1$. Substituindo, vem:

$$x_1y_1 = x.yh_1.h' = xy.h_1h' \quad , \quad \text{onde } h_1h' \in H;$$

quer dizer, x_1y_1 e xy pertencem à mesma classe de $\sim$.

Reciprocamente, suponhamos que a operação é bem definida e sejam $y \in G$, $h \in H$. Então, $\widetilde{h.y} = \tilde{h}.\tilde{y}$. Mas $\tilde{h} = \tilde{e}$ de vez que

$h = e.h$. Logo $\tilde{h}.\tilde{y} = \tilde{y}$, resultando $\widetilde{hy} = \tilde{y}$. Por definição, tem-se então que $hy = yh_1$ para algum $h_1 \in H$, do que advém, finalmente, $y^{-1}hy = h_1 \in H$. C.Q.D.

A condição (*) é por demais importante para que passe desapercebida. Marquemos sua presença com a seguinte

Definição - Seja G um grupo. Um subgrupo H de G é chamado normal (em G) se e só se satisfaz a condição (*).

Exemplos: (1) Se G é abeliano, todo subgrupo de G é automaticamente normal. Assim, $2\pi\mathbb{Z}$ é um subgrupo normal em $\mathbf{R}$. Também $m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}$ é normal em $\mathbb{Z}$, qualquer que seja $m \in \mathbb{Z}$.

(2) Seja G um grupo qualquer. O subconjunto $C(G) = \{a \in G \mid ag = ga$ para todo $g \in G\}$ é um subgrupo de G (isto se verifica facilmente), chamado o centro de G. Se H é um subgrupo de G contido em $C(G)$, é fácil ver que H é normal em G.

Foi esta a situação do exemplo (2) revisto mais acima.

(3) Seja G um grupo qualquer e H um subgrupo tal que $G/\sim$ tem apenas 2 elementos, onde $\sim$ é a relação de equivalência determinada por H (como na Proposição anterior (p.65)). Neste caso, H é normal em G.

Adiante veremos a demonstração deste fato. (vide p. 71)

O exemplo (3) mais acima é uma situação deste tipo. Mais geralmente, o grupo alternado A_n é normal em S_n, para todo n. O subgrupo das rotações planas é normal no grupo diédrico D_n, para todo n.

Um modo alternativo de introduzir a noção de subgrupo normal é através da idéia de automorfismo interno de um grupo.

Assim, dado um grupo G e um elemento $y \in G$, podemos considerar a aplicação $\varphi_y : G \to G$ definida da seguinte maneira:

$$\varphi_y(x) = y^{-1}xy \quad , \quad \text{para todo } x \in G.$$

Como $y^{-1}xy.y^{-1}x'y = y^{-1}xx'y$ para todos $x,x' \in G$, φ_y é um homomorfismo. Por outro lado, a equação $y^{-1}xy = z$ (dado $z \in G$) admite uma única solução $x = yzy^{-1}$. Isto mostra que φ_y é sobrejetor. Logo, φ_y é um isomorfismo de G sobre si mesmo e é chamado <u>automorfismo interno</u> de G (relativamente a y).

Mediante esta noção, vemos que um subgrupo H de G é normal se e só se, para todo automorfismo interno φ_y de G, a imagem $\varphi_y(H)$ de H está contida no próprio H.

A notação $\varphi_y(H) = y^{-1}Hy$ é usual (e conveniente).

<u>Exercício</u>: Se H é normal em G, tem-se na verdade que $y^{-1}Hy = H$ para todo $y \in G$.

Em outras palavras, um subgrupo H de um grupo G é normal se e só se permanece invariante (globalmente como conjunto, não elemento a elemento) sob a ação de todos os automorfismos internos de G.

Ainda outra maneira de introduzir a noção de subgrupo normal é mediante as relações de equivalência determinadas pelo subgrupo. Com efeito, um subgrupo H de um grupo G determina pelo menos duas relações de equivalência em G:

$x \sim_H y$ se e só se $y = xh$, algum $h \in H$

e

$x \,{}_H\!\sim y$ se e só se $y = h_1 x$, algum $h_1 \in H$.

A primeira delas foi considerada na proposição à pag. 65 e nos exemplos que precedem tal proposição. Se designarmos por xH e por Hx, respectivamente, os subconjuntos $\{xh \mid h \in H\}$ e $\{hx \mid h \in H\}$ de G, teremos que a classe de um elemento $x \in G$ nas equivalências $\sim_H$ e ${}_H\!\sim$ é, respectivamente, xH e Hx.

Proposição - H é subgrupo normal em G se e só se as relações $\sim_H$ e ${}_H\!\sim$ coincidem, isto é, se toda classe Hx é uma classe yH.

Demonstração: Se H é normal e $x \in G$, tem-se $x^{-1}Hx = H$. Multiplicando à esquerda por x, vem $Hx = xH$ (calcular com as classes xH e Hy, tal como fazemos com elementos de G, é lícito. Com efeito, dado $hx \in Hx$, tem-se $x^{-1}hx = h_1 \in H$, logo $hx = xh_1 \in xH$, isto é, $Hx \subset xH$. A inclusão recíproca é inteiramente análoga).

Reciprocamente, seja $x \in G$ qualquer Por hipótese, existe $y \in G$ tal que $Hx = yH$. Mostremos que yH é, neste caso, necessariamente, igual a xH. Com efeito, de $Hx = yH$ concluímos que $x = yh$, para algum $h \in H$. Ora, $x = xe \in xH$, logo $yh \in xH \cap yH$. Como xH e yH são classes de uma mesma equivalência, deve-se ter $xH = yH$.

Em resumo, $Hx = xH$, logo $x^{-1}Hx = H$. C.Q.D.

Resumindo, demonstramos que as condições seguintes são equivalentes para um subgrupo H de um grupo G:

(i) H é normal em G

(ii) As relações de equivalência $\sim_H$ e $_H\sim$ determinadas por H coincidem (isto é, determinam a mesma partição de G)

(iii) A expressão $\tilde{x}.\tilde{y} = \widetilde{x.y}$ define uma operação no conjunto quociente $G/\sim$, onde $\sim = \sim_H$.

Suponhamos, então, que H é um subgrupo normal de um grupo G. Neste caso, o conjunto quociente $G/\sim_H = G/_H\sim$ é designado simplesmente por G/H. A operação definida em G/H equipa-o, automaticamente, com uma estrutura de grupo. Com efeito, é imediato verificar que a classe do elemento neutro de G é o elemento neutro para a operação considerada e que uma classe xH admite $x^{-1}H$ por inverso. Finalmente, a aplicação $G \to G/H$ definida por $x \mapsto xH$ é, automaticamente, um homomorfismo (sobrejetor); tal homomorfismo é dito <u>homomorfismo quociente</u> (ou <u>residual</u>). O grupo G/H é dito <u>grupo quociente</u> de G por H. A classe de um elemento $x \in G$ é designada, por vezes, como <u>classe de</u> x <u>módulo</u> H ou <u>resíduo de</u> x <u>módulo</u> H.

É pura rotina verificar que se G é abeliano (resp. finito, cíclico, gerado por um conjunto finito de elementos), então o grupo quociente G/H também o é.

<u>Exemplo</u>: Seja $G = \mathbb{Z}$, $H = m\mathbb{Z}$, onde $m \in \mathbb{Z}$. Neste caso, $G/H = \mathbb{Z}/m\mathbb{Z}$ é isomorfo ao grupo cíclico C_m de ordem $|m|$ através do isomorfismo

$$(\text{classe de } 1 \text{ módulo } m\mathbb{Z}) \mapsto a,$$

onde $a \in C_m$ é um gerador de C_m (N.B. tal isomorfismo não é canonicamente determinado por $\mathbb{Z}/m\mathbb{Z}$ e C_m pois envolve a escolha de um

gerador de C_m ; no total, existem $\varphi(m)$ tais isomorfismos, onde φ é a função aritmética de Euler).

O grupo $\mathbb{Z}/m\mathbb{Z}$ é chamado o grupo dos inteiros módulo m. A "prova dos nove" escolar é calcada no grupo $\mathbb{Z}/9\mathbb{Z}$. A teoria das congruências

$$a \equiv b \pmod{m}$$

transfere-se para um problema de grupos. Teoremas clássicos de congruências em aritméticas, tais como o pequeno teorema de Fermat e o teorema de Wilson, são resultados simples da teoria dos grupos finitos (vide os exercícios propostos ao final do livro).

Retornemos ao caso em que H é apenas um subgrupo (não necessariamente normal) de um grupo G. Dado $x \in G$ qualquer, é imediato que os conjuntos H e xH estão em bijeção. A saber, a aplicação $H \to xH$, definida por $y \mapsto x.y$, é claramente bijetora. Em particular, se H é finito, H e xH têm o mesmo número de elementos para todo $x \in G$. É este, essencialmente, o conteúdo do renomado

Teorema (Lagrange) - Se G é um grupo finito e H, um subgrupo de G, o número de elementos de H é um divisor do número de elementos de G.

Demonstração: Como $\sim_H$ é uma relação de equivalência em G, temos $G = x_1H \cup x_2H \cup \ldots \cup x_kH$, para alguns $x_1, \ldots, x_k \in G$. Digamos, $x_1H = H$ (podemos tomar $x_1 = e$). Se tal é a partição de G determinada por $\sim_H$, então $x_iH \cap x_jH = \emptyset$ se $i \neq j$. Pela observação anterior ao teorema, x_iH e x_jH têm o mesmo número de elementos. Logo, G tem km elementos, onde m é o número de elementos de H.

C.Q.D.

. Definição - O número de elementos de um grupo finito G é chamado a ordem de G. Notação: $|G|$. Se G é infinito, dizemos, por extensão, que G tem ordem infinita. Se $a \in G$, a ordem de a é a ordem do subgrupo cíclico $\langle a \rangle$ gerado por a. Se H é um subgrupo de G, o número de elementos de $G/\sim_H$ é o índice de H em G (N.B. É fácil ver que $G/\sim_H$ e $G/_H\sim$ estão em bijeção mesmo que H não seja normal em G. O caso em que G é finito deixa isto por demais claro).

Uma boa parte dos livros sobre grupos usa as seguintes notações:

$H < G$	H é subgrupo de G
$H \lhd G$	H é subgrupo normal de G
$(G:H)$	índice de H em G.

Observemos que se H é normal em G, tem-se $(G:H) = |G/H|$.

Um critério interessante para decidir se um subgrupo é normal é dado pela

Proposição - Seja G um grupo e seja $H < G$. Se $(G:H) = 2$, H é normal em G.

Demonstração: Já sabemos que $G/\sim_H$ e $G/_H\sim$ estão em bijeção canônica, qualquer que seja o subgrupo H (normal ou não). Com efeito, a aplicação dada por

$$xH \mapsto Hx^{-1}$$

fornece a tal bijeção. Em outras palavras, se o número de classes "à direita" é finito, o número de classes "à esquerda" também é e tais

números coincidem. Sejam, então, $G = H \cup xH$ e $G = H \cup Hy$ as partições de G em classes direitas e esquerdas, respectivamente. Necessariamente, tem-se $x \notin H$ e $y \notin H$. Para mostrar que H é normal em G é suficiente, pela Proposição da pág. 68 , provar que $xH = Hy$. Ora, dado $xh \in xH$, não pode ter-se $xh \in H$ - caso contrário, $x \in H$. Deve ter-se, então, $xh \in Hy$. Analogamente, $Hy \subset xH$. Logo, $xH = Hy$.

C.Q.D.

Corolário - Para todo $n \geq 1$, o grupo alternado A_n é normal em S_n.

Exercício: Exemplo mostrando que $(G:H) = 3$ não implica em que H seja normal em G.

Exercício: Se H,K são subgrupos de G e se H (ou K) é normal em G, então o conjunto $HK = \{hk \mid h \in H, k \in K\}$ é um subgrupo de G. Além disso, neste caso, $HK = \langle H \cup K \rangle$ (= subgrupo gerado pela reunião dos conjuntos H e K).

A principal característica dos grupos quocientes, que ora queremos por em relevo, é a de produzir, da maneira mais econômica possível, um isomorfismo a partir de um homomorfismo dado. Nos exemplos tratados neste curso, foi esta a razão de munir o conjunto quociente $G/\sim$ com estrutura de grupo.

Primeiramente, idéias de ordem geral.

Seja $\varphi: G \to G'$ um homomorfismo. Vimos, anteriormente, que, dado um subgrupo $H < G$, a imagem $\varphi(H) = \{\varphi(h) \mid h \in H\}$ de H é um subgrupo de G'. Por outro lado, seja $H' < G'$. Então o subconjunto $\varphi^{-1}(H') = \{g \in G \mid \varphi(g) \in H'\}$ é um subgrupo de G, o que se verifica igualmente sem dificuldade $(\varphi^{-1}(H')$ é chamado a imagem inver-

sa completa de H').

Em particular, se $H' = \{e'\}$, o subgrupo $\varphi^{-1}(H')$ é chamado o núcleo do homomorfismo φ. Notação: $N(\varphi)$. Este novo personagem já apareceu, essencialmente, no ato anterior:

Proposição - Seja G um grupo, $H < G$. Então H é normal se e só se $H = N(\varphi)$ para algum homomorfismo $\varphi: G \to G'$ (G' depende de H).

Demonstração: Se H é normal, temos o homomorfismo quociente canônico $\varphi: G \to G/H$. Ora, um elemento $g \in G$ é tal que $\varphi(g) = eH = H$ se e somente se $g \in H$. Logo, $H = N(\varphi)$, com $G' = G/H$. Reciprocamente, seja $H = N(\varphi)$ para um dado $\varphi: G \to G'$. Dados $h \in H$ e $x \in G$, tem-se

$$\varphi(x^{-1}hx) = \varphi(x^{-1})\varphi(h)\varphi(x) = \varphi(x^{-1})\cdot e'\cdot\varphi(x) = \varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) =$$

$$= \varphi(e) = e'.$$

Logo, $x^{-1}hx \in N(\varphi) = H$. Consequentemente, H é normal. C.Q.D.

Exemplo: Consideremos o produto usual de números inteiros: por definição, se $m,n \in \mathbb{Z}$, tem-se

$$m\cdot n = \begin{cases} 0, & \text{se } m = 0 \\ n + \ldots + n \quad (m \text{ vezes}), & \text{se } m > 0 \\ n - \ldots - n \quad (-m \text{ vezes}), & \text{se } m < 0. \end{cases}$$

Podemos, às custas de tal produto, definir uma operação adicional em $\mathbb{Z}/m\mathbb{Z}$, qualquer que seja m. Como no caso da adição de inteiros módulo m, definimos produto de inteiros módulo m: $\tilde{r}\cdot\tilde{s} = \widetilde{r\cdot s}$. Atenção, contudo! $\mathbb{Z}$ não é grupo relativamente ao produto: tampouco $\mathbb{Z}/m\mathbb{Z}$ é

grupo relativamente ao produto acima (N.B. se m é um número primo, $(\mathbb{Z}/m\mathbb{Z}) - \{\bar{0}\}$ tem uma estrutura de grupo relativamente ao produto, o que se vê, por exemplo, usando o pequeno teorema de Fermat).

É fácil verificar que o homomorfismo quociente canônico $\varphi: \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ preserva o produto, isto é, $\varphi(nn') = \varphi(n)\cdot\varphi(n')$.

Consideremos o subconjunto $SL(2,\mathbb{Z}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{R}) \mid a,b,c,d \in \mathbb{Z}\}$. É fácil verificar que $SL(2,\mathbb{Z})$ é um subgrupo de $SL(2,\mathbb{R})$, chamado o <u>grupo modular</u> (homogêneo).

Analogamente, podemos considerar matrizes a coeficientes em $\mathbb{Z}/m\mathbb{Z}$ e somar e multiplicar tais matrizes usando a operação de soma e produto de $\mathbb{Z}/m\mathbb{Z}$, na maneira usual como é feita para matrizes reais.

Deixamos ao leitor o cuidado de verificar que o conjunto

$$SL(2, \mathbb{Z}/m\mathbb{Z}) = \{\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mid \alpha,\beta,\gamma,\delta \in \mathbb{Z}/m\mathbb{Z} \ , \ \alpha\delta - \beta\gamma = \bar{1}\}$$

($\bar{1}$ designa a classe do inteiro 1 módulo m) é um grupo relativamente ao produto de matrizes acima citado.

Finalmente, $\varphi: \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ induz naturalmente um homomorfismo (também designado por φ, sem confusão possível):

$$\varphi: SL(2, \mathbb{Z}) \to SL(2, \mathbb{Z}/m\mathbb{Z})$$

$$\varphi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}, \text{ onde } \bar{a} = \varphi(a) \text{ , etc.}$$

O núcleo $N(\varphi)$ deste homomorfismo é designado por <u>subgrupo (principal) de congruência de nível</u> m. Tal grupo aparece frequentemente na

teoria das funções automórficas e das superfícies de Riemann. Notação: Γ'_m.

O primeiro resultado sobre tal grupo é:

Proposição - $SL(2, \mathbb{Z})/\Gamma'_m$ é isomorfo a $SL(2, \mathbb{Z}/m\mathbb{Z})$.

Demonstração: Como Γ'_m é o núcleo de φ, Γ'_m é normal pela proposição anterior (pág. 73). Logo, existe o grupo quociente $SL(2, \mathbb{Z})/\Gamma'_m$. Evidentemente, φ induz um homomorfismo injetor ρ': $SL(2, \mathbb{Z})/\Gamma'_m \to SL(2, \mathbb{Z}/m\mathbb{Z})$ tal que φ' (classe de $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$) = $= \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$. Basta, então ver que φ' é sobrejetor ou, que φ é sobrejetor. Assim, seja $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL(2, \mathbb{Z}/m\mathbb{Z})$. Ora, $\alpha\delta - \beta\gamma = \bar{1}$ significa que $ad - bc - km = 1$, para algum $k \in \mathbb{Z}$, onde $\alpha = \bar{a}$, $\beta = \bar{b}$, $\gamma = \bar{c}$, $\delta = \bar{d}$ $(a,b,c,d \in \mathbb{Z})$. Segue-se que m.d.c. $(c,d,m) = 1$, logo existe $n \in \mathbb{Z}$ tal que m.d.c. $(c,d+nm) = 1$. Logo, podemos supor que m.d.c. $(c,d) = 1$. Neste caso, existem $e', f' \in \mathbb{Z}$ tais que $1 = f'c - e'd$. Ponhamos $f = kf'$, $e = ke'$, de modo que $k = fc - ed$. Consideremos a matriz

$$A = \begin{pmatrix} a+em & b+fm \\ c & d \end{pmatrix}$$

Temos $\det A = ad-bc + m(ed-fc) = ad-bc-mk = 1$, logo $A \in SL(2,\mathbb{Z})$. Por outro lado, $\varphi(A) = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. C.Q.D.

Calcular o índice do grupo de congruência de nível m no grupo modular, isto é, a ordem do grupo $SL(2,\mathbb{Z}/m\mathbb{Z})$, é um problema de aritmética que pode ser resolvido ao longo das seguintes etapas:

1. Um par $c,d \in \mathbb{Z}$ é chamado primitivo mod m se m.d.c.$(c,d,m) = 1$.

O número de pares primitivos mod m, que são incongruentes mod m, será designado por $\lambda(m)$. A função λ é multiplicativa, isto é, se m.d.c. $(m_1,m_2) = 1$ então $\lambda(m_1m_2) = \lambda(m_1)\lambda(m_2)$.

2. Para um par primitivo mod m, c,d, existem m pares $a,b \in \mathbb{Z}$, incongruentes mod m, tais que $ad-bc-1 \in m\mathbb{Z}$. Em outras palavras, dado um par primitivo c,d, existem m elementos distintos da forma $\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$ em $SL(2,\mathbb{Z}/m\mathbb{Z})$.

3. Se p é primo, tem-se $\lambda(p^k) = p^{2k}(1 - \frac{1}{p^2})$, $k \geq 0$.

4. Conclusão: o índice de Γ'_m em $SL(2,\mathbb{Z})$ é

$$m^3 \cdot \prod_{\substack{p \mid m \\ p \text{ primo}}} (1 - \frac{1}{p^2}).$$

Em particular, se $m = p$ é primo, o índice é p^3-p.

Voltando às generalidades, concluiremos esta primeira parte do curso com os chamados "teoremas de isomorfismo".

1º Teorema d Isomorfismo. Seja $\varphi: G \to G'$ um homomorfismo sobrejetor. Então φ induz um isomorfismo $\bar{\varphi}: G/N(\varphi) \xrightarrow{\sim} G'$.

Demonstração: Já vimos este fato em várias situações particulares, inclusive no último exemplo acima. Em geral, definimos $\bar{\varphi}$ tal que $\bar{\varphi}(\bar{g}) = \varphi(g)$, onde $\bar{g} = g\,N(\varphi)$. Se $\bar{g} = \bar{h}$, então $h = gn$, com $n \in N(\varphi)$, logo $\varphi(h) = \varphi(g)\varphi(n) = \varphi(g)e' = \varphi(g)$. Consequentemente, $\bar{\varphi}(\bar{g}) = \bar{\varphi}(\bar{h})$, isto é, $\bar{\varphi}$ está bem definida. Como $\bar{\varphi}(\bar{g}\cdot\bar{g}') = \varphi(g\cdot g') = \varphi(g)\varphi(g') = \bar{\varphi}(\bar{g})\bar{\varphi}(\bar{g}')$, $\bar{\varphi}$ é um homomorfismo. Evidentemen

te, $\bar{\varphi}$ é também sobrejetor.

Finalmente, $\bar{\varphi}(\bar{g}) = e'$ se e só se $\varphi(g) = e'$ se e só se $g \in N(\varphi)$ se e só se $\bar{g}$ = elemento neutro de $G/N(\varphi)$. Logo, $\bar{\varphi}$ é injetor. C.Q.D.

2º Teorema do Isomorfismo. Seja $\varphi: G \to G'$ um homomorfismo sobrejetor. Dado um subgrupo $H' \subset G'$, $\varphi^{-1}(H') \subset G$ designará sua imagem inversa completa (vide pág. 72). Então:

(i) A aplicação $H' \mapsto \varphi^{-1}(H')$ é uma bijeção do conjunto dos subgrupos de G' sobre o conjunto dos subgrupos de G que contém o núcleo $N(\varphi)$ de φ.

(ii) Se H' é normal em G' então $\varphi^{-1}(H')$ é normal em G (e reciprocamente) e tem-se $G/\varphi^{-1}(H') \cong G'/H'$.

Demonstração: (i) Primeiramente, tem-se $\{e'\} \subset H'$ sempre. Logo, $N(\varphi) = \varphi^{-1}(\{e'\}) \subset \varphi^{-1}(H')$. Reciprocamente, dado $H < G$ tal que $N(\varphi) \subset H$, tem-se que $H = \varphi^{-1}(\varphi(H))$. Com efeito, a inclusão $H \subset \varphi^{-1}(\varphi(H))$ é sempre válida. Por outro lado, seja $g \in \varphi^{-1}(\varphi(H))$. Então $\varphi(g) = \varphi(h) \in \varphi(H)$, com $h \in H$, donde $\varphi(gh^{-1}) = e'$, isto é, $gh^{-1} \in N(\varphi)$. Mas $N(\varphi) \subset H$, logo $gh^{-1} \in H$, isto é, $g \in H$. Assim, a aplicação $H \mapsto \varphi(H)$ do conjunto dos subgrupos de G contendo $N(\varphi)$ no conjunto dos subgrupos de G' é injetora (vide Apêndice, Exercício à pág. 114). Analogamente, dado $H' < G'$ tem-se sempre $\varphi(\varphi^{-1}(H')) \subset H'$. Por outro lado, se $h' \in H'$, existe $g \in G$ tal que $\varphi(g) = h'$ (porque φ é sobrejetor). Por definição, $g \in \varphi^{-1}(H')$, logo, $h' = \varphi(g) \in \varphi(\varphi^{-1}(H'))$. Assim $\varphi(\varphi^{-1}(H')) = H'$, mostrando que a aplicação $H \mapsto \varphi(H)$ é sobrejetora, logo é uma bije-

ção. A aplicação inversa é precisamente $H' \mapsto \varphi^{-1}(H')$.

(ii) Suponhamos $H' \lhd G'$. Seja $h \in \varphi^{-1}(H')$ e $g \in G$. Então, $\varphi(g^{-1}hg) = \varphi(g)^{-1}\varphi(h)\varphi(g) \in H'$ já que $\varphi(h) \in H'$. Segue-se que $g^{-1}hg \in \varphi^{-1}(H')$, isto é, $\varphi^{-1}(H') \lhd G$. Reciprocamente, suponhamos que $\varphi^{-1}(H') \lhd G$. Seja $h' \in H'$ e $g' \in G'$. Como φ é sobrejetor, existem $g,h \in G$ tais que $\varphi(g) = g'$ e $\varphi(h) = h'$. Notemos que $h \in \varphi^{-1}(H')$. Por hipótese, $g^{-1}hg \in \varphi^{-1}(H')$. Logo, $g'^{-1}h'g' = \varphi(g)^{-1}\varphi(h)\varphi(g) = \varphi(g^{-1}hg) \in \varphi(\varphi^{-1}(H')) = H'$, isto é, $H' \lhd G'$.

Suponhamos, novamente, que $H' \lhd G'$ e consideremos a aplicação composta $G \to G' \to G'/H'$; trata-se, evidentemente, de um homomorfismo sobrejetor, cujo núcleo é $\varphi^{-1}(H')$. Pelo 1º Teorema, segue-se que $G/\varphi^{-1}(H') \cong G'/H'$.

Observação: Dado $H \lhd G$ tal que $N(\varphi) \subset H$ tem-se ainda que $H/N(\varphi) \cong \varphi(H)$ (1º Teorema). Logo, o isomorfismo do ítem (ii) também lê-se $G/H \cong (G/N(\varphi))/(H/N(\varphi))$, onde $H = \varphi^{-1}(H')$. Tudo funciona como no processo de simplificação de frações, justificando a notação G/H !!! C.Q.D.

Teorema "Diamante" de Noether. Seja G um grupo, H e K subgrupos de G, sendo que K é normal em G.

Então:

(i) HK é um subgrupo de G, onde $HK = \{h \cdot k \mid h \in H, k \in K\}$.

(ii) $H \cap K$ é normal em H.

(iii) $HK/K \cong H/H \cap K$, induzido pela inclusão $H \subset HK$.

Demonstração: (i) (vide Exercício à pág. 72). O principal ponto é mos

trar que HK é subconjunto estável. Sejam $hk, h'k' \in HK$. Como K é normal em G. $h'^{-1}kh' = k'' \in K$. Resulta que $kh' = h'k''$, logo $hk \cdot h'k' = h \cdot kh' \cdot k' = h \cdot h'k'' \cdot k' = hh' \cdot k''k' \in HK$.

(ii) Sejam $k \in H \cap K$ e $h \in H$. Em particular, $k \in K$ e como $K \lhd G$, tem-se $h^{-1}kh \in K$. Mas, também $k \in H$, logo $h^{-1}kh \in H$, portanto $h^{-1}kh \in K \cap H$, mostrando que $H \cap K \lhd H$.

(iii) É claro que $K \lhd G$ implica $K \lhd K'$ para todo $K' < G$ tal que $K \subset K'$. Em particular, $K \lhd HK$, logo HK/K existe. Seja $\varphi: H \to HK/K$ o homomorfismo composto da inclusão $H \subset HK$ e do homomorfismo quociente $HK \to HK/K$. Explicitamente, $\varphi(h) = hK$. Operando com classes, vemos que $hK = h(kK)$ para todos $h \in H$, $k \in K$. Logo, φ é sobrejetor. Finalmente, $N(\varphi) = H \cap K$, o que se vê imediatamente (de passagem, isto prova (ii) novamente). Pelo 1º Teorema, $H/H \cap K \cong HK/K$. C.Q.D.

Para finalizar, citaremos algumas aplicações.

Exemplos: (1) A aplicação exponencial complexa $\alpha \to e^{i\alpha}$ define um homomorfismo sobrejetor do grupo aditivo $\mathbb{R}$ sobre o grupo $\mathbb{C}$ dos complexos de norma $= 1$. O núcleo deste homomorfismo é $2\pi\mathbb{Z}$, pois 2π é o período da função $e^{i\alpha}$. Logo $\mathbb{R}/2\pi\mathbb{Z} \cong \mathbb{C}$, daí, chamar-se $\mathbb{R}/2\pi\mathbb{Z}$ de "grupo do círculo" (este exemplo já apareceu anteriormente).

(2) Seja $G = GL(n,F)$, onde F é um dos objetos seguintes: $\mathbb{Q}$ (racionais), $\mathbb{R}$ (reais), $\mathbb{C}$ (complexos), $\mathbb{Z}/p\mathbb{Z}$ (inteiros módulo um primo p). A aplicação "determinante"

$$\det: GL(n,F) \to F^* = F\setminus\{0\}$$

$$A \mapsto \det A,$$

é um homomorfismo sobrejetor. O núcleo $N(\det)$ é precisamente o grupo especial $SL(n,F)$. Pelo 1º Teorema, tem-se $GL(n,F)/SL(n,F) \cong F^*$.

(3) O centro de $GL(n,F)$ é o grupo $F^*I = \{\lambda I, \lambda \in F^*\}$ das matrizes escalares $\neq 0$ (leitor: exercício).

O grupo quociente $PL(n,F) = GL(n,F)/F^*I$ é chamado grupo linear projetivo (de grau n). O grupo linear especial projetivo é o grupo $SPL(n,F) = SL(n,F)/(F^*I \cap SL(n,F))$; pelo item (ii) do Teorema "Diamante", $SPL(n,F)$ existe. Pelo item (ii) deste mesmo teorema, tem-se $SPL(n,F) \cong (SL(n,F)\cdot F^*I)/F^*I$, logo $SPL(n,F)$ é isomorfo a um subgrupo do grupo $PL(n,F)$.

Tais grupos são os grupos de transformações básicos da Geometria Projetiva clássica.

Exercício: Mostre que o conjunto $\mathcal{J}(G)$ de todos os automorfismos internos de um grupo G constitui um grupo relativamente à composição de aplicações. Mostre que $G/\mathcal{C}(G) \cong \mathcal{J}(G)$, onde $C(G)$ é o centro de G.

Exercício: Seja G um grupo e seja G' o subgrupo de G gerado pelos elementos $ghg^{-1}h^{-1}$, com $g,h \in G$ quaisquer. Mostre:

(i) G' é normal em G;

(ii) G/G' é abeliano;

(iii) Se $H \lhd G$ e G/H é abeliano, então $G' \subset H$ (em outras palavras, G' é o menor subgrupo normal de G tal que o quociente é abeliano. G é chamado o grupo dos comutadores de G).

4. Iniciação à teoria dos corpos e dos polinômios a uma indeterminada

4.1. A noção de corpo.

Até o presente, lidamos com grupos apenas, estruturas que dependem de uma única operação. Contudo, se olharmos diversas partes da matemática (ou mesmo da natureza), notaremos que mais de uma operação faz-se presente na solução dos problemas. Por exemplo, a Álgebra Linear apoia-se na existência de duas operações (adição de vetores e produto de um escalar por um vetor). Como tal, ela está de permeio na solução de toda uma gama de problemas na natureza. Questões de economia, otimização, antropologia são aí típicas. Para ir menos longe, basta observar que o vendedor de tecidos por metragem usa Álgebra Linear diariamente ...

Em Cálculo, aprendemos a somar e multiplicar funções, tais operações derivando essencialmente da soma e produto dos números reais. Fazemos isto tão automaticamente que se perguntarmo-nos quais as propriedades fundamentais dessas operações em uso (ou como derivam umas das outras), a resposta ficará detida por alguns momentos.

No presente parágrafo, queremos atenuar tais dificuldades, pondo em relevo as propriedades que caracterizam o que há de comum

entre objetos como $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (números racionais, reais e complexos respectivamente), no que pese a diferença entre eles. O conjunto de tais propriedades caracterizará a noção de corpo.

Com a experiência adquirida na primeira parte do Curso (seja em axiomatizar ou em apreciar exemplos), passamos diretamente à abstração das idéias acima:

Definição - Um corpo é um conjunto K, munido de duas operações, designadas por $+$ e $\cdot$, satisfazendo as seguintes condições:

K.1. K, munido de $+$, é um grupo abeliano.
O elemento neutro deste grupo será designado por 0.

K.2. $K^* = K \setminus \{0\}$, munido de $\cdot$, é um grupo abeliano.
O elemento neutro deste grupo será designado por 1.

K.3. A operação $+$ é distributiva relativamente à operação $\cdot$, quer dizer, tem-se $a\cdot(b+c) = a\cdot b + b\cdot c$ para todos $a,b,c \in K$.

Exemplos de corpos são, conforme mencionamos acima, o conjunto dos números racionais (respectivamente, reais, complexos) munido das operações de soma e produto usuais. Estes exemplos, se bem que fundamentais, por si só não justificariam introduzir a noção abstrata de corpo. Mais abaixo, veremos como os exemplos se multiplicam naturalmente. Para já, temos algo suficientemente bizarro, isto é, fora dos moldes de $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$:

Exemplo: Seja $K = \mathbb{Z}/p\mathbb{Z}$, p primo. Munido da adição módulo p (isto é, adição de classes de inteiros módulo p), $\mathbb{Z}/p\mathbb{Z}$ é, como vimos, um grupo abeliano. Mas, em $\mathbb{Z}/p\mathbb{Z}$ temos também a operação

de multiplicação módulo p, conforme vimos anteriormente (vide Exemplo na pág. 73). Usando a distributividade da soma usual de inteiros relativamente ao produto, deduzimos que K.3 é válido para $\mathbb{Z}/p\mathbb{Z}$. Verifiquemos, finalmente que $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$ é grupo (abeliano). Como $\mathbb{Z}/p\mathbb{Z}$ é finito, basta verificar que $(\mathbb{Z}/p\mathbb{Z})^*$ é fechado relativamente ao produto. Em outras palavras, queremos demonstrar que se $\bar{a} \neq \bar{0}$ e $\bar{b} \neq \bar{0}$, então $\bar{a}\cdot\bar{b} \neq \bar{0}$. Ora, $\bar{a}\cdot\bar{b} = \bar{0}$ significa $ab = kp$ para algum $k \in \mathbb{Z}$. Como p é primo, resulta $p|a$ ou $p|b$, isto é, $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$.

Observação: O grupo multiplicativo $(\mathbb{Z}/p\mathbb{Z})^*$ é cíclico, o que se vê por um argumento sobre as raízes da equação $x^{p-1} - 1 = 0$, usando a função φ de Euler. Uma extensão deste argumento prova que dado um corpo qualquer K e um subgrupo finito de $K^* = K \setminus \{0\}$, tal subgrupo é sempre cíclico (o leitor pode tentar demonstrar este fato como exercício).

Regras de cálculo num corpo. As seguintes regras, válidas em $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, são válidas em qualquer corpo K:

(i) $a\cdot 0 = 0$ para todo $a \in K$

(ii) $a\cdot(-b) = (-a)\cdot b = -(a\cdot b)$ para todos $a,b \in K$

(iii) $(-a)\cdot(-b) = a\cdot b$ para todos $a,b \in K$

(iv) $a\cdot b = 0$ implica em $a = 0$ ou $b = 0$.

Demonstração: (i) Basta mostrar que $a\cdot 0 + a\cdot 0 = a\cdot 0$, pois K, + é um grupo abeliano. Ora, $0 = 0 + 0$; logo, a igualdade exigida decorre da distributividade. (ii) Resulta de (i) e da distributividade. (iii) Resulta de (ii). (iv) Se $a \neq 0$, seja a^{-1} o inverso multiplicativo de a. Tem-se $b = (a^{-1}\cdot a)\cdot b = a^{-1}\cdot(a\cdot b) =$

$= a^{-1} \cdot 0 = 0$.

Doravante, usaremos sistematicamente a notação $-a$ para o inverso aditivo de $a \in K$ e a^{-1} (ou $\frac{1}{a}$) para o inverso multiplicativo de $a \in K^*$.

Pode-se argumentar que a escolha nos axiomas de corpo é um tanto quanto arbitrária. Na verdade, exigindo menos axiomas obtemos estruturas igualmente importantes. Por exemplo, o conjunto $\mathbb{Z}$ dos inteiros possui duas operações, $+$ e $\cdot$, apesar de não constituir um corpo relativamente a tais operações. Com o intuito de prever tais situações, damos a seguinte

Definição - Um anel é um conjunto A, munido de duas operações, aqui designadas $+$ e $\cdot$, tais que:

A.1. $\langle A,+\rangle$ é um grupo abeliano.

A.2. A operação $\cdot$ é associativa e admite identidade.

A.3. A operação $+$ distribui-se relativamente à operação $\cdot$.

Um anel é comutativo se $\cdot$ é comutativa.

Doravante, estudaremos apenas anéis comutativos, de modo que suprimiremos o adjetivo "comutativo".

Exemplos de anéis comutativos são $\mathbb{Z}$, com as operações usuais de adição e multiplicação, $\mathbb{Z}/m\mathbb{Z}$ (m inteiro qualquer) com a adição e multiplicação módulo m.

Vemos que um anel comutativo é um corpo se todo elemento $a \in A$, distinto do elemento neutro do grupo $\langle A,+\rangle$, admite inverso relativamente à operação $\cdot$. Também para um anel A, designaremos

por 0, 1 os elementos identidade de $+$ e $\cdot$, respectivamente.

Uma variante do conceito de anel comutativo, intermediária entre este e o conceito de corpo, é o de <u>domínio de integridade</u>. Trata-se de um anel (comutativo) com a propriedade adicional:

A.4. Se $a \cdot b = 0$, então ou $a = 0$ ou $b = 0$.

A propriedade A.4 expressa-se, alternativamente, dizendo-se que o anel A não admite <u>divisores (próprios) de zero</u>.

<u>Exercício</u>: Mostre que as seguintes condições são equivalentes para um inteiro m:

(1) m é primo

(2) $\mathbb{Z}/m\mathbb{Z}$ é um domínio de integridade

(3) $\mathbb{Z}/m\mathbb{Z}$ é um corpo.

<u>Exercício</u>: Mostre que um domínio de integridade finito é um corpo (vide exercício anterior).

Um domínio de integridade induz, naturalmente, um corpo. Precisamente, existe um processo de construção de um corpo contendo tal domínio e de uma maneira mais "econômica" possível. Como modelo, tomaremos a construção dos números racionais a parir dos números inteiros. Recordemos que isto é feito tomando-se frações de inteiros, cujo denominador é $\neq 0$, e somando e multiplicando tais frações mediante certas regras. Em geral, procede-se da seguinte maneira.

Seja A um domínio de integridade. Consideremos o produto cartesiano $A \times (A \setminus \{0\})$ e nele definamos a seguinte relação:

$$(a,b) \sim (c,d) \quad \text{se e só se} \quad a \cdot d = b \cdot c$$

(pensemos em (a,b) como uma fração de numerador a e denominador b, e pensemos quando duas frações são "iguais").

Usando a comutatividade do produto em A, é fácil ver que $\sim$ é uma relação de equivalência. Seja K o conjunto quociente $A \times (A \setminus \{0\})/\sim$. K é nosso candidato.

Precisamos definir duas operações em K. Para tal, designaremos por $\frac{a}{b}$ a classe do par (a,b). O modelo é, novamente, o dos números racionais:

$$\frac{a}{c} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} .$$

Deixaremos como exercício a verificação de que tais operações estão bem definidas, isto é, independem dos representantes escolhidos. A esta altura, o leitor tem experiência suficiente para fazer tal verificação.

Vejamos que $\langle K,+\rangle$ é, efetivamente, um grupo abeliano. Primeiramente, K admite $\frac{0}{1}$ por elemento neutro para a adição: $\frac{a}{b}+\frac{0}{1} = \frac{a\cdot 1 + b\cdot 0}{b\cdot 1} = \frac{a + b\cdot 0}{b}$; ora, $b\cdot 0 = 0$ também num anel A (a demonstração deste fato independe da existência de inversos multiplicativos). Logo, $\frac{a}{b} + \frac{0}{1} = \frac{a}{b}$. O inverso aditivo de $\frac{a}{b}$ existe e é dado por $\frac{-a}{b}$; com efeito, $\frac{a}{b} + \frac{-a}{b} = \frac{a\cdot b + (-a)\cdot b}{b^2} = \frac{0}{b^2} = \frac{0}{1}$ (novamente, a propriedade $(-a)\cdot b = -(a\cdot b)$ é válida num anel qualquer).

Análoga é a verificação de que $\langle K^*,\cdot\rangle$ é um grupo abeliano. A identidade é a classe $\frac{1}{1}$ e o inverso de $\frac{a}{b} \neq \frac{0}{1}$ é $\frac{b}{a}$ (N.B. $\frac{a}{b} \neq \frac{0}{1} \Rightarrow a \neq 0$).

A associatividade e comutatividade das operações derivam

imediatamente das propriedades de mesmo nome em A, bem como a distributividade.

Assim, K é um corpo. Os elementos de K são chamados frações. K é chamado o corpo de frações de A.

Para finalizar a discussão, queremos por em relevo o fato de que K contém A de maneira mais econômica possível. Para tal, necessitamos a noção paralela à noção de homomorfismo de grupos.

Se A, A' são anéis, um homomorfismo de A em A' é uma aplicação $\varphi: A \to A'$ tal que:

(i) $\varphi(a+b) = \varphi(a) + \varphi(b)$

(ii) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

(iii) $\varphi(1_A) = 1_{A'}$, onde 1_A é a identidade multiplicativa de A e $1_{A'}$ é a identidade multiplicativa de A'.

A condição (i) diz apenas que φ é um homomorfismo dos grupos aditivos $\langle A,+\rangle$ e $\langle A',+\rangle$. A condição (ii) afirma que φ preserva a multiplicação. De (i) resulta, como já mencionamos anteriormente, que $\varphi(0) = 0$; não se pode, contudo, deduzir de (ii) que $\varphi(1) = 1$ já que a operação de multiplicação não tem a propriedade de inverso. Logo, a condição (iii) tem de ser exigida separadamente.

O núcleo de um homomorfismo $\varphi: A \to A'$ de anéis é o núcleo $N(\varphi)$ de φ, considerado como homomorfismo dos grupos abelianos $\langle A,+\rangle$ e $\langle A',+\rangle$. Assim, $N(\varphi) = \{a \in A \mid \varphi(a) = 0\}$. Um homomorfismo injetor φ é um monomorfismo. Como antes, isto acontece se e só se $N(\varphi) = (0)$. Um monomorfismo sobrejetor é um isomorfismo; neste caso, os anéis em questão são ditos isomorfos, podendo ser identificados

para a maioria dos propósitos.

Exercício: Um homomorfismo de um corpo num anel qualquer é um monomorfismo, a menos que o anel seja nulo.

Um subanel de um anel A é um subconjunto $B \subset A$ que constitui um anel com respeito às operações induzidas de A. Em outras palavras, $B \subset A$ é um subanel se é um subgrupo do grupo $\langle A,+\rangle$ que contém $1 \in A$ e é fechado relativamente ao produto em A. Um subanel que é um corpo é chamado subcorpo.

Exercício: As seguintes condições são equivalentes para um subconjunto B de um anel A:

(1) B é subanel de A

(2) Existe um anel A' e um homomorfismo $\varphi: A' \to A$ tal que $\varphi(A') = B$.

Voltemos à propriedade fundamental do corpo de frações K de um domínio de integridade A. Ela pode ser enunciada na seguinte forma:

Proposição - A é isomorfo a um subanel de K por meio de uma aplicação canônica $\iota: A \to K$. Se L é um corpo e $\varphi: A \to L$ um monomorfismo, então existe um (e um só) homomorfismo $\varphi': K \to L$ tal que $\varphi = \varphi' \circ \iota$.

Demonstração: Definimos $\iota: A \to K$ por $\iota(a) = \frac{a}{1}$. É fácil verificar que ι é um homomorfismo de anéis e que ι é injetor. Dado $\varphi: A \to L$, definimos $\varphi'(\frac{a}{b}) = \varphi(a) \cdot (\varphi(b))^{-1}$. Isto tem sentido pois $\varphi(b) \neq 0$, uma vez que φ é injetor e $b \neq 0$. Obtemos, desta maneira, uma aplicação $\varphi': K \to L$, a qual se verifica, por um cálcu-

lo direto, ser um homomorfismo.

Por outro lado, $\varphi'(\iota(a)) = \varphi'(\frac{a}{1}) = \varphi(a) \cdot \varphi(1)^{-1} = \varphi(a) \cdot 1 =$ $= \varphi(a)$ para todo $a \in A$, mostrando que $\varphi = \varphi' \circ \iota$.

Deixamos ao leitor o cuidado de verificar que φ' é única com a condição $\varphi = \varphi' \circ \iota$. C.Q.D.

Assim, quando dizemos que o número racional $\frac{m}{1}$ é igual ao inteiro m, estamos afirmando no fundo que o anel $\mathbb{Z}$ é isomorfo a um subanel de $\mathbb{Q}$ através do homomorfismo $m \to \frac{m}{1}$!! A proposição acima diz que $\mathbb{Q}$ é o "menor" corpo contendo $\mathbb{Z}$; todo corpo que contém um anel isomorfo a $\mathbb{Z}$ já contém um subcorpo isomorfo a $\mathbb{Q}$.

Exercício: Seja K um corpo e $m \in \mathbb{Z}$. Defina

$$m \cdot 1 = \begin{cases} 1 + \ldots + 1 \quad (m \text{ vezes}) & \text{se } m > 0 \\ 0 & m = 0 \\ -1 - \ldots - 1 \quad (-m \text{ vezes}) & \text{se } m < 0. \end{cases}$$

Suponha que existe $m \in \mathbb{Z}$ $m \neq 0$ tal que $m \cdot 1 = 0$. Mostre que já existe um $m \in \mathbb{Z}$, $m > 0$, tal que $m \cdot 1 = 0$ e que o menor tal m é um número primo (tal primo é chamado a característica do corpo K; se nenhum $m \neq 0$ existe tal que $m \cdot 1 = 0$, dizemos que K tem <u>característica</u> 0).

Exercício: Mostre K tem característica 0 se e só se $\mathbb{Q}$ é isomorfo a um subcorpo de K e que K tem característica p (p primo) se e só se $\mathbb{Z}/p\mathbb{Z}$ é isomorfo a um subcorpo de K.

Dados corpos K e L e um homomorfismo $\varphi: K \to L$, temos

que φ é automaticamente injetor, logo K é isomorfo a um subcorpo de L. Dizemos que L é uma <u>extensão</u> de K. Usamos a notação $L|K$ e dizemos também que $L|K$ é uma <u>extensão de corpos</u> (sempre subentendido o monomorfismo original $\varphi: K \to L$, chamado <u>estrutural</u>).

Dada uma extensão de corpos $L|K$, L admite uma estrutura natural de espaço vetorial sobre o corpo K. Em outras palavras temos uma adição de "vetores", que é a adição de L como corpo, e um produto de elementos de L ("vetores") por "escalares" (elementos de K), a saber:

$$\lambda \cdot a \stackrel{\text{def.}}{=} \varphi(\lambda) \cdot a,$$

onde $\lambda \in K$, $a \in L$, e $\varphi: K \to L$ é o monomorfismo estrutural.

Por exemplo, se $L = \mathbb{C}$ e $K = \mathbb{R}$, L é um espaço vetorial de dimensão 2 sobre K. Contudo, nem sempre L é de dimensão finita sobre K, como veremos adiante.

4.2. <u>Polinômios a uma indeterminada sobre um corpo</u>.

Vamos considerar polinômios com coeficientes não somente em $\mathbb{R}$ ou $\mathbb{C}$, mas com coeficientes num corpo qualquer K.

Num curso de Cálculo, polinômios aparecem como funções que procuramos integrar, derivar ou calcular seus limites. Aqui, nossa preocupação estará em torno das propriedades "algébricas" dos polinômios, em especial, de suas propriedades aritméticas. Este é um aspecto a ser enfatizado no nosso Curso.

Por outro lado, no Secundário insistimos, com obstinação cega, em calcular raízes de um polinômio. Como trata-se de tarefa inexequível na prática (em geral) calcular raízes explicitamente, optamos por uma linha conceitual. Nomeadamente, construímos ao menos um corpo que contém alguma raiz do polinômio. Esta construção é o portão de entrada para a Teoria de Galois, a ser vista em outro Curso.

Com tais objetivos delineados claramente, partamos às definições.

Um polinômio sobre um corpo K (ou com coeficientes em K) é uma expressão formal $a_o + a_1X + \ldots + a_nX^n$, onde X é um símbolo (sem significado no momento) e $a_i \in K$, $i = 0, \ldots, n$. É assim que somos apresentados aos polinômios no Secundário ou num curso de Cálculo. Esta é, como dissemos, uma apresentação formal. Um relacionamento mais profundo exige a personalidade autêntica dos objetos em questão. Rigorosamente, portanto, um polinômio deve ser definido como uma seqüência $a_o, a_1, \ldots, a_n, \ldots$ de elementos de K tal que existe n para o qual $a_i = 0$, se $i > n$.

Duas seqüências $a_o, \ldots, a_n, \ldots$ e $b_o, \ldots, b_n, \ldots$ são ditas "iguais" se $a_i = b_i$, $i = 0, 1, 2, \ldots$ (pensando em tais seqüências como funções de $\mathbb{N}$ em K, trata-se do conceito de igualdade de funções). Dois polinômios $\sum_i a_iX^i$ e $\sum_i b_iX^i$ são "iguais" (isto é, uma relação de equivalência!) se as seqüências que os definem são iguais.

Seja $K[X]$ o conjunto de todos os polinômios sobre K (ou, melhor, das classes de "igualdade" de polinômios !). Introduzimos operações em $K[X]$ da maneira usual:

$$\sum_i a_i X^i + \sum_i b_i X^i = \sum_i (a_i + b_i) X^i$$

$$(\sum_i a_i X^i) \cdot (\sum_i b_i X^i) = \sum_k \left(\sum_{i=0}^{k} a_i \, b_{k-i} \right) X^k$$

É mera rotina verificar que $K[X]$, munido dessas operações, é um anél (comutativo). O elemento neutro de $+$ é o polinômio $0 + 0X + \ldots + 0X^n + \ldots$. O elemento identidade de $\cdot$ é $1 + 0X + \ldots$.

A primeira observação é que os elementos de K são polinômios de um tipo especial. Precisamente, existe um monomorfismo canônico $K \to K[X]$ definido por $a \mapsto a + 0X + \ldots$. Isto permite identificar elementos de K com polinômios de $K[X]$, os quais serão chamados os <u>polinômios constantes</u> ou as <u>constantes</u> de $K[X]$.

A segunda observação é a propriedade essencial seguinte (que caracteriza $K[X]$ no sentido precisado no exercício que se segue):

<u>Proposição</u> - Para todo anel A, dado um homomorfismo qualquer $\varphi: K \to A$ e dado um elemento qualquer $a \in A$, existe um e um só homomorfismo $\tilde{\varphi}: K[X] \to A$ tal que $\tilde{\varphi}(\alpha) = \varphi(\alpha)$ para todo $\alpha \in K$ e tal que $\tilde{\varphi}(X) = a$.

<u>Demonstração</u>: A existência é o ponto essencial, pelo que deixaremos a unicidade como exercício. Definimos $\tilde{\varphi}$ da seguinte maneira:

$$\tilde{\varphi}(\sum a_i X^i) = \sum \varphi(a_i) \cdot a^i.$$

É fácil ver que $\tilde{\varphi}$ é um homomorfismo de $K[X]$ em A, para o que usa-se simplesmente que φ é um homomorfismo. Por outro lado, $\tilde{\varphi}(X) = \tilde{\varphi}(0 + 1 \cdot X + 0 \cdot X^2 + \ldots) = \varphi(0) \cdot a^0 + \varphi(1) \cdot a^1 + \varphi(0) \cdot a^2 + \ldots = 0 \cdot a^0 +$

$+ 1\cdot a^1 + 0\cdot a^2 + \ldots = a$, fornecendo uma das propriedades requeridas. Demonstra-se, analogamente, que $\tilde{\varphi}(a_o + 0\cdot X + 0\cdot X^2 + \ldots) = \varphi(a_o)$ para todo $a_o \in K$.

Observação: Se bem que todo homomorfismo $K \to A$ seja injetor, em virtude de K ser corpo, o homomorfismo induzido $K[X] \to A$ (uma vez prescrito um elemento $a \in A$) nem sempre é injetor. Por exemplo, se $A = K$ e $K \to K$ é o homomorfismo identidade e $a = 1$, o homomorfismo induzido $K[X] \to K$ leva todo polinômio da forma $(X-1)\cdot f(X)$, com $f(X) \in K[X]$ qualquer, no 0. (Na verdade, o núcleo é exatamente constituído por tais polinômios).

Exercício: Determine todos os isomorfismos φ de $K[X]$ sobre $K[X]$ tais que $\varphi(a) = a$ para todo $a \in K$.

Com o objetivo de analisar mais de perto a estrutura do anel $K[X]$, necessitamos a noção de grau de um polinômio $\Sigma\, a_i X^i \neq 0$: trata-se do menor natural n tal que $a_i = 0$ para todo $i \geq n$. O grau de 0 não está definido (alguns autores definem o grau de 0 como sendo ∞ ou -1). Usamos a notação $gr(f)$ para o grau de $f \in K[X]$.

Proposição - (1) $K[X]$ é um domínio de integridade.

(2) Se $f, g \in K[X]$ são diferentes de 0,

tem-se:

$$gr(f\cdot g) = gr(f) + gr(g).$$

Demonstração: Sejam $f = a_o + a_1 X + \ldots + a_n X^n$, $a_n \neq 0$, e $g = b_o + b_1 X + \ldots + b_m X^m$, $b_m \neq 0$. Em outras palavras, $gr(f)=n$, $gr(g) = m$. Por definição, $f\cdot g = a_o b_o + (a_o b_1 + b_o a_1)X + \ldots + a_n b_m X^{n+m}$.

Como K é um corpo, tem-se $a_n b_m \neq 0$. Logo, $f \cdot g \neq 0$ e $gr(f \cdot g) = n+m = gr(f) + gr(g)$. C.Q.D.

O grau de um polinômio é a noção que está para os polinômios assim como o módulo $|m|$ de um inteiro m está para o anel dos inteiros. Isto pode parecer bizarro à primeira vista, uma vez que o grau satisfaz a condição (2) da Proposição acima, ao passo que $|m \cdot n| = |m| \cdot |n|$. No entanto, do ponto de vista da estrutura interna de $K[X]$ e $\mathbb{Z}$, as funções "grau" e "módulo" provocam resultados paralelos. Por exemplo, $K[X]$ admite um algoritmo de divisão análogo ao algoritmo euclideano de $\mathbb{Z}$:

Teorema (Divisão euclideana em $K[X]$) - Dados $f,g \in K[X]$, com $g \neq 0$, existem $q,r \in K[X]$ tais que

$$f = g \cdot q + r,$$

com $r = 0$ ou $gr(r) < gr(g)$.

Demonstração: Consiste em formalizar o processo de "longa divisão" de polinômios aprendido (?) no Secundário. Poremos de parte os casos em que $f = 0$ ou $gr(f) < gr(g)$ por admitirem solução imediata. Supomos, pois, que $f = a_o + \ldots + a_n X^n$, $g = b_o + \ldots + b_m X^m$, com $a_n \neq 0$, $b_m \neq 0$ e $n \geq m$. Consideremos o polinômio $h = f - (\frac{a_n}{b_m}) X^{n-m} \cdot g(X)$. Tem-se $gr(h) < gr(f)$ evidentemente, o que nos convida a aplicar indução finita sobre o grau de f. Façamo-lo, pois (a 1ª etapa da indução, isto é, o caso em que $gr(f) = 0$, será deixada aos cuidados do leitor). Pela hipótese de indução, existem $q_1, r_1 \in K[X]$, com $r_1 = 0$ ou $gr(r_1) < gr(g)$, tais que $h = g \cdot q_1 + r_1$. Comparando, resulta:

$$f = ((\frac{a_n}{b_m})X^{n-m} + q_1)\cdot g + r_1 .$$

Basta, então, tomar $q = (\frac{a_n}{b_m})X^{n-m} + q_1$ e $r = r_1$. C.Q.D.

Exercício: Dados polinômios $h,k \in K[X]$ tais que $h+k \neq 0$, mostre q
$gr(h+k) \leq \max\{gr(h), gr(k)\}$. Se $h \neq 0$ e $k \neq 0$, mostre que $gr(h) \leq gr(h\cdot k)$. Deduza que os polinômios $q,r \in K[X]$ no algoritmo de divisão são unicamente determinados.

Os polinômios $q,r \in K[X]$ acima determinados são chamados o quociente e o resto da divisão, respectivamente. Se $r = 0$, f é divisível por g.

Recordemos que uma das conseqüências mais interessantes da existência de algoritmo de divisão em $\mathbb{Z}$ foi o fato de que todo subgrupo de $\langle \mathbb{Z},+\rangle$ é cíclico. Qual a conseqüência paralela para o anel $K[X]$? Certamente, não há qualquer chance de provar que todo subgrupo de $\langle K[X],+\rangle$ é cíclico, já que, em particular, os subgrupos de $\langle K,+\rangle$ são subgrupos de $\langle K[X],+\rangle$ e entre aqueles alguns podem deixar de ser cíclicos (considere, por exemplo, o caso $K = \mathbb{Q}$).

O que precisamos é de uma noção paralela a de subgrupo normal. Um subgrupo normal era exatamente o núcleo de um homomorfismo de grupos. Quais são as propriedades de $N(\varphi)$, se $\varphi: A \to A'$ é um homomorfismo de anéis ? Primeiramente, $N(\varphi)$ é um subgrupo de $\langle A,+\rangle$. Em seguida, se $b \in N(\varphi)$ e $a \in A$, então $ab \in N(\varphi)$. Abstraindo tais propriedades, temos a noção de ideal: trata-se de um subgrupo I de um anel A (isto é, do grupo $\langle A,+\rangle$ do anel A) tal que $ab \in I$ sempre que $b \in I$ e $a \in A$.

Definimos, analogamente, o conceito de ideal gerado por

um subconjunto $S \subset A$: é o menor (relativamente à inclusão) ideal de A contendo S. Tal ideal, designado por (S), sempre existe e é dado, como no caso de subgrupo gerado por um subconjunto, pela interseção $\bigcap_i I_i$, onde I_i varre o conjunto de ideais de A contendo S (existe ao menos um, a saber, o próprio A).

Exemplo: Em $\mathbb{Z}$, todo ideal é da forma $m\mathbb{Z}$, para algum m. Em outras palavras, ideais de $\langle \mathbb{Z},+,\cdot \rangle$ e subgrupos de $\langle \mathbb{Z},+ \rangle$ são a mesma coisa.

Exercício: Sejam $I,J \subset A$ ideais. Mostre que $I \cap J$, $I + J = \{a+b \mid a \in I,\ b \in J\}$, $I \cdot J = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in I,\ b_i \in J,\ n \in \mathbb{N}\}$ são ideais de A.

Exercício: Mostre que se $S \subset A$ é um subconjunto qualquer,
$$(S) = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in S,\ b_i \in A,\ n \in \mathbb{N}\}.$$

Um ideal é dito principal se puder ser gerado por $\{a\}$, para algum elemento a de A. Por exemplo, os ideais de $\mathbb{Z}$ são todos principais. Eis o fato análogo para $K[X]$ a que nos referíamos acima.

Proposição - Todo ideal de $K[X]$ é principal.

Demonstração: Seja $I \subset K[X]$ um ideal. Se $I = \{0\}$, I é certamente gerado por 0. Se $I \neq \{0\}$, seja $0 \neq g \in I$ de menor grau possível (pode haver mais de um tal g, não importa). Dado $f \in I$, dividamos f por g pela divisão euclideana: $f = g \cdot q + r$, com $q,r \in K[X]$ e $r = 0$ ou $gr(r) < gr(g)$. Como $f \in I$ e $g \in I$, segue-se que $r = f - g \cdot q \in I$. Se $r \neq 0$, tem-se $gr(r) < gr(g)$, con-

tradizendo a escolha de g. Logo, $r = 0$, o que mostra que $f = g \cdot q \in$ $\in (g)$. Em outras palavras, $I = (g)$. C.Q.D.

Exercício: Seja $\mathbb{Z}[X] = \{\Sigma a_i X^i \in \mathbb{Q}[X] \mid a_i \in \mathbb{Z}\}$. Mostre que $\mathbb{Z}[X]$ é um subanel de $\mathbb{Q}[X]$ (chamado anel de polinômios a coeficientes inteiros). Mostre que o ideal de $\mathbb{Z}[X]$ gerado pelo subconjunto $\{2,X\}$ não é principal.

O exercício acima mostra que existem anéis admitindo ideais que não são principais. Desta maneira, $\mathbb{Z}$ e $K[X]$ são bastante especiais.

Outra conseqüência, de caráter aritmético, análoga às que ocorrem com $\mathbb{Z}$, diz respeito a máximo divisor comum. Dois polinômios $f,g \in K[X]$ admitem um máximo divisor comum $d \in K[X]$ se d satisfaz as condições seguintes:

(1) f e g são ambos divisíveis por d.

(2) Se $d' \in K[X]$ divide f e g, então d' divide d.

Notemos que um máximo divisor comum não é unicamente determinado. Com efeito, se d é m.d.c. de f, g, ad também o é para qualquer $a \in K$, $a \neq 0$. Mas, esta falta de unicidade é o único mal presente, como mostra o exercício abaixo.

Exercício: Se d, d' são máximos divisores comuns de f, g então existe $a \in K$, $a \neq 0$, tal que $d' = ad$.

Proposição - Se d é um m.d.c. de $f,g \in K[X]$, então existem $h,k \in K[X]$ tais que $d = f \cdot h + g \cdot k$. Mais precisamente, o conjunto dos m.d.c.'s de f e g coincide com o conjunto dos po-

linômios d' tais que $(f,g) \subset (d')$ (isto é, (d') gera o ideal (f,g) gerado por f e g).

Demonstração: Exercício.

Observação: A teoria dos ideais tem aplicações geométricas importantes. Para ilustrar, temos a noção de resultante de dois polinômios $f,g \in K[X]$, que é definida como um certo polinômio $f \cdot h + g \cdot k \in (f,g)$, onde $gr(h) = gr(g)-1$ e $gr(k) = gr(f)-1$. Esta noção é bastante clássica e serve para demonstrar teoremas fundamentais da teoria das curvas algébricas, tais como o teorema de Bézout, que conta o número de pontos de interseção (com respectivas multiplicidades) de duas curvas algébricas.

Exercício: Mostre como polinômios h, k da proposição acima podem ser determinados usando o algoritmo de divisão. Ilustre no caso em que $f = 2X^4 + 9X^3 - 11X^2 + 5X-1$ e $g = 2X^3 - 3X^2 + 5X-2$.

Exercício: Seja $f(X) \in K[X]$ e seja $a \in L$ uma raiz de $f(x) = 0$, onde $L|K$ é uma extensão de corpos. Mostre:

(i) $X-a$ divide $f(X)$ em $L[X]$

(ii) O núcleo do homomorfismo $K[X] \to L$ tal que $X \to a$ e tal que $K \to L$ é a injeção estrutural, é gerado por $X-a$.

Deduza que $f(x) = 0$ admite no máximo $gr(f)$ raízes distintas em qualquer extensão L de K.

Com o objetivo de prosseguir nossa exploração do anel $K[X]$, convém retomar um pouco os ideais em abstrato.

Dado um anel A e um ideal I, temos o grupo quociente

A/I do grupo aditivo de A pelo subgrupo I, conforme o exposto na primeira parte do Curso. Queremos munir A/I de uma estrutura de anel, o que será possível graças a que I é não só subgrupo, mas também ideal.

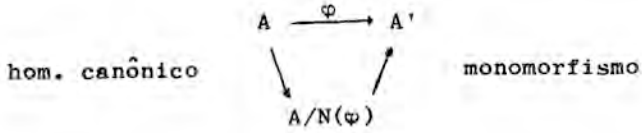
A idéia é definir uma operação imitando o que se fez com $\mathbb{Z}/p\mathbb{Z}$. No caso de $\mathbb{Z}/p\mathbb{Z}$, definimos:

$$\bar{a}\cdot\bar{b} = \overline{ab},$$

onde a barra sobre um $a \in \mathbb{Z}$ designa sua classe de equivalência módulo p. A operação estava bem definida graças ao fato (um tanto camuflado àquela altura) de que $p\mathbb{Z}$ era um ideal.

Em geral, o procedimento é análogo. Os elementos do grupo A/I são classes $\bar{a}$, com $a \in A$. Decretamos, como no caso de $\mathbb{Z}/p\mathbb{Z}$, que $\bar{a}\cdot\bar{b} = \overline{ab}$, para $a,b \in A$. Se $\bar{a}' = \bar{a}$ e $\bar{b}' = \bar{b}$, tem-se $a' = a+u$ e $b' = b+v$, com $u,v \in I$. Logo, $a'b' = (a+u)(b+v) = ab + av + ub + uv$. Como I é ideal, av, ub, $uv \in I$, seguindo-se, portanto, que $\overline{a'b'} = \overline{ab}$. Assim, a operação está bem definida. O fato de que A/I torna-se um anel com tal operação é trabalho de verificação rotineira.

É imediato que a aplicação canônica $A \to A/I$ é um homomorfismo de anéis. Todo homomorfismo de anéis, $\varphi: A \to A'$, decompõe-se em um homomorfismo sobrejetor seguido de um homomorfismo injetor, de acordo com o seguinte diagrama:



Mais geralmente, se $\varphi: A \to A'$ é um homomorfismo e se $I \subset N(\varphi)$, então tem-se um homomorfismo induzido (de maneira natural) $\bar{\varphi}: A/I \to A'$. Disso segue-se, como é fácil de verificar, que se $I' \subset A'$ é um ideal e $\varphi^{-1}(I') = I \subset A$ a imagem inversa de I' (exercício: I é um ideal), tem-se um monomorfismo induzido $\bar{\varphi}: A/I \to A'/I'$.

Todos os fatos acima são completamente análogos aos da teoria dos grupos; em particular, temos os teoremas de isomorfismo (essencialmente, a existência de $\bar{\varphi}$ acima), etc. Deixaremos ao leitor o cuidado de formular para si próprio as proposições paralelas para anéis e demonstrá-las.

Exercício: Seja $A = \mathbb{Z}[X]$, $A' = \mathbb{Q}[X]$ e $\varphi: A \to A'$ a injeção canônica $\mathbb{Z}[X] \subset \mathbb{Q}[X]$ induzida pela injeção canônica de $\mathbb{Z}$ em $\mathbb{Q}$. Seja $I' = (X + \frac{1}{2})$. Mostre que $\varphi^{-1}(I') = I' \cap \mathbb{Z}[X] = (2X+1)$ e que $\mathbb{Q}[X]/(X + \frac{1}{2})$ é isomorfo a $\mathbb{Q}$. Qual é a imagem de $\mathbb{Z}[X]/(2X+1)$ em $\mathbb{Q}$?

Além de ideais principais, os seguintes ideais são importantes: um ideal $I \subset A$ é **máximo** se $I \neq A$ e se $I \subset I' \subset A$, com I' ideal, implicar $I = I'$ ou $I' = A$. Um ideal $I \subset A$ é **primo** se $I \neq A$ e se a seguinte condição tiver lugar: $a \cdot b \in I$ implica $a \in I$ ou $b \in I$.

Exemplos: (1) Em $\mathbb{Z}$, os ideais primos são precisamente os ideais (p), onde $p \in \mathbb{Z}$ é um número primo (daí a designação). Como os ideais de $\mathbb{Z}$ são todos principais, segue-se facilmente que os ideais máximos de $\mathbb{Z}$ são exatamente os ideais primos de $\mathbb{Z}$.

(2) Como em (1) os ideais primos de $K[X]$ são os ideais $(f(X))$, com $f(X)$ irredutível. Pelo mesmo motivo acima, estes são exatamente os ideais máximos de $K[X]$.

Exercício: Mostre que todo ideal de $\mathbb{Z}$ escreve-se de maneira única na forma $P_1^{r_1} \cdot \ldots \cdot P_n^{r_n}$, com P_i ideal primo e $r_i \geq 0$ ($P_i \neq P_j$ se $i \neq j$).

(N.B. Por definição, $I^r = I \cdot \ldots \cdot I$ (r vezes), e $I_1 \cdot I_2 \cdot I_3 = (I_1 \cdot I_2) \cdot I_3$, etc.).

Eis um critério para decidir se um ideal é máximo (respectivamente, primo).

Proposição - Seja A um anel, $I \subset A$ um ideal.

(i) I é máximo se e só se A/I é um corpo

(ii) I é primo se e só se A/I é domínio de integridade.

Corolário - Se $I \subset A$ é um ideal máximo então I é primo.

Exercício: Mostre que $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$. Qual é a imagem do subanel $\mathbb{Q}[X]/(X^2+1)$ mediante tal isomorfismo ?

Exercício: Mostre que o corpo de frações de $\mathbb{Z}[X]$ e o de $\mathbb{Q}[X]$ são canonicamente isomorfos.

Exercício: Se A é um domínio de integridade de $P \subset A$ um ideal primo, mostre que $A_p = \{\frac{a}{b} \in K \mid b \notin P\}$ é um subanel do corpo K de frações de A. Mostre que A_p admite um único ideal máximo, descreva-o ! Se $A = \mathbb{Z}$ e $P = (p)$, com p primo, mostre que A_p admite apenas dois ideais primos.

4.3. Aplicações ligeiras às extensões de corpos e aos números algébricos.

Recordemos que um corpo L é dito uma extensão de um corpo K se $K \subset L$ (vide pág. 90). Um polinômio $f(X) \in K[X]$ é irredutível (sobre K) se sempre que $f(X) = g(X) \cdot h(X)$, com $g, h \in K[X]$, então $g(X) = \text{const.}$ ou $h(X) = \text{const.}$

O problema que se põe é o seguinte: dado $f(X) \in K[X]$ irredutível, K pode não conter nenhuma raiz de $f(X)$ (uma raiz de f é um elemento α de uma extensão $L|K$ tal que $f(\alpha) = 0$, onde $f(\alpha)$ é a imagem de $f(X)$ mediante o K-homomorfismo(*) $K[X] \to L$ tal que $X \to \alpha$). É possível construir um corpo L contendo K e contendo uma raiz de $f(X)$?

A resposta é afirmativa. Mais precisamente, tem-se:

Proposição - Seja K um corpo e seja $f = f(X) \in K[X]$ irredutível. Então $K[X]/(f)$ é um corpo e o elemento $\bar{X} \in K[X]/(f)$, imagem de X pelo homomorfismo quociente $K[X] \to K[X]/(f)$, é uma raiz de f.

Demonstração: De acordo com o Exemplo (2) à pág. 101 e pela Proposição à pág. 101, concluímos que $K[X]/(f)$ é um corpo. Como K é um corpo, a aplicação canônica $K \to K[X]/(f)$ (composta

(*) Um homomorfismo $\varphi: K[X] \to A$, onde A é um anel contendo K como subcorpo, é dito um K-homomorfismo se $\varphi(a) = a$ para todo $a \in K$.

da aplicação canônica $K \to K[X]$ e da aplicação quociente $K[X] \to$ $\to K[X]/(f))$ é um monomorfismo. Logo, $K[X]/(f)$ é uma extensão de K.

Finalmente, se $\bar{\varphi}: K[X] \to K[X]/(f)$ é o homomorfismo quociente, tem-se $f(\bar{X}) = f(\bar{\varphi}(X)) = \bar{\varphi}(f(X)) = \bar{0}$ (Proposição da pág. 92) Logo, $\bar{X}$ é uma raiz de f em $K[X]/(f)$. C.Q.D.

Definição - Seja B um domínio de integridade, seja $A \subset B$ um subanel (como sempre, A possui a mesma identidade 1 de B) e seja $S \subset B$ um subconjunto. O subanel de B gerado por S sobre A é o menor subanel de B contendo A e S.

Analogamente, dada uma extensão $L|K$ de corpos e um subconjunto $S \subset L$, o subcorpo de L gerado por S sobre K é o menor subcorpo de L contendo S e K.

A técnica para mostrar a existência dos objetos ora definidos é sempre a mesma. Usaremos as seguintes notações, respectivamente: $A[S]$, $K(S)$. Se $S = \{x_1, \ldots, x_n\}$, escreveremos apenas $A[x_1, \ldots, x_n]$, $K(x_1, \ldots, x_n)$, esquecendo as chaves $\{\ \}$. É fácil verificar que $K(S)$ é o corpo de frações (ou melhor, isomorfo ao corpo de frações) de $K[S]$.

Eis uma descrição explícita dos elementos de $A[x_1, \ldots, x_n]$. Um elemento genérico é da forma $\sum_{i_1, \ldots, i_n} a_{i_1, \ldots, i_n} \cdot x_1^{r_1} \cdot \ldots \cdot x_n^{r_n}$, com $r_1, \ldots, r_n \geq 0$ e $a_{i_1}, \ldots, a_n \in A$. Consequentemente, os elementos de $K(x_1, \ldots, x_n)$ são da forma

$$\frac{\sum_{i_1,\ldots,i_n} a_{i_1\ldots i_n} \cdot x_1^{r_1} \cdot \ldots \cdot x_n^{r_n}}{\sum_{i_1,\ldots,i_n} b_{i_1,\ldots i_n} \cdot x_1^{r_1} \cdot \ldots \cdot x_n^{r_n}}, \quad \text{com } a_{i_1\ldots i_n},\ b_{i_1\ldots i_n} \in K.$$

Em particular, se $n = 1$, $K[x] = \{\sum_i a_i \cdot x^i \mid a_i \in K\}$, de maneira que os elementos de $K[x]$ parecem-se "polinômios em x". Contudo, cuidado ! $\sum a_i x^i$ não se comporta como polinômio em geral, podendo acontecer que $\sum a_i x^i = \sum b_i x^i$ sem que necessariamente $a_i = b_i$ para todo i. Por exemplo, se $K = \mathbb{R}$, se $L = \mathbb{C}$ e $x = i$, onde $i^2 = -1$, tem-se em $\mathbb{R}[i]$:

$$1 + i^2 = 0,$$

mas $1 \neq 0$.

A razão de tal fenômeno é que x pode comportar-se de dois modos distintos sobre um corpo K.

Definição - Seja $L|K$ uma extensão de corpos e seja $x \in L$. Se existir um polinômio $f(X) \in K[X]$, $f \neq 0$, tal que x seja raiz de $f(X)$, dizemos que x é algébrico sobre K. Caso contrário, x é transcendente sobre K.

A segunda noção parece familiar ? Na verdade, o é ! Se $K = \mathbb{Q}$ e $L = \mathbb{C}$ (ou $L = \mathbb{R}$), a noção de $x \in \mathbb{C}$ ser transcendente sobre $\mathbb{Q}$ coincide com a de "número transcendente". Assim, os números π e e (base dos logaritmos neperianos) são transcendentes sobre $\mathbb{Q}$. As únicas provas disso são analíticas, não se conhecendo prova puramente algébrica ! Pode-se mostrar que o conjunto dos transcendentes (sobre $\mathbb{Q}$) tem um cardinal igual ao cardinal de $\mathbb{R}$ ($2^{\aleph_0}$), de mo

do que, neste sentido, existem muito mais números transcendentes do que algébricos (o conjunto dos números algébricos tem apenas o cardinal do conjunto $\mathbb{N}$ dos naturais). Ironia matemática, contudo, a de que até metade do século passado não se conhecia explicitamente nenhum número transcendente ...

Dados uma extensão $L|K$ de corpos e um elemento $x \in L$, temos um único K-homomorfismo $K[X] \to L$ tal que $X \mapsto x$. Dizer que x é transcendente sobre K significa exatamente que o núcleo deste homomorfismo é (0). Em outras palavras, x é transcendente sobre K se e só se $K[X]$ é isomorfo ao subanel $K[x]$ de L gerado por x sobre K. Assim, no caso transcendente, os elementos de $K[x]$ são efetivamente polinômios em x.

Que acontece no caso algébrico ? A resposta encontra-se na seguinte

Proposição - Seja $K|L$ uma extensão, seja $x \in L$ um elemento algébrico sobre K e seja $f(X) \in K[X]$ um polinômio, de menor grau possível, do qual x é raiz. Então:

(i) $K[x]$ é um corpo, isto é, $K[x] = K(x)$

(ii) $K[X]/(f(X))$ é isomorfo a $K[x] = K(x)$

(iii) $K(x)$ é um espaço vetorial de dimensão $gr(f)$ sobre o corpo K. Precisamente, $\{1, x, \ldots, x^{gr(f)-1}\}$ constitui uma base para tal espaço vetorial.

Demonstração: Seja $n = gr(f)$, digamos, $f = a_n X^n + \ldots + a_1 X + a_o$, com $a_n \neq 0$. (Podemos supor que $a_n = 1$, mas isto é irrelevante). Por hipótese, $a_n x^n + \ldots + a_1 x + a_o = 0$, logo tem-se que

$$x^n = -a_o a_n^{-1} - a_1 a_n^{-1} x - \ldots - a_{n-1} a_n^{-1} x^{n-1}.$$

Disso segue-se que, de fato, não só x^n, mas x^{n+r} para todo $n \geq 0$, escreve-se na forma $\alpha_o \cdot 1 + \alpha_1 \cdot x + \ldots + \alpha_{n-1} \cdot x^{n-1}$ para certos $\alpha_i \in K$. Mostramos, assim, que

$$K[x] = \{\alpha_o + \alpha_1 x + \ldots + \alpha_{n-1} x^{n-1} \mid \alpha_i \in K\}.$$

Ora, seja $\alpha_o + \alpha_1 x + \ldots + \alpha_{n-1} x^{n-1} \neq 0$ e ponhamos $h(X) = \alpha_o + \alpha_1 X + \ldots + \alpha_{n-1} X^{n-1}$. Tem-se $gr(h) = n-1 < n = gr(f)$ e $h(x) \neq 0$. Logo, h e f são primos entre si, isto é, 1 é m.d.c. de f,h. Por proposições anteriores, sabemos que existem $k, \ell \in K[X]$ tais que $1 = f(X)k(X) + h(X)\ell(X)$. Daqui que $1 = f(x)k(x) + h(x)\ell(x)$, aplicando o K-homomorfismo $K[X] \to L$ tal que $X \mapsto x$. Ora, $f(x) = 0$ por hipótese, logo $1 = h(x)\ell(x) = (\alpha_o + \alpha_1 x + \ldots + \alpha_{n-1} x^{n-1})\ell(x)$, mostrando que $\alpha_o + \alpha_1 x + \ldots + \alpha_{n-1} x^{n-1}$ admite inverso. O item (i) fica, assim, demonstrado.

Passemos ao ítem (ii). Consideremos o K-homomorfismo $\varphi: K[X] \to L$ tal que $\varphi(X) = x$. Como $K[x] = \{\alpha_o + \alpha_1 x + \ldots + \alpha_{n-1} x^{n-1} \mid \alpha_i \in K\}$ pela demonstração do ítem (i), resulta que a imagem de $K[X]$ por φ é $K[x]$. Por outro lado, se $g(X)$ é tal que $g(x) = \varphi(g(X)) = 0$, efetuamos a divisão de g por f: $g = f \cdot q + r$, com $r = 0$ ou $gr(r) < n$. Aplicando φ, vem $0 = g(x) = f(x)q(x) + r(x) = r(x)$. Se $r \neq 0$, $gr(r) < n$ e $r(x) = 0$, contradizendo a escolha de $f(X)$. Necessariamente, $r = 0$, mostrando que o núcleo de φ é o ideal gerado por $f(X)$.

Observação: Do ítem (i) e (ii) segue-se que $K[X]/(f(X))$ é, em verdade, um corpo. Logo, $f(X)$ é irredutível. Na verdade, isto pode ser verificado diretamente. Em todo caso, um po-

linômio f de menor grau possível tal que $f(x) = 0$, é automaticamente irredutível. Tal f é unicamente determinado a menos de uma constante $\neq 0$ e é conhecido como o polinômio mínimo de x.

Enfim, o ítem (iii). A estrutura de $K(x)$, como espaço vetorial sobre o corpo K, está explicado à pág. 90 . Vê-se, então, que os elementos $1, x, \ldots, x^{n-1}$ pelo menos geram $K(x)$ sobre K. Por outro lado, se houvesse uma relação de dependência linear $a_0 1 + a_1 x + \ldots + a_{n-1} x^{n-1} = 0$, com algum $a_i \neq 0$, teríamos uma contradição do fato que f é de menor grau possível tal que $f(x) = 0$. C.Q.D.

Uma extensão $L|K$ é dita simples se for gerada por um único elemento. Em outras palavras, se $L = K(x)$, para algum $x \in L$. Vimos que as extensões simples são exatamente aquelas que se podem obter como anéis quocientes de $K[X]$. É claro que toda extensão do tipo $K(x_1, \ldots, x_n)$ pode ser obtida como uma seqüência finita de extensões simples, a saber, $K(x_1, \ldots, x_n) = K(x_1)(x_2)\ldots(x_n)$. Poderíamos tentar algo mais atrevido: será que toda extensão do tipo $K(x_1, \ldots, x_n)$ é simples ?

Exemplo: Seja $K = \mathbb{Q}$ e $L = \mathbb{Q}(i, \sqrt{2}) \subset \mathbb{C}$. É fácil verificar que L é um espaço vetorial sobre K admitindo $\{1, i, \sqrt{2}, i\sqrt{2}\}$ como base. Consideremos o subcorpo $\mathbb{Q}(i+\sqrt{2})$ de $\mathbb{Q}(i, \sqrt{2})$. Calculando as potências $(i+\sqrt{2})^2$ e $(i+\sqrt{2})^4$, escrevemos sem dificuldade um polinômio $f(X) \in \mathbb{Q}[X]$ tal que $f(i+\sqrt{2}) = 0$, a saber, $f(X) = X^4 - 2X^2 + 9$. Para mostrar que f é irredutível, basta verificar que f não admite fatores $g(X) \in \mathbb{Q}[X]$ de grau 2 (uma vez que as raízes de $f(X)$ em $\mathbb{C}$ são $\pm(i+\sqrt{2})$ e $\pm(i-\sqrt{2})$, nenhuma delas pertencendo a $\mathbb{Q}$). Ora, supondo $X^4 - 2X^2 + 9 = (X^2 + a_1 X + a_0)(X^2 + b_1 X +$

$+ b_o$), resulta $a_1 = -b_1$, $a_o + a_1 b_1 + b_o = -2$, $a_o b_1 + a_1 b_o = 0$ e $a_o b_o = 9$. Da primeira e segunda equações, tem-se $a_1(b_o - a_o) = 0$, logo $a_1 = 0$ ou $b_o = a_o$. No primeiro caso, somos levados a procurar soluções racionais do sistema $a_o + b_o = 2$, $a_o b_o = 9$, que são inexistentes como se verifica. No segundo caso, obtemos a equação $a_1^2 = 8$, que também não admite solução racional.

Logo, $f = X^4 - 2X^2 + 9$ é irredutível sobre $\mathbb{Q}$. Pela proposição à pág. 105, $\mathbb{Q}(i + \sqrt{2})$ é um subespaço vetorial de $\mathbb{Q}(i , \sqrt{2})$ cuja dimensão é 4. Consequentemente, tem-se $\mathbb{Q}(i , \sqrt{2}) = \mathbb{Q}(i + \sqrt{2})$, isto é, $\mathbb{Q}(i , \sqrt{2})$ é, em última instância, gerada por um só elemento.

O exemplo acima não é acidental. Na verdade:

Proposição - Seja L um subcorpo de $\mathbb{C}$ tal que L tenha dimensão finita como espaço vetorial sobre $\mathbb{Q}$. Então, $L = \mathbb{Q}(x)$ para algum $x \in L$.

Demonstração: Como L é de dimensão finita sobre $\mathbb{Q}$, certamente tem-se $L = \mathbb{Q}(x_1 , \ldots , x_n)$ para certos $x_1 , \ldots , x_n \in L$ (leitor; por que?) Por indução sobre n-1, basta supor que $L = \mathbb{Q}(x,y)$, onde colocamos $y = x_2$, $x = x_1$. Sejam f e g os polinômios mínimos de x e y sobre $\mathbb{Q}$, respectivamente. Se $m = gr(f)$ e $n = gr(g)$, f admite m raízes distintas $a_1 = x, a_2 , \ldots , a_m$ e g admite n raízes distintas $b_1 = y, b_2 , \ldots , b_n$ (por que?). Para cada i $\ldots , m$ e para cada $j = 2 , \ldots , n$, a equação $a_i + \lambda b_j =$ $= a_1$ $= x + \lambda y$ admite uma única solução em $\mathbb{C}$, a saber, $\lambda = \frac{a_i}{y\ b}$. Segue-se que é possível escolher $\gamma \in \mathbb{Q}$ tal que $a_i + \gamma b_j \neq$

$\neq x + \gamma y$ para todo $i = 1, \ldots, m$ e para todo $j = 2, \ldots, n$. Ponhamos $c = x + \gamma y$. Propomo-nos a mostrar que $Q(x,y) = Q(c)$.

De qualquer maneira, tem-se, evidentemente $Q(c) \subset Q(x,y)$. Seja $h(X) = f(c - \gamma X) \in Q(c)[X]$ (precisamente, $f(c - \gamma X)$ é a imagem de $f(X)$ pelo $Q(c)$-isomorfismo de $Q(c)[X]$ em si mesmo tal que $x \mapsto c - \gamma X$). Ora, $h(y) = f(c - \gamma y) = f(x) = 0$. Logo, $X-y$ divide $h(X)$ exatamente no anel $Q(c)(y)[X]$ (isto é, o quociente tem coeficiente em $Q(c)(y)$). Analogamente, tem-se $g(y) = 0$ por hipótese, logo $X-y$ divide $g(X)$ exatamente em $Q(y)[X]$, logo, em $Q(c)(y)[X]$ por maior razão. Afirmamos que $X-y = \text{m.d.c.}\,(h(X), g(X))$ em $Q(c)(y)[X]$. Na verdade, $h(b_j) = f(c - \gamma b_j) \neq 0$ para $j = 2, \ldots, n$ pela escolha de γ. Também, $(X-y)^2$ não divide $g(X)$ porque y tem multiplicidade 1 como raiz de $g(X)$; logo $(X-y)^2$ não divide m.d.c. (h,g). Portanto, $X-y = \text{m.d.c.}\,(h,g)$ em $Q(c)(y)[X]$. Neste caso, h e g não podem ser primos entre si em $Q(c)[X]$ (por causa da relação $1 = h \cdot k + g \cdot \ell$ em $Q(c)[X]$, que é uma relação ainda válida em $Q(c)(y)[X]$). Necessariamente, $X-y = \text{m.d.c.}\,(h,g)$ em $Q(c)[X]$ também. Em particular, $X-y \in Q(c)[X]$, isto é, $y \in Q(c)$. Como $x = c - \gamma y$, resulta $x \in Q(c)$. Logo, $Q(x,y) \subset Q(c)$. C.Q.D.

APÊNDICE

Noções correntes do Curso

Os seguintes termos são "noções primitivas", isto é, serão empregados, sem definição, como blocos fundamentais para a construção do edifício matemático.

termo	sinonímia	símbolo
OBJETO		a,b,... A,B,...
IGUAL A	IDÊNTICO A, O MESMO QUE	a = b, A = B
CONJUNTO	CLASSE, COLEÇÃO	A,B,... , X,Y,Z
ELEMENTO DE	PERTENCE A	$\in$
(ELEMENTO	MEMBRO	a,b,...)
PAR ORDENADO		(a,b)

Intuitivamente, um par ordenado (a,b) é uma correspondência que associa ao conjunto {a,b}, primeiro o objeto a, em seguida o objeto b.

As seguintes são definições a partir dos termos primitivos acima.

O produto cartesiano de dois conjuntos E e F é o conjunto $E \times F = \{(a,b) \mid a \in E,\ b \in F\}$. Por exemplo, se $\mathbb{R}$ é o conjunto dos reais, $\mathbb{R} \times \mathbb{R}$ é o plano usual da geometria analítica clássica.

Dados dois conjuntos E, F, diz-se que E é um subconjunto de F, ou que E está contido em F (Notação: $E \subset F$) se todo elemento de E for elemento de F. Dizemos que $E = F$ se $E \subset F$ e $F \subset E$.

O conjunto vazio é denotado $\emptyset$. Propriedade fundamental: $\emptyset \subset E$ para todo conjunto E. Dados subconjuntos E, F de G, a reunião $E \cup F$, a interseção $E \cap F$ e o complementar $G \setminus E$ definem-se da maneira usual.

Dados dois conjuntos E, F, uma função (ou aplicação ou transformação) de E em F é um subconjunto do produto cartesiano $E \times F$ tal que, se $(x,y) \in F$ e $(x,z) \in f$ então $y = z$. O conjunto $D(f) = \{x \in E \mid (x,y) \in f \text{ para algum } y \in F\}$ é chamado o domínio de definição (ou, simplesmemte, o domínio) da função f.

Intuitivamente (e na prática), uma função de E em F é uma correspondência que associa a cada elemento de um certo subconjunto de E, um único elemento de F.
Notação: $f: E \to F$. Na prática, podemos considerar uma função $f \subset E \times F$ como função de $D(f)$ em F. Por isso, quase sempre quando dissermos que f é uma função de E em F, estaremos pressupondo que E já é o domínio de definição de f. Por exemplo, o conjunto $f = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid y = \frac{1}{x}\}$ é uma função de $\mathbb{R}$ em $\mathbb{R}$. O domínio de definição de f é, contudo $\mathbb{R} \setminus \{0\}$. Na linguagem corrente, dizemos que f está "definida fora da origem".

O conjunto F é chamado o contradomínio da função f. Um elemento $y \in F$ tal que existe $x \in E$ satisfazendo $(x,y) \in f$, é chamado uma imagem, mais precisamente, a imagem de x por meio de

f. Um mesmo $y \in F$ pode ser imagem de mais de um elemento de E. Notação: $y = f(x)$.

Noção mais geral do que a de uma função de um conjunto E em si mesmo, é a de relação: uma relação num conjunto E é um subconjunto R do produto cartesiano $E \times E$. Uma relação $R \subset E \times E$ é chamada uma relação de equivalência (em E) se satisfizer as seguintes condições:

(E.1) R é reflexiva, isto é, $(x,x) \in R$ para todo $x \in E$

(E.2) R é simétrica, isto é, se $(x,y) \in R$ então $(y,x) \in R$

(E.3) R é transitiva, isto é, se $(x,y) \in R$ e $(y,z) \in R$ então $(x,z) \in R$.

Se $(x,y) \in R$, na prática corrente escrevemos xRy. Outras notações para uma relação de equivalência: $\sim$, r , ρ , etc.

Dada uma relação de equivalência R em E, para cada $x \in E$ o conjunto $\bar{x}_R = \{y \in E \mid xRy\}$ é chamado a classe de equivalência de x determinada por R. Quando R estiver subentendida, a notação $\bar{x}$ é bastante. O conjunto $E/R = \{\bar{x}_R \mid x \in E\}$, cujos elementos são subconjuntos de E, é chamado o conjunto quociente de E pela relação R. É claro que E/R é uma partição de E, isto é, uma coleção de subconjuntos $\neq \emptyset$ de E cuja reunião é o E todo e tais que dois tais subconjuntos têm interseção vazia. Desta maneira, obtém-se facilmente uma "correspondência biunívoca" entre relações de equivalência em E e partições de E.

O subconjunto $\varpi_R \subset E \times (E/R)$ definido por: $(x,\bar{y}_R) \in \varpi_R$ se e só se $x \in \bar{y}_R$ (isto é, $\bar{x}_R = \bar{y}_R$), é uma aplicação de E em E/R,

chamada aplicação (quociente) canônica. Na prática, $\varphi_R(x) = \bar{x}_R$. Dois elementos $x,y \in E$ têm mesma imagem por meio de φ_R se e só se x e y pertencem à mesma classe de equivalência.

Outra relação importante é a de ordem: uma tal relação satisfaz as condições E.1 e E.2 de uma relação de equivalência e a condição de:

Antisimetria: se $(x,y) \in R$ e $(y,x) \in R$, então $x = y$.

Dado um conjunto E, uma operação em E é uma função de $E \times E$ em E. Sempre que possível, usaremos o símbolo $\cdot$ para uma operação e, em lugar de escrever $\cdot(a,b)$, que é desajeitado e pedante, escreveremos simplesmente $a \cdot b$ (ou mesmo ab, quando a operação é subentendida).

Uma operação $\cdot$ em E é:

1) Associativa se $(a\cdot b)\cdot c = a\cdot(b\cdot c)$, para todos $a,b,c \in E$

2) Comutativa se $a\cdot b = b\cdot a$ para todos $a,b \in E$

3) Cancelativa se $a\cdot b = a\cdot c$ implicar $b = c$, para todos $a,b,c \in E$.

Um conjunto munido de uma ou mais operações é chamado uma estrutura algébrica. Se $\langle E,\cdot\rangle$ designa uma estrutura algébrica a uma operação, dizemos que $\langle E,\cdot\rangle$ (ou E, ou $\cdot$) tem a propriedade do:

4) Elemento neutro se $a\cdot e = e\cdot a = a$ para algum $e \in E$ e para todo $a \in E$

5) Inverso se para todo $a \in E$ existir $a' \in E$ tal que $a\cdot a' = a'\cdot a = e$.

Observação: elementos neutros e inversos são únicos (no caso de inversos, deve-se supor que a operação é associativa).

Assim, um grupo G é uma estrutura algébrica e uma operação associativa com as propriedades do elemento neutro e do inverso.

Algo mais sobre funções

Uma função $f: E \to F$ (atenção: E = domínio de f) é injetora (ou uma injeção) se $f(x) = f(y)$ acarretar $x = y$, para todos $x, y \in E$; f é sobrejetora (ou uma sobrejeção) se todo elemento $y \in F$ for imagem de algum $x \in E$; f é bijetora (ou uma bijeção) se f for injetora e sobrejetora. Sinônimo para bijetora é biunívoca. Se $f: E \to F$ é uma bijeção, a aplicação $f^{-1}: F \to E$ definida por: $f^{-1}(y) = x$ se e só se $f(x) = y$, é chamada a função inversa de f. Se I_E, I_F designam as aplicações identidade de E, F respectivamente ($I_E(x) = x$, $I_F(y) = y$ para todos $x \in E$, $y \in F$), então tem-se evidentemente: $f \circ f^{-1} = I_F$ e $f^{-1} \circ f = I_E$, onde $\circ$ designa a composição usual de funções. Reciprocamente:

Exercício: Seja $f: E \to F$ uma função. Se existem funções $g: F \to E$ e $h: F \to E$ tais que

$$g \circ f = I_E \qquad f \circ h = I_F ,$$

então f é bijetora e tem-se $g = h = f^{-1}$.

EXERCÍCIOS

1. Mostre que os seguintes subconjuntos de $\mathbb{R} \times \mathbb{R}$ ($\mathbb{R}$ = reais) são funções de $\mathbb{R}$ em $\mathbb{R}$ e, em cada caso, determine o domínio de definição correspondente:

$$\{(x,y) \in \mathbb{R}\times\mathbb{R} \mid y = \frac{\operatorname{sen} x}{\cos x}\}$$

$$\{(x,y) \in \mathbb{R}\times\mathbb{R} \mid y = \log(x^2+1)\}$$

$$\{(x,y) \in \mathbb{R}\times\mathbb{R} \mid x = y\}$$

Verifique se as funções acima são injetoras em seus respectivos domínios de definição.

2. Seja C^0 o conjunto das funções reais no intervalo $[0,1]$ que são contínuas neste intervalo. Seja $C(0,1)$ o conjunto de todas as funções reais definidas em $[0,1]$. Considere a função $\varphi: C^0 \to C(0,1)$ definida pela condição:

$$(\varphi(f))(x) = \int_0^x f(t)dt.$$

Mostre que φ é injetora e descreva a imagem de φ, isto é, o conjunto $\{g \in C(0,1) \mid$ existe $f \in C^0$ tal que $\varphi(f) = g\}$.

3. Seja $f: E \to F$ uma sobrejeção. Mostre que

$$R_f = \{(x,y) \in E\times E \mid f(x) = f(y)\}$$

é uma relação de equivalência em E. Descreva as classes de equi-

valência de R_f. Mostre que existe uma única bijeção $g: E/R_f \to F$ tal que $g \circ \varphi = f$, onde φ é a aplicação quociente $E \to E/R_f$. Aplique no caso em que E = {habitantes da terra com nomes em letras latinas}, F = {alfabeto latino}, f = {(habitante, inicial do nome)}.

4. Seja $\mathbb{N}$ o conjunto dos naturais munido da operação $+$ e da relação $\leq$, conforme a axiomática dada no §1.1. Se $m,n \in \mathbb{N}$ são tais que $m \leq n$ e $m \neq n$, escrevemos $m < n$ como é usual.

   (a) Se 0 é o menor elemento de $\mathbb{N}$, prove que $n = n + 0$ para todo $n \in \mathbb{N}$.

   (b) Se 1 é o menor elemento de $\mathbb{N} \setminus \{0\}$, prove que $n < n+1$ para todo $n \in \mathbb{N}$.

   (c) (Princípio de indução finita). Sejam $m \in \mathbb{N}$ e $N' = \{r \in \mathbb{N} \mid r \geq m\}$. Seja S um subconjunto de N' tal que $m \in S$ e tal que para todo $n \in S$, tem-se $n+1 \in S$. Prove que $S = N'$.

   (Sugestão: por indução ao absurdo suponha $S \neq N'$ e tome um menor elemento, a, do complementar $N' \setminus S$. Use (b) para deduzir que $a-1 \in S$ onde $a-1$ designa a diferença entre a e 1).

   (c') (Caso particular de (c). Seja S um subconjunto de $\mathbb{N}$ tal que $0 \in S$ e tal que, para todo $n \in S$ tem-se $n+1 \in S$. Prove que $S = \mathbb{N}$.

   (d) Deduza de (b) e (c) que $\mathbb{N} = \{0, 1, 1+1, 1+1+1, \ldots\}$. (A notação $2 = 1+1$, $3 = 1+1+1$, $4 = 1+1+1+1$ etc. é também usual!.). Isto prova que $\mathbb{N}$ é infinito ? Justifique.

   (e) (Algoritmo euclideano de divisão). Dados inteiros $a, b \in \mathbb{Z}$, com $b > 0$, existem q e $r \in \mathbb{Z}$ tais que

$$a = b \cdot q + r \quad , \quad \text{com} \quad 0 \leq r < b.$$

(Sugestão: considere o conjunto $C = \{a-bx \geq 0 \mid x \in \mathbb{Z}\}$. Mostre que $C \neq \emptyset$ e seja $r = a-bq$, para algum $q \in \mathbb{Z}$, um menor elemento de C).

Como aplicação, determine todos os subgrupos de $\mathbb{Z}$.

5. Seja $n \in \mathbb{N}$.

(i) Prove, por indução, que

$$1 + 2 + \ldots + n = \frac{1}{2}\, n(n+1).$$

(ii) Prove, por indução, que

$$(1 + 2 + \ldots + n)^2 = 1^3 + 2^3 + \ldots + n^3$$

6. Sejam

$$\begin{aligned} u_1 &= 7 \\ u_2 &= u_1 \\ u_3 &= u_2 + 2u_1 \\ &\vdots \\ u_n &= u_{n-1} + 2u_{n-2} + \ldots + (n-1)u_1 \end{aligned}$$

Prove, por indução, que u_n é divisível por 7.

7. Prove, por indução, que se $n \in \mathbb{N}$, então

(i) $\sum_{r=1}^{n} r^2 = \frac{1}{6}\, n(n+1)(2n+1)$

(ii) $\sum_{r=1}^{n} \frac{1}{r(r+1)} = 1 - \frac{1}{n+1}$

(iii) $\sum_{r=1}^{n} (-1)^r \frac{r+1}{(2r+1)(2r+3)} = (-1)^n \frac{1}{4(2n+3)} - \frac{1}{12}$

(iv) $5^{2n} - 1$ é divisível por 24 se $n \geq 1$

(v) $\sum_{r=0}^{n-1} x^r = \frac{x^n - 1}{x-1}$ onde x é um número real qualquer.

(vi) $\sum_{r=1}^{n} rx^{r-1} = \frac{1 - (n+1)x^n + nx^{n+1}}{(x-1)^2}$ onde x é um número real qualquer.

8. Prove, por redução ao absurdo, que se $n \in \mathbb{N}$, então $3^{2n} + 5$ não é divisível por 8.

9. Prove, por redução ao absurdo, que existe um número infinito de números primos.

10. Se G é um grupo abeliano, com operação designada por $\cdot$, tem-se $(a \cdot b) = a^n \cdot b^n$ para todos $a, b \in G$ e para todo inteiro n. (Lembrete: por definição,

$$a^n = \begin{cases} a \cdot \ldots \cdot a \quad (n \text{ vezes}) & , \text{ se } n > 0 \\ e & , \text{ se } n = 0 \\ (a^{-1})^{-n} & , \text{ se } n < 0 \end{cases}).$$

11. Se G é um grupo (operação $\cdot$) tal que $(a \cdot b)^2 = a^2 \cdot b^2$ para todos $a, b \in G$, então G é abeliano.

12. Considere o conjunto G constituído pelas seguintes matrizes 2×2:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Verifique se G é um grupo mediante o produto usual de matrizes.

13. Verifique se os seguintes são grupos:

$G = \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a,b \in \mathbb{R}\}$; adição usual de matrizes

$H = \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a,b \in \mathbb{R}$ com $a^2+b^2 \neq 0\}$; produto usual de matrizes.

14. Seja G o conjunto das simetrias espaciais de um triângulo equilátero, munido da operação de composição de simetrias.

(i) Verifique que G é um grupo não comutativo.

(ii) Escreva a tabela de multiplicação de G.

(iii) Calcule a ordem de cada elemento de G.

15. Sejam α e β dois elementos de $\mathbb{Z}$. Seja $H = \{r\alpha + s\beta \mid r,s \in \mathbb{Z}\}$. Mostre que $(H,+)$ é um subgrupo de $(\mathbb{Z},+)$. Mostre que existem elementos $u,v \in \mathbb{Z}$ tais que $u\alpha+v\beta$ = Máximo Divisor Comum de α e β. Assim, em particular, se α e β são primos entre si, existem $u,v \in \mathbb{Z}$ tais que $u\alpha + v\beta = 1$.

16. Seja p um número inteiro ≥ 1. Seja $F_p = \{1,2,\ldots,p-1\}$. Sobre esse conjunto F_p defina a multiplicação módulo p, i.e. se $\alpha,\beta \in F_p$, $\alpha\cdot\beta$ = resto da divisão de $\alpha\beta$ por p.
Mostre que $(F_p,\cdot)$ é um grupo abeliano se e só se p é primo.

17. Seja $\mathbb{Z}_n = (\{0,1,\ldots,n-1\}$, adição módulo $n)$. Mostre que $\mathbb{Z}_n$ é um grupo abeliano.

18. Sejam $(G_1,\circ)$ e $(G_2,\circ)$ dois grupos. Seja $G_1 \times G_2 = \{(x,y) \mid x \in G_1, y \in G_2\}$ o produto cartesiano dos conjuntos G_1 e G_2. Defina sobre $G_1 \times G_2$ a operação seguinte:

$$(x_1,y_1) \square (x_2,y_2) = (x_1 \circ x_2 , y_1 \circ y_2)$$

(i) Mostre que $(G_1 \times G_2 , \square)$ é um grupo (chamado produto direto de G_1 e G_2), que nós escreveremos simplesmente $G_1 \times G_2$.

(ii) Mostre que $(G_1 \times G_2 , \square)$ é abeliano se e só se $(G_1,\circ)$ e $(G_2,\circ)$ são abelianos.

19. Seja $\varphi: G \to H$ um homomorfismo de grupos. Seja $g \in G$.

(i) Mostre que ordem de $\varphi(g) \leq$ ordem de g.

(i') Mais precisamente, mostre que a ordem de $\varphi(g)$ é um divisor da ordem de g.

(ii) Se φ é um isomorfismo, mostre que g e $\varphi(g)$ têm ordens iguais.

20. Seja G um grupo abeliano.

(i) Mostre que $\varphi: G \to G$ definido por $\varphi(x) = x^{-1}$ é um automorfismo de G.

(ii) Se existe em G um elemento x de ordem ≥ 2, então $Aut(G) \supsetneq \mathcal{I}(G) = \{\text{Identidade}\}$ onde $Aut(G)$ e $\mathcal{I}(G)$ designam respectivamente, o grupo dos automorfismos e o grupo dos automorfismos internos de G.

21. Se $s = (a_1 \ \ldots \ a_r)$ é um r-ciclo em S_n, então s tem ordem r.

22. Mostre que as transposições $(12), (13), \ldots, (1n)$ geram S_n.

23. Mostre que em S_3 todo elemento é um ciclo.

24. Mostre que, para todo ciclo $s \in S_4$ e para todo $r \geq 0$, s^r é um ciclo ou uma permutação cujos ciclos têm todos a mesma ordem.

25. Se $s_1 = (a_1 a_2 \ldots a_r) \in S_n$ e $s_2 = (a_r a_{r+1} \ldots a_n)$, calcule o produto $s_1^{-1} \cdot s_2^{-1} \cdot s_1 \cdot s_2$.

26. Considere a função $f = x_1x_2 + x_3x_4$ a quatro variáveis. Para cada permutação

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ a_1 & a_2 & a_3 & a_4 \end{pmatrix} \in S_4 ,$$

definimos $s(f) = x_{a_1}x_{a_2} + x_{a_3}x_{a_4}$. Mostre que o subconjunto $S(f)$ de S_4 cujos elementos deixam f invariante, isto é, tais que $s(f) = f$, constitui um subgrupo de S_4. Exibir os elementos de $S(f)$ explicitamente.

(Sugestão: pelo menos os seguintes elementos pertencem a $S(f)$: I , (12) , (34) , (12)(34) , (13)(24), (14)(23) , (1423) , (1324)).

27. Seja $g = x_1x_2 + x_3x_4$. Determine o subconjunto de S_4 cujos elementos deixam g invariante. Mostre que tal subconjunto é um subgrupo com quatro elementos e escreva sua tabela de multiplicação.

Observação: uma função f em n variáveis $x_1, \ldots, x_n$ é chamada simétrica se o subconjunto de S_n cujos elementos deixam f invariante coincidir com o próprio S_n.

28. Escreva a tabela de multiplicação do grupo S_3. Procure todos os subgrupos de S_3. Quais deles são normais em S_3 ? Qual é o centro de S_3 ? Mostre que $\mathcal{J}(S_3) \cong S_3$. Mostre que $\mathrm{Aut}(S_3) = \mathcal{J}(S_3)$.

29. (i) Mostre que S_3 e $\mathbb{Z}_6$ não são isomorfos.

(ii) Mostre que S_3 e $\mathbb{Z}_6$ são, a menos de isomorfismos, os únicos grupos de ordem 6.

30. Mostre que $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$ são, a menos de isomorfismos, os únicos grupos de ordem 4.

31. Mostre que se $\langle a \rangle$ é um grupo cíclico finito de ordem n então, para todo divisor positivo r de n, $\langle a \rangle$ admite exatamente um subgrupo com r elementos e tal subgrupo é cíclico.

32. Verifique (e justifique) se existe algum inteiro $n \geq 1$ tal que as raízes complexas da equação $x^n+1 = 0$ constituam um subgrupo do grupo multiplicativo dos complexos $\neq 0$.

33. Considere as permutações $s = (1234)(5678)$, $t = (1638)(5274)$ de S_8. Pede-se:

(i) Mostrar que s e t comutam (isto é, $s \cdot t = t \cdot s$) e determinar explicitamente o subgrupo de S_8 gerado por s e t.

(ii) Verificar se o subgrupo $\langle s,t \rangle$ de S_8 é ou não cíclico.

34. Seja G um grupo com 8 elementos, abeliano, não cíclico, satisfazendo a condição de que existe um elemento $a \in G$ tal que $\langle a \rangle$ tem ordem 4. Mostre que:

(i) G admite um elemento b tal que $b \notin \langle a \rangle$ e tal que $\langle b \rangle$ tem ordem 2.

(ii) G é isomorfo ao grupo $\mathbb{Z}_4 \times \mathbb{Z}_2$.

35. Escreva a tabela de multiplicação do grupo diédrico D_4. Procure todos os subgrupos de D_4. Quais deles são normais em D_4 ? Qual

é o centro de D_4 ? Mostre que $\mathcal{J}(D_4) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

36. Considere as matrizes

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} \cos \frac{2\pi}{n} & -\text{sen } \frac{2\pi}{n} \\ \text{sen } \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix}.$$

Mostre que A e B são ortogonais e que o subgrupo $G = \langle A,B \rangle$ de $\mathcal{O}(2, \mathbb{R})$ é isomorfo ao grupo diédrico D_n.

37. Procure a ordem de cada um dos elementos seguintes de S_4, e decida se são permutações pares ou ímpares

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$; (ii) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$; (iii) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$.

38. Sejam $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ $b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$. Determine (i) ab; (ii) ba; (iii) a^2b; (iv) $(ab)^2$; (v) aba^3.

39. Escreva as permutações seguintes como produtos de transposições, e determine se elas são pares ou ímpares:

(i) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

(ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix}$

(iii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$

(iv) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 5 & 1 & 2 \end{pmatrix}$

40. Mostre que o grupos dos números racionais com a adição não admite um conjunto finito de geradores.

41. Determine se os seguintes são subanéis:

(i) $A = \{m + n\sqrt{5} \mid m,n \in \mathbb{Z}\}$, de $\langle \mathbb{R},+,\cdot \rangle$

(ii) $A = \{m + n\sqrt[3]{2} \mid m,n \in \mathbb{Z}\}$, de $\langle \mathbb{R},+,\cdot \rangle$

(iii) $A = \{m + ni \mid m,n \in \mathbb{Z},\ i^2 = -1\}$, de $\langle \mathbb{C},+,\cdot \rangle$

(iv) $A = \{m/n \in \mathbb{Q} \mid n \not\equiv 0 \mod 7\}$, de $\langle \mathbb{Q},+,\cdot \rangle$.

42. Se A é um anel, mostre que o subconjunto $U(A) \subset A$ constituído pelos elementos que admitem inverso multiplicativo é um grupo (abeliano). Em cada um dos aneis seguintes, descreva $U(A)$: $\mathbb{Z}$; $\mathbb{Z}/m\mathbb{Z}$ $(m \in \mathbb{Z})$; $K[X]$ (K um corpo); $\mathbb{Z}[\frac{1}{2}] = \{m/2^n \mid m,n \in \mathbb{Z}, n \geq 0\}$; $\mathbb{M}_n(K) = \{$matrizes $n\times n$ com coeficientes num corpo K, com a soma e o produto usual de matrizes$\}$.

43. Sejam A , B anéis (comutativos com identidade).

(i) Introduza no produto cartesiano $A \times B$ uma estrutura natural de anel tal que as aplicações "projeções" $A\times B \to A$ e $A\times B \to B$, definidas por $(a,b) \to a$ e $(a,b) \to b$, respectivamente, sejam homomorfismos.

(ii) Se $p,q \in \mathbb{Z}$ são primos, mostre que os anéis $\mathbb{Z}/(pq)\mathbb{Z}$ e $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ (vide (i)) são isomorfos.

44. (i) Se K é um corpo finito, tem-se $\prod_{a\in K^*} a = -1$.
Sugestão: K^* é um grupo.

(ii) (Teorema de Wilson) Se $p \in \mathbb{Z}$ é um primo, tem-se $(p-2)! \equiv 1 \pmod p$.

45. Mostre que o subconjunto $\mathbb{Z}(X) = \{\Sigma\, a_i X^i \in \mathbb{Q}[X] \mid a_i \in \mathbb{Z}\}$ é um subanel de $\mathbb{Q}[X]$.

(i) Determine $U(\mathbb{Z}[X])$ (vide Ex. 42).

(ii) Mostre que o ideal (p,X) de $\mathbb{Z}[X]$ é máximo onde p é um primo, e que o ideal (X) é primo, mas não máximo.

(iii) Determine um subanel de $\mathbb{Q}$ isomorfo ao anel quociente $\mathbb{Z}[X]/(3X+1)$.

46. Seja G o conjunto das funções de $\mathbb{C}$ em $\mathbb{C}$ da forma $z \to \frac{az+b}{cz+d}$, com $a,b,c,d \in \mathbb{R}$ e $ad-bc \neq 0$. (i) Mostre que G, munido da composição de funções, é um grupo; (ii) Calcule os elementos de ordem 2 de G; (iii) Quais, dentre os elementos encontrados em (ii), pertencem ao subgrupo das transformações lineares fracionárias (vide Proposição à pag. 56) ?

47. Seja G o conjunto das funções $f_{a,b}: x \to ax+b$ $(a \neq 0)$, de $\mathbb{R}$ em $\mathbb{R}$.

(i) Mostre que G é um grupo com respeito à composição de funções

(ii) Mostre que o subconjunto de G constituido pelas funções $f_{1,b}$ é um subgrupo normal de G. Deduza que G não pode ser gerado por um conjunto finito de elementos.

48. Considere a expressão polinomial $f = f(X_1, X_2, X_3, X_4) = 2X_1^2X_2^2 + 2X_1^2X_3^2 + 2X_1^2X_4^2 + 2X_2^2X_3^2 + 2X_2^2X_4^2 + 2X_3^2X_4^2 + X_1X_2X_3X_4 - 5$. Determine todas as permutações de 4 símbolos que mantêm f invariante.

49. Mostre que as permutações de 3 símbolos que mantêm invariante o polinômio $f = X_1^2X_2 - X_1X_2^2 + X_1^2X_3 - X_1X_3^2 + X_2^2X_3 + X_2X_3^2 + 3X_1X_2X_3 - 5$ formam um subgrupo de ordem 2 de S_3.

50. Seja G um subgrupo finito do grupo multiplicativo dos números complexos $\neq 0$. Mostre que todo elemento de G tem norma 1 (N.B. A norma de um complexo $z = x+iy$ é $|z| = +\sqrt{x^2+y^2}$).

51. Se m,n são inteiros, determine o número de homomorfismos distintos $\langle \mathbb{Z}/m\mathbb{Z}, + \rangle \to \langle \mathbb{Z}/n\mathbb{Z}, + \rangle$ em termos de m e n.

52. Determine o grupo $U(\mathbb{Z}/m\mathbb{Z})$ dos elementos inversíveis do anel $\mathbb{Z}/m\mathbb{Z}$, $m \in \mathbb{Z}$. Deduza o <u>teorema de Euler</u>: se $\phi(m)$ é o número dos inteiros positivos menores que m e primos com m, então $a^{\phi(m)} \equiv 1 \mod m$ para todo inteiro a primo com m. (O caso particular do teorema de Euler em que m é primo é conhecido como <u>pequeno teorema de Fermat</u>).

53. Mostre que a função $f: \mathbb{Z} \to U(\mathbb{Z}/17\mathbb{Z})$, definida por $f(n) =$ classe de $3^n \mod 17$, induz um isomorfismo de $\langle \mathbb{Z}/16\mathbb{Z}, + \rangle$ sobre $U(\mathbb{Z}/17\mathbb{Z})$.

54. Mostre que a ordem de um elemento $\sigma \in S_n$ é o mínimo múltiplo comum das ordens dos ciclos de σ (vide Proposição à pag. 18) (Sugestão: ciclos disjuntos comutam).

55. Se $\sigma \in S_n$ é escrita como produto de ciclos e se $\tau \in S_n$, determine uma receita para escrever $\tau\sigma\tau^{-1}$ como produto de ciclos (Sugestão: se $\sigma = \ldots(\lambda_{i1}\ \lambda_{i2} \ldots \lambda_{ik_i})\ldots$, o que é $\tau(\lambda_{ij})$?).

56. Mostre que o conjunto das matrizes

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} w & 0 \\ 0 & w^2 \end{pmatrix}, \begin{pmatrix} w^2 & 0 \\ 0 & w \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & w^2 \\ w & 0 \end{pmatrix}, \begin{pmatrix} 0 & w \\ w^2 & 0 \end{pmatrix},$$

onde $w^3 = 1$, $w \neq 1$ $(w \in \mathbb{C})$ é um grupo com respeito à multiplicação usual de matrizes. Mostre que tal grupo é isomorfo ao grupo das simetrias espaciais do triângulo equilátero.

57. Se G é um grupo finito tal que todo elemento de G, exceto o neutro, tem ordem 2, então G é isomorfo a um produto direto $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \ldots \times \mathbb{Z}/2\mathbb{Z}$ (vide exercício 18 para a definição de produto direto).

58. A menos de isomorfismos, os únicos grupos de ordem 6 são o grupo cíclico de ordem 6 e o das simetrias espaciais do triângulo equilátero (Sugestão: use o exercício 57 e calcule com elementos do grupo)

59. Existe um grupo G de ordem 8 definido por dois geradores a,b satisfazendo as relações

$$a^4 = e \quad , \quad a^2 = b^2 \quad , \quad ba = a^3b.$$

(Sugestão: considere o subgrupo de $GL(n,\mathbb{C})$ gerado pelas matrizes $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ e $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, onde $i^2 = -1$). Escreva a tabela deste grupo.

60. Mostre que $U(\mathbb{Z}/21\mathbb{Z}) \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.