UFF/MATEMÁTICA
NOTAS DE CURSO: TEORIA DOS GRUPOS

Resumo

Estas são notas de um curso de introdução à Teoria dos Grupos, visando o estudo da Teoria de Galois de equações algébricas. O objetivo aqui é complementar o assunto visto em sala de aula. Fiz um esforço em apresentar demonstrações simples e diretas dos vários resultados conhecidos.

Encontram-se em estágio rudimentar: há afirmações sem prova (receba como um convite para pensar a respeito), não há muitos exercícios, o detalhamento não está balanceado. Quanto a erros e equívocos, posso prometer duas coisas: existem; não os cometi propositadamente dessa vez.

Mea culpa a parte, espero que o texto seja útil. Quaisquer observações, considerações, recomendações, sugestões, correções (tradução: estou realmente pedindo ajuda!) são muito bem-vindas. Para contribuir ou, com sorte, encontrar uma versão mais recente:

www.professores.uff.br/nmedeiros

07 dezembro 2016
N.

≈

Sumário

1 Conceitos básicos

Um *grupo* G é um conjunto com uma operação "$\cdot$", satisfazendo três propriedades:

1. *Associatividade*:
$$(a \cdot b) \cdot c = a \cdot (b \cdot c), \qquad \text{para quaisquer } a, b, c \in G;$$
2. *Elemento neutro*: existe um elemento em G, denotado simplesmente por "1", que satisfaz:
$$1 \cdot g = g \cdot 1 = g, \qquad \text{para todo } g \in G;$$
3. *Inversos*: dado $g \in G$, existe $h \in G$ tal que
$$g \cdot h = h \cdot g = 1.$$

O elemento neutro de G é único. Dado $g \in G$, o inverso de g é único, e é denotado sugestivamente por g^{-1}. Da associatividade, o elemento

$$g^n := \underbrace{g \cdot g \cdots g}_{(n \text{ vezes})}$$

fica bem definido. Se $n < 0$, tomamos $g^n := (g^{-1})^{-n}$ e, para $n = 0$, $g^0 := 1$, para todo $g \in G$. Com estas convenções,

$$g^n \cdot g^m = g^{n+m} \qquad \text{para todos } n, m \in \mathbb{Z} \text{ e todo } g \in G. \tag{1.1}$$

Exemplo 1.1.

(a) Os números inteiros $\mathbb{Z}$ com a operação de soma; ou ainda $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ também com a operação de soma.

(b) O anel $\mathbb{Z}_n$ das classes residuais módulo n, com a operação de soma.

(c) Os elementos não nulos em $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, com a operação de multiplicação.

(d) Mais geralmente, os elementos invertíveis A^* de um anel A, com a operação de produto do anel.

(e) O conjunto S^1 dos números complexos z com módulo $|z| = 1$, com a operação de produto.

(f) (O *grupo linear geral*). Seja K um corpo (por exemplo, $K = \mathbb{C}$, $\mathbb{R}$ ou $\mathbb{Q}$). Denotamos por $\mathrm{GL}_n(K)$ o conjunto das matrizes quadradas de ordem n invertíveis, com entradas em K. Então, com o produto usual de matrizes, $\mathrm{GL}_n(K)$ é um grupo. O elemento neutro é a matriz identidade.

(g) As transformações lineares invertíveis de um espaço vetorial V em si mesmo, com a operação de composição.

(h) Se C é um conjunto qualquer, então o conjunto das bijeções $C \to C$, denotadas por $\mathrm{Perm}\, C$, formam, com a operação de composição, um grupo, chamado o *grupo das permutações* de C. A notação para conjuntos finitos é especial: indicamos $\mathrm{Perm}\{1, 2, \ldots, n\}$ abreviadamente por S_n, que é chamado o *grupo simétrico*.

(i) O conjunto das bijeções do plano em si mesmo que preservam distâncias, com a operação de composição, é o grupo das *isometrias* do plano. É um fato notável que toda isometria do plano possa ser escrita como composição de translações, rotações e reflexões. Veja [M. Artin, *Algebra*, Cap. 5].

(j) Se $X \subset \mathbb{R}^2$ é um subconjunto não vazio, então o conjunto das isometrias do plano que preservam X, isto é,

$$\mathrm{Sim}(X) := \{\sigma \text{ é isometria} \mid \sigma(X) = X\}$$

é o grupo das *simetrias de* X. O grupo de simetrias de um polígono regular P de n lados é denominado o *grupo diedral* D_n.

O grupo D_n possui exatamente $2n$ elementos: n deles são rotações de ângulos $2k\pi/n$ ($k = 0, \ldots, n-1$) em torno do baricentro b de P; os outros n elementos são as reflexões com respeito as n retas que ligam b ao conjunto formado pelos vértices e pontos médios dos lados de P (note que há $2n$ desses pontos).

(k) (Quatérnios) O conjunto $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ de 8 elementos com a operação multiplicativa definida pelas relações

$$i^2 = j^2 = k^2 = ijk = -1$$

forma um grupo, conhecido como o grupo dos *quatérnios*, e surge em diversos contextos, como por exemplo na classificação de álgebras. Estas relações são suficientes para deduzir todos os produtos possíveis no grupo. Por exemplo, $i^{-1} = -i, k = ij = -ji$, etc.

Assim, em cada uma dessas situações, temos um conjunto com uma operação que satisfaz as três propriedades exigidas para um grupo. Independentemente do caso, escrevemos a operação como "$\cdot$" e a chamamos simplesmente de "produto". Qualquer teorema ou conceito que apresentarmos, se não impusermos restrições, se aplica a qualquer um dos exemplos apresentados.

É tradicional utilizar uma notação especial para o caso dos grupos nos quais a operação é *comutativa*, isto é $gh = hg$ para quaisquer g, h. Tais grupos são chamados *abelianos*, ou *aditivos*. A simbologia com respeito à operação é convencionada assim: trocamos "$\cdot$" por "$+$", g^{-1} por $-g$; o elemento neutro é denotado por 0; e, finalmente, substituímos g^n por ng. Na lista acima, os grupos em (a), (b) e (d) são exemplos de grupos abelianos.

A *ordem* de um grupo G é simplesmente a sua cardinalidade e a denotamos por $|G|$. Por exemplo, os grupos S_n e $\mathbb{Z}_n$ são finitos, e suas ordens são $n!$ e n, respectivamente.

2 Subgrupos

Dado um grupo G, um subconjunto $H \subset G$ é um *subgrupo* de G se é não-vazio e se é fechado com respeito a inversos e produtos de seus elementos, isto é, se

$$h^{-1} \in H \quad \text{e} \quad h \cdot h' \in H \qquad \text{para todo } h, h' \in H.$$

Em particular, $1 \in H$. Notação: $H < G$. Note que, herdando o produto de G, o subgrupo H é também um grupo.

Exemplo 2.1.

(a) Para qualquer grupo G, os subconjuntos $\{1\}$ e G são subgrupos, apelidados *triviais*.

(b) $\mathbb{Z}$ é um subgrupo do grupo aditivo $\mathbb{Q}$;

(c) S^1 é um subgrupo do grupo multiplicativo $\mathbb{C}^*$;

(d) O *grupo linear especial*

$$\mathrm{SL}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) \mid \det M = 1\}$$

formado pelas matrizes de determinante 1, é um subgrupo de $\mathrm{GL}_n(\mathbb{R})$;

(e) O *grupo das matrizes ortogonais*, isto é, aquelas que preservam o produto interno canônico em espaços euclidianos,

$$O_n(R) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \langle Au, Av\rangle = \langle u, v\rangle, \quad \forall u, v \in \mathbb{R}^n\}$$

é um subgrupo de $\mathrm{GL}_n(\mathbb{R})$. Como toda transformação ortogonal também preserva distâncias, $O_n(\mathbb{R})$ é também um subgrupo do grupo das isometrias de $\mathbb{R}^n$.

(f) $\mathbb{Z}_n$ **não é** um subgrupo aditivo de $\mathbb{Z}$.

(g) As translações e as rotações (em torno de um centro fixado) são subgrupos das isometrias do plano. Já o conjunto das reflexões não: a composição de duas reflexões com respeito a retas distintas não é uma reflexão, já que a composta de duas reflexões preserva orientação.

Exercício 2.2. Mostre que a interseção de dois subgrupos de um grupo G é ainda um subgrupo de G. De modo geral, prove que a interseção arbitrária de subgrupos é um subgrupo.

Dado um subconjunto S de um grupo G, definimos o subgrupo *gerado por* S, denotado por $\langle S\rangle$, como o menor subgrupo de G que contém S. Formalmente: $\langle S\rangle$ é, por definição, a interseção de todos os subgrupos de G que contém S.

De maneira equivalente, o subgrupo gerado por S é o conjunto de todos os produtos finitos de elementos de S ou seus inversos:

$$\langle S\rangle = \{s_1 s_2 \cdots s_n \mid n \in \mathbb{N},\ s_i \in S \cup S^{-1}\}.$$

No caso particular em que $S = \{g\}$ é um conjunto unitário, temos

$$\langle\{g\}\rangle = \{g^n \mid n \in \mathbb{Z}\}$$

que denotamos simplesmente por $\langle g\rangle$. Pode acontecer que este subgrupo seja finito, uma vez que pode ocorrer $g^i = g^j$ mesmo que $i \neq j$.

A *ordem* de g, denotada $o(g)$, é definida como o menor inteiro positivo n tal que $g^n = 1$, caso tal inteiro exista; caso contrário, definimos $o(g) := \infty$. É um fato básico que este número coincide com a cardinalidade de $\langle g\rangle$, como provaremos a seguir.

Proposição 2.3. $o(g) = |\langle g \rangle|$.

Demonstração. Suponha que g tem ordem finita n. Dado um inteiro a, perfazemos a divisão euclidiana por n, obtendo $a = qn + r$ com $0 \leq r \leq n-1$. Daí $g^a = (g^n)^q \cdot g^r = g^r$, donde concluímos

$$\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}.$$

Caso a ordem seja infinita, então $g^i \neq g^j$ sempre que $i \neq j$: caso contrário (digamos $j > i$), tem-se $g^{j-i} = 1$, contradição. Logo $\langle g \rangle$ é infinito neste caso. □

Exemplo 2.4.

(a) É claro que se G é um grupo finito, então todo elemento de G tem ordem finita. A recíproca não vale: todo elemento do grupo infinito

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots$$

possui ordem 2 (veja seção 7).

(b) Todo inteiro não nulo possui ordem infinita em $\mathbb{Z}$.

(c) O grupo multiplicativo $\mathrm{GL}_2(\mathbb{R})$ das matrizes 2×2 invertíveis com entradas reais é infinito; entretanto, toda matriz idempotente, isto é, as matrizes A para as quais existe n tal que $A^n = I$, possui ordem finita (você é capaz de encontrar alguma?).

(d) Pode ocorrer que g e h possuam ordem finita mas gh seja um elemento de ordem infinita! Procure por exemplos no grupo $\mathrm{GL}_2(\mathbb{R})$ do item anterior.

3 Classes laterais

A operação de um grupo G diz respeito a seus elementos. Mas naturalmente podemos estendê-la para subconjuntos: dados $A, B \subseteq G$, definimos

$$AB = \{a \cdot b \mid a \in A,\ b \in B\} \qquad \text{e} \qquad A^{-1} = \{a^{-1} \mid a \in A\}.$$

Note que

$$A(BC) = (AB)C \qquad \text{e} \qquad (AB)^{-1} = B^{-1}A^{-1}$$

uma vez que estas propriedades são válidas para elementos. Quando um dos conjuntos é unitário, abreviamos $\{a\}B$ por aB.

Exercício 3.1. Dados $A, B \subseteq G$, então $xA = yB$ se e somente se $y^{-1}xA = B$.

Produtos de conjuntos são muito úteis e serão utilizados frequentemente a seguir. De partida, temos uma caracterização bastante simpática para subgrupos:

Exercício 3.2. Se $H \subseteq G$ é não-vazio, então

$$H < G \iff HH = H \text{ e } H^{-1} = H.$$

Exercício 3.3. Se H é um subgrupo de G, então: $xH = H \iff x \in H \iff Hx = H$.

Seja H um subgrupo de um grupo G. Associamos a H duas relações de equivalência. A primeira delas:

$$x \sim_e y \quad \text{se} \quad xH = yH,$$

para $x, y \in G$. Assim, $x \sim_e y$ se e somente se $x \in yH$ ou ainda se e somente se $y^{-1}x \in H$. O conjuntos dos elementos que são equivalentes a x é portanto xH, e é denominado a *classe lateral à esquerda* de x. A segunda relação de equivalência é definida por

$$x \sim_d y \quad \text{se} \quad Hx = Hy.$$

Analogamente, o conjunto dos elementos equivalentes a x sob esta relação é Hx, e é chamado *classe lateral à direita de* x. Com frequência mencionamos apenas "classe lateral", omitindo "à esquerda" ou "à direita" sempre que o contexto o permitir.

Em geral, as classes laterais à esquerda e à direita de um elemento $g \in G$ não coincidem. Por exemplo, tome H como sendo o subgrupo gerado por uma reflexão qualquer em D_3 e considere as classes laterais de uma rotação $r \neq 1$; então $rH \neq Hr$. Se G é abeliano, então $gH = Hg$ para todo subgrupo H e todo elemento $x \in G$ (porém esta propriedade não caracteriza um grupo abeliano; veja o exemplo dos quatérnios). Portanto, os conjuntos quocientes

$$G/\sim_e := \{\text{classes laterais à esquerda de } H \text{ em } G\}$$

e

$$G/\sim_d := \{\text{classes laterais à direita de } H \text{ em } G\}$$

não coincidem em geral. Ainda assim, a aplicação

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

está bem definida e define uma bijeção entre estes dois conjuntos. Isto nos permite definir o *índice de H em G*, que denotamos por $(G : H)$, como sendo a cardinalidade de qualquer um dos conjuntos quocientes acima do conjunto acima. O índice de um subgrupo pode ser finito ou infinito.

Por outro lado, dado $g \in G$, a aplicação

$$\begin{aligned} H &\to gH \\ h &\mapsto gh \end{aligned}$$

define uma bijeção; consequentemente, todas as classes laterais possuem a mesma cardinalidade, igual a ordem de H. Como G é a união disjunta de suas $(G : H)$ classes laterais (à esquerda, digamos), fica demonstrado então o teorema a seguir.

Teorema 3.4. *Seja G um grupo finito. Então*

$$|G| = |H|\,(G : H).$$

Corolário 3.5. (Lagrange) *Se G é um grupo finito e H é um subgrupo de G, então a ordem de H divide a ordem de G.*

O corolário acima foi provado por Lagrange quando G é um grupo simétrico. Foi Jordan quem, percebendo na prova de Lagrange os elementos essenciais, provou o Teorema 3.4.

Como ilustração, em um grupo de ordem 20 podemos ter subgrupos apenas de ordens $1, 2, 4, 5, 10$ e 20. Nada nos garante que existam subgrupos com cada uma dessas ordens. Por exemplo, o grupo A_4 de permutações pares tem ordem 60 mas não possui nenhum subgrupo de ordem 30 (veja Seção 8).

4 Subgrupos normais

Seja H um subgrupo de um grupo G. É relativamente rara a situação em que as classes laterais à esquerda e à direita de H em G coincidam. Os casos em isto acontece são importantes e os estudamos agora.

Dizemos que o subgrupo H é *normal* em G, o que indicamos por $H \lhd G$, se, para todo elemento de G, suas classes laterais à esquerda e à direita coincidem; mais precisamente, se $Hg = gH$ para todo $g \in G$.

Este conceito pode ser reformulado de outras maneiras. De fato, são equivalentes:

Proposição 4.1. (a) *H é normal em G;*

(b) *$gHg^{-1} = H$, para todo $g \in G$;*

(c) *$gHg^{-1} \subseteq H$, para todo $g \in G$.*

Demonstração. Mostremos (c) $\implies$ (b). Seja g um elemento de G. Aplicando (c) para g^{-1} no lugar de g, obtemos $g^{-1}Hg \subseteq H$ e daí segue $H \subseteq gHg^{-1}$. A outra inclusão decorre diretamente de (c) e portanto vale a igualdade em (b). □

Na proposição acima, a formulação mais útil sem dúvida é a do item (c): nos diz que um subgrupo é normal se e somente se é fechado por conjugações.

Seja H um subgrupo normal de um grupo G. Então os conjuntos quocientes $G/\sim_e$ e $G/\sim_d$ são iguais; denotemo-los por G/H. Se xH e yH são classes laterais, então temos as igualdades (como conjuntos)

$$(xH)(yH) = (xH)(Hy) = x(Hy) = (xy)H$$

visto que H é normal em G. Isto nos leva a *definir* uma operação em G/H, a saber,

$$(xH) \cdot (yH) := (xy)H.$$

Esta operação faz do conjunto G/H um grupo. Com efeito, esta operação herda a associatividade do grupo G; o elemento neutro é a classe $1H = H$; e o inverso da classe xH é a classe $x^{-1}H$. O grupo $(G/H, \cdot)$ é denominado o *grupo quociente* de G por H.

Exemplo 4.2.

1. Dado um grupo G, o *centro* de G, denotado por $Z(G)$, é o conjunto dos elementos de G que comutam com todos os outros, ou seja,

   $$Z(G) = \{x \in G \mid gx = xg, \text{ para todo } g \in G\}.$$

   O centro de G é sempre um subgrupo normal. Note que G é abeliano se e somente se $G = Z(G)$.

2. O subgrupo dos comutadores de G é definido por

   $$G' := \langle \{xyx^{-1}y^{-1} \mid x, y \in G\} \rangle$$

   ou seja, G' é o menor subgrupo de G que contém todos os comutadores $[x, y] := xyx^{-1}y^{-1}$. Este é um subgrupo normal de G e, além disso, o quociente G/G' é abeliano. Note que G é abeliano se e somente se $G' = \{1\}$.

5 Produtos de subgrupos

Sejam A, B, subgrupos de um grupo G. Perguntamos: o produto

$$AB = \{ab \mid a \in A, b \in B\}$$

é um subgrupo de G? Em geral, a resposta é não (busque um contra-exemplo em S_3: tome duas transposições distintas). Ainda assim, podemos determinar a ordem do *conjunto* AB:

Proposição 5.1. *Sejam A, B subgrupos finitos de um grupo G. Então*

$$|AB| = \frac{|A|\,|B|}{|A \cap B|}. \tag{5.1}$$

Demonstração: Considere a função $A \times B \to AB$ dada por $(a, b) \mapsto ab$. Dados $a \in A$ e $b \in B$, tudo que precisamos fazer é mostrar que a imagem inversa de ab possui exatamente $|A \cap B|$ elementos, pois segue daí que

$$|A \times B| = |A \cap B|\,|AB|\,.$$

Para tal fim, escrevemos $A \cap B = \{g_1, \ldots, g_n\}$ e definimos $a_i = ag_i$ e $b_i = g_i^{-1}b$. Então $a_i b_i = ab$, para cada i. Por outro lado, se $x \in A$ e $y \in B$ são tais que $xy = ab$, então $a^{-1}x = by^{-1} \in A \cap B$ e logo $x = a_i$ e $y = b_i$ para algum i. □

Felizmente não é difícil caracterizar as situações em que o produto de subgrupos ainda é um subgrupo.

Proposição 5.2. *AB é um subgrupo de G se e somente se $AB = BA$.*

Demonstração: Suponha que AB é um subgrupo de G. Então, pelo Exercício 3.2,

$$BA = (A^{-1}B^{-1})^{-1} = (AB)^{-1} = AB$$

como desejado. Reciprocamente, se $AB = BA$, então

$$(AB)(AB) = A(BA)B = A(AB)B = (AA)(BB) = AB \qquad \text{e}$$

$$(AB)^{-1} = B^{-1}A^{-1} = BA = AB$$

e daí decorre AB é um subgrupo, mais uma vez pelo Exercício 3.2. □

Exercício 5.3. Mostre que:

(a) Se A é normal em G, então AB é um subgrupo de G;

(b) Se A e B são normais em G, então AB é normal de G.

6 O teorema dos homomorfismos

Uma aplicação $f\colon G \to H$ entre dois grupos é um *homomorfismo*[1] se

$$f(x \cdot y) = f(x) \cdot f(y) \qquad \forall x, y \in G.$$

Note que o produto do lado direito é feito em G, enquanto o do lado esquerdo é realizado em H.

Decorre da definição que

$$f(1_G) = 1_H \qquad \text{e} \qquad f(x^{-1}) = f(x)^{-1}.$$

Sejam A e B subconjuntos de G e H, respectivamente. A *imagem* de A por f é definida da maneira usual

$$f(A) = \{f(g) \mid g \in G\}$$

Em contrapartida, a *imagem inversa* de B por f é o subconjunto dos elementos de G que são levados em B:

$$f^{-1}(B) = \{g \in G \mid f(g) \in B\}.$$

Proposição 6.1. *Se A e B são subgrupos de G e H, então $f(A)$ é um subgrupo de H e $f^{-1}(B)$ é um subgrupo de G.*

Demonstração: Dados x, y em $f(A)$, tome a, b em A tais que $x = f(a)$ e $y = f(b)$. Então $xy = f(a)f(b) = f(ab)$ e $x^{-1} = f(a)^{-1} = f(a^{-1})$. Como A é um subgrupo, temos ab e a^{-1} em A e logo xy e x^{-1} estão em $f(A)$.

Tome agora a, b em $f^{-1}(B)$ e sejam $x = f(a), y = f(b)$, que estão no subgrupo B. Logo $xy = f(ab)$ e $x^{-1} = f(a^{-1})$ estão em B, donde concluímos que ab e a^{-1} estão $f^{-1}(B)$, o que termina a prova. □

Um *isomorfismo* é, por definição, um homomorfismo bijetor. Um fato importante:

Exercício 6.2. Se $f\colon G \to H$ é um isomorfismo, se e somente se a aplicação inversa $\varphi = f^{-1}\colon H \to G$ também é um homomorfismo de grupos.

Observe que um homomorfismo injetor induz um isomorfismo de G sobre sua imagem $f(G)$. Por este motivo, um homomorfismo injetor é por vezes chamado um *mergulho*.

Como usual, o *núcleo* N de um homomorfismo $f\colon G \to H$ é definido como o conjunto dos elementos de G que são levados no elemento neutro de H, ou seja,

$$\text{núcleo}\, f = \{g \in G \mid f(g) = 1_H\}.$$

O núcleo de um homomorfismo é um subgrupo de G. Mais ainda, se n pertence ao núcleo de f e $g \in G$ é arbitrário,

$$f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(gg^{-1}) = 1_H$$

ou seja, $gNg^{-1} \subseteq N$. Portanto, o núcleo é um subgrupo normal de G.

[1] Por vezes uso no texto a palavra *mapa* no lugar de 'homomorfismo'. Trata-se de uma terminologia universal para designar funções que preservam as propriedades da categoria envolvida; assim, em topologia, os mapas são as funções contínuas, em Álgebra Linear são as transformações lineares, etc.

E vale a recíproca: todo subgrupo normal é de fato o núcleo de algum homomorfismo: dado N normal em G, temos a *projeção canônica* $\pi\colon G \to G/N$, dada por $g \mapsto gN$, um mapa sobrejetor cujo núcleo é exatamente N.

Dois elementos x, y em G definem a mesma classe lateral com respeito ao núcleo se e somente se possuem a mesma imagem pelo homomorfismo f:

$$xN = yN \iff y^{-1}x \in N \iff f(x) = f(y).$$

Temos portanto uma aplicação induzida do grupo quociente G/N no grupo H, $xN \mapsto f(x)$, que analisamos a seguir.

Teorema 6.3 (Teorema dos Homomorfismos)**.** *Seja $f\colon G \to H$ um homomorfismo de grupos, N o seu núcleo. Então a aplicação*

$$\begin{aligned} \varphi\colon G/N &\to H \\ xN &\mapsto f(x) \end{aligned}$$

é um homomorfismo injetor. Em particular, os grupos G/N e $f(G)$ são isomorfos.

Demonstração: Temos

$$\varphi(xN \cdot yN) = \varphi(xyN) = f(xy) = f(x)f(y) = \varphi(xN) \cdot \varphi(yN)$$

e logo a aplicação é realmente um homomorfismo. Se $\varphi(xN) = \varphi(yN)$, então

$$1_H = \varphi(xN)\varphi(yN)^{-1} = \varphi((xN)(yN)^{-1}) = \varphi(xy^{-1}N) = f(xy^{-1})$$

e logo $xy^{-1} \in N$, isto é, $xN = yN$, mostrando a injetividade e terminando a demonstração. □

Exemplo 6.4. O teorema dos homomorfismos é uma ferramenta eficaz para descrever quocientes de grupos em termos de isomorfismos. Na prática, para mostrar que $A/B \cong C$, tudo o que você necessita é um homomorfismo sobrejetor $A \to C$ cujo núcleo seja exatamente B. Vejamos alguns exemplos.

(a) O núcleo do homomorfismo $\mathbb{R} \to S^1$ dado por $t \mapsto e^{2\pi it}$ é exatamente o grupo dos inteiros $\mathbb{Z}$. Como esta aplicação é sobrejetora, segue do Teorema 6.3 que $\mathbb{R}/\mathbb{Z} \cong S^1$. Da mesma forma, mostra-se que o quociente $\mathbb{R}^2/\mathbb{Z}^2$ é isomorfo ao toro $S^1 \times S^1$.

(b) O determinante $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ é um homomorfismo sobrejetor, cujo núcleo é $\mathrm{SL}_n(\mathbb{R})$, as matrizes de determinante 1. Assim, $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^*$.

(c) Suponha que H e N são subgrupos de G, e que N é normal. Então HN é ainda um subgrupo de G. Por outro lado, a aplicação $H \to HN/N$ dada por $h \mapsto hN$ é um homomorfismo sobrejetor, cujo núcleo é $H \cap N$. Segue daí que

$$\frac{H}{H \cap N} \cong \frac{HN}{N}$$

(compare com a Proposição 5.1).

7 O produto direto

A maneira mais simples de construir um grupo a partir de dois grupos G e H é através do produto direto: como conjunto, consiste do produto cartesiano $G \times H$. O produto é feito coordenada a coordenada:

$$(g_1, h_1) \cdot (g_2, h_2) := (g_1 g_2, h_1 h_2)$$

com $g_1, g_2 \in G$, $h_1, h_2 \in H$. O elemento neutro é $(1_G, 1_H)$. O inverso de (g, h) é (g^{-1}, h^{-1}). Nessa construção, observe que, identificando $G = G \times \{1_H\}$ e $H = \{1_G\} \times H$, temos

$$G \lhd G \times H, \quad H \lhd G \times H, \quad G \cap H = \{1\} \quad \text{e} \quad GH = G \times H.$$

O produto direto de uma família finita de grupos $G_1, G_2, \ldots, G_k$ é definido de maneira análoga. O produto direto de uma família infinita $\{G_\lambda\}_{\lambda \in \Lambda}$ é definido como sendo o subconjunto dos elementos $(g_\lambda) \in \prod_{\lambda \in \Lambda} G_\lambda$ tais que $g_\lambda \neq 1$ somente para um número finito de índices λ.

A seguinte situação em álgebra linear deve ser familiar: se U e V são subespaços vetoriais de um espaço W tais que $U + V = W$ e $U \cap V = \{0\}$, então $W = U \oplus V$, ou seja, é a soma direta dos subespaços. Em particular, cada vetor de W se escreve, de maneira única, como soma de vetores de U e V.

Vale algo similar para grupos, desde que seja acrescida, naturalmente, a hipótese de que os subgrupos envolvidos sejam normais.

Proposição 7.1. *Sejam A, B subgrupos normais de um grupo G, tais que $AB = G$ e $A \cap B = \{1\}$. Então $\varphi\colon A \times B \to G$ dada por $(a, b) \mapsto ab$ é um isomorfismo. Em particular, todo elemento de G se escreve, de maneira única, como produto de elementos de A e B.*

Demonstração: Para começar, note que se $a \in A$ e $b \in B$, então $ab = ba$. Para isto, basta mostrar que $aba^{-1}b^{-1} \in A \cap B = \{1\}$, o que de fato ocorre: por um lado, $aba^{-1} \in B$ uma vez que B é normal; por outro $ba^{-1}b^{-1} \in A$, pois A é normal.

Agora, como a aplicação do enunciado é sobrejetora, basta mostrar que se trata de um homomorfismo injetor. Se $x = (a, b)$ e $y = (a', b')$, então

$$\varphi(xy) = \varphi(aa', bb') = aa'bb' = aba'b = \varphi(x)\varphi(y)$$

onde vale a penúltima igualdade vale pois mostramos que os elementos de A e B comutam entre si. Finalmente:

$$1 = \varphi((a, b)) = ab \implies a = b^{-1} \implies a, b \in A \cap B = \{1\}$$

e portanto o núcleo é trivial, ou seja, a aplicação é injetora. □

Nas condições da proposição, dizemos que G é o *produto direto interno* dos subgrupos, o que fica indicado por $G = A \odot B$.

Há uma generalização importante desta construção para o caso em que apenas um dos subgrupos é normal. Veja a seção sobre o produto semi-direto.

8 Grupos de permutações

Recorde que denotamos por $\mathrm{Perm}\, A$ o grupo das permutações de um conjunto A. Assim, $\mathrm{Perm}\, A = \{\text{bijeções } A \to A\}$, e a operação é a composição de funções. De fato, o conjunto A em si não interessa muito, apenas sua cardinalidade: se B é um outro conjunto e existe uma bijeção entre A e B, então $\mathrm{Perm}\, A$ e $\mathrm{Perm}\, B$ são isomorfos. Se A é finito com n elementos, então na maioria das vezes consideramos $A = \{1, 2, \ldots, n\}$ e abreviamos $\mathrm{Perm}\, A$ por S_n.

Seja G um grupo. Uma maneira de definir uma ação de G em si mesmo é através das *translações*: dado $g \in G$, definimos $\tau_g \colon G \to G$ por $\tau_g(x) = gx$ $(x \in G)$. Assim, a cada elemento de G fica associada uma bijeção, isto é, um elemento do grupo $\mathrm{Perm}\, G$. Dessa observação segue um resultado famoso de Cayley, que mostra quão importante são os grupos simétricos.

Teorema 8.1. (Cayley) *A aplicação $\tau \colon G \to \mathrm{Perm}\, G$ dada por $g \mapsto \tau_g$ é um homomorfismo injetor. Como consequência, todo grupo finito de ordem n é isomorfo a um subgrupo de S_n.*

Demonstração: Se $g, h, x \in G$, então

$$\tau_{gh}(x) = (gh)x = g(hx) = \tau_g(\tau_h(x)),$$

isto é, $\tau_{gh} = \tau_g \circ \tau_h$, e portanto τ é um homomorfismo, que é injetor. Logo G e sua imagem $\tau(G)$ são isomorfos e este último é um subgrupo de $\mathrm{Perm}\, G$. □

Seja σ uma permutação. Como descrevê-la? Uma maneira simples, porém de escrita longa, é arranjar o domínio e imagem em linhas, fazendo corresponder em uma mesma coluna um elemento e sua imagem:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Entretanto certos tipos de permutações podem ser descritas de maneira mais eficiente.

Sejam $j_1, j_2, \ldots, j_r$ letras distintas. Denotamos por

$$(j_1\, j_2\, \cdots\, j_r)$$

a permutação que leva j_i em j_{i+1} para $i < r$, leva j_r em j_1 e fixa todo elemento diferente dos j_i's. Uma tal permutação é chamada um *r-ciclo* ou um *ciclo de comprimento r*. Por exemplo, o 4-ciclo $(1\,5\,2\,6)$ denota a permutação

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 4 & 2 & 1 \end{pmatrix}.$$

Um mesmo r-ciclo pode ser representado de várias formas diferentes. Por exemplo, $(5\,2\,6\,1)$, $(2\,6\,1\,5)$ e $(6\,1\,5\,2)$ representam exatamente o mesmo 4-ciclo acima, como você deve verificar. Nem toda permutação é um ciclo: $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix}\right)$ é um exemplo.

Um r-ciclo possui ordem r, mas a recíproca não vale. Todavia, se p é primo, uma permutação de ordem p em S_p é um p-ciclo.

Dois ciclos $(j_1 \cdots j_r)$ e $(k_1 \cdots k_s)$ são ditos *disjuntos* se os conjuntos dos j_i's e k_i's são disjuntos. Ciclos disjuntos permutam entre si.

Toda permutação pode ser escrita como um produto de ciclos disjuntos. Tal escrita é única, a menos da ordem na qual os ciclos aparecem. Em outras palavras, toda permutação se fatora como um produto de ciclos; neste sentido, os ciclos desempenham o mesmo papel que os números primos na aritmética dos inteiros.

O ciclo mais simples depois da identidade é um 2-ciclo e estes chamados de *transposições*. Um r-ciclo qualquer se escreve como um produto de transposições: de fato,

$$(j_1\ j_2\ \cdots\ j_r) = (j_1\ j_2)(j_2\ j_3)\cdots(j_{r-1}\ j_r).$$

Em particular, toda permutação pode ser escrita como um produto de transposições. Tal produto, em geral, não é único; por exemplo,

$$(1\,2\,3\,4) = (1\,2)(2\,3)(3\,4) = (1\,4)(1\,3)(1\,2).$$

Entretanto a *paridade* do número de transposições que aparecem em um decomposição está bem definida, como veremos a seguir.

O *sinal* de uma permutação σ é definido por

$$\operatorname{sinal}(\sigma) = \prod_{i<j} \frac{\sigma j - \sigma i}{j - i}$$

onde abreviamos $\sigma(i)$ por σi. Uma permutação é dita *par* se seu sinal é positivo e *ímpar* caso contrário. Por exemplo, a identidade é uma permutação par e a transposição $(1\,2)$ é ímpar.

Teorema 8.2. *Seja $n \geq 2$ um inteiro. A aplicação $\operatorname{sinal} : S_n \to \{-1, +1\}$ é um homomorfismo sobrejetor. Mais ainda, se $\sigma = \tau_1\tau_2\cdots\tau_k$ é um produto de transposições, então $\operatorname{sinal}(\sigma) = (-1)^k$.*

Demonstração: Se σ e ρ são duas permutações quaisquer, então

$$\begin{aligned}\operatorname{sinal}(\sigma\rho) &= \prod_{i<j} \frac{\sigma\rho j - \sigma\rho i}{j - i} \\ &= \prod_{i<j} \frac{\sigma\rho j - \sigma\rho i}{\rho j - \rho i} \cdot \prod_{i<j} \frac{\rho j - \rho i}{j - i} = \operatorname{sinal}(\sigma)\operatorname{sinal}(\rho)\end{aligned}$$

(pois se $\rho j - \rho i$ e $j - i$ têm sinais opostos, então $\sigma\rho j - \sigma\rho i$ e $\rho j - \rho i$ têm sinais opostos). Assim, a aplicação sinal é de fato um homomorfismo. Se $\tau = (12)$, então $j > i$ e $\tau j < \tau i$ se e somente se $j = 2$ e $i = 1$, ou seja, $\operatorname{sinal}(12) = -1$, donde temos a sobrejetividade. Das igualdades

$$(1k) = (2k)(12)(2k) \qquad \text{e} \qquad (ij) = (j1)(i1)(j1) \qquad (i, j, k \notin \{1, 2\})$$

segue-se que toda transposição tem sinal negativo, o que prova a última afirmação do teorema. □

O núcleo A_n do homomorfismo sinal é portanto um subgrupo normal de índice 2 de S_n e constitui-se de todas as permutações que se escrevem como o produto de um número par de transposições. O subgrupo A_n é chamado o *grupo alternado* de grau n.

Proposição 8.3. *Para todo $n \geq 3$, $A_n = \langle$3-ciclos$\rangle$.*

Demonstração: Se σ é um k-ciclo, então σ se escreve como um produto de $k-1$ transposições. Em particular, todo 3-ciclo pertence a A_n. Por outro lado, dado σ em A_n, então σ se escreve como um produto de um número par de transposições. Agrupando-as de par em par, temos dois casos: elas são disjuntas ou não. Como:

$$(ab)(cd) = (acb)(acd) \qquad \text{e} \qquad (ab)(bc) = (abc)$$

a demonstração está terminada. □

9 O Teorema dos Homomorfismos, II

Nosso próximo passo é descrever a estrutura dos subgrupos de um quociente G/N em termos dos subgrupos de G que contém N. Necessitamos de um resultado auxiliar.

Lema 9.1. *Seja $f\colon G \to H$ um homomorfismo de grupos e tome N seu núcleo.*

(a) Se A é um subgrupo de G contendo N, então $f^{-1}(f(A)) = A$.

(b) Se K é um subgrupo de $f(G)$, então $f(f^{-1}(K)) = K$.

Demonstração: Para começar, observe que para quaisquer subconjuntos $A \subset G$ e $K \subset H$ valem

$$f^{-1}(f(A)) \supseteq A \qquad \text{e} \qquad f(f^{-1}(K)) = K \cap f(G).$$

Isso prova (b) e nos deixa apenas a tarefa de provar a inclusão restante em (a). Tome x em $f^{-1}(f(A))$. Então $f(x) = f(a)$ para algum $a \in A$ e, sendo f um homomorfismo, segue-se que $a^{-1}x$ pertence a N, que supomos contido em A; logo $x \in A$, como desejado. □

Teorema 9.2 (Teorema dos Homomorfismos II)**.** *Seja $f\colon G \to H$ um homomorfismo de grupos e N o seu núcleo. Temos uma bijeção*

$$\begin{array}{rcl} \Psi\colon \{\textit{subgrupos de } G \textit{ contendo } N\} & \to & \{\textit{subgrupos de } f(G)\} \\ A & \mapsto & f(A) \\ f^{-1}(K) & \leftarrow & K \end{array}$$

onde as aplicações indicadas são inversas uma da outra. Esta bijeção preserva quase tudo que você possa desejar: inclusões, índices, interseções, produtos, subgrupos normais e quocientes. De maneira precisa, se A e B são subgrupos de G que contém N, então:

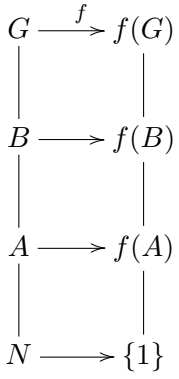
(a) $(G : A) = (f(G) : f(A))$.

(b) $f(A \cap B) = f(A) \cap f(B)$.

(c) $f(A \cdot B) = f(A) \cdot f(B)$.

(d) *$A \lhd G$ se e somente se $f(A) \lhd f(G)$.*

(e) *Se $A \lhd G$, então $G/A \cong f(G)/f(A)$.*



Demonstração: O ponto mais importante, de que as aplicações indicadas são inversas (tanto à esquerda quanto à direita) uma da outra, foi provado no oportuno Lema 9.1. É evidente que inclusões são preservadas. Resta-nos conferir a lista de afirmações.

Para o item (a), note que $xA \mapsto f(x)f(A)$ estabelece uma bijeção entre {classes laterais de A em G} e {classes laterais de $f(A)$ em $f(G)$}; sua inversa se define assim: dado $y \in f(G)$, associe $yf(A) \mapsto zA$, onde $z \in G$ satisfaz $f(z) = y$ (qualquer escolha serve). Convido você a verificar os pormenores.

Para (b), observe que para conjuntos sempre vale $f^{-1}(f(A) \cap f(B)) = f^{-1}(f(A)) \cap f^{-1}(f(B))$ e logo a igualdade segue do item (b) do Lema 9.1. Prova-se (c) com um artífício similar. Para (d):

$$gAg^{-1} = A \iff f(gAg^{-1}) = f(A) \iff f(g)f(A)f(g)^{-1} = f(A).$$

Finalmente, o item (e): como o homomorfismo $G \to f(G)/f(A)$ dado por $x \mapsto f(x)f(A)$ é sobrejetor e tem como núcleo $f(A)$, basta aplicar o teorema dos homomorfismos 6.3. □

Um caso típico de aplicação do teorema é o estudo de grupos quocientes: dado um subgrupo normal N de um grupo G, consideramos a projeção canônica $\pi\colon G \to G/N$. Traduzindo os resultados do teorema, temos uma correspondência (informalmente: um espelho) entre os subgrupos do quociente e os subgrupos de G que contém N. Podemos então aprender muito sobre um lado se conhecemos informações sobre o outro. Vejamos um exemplo.

Exemplo 9.3. Faremos aqui algumas afirmações que serão justificadas mais tarde. O objetivo aqui é ilustrar o uso do Teorema 9.2.

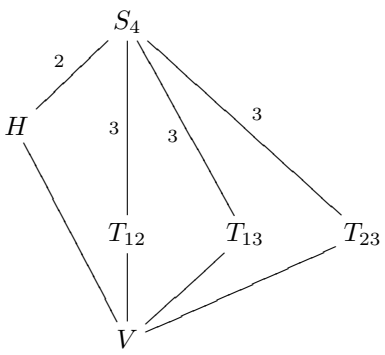
Tome S_4 o grupo das permutações de 4 elementos e considere o *grupo de Klein*

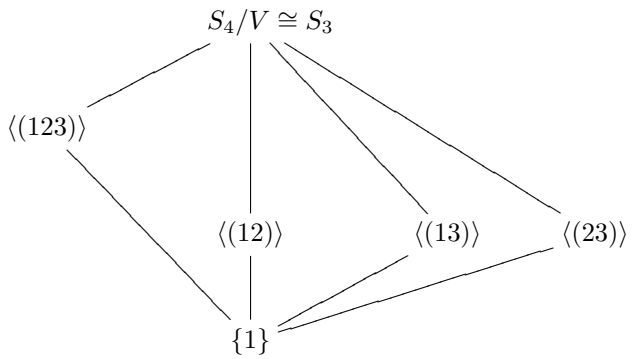
$$V = \{(1), (12)(34), (13)(24), (14)(23)\}$$

(V vem de *Vier*, em alemão). Note que o grupo V é formado por todos os produtos possíveis de transposições disjuntas em quatro elementos. Ocorre que de fato este é um subgrupo normal de S_4. O quociente S_4/V é portanto um grupo com seis elementos. Para $\alpha = (12)V$ e $\beta = (13)V$, temos

$$\alpha\beta = (213)V \neq (312)V = \beta\alpha.$$

e logo S_4/V não é abeliano. Da classificação dos grupos de ordem 6 que veremos adiante, segue-se que $S_4/V \cong S_3$. Agora, como conhecemos todos os subgrupos de S_3, podemos dizer que conhecemos todos os subgrupos de S_4 que contém V, via o Teorema 9.2. Um diagrama, mil palavras:





Aqui, H e T_{ij} indicam os subgrupos de S_4 correspondendo aos subgrupos $\langle(123)\rangle$ e $\langle(ij)\rangle$ de S_3, respectivamente. Os números acima das linhas representam o índice. Por exemplo, $(S_4 : H) = 2$, ou seja, H possui 12 elementos. Deduzimos daí que $H = A_4$, pois este é o único subgrupo de S_4 com esta cardinalidade.

Cada um dos grupos T_{ij} possui 8 elementos. Ocorre que *todo subgrupo T de S_4 com ordem 8 contém V como subgrupo.* Para ver isto, note que T não está contido em A_4 e logo metade dos seus elementos são permutações pares. Em S_4, as únicas permutações pares são os elementos do grupo de Klein ou os 3-ciclos. Porém T não contém 3-ciclos e logo $V \subset T$.

A conclusão é que S_4 possui exatamente 3 subgrupos de ordem 8, os subgrupos T_{ij} que aparecem na correspondência acima. Um deles é nosso velho conhecido, é o famigerado $D_4 = \langle(1234), (12)(34)\rangle$. Por simetria, os outros subgrupos são $\langle(1324), (12)(34)\rangle$ e $\langle(1243), (12)(34)\rangle$. Note que nenhum destes três subgrupos é normal em S_4, visto que os subgrupos correspondentes não são normais em S_3.

Embora trabalhoso, é um instrutivo exercício estabelecer concretamente a correspondência acima. Para isso é necessário escolher um isomorfismo entre $S_4/V \to S_3$ e há vários deles: basta escolher elementos de ordens 2 e 3. Em um exemplo, tome $\alpha = (12)V$ e $\gamma = (123)V$ e associe $\alpha \mapsto (12)$ e $\gamma \mapsto (123)$. Você está escalado para descobrir o que acontece neste caso. □

10 Grupos cíclicos

Um grupo G é dito *cíclico* se G é gerado por um único elemento, isto é, se existe $g \in G$ tal que $G = \langle g\rangle = \{g^n \mid n \in \mathbb{Z}\}$. Em virtude de (1.1), todo grupo cíclico é abeliano. A recíproca não vale: o exemplo mais simples é $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Exemplo 10.1.

1. O grupo aditivo dos números inteiros é um grupo cíclico infinito. De fato, $\mathbb{Z}$ é gerado por 1 ou por -1 e estes são seus únicos geradores.

2. Para cada $n > 0$, $\mathbb{Z}_n$ é um grupo cíclico de ordem n, gerado por exemplo por $\bar{1}$. De forma geral, $\mathbb{Z}_n = \langle\bar{k}\rangle$ se e somente se $\mathrm{mdc}(k, n) = 1$. Logo $\mathbb{Z}_n$ possui $\phi(n)$ geradores distintos, onde ϕ é a função de Euler.

Esses exemplos compreendem, a menos de isomorfismos, todos os grupos cíclicos, como vemos na proposição a seguir.

Proposição 10.2. *Seja G um grupo cíclico, digamos $G = \langle g\rangle$. Então:*

(a) *A aplicação $\mathbb{Z} \to G$ dada por $k \mapsto g^k$ é um homomorfismo sobrejetor.*

(b) *Se G é infinito, então $G \cong \mathbb{Z}$; se G é finito, então $G \cong \mathbb{Z}_n$, onde $n = |G|$.*

(c) *Todo subgrupo de G é cíclico. Se G é finito de ordem n e $A < G$ tem ordem m, então $A = \langle g^{n/m}\rangle$.*

(d) *Se G é finito de ordem n e $m \mid n$, então existe um único subgrupo de G com ordem m.*

Demonstração: (a) e (b): Sendo um subgrupo de $\mathbb{Z}$, o núcleo da aplicação acima é da forma $n\mathbb{Z}$, para algum $n \geq 0$. Daí, pelo teorema dos homomorfismos, temos $G \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. Se $n = 0$, então $G \cong \mathbb{Z}$; se $n > 0$, então G é isomorfo ao grupo de resíduos módulo n.

(c): Se G é infinito, então $G \cong \mathbb{Z}$ e logo $A \cong k\mathbb{Z}$ para algum inteiro $k \geq 0$. Suponha que G é finito. Seja d o menor inteiro positivo tal que $g^d \in A$. Seja $a \in A$, digamos $a = g^k$. Então existem únicos $q, r \in \mathbb{Z}$ tais que

$$k = qd + r, \qquad \text{com } 0 \leq r < d.$$

Logo $g^r = g^{k-qd}$ é um elemento de A. Segue-se que $r = 0$, pela escolha de d. Assim, $A = \langle g^d \rangle$. Em particular, se $|A| = m$, então $d = n/m$.
(d): O subgrupo $\langle g^{n/m} \rangle$ possui ordem m e, pelo item (c), é o único com esta propriedade. □

Recorde que a *ordem* de um elemento g é a cardinalidade do subgrupo gerado por g. Em particular, se G é finito, então $o(g)$ divide $|G|$ e portanto $g^{|G|} = 1$. Desta observação temos imediatamente o:

Teorema 10.3. (Euler) *Seja $n > 0$ um inteiro. Se $\mathrm{mdc}(a, n) = 1$, então*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Demonstração: O resultado segue simplesmente do fato de que o grupo multiplicativo $(\mathbb{Z}_n)^*$ possui ordem $\phi(n)$. □

Como um caso particular do teorema de Euler, temos o

Corolário 10.4. (Pequeno Teorema de Fermat) *Se p é um primo e $p \nmid a$, então $a^{p-1} \equiv 1 \pmod{p}$.*

11 Classificação de grupos de ordem pequena

Vamos agora classificar todos os grupos de ordem ≤ 8. Em primeiro lugar, se G é um grupo de ordem $m = 2, 3, 5$ ou 7, então G é um grupo cíclico e portanto, pela Proposição 10.2, isomorfo a $\mathbb{Z}_m$ nesses casos. Passamos ao estudo dos grupos de ordem 4, 6 e 8.

11.1 Grupos de ordem 4

Seja G um grupo de ordem 4. Pelo Teorema de Lagrange, as possíveis ordens de elementos de G são $1, 2, 4$. Se G possui um elemento de ordem 4, então G é cíclico e logo $G \cong \mathbb{Z}_4$. Por outro lado, se $g^2 = 1$ para todo $g \in G$, então G é abeliano. Dados $x, y \in G$ distintos, então $G = \{1, x, y, z\}$, onde $z = xy$. A aplicação $G \to \mathbb{Z}_2 \times \mathbb{Z}_2$ dada por

$$\begin{aligned} 1 &\mapsto (\bar{0}, \bar{0}), \quad x \mapsto (\bar{0}, \bar{1}) \\ y &\mapsto (\bar{1}, \bar{0}), \quad z \mapsto (\bar{1}, \bar{1}) \end{aligned}$$

é um homomorfismo bijetor (a verificação disto é deixada ao leitor), e portanto um isomorfismo. Em resumo, provamos o

Teorema 11.1. *Seja G um grupo de ordem 4. Então $G \cong \mathbb{Z}_4$ ou $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.*

11.2 Grupos de ordem 6

Classificamos agora os grupos de ordem 6. Como veremos a seguir, existem apenas duas possibilidades: o grupo cíclico de ordem 6 ou o grupo das permutações de 3 elementos.

Teorema 11.2. *Seja G um grupo de ordem 6. Então $G \cong \mathbb{Z}_6$ ou $G \cong S_3$.*

Demonstração: As possíveis ordens para elementos de G são $1, 2, 3$ ou 6. Mas podemos ser mais precisos:

Afirmação: *Existem elementos x e y em G tais que $o(x) = 3$ e $o(y) = 2$.*

De fato, se $g \in G$ é tal que $o(g) = 6$, então $o(g^2) = 3$ e $o(g^3) = 2$. Logo podemos supor que G não possui elementos de ordem 6. Daí, para demonstrar a afirmação, basta mostrar que nenhuma das duas possibilidades abaixo ocorre:

- Todo elemento de $G \setminus \{1\}$ possui ordem 2: tome $g, h \in G$ distintos. Então $gh \notin \{1, g, h\}$ e, como gh tem ordem 2, segue-se que $gh = hg$. Fica então facil verificar que $\{1, g, h, gh\}$ é um subgrupo de G de 4 elementos, o que não é possível pelo Teorema de Lagrange.

- Todo elemento de $G \setminus \{1\}$ possui ordem 3: tome $x, y, z \in G$ distintos entre si e de ordem 3. Então:
$$\langle x \rangle \cap \langle y \rangle = \langle x \rangle \cap \langle z \rangle = \langle y \rangle \cap \langle z \rangle = \{1\}.$$
Logo G possui pelo menos sete elementos distintos, a saber, $1, x, x^2, y, y^2, z$ e z^2, o que não é possível.

A afirmação fica assim demonstrada. Agora, a classificação de G fica subordinada à análise de duas possibilidades:

Caso 1: $xy = yx$.

Aqui G é um grupo cíclico. Com efeito, defina $g := xy$. Não é lá muito trabalhoso verificar que $g^a \neq 1$ para cada $a = 1, \ldots, 5$. Logo os seis elementos
$$1, g, g^2, g^3, g^4, g^5$$
são distintos entre si, constituindo assim o grupo G. Concluímos assim que $G = \langle g \rangle$ e portanto, da Proposição 10.2, segue-se que $G \cong \mathbb{Z}_6$.

Caso 2: $xy \neq yx$.

Nesse caso, temos que $G = \{1, x, x^2, y, xy, yx\}$, pois esses seis elementos são necessariamente distintos entre si. Também,
$$yx = x^2 y. \tag{11.1}$$
Com efeito, basta provar que $yxy^{-1} \notin \{1, x, y, xy, yx\}$ o que é facilmente verificado utilizando o fato que $y = y^{-1}$. Logo todo elemento de G pode ser escrito (de maneira única) na forma $x^i y^j$ com $i = 0, 1, 2$ e $j = 0, 1$. Por outro lado, utilizando-se a equação (11.1) e indução, obtemos que
$$y^s x^t = x^{2^t s} y^s \qquad (s, t \geq 0)$$
e logo um produto de dois elementos de G é da forma
$$x^i y^j x^a y^b = x^{i+2^a j} y^{j+b}. \tag{11.2}$$

Isso mostra que só existe, a menos de isomorfismos, um grupo de ordem 6 satisfazendo as condições do segundo caso. Mais precisamente, se H é um grupo de ordem 6 com elementos α e β tais que

$$o(\alpha) = 3, \quad o(\beta) = 2 \quad \text{e} \quad \alpha\beta \neq \beta\alpha$$

então $G \cong H$. De fato, todas as considerações tecidas a respeito de G se aplicam a H; em particular, $H = \{\alpha^i\beta^j \mid i = 0, 1, 2, j = 0, 1\}$. Mais ainda, a aplicação $G \to H$ dada por $x^iy^j \mapsto \alpha^i\beta^j$ é um homomorfismo (bijetor), pois a relação em (11.2) se verifica ao substituirmos x por α e y por β.

Agora, sejam $\sigma = \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right)$ e $\tau = \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right)$ elementos do grupo S_3. Então $o(\sigma) = 3$, $o(\tau) = 2$ e $\sigma\tau \neq \tau\sigma$. Como S_3 possui ordem 6, concluímos que todo grupo que se enquadra no segundo caso é isomorfo a S_3. □

Uma generalização das idéias utilizadas na demonstração do Teorema 11.2 pode ser encontrada no livro de A. Garcia e Y. Lequain, "Elementos de Álgebra", seção V.7 (grupos gerados por dois elementos).

11.3 Grupos de ordem 8

Existem exatamente 5 subgrupos de ordem 8 não-isomorfos entre si, como descrito no teorema a seguir.

Teorema 11.3. *Seja G um grupo de ordem 8.*

1. *Se G é abeliano, então $G \cong \mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2$ ou $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.*
2. *Se G não é abeliano, então $G \cong D_4$ ou $G \cong Q$, o grupo dos quatérnios.*

Estes cinco grupos não são isomorfos entre si.

Demonstração: Analisando ordens de elementos, fica claro que os grupos listados não são isomorfos entre si; note Q possui três elementos de ordem 4 e D_4 apenas dois.

Resta mostrar que estes cinco grupos são de fato os únicos possíveis, mas não faremos os detalhes agora. O caso abeliano é bem mais simples e decorre, por exemplo, da teoria de Sylow, que veremos adiante. □

12 Automorfismos

Um *automorfismo* de um grupo G é um isomorfismo de G em si mesmo. Com a operação de composição, os automorfismos de G formam um grupo, denotado por $\operatorname{Aut} G$.

Dado $g \in G$, a função $\iota_g \colon G \to G$ dada por $x \mapsto gxg^{-1}$ é um automorfismo de G. Como

$$\iota_{gh} = \iota_g \circ \iota_h \qquad (g, h \in G) \tag{12.1}$$

temos um homomorfismo $G \to \operatorname{Aut} G$. Em particular, sua imagem, $\operatorname{Int}(G)$, é um subgrupo de $\operatorname{Aut} G$, chamado o grupo dos *automorfismos internos*. Um automorfismo interno ι_g é a aplicação identidade de G se e somente se g comuta com todos os elementos de G. Pelo teorema dos homomorfismos, temos

$$\operatorname{Int}(G) \cong \frac{G}{Z(G)}.$$

Como consequência:

Proposição 12.1. *Todo grupo finito G de ordem ≥ 3 possui pelo menos um automorfismo não-trivial.*

Demonstração: Com efeito, temos três casos. Se G é não abeliano, então G possui um automorfismo interno não-trivial; se G é abeliano, então $x \mapsto x^{-1}$ $(x \in G)$ define um automorfismo, que é trivial se, e somente se, todo elemento de $G \setminus \{1\}$ possui ordem 2; e, por fim, se todo elemento de $G \setminus \{1\}$ possui ordem 2, então $G \cong \mathbb{Z}_2^k = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ para algum k (tente prová-lo!). Como $|G| \geq 3$, temos $k \geq 2$; aqui, $(x, y, \dots) \mapsto (y, x, \dots)$ define um automorfismo não trivial de G. □

13 Ações de grupos

Nosso ponto de vista até aqui tem sido estudar os grupos de maneira puramente abstrata: a princípio, os elementos de grupo não tem significado algum. Historicamente, a noção de grupo não surgiu assim. De fato, percebeu-se, de maneira cada vez mais frequente, que certas coleções de *funções* definidas em contextos muito distintos possuiam propriedades similares. Uma situação típica são as permutações (interpretando geometricamente, funções que "misturam" o conjunto dado). Eis bons exemplos: se um objeto X possui alguma estrutura (um espaço vetorial, um espaço topológico, uma variedade, um corpo), os *automorfismos* com respeito a essa estrutura formam um grupo. Outro exemplo: se X é um subconjunto do plano, as *simetrias* de X também formam um grupo, como já tivemos oportunidade de analisar. Note que nestes exemplos a operação nos grupos é a composição de funções.

Nesta seção buscamos recuperar esse viés mais geométrico.

Um grupo G *age* em um conjunto S se existe uma aplicação $\sigma\colon G \times S \to S$ tal que

$$\sigma(1, s) = s \quad \text{e} \quad \sigma(gh, s) = \sigma(g, \sigma(h, s))$$

para quaisquer $g, h \in G$, $s \in S$. Fica mais sugestivo escrever $\sigma_g(s) = \sigma(g, s)$ ou mesmo $gs = \sigma(g, s)$, quando a ação estiver subentendida. Assim, nossas exigências se traduzem simplesmente em: $1 \cdot s = s$ e $(gh)s = g(hs)$.

Se G age em S, então G define um conjunto de funções sobre S. De fato, segue das definições acima que cada elemento define uma bijeção $g\colon S \to S$ (cuja inversa é g^{-1}). O que torna a coisa toda mais interessante é que pedimos que a multiplicação em G seja compatível com a composição das funções induzidas. Dizendo de maneira equivalente, uma ação de G em S é simplesmente um homomorfismo

$$G \to \operatorname{Perm} S$$

de G no grupo das permutações de S. Tal homomorfismo também é chamado uma *representação* de G.

Fixe um ponto $s \in S$. A *órbita* de s é o conjunto de todas as possíveis imagens de s por elementos de G, isto é,

$$\mathcal{O}_s := \{gs \mid g \in G\} \subseteq S$$

Duas órbitas $\mathcal{O}_s$ e $\mathcal{O}_t$ ou são disjuntas ou coincidem: se $x \in \mathcal{O}_s \cap \mathcal{O}_t$, então $x = gs = ht$ e logo $s = g^{-1}ht$, ou seja, s pertence à órbita de t e, consequentemente, $\mathcal{O}_s \subseteq \mathcal{O}_t$. Da mesma forma temos a inclusão oposta e logo $\mathcal{O}_s = \mathcal{O}_t$. Mais ainda, o conjunto S é a união de suas órbitas, uma vez que $s \in \mathcal{O}_s$.

O *estabilizador* de $s \in S$ é o subconjunto dos elementos de G que deixam s fixo, isto é,

$$G_s := \{g \in G \mid gs = s\}.$$

Produtos e inversos de elementos de G_s também fixam s e logo G_s é um subgrupo de G.

Dizemos que um grupo G age *transitivamente* no conjunto S se dados s e t em S, existe $g \in G$ tal que $gs = t$, ou seja, se $\mathcal{O}_s = S$, para algum (e logo para todo) $s \in S$.

Exemplo 13.1.

(a) Seja $G = \mathrm{GL}_2(\mathbb{R})$ o grupo das matrizes 2×2 invertíveis. Sejam $X = \mathbb{R}^2$, $Y = \{\text{bases ordenadas de } \mathbb{R}^2\}$ e $Z = \{\text{retas de } \mathbb{R}^2\}$. Então G age nestes três espaços, respectivamente, por

$$(g, x) \mapsto g(x), \quad (g, \{v_1, v_2\}) \mapsto \{g(v_1), g(v_2)\} \quad \text{e} \quad (g, \ell) \mapsto g(\ell).$$

No primeiro caso, a ação é transitiva: dados dois pontos do plano, existe uma matriz invertível que leva um no outro. Da mesma forma, G age transitivamente em Y. Entretanto a ação de G em Z não é transitiva: por exemplo, a órbita de uma reta ℓ passando pela origem é o conjunto das retas que passam pela origem. Você consegue identificar o estabilizador de ℓ?

(b) Seja $H = \mathrm{SO}_2(\mathbb{R})$ o grupo das matrizes 2×2 de rotação, isto é,

$$H = \left\{ r_\theta = \left(\begin{smallmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{smallmatrix}\right) \mid \theta \in [0, 2\pi) \right\}.$$

Então o grupo H age em $\mathbb{R}^2$, simplesmente por $(r_\theta, p) \mapsto r_\theta(p)$. A ação não é transitiva: a órbita de um ponto p é o círculo centrado na origem e que passa por p.

O grupo H age sobre o conjunto das bases ordenadas ortonormais, como em (a). Note que uma matriz de rotação preserva orientação. Portanto, esta ação não é transitiva.

(c) Na mesma notação de (b), o grupo H também age (transitivamente) no conjunto das retas do plano que passam pela origem. Aqui, o estabilizador de uma reta é o subgrupo $\{\mathrm{id}, r_\pi\}$.

(d) Inspirados no exemplo (b), definimos uma ação de $G = (\mathbb{R}, +)$ em $\mathbb{R}^2$ por $(t, p) \mapsto r_t(p)$. Observe que $r_{t+t'} = r_t \circ r_{t'}$. Aqui, o estabilizador de um ponto $p \neq (0, 0)$ é o subgrupo $2\pi\mathbb{Z}$.

(e) Sejam $G = (\mathbb{R} - \{0\}, \cdot)$, $X = \mathbb{R}^2$ e considere a ação $(\lambda, p) \mapsto \lambda \cdot p$. Se $p \neq (0, 0)$, então $\mathcal{O}_p$ é a reta (perfurada) que passa pela origem na direção dada pelo vetor p e $G_p = \{1\}$. Porém, a órbita da origem é a própria origem e o estabilizador é todo o grupo G.

Seja G um grupo agindo em um conjunto S, s um elemento de S e G_s seu estabilizador. Cada elemento de uma classe lateral gG_s leva s no elemento gs. Por outro lado, se $gs = hs$, então $h^{-1}gs = s$, isto é, $h^{-1}g \in G_s$ e logo as classes laterais gG_s e hG_s são iguais. Em suma, para cada $s \in S$, temos uma bijeção entre as classes laterais do estabilizador G_s e os elementos da órbita $\mathcal{O}_s$, dada por $gG_s \mapsto gs$.

A conclusão é que o índice de G_s em G é exatamente a cardinalidade da órbita O_s. Como G é uma união disjunta das classes laterais, segue pelo mesmo argumento do teorema de Lagrange que

$$|G| = |\mathcal{O}_s| \, |G_s| \tag{13.1}$$

que é chamada a *equação das órbitas*. Em particular, a cardinalidade de uma órbita divide a ordem de G. A maior parte das aplicações que faremos estão baseadas nesta identidade.

Exemplo 13.2.

(a) Seja H um subgrupo de G. Definimos uma ação de H em G por $h(x) := hx$ para cada $h \in H$, $x \in G$. Dado x em G, sua órbita é a classe lateral Hx e seu estabilizador é trivial. A bijeção entre as classes laterais do estabilizador e a órbita dizem neste caso que Hx e H têm a mesma cardinalidade, para todo $x \in G$. Como as órbitas são disjuntas e sua união é todo o grupo G, reobtemos o Teorema de Lagrange: se G é finito, então $|G| = (G : H)\,|H|$.

(b) (Ação por translação) Seja H um subgrupo de G. Então G age no conjunto das classes laterais (digamos à esquerda) de H simplesmente por $(g, xH) \mapsto gxH$. Esta ação é transitiva. Dado $x \in G$, o estabilizador da classe xH é o subgrupo $E_x = \{g \in G \mid x^{-1}gx \in H\}$. Note que $g \mapsto x^{-1}gx$ define uma bijeção $E_x \to H$.

A idéia por trás de uma ação é que podemos obter informações sobre S se conhecemos suas órbitas. Isso vai muito mais além do que meras relações como (13.1), principalmente quando aspectos geométricos, topológicos, etc., são também levados em conta.

14 A equação de classes de conjugação

Um grupo G sempre age em si mesmo, e de várias maneiras distintas. A análise de diferentes ações nos fornece informações fundamentais sobre a estrutura de G.

Começamos pela *ação por conjugação*, definida por $g \mapsto \iota_g$, onde $\iota_g \colon G \to G$ é dada por $\iota_g x = gxg^{-1}$ (o *conjugado* de x por g). Então

$$\iota_{gh} = \iota_g \iota_h$$

e portanto, de fato, esta é uma ação de G em si mesmo. Aqui, a órbita de um elemento x são exatamente seus conjugados, e é denominada a *classe de conjugação* de x:

$$\mathcal{C}\ell_x = \{gxg^{-1} \mid g \in G\}.$$

O estabilizador de x é chamado o *centralizador* de x em G:

$$C_G(x) = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}.$$

Em particular, o número de conjugados de x é $|\mathcal{C}\ell_x| = (G : C_G(x))$.

Note que x pertence ao centro $Z(G)$ de G se e somente se $\mathcal{C}\ell_x = \{x\}$. Desta observação aparentemente inócua e do fato de que as órbitas através de uma ação são disjuntas, obtemos a *equação de classes (de conjugação)* para um grupo finito G

$$|G| = |Z(G)| + \sum_{i=1}^{k} |\mathcal{C}\ell_{g_i}| \tag{14.1}$$

onde $g_1, g_2, \ldots, g_k$ são representantes das distintas classes de conjugação *fora* do centro de G. Há um pequeno abuso de notação aqui: o somatório do lado esquerdo pode não aparecer, o que ocorre se e somente se G é abeliano.

Vimos que todo grupo de ordem prima é cíclico. Vale algo similar para grupos cuja ordem é o quadrado de um primo: são abelianos. Surpreendente, não? Vamos deduzir isto como uma aplicação da equação de classes. Necessitamos de um resultado auxiliar.

Lema 14.1. *Seja Z o centro de um grupo G. Se G/Z é cíclico, então $G = Z$. Em particular, o índice do centro não pode ser um número primo.*

Demonstração: Desejamos mostrar que G é abeliano. Para isso, tome $x, y \in G$. Por hipótese existe $g \in G$ tal que a classe gZ gera o quociente G/Z. Daí, existem inteiros m, n tais que $xZ = g^m Z$ e $yZ = g^n Z$, o que pode ser reinterpretado assim: existem $u, v \in Z$ tais que

$$x = g^m u \qquad \text{e} \qquad y = g^n v$$

e agora é imediato verificar x e y comutam entre si, o que termina a prova. □

Proposição 14.2. *Se p é um número primo e $|G| = p^2$, então G é abeliano.*

Demonstração: Seja Z o centro de G. Aqui, os casos possíveis para $|Z|$ são $1, p$ e p^2. Para cada $g \notin Z$ temos que $|\mathcal{C}\ell_g|$ é maior que 1 e divide a ordem de G (a cardinalidade de uma órbita divide a ordem do grupo), e logo segue da equação de classes que a ordem do centro é divisível por p. Como o índice do centro não pode ser um número primo (Lema acima), devemos ter $|Z| = p^2$, ou seja, G é abeliano. □

É natural perguntar se algo similar vale para grupos cuja ordem é o cubo de um primo ou potências superiores. Não sei de nenhum resultado de maior destaque nessa direção. Entretanto, com o auxílio do produto semi-direto, prova-se:

Teorema 14.3. *Seja p um número primo. Dado $n \geq 3$, existe um grupo não-abeliano de ordem p^n.*

15 Geradores e relações

16 O produto semi-direto

Sejam N e H subgrupos de um grupo G. Se

$$H \cap N = 1 \quad \text{e} \quad G = HN,$$

e tanto H como N são normais em G, então vimos que G é produto direto interno de H e N. Em particular, $G \cong H \times N$. Um aspecto vantajoso dessa situação é que recuperamos a estrutura de G a partir de H e N: de fato, dados $g_1, g_2 \in G$, escreva $g_i = h_i n_i$ com h_i em H e n_i em N; então

$$g_1 g_2 = h_1 n_1 h_2 n_2 = (h_1 h_2) \cdot (n_1 n_2),$$

ou seja, o produto fica dado em termos de elementos de H e N.

Suponha agora que apenas um dos subgrupos seja normal em G, digamos

$$H < G, \quad N \lhd G, \quad H \cap N = 1 \quad \text{e} \quad G = HN. \tag{16.1}$$

Se g_1, g_2 são como acima, então escrevemos

$$g_1 g_2 = h_1 n_1 h_2 n_2 = (h_1 h_2) \cdot (h_2^{-1} n_1 h_2) n_2 \tag{16.2}$$

que é o produto de elementos de H e N, já que N é normal em G. De maneira análoga, o inverso de $h \cdot n$ é

$$n^{-1} h^{-1} = h^{-1} (h n^{-1} h^{-1}).$$

Novamente, recuperamos a estrutura de G a partir de H e N. Se H e N satisfazem (16.1), então dizemos que G é o produto *semi-direto interno* de H e N, indicado por $G = H \ltimes N$.

Como no caso do produto direto, desejamos uma versão "externa" dessa construção. Como fazê-la? Eis a pista: sendo N normal em G, cada h em H define um automorfismo ι_h de N, a conjugação por h. Como $\iota_{h_1 h_2} = \iota_{h_1} \circ \iota_{h_2}$, temos um homomorfismo $H \to \operatorname{Aut} N$. Temos em mãos o necessário para a generalização.

Sejam N e H dois grupos e suponha que tenhamos um homomorfismo $\sigma\colon H \to \operatorname{Aut} N$, dado por $h \mapsto \sigma_h$. Inspirados em (16.2), definimos no *conjunto* $H \times N$ a operação

$$(h_1, n_1) \cdot_\sigma (h_2, n_2) := (h_1 h_2, \sigma_{h_2^{-1}}(n_1) n_2).$$

Esta operação é associativa; o elemento neutro é $(1_H, 1_N)$; o inverso de (h, n) é $(h^{-1}, \sigma_h(n^{-1}))$. Assim, $(H \times N, \cdot_\sigma)$ é realmente um grupo, que denotamos por $H \ltimes_\sigma N$ ou $N \rtimes_\sigma H$, chamado o *produto semi-direto* de H e N por σ.

Se $G = H \ltimes_\sigma N$, então

$$\begin{array}{ccc} H \to & G & \qquad\text{e}\qquad \\ h \mapsto & (h, 1_N) & \end{array} \qquad\qquad \begin{array}{ccc} N \to & G \\ n \mapsto & (1_H, n) \end{array}$$

são mergulhos. Sejam $H^\bullet$ e $N^\bullet$ suas respectivas imagens. Como $(h, 1_N)(1_H, n) = (h, n)$, temos que $G = H^\bullet N^\bullet$. Por outro lado, de

$$(h, 1_N)(1_H, n)(h, 1_N)^{-1} = (1_H, \sigma_h(n))$$

segue-se que $N^\bullet$ é normal em G. Por fim, $H^\bullet \cap N^\bullet = 1$ e logo G é o produto semi-direto interno de $H^\bullet$ e $N^\bullet$. Na maioria das vezes identificamos H com $H^\bullet$ e N com $N^\bullet$ e escrevemos $H \ltimes N$ no lugar de $H \ltimes_\sigma N$.

Nada melhor que uma série de exemplos para estressar a importância dessa construção.

Exemplo 16.1. Dados grupos H e N quaisquer, sempre é possível encontrar um homomorfismo $H \to \operatorname{Aut} N$: basta tomar $h \mapsto \mathrm{id}_N$ para todo $h \in H$. O produto semi-direto daí resultante é simplesmente o produto direto $H \times N$ usual.

Exemplo 16.2. Seja N um grupo com um automorfismo ψ de ordem 2. (Por exemplo, se $N = \mathbb{Z}_n$ é cíclico de ordem n, então $\operatorname{Aut} N \cong (\mathbb{Z}_n)^*$ e, se $n \geq 3$, $-\bar{1}$ possui ordem 2). Há então duas maneiras de definir um homomorfismo $\mathbb{Z}_2 \to \operatorname{Aut} N$. A primeira, trivial, foi considerada no exemplo anterior. A segunda, é tal que $\bar{1} \mapsto \psi$. Nesse último caso, o grupo

$$\mathbb{Z}_2 \ltimes \mathbb{Z}_n$$

é o grupo diedral de $2n$ elementos (cf. Teorema 16.5 a seguir).

Exemplo 16.3. Seja $\sigma\colon H \to \operatorname{Aut} N$ um homomorfismo não trivial. Então $H \ltimes_\sigma N$ é um grupo não abeliano, ainda que H e N sejam abelianos. Com efeito, seja $h \in H$ tal que $\sigma_h \neq \mathrm{id}_N$. Então existe $x \in N$ tal que $\sigma_h(x) = y$ com $y \neq x$. Então

$$(1, x) \cdot_\sigma (h^{-1}, y) = (h^{-1}, \sigma_h(x) y) = (h^{-1}, y^2)$$

e, por outro lado,

$$(h^{-1}, y) \cdot_\sigma (1, x) = (h^{-1}, \sigma_1(y) x) = (h^{-1}, yx).$$

Em particular, se K é um grupo finito, consideramos o produto semi-direto $\operatorname{Aut} K \ltimes K$ com respeito ao homomorfismo $\mathrm{Id}\colon \operatorname{Aut} K \to \operatorname{Aut} K$. Se $|K| \geq 3$, então K possui um automorfismo não trivial (Proposição 12.1) e logo $\operatorname{Aut} K \ltimes K$ é um grupo não abeliano de ordem $|K|\,|\operatorname{Aut} K|$.

Exemplo 16.4. Na situação do exemplo anterior, seja $G = \operatorname{Aut} K \ltimes K$. Se $K = \mathbb{Z}_3$, então G é um grupo não abeliano de ordem 6, e portanto isomorfo a S_3. Tomando $K = \mathbb{Z}_4$, temos que $\operatorname{Aut} \mathbb{Z}_4 \cong (\mathbb{Z}_4)^* \cong \mathbb{Z}_2$. Logo G é não abeliano de ordem 8. As possibilidades são: $G \cong D_4$ ou $G \cong$ quatérnios. Como G possui um elemento de ordem 4, a saber, $(\bar{0}, \bar{1})$, concluímos que G é o grupo D_4.

A importância do produto semi-direto reside na sua eficiência em construir novos grupos a partir de grupos conhecidos. Os grupos cíclicos são aqueles que melhor conhecemos e podemos realizar construções interessantes já a partir deles.

Sejam m, n inteiros positivos. Procuramos pelos possíveis produtos semi-diretos entre $\mathbb{Z}_m$ e $\mathbb{Z}_n$, ou seja, procuramos pelos possíveis homomorfismos $\sigma : \mathbb{Z}_m \to \operatorname{Aut} \mathbb{Z}_n \cong (\mathbb{Z}_n)^*$. A condição necessária e suficiente é que, se $\sigma(\bar{1}) = \bar{s}$, então $s^m \equiv 1 \pmod{n}$.

Teorema 16.5. *Sejam m, n, s inteiros positivos tais que*

$$s^m \equiv 1 \pmod{n}.$$

Então existe um único *grupo G satisfazendo*

$$|G| = m \cdot n, \tag{16.3}$$

$$G = \langle a, b\rangle = \langle a\rangle\langle b\rangle \tag{16.4}$$

$$a^n = b^m = 1 \qquad e \tag{16.5}$$

$$bab^{-1} = a^s. \tag{16.6}$$

Demonstração: Seja $G = \mathbb{Z}_m \ltimes_\sigma \mathbb{Z}_n$, onde $\sigma : \mathbb{Z}_m \to \mathbb{Z}_n^*$ é o homomorfismo definido por $\bar{1} \mapsto \bar{s}$. Sejam $a = (\bar{0}, \bar{1})$, $b = (\bar{1}, \bar{0})$. Então $\langle a\rangle$ e $\langle b\rangle$ são as imagens dos mergulhos canônicos de $\mathbb{Z}_n$ e $\mathbb{Z}_m$ em G, e portanto as três primeiras propriedades são válidas. Por fim, temos

$$bab^{-1} = (\bar{1}, \bar{0}) \cdot_\sigma (\bar{0}, \bar{1}) \cdot_\sigma (\bar{1}, \bar{0})^{-1} = (\bar{0}, \sigma_{\bar{1}}(\bar{1})) = (\bar{0}, \bar{s}) = a^s$$

o que prova a última das relações. A unicidade de G foi vista em ??. Note que $\langle a\rangle$ é normal em G. □

17 Os teoremas de Sylow

Nesta seção apresentamos uma demonstração dos teoremas de Sylow. A abordagem que seguimos é através da ação de grupos, que torna os argumentos bastante elegantes.

Necessitamos de um lema auxiliar e conto com a sua ajuda para demonstrá-lo.

Exercício 17.1. Seja p um primo. Se $a \leq b$, então

$$\binom{pb}{pa} \equiv \binom{b}{a} \pmod{p}.$$

Sugestão: compare os coeficientes de x^{pa} em ambos os lados da identidade de polinômios $(1+x)^{pb} \equiv (1+x^p)^b \pmod{p}$.

Lema 17.2. *Se p é um primo que não divide m e $k \geq 0$, então $p \nmid \binom{p^k m}{p^k}$.*

Demonstração: Tomando $a = 1$ e $b = m$ e aplicando recursivamente o exercício acima, resulta que $\binom{p^k m}{p^k} \equiv m \pmod{p}$ e logo p não divide $\binom{p^k m}{p^k}$. □

Teorema 17.3. (Sylow) *Se G é um grupo de ordem $p^k m$, onde p é um primo que não divide m, então G contém um subgrupo de ordem p^k.*

Demonstração: (Wielandt) Seja X a coleção de todos os subconjuntos de G de cardinalidade p^k. O grupo G age em X pela translação à esquerda: dado $A \in X$, definimos

$$gA = \{ga \mid a \in A\}.$$

Seja $B \in X$ tal que $p \nmid |\mathcal{O}_B|$ (tal B existe, pois caso contrário p dividiria a cardinalidade de todas as órbitas de X, e logo dividiria $|X|$, contradição com o Lema 17.2). De (13.1), temos $|G| = |\mathcal{O}_B|\,|G_B|$ e portanto p^k divide $|G_B|$. Em particular, $|G_B| \geq p^k$. Por outro lado, se $b \in B$ e $g \in G_B$, então $gb \in gB = B$; além disso, se g e h são elementos distintos de G_B, então gb e hb são também elementos distintos de B, donde $|G_B| \leq p^k$. Concluímos que G_B é um subgrupo de G de ordem p^k. □

Seja G um grupo finito. Fixado um primo p, sempre podemos escrever $|G| = p^k m$ com $k \geq 0$ e de forma que $p \nmid m$. Um subgrupo de G com ordem p^k é chamado um *p-subgrupo de Sylow*. Pelo teorema que acabamos de provar, um tal subgrupo sempre existe.

Note que se p não divide a ordem de G (ou seja, se $k = 0$), então o único p-subgrupo de Sylow de G é $\{1\}$. O outro caso extremo é quando $m = 1$: aqui o único p-subgrupo de Sylow de G é o próprio G.

Exemplo 17.4. Considere A_4, o grupo das permutações pares de quatro elementos, de ordem $12 = 2^2 \cdot 3$. Então o subgrupo de Klein, de ordem 4, é um 2-subgrupo de Sylow. Como consequência dos Teoremas de Sylow, veremos que ele é o único subgrupo de ordem 4. Por outro lado, A_4 possui quatro 3-subgrupos de Sylow distintos, todos de ordem 3, cada um deles gerado por um 3-ciclo. Para um primo p distinto de $2, 3$, o único p-subgrupo de Sylow de A_4 é $\{(1)\}$.

Corolário 17.5. (Cauchy) *Se p é um primo que divide a ordem de um grupo finito G, então G possui um elemento de ordem p.*

Demonstração: Seja P um p-subgrupo de Sylow de G e seja $g \in P$, com $g \neq 1$. Então a ordem de g é p^e, para algum $e > 0$. Se $e = 1$, então g é o elemento que buscamos; se $e > 1$, então $g^{p^{e-1}}$ possui ordem p. □

Seja S o conjunto de todos os p-subgrupos de Sylow de G. Então G age em S por conjugação. Esta observação é o ponto de partida para obter outras informações sobre os subgrupos de Sylow. De fato, vamos considerar não somente a ação de G, mas também a ação de seus subgrupos.

Lema 17.6. *Seja $H < G$ com ordem uma potência de p (mas não necessariamente de Sylow). Então um elemento $Q \in S$ é fixado por todo elemento de H (na ação por conjugação de H em S) se e somente se $H \subseteq Q$.*

Demonstração: Se H está contido em Q, não a nada a fazer. Tratemos então da recíproca.

Se Q é fixado por H, então $hQh^{-1} = Q$ para todo $h \in H$, ou seja, vale $HQ = QH$. Segue da Proposição 5.2 que HQ é um subgrupo de G cuja ordem, calculada na Proposição 5.1, é uma potência de p; como HQ contém o p-subgrupo de Sylow Q, a conclusão é $HQ = Q$ e portanto $H \subseteq Q$, como desejado. □

Teorema 17.7. (Sylow) *Seja G um grupo finito. Tome p um número primo, e escreva $|G| = p^k m$, onde $k \geq 0$ e $p \nmid m$. Seja S o conjunto dos p-subgrupos de Sylow de um grupo finito G. Então:*

(i) *A ação por conjugação de G em S é transitiva; isto é, dados $P, Q \in S$, existe $g \in G$ tal que $Q = gPg^{-1}$. Em particular, os p-subgrupos de Sylow de G são p-grupos isomorfos.*

(ii) *Se n_p é o número de p-subgrupos de Sylow de G, então*

$$n_p \mid m \qquad e \qquad n_p \equiv 1 \pmod{p}.$$

(iii) *Se H é um subgrupo de G cuja ordem é uma potência de p, então H está contido em algum p-subgrupo de Sylow de G.*

Demonstração: Como já anunciamos, a prova consiste em comparar os resultados de ações de certos subgrupos de G em S. Nesta demonstração, as ações são sempre por conjugação.

Seja $P \in S$ e considere a ação de P em S. Do Lema 17.6, o único p-subgrupo de Sylow fixado por esta ação é o próprio P. As outras órbitas são não-triviais e, como dividem a ordem de P, são divisíveis pelo primo p. Como S é a união disjunta de suas órbitas, segue-se que $n_p = |S|$ é côngruo a $1 \pmod{p}$.

Sejam $\mathcal{O}_P$ e G_P a órbita e o estabilizador de P pela ação de G em S, respectivamente. Da equação das órbitas (13.1),

$$|G| = |G_P|\,|\mathcal{O}_P|\,.$$

Como $G_P \supseteq P$, segue-se que $|\mathcal{O}_P|$ divide m e, em particular, $p \nmid |\mathcal{O}_P|$.

Agora, seja $Q \in S$ um p-subgrupo de Sylow qualquer. Suponha, por contradição, que $Q \notin \mathcal{O}_P$. Observe que Q também age em $\mathcal{O}_P$, mais uma vez por conjugação. Então, argumentando como na demonstração do Lema 17.6, vem que Q que não fixa nenhum dos elementos de $\mathcal{O}_P$, ou seja, não há Q-órbitas triviais; consequentemente, p divide cada Q-órbita, mais uma vez por (13.1). Resulta daí que p divide $|\mathcal{O}_P|$, contradição.

Em resumo, mostramos $S = \mathcal{O}_P$, ou seja, a ação de G em S é transitiva. E como $|\mathcal{O}_P|$ divide m, fica mostrado também que $n_p \mid m$, terminando assim a prova de (i) e (ii).

Para provar (iii) usamos um artifício similar. Se H não está contido em nenhum p-subgrupo de Sylow de G, então, novamente pelo Lema 17.6, a ação de H em S não possui órbitas triviais, donde $p \mid n_p$, contradição com (ii). □

Corolário 17.8. *Um p-subgrupo de Sylow é normal em G se e somente se $n_p = 1$.*

Exemplo 17.9. Seja G um grupo de ordem $35 = 5{\cdot}7$. Seja n_5 o número de subgrupos de G de ordem 5 e n_7 o número de subgrupos de G de ordem 7. Pelo Teorema de Sylow:

$$n_5 \mid 7 \text{ e } n_5 \equiv 1 \pmod 5 \implies n_5 = 1,$$

$$n_7 \mid 5 \text{ e } n_7 \equiv 1 \pmod 7 \implies n_7 = 1.$$

Sejam A, B subgrupos de G com $|A| = 5$ e $|B| = 7$. Então, pelo Corolário 17.8, A e B são normais em G. Mais ainda, temos $A \cap B = \{1\}$ e $AB = G$. Segue daí que $G \cong A \times B$. Agora, $A \cong \mathbb{Z}/5\mathbb{Z}$, $B \cong \mathbb{Z}/7\mathbb{Z}$ e como $\mathrm{mdc}(5,7) = 1$, segue do Teorema Chinês dos Restos que $G \cong \mathbb{Z}/35\mathbb{Z}$, ou seja, G é um grupo cíclico.

Exercício 17.10. Prove que se p e q são primos gêmeos e $|G| = pq$, então G é cíclico.

18 Algumas palavras sobre p-grupos

Seja p um número primo. Dizemos que um grupo é um *p-grupo* se a ordem de cada um dos seus elementos é uma potência de p. São exemplos de 2-grupos:

$$D_4, \quad Q, \quad \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots .$$

Pelo Teorema de Cauchy 17.5, a ordem de um p-grupo finito é sempre uma potência de p.

Proposição 18.1. *Sejam p um número primo e G um p-grupo finito, digamos $|G| = p^n$. Então existe uma cadeia de subgrupos*

$$G = G_n \rhd G_{n-1} \rhd \cdots \rhd G_1 \rhd \{1\} \tag{18.1}$$

tal que $|G_i| = p^i$ para $i = 1, \ldots, n$.

Demonstração: Feita por indução. Se $n = 0$, nada a fazer. Suponha a Proposição válida para todos os p-grupos de ordem p^{n-1}, para algum $n \geq 1$. Segue da equação de classes (14.1) que o centro Z de G é não trivial e portanto, pelo Teorema de Cauchy 17.5, existe um elemento $x \in Z$ de ordem p. Como x comuta com todos os elementos de G, o subgrupo $\langle x \rangle$ é normal em G e o quociente $\overline{G} := G/\langle x \rangle$ é um p-grupo de ordem p^{n-1}. Pela hipótese de indução, existe uma cadeia de subgrupos

$$\overline{G} = \overline{G}_{n-1} \rhd \overline{G}_{n-2} \rhd \cdots \rhd \overline{G}_1 \rhd \{1\}$$

tal que $(\overline{G}_i : \overline{G}_{i-1}) = p$ para cada i. Agora, segue do Teorema dos Homomorfismos 9.2 (aplicado à projeção canônica $G \to G/\langle x \rangle$) que a essa cadeia corresponde uma cadeia de subgrupos em G como em (18.1) com $G_1 = \langle x \rangle$ e tal que o índice em cada passo da cadeia ainda é p, como desejado. □

19 Grupos abelianos finitos

Nosso objetivo nesta seção é provar o Teorema de Decomposição Primária para os grupos abelianos finitos.

Lema 19.1. *Sejam A um p-grupo abeliano finito e $H = \langle h\rangle$, onde $h \in A$ possui ordem máxima em A. Se $A \neq H$, então existe $a \in A \setminus H$ de ordem p.*

Demonstração: Com efeito, pelo Teorema de Cauchy existe $y \in A$ tal que a ordem de $y + H$ em A/H é igual a p. Logo $py = kh$, para algum inteiro $k > 0$. Escrevendo $k = pq + r$, com $0 \leq r < p$, obtemos $r = 0$: de fato, temos que $rh = p(y - qh)$; por um lado, $p(y - qh)$ não possui ordem máxima em A já que é múltiplo de p; por outro lado, se $r \neq 0$, então $o(rh) = o(h)$ já que $\mathrm{mdc}(r, p) = 1$. Logo $p(y - qh) = 0$ e daí $y - qh \notin H$ possui ordem p. □

Lema 19.2. *Seja A p-grupo abeliano finito. Se $h \in A$ possui ordem máxima, então $H = \langle h\rangle$ é uma parcela direta de A.*

Demonstração: Por indução em n, onde $|A| = p^n$. Se $n = 1$ ou $A = H$, então A é cíclico e logo o resultado é válido. Supomos portanto $n > 1$ e que H é um subgrupo próprio de A.

Seja $a \in A \setminus H$ de ordem p (Lema 19.1). Sejam $\overline{A} = A/\langle a\rangle$, $\phi : A \to \overline{A}$ a projeção canônica e $\overline{H} = \phi(H)$. Então $H \cong \overline{H}$, pois $H \cap \langle a\rangle = \{1\}$. Assim, $\phi(h) \in \bar{A}$ possui ordem máxima e, pela hipótese de indução, $\overline{A} = \overline{H} \oplus \overline{K}$, para algum subgrupo $\overline{K}$. Tomando $K = \phi^{-1}(\overline{K})$, temos que $H \cap K = \{1\}$ e, como $|K| = p\left|\overline{K}\right|$ e $|A| = p\left|\overline{A}\right|$, segue-se que $|A| = |H|\,|K|$, ou seja, $A = H \oplus K$. □

Proposição 19.3. *Um p-grupo abeliano finito A se escreve de maneira única como uma soma direta*

$$A = H_1 \oplus H_2 \oplus \cdots \oplus H_r$$

onde cada H_i é um p-grupo cíclico com $1 < |H_i| \leq |H_{i+1}|$ para $i = 1, \ldots, r - 1$.

Demonstração: A existência de uma tal decomposição segue do Lema 19.2, aplicado repetidas vezes. A unicidade vem do fato de que podemos cancelar cada parcela de maior ordem, já que ela possui um elemento de ordem máxima em A. □

Teorema 19.4. (Decomposição primária) *Seja A um grupo abeliano finito. Então existe uma decomposição de A como soma direta de p-grupos cíclicos, onde p percorre os primos que dividem $|A|$. Tais p-grupos, a menos de isomorfismos, são unicamente determinados.*

Demonstração: Sendo A abeliano, cada p-subgrupo de Sylow de A é normal. Logo, A se escreve como soma direta dos seus subgrupos de Sylow. Agora aplicamos a Proposição 19.3 a cada um deles para obter o resultado. A unicidade se segue olhando-se os elementos de cujas ordens são potências de p máximas. □

20 O teorema de Jordan-Hölder

Tome G um grupo finito. Se G não é simples, então existe um subgrupo H *normal* em G, tal que $\{1\} \subsetneq H \subsetneq G$ Temos então uma cadeia

$$G \rhd H \rhd \{1\}.$$

Perguntamo-nos se podemos repetir esse processo, ou seja, inserir subgrupos normais não repetidos nesta cadeia; claro, se H não é simples, podemos fazer isto entre $\{1\}$ e H. Por outro lado, se G/H não é simples, então decorre do Teorema dos Homomorfismos que existe um subgrupo K de G tal que $H \underset{\neq}{\rhd} K \underset{\neq}{\rhd} G$. Sendo G finito, esse processo não pode continuar indefinidamente. Chegamos assim a uma cadeia

$$G \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n \rhd \{1\}$$

tal que cada grupo quociente G_i/G_{i+1} é um grupo simples. Isso certamente não surpreende. A surpresa vem do seguinte resultado, o Teorema de Jordan-Hölder: independentemente da maneira com que façamos essa inserção de subgrupos, sempre obteremos, a menos de reordenação, *os mesmos quocientes*, desde que prossigamos inserindo subgrupos normais até obter quocientes simples. Provar este teorema é o nosso próximo objetivo.

Seja G um grupo. Uma *série subnormal*[2] é uma sequência de subgrupos

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{1\} \tag{20.1}$$

onde cada subgrupo G_{i-1} é normal no subgrupo anterior G_i, para $i = 1, \ldots, n$. Os subgrupos G_i são chamados *termos*. Os quocientes G_{i-1}/G_i são os *fatores quocientes* (ou simplesmente fatores) da série. Se cada G_i é normal no grupo ambiente G, então a série é dita *normal*. Não pressupomos que os grupos G_i sejam distintos. Um *refinamento* de uma série subnormal é simplesmente uma nova série obtida pela inserção de subgrupos, não necessariamente distintos. Um refinamento é *próprio* se subgrupos novos foram acrescentados.

Para terminar essa longa sequência de definições, eis a última: uma série subnormal é uma *série de composição* se não admite refinamentos próprios.

Exemplo 20.1.

1. Se G é um grupo simples, então $G \rhd \{1\}$ é uma série de composição.
2. Todo grupo finito possui uma série de composição; o grupo $\mathbb{Z}$ não possui nenhuma.
3. Séries de composição não são únicas. O caso do grupo $\mathbb{Z}_{30}$ ilustra bem isso: suas possíveis séries de composição são

   $$\mathbb{Z}_{30} \rhd \langle\bar{5}\rangle \rhd \langle\bar{10}\rangle \rhd \{\bar{0}\}, \qquad \mathbb{Z}_{30} \rhd \langle\bar{3}\rangle \rhd \langle\bar{6}\rangle \rhd \{\bar{0}\}$$

   e

   $$\mathbb{Z}_{30} \rhd \langle\bar{2}\rangle \rhd \langle\bar{6}\rangle \rhd \{\bar{0}\}$$

   A primeira delas tem como fatores quocientes os grupos $\mathbb{Z}_5$, $\mathbb{Z}_2$ e $\mathbb{Z}_3$, a segunda $\mathbb{Z}_3$, $\mathbb{Z}_2$ e $\mathbb{Z}_5$ e a terceira $\mathbb{Z}_2$, $\mathbb{Z}_3$ e $\mathbb{Z}_5$, respectivamente.

[2] *subnormal* (e não *normal*, o que soaria mais natural) é para enfatizar que se $i > 1$ então o subgrupo G_i não é normal em G em geral, como é sempre tentador pressupor...não é?

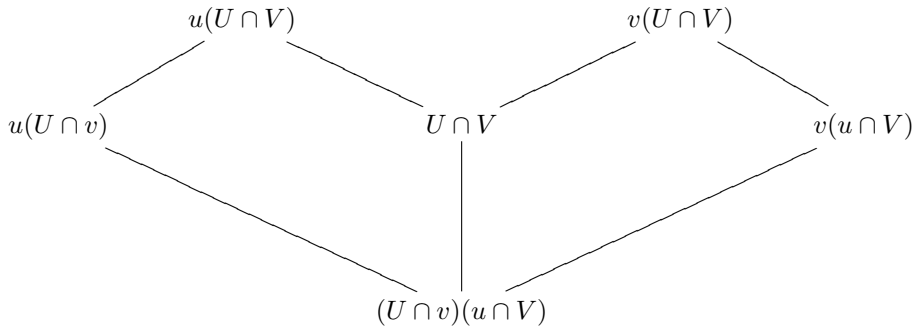
Dizemos que duas séries subnormais são *equivalentes* se os fatores não-triviais de uma série estão em bijeção com os fatores não-triviais da outra, e de forma que fatores isomorfos estejam em correspondência. No último exemplo, vimos que as duas séries de composição de $\mathbb{Z}_{30}$ apresentadas são equivalentes. Isto não foi obra do acaso: o teorema de Jordan-Hölder (Teorema 20.5) afirma que o mesmo acontece em qualquer grupo G. Este resultado notável será provado como consequência de um outro ainda mais forte: o teorema de Schreier (Teorema 20.4). Tudo começa com o seguinte lema.

Lema 20.2. (Lei modular de Dedekind) *Sejam A, B, C subgrupos de um grupo G, com $B \subseteq C$. Então $(AB) \cap C = (A \cap C)B$. Em particular, se $AB = BA$, então $\langle A, B\rangle \cap C = \langle A \cap C, B\rangle$*

Demonstração: Seja $ab \in C$, com $a \in A$ e $b \in B$. Então $a \in A \cap C$ e logo $ab \in (A \cap C)B$. Isto mostra que $(AB) \cap C \subseteq (A \cap C)B$. Para a inclusão oposta, tome $a \in A \cap C$ e $b \in B$. Como $B \subseteq C$, segue-se que $ab \in C$ e, claro, $ab \in AB$. Isto termina a prova. □

Lema 20.3. *(Zassenhaus ou Lema da Borboleta) Sejam u, U, v, V subgrupos de um grupo G, com $u \lhd U$, $v \lhd V$. Então:*

1. *$u(U \cap v) \lhd u(U \cap V)$ e $v(u \cap V) \lhd v(U \cap V)$;*
2. $\dfrac{u(U \cap V)}{u(U \cap v)} \cong \dfrac{v(U \cap V)}{v(u \cap V)} \cong \dfrac{U \cap V}{(U \cap v)(u \cap V)}$.



Demonstração:
1. Sendo $v \lhd V$, obtemos $(U \cap v) \lhd (U \cap V)$ e como $u \lhd U$, segue-se que $u(U \cap v) \lhd u(U \cap V)$. A outra asserção é provada de maneira análoga.
2. Da lei modular de Dedekind (Lema 20.2), segue que

$$u(U \cap v) \cap (U \cap V) = (u \cap V)(U \cap v)$$

e portanto de $AB/A \cong B/(A \cap B)$, aplicado quando $A = u(U \cap v)$ e $B = U \cap V$, obtemos

$$\frac{u(U \cap V)}{u(U \cap v)} \cong \frac{U \cap V}{(U \cap v)(u \cap V)}.$$

O outro isomorfismo segue de maneira similar (após trocarmos u por v nos lugares adequados) e isto termina a prova do lema. □

Teorema 20.4. *(Schreier) Duas séries subnormais quaisquer de um grupo G admitem refinamentos equivalentes.*

Demonstração: Sejam

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_m = \{1\} \qquad \text{e}$$

$$G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_n = \{1\}$$

duas séries subnormais de G. A idéia é construir um refinamento da primeira, inserindo $n-1$ termos entre cada passo, usando os termos da segunda série. Assim, no passo de índice i, o refinamento é

$$G_i = G_{i+1}(G_i \cap H_0) \rhd G_{i+1}(G_i \cap H_1) \rhd \cdots \rhd G_{i+1}(G_i \cap H_n) = G_{i+1}$$

Mutatis mutandis, construímos um refinamento para a segunda série. Cada uma das novas séries obtidas possui $mn+1$ termos. Tipicamente, os termos desses refinamentos são, respectivamente, da forma

$$\cdots \rhd G_{i+1}(G_i \cap H_j) \rhd G_{i+1}(G_i \cap H_{j+1}) \rhd \cdots$$

$$\cdots \rhd H_{j+1}(G_i \cap H_j) \rhd H_{j+1}(G_{i+1} \cap H_j) \rhd \cdots$$

O Lema 20.3 aplicado aos grupos $G_{i+1} \lhd G_i$ e $H_{j+1} \lhd H_j$, nos diz que o quociente entre os termos indicados na primeira das linhas acima é isomorfo ao quociente dos da segunda. Concluímos que os refinamentos são equivalentes. □

Teorema 20.5. (Jordan-Hölder) *Duas séries de composição de um grupo G são equivalentes.*

Demonstração: Pelo Teorema de Schreier, dadas duas séries de composição de G, elas admitem refinamentos equivalentes. Como os fatores quocientes não-triviais de uma série de composição não se alteram após um refinamento, temos o resultado. □

21 Grupos solúveis

Um grupo G é dito *solúvel* se existe uma série subnormal

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{1\} \tag{21.1}$$

tal que fator quociente G_{i-1}/G_i é abeliano, para cada $i = 1, 2, \ldots, n$. Nesse caso dizemos que a série é *solúvel*. Alguns exemplos:

1. Todo grupo abeliano G é solúvel; basta considerar a série $G \rhd 1$;
2. O grupo simétrico S_3 é solúvel: a série $S_3 \rhd \langle (1\,2\,3) \rangle \rhd \{(1)\}$ tem como fatores quocientes os grupos $\mathbb{Z}_2$ e $\mathbb{Z}_3$.
3. O grupo simétrico S_4 é solúvel: de fato,

   $$S_4 \rhd A_4 \rhd V \rhd \{(1)\}$$

   onde $V = \{(1), (12)(34), (13)(24), (14)(23)\}$ é o grupo de Klein, é uma série solúvel.
4. Todo p-grupo finito G é solúvel: se $|G| = p^n$, então existem subgrupos $P_i \lhd G$ de ordem p^i para $i = 0, 1, \ldots, n$ e portanto

   $$G = P_n \rhd P_{n-1} \rhd \cdots \rhd P_1 \rhd \{1\}$$

   é uma série solúvel cujos fatores quocientes são cíclicos de ordem prima.

Existe uma maneira elegante de lidar com grupos solúveis, que se faz com o uso do subgrupo dos comutadores.

Recorde que o subgrupo G' dos comutadores de um grupo G é, por definição, o menor subgrupo de G que contém todos os elementos da forma $xyx^{-1}y^{-1}$. Eis uma lista de propriedades que nos serão úteis:

1. G é abeliano se e somente se $G' = \{1\}$.
2. G' é normal em G; o quociente G/G' é um grupo abeliano.
3. E este é o menor subgrupo de G com esta propriedade: dado $N \lhd G$, vale

   $$G/N \text{ é abeliano } \iff G' \subset N$$

   De fato, se $G' \subset N$, então $G/N \cong (G/G')/(N/G')$, ou seja, G/N é isomorfo ao quociente de um grupo abeliano e portanto é também abeliano; reciprocamente, se G/N é abeliano, então $xyx^{-1}y^{-1}N = N$ para quaisquer x, y em G, donde concluímos $N \supset G'$.

A partir daí construímos recursivamente uma série subnormal em G: tome $G^{(0)} = G$ e para $n > 0$, defina $G^{(n)} = (G^{(n-1)})'$. Por exemplo, $G^{(1)} = G'$, $G^{(2)} = G''$, etc. Assim,

$$G = G^{(0)} \rhd G^{(1)} \rhd G^{(1)} \rhd \cdots \rhd G^{(n)} \rhd \cdots \tag{21.2}$$

Repare que cada quociente é abeliano.

É claro que se G é finito, essa cadeia é também finita e portanto estacionária, ou seja, para algum n_0 tem-se $G^{(n)} = G^{(n_0)}$ para todo $n \geq n_0$. O que ocorre é que, em alguns casos, esta cadeia é estacionária em algum grupo não trivial!

Exemplo 21.1.

1. Considere o grupo A_4 e seja V o subgrupo de Klein. Como o quociente é abeliano, vem que $V \supseteq A_4' \supsetneq \{1\}$, e a última inclusão segue do feito que A_4 não é abeliano. Assim, A_4' possui ordem 2 ou 4; porém não há subgrupos normais de ordem 2 em A_4 (elementos de ordem 2 aqui são produtos de transposições disjuntas), o que nos leva a $A_4' = V$. Em seguida, temos $A_4^{(2)} = \{1\}$, uma vez que o grupo de Klein é abeliano.

2. Como vimos A_5 é um grupo não-abeliano simples. Logo $A_5' = A_5$ e logo $A_5^{(n)} = A_5$ para todo n. Este é um exemplo onde a cadeia dos subgrupos derivados não estaciona na identidade. O mesmo ocorre para A_n para todo $n \geq 5$.

A distinção entre os dois casos do exemplo acima se dá de acordo com a solubilidade do grupo envolvido. Este é exatamente o resultado da proposição a seguir.

Proposição 21.2. *Um grupo G é solúvel se e somente se $G^{(n)} = \{1\}$ para algum inteiro n.*

Demonstração: Se $G^{(n)} = \{1\}$ para algum n, então G é solúvel, pois cada quociente $G^{(n)}/G^{(n+1)}$ é abeliano. Reciprocamente, suponha G solúvel e considere uma série

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{1\}$$

com fatores abelianos. Basta então demonstrar que $G_i \supset G^{(i)}$ para todo i, o que é feito indutivamente. Para $i = 0$ não há nada a fazer. Se a inclusão vale para $i > 0$, então como o quociente G_i/G_{i+1} é abeliano, temos

$$G_{i+1} \supset G_i' \supset G^{(i)} \implies G_{i+1} \supset G_{i+1}' \supset (G^{(i)})' = G^{(i+1)}$$

como desejado. □

Exercício 21.3. Seja N um subgrupo normal de G. O objetivo é caracterizar o subgrupo dos comutadores do quociente. Mostre que

$$(G/N)' = \{zN \mid z \in G'\}.$$

Conclua que $(G/N)' = (G'N)/N$ e que, por indução, tem-se para todo $n \geq 0$ a igualdade

$$(G/N)^{(n)} = (G^{(n)}N)/N. \tag{21.3}$$

Proposição 21.4. *Seja G um grupo.*

(a) *Se G é solúvel, todo subgrupo de G também é solúvel.*

(b) *Se G é solúvel e $N \lhd G$, então G/N é solúvel.*

(c) *Reciprocamente, dado N normal em G, se N e o quociente G/N são solúveis, então G é solúvel.*

Demonstração: É uma aplicação direta da proposição anterior e do Exercício subsequente. Para começar, suponha G solúvel. Então $G^{(n)}$ é trivial para algum n. Com isto, o item (a) se segue imediatamente. Para (b), segue-se de (21.3) que $(G/N)^{(n)}$ é trivial e, portanto, G/N é solúvel.

Para (c), suponha que N e G/N são solúveis. Então existem inteiros n, m para os quais $N^{(m)} = \{1\}$ e $(G/N)^{(n)} = \{N\}$. Decorre de (21.3) que $G^{(n)}N = N$, ou seja, que $G^{(n)} \subset N$. Daí $G^{(n+m)} = \{1\}$, o que demonstra que G é solúvel. □

A seguir uma demonstração do mesmo teorema, porém sem utilizar comutadores. É a versão anterior dessas notas, provavelmente vai desaparecer em breve.

Proposição 21.5. *Seja H um subgrupo de um grupo G. Então:*

(a) *Se G é solúvel, então H é solúvel; se H é normal em G, então G/H é solúvel.*

(b) *Reciprocamente, se H é normal em G e tanto H como G/H são solúveis, então G é solúvel.*

Demonstração: (a) Suponha que G possua uma série solúvel (20.1). Definindo $H_i := H \cap G_i$ para $i = 0, 1, \ldots, n$, então

$$H = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_n = \{1\}$$

é uma série subnormal em H. Agora, pelo teorema dos homomorfismos, cada fator H_i/H_{i+1} é isomorfo a um subgrupo de G_i/G_{i+1}, sendo portanto abeliano. Logo H é solúvel.

Suponha agora que $H \lhd G$ e seja $K_i := H \cdot G_i$ para $i = 0, \ldots, n$. Então $K_{i+1} \lhd K_i$ e logo, pela correspondência do teorema dos homomorfismos (Teorema 9.2)

$$G/H = K_0/H \rhd K_1/H \rhd K_2 \rhd \cdots \rhd K_n/H = \{1\}$$

é uma série subnormal de G/H. Mais ainda, dados $x, y \in G_i$ e $h, k \in H$, então do fato de que

$$hH = kH = H, \qquad xH = Hx, yH = Hy, \qquad \text{e} \qquad xyG_{i+1} = yxG_{i+1}$$

(pois G_i/G_{i+1} é abeliano), segue-se que

$$hxHG_{i+1} \cdot kyHG_{i+1} = kyHG_{i+1} \cdot hxHG_{i+1}$$

isto é, K_i/K_{i+1} é abeliano. Como este último quociente é isomorfo ao grupo $(K_i/H)/(K_{i+1}/H)$, deduzimos que G/H é solúvel.

(b) Suponhamos agora que H é normal em G e que tanto H como G/H são solúveis. Então, existe uma série subnormal

$$G/H = K_0/H \rhd K_1/H \rhd \cdots \rhd K_n/H = 1$$

com fatores abelianos e onde os K_i's são subgrupos de G contendo H e $K_i \lhd K_{i-1}$ (Teorema 9.2). Usando que $K_{i-1}/K_i \cong (K_{i-1}/H)/(K_i/H)$ e colando a série $G = K_0 \rhd K_1 \rhd \cdots \rhd K_n = H$ com uma série subnormal de H com fatores abelianos, obtemos uma série subnormal em G cujos fatores são abelianos. Logo G é solúvel. □

Corolário 21.6. *O produto direto $H \times N$ de dois grupos é solúvel se e somente se H e N são solúveis. Em geral, um produto semidireto $H \ltimes N$ é solúvel se e somente se H e N são solúveis.*

Demonstração: Com efeito, podemos supor que H e N são subgrupos de um grupo G, com N normal em G, $H \cap N = \{1\}$ e $G = HN$. Então, pelo teorema dos homomorfismos,

$$G/N = HN/N \cong H/(H \cap N) \cong H$$

e logo o resultado segue da Proposição 21.5. □

Nenhuma discussão sobre grupos solúveis poderia omitir o celebrado e surpreendente

Teorema 21.7 (Feit-Thompson)**.** *Todo grupo finito de ordem ímpar é solúvel.*

Demonstração: É profunda, não a faremos aqui. Veja [Robinson, Theory of Groups, Springer]. □

22 Grupos de permutações, II

Provamos aqui um resultado básico sobre grupos de permutações, com uma surpreendente aplicação para o estudo da solubilidade de equações algébricas por radicais: para $n \geq 5$, A_n é um grupo simples.

Lema 22.1. *Se $H \lhd A_5$ contém um 3-ciclo, então $H = A_5$.*

Demonstração: Eis um roteiro. Você está convidado a preencher os detalhes.

(a) Mostre que o número de 3-ciclos em S_5 é exatamente 20.

(b) Seja α um 3-ciclo, digamos $\alpha = (3\,4\,5)$. Pelo item (a), α possui exatamente 20 conjugados em S_5. Os seis elementos

$$C = \{1, \alpha, \alpha^2, (1\,2), (1\,2)\alpha, (1\,2)\alpha^2\}$$

evidentemente comutam com α e de fato são todos: isto se segue da equação

$$\#\{\text{conjugados a } \alpha \text{ em } S_5\} = (S_5 : C_{S_5}(\alpha)).$$

(c) Há três permutações pares em C; logo $(A_5 : C_{A_5}(\alpha)) = 60/3 = 20$, ou seja, o número de conjugados a α por permutações pares é 20. Conclua que todos os 3-ciclos são conjugados entre si por permutações **em** A_5 (use o item (a)).

(d) Conclua o lema.

□

Generalize o resultado anterior:

Exercício 22.2. Prove que se $n \geq 5$ e $H \lhd A_n$ contém um 3-ciclo, então $H = A_n$.

Recorde que um grupo é *simples* se seus únicos subgrupos normais são os triviais.

Teorema 22.3. *A_5 é um grupo simples.*

Demonstração: Seja $H \lhd A_5$, $H \neq \{1\}$. Então H possui uma permutação par, que podemos supor uma entre

$$\alpha = (1\,2\,3), \qquad \beta = (1\,2)(3\,4) \qquad \text{ou} \qquad \sigma = (1\,2\,3\,4\,5).$$

1. Se $\beta \in H$, então tome $\tau = (1\,2)(3\,5)$. Mostre que:

$$\tau\beta\tau^{-1} = (1\,2)(4\,5) \qquad \text{e} \qquad (\tau\beta\tau^{-1})\beta^{-1} = (3\,5\,4) \in H.$$

2. Se $\sigma \in H$, mostre que para $\tau = (1\,3\,2)$, temos

$$\tau\sigma\tau^{-1} = (3\,1\,2\,4\,5) \qquad \text{e} \qquad (\tau\sigma\tau^{-1})\sigma^{-1} = (1\,3\,4) \in H.$$

Assim, em qualquer caso, H contém um 3-ciclo. O resultado segue do Lema 22.1.

□

Observação 22.4. Uma outra prova, mais aritmética, consiste em contar as estruturas de ciclos dos tipos $(1\ 2)(3\ 4)$ e $(1\ 2\ 3\ 4\ 5)$ e usar o teorema de Lagrange. Neste mesma linha de idéias, pode-se provar que A_6 é simples. Para $n > 6$, usa-se o fato de que A_6 é simples e o Exercício 22.2. Uma prova surpreendemente curta pode ser encontrada em [Van der Waerden].

Os grupos simétricos apresentam comportamento bem distinto para $n \geq 5$: A_n é um grupo não abeliano simples, e portanto não é solúvel. Isto pode ser provado diretamente com um argumento elegante (cf. apêndice de [Artin]), que apresentamos abaixo.

Proposição 22.5. *Se $n \geq 5$, então o grupo simétrico S_n não é solúvel.*

Demonstração: Pela Proposição 21.5, basta mostrar que A_n não é solúvel. Seja H um subgrupo normal de A_n tal que A_n/H seja abeliano. Dados $x, y \in A_n$, temos

$$(xH)(yH)(x^{-1}H)(y^{-1}H) = (xH)(x^{-1}H)(yH)(y^{-1}H) = H$$

e logo $xyx^{-1}y^{-1} \in H$. Tomando $x = (abc)$ e $y = (cde)$ com a, b, c, d, e distintos, temos

$$xyx^{-1}y^{-1} = (abc)(cde)(cba)(edc) = (cad)$$

Assim, H contém todos os 3-ciclos e é portanto, pelo Lema 22.1, igual a A_n. Isto mostra que não existe uma série subnormal de A_n com fatores quocientes abelianos, ou seja, A_n não é solúvel. □