NOTAS DE AULA DE ÁLGEBRA

TIAGO MACEDO

Aula 1

Avisos:

- Livro-texto: Abstract Algebra de D. Dummit e R. Foote. (Ler e entender a Seção 0.1.)
- Provas do curso: P1 em 19/set, P2 em 31/out, P3 em 14/dez, e Exame em 30/nov.

1.1. Axiomas e exemplos básicos

Vamos começar com a definição abstrata de grupo.

Definição 1.1. Um grupo é um conjunto não-vazio G munido de uma função $m\colon G \times G \to G$ (ou seja, uma operação binária) satisfazendo as seguintes condições:

(i) m é associativa, ou seja, $m(m(a,b),c) = m(a,m(b,c))$ para todos $a,b,c \in G$.
(ii) Existe $e \in G$ tal que $m(e,g) = g = m(g,e)$ para todo $g \in G$.
(iii) Para cada $g \in G$ existe $\tilde{g} \in G$ tal que $m(g,\tilde{g}) = e = m(\tilde{g},g)$.

O elemento e é chamado de elemento neutro ou identidade de G. O elemento $\tilde{g}$ é chamado de inverso de g. Um grupo (G,m) é dito comutativo ou abeliano quando m é uma operação binária comutativa, ou seja, quando $m(g,h) = m(h,g)$ para todos $g,h \in G$. Um grupo (G,m) é dito finito quando $|G|$ (a cardinalidade do conjunto G) é finita.

Agora vamos ver alguns exemplos conhecidos de grupos.

Exemplo 1.2. Considere o conjunto dos números inteiros $\mathbb{Z} = \{\dots,-2,-1,0,1,2,\dots\}$ munido da operação binária $m\colon \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ dada por $m(a,b) = a+b$. Verifique que $(\mathbb{Z},m)$ é um grupo abeliano. (Encontre explicitamente e e $\tilde{g}$ para cada $g \in \mathbb{Z}$.)

Exemplo 1.3. Considere um espaço vetorial $(V,+,\cdot)$. Verifique que o conjunto V munido da operação binária $+\colon V\times V \to V$ é um grupo abeliano. Em particular, os conjuntos dos números racionais $\mathbb{Q}$, dos números reais $\mathbb{R}$ e dos números complexos $\mathbb{C}$ são grupos abelinos quando munidos de suas somas usuais.

Outra operação binária conhecida em $\mathbb{R}$ é a multiplicação.

Exemplo 1.4. Considere o conjunto $\mathbb{R}$ e a operação binária $m\colon \mathbb{R}\times\mathbb{R} \to \mathbb{R}$ dada por $m(a,b) = ab$. Observe que $(\mathbb{R},m)$ **não** é um grupo. Apesar de m ser associativa (verifique) e existir elemento neutro (verifique que 1 é o único elemento neutro), não existe o inverso de 0. De fato, $m(a,0) = 0$ para todo $a \in \mathbb{R}$, portanto não existe $\tilde{0} \in \mathbb{R}$ tal que $m(\tilde{0},0) = 1$.

Vamos tentar corrigir o (não-)exemplo anterior.

Exemplo 1.5. Considere o conjunto $\mathbb{R}\setminus\{0\}$ e a operação binária $m\colon \mathbb{R}\setminus\{0\}\times\mathbb{R}\setminus\{0\} \to \mathbb{R}\setminus\{0\}$ dada por $m(a,b) = ab$. Observe que m está bem definida, pois $ab = 0$ se, e somente se, $a = 0$ ou $b = 0$. Verifique que $(\mathbb{R}\setminus\{0\},m)$ é um grupo abeliano.

Exemplo 1.6. Considere o conjunto $\mathbb{Z}\setminus\{0\}$ e a operação binária $m\colon \mathbb{Z}\setminus\{0\}\times\mathbb{Z}\setminus\{0\} \to \mathbb{Z}\setminus\{0\}$ dada por $m(a,b) = ab$. Verifique que m está bem definida, é associativa, e 1 é o único elemento neutro de $\mathbb{Z}\setminus\{0\}$. Mas $(\mathbb{Z}\setminus\{0\},m)$ **não** é um grupo, pois, se $g \notin \{-1,1\}$, então não existe $\tilde{g} \in \mathbb{Z}\setminus\{0\}$ tal que $g\tilde{g} = 1$.

Nós podemos corrigir o (não-)exemplo anterior de duas formas. A primeira é incluir todos os inversos dos números inteiros não-nulos e todos os produtos entre números inteiros e inversos de inteiros não-nulos (ou seja, todos os números racionais).

Exemplo 1.7. Considere o conjunto $\mathbb{Q}\setminus\{0\}$ e a operação binária $m\colon \mathbb{Q}\setminus\{0\}\times\mathbb{Q}\setminus\{0\}\to\mathbb{Q}\setminus\{0\}$ dada por $m(a,b)=ab$. Verifique que $(\mathbb{Q}\setminus\{0\},m)$ é um grupo abeliano.

A segunda é excluir todos os inteiros não-nulos que não têm inversos multiplicativos.

Exemplo 1.8. Considere o conjunto $G=\{-1,1\}$ e a operação binária $m\colon G\times G\to G$ dada por $m(a,b)=ab$. Verifique que m está bem definida e que (G,m) é um grupo abeliano finito.

Pelo Exemplo 1.3, o conjunto de matrizes n por n com entradas reais, $M_n(\mathbb{R})$ é um grupo abeliano quando munido da soma usual de matrizes. Outra operação binária bem conhecida em $M_n(\mathbb{R})$ é o produto de matrizes.

Exemplo 1.9. Observe que $M_n(\mathbb{R})$ munido do produto usual de matrizes **não** é um grupo. De fato, apesar do produto ser associativo e da matriz identidade ser um elemento neutro para essa operação, nem todas as matrizes têm inversos multiplicativos (por exemplo, a matriz nula). Então denote por $GL_n(\mathbb{R})$ o conjunto de matrizes invertíveis de $M_n(\mathbb{R})$ e considere a operação binária $m\colon GL_n(\mathbb{R})\times GL_n(\mathbb{R})\to GL_n(\mathbb{R})$ dada por $m(A,B)=AB$. Verifique que $(GL_n(\mathbb{R}),m)$ é um grupo e que esse grupo **não** é abeliano.

Proposição 1.10. *Seja (G,m) um grupo.*

(a) Existe um único elemento neutro em G.
(b) Para cada $g\in G$ existe um único elemento inverso.
(c) Para todo $g\in G$ o elemento inverso de $\tilde{g}$ (o inverso de g) é g.
(d) Para todos $g,h\in G$, $\widetilde{m(g,h)}=m(\tilde{h},\tilde{g})$.
(e) Dados $a,b\in G$, existe um único $x\in G$ tal que $m(a,x)=b$.
(f) Dados $a,b\in G$, existe um único $x\in G$ tal que $m(x,a)=b$.
(g) Se $a,b,c\in G$ são tais que $m(a,b)=m(a,c)$, então $b=c$.
(h) Se $a,b,c\in G$ são tais que $m(b,a)=m(c,a)$, então $b=c$.

Demonstração. (a) Pela Definição 1.1(ii), existe pelo menos um elemento neutro em G. Suponha que $e,e'\in G$ sejam tais que $m(e,g)=g=m(g,e)$ e $m(e',g)=g=m(g,e')$ para todo $g\in G$. Então temos que $e=m(e,e')=e'$. Isso mostra a unicidade do elemento neutro.

(b) Pela Definição 1.1(iii), para cada $g\in G$, existe pelo menos um elemento inverso para g. Suponha que $\tilde{g},\tilde{g}'\in G$ sejam tais que $m(g,\tilde{g})=e=m(\tilde{g},g)$ e $m(g,\tilde{g}')=e=m(\tilde{g}',g)$. Então temos que $\tilde{g}=m(\tilde{g},e)=m(\tilde{g},m(g,\tilde{g}'))=m(m(\tilde{g},g),\tilde{g}')=m(e,\tilde{g}')=\tilde{g}'$. Isso mostra a unicidade do inverso de g.

(c) Fixe $g\in G$. Pela Definição 1.1(iii) e item (b), o inverso de $\tilde{g}$ é o único $x\in G$ que satisfaz $m(\tilde{g},x)=e=m(x,\tilde{g})$. Também pela Definição 1.1(iii), $\tilde{g}$ satisfaz $m(g,\tilde{g})=e=m(\tilde{g},g)$. Ou seja, g é o (único) inverso de $\tilde{g}$.

(d) Fixe $g,h\in G$. Pela Definição 1.1(iii) e item (b), o inverso de $m(g,h)$ é o único $x\in G$ que satisfaz $m(m(g,h),x)=e=m(x,m(g,h))$. Vamos mostrar que $x=m(\tilde{h},\tilde{g})$ satisfaz essas equações.

$$\begin{aligned} m(m(g,h),m(\tilde{h},\tilde{g})) &= m(m(m(g,h),\tilde{h}),\tilde{g}) \\ &= m(m(g,m(h,\tilde{h})),\tilde{g}) \\ &= m(m(g,e),\tilde{g}) \\ &= m(g,\tilde{g}) \\ &= e, \end{aligned} \qquad \begin{aligned} m(m(\tilde{h},\tilde{g}),m(g,h)) &= m(m(m(\tilde{h},\tilde{g}),g),h) \\ &= m(m(\tilde{h},m(\tilde{g},g)),h) \\ &= m(m(\tilde{h},e),h) \\ &= m(\tilde{h},h) \\ &= e. \end{aligned}$$

(e) Observe que, se $m(a,x)=b$, então $m(\tilde{a},b)=m(\tilde{a},m(a,x))=m(m(\tilde{a},a),x)=m(e,x)=x$. Por outro lado, $m(a,m(\tilde{a},b))=m(m(a,\tilde{a}),b)=m(e,b)=b$. Como $m(\tilde{a},b)\in G$ e $\tilde{a}$ é único, então $x=m(\tilde{a},b)$ é o único elemento de G que satisfaz $m(a,x)=b$.
(f) Similar à do item (e).
(g) Segue do item (e) substituindo x por b e b por $m(a,c)$.
(h) Segue do item (f) substituindo x por b e b por $m(c,a)$. □

Observação 1.11. A definição de grupo é completamente abstrata. Ou seja, um grupo é um conjunto não-vazio qualquer, munido de uma operação binária qualquer, desde que essa operação binária satisfaça as condições (i)-(iii) da Definição 1.1. Em particular, podemos criar um grupo a partir de um conjunto $G\neq\emptyset$ qualquer, se especificarmos toda uma *tabela de multiplicação*

G	e	g	h	$\cdots$
e	e	g	h	$\cdots$
g	g	?	??	$\cdots$
h	h	???		
$\vdots$	$\vdots$	$\vdots$		

satisfazendo as condições (i)-(iii).

Além disso, é fácil ver que existe uma quantidade enorme de grupos (não só os que nós exemplificamos acima). Portanto um problema interessante seria descrever todos os possíveis grupos que existem e classificá-los.

Aula 2

Avisos: A página da disciplina é http://ict.unifesp.br/tmacedo/algebra, e ela vai conter a ementa da disciplina e notas de aula.

Notação 2.1. Dado um grupo (G, m), a partir de agora, vamos denotar:

- $m(g, , h)$ por gh para quaisquer $g, h \in G$,
- $gg \cdots g$ (k vezes) por g^k para quaisquer $g \in G$ e $k > 0$,
- $\tilde{g}$ por g^{-1} para qualquer $g \in G$,
- $g^{-1}g^{-1} \cdots g^{-1}$ (k vezes) por g^{-k} para quaisquer $g \in G$ e $k > 0$,
- g^0 por e para qualquer $g \in G$.

Além disso, quando não gerar confusão, nós vamos omitir a operação binária m e denotar o grupo (G, m) simplesmente por G.

Exemplo 2.2. O conjunto com um único elemento $\{e\}$ munido da única operação binária $m\colon \{e\} \times \{e\} \to \{e\}$ (dada por $m(e, e) = e$) é um grupo (abeliano). Esse grupo é chamado de grupo trivial.

Exercício 2.3. Dado um grupo G, mostre que $e^k = e$ para todo $k \in \mathbb{Z}$. (Sugestão: mostre que $e^{-1} = e$ e use indução duas vezes, para $k > 0$ e para $k < 0$.)

Definição 2.4. Dados um grupo G, definimos a ordem de G como $|G|$. Dado um elemento $g \in G$, definimos a ordem de g como o menor inteiro positivo o tal que $g^o = e$, se tal inteiro existir; e como infinito, se tal inteiro não existir. Denote a ordem de g em G por $|g|$ ou por $o(g)$.

Exemplo 2.5. Considere o conjunto $\mathbb{C}\backslash\{0\}$ munido da operação binária dada pela multiplicação usual de números complexos. Verifique que $(\mathbb{C}\backslash\{0\}, \cdot)$ é um grupo abeliano, cujo elemento neutro é 1 e o elemento inverso de $z \in \mathbb{C} \setminus \{0\}$ é $z^{-1} = \frac{\overline{z}}{\|z\|}$.

Se $z = e^{\frac{\pi}{3}}$, a raiz sexta primitiva da unidade, então $o(z) = 6$. De fato,

$$z^2 = e^{\frac{2\pi}{3}} \neq 1, \quad z^3 = e^{\pi} \neq 1, \quad z^4 = e^{\frac{4\pi}{3}} \neq 1, \quad z^5 = e^{\frac{5\pi}{3}} \neq 1 \quad \text{e} \quad z^6 = e^{2\pi} = 1.$$

Verifique também que $o\left(e^{\pi}\right) = 2$, $o\left(e^{\frac{2\pi}{3}}\right) = o\left(e^{\frac{4\pi}{3}}\right) = 3$ e $o\left(e^{\frac{5\pi}{3}}\right) = 6$.

Exemplo 2.6. Considere o grupo abeliano $(\mathbb{Z}, +)$. Observe que a ordem do elemento 0 é 1. Além disso, a ordem de todo elemento $n \neq 0$ é infinita. De fato, se a ordem de n fosse $k > 0$, então teríamos que $kn = 0$. Como $n \neq 0$ e $k \neq 0$, isso é impossível.

A seguir, nós vamos dar outros exemplos de grupos e, em particular, calcular as ordens de alguns de seus elementos.

0.3. Inteiros módulo n

Durante toda essa seção, fixe um inteiro positivo n. Considere o conjunto $\mathbb{Z}_n$ formado pelos símbolos $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Para definir a operação binária $m\colon \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$, vamos explicar o que esses símbolos representam.

Considere a relação no conjunto $\mathbb{Z}$ dada por

$$a \sim b \qquad \text{se, e somente se,} \qquad n \text{ divide } a - b \quad (\text{denotado } n|(a-b)).$$

Observe que essa é uma relação de equivalência. De fato:

- Para todo $a \in \mathbb{Z}$, temos que $a \sim a$, pois $n|0 = a - a$;
- Se $a, b \in \mathbb{Z}$ e $a \sim b$, ou seja, $n|(a-b)$, então $n|(b-a)$, ou seja, $b \sim a$;

- Se $a, b, c \in \mathbb{Z}$, $a \sim b$ e $b \sim c$, isso significa que existem $k, \ell \in \mathbb{Z}$ tais que $kn = (a - b)$ e $\ell n = (b - c)$. Então temos que $(a - c) = (a - b) + (b - c) = kn + \ell n = (k + l)n$, ou seja, $n|(a - c)$. Portanto $a \sim c$.

As classes de equivalência desta relação $\sim$ (ou seja, os subconjuntos disjuntos de $\mathbb{Z}$ dentro dos quais todos os elementos são equivalentes entre si) serão denotados por $\overline{k}$ ($k \in \mathbb{Z}$). Observe que essas classes de equivalência podem ser representadas pelos restos das divisões dos inteiros por n. De fato, se $k \in \mathbb{Z}$ for escrito como $k = qn + r$ (onde q é o quociente e r é o resto da divisão), então $(k - r) = qn$, ou seja, $k \sim r$, ou equivalentemente, $\overline{k} = \overline{r}$. Como $0 \leq r < n$ e n não divide $a - b$ quando $a, b \in \{0, \ldots, n - 1\}$, então o conjunto $\mathbb{Z}_n$ é formado exatamente pelas classes de equivalência dos inteiros pela relação $\sim$.

Agora defina uma operação binária $m\colon \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ da seguinte forma $m(\overline{a}, \overline{b}) = \overline{(a + b)}$. Primeiro, vamos verificar que m está bem definida (ou seja, que ela não depende dos representantes que nós pegamos para $\overline{a}$ e $\overline{b}$). Lembre que os elementos da classe de equivalência $\overline{a}$ (respectivamente, $\overline{b}$) são da forma $a + nz$ (resp. $b + nz$) para algum $z \in \mathbb{Z}$. Para quaisquer $z, w \in \mathbb{Z}$, pela definição, temos que $m(\overline{a + nz}, \overline{b + nw}) = \overline{(a + b + n(z + w))} = \overline{(a + b)} = m(\overline{a}, \overline{b})$. Portanto m está bem definida.

Exercício 2.7. Verifique que $(\mathbb{Z}_n, m)$ é um grupo abeliano (finito). Além disso, mostre que

$$o(\overline{k}) = \frac{\operatorname{mmc}(k, n)}{k} = \frac{n}{\operatorname{mdc}(k, n)} \qquad \text{para todo } k \in \{1, \ldots, n - 1\}.$$

1.3. Grupos simétricos

Para cada $n > 0$, denote por S_n o conjunto formado por todas as permutações (ou seja, todas as bijeções) do conjunto $X = \{1, \ldots, n\}$. Defina uma operação binária $m\colon S_n \times S_n \to S_n$ da seguinte forma $m(f, g) = f \circ g$ (a composição das funções f e g). Vamos verificar que $(S_n, \circ)$ é um grupo.

(i) $m(m(f, g), h)$ e $m(f, m(g, h))$ são bijeções do conjunto $\{1, \ldots, n\}$, então para compará-las, vamos aplicá-las nos elementos de $\{1, \ldots, n\}$. Para cada $x \in \{1, \ldots, n\}$, temos:

$$\begin{aligned} m(m(f, g), h)(x) &= (m(f, g) \circ h)(x) & m(f, m(g, h))(x) &= (f \circ m(g, h))(x) \\ &= ((f \circ g) \circ h)(x) & &= (f \circ (g \circ h))(x) \\ &= (f \circ g)(h(x)) & &= f((g \circ h)(x)) \\ &= f(g(h(x))), & &= f(g(h(x))). \end{aligned}$$

(ii) A função identidade $\mathrm{id}_X\colon X \to X$ dada por $\mathrm{id}_X(x) = x$ para todo $x \in \{1, \ldots, n\}$ é uma permutação. Além disso, temos que $m(f, \mathrm{id}_X) = f \circ \mathrm{id}_X = f = \mathrm{id}_X \circ f = m(\mathrm{id}_X, f)$ para toda $f \in S_n$. Portanto id_X é o (único) elemento neutro de $(S_n, \circ)$.

(iii) Para cada permutação (uma bijeção) σ do conjunto $\{1, \ldots, n\}$, existe uma função inversa, denotada $\sigma^{-1}\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$. Pela definição, a função inversa de σ é aquela que satisfaz $\sigma \circ \sigma^{-1} = \mathrm{id}_X = \sigma^{-1} \circ \sigma$. Portanto σ^{-1} é exatamente o elemento inverso de σ em $(S_n, \circ)$, um 2-ciclo.

Agora vamos introduzir uma notação para lidar com os elementos de S_n. Fixe $\sigma \in S_n$. Primeiro, verifique que, para cada $x \in \{1, \ldots, n\}$ existe $k \leq n$ (que depende de σ e x) tal que $\sigma^k(x) = x$. (Use o fato de que σ é uma bijeção e que $\{1, \ldots, n\}$ é um conjunto finito.) Em particular, tome o menor $k \leq n$ tal que $\sigma(1) = 1$. Se $k = n$, então denotamos σ por $(1\ \sigma(1)\ \ldots\ \sigma^{n-1}(1))$. Se $k < n$, então $\{1, \sigma(1), \ldots, \sigma^{k-1}(1)\} \subsetneq \{1, \ldots, n\}$. Tome o menor $i \in \{1, \ldots, n\} \setminus \{1, \sigma(1), \ldots, \sigma^{k-1}(1)\}$ e o menor $\ell \leq n$ tal que $\sigma^\ell(i) = i$. Se $k + \ell = n$, então

denotamos σ por $(i\ \sigma(i)\ \dots\ \sigma^{\ell-1}(i))(1\ \sigma(1)\ \dots\ \sigma^{k-1}(1))$. Caso contrário, repita esse processo até esgotar todos os elementos de $\{1,\dots,n\}$.

Os termos da forma $(i\ \sigma(i)\ \dots\ \sigma^{p}(i))$ são chamados de p-ciclos. Caso existam 1-ciclos na decomposição de σ, eles são cancelados (exceto se $\sigma = \mathrm{id}_X$). Por exemplo, se $\sigma = \mathrm{id}_{\{1,\dots,n\}}$, então nós teríamos $\sigma = (n)(n-1)\dots(2)(1)$, e nesse caso, nós denotamos σ simplesmente por (1).

Exemplo 2.8. Considere S_2, o conjunto de permutações do conjunto $X = \{1,2\}$. Observe que as únicas permutações de $\{1,2\}$ são: id_X e $\sigma\colon \{1,2\} \to \{1,2\}$ dada por $\sigma(1) = 2$ e $\sigma(2) = 1$. Portanto $|S_2| = 2$. Além disso, observe que $\sigma^2 = \mathrm{id}_X$, ou seja, $o(\sigma) = 2$. Usando a notação acima, denotamos id_X por (1) e σ por $(1\ 2)$.

Exemplo 2.9. Considere S_3, o conjunto de permutações do conjunto $X = \{1,2,3\}$. Usando a notação acima, observe que as permutações de $\{1,2,3\}$ são as seguintes:

$$\begin{array}{rcl} \mathrm{id}_X = (1)\colon X & \to & X \\ 1 & \mapsto & 1 \\ 2 & \mapsto & 2 \\ 3 & \mapsto & 3 \end{array} \qquad \begin{array}{rcl} (1\ 2)\colon X & \to & X \\ 1 & \mapsto & 2 \\ 2 & \mapsto & 1 \\ 3 & \mapsto & 3 \end{array} \qquad \begin{array}{rcl} (1\ 3)\colon X & \to & X \\ 1 & \mapsto & 3 \\ 2 & \mapsto & 2 \\ 3 & \mapsto & 1 \end{array}$$

$$\begin{array}{rcl} (2\ 3)\colon X & \to & X \\ 1 & \mapsto & 1 \\ 2 & \mapsto & 3 \\ 3 & \mapsto & 2 \end{array} \qquad \begin{array}{rcl} (1\ 2\ 3)\colon X & \to & X \\ 1 & \mapsto & 2 \\ 2 & \mapsto & 3 \\ 3 & \mapsto & 1 \end{array} \qquad \begin{array}{rcl} (1\ 3\ 2)\colon X & \to & X \\ 1 & \mapsto & 3 \\ 2 & \mapsto & 1 \\ 3 & \mapsto & 2 \end{array}$$

Em particular, observe que $|S_3| = 6$. Para calcular a multiplicação entre desses elementos, basta ler os elementos como funções (da direita para a esquerda), seguindo o caminho que cada $x \in \{1,2,3\}$ faz. Por exemplo, $(1\ 2) \circ (1\ 3) = (1\ 3\ 2)$. Em particular, observe que os 2-ciclos $(1\ 2)$, $(1\ 3)$, $(2\ 3)$ tem ordem 2, e os 3-ciclos $(1\ 2\ 3)$, $(1\ 3\ 2)$ tem ordem 3. Além disso, observe que esse grupo não é comutativo. De fato $(1\ 2) \circ (1\ 3) = (1\ 3\ 2)$ e $(1\ 3) \circ (1\ 2) = (1\ 2\ 3)$.

Exercício 2.10. Mostre que $|S_n| = n!$ e que a ordem de todo p-ciclo é p.

Aula 3

Exercício 3.1. Dado um grupo G, mostre que, se $|G| \leq 5$, então G é abeliano.

1.5. Grupo dos quatérnios

Considere o conjunto $\mathbb{H}$ (ou Q_8) formado pelos símbolos $\{1, -1,\ i, -i,\ j, -j,\ k, -k\}$. Defina $m\colon \mathbb{H} \times \mathbb{H} \to \mathbb{H}$ como sendo a única operação binária tal que $(\mathbb{H}, m)$ é um grupo e que satisfaz:

$$m(1,h) = m(h,1) = h \quad \text{para todo } h \in \mathbb{H},$$
$$m(-1,-1) = 1, \qquad m(i,i) = m(j,j) = m(k,k) = -1,$$
$$m(-1,i) = m(i,-1) = -i, \quad m(-1,j) = m(j,-1) = -j, \quad m(-1,k) = m(k,-1) = -k,$$
$$m(i,j) = -m(j,i) = k, \quad m(j,k) = -m(k,j) = i, \quad m(k,i) = -m(i,k) = j.$$

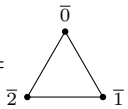
Observe que $\mathbb{H}$ é um grupo finito, $|\mathbb{H}| = 8$, e que não é abeliano. Observe também que $o(1) = 1$, $o(-1) = 2$ e $o(\pm i) = o(\pm j) = o(\pm k) = 4$.

1.2. Grupos diedrais

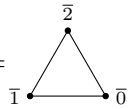
Para cada $n > 2$, denote por D_{2n} o conjunto formado por todas as simetrias de um n-ágono regular Δ_n (movimentos rígidos no espaço, ou seja, composições de translações, rotações e reflexões, que preservam Δ_n). Como toda simetria de Δ_n é uma função $f\colon \Delta_n \to \Delta_n$, defina a operação binária $m\colon D_{2n} \times D_{2n} \to D_{2n}$ como $m(f,g) = f \circ g$, a composição dessas funções.

Vamos verificar que $(D_{2n}, \circ)$ é um grupo. Primeiro, observe que a composição de duas simetrias de Δ_n é uma simetria de Δ_n. Depois, lembre que a composição de funções é associativa (veja, por exemplo, a verificação da associatividade para o grupo simétrico). Agora observe que a função identidade id_{Δ_n} é uma simetria de Δ_n e satisfaz $\mathrm{id}_{\Delta_n} \circ \sigma = \sigma = \sigma \circ \mathrm{id}_{\Delta_n}$ para todo $\sigma \in D_{2n}$. Finalmente, observe que toda translação, rotação e reflexão é invertível, portanto todo movimento rígido σ que preserva Δ_n admite uma inversa, ou seja, uma função σ^{-1} satisfazendo $\sigma \circ \sigma^{-1} = \mathrm{id}_{\Delta_n} = \sigma^{-1} \circ \sigma$, e que σ^{-1} também preserva Δ_n.

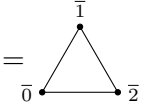
Exemplo 3.2. Considere o grupo D_6 de simetrias de um triângulo equilátero Δ_3. Para descrever as simetrias de Δ_3, vamos enumerar seus vértices com inteiros módulo 3:

$\Delta_3 \ =$ 

Observe que a rotação (no sentido horário) em torno do centro de Δ_3 de um ângulo de $2\pi/3$ (ou $120°$), é uma simetria de Δ_3. De fato, se denotarmos essa rotação por r, teremos:

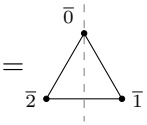
$r\,(\Delta_3) \ =$ 

Observe ainda que $r^2 = (r \circ r)$ é a rotação de um ângulo de $4\pi/3$ (no sentido horário em torno do centro) de Δ_3,

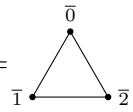
$r^2\,(\Delta_3) \ =$ 

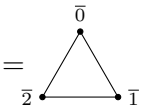
e que r^3 é a rotação de um ângulo de 2π, ou seja, $r^3 = \mathrm{id}_{\Delta_3}$. Com isso, concluímos que $o(r) = 3$.

Observe também que a reflexão de Δ_3 em relação à reta que passa pelo vértice $\overline{0}$ e pelo centro de Δ_3,

$\Delta_3 \;=$ 

é uma outra simetria de Δ_3. De fato, se denotarmos essa reflexão por s, teremos:

$s\,(\Delta_3) \;=$ 

$s^2\,(\Delta_3) \;=$ 

Como s troca a ordem dos vértices (no sentido horário, de $\overline{0}\ \overline{1}\ \overline{2}$ para $\overline{0}\ \overline{2}\ \overline{1}$), mas id_{Δ_3}, r e r^2 não invertem, é fácil concluir que $s \notin \{\mathrm{id}_{\Delta_3}, r, r^2\}$. Além disso, $o(s) = 2$.

De fato, a disposição dos vértices é uma forma de identificar as simetrias de Δ_3, pois toda simetria de Δ_3 pode ser unívocamente identificada com uma permutação do conjunto $\{\overline{0}, \overline{1}, \overline{2}\}$. Por exemplo, r pode ser identificada com a permutação $(\overline{0}\ \overline{2}\ \overline{1})$, r^2 pode ser identificada com a permutação $(\overline{0}\ \overline{1}\ \overline{2})$ e s pode ser identificada com a permutação $(\overline{1}\ \overline{2})$. Verifique que, identificando os elementos de D_6 com permutações em S_3, podemos concluir que $\mathrm{id}_{\Delta_3}, r, r^2, s, sr, sr^2$ são elementos distintos. Isso implica que $|D_6| \geq 6$.

Além disso, como toda simetria é um movimento rígido, um elemento $\sigma \in D_6$ é unicamente determinado pela permutação induzida dos vértices de Δ_3. Consequentemente, $|D_6| \leq |S_3| = 6$. Juntando essas duas desigualdades, concluímos que $|D_6| = 6$ e que as simetrias de Δ_3 são $\{\mathrm{id}_{\Delta_3}, r, r^2, s, sr, sr^2\}$. Em particular, todas as outras possíveis simetrias se identificam com uma dessas. Por exemplo, $rs = sr^2$, $srs = r^2$ e $r^2 s = sr$.

Voltando ao caso geral, vamos mostrar que $|D_{2n}| = 2n$ e vamos descrever todos as simetrias de Δ_n. Primeiro, enumere os vértices de um n-ágono regular Δ_n no sentindo horário com os inteiros módulo n. Denote por r a simetria que rotaciona Δ_n de um ângulo de $2\pi/n$ no sentido horário e por s a reflexão em relação a reta que passa pelo vértice $\overline{0}$ e pelo centro de Δ_n. Assim como no caso $n = 3$, toda simetria de Δ_n pode ser unívocamente identificada com uma permutação do conjunto $\mathbb{Z}_n$. (Ou seja, podemos definir uma função $\vartheta\colon D_{2n} \to S_n$.) Em particular, r se identifica com a permutação $(\overline{0}\ \ \overline{n-1}\ \ \cdots\ \ \overline{1})$; se n for par, s se identifica com a permutação $(\overline{1}\ \ \overline{-1})(\overline{2}\ \ \overline{-2})\cdots(\overline{\frac{n}{2}-1}\ \ \overline{\frac{n}{2}+1})$, e se n for ímpar, s se identifica com a permutação $(\overline{1}\ \ \overline{-1})(\overline{2}\ \ \overline{-2})\cdots(\overline{\frac{n-1}{2}}\ \ \overline{\frac{n+1}{2}})$.

Além disso, como toda simetria é um movimento rígido, todo elemento em D_{2n} é unicamente determinado pela permutação de $\mathbb{Z}_n$ ao qual ele está associado. (Ou seja, a função ϑ é injetora.) Verifique que, para cada $i \in \{1, \ldots, n\}$, r^i pode ser identificada com a permutação $(\overline{0}\ \ \overline{-i}\ \ \overline{-2i}\ \ \cdots\ \ \overline{i})$. Use esse fato para concluir que $o(r) = n$ e que $\mathrm{id}_{\Delta_n}, r, \ldots, r^{n-1}$ são todas simetrias distintas. Verifique também que $o(s) = 2$ e que, para cada $i \in \{1, \ldots, n\}$, sr^i pode ser identificada com a permutação $(\overline{0}\ \ \overline{i}\ \ \overline{2i}\ \ \cdots\ \ \overline{-i})$. Use esses fatos (e o fato de s trocar a ordem dos vértices de Δ_n e r não trocar) para concluir que $\mathrm{id}_{\Delta_n}, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}$ são todos elementos distintos de Δ_n. Com isso, concluímos que $|D_{2n}| \geq 2n$.

Agora observe que, como toda simetria é um movimento rígido, se dois vértices são adjacentes, então suas imagens pela simetria devem continuar adjacentes. Em particular, se soubermos as imagens dos vértices $\overline{0}$ e $\overline{1}$ (que devem ser adjacentes), podemos determinar unicamente as imagens de todos os outros vértices. De fato, se $\sigma(\overline{0}) = \overline{i}$, então $\sigma(\overline{1}) \in \{\overline{i-1},\ \overline{i+1}\}$. Se $\sigma(\overline{1}) = \overline{i+1}$ (resp. $\sigma(\overline{1}) = \overline{i-1}$), como $\sigma(\overline{2})$ deve ser adjacente a $\sigma(\overline{1})$ e $\overline{i} = \sigma(\overline{0})$, então $\sigma(\overline{2}) = \overline{i+2}$ (resp. $\sigma(\overline{2}) = \overline{i-2}$). Usando esse mesmo argumento, verifique que $\sigma(\overline{k}) = \overline{i+k}$ (resp. $\sigma(\overline{k}) =$

$\overline{i-k}$) para todo $\overline{k} \in \mathbb{Z}_n$. Com isso, concluímos que existem n possibilidades para escolhermos $\sigma(\overline{0})$ e 2 possibilidades para escolhermos $\sigma(\overline{1})$ (os outros seguem como consequência), ou seja, $|D_{2n}| \leq 2n$.

Juntando essas duas desigualdades, concluímos que $|D_{2n}| = 2n$ e que

$$D_{2n} = \{\mathrm{id}_{\Delta_n}, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}.$$

Exercício 3.3. Escreva o elemento $rsrsrsrs$ em termos de $\mathrm{id}_{\Delta_n}, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}$.

Geradores e relações

Da discussão acima, nós observamos que todos os elementos de D_{2n} podem ser obtidos como produtos finitos dos elementos r e s. Por isso, dizemos que D_{2n} é gerado por $\{r, s\}$, ou que r, s são geradores de D_{2n}. Mas nem todos os produtos de r com s são distintos. Por exemplo, nós vimos que $r^2 = s^n = \mathrm{id}_{\Delta_n}$. Essas identidades são chamadas de relações. Todo grupo pode ser descrito através de um conjunto de geradores satisfazendo um conjunto de relações. (Esse não é um resultado imediato.) Uma descrição de um grupo G dessa forma,

$$G = \langle \text{geradores} \mid \text{relações} \rangle$$

é chamada de presentação de G.

A presentação de um grupo, em geral, não é única. Mas, dada uma presentação de um grupo G, deve ser possível escrever todos os elementos de G como produtos finitos dos elementos do conjunto de geradores, e deduzir todas as relações entre elementos de G a partir do conjunto de relações.

Exemplo 3.4. Uma presentação de D_{2n} é $\langle r, s \mid r^2 = s^n = e, sr = rs^{-1} \rangle$.

Exemplo 3.5. Uma presentação de $(\mathbb{Z}, +)$ é $\langle 1 \mid \emptyset \rangle$, ou simplesmente $\langle 1 \rangle$.

Exemplo 3.6. Uma presentação de $\mathbb{Z}_n$ é $\langle \overline{1} \mid n\overline{1} = \overline{0} \rangle$.

Exemplo 3.7. Uma presentação de $\mathbb{H} = Q_8$ é $\langle i, j \mid i^4 = 1, i^2 = j^2, iji = j \rangle$.

Exemplo 3.8. Uma presentação de S_n é

$$\langle s_1, \ldots, s_{n-1} \mid s_i^2 = e,\ (s_i s_{i+1})^3 = e,\ s_i s_j = s_j s_i\ (j \neq i \pm 1) \rangle.$$

Aula 4

1.6. Homomorfismos e isomorfimos

Definição 4.1. Sejam (G, m_G) e (H, m_H) dois grupos. Um homomorfismo de grupos de G para H é uma função $f\colon G \to H$ satisfazendo:

$$f(m_G(g_1, g_2)) = m_H(f(g_1), f(g_2)) \quad \text{para todos } g_1, g_2 \in G.$$

Um isomorfismo de grupos é um homomorfismo de grupos que é bijetor. Dizemos que o grupo G é isomorfo ao grupo H quando existe algum isomorfismo de grupos $f\colon G \to H$. Neste caso, denotamos $G \cong H$.

Um homomorfismo entre dois grupos é uma função que preserva a estrutura importante que esses conjuntos têm, a de grupo. Quando existe um isomorfismo entre dois grupos, isso significa que a estrutura de grupo de um pode ser transferida para o outro sem perder informação. Ou seja, quando dois grupos são isomorfos, eles são, de certa forma, idênticos. O próximo resultado mostra algumas evidências disso.

Lema 4.2. *Sejam G e H dois grupos.*

(a) Se $f\colon G \to H$ é um homomorfismo de grupos, então $f(g^n) = f(g)^n$ para todo $n \in \mathbb{Z}$. Em particular, $f(e_G) = e_H$ e $f(g^{-1}) = f(g)^{-1}$ para todo $g \in G$.
(b) Se $G \cong H$, então $|G| = |H|$ (os dois conjuntos têm a mesma cardinalidade).
(c) Se $G \cong H$ e G é abeliano, então H é abeliano.
(d) Se $f \cong G \to H$ for um isomorfismo, então $o(f(g)) = o(g)$ para todo $g \in G$.

Demonstração. (a) Fixe $g \in G$. Vamos usar indução para $n > 0$. O caso $n = 1$ é óbvio, então suponha que $f(g^{n-1}) = f(g)^{n-1}$. Como f é um homomorfismo de grupos, pela hipótese de indução, nós temos que

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

Isso prova o caso $n > 0$. Para $n = 0$, temos que

$$f(g) = f(ge_G) = f(g)f(e_G)$$

para qualquer $g \in G$. Da Proposição 1.10(e), segue que $f(e_G) = e_H$.

Para $n = -1$, observe que $f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$ e $f(g^{-1})f(g) = f(g^{-1}g) = f(e_G) = e_H$. Portanto $f(g^{-1})$ é o inverso de $f(g)$. Para completar a demonstração, use indução para $n < 0$.

(b) Se $G \cong H$, então exite um isomorfismo $f\colon G \to H$. Em particular, f é uma bijeção entre os conjuntos G e H. Portanto $|G| = |H|$.

(c) Seja $f\colon G \to H$ um isomorfismo. Em particular, f é sobrejetora, ou seja, para cada $h \in H$, existe $g \in G$ tal que $f(g) = h$. Dados $h_1, h_2 \in H$, tome $g_1, g_2 \in G$ tais que $f(g_1) = h_1$ e $f(g_2) = h_2$. Como$f$ é um homomorfismo de grupos e G é abeliano, então

$$h_1h_2 = f(g_1)f(g_2) = f(g_1g_2) = f(g_2g_1) = f(g_2)f(g_1) = h_2h_1.$$

Isso mostra que H é abeliano.

(d) Dado $g \in G$, denote $o(g) = n$ e lembre que $g^n = e_G$ e $e_G \notin \{g, g^2, \ldots, g^{n-1}\}$. Como f é um isomorfismo, em particular, $f(e_G) = e_H$ e f é injetora. Logo, $f(g) = e_H$ se, e somente se, $g = e_G$. Portanto $f(g)^n = f(g^n) = f(e_G) = e_H$ e $e_H \notin \{f(g), f(g)^2, \ldots, f(g)^{n-1}\}$. Isso mostra que $o(f(g)) = n$. □

Exercício 4.3. Sejam G, H e K três grupos.

(a) Mostre que $\mathrm{id}_G\colon G \to G$ é um isomorfismo de grupos.
(b) Se $f\colon G \to H$ é um isomorfismo de grupos, mostre que $f^{-1}\colon H \to G$ também é um isomorfismo de grupos.
(c) Se $\phi\colon G \to H$ e $\psi\colon H \to K$ forem homomorfismos (resp. isomorfismos) de grupos, mostre que $(\psi \circ \phi)\colon G \to K$ é um homomorfismo (resp. isomorfismo) de grupos.
(d) Conclua que $\cong$ (isomorfismo de grupos) é uma relação de equivalência.

Um exemplo de homomorfismo de grupos que já é familiar é o seguinte.

Exemplo 4.4. Considere dois $\mathbb{R}$-espaços vetoriais $(V, +_V, \cdot_V)$ e $(W, +_W, \cdot_W)$. Pela definição, toda transformação linear $T\colon V \to W$ é um homomorfismo do grupo $(V, +_V)$ para o grupo $(W, +_W)$. Além disso, todo isomorfismo linear $T\colon V \to W$ é um isomorfismo do grupo $(V, +_V)$ para o grupo $(W, +_W)$.

Um caso particular do exemplo anterior é o seguinte.

Exemplo 4.5. Considere o grupo aditivo $\mathbb{R}$, o grupo multiplicativo $\mathbb{R}_{>0} = \{\alpha \in R \mid \alpha > 0\}$ e a função $\exp\colon \mathbb{R} \to \mathbb{R}_{>0}$ dada por $\exp(a) = e^a$. Vamos mostrar que exp é um isomorfismo de grupos.

(i) $\exp(a+b) = e^{a+b} = e^a e^b = \exp(a) \cdot \exp(b)$ para todos $a, b \in \mathbb{R}$.
(ii) $\exp(0) = e^0 = 1$

Isso mostra que exp é um homomorfismo de grupos. Além disso, $\ln\colon \mathbb{R}_{>0} \to \mathbb{R}$ é a inversa de exp. Portanto, exp é uma bijeção, e consequentemente, um isomorfismo de grupos.

O próximo exemplo mostra que, dados quaisquer dois grupos, sempre existe algum homomorfismo entre eles.

Exemplo 4.6. Sejam G e H dois grupos. Verifique que a função $f\colon G \to H$ dada por $f(g) = e_H$ para todo $g \in G$ é um homorfismo de grupos. Esse homomorfismo é chamado de homomorfismo trivial. Observe que esse homomorfismo é um isomorfismo se, e somente se, $G = H = \{e\}$.

Exemplo 4.7. Seja $n \geq 3$. Verifique que a função $\vartheta\colon D_{2n} \to S_n$ definida na Seção 1.2 (Aula 3) é um homomorfismo de grupos. Além disso, mostre que ϑ é um isomorfismo se, e somente se, $n = 3$.

Nos próximos exemplos, vamos usar geradores e relações para construir homomorfismo de grupos.

Exemplo 4.8. Considere os grupos abelianos $\mathbb{Z}$ e $\mathbb{Z}_n$ $(n \geq 2)$. Para cada $k \in \mathbb{Z}$, podemos definir um único homomorfimo de grupos $f_k\colon \mathbb{Z} \to \mathbb{Z}_n$ satisfazendo $f_k(1) = \overline{k}$. De fato, como 1 gera $\mathbb{Z}$ e queremos que f_k seja um homomorfismo de grupos, então $f_k(\ell) = k\ell$ para todo $\ell \in \mathbb{Z}$. Em particular, se escolhermos $k = 0$, obteremos o homoorfismo trivial; e se escolhermos $k = 1$, obteremos um homomorfismo chamado de projeção canônica.

Exemplo 4.9. Considere agora os grupos aditivos $\mathbb{Z}_2$ e $\mathbb{Z}_6$. Assim como no exemplo anterior, para cada $k \in \mathbb{Z}$, vamos tentar construir um homomorfismo de grupos $f_k\colon \mathbb{Z}_2 \to \mathbb{Z}_6$. Se definirmos $f_k(\overline{1}) = \overline{k}$, como queremos que f_k seja um homomorfismo de grupos, teremos que:

$$f_k(\overline{0}) = f_k(\overline{1} + \overline{1}) = f_k(\overline{1}) + f_k(\overline{1}) = \overline{2k} = \overline{0}.$$

Mas, observe que $\overline{2k} = \overline{0}$ se, e somente se, $\overline{k} \in \{\overline{0}, \overline{3}\}$. Em particular, $f_1(\overline{1}) = \overline{1}$ **não** induz um homomorfismo de grupos.

Mas se, assim como $\mathbb{Z}$, o grupo $\mathbb{Z}_2$ é gerado por um único elemento, qual é a diferença desse exemplo para o anterior? A diferença é que o gerador $\overline{1} \in \mathbb{Z}_2$ satisfaz a relação $2\overline{1} = \overline{0}$ (enquanto o gerador $1 \in \mathbb{Z}$ não satisfaz relação nenhuma). Então, no caso de $\mathbb{Z}_2$, nós podemos definir f_k só no gerador $\overline{1}$, mas nós temos que verificar que $f_k(\overline{1})$ também satisfaz a relação $2f_k(\overline{1}) = \overline{0}$.

Vamos usar a idéia do exemplo anterior no próximo exemplo.

Exemplo 4.10. Sejam $n \geq 2$ e $f\colon \mathbb{Z}_n \to \mathbb{Z}$ um homomorfismo de grupos. Como $\mathbb{Z}_n$ é gerado por $\overline{1}$, então f é únicamente determinado por $f(\overline{1})$. Ou seja, se $f(\overline{1}) = k$, então $f(\overline{\ell}) = \overline{k\ell}$ para todo $\overline{\ell} \in \mathbb{Z}_n$. Agora, como $f(\overline{1}) = k$ deve satisfazer a relação $nk = 0$ e $n \neq 0$, concluímos que $k = 0$. Ou seja, não existe nenhum homomorfismo de grupos $f\colon \mathbb{Z}_n \to \mathbb{Z}$ além do trivial.

1.7. Ações de grupos

Definição 4.11. Sejam G um grupo e X um conjunto. Uma ação de G em X é uma função $\alpha\colon G \times X \to X$ satisfazendo:

(i) $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$ para todos $g, h \in G$ e $x \in X$,
(ii) $\alpha(e, x) = x$ para todo $x \in X$.

Nesse caso, dizemos que G age em X. Quando não gerar confusão, nós denotaremos $\alpha(g, x)$ por $g \cdot x$ ou simplesmente gx.

Um exemplo que deve ser familiar é o seguinte.

Exemplo 4.12. Considere um $\mathbb{R}$-espaço vetorial $(V, +\cdot)$ e o grupo multiplicativo $\mathbb{R} \setminus \{0\}$. A multiplicação escalar em V induz uma função $\alpha\colon \mathbb{R} \setminus \{0\} \times V \to V$ dada por $\alpha(\lambda, v) = \lambda \cdot v$. Vamos verificar que α é uma ação de $\mathbb{R} \setminus \{0\}$ em V.

(i) Para todos $\lambda, \mu \in \mathbb{R} \setminus \{0\}$ e $v \in V$, por um dos axiomas de espaço vetorial, temos:
$$\alpha(\lambda, \alpha(\mu, v)) = \alpha(\lambda, \mu \cdot v) = \lambda \cdot (\mu \cdot v) = (\lambda\mu) \cdot x = \alpha(\lambda\mu, v).$$
(ii) Para todo $v \in V$, por outro axioma de espaço vetorial, temos $\alpha(1, v) = 1 \cdot v = v$.

Exemplo 4.13. Considere um conjunto X (por exemplo, tome $X = \{1, \ldots, n\}$) e o grupo S_X formado por todas as permutações de X (bijeções de X em X) munido da composição (por exemplo, $S_{\{1,\ldots,n\}} = S_n$). Defina uma função $\alpha\colon S_X \times X \to X$ como sendo $\alpha(\sigma, x) = \sigma(x)$. Vamos verificar que α é uma ação de S_X em X:

(i) Para todos $\sigma, \rho \in S_X$ e $x \in X$, temos:
$$\alpha(\sigma, \alpha(\rho, x)) = \alpha(\sigma, \rho(x)) = \sigma(\rho(x)) = (\sigma \circ \rho)(x) = \alpha(\sigma\rho, x).$$
(ii) Para todo $x \in X$, temos $\alpha(e, x) = \mathrm{id}_X(x) = x$.

Exemplo 4.14. Considere $G = D_{2n}$, $X = \Delta_n$ um n-ágono regular, e defina uma função $\alpha\colon G \times X \to X$ como sendo $\alpha(\sigma, x) = \sigma(x)$. Verifique que α define uma ação de D_{2n} em Δ_n.

Exemplo 4.15. Considere um grupo G e a função $m\colon G \times G \to G$. Vamos verificar que m define uma ação de G em G:

(i) Pela associatividade de m, para todos $a, b, c \in G$, temos $m(a, m(b, c)) = m(ab, c)$.
(ii) Como e é o elemento neutro de G, para todo $g \in G$, temos $m(e, g) = g$.

Proposição 4.16. *Sejam G um grupo e X um conjunto.*

(a) Se $\alpha\colon G \times X \to X$ é uma ação de G em X, então a função $\varphi_\alpha\colon G \to S_X$ dada por $\varphi_\alpha(g) = \alpha(g, -)$ é um homomorfismo de grupos.

(b) Se $\phi\colon G \to S_X$ é um homomorfismo de grupos, então $\alpha_\phi\colon G \times X \to X$ dada por $\alpha_\phi(g,x) = \phi(g)(x)$ é uma ação de G em X.

Demonstração. (a) Como α é uma ação, para quaisquer $g_1, g_2 \in G$, temos que

$$\varphi_\alpha(g_1) \circ \varphi_\alpha(g_2) = \alpha(g_1, \alpha(g_2, -)) = \alpha(g_1 g_2, -) = \varphi_\alpha(g_1 g_2).$$

Além disso, como α é uma ação, $\varphi_\alpha(e_G) = \alpha(e_G, -) = \mathrm{id}_X$. Juntando esses dois fatos, temos que, para todo $g \in G$,

$$\varphi_\alpha(g) \circ \varphi_\alpha(g^{-1}) = \alpha(gg^{-1}, -) = \mathrm{id}_X = \alpha(g^{-1}g, -) = \varphi_\alpha(g^{-1}) \circ \varphi_\alpha(g).$$

Ou seja, $\varphi_\alpha(g)$ é uma bijeção (com inversa $\varphi_\alpha(g^{-1})$) e φ_α é um homomorfismo de grupos.

(b) Como ϕ é um homomorfismo de grupos, para quaisquer $g_1, g_2 \in G$, temos que

$$\alpha_\phi(g_1, \alpha_\phi(g_2, x)) = \phi(g_1)(\phi(g_2)(x)) = (\phi(g_1) \circ \phi(g_2))(x) = \phi(g_1 g_2)(x) = \alpha_\phi(g_1 g_2, x)$$

para todo $x \in X$. Além disso, $\alpha_\phi(e_G, x) = \phi(e_G)(x) = \mathrm{id}_X(x) = x$ para todo $x \in X$. Isso mostra que α_ϕ é uma ação de G em X. □

Corolário 4.17. *Sejam G, H dois grupos e X um conjunto. Se $f\colon G \to H$ é um homomorfismo de grupos e $\alpha\colon H \times X \to X$ é uma ação de H em X, então a função $\beta\colon G \times X \to X$, dada por $\beta(g,x) = \alpha(f(g), x)$, é uma ação de G em X.*

Demonstração. Pela Proposição 4.16(a), $\varphi_\alpha\colon H \to S_X$ é um homomorfismo de grupos dado por $\varphi_\alpha(h) = \alpha(h, -)$. Pelo Exercício 4.3(c), $(\varphi_\alpha \circ f)\colon G \to S_X$ é um homomorfismo de grupos dado por $(\varphi_\alpha \circ f)(g) = \alpha(f(g), -)$. Pela Pela Proposição 4.16(b), $\alpha_{(\varphi_\alpha \circ f)}\colon G \times X \to X$ é uma ação de G em X dada por $\alpha_{(\varphi_\alpha \circ f)}(g,x) = \alpha(f(g), x)$. Como $\beta = \alpha_{(\varphi_\alpha \circ f)}$, o resultado segue. □

Exemplo 4.18. Sejam G um grupo e X um conjunto. Verifique que a função $\alpha\colon G \times X \to X$ dada por $\alpha(g,x) = x$ para todo $g \in G$, $x \in X$, é uma ação de G em X. (Sugestão: mostre que φ_α é o homomorfismo trivial.) Essa ação é chamada de ação trivial.

Exemplo 4.19. Seja $n \geq 3$. Lembre do Exemplo 4.13 que $\alpha\colon S_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ dada pela permutação dos elementos de $\mathbb{Z}_n$ é uma ação, e lembre do Exemplo 4.7 que $\vartheta\colon D_{2n} \to S_n$ é um homomorfismo de grupos. Verifique que a ação de D_{2n} no conjunto $\mathbb{Z}_n$ (que enumera os vértices de um n-ágono regular Δ_n) é dada por $\alpha_{(\varphi_\alpha \circ \vartheta)}$.

Aula 5

Avisos: Aulas 03 e 04 atualizadas, Lista de Exercícios 01 adicionada à página da disciplina.

2.1. Definição e exemplos de subgrupos

Definição 5.1. Seja (G, m_G) um grupo. Um subgrupo de G é um subconjunto não-vazio $H \subseteq G$ satisfazendo:

(i) Se $h_1, h_2 \in H$, então $m_G(h_1, h_2) \in H$.
(ii) Se $h \in H$, então $h^{-1} \in H$.

Exemplo 5.2. Considere o grupo aditivo $\mathbb{Q}$. Observe que, se $a, b \in \mathbb{Z}$, então $a + b \in Z$ e $-a, -b \in \mathbb{Z}$. Portanto $\mathbb{Z}$ é um subgrupo de $\mathbb{Q}$. Análogamente, verifique que $\mathbb{Q}$ é um subgrupo do grupo aditivo $\mathbb{R}$. Como $\mathbb{Q}$ não é um subespaço vetorial de $\mathbb{R}$ (não é fechado pela multiplicação escalar), esse exemplo mostra, em particular, que subgrupos **não** correspondem a subespaços vetoriais.

Exemplo 5.3. O grupo multiplicativo $(\mathbb{R} \setminus \{0\}, \cdot)$ **não** é um subgrupo do grupo aditivo $(\mathbb{R}, +)$. De fato, pela Definição 5.1, um subgrupo é um subconjunto fechado com relação a mesma operação do grupo. Ou seja, neste caso, $\mathbb{R} \setminus \{0\}$ não é fechado pela soma (para todo $a \in \mathbb{R} \setminus \{0\}$, temos que $a - a = 0 \notin \mathbb{R} \setminus \{0\}$) e nós não podemos trocar a soma pelo produto.

Exercício 5.4. Sejam G um grupo e $H \subseteq G$ um subgrupo.

(a) Mostre que $h_1 h_2^{-1} \in H$ para todos $h_1, h_2 \in H$.
(b) Mostre que $e_G \in H$. Em paticular, $e_H = e_G$.
(c) Se $K \subseteq H$ for um subgrupo, mostre que $K \subseteq G$ é um subgrupo.

Exemplo 5.5. Dado qualquer grupo G, os subconjuntos $\{e_G\}$ e G são subgrupos de G.

Exemplo 5.6. Considere o grupo aditivo $\mathbb{Z}$. Vamos descrever todos os subgrupos $H \subseteq \mathbb{Z}$. Primeiro, temos pelo Exemplo 5.5 que $\{0\}$ e $\mathbb{Z}$ são subgrupos. Agora, verifique (usando indução) que, se $a \in H$ e H é um subgrupo, então $na \in H$ para todo $n \in \mathbb{Z}$. De fato, para todo $a \in \mathbb{Z}$, temos um subgrupo $\langle a \rangle = \{na \mid n \in \mathbb{Z}\}$. (Em particular, $\{0\} = \langle 0 \rangle$ e $G = \langle 1 \rangle$.)

Agora suponha que $H \subseteq \mathbb{Z}$ seja um subgrupo e que existam $a, b \in H$ com $a \notin \langle b \rangle$, $b \notin \langle a \rangle$. Como H é um subgrupo e $na, mb \in H$ para todos $n, m \in \mathbb{Z}$, então $na + mb \in H$. Em particular, $\mathrm{mdc}(a, b) \in H$. Então $\langle \mathrm{mdc}(a, b) \rangle \subseteq H$, e em particular, temos que $\langle a \rangle, \langle b \rangle \subseteq \langle \mathrm{mdc}(a, b) \rangle$. Com isso, concluímos que todo subgrupo $H \subseteq \mathbb{Z}$ é da forma $H = \langle a \rangle$ para algum $a \in \mathbb{Z}$.

Exemplo 5.7. Dado um grupo G, $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$ é um subgrupo para todo $g \in G$. De fato, $g^n g^m = g^{n+m} \in \langle g \rangle$ e $(g^n)^{-1} = g^{-n} \in \langle g \rangle$ para todos $g \in G$ e $n, m \in \mathbb{Z}$. Além disso, como $g, g^2, \ldots, g^{o(g)}$ são todos elementos distintos (verifique!), então $|\langle g \rangle| = o(g)$ para todo $g \in G$.

Exemplo 5.8. Verifique que todos os subgrupos de $\mathbb{Z}_n$ são da forma $\{\overline{na} \mid n \in \mathbb{Z}\}$ para algum $\overline{a} \in \mathbb{Z}_n$. Em particular, os únicos subgrupos de $\mathbb{Z}_2$ são $\{\overline{0}\}$ e $\mathbb{Z}_2$.

Proposição 5.9. *Seja (G, m_G) um grupo. Se $H \subseteq G$ é um conjunto finito e não-vazio satisfazendo $m_G(h_1, h_2) \in H$ para todos $h_1, h_2 \in H$, então H é um subgrupo de G.*

Demonstração. Pela Definição 5.1, basta verificar que $h^{-1} \in H$ para todo $h \in H$. Fixe $h \in H$. Como $m_G(h_1, h_2) \in H$ para todos $h_1, h_2 \in H$, então $h^n \in H$ para todo $n > 0$. Como H é um conjunto finito, existem $k, \ell > 0$ tais que $k < \ell$ e $h^k = h^\ell$. Consequentemente, $h^{\ell - k} = e_G$. Se $\ell - k$ fosse igual a 1, então $h = e_G$ e $h^{-1} = h \in H$. Se $\ell - k > 1$, então $k - \ell - 1 > 0$ e portanto $h^{k-\ell-1} = h^{-1} \in H$. □

Observe que o resultado anterior não é válido se retirarmos a hipótese de que H é finito.

Exemplo 5.10. Considere o grupo aditivo $\mathbb{Z}$ e o subconjunto $\mathbb{Z}_{>0} = \{1, 2, 3, \dots\}$. Observe que, se $a, b \in \mathbb{Z}_{>0}$, então $a + b \in \mathbb{Z}_{>0}$. Mas $\mathbb{Z}_{>0}$ não é um subgrupo de $\mathbb{Z}$, pois não contém nem o elemento neutro, nem elementos inversos.

Lema 5.11. *Sejam G um grupo, I um conjunto e H_i $(i \in I)$ uma família de subgrupos de G. O subconjunto $\bigcap_{i\in I} H_i$ também é um subgrupo de G.*

Demonstração. Sejam $a, b \in \bigcap_{i\in I} H_i$, ou seja, $a, b \in H_i$ para todo $i \in I$. Como H_i é um subgrupo de G, então $ab \in H_i$ para todo $i \in I$. Portanto $ab \in \bigcap_{i\in I} H_i$. Além disso, como H_i é um subgrupo de G, então $a^{-1}, b^{-1} \in H_i$ para todo $i \in I$. Portanto $a^{-1}, b^{-1} \in \bigcap_{i\in I} H_i$. Isso mostra que $\bigcap_{i\in I} H_i$ é um subgrupo de G. □

Exercício 5.12. Encontre dois subgrupos (distintos) $H_1, H_2 \subseteq \mathbb{Z}$ tais que $(H_1 \cup H_2)$ não é um subgrupo de $\mathbb{Z}$.

2.2. Centralizadores, normalizadores, estabilizadores, núcleos e imagens

Definição 5.13. Seja $f\colon G \to H$ um homomorfismo de grupos. Defina o núcleo de f como sendo o conjunto

$$\ker(f) = \{g \in G \mid f(g) = e_H\}.$$

Defina a imagem de f como sendo a imagem da função f, ou seja,

$$\mathrm{im}(f) = \{h \in H \mid \text{existe } g \in G \text{ tal que } f(g) = h\}.$$

Lema 5.14. *Se $f\colon G \to H$ for um homomorfismo de grupos, então $\ker(f)$ é um subgrupo de G e $\mathrm{im}(f)$ é um subgrupo de H.*

Demonstração. Primeiro vamos mostrar que $\ker(f)$ é um subgrupo de G. Se $g_1, g_2 \in \ker(f)$, como f é um homomorfismo de grupos, então $f(g_1g_2) = f(g_1)f(g_2) = e_He_H = e_H$. Isso mostra que $g_1g_2 \in \ker(f)$. Além disso, se $g \in \ker(f)$, então $f(g^{-1}) = f(g)^{-1} = e_H^{-1} = e_H$. Isso mostra que $g^{-1} \in \ker(f)$, e que $\ker(f)$ é um subgrupo de G.

Agora vamos mostrar que $\mathrm{im}(f)$ é um subgrupo de H. Se $h_1, h_2 \in \mathrm{im}(f)$, então existem $g_1, g_2 \in G$ tais que $f(g_1) = h_1$ e $f(g_2) = h_2$. Como f é um homomorfismo de grupos, temos que $f(g_1g_2) = f(g_1)f(g_2) = h_1h_2 \in \mathrm{im}(f)$. Além disso, $f(e_G) = e_H \in \mathrm{im}(f)$. Isso mostra que $\mathrm{im}(f)$ é um subgrupo de H e termina a demonstração. □

Lembre que uma função é sobrejetora quando a sua imagem é igual ao seu contra-domínio. O próximo resultado nos dá um critério para determinar quando um homomorfismo é injetor.

Proposição 5.15. *Um homomorfismo de grupos $f\colon G \to H$ é injetor se, e somente se, $\ker(f) = \{e_G\}$. Em particular, f é um isomorfismo se, e somente se, $\ker(f) = \{e_G\}$ e $\mathrm{im}(f) = H$.*

Demonstração. ("somente se":) Como f é um homomorfismo de grupos, em particular, $f(e_G) = e_H$. Se f for injetora, então e_G é o único elemento $g \in G$ tal que $f(g) = e_H$. Isso mostra que $\ker(f) = \{e_G\}$.

("se":) Se $g_1, g_2 \in G$ forem tais que $f(g_1) = f(g_2)$, então $g_1g_2^{-1} \in \ker(f)$. (De fato, $f(g_1g_2^{-1}) = f(g_1)f(g_2^{-1}) = f(g_1)f(g_2)^{-1} = f(g_1)f(g_1)^{-1} = e_G$.) Se $\ker(f) = \{e_G\}$, então $g_1g_2^{-1} = e_G$, ou seja, $g_1 = g_2$. Isso mostra que f é injetora. □

Aula 6

Exercício 6.1. Dados dois grupos, (G, m_G) e (H, m_H), considere o conjunto $(G \times H) = \{(g, h) \mid g \in G, h \in H\}$ munido da função

$$m\colon (G \times H) \times (G \times H) \to (G \times H), \quad m\left((g_1, h_1), (g_2, h_2)\right) = \left(m_G(g_1, g_2), m_H(h_1, h_2)\right).$$

Mostre que $((G \times H), m)$ é um grupo. Além disso, mostre que $(G \times H)$ é abeliano se, e somente se, G e H são abelianos.

2.2. Centralizadores, normalizadores, estabilizadores, núcleos e imagens

Definição 6.2. Seja G um grupo.

(1) Dado um subconjunto $A \subseteq G$, defina o centralizador de A como sendo

$$C_G(A) = \{g \in G \mid ga = ag \text{ para todo } a \in A\}.$$

(2) Defina o centro de G como sendo $Z(G) = C_G(G)$.
(3) Dados um subconjunto $A \subseteq G$ e um elemento $g \in G$, denote por gAg^{-1} o subconjunto $\{gag^{-1} \mid a \in A\}$. Defina o normalizador de A como sendo

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}.$$

(4) Dados uma ação de G em um conjunto X e um elemento $x \in X$, defina o estabilizador de x como sendo

$$G_x = \{g \in G \mid gx = x\}.$$

(5) Dada uma ação $\alpha\colon G \times X \to X$, defina o núcleo da ação α como sendo

$$\ker(\alpha) = \{g \in G \mid gx = x \text{ para todo } x \in X\}.$$

Proposição 6.3. *Seja $\alpha\colon G \times X \to X$ uma ação de um grupo G em um conjunto X.*

(a) Para todo $x \in X$, G_x é um subgrupo de G.
(b) O núcleo de α é um subgrupo de G.
(c) Para todo subconjunto não-vazio $A \subseteq G$, $N_G(A)$ é um subgrupo de G.
(d) Para todo subconjunto não-vazio $A \subseteq G$, $C_G(A)$ é um subgrupo de G.
(e) $Z(G)$ é um subgrupo de G.

Demonstração. (a) Se $a, b \in G_x$, então $ax = x = bx$. Portanto $(ab)x = a(bx) = ax = x$ e $a^{-1}x = a^{-1}(ax) = (a^{-1}a)x = e_G x = x$. Isso mostra que $ab, a^{-1} \in G_x$.
(b) Observe da Definição 6.2 que $\ker(\alpha) = \bigcap_{x \in X} G_x$. Do Lema 5.11 e do item (a), segue que $\ker(\alpha)$ é um subgrupo de G.
(c) Considere o conjunto $\mathcal{P}(G)$ formado por todos os subconjuntos de G. Defina uma ação de G em $\mathcal{P}(G)$ da seguinte forma:

$$\beta\colon G \times \mathcal{P}(G) \to \mathcal{P}(G), \quad \beta(g, A) = gAg^{-1}.$$

(Verifique que β é uma ação.) Observe que $N_G(A)$ é o estabilizador de A em G por esta ação. Do item (a), segue que, para todo $A \subseteq G$, $N_G(A)$ é um subgrupo de G.
(d) Primeiro observe que $N_G(a) = C_G(a)$ para todo $a \in A$. Além disso, $C_G(A) = \bigcap_{a \in A} C_G(a) = \bigcap_{a \in A} N_G(a)$. Do item (c) e do Lema 5.11, segue que, para todo $A \subseteq G$, $C_G(A)$ é um subgrupo de G.
(e) Como $Z(G) = C_G(G)$, segue do item (d) que $Z(G)$ é um subgrupo de G. □

2.3. Grupos e subgrupos cíclicos

Definição 6.4. Dados um grupo G e um elemento $g \in G$, defina $\langle g \rangle$ como sendo o subgrupo $\{g^k \mid k \in \mathbb{Z}\}$ de G. O grupo G é dito cíclico se existe $g \in G$ tal que $G = \langle g \rangle$.

Lema 6.5. *Se G for um grupo cíclico, então G é abeliano.*

Demonstração. Se G for cíclico, então existe $g \in G$ tal que $G = \langle g \rangle$. Ou seja, todo elemento de G é da forma g^k para algum $k \in \mathbb{Z}$. Então, dados quaisquer dois elementos de G, g^k, g^ℓ, temos: $g^k g^\ell = g^{k+\ell} = g^\ell g^k$. Isso mostra que G é cíclico. □

Exemplo 6.6. O grupo trivial é cíclico. De fato, $\langle e \rangle = \{e\}$.

Exemplo 6.7. O grupo aditivo $\mathbb{Z}$ é cíclico. De fato, $\mathbb{Z} = \langle 1 \rangle$. Observe que $\mathbb{Z}$ é abeliano. Observe também que o gerador de $\mathbb{Z}$ não é único. De fato, $\mathbb{Z} = \langle -1 \rangle$.

Exemplo 6.8. Para todo $n \geq 2$, o grupo $\mathbb{Z}_n$ é cíclico. De fato, $\mathbb{Z}_n = \langle \overline{1} \rangle$. Observe que $\mathbb{Z}_n$ também é abeliano.

Exemplo 6.9. Considere o grupo S_3. Se S_3 fosse cíclico, pelo Lema 6.5, S_3 seria abeliano. Mas no Exemplo 2.9 nós vimos que S_3 não é abeliano. Portanto S_3 não é cíclico. De fato, observe que os subgrupos cíclicos de S_3 são:

$$\langle (1) \rangle = \{(1)\}, \quad \langle (1\ 2) \rangle = \{(1), (1\ 2)\}, \quad \langle (1\ 3) \rangle = \{(1), (1\ 3)\},$$
$$\langle (2\ 3) \rangle = \{(1), (2\ 3)\}, \quad \langle (1\ 2\ 3) \rangle = \{(1), (1\ 2\ 3), (1\ 3\ 2)\} = \langle (1\ 3\ 2) \rangle.$$

Exemplo 6.10. Considere o grupo D_{2n} ($n \geq 3$). Como D_{2n} não é abeliano, então já podemos concluir que D_{2n} não é cíclico. De fato, para todo $i \in \{0, \ldots, n-1\}$, temos:

$$\langle r^i \rangle \subseteq \langle r \rangle = \{e, r, \ldots, r^{n-1}\} \quad \text{e} \quad \langle sr^i \rangle = \{e, sr^i\}.$$

Nosso objetivo agora será mostrar que, se G for um grupo cíclico, então G é isomorfo a $\mathbb{Z}$ ou $\mathbb{Z}_n$ (dependendo da ordem de G). Para isso, vamos precisar de um resultado auxiliar.

Lema 6.11. *Se $G = \langle g \rangle$ for um grupo cíclico, então $|G| = o(g)$.*

Demonstração. Como $G = \{e, g, g^2, \ldots\}$, nós precisamos determinar quantas dessas potências de g são distintas. Primeiro suponha que $o(g)$. Vamos mostrar que $g^k = g^\ell$ somente se $k = \ell$. De fato, suponha que $k, \ell \in \mathbb{Z}$ e $g^k = g^\ell$, então $g^{\ell - k} = e$. Como g tem ordem infinita, $\ell - k$ não pode ser diferente de 0. Ou seja, $k = \ell$.

Agora suponha que $o(g) = n$ é finita. Vamos mostrar que $e, g, \ldots, g^{n-1}$ são todos elementos distintos. Se $0 \leq k \leq \ell < n$ e $g^k = g^\ell$, então $g^{\ell - k} = e$. Como $o(g) = n$ e $\ell - k < n$, segue que $\ell - k = 0$. Isso mostra que $e, g, \ldots, g^{n-1}$ são todos elementos distintos. Além disso, observe que, se $k \geq n$, então $g^k = g^r$, onde $0 \leq r < n$ é o resto da divisão de k por n ($k = qn + r$). □

O próximo resultado segue direto da demonstração do Lema 6.11 (parte $o(g)$ finita).

Corolário 6.12. *Sejam G um grupo e $g \in G$ um elemento de ordem finita. Então $g^k = e$ se, e somente se, $o(g)$ divide k.*

Com esses resultados, nós podemos caracterizar todos os grupos cíclicos.

Teorema 6.13. *Seja $G = \langle g \rangle$ um grupo cíclico.*

(a) Se $o(g) = n$ é finita, então $G \cong \mathbb{Z}_n$.
(b) Se $o(g)$ é infinita, então $G \cong \mathbb{Z}$.

Demonstração. (a) Se $G = \langle g \rangle$ e $o(g) = n$, pelo Lema 6.11, temos que $G = \{e, g, \ldots, g^{n-1}\}$. Então podemos definir uma função $\varphi\colon G \to \mathbb{Z}_n$ como $\varphi(g^i) = \overline{i}$ para cada $i \in \{0, \ldots, n-1\}$. Vamos verificar que φ é um homomorfismo de grupos. Se $k, \ell \in \{0, \ldots, n-1\}$, então:

$$\varphi(g^k g^\ell) = \varphi(g^{k+\ell}) = \overline{k+\ell} = \overline{k} + \overline{\ell} = \varphi(g^k) + \varphi(g^\ell).$$

Agora observe que φ é injetora e sobrejetora. Portanto φ é um isomorfismo de grupos.

(b) Considere a função $\psi\colon \mathbb{Z} \to G$ dada por $\psi(i) = g^i$. Primeiro, vamos verificar que ψ é um homomorfismo de grupos. Se $k, \ell \in \mathbb{Z}$, então:

$$\psi(k+\ell) = g^{k+\ell} = g^k g^\ell = \psi(k)\psi(\ell).$$

Do Lema 6.11, segue que ψ é injetora. Como $G = \{g^k \mid k \in \mathbb{Z}\}$, então ψ também é sobrejetora. Portanto ψ é um isomorfismo de grupos. □

Agora, nós vamos descrever todos os possíveis geradores e subgrupos de um grupo cíclico. Nós começamos com um resultado auxiliar.

Lema 6.14. *Sejam G um grupo e g um elemento de G.*

(a) Se g tem ordem infinita, então a ordem de g^k é infinita para todo $k \in \mathbb{Z} \setminus \{0\}$.
(b) Se $o(g) = n$, então $o(g^k) = \frac{n}{\operatorname{mdc}(n,k)}$ para todo $k \in \mathbb{Z} \setminus \{0\}$. Em particular, $o(g^k) = n$ para todo $k \in \mathbb{Z} \setminus \{0\}$ coprimo com n, e $o(g^k) = \frac{n}{k}$ para todo $k \in \mathbb{Z} \setminus \{0\}$ que divide n.

Demonstração. (a) Se g tem ordem infinita, então $g^i \neq e$ para todo $i \in \mathbb{Z} \setminus \{0\}$. Em particular, $(g^k)^\ell = g^{k\ell} \neq e$ para todos $k, \ell \in \mathbb{Z} \setminus \{0\}$. Isso mostra que g^k tem ordem infinita, para todo $k \in \mathbb{Z} \setminus \{0\}$.

(b) Assuma que $o(g) = n$, tome $k \in \mathbb{Z} \setminus \{0\}$, e considere $n', k' \in \mathbb{Z}$ tais que $n = \operatorname{mdc}(n,k)n'$, $k = \operatorname{mdc}(n,k)k'$. Queremos mostrar que $o(g^k) = n'$. Observe que, para cada $\ell \in \mathbb{Z}$, temos:

$$(g^k)^\ell = g^{k\ell} = g^{\operatorname{mdc}(k,n)(k'\ell)}.$$

Como $o(g) = n$, segue do Corolário 6.12 que $(g^k)^\ell = e$ se, e somente se, $n \mid \operatorname{mdc}(k,n)(k'\ell)$, ou seja, $n' \mid k'\ell$. Como n' e k' não tem fatores em comum (se tivessem, eles seriam fatores do $\operatorname{mdc}(n,k)$), concluímos que $(g^k)^\ell = e$ se, e somente se, $n' \mid \ell$. Em particular, $(g^k)^\ell \neq e$ se $0 < \ell < n'$, e $(g^k)^\ell = e$ se $\ell = n'$. Isso mostra que $o(g^k) = n'$. □

Proposição 6.15. *Seja $G = \langle g \rangle$ um grupo cíclico.*

(a) Se $o(g)$ é infinita, então $G = \langle g^k \rangle$ se, se somente se, $k \in \{-1, 1\}$.
(b) Se $o(g) = n$ é finita, então $G = \langle g^k \rangle$ se, se somente se, k é coprimo com n.

Demonstração. (a) Primeiro verifique que $G = \langle g^k \rangle$ se, e somente se, $g = g^{k\ell}$ para algum $\ell \in \mathbb{Z}$. Depois observe que $g = g^{k\ell}$ se, e somente se, $g^{k\ell - 1} = e$. Como g tem ordem infinita, $g^{k\ell-1} = e$ se, e somente se, $k\ell - 1 = 0$. Como $k, \ell \in \mathbb{Z}$, $k\ell = 1$ se, e somente se, $k = \ell$ e $k, \ell \in \{-1, 1\}$.

(b) Pelo Lema 6.11, temos que $|G| = o(g)$ e $|\langle g^k \rangle| = o(g^k)$. Como G é um grupo finito, então $G = \langle g^k \rangle$ se, e somente se, $o(g^k) = o(g)$. Pelo Lema 6.14(b), $o(g^k) = o(g)$ se, e somente se, k é coprimo com n. Isso termina a demonstração. □

Aula 7

Avisos: Definição de homomorfismo de grupos corrigida.

2.4. Subgrupo gerado por um subconjunto de um grupo

Assim como acontece com espaços vetoriais, podemos criar subgrupos (analogamente a subespaços) a partir de subconjuntos do grupo que tem mais de um elemento (analogamente aos subespaços gerados).

Definição 7.1. Seja G um grupo e $X \subseteq G$ um subconjunto. Defina o subgrupo gerado por X como o subconjunto

$$\langle X \rangle = \{(x_1)^{\varepsilon_1}(x_2)^{\varepsilon_2}\cdots(x_n)^{\varepsilon_n} \mid n \geq 0, x_1, \ldots, x_n \in X, \varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}\}.$$

Observe que, quando escolhemos $n = 0$ acima, obtemos $(x_1)^{\varepsilon_1}(x_2)^{\varepsilon_2}\cdots(x_n)^{\varepsilon_n} = e_G$. Em particular, $\langle \emptyset \rangle = \{e_G\}$. Observe também que, quando $X = \{g\}$, então $x_1 = x_2 = \cdots = x_n = g$ acima e $\langle X \rangle = \langle g \rangle$ (como na Definição 6.4).

Vamos mostrar que, de fato, $\langle X \rangle$ é um subgrupo de G. Para isso, vamos usar que a intersecção arbitrária de subgrupos de G é um subgrupo de G (Lemma 5.11).

Proposição 7.2. *Sejam G um grupo e $X \subseteq G$ um subconjunto. Denote por I o subconjunto de $\mathcal{P}(G)$ formado por todos os subgrupos de G que contem X. Então*

$$\langle X \rangle = \bigcap_{H \in I} H.$$

Demonstração. Como $X \subseteq H$ para todo $H \in I$ (pela definição de I) e como $H \in I$ são subgrupos de G, então $(x_1)^{\varepsilon_1}(x_2)^{\varepsilon_2}\cdots(x_n)^{\varepsilon_n} \in H$ para todos $n \geq 0$, $x_1, \ldots, x_n \in X$, $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$ e $H \in I$. Isso mostra que $\langle X \rangle \subseteq \bigcap_{H \in I} H$.

Para terminar a demonstração, vamos mostrar que $\langle X \rangle \in I$. Primeiro observe que $X \subseteq \langle X \rangle$ (para cada $x \in X$, podemos tomar $n = 1$, $x_1 = x$ e $\varepsilon_1 = 1$). Agora observe que

$$(x_1)^{\varepsilon_1}(x_2)^{\varepsilon_2}\cdots(x_n)^{\varepsilon_n}(y_1)^{\eta_1}(y_2)^{\eta_2}\cdots(y_m)^{\eta_m} \in \langle X \rangle$$

para todos $n, m \geq 0$, $x_1, \ldots, x_n, y_1, \ldots, y_m \in X$ e $\varepsilon_1, \ldots, \varepsilon_n, \eta_1, \ldots, \eta_m \in \{-1, 1\}$. Finalmente, observe que $((x_1)^{\varepsilon_1}(x_2)^{\varepsilon_2}\cdots(x_n)^{\varepsilon_n})^{-1} = (x_n)^{-\varepsilon_1}\cdots(x_2)^{-\varepsilon_2}(x_1)^{-\varepsilon_1} \in \langle X \rangle$ para todos $n \geq 0$, $x_1, \ldots, x_n \in X$ e $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$. Portanto, $\langle X \rangle$ é um subgrupo de G contendo X. □

A proposição anterior mostra, não só que $\langle X \rangle$ é um subgrupo de G, mas que $\langle X \rangle$ é o menor (no sentido da inclusão) subgrupo de G que contem G. De fato, para todo subgrupo $K \subseteq G$ que contem X, temos que $K \in I$ e portanto $\bigcap_{H \in I} H \subseteq K$.

Exemplo 7.3. Lembre que $D_{2n} = \langle r, s \rangle$ para todo $n \geq 3$.

Exercício 7.4. Verifique que $S_n = \langle (1\ 2), (1\ 2\ \ldots\ n) \rangle$ para todo $n \geq 2$.

Exercício 7.5. Considere $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ e $B = \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix}$. Verifique que $A^2 = B^2 = e$, e que $\langle A, B \rangle$ é um subgrupo próprio de GL_2 de ordem infinita.

Exercício 7.6. Considere $n \geq 0$, $G_1, \ldots, G_n$ grupos e, para cada $i \in \{1, \ldots, n\}$, um subconjunto $X_i \subseteq G_i$. Denote por $\tilde{X}_i$ o subconjunto

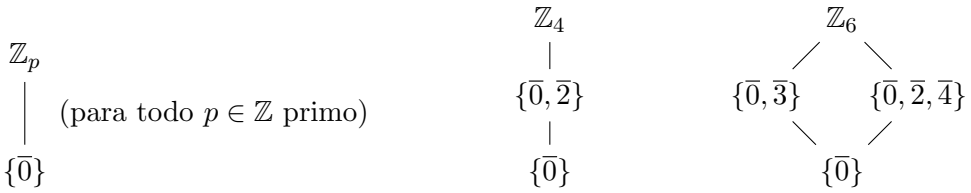
$$\tilde{X}_i = \{(x_1, \ldots, x_n) \in (G_1 \times \cdots \times G_n) \mid x_i \in X_i \text{ e } x_j = e_{G_j} \text{ para todo } j \neq i\}.$$

Se $G_1 = \langle X_1 \rangle, \ldots, G_n = \langle X_n \rangle$, mostre que $G_1 \times \cdots \times G_n = \langle \tilde{X}_1 \cup \cdots \cup \tilde{X}_n \rangle$.

2.5 Reticulado de subgrupos de um grupo

Dado um grupo G, uma forma de vizualizar a estrutura de G é desenhando o seu reticulado de subgrupos, ou seja, um grafo cujos vértices são os subgrupos de G e as arestas ligam um subgrupo H_1 a um subgrupo H_2 quando $H_1 \subsetneq H_2$ e não existe nenhum subgrupo $H \subseteq G$ tal que $H_1 \subsetneq H \subsetneq H_2$.

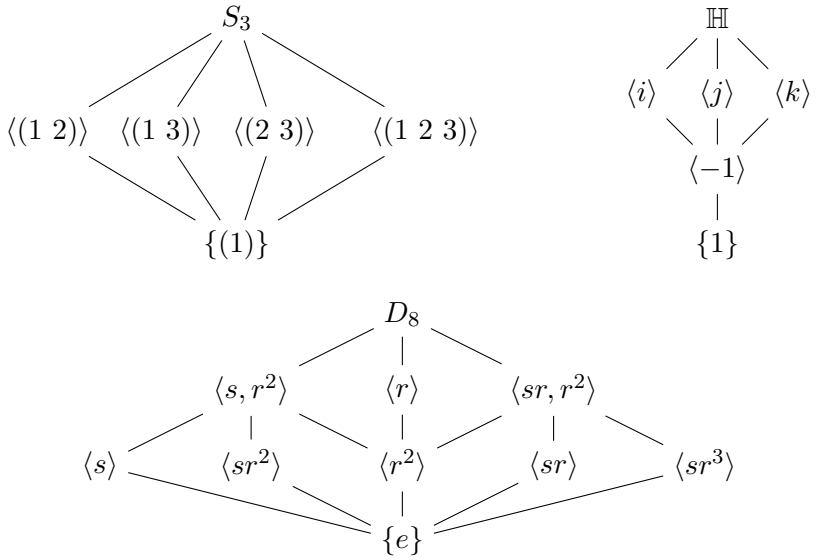
Exemplo 7.7. Pelos Lemas 6.11 e 6.14(b), podemos desenhar os retiiculados de subgrupos de $\mathbb{Z}_n$ para todo $n \geq 2$. Em particular, temos:



É fácil ver o quão complicado os reticulados de subgrupos podem ficar. Em particular, quando o grupo é infinito.

Exercício 7.8. Esboce o reticulado de grupos de $\mathbb{Z}$.

A seguir, vamos desenhar os reticulados de subgrupos de três grupos finitos sobre os quais nós já temos informações suficientes.



3.1. Grupos quocientes e homomorfismos: Definições e exemplos

Vamos começar analisando um exemplo que nós já conhecemos.

Exemplo 7.9. Considere os grupos $\mathbb{Z}$ e $\mathbb{Z}_n$ ($n \geq 2$). Lembre do Exemplo 4.8 que a função $f\colon \mathbb{Z} \to \mathbb{Z}_n$ dada por $f(a) = \overline{a}$ é um homomorfismo de grupos, chamado de projeção canônica. Observe que, para cada $\overline{k} \in \mathbb{Z}_n$, o subconjunto $f^{-1}(\overline{k})$, chamado de fibra de f sobre $\overline{k}$ é dado por

$$\begin{aligned} f^{-1}(\overline{k}) &= \{a \in \mathbb{Z} \mid f(a) = \overline{k}\} \\ &= \{a \in \mathbb{Z} \mid \overline{a} = \overline{k}\} \\ &= \{a \in \mathbb{Z} \mid n \text{ divide } (k-a)\}. \end{aligned}$$

Ou seja, $f^{-1}(\overline{k})$ é o conjunto de elementos na classe de equivalência $\overline{k}$. De outra forma, $f^{-1}(\overline{k})$ consiste de elementos da forma $qn+k$, para algum $q \in \mathbb{Z}$. Observe, em particular, que $f^{-1}(\overline{0})$ (que, por definição, é igual a $\ker(f)$) consiste de múltiplos de n, ou seja, elementos da forma qn, para algum $q \in \mathbb{Z}$. Então podemos concluir que $f^{-1}(\overline{k}) = \{k+\ell \mid \ell \in \ker(f)\} =: k+\ker(f)$.

Além disso, observe que a operação de grupo definida em $\mathbb{Z}_n$ reflete a operação de grupo definida em $\mathbb{Z}$: $\overline{a}+\overline{b} = \overline{a+b}$. Em particular, como $\overline{a}+\overline{b}$ está bem definida, ela independe dos representantes escolhidos para $\overline{a}$ e $\overline{b}$. De fato, $\overline{a+\ell_1}+\overline{b+\ell_2} = \overline{a+b+(\ell_1+\ell_2)} = \overline{a+b}$ para quaisquer $\ell_1, \ell_2 \in \ker(f)$.

Agora, nós queremos generalizar esse exemplo para quaisquer homomorfismos entre grupos. Primeiro, vamos generalizar a relação de equivalência que define $\mathbb{Z}_n$ e formar o quociente.

Considere um grupo G e um subgrupo $K \subseteq G$. Defina uma relação em G da seguinte forma:

$$g \sim h \quad \text{se e somente se} \quad h^{-1}g \in K.$$

Vamos verificar que $\sim$ é uma relação de equivalência:

- Para todo $g \in G$, temos que $g \sim g$, pois, como K é um subgrupo de G, $g^{-1}g = e_G \in K$.
- Se $g \sim h$, então $h^{-1}g \in K$. Como K é um subgrupo de G, segue que $g^{-1}h = (h^{-1}g)^{-1} \in K$. Logo $h \sim g$.
- Se $a \sim b$ e $b \sim c$, então $b^{-1}a, c^{-1}b \in K$. Como K é um subgrupo de G, segue que $c^{-1}a = (c^{-1}b)(b^{-1}a) \in K$. Logo $a \sim c$.

Denote por G/K o conjunto de classes de equivalência da relação $\sim$, denote por $\overline{g} \in G/K$ a classe de equivalência a qual o elemento $g \in G$ pertence, e por gK (resp. Kg) o subconjunto $\{gk \in G \mid k \in K\}$ (resp. $\{kg \in G \mid k \in K\}$). O conjunto gK (resp. Kg) é chamado de classe lateral de g à esquerda (resp. classe lateral de g à direita). (Observe que $\overline{h} = \overline{g}$ para todo $h \in gK$. Ou seja, os elementos da classe lateral de g à esquerda são os representantes da classe de equivalência $\overline{g}$.)

O próximo resultado mostra que, quando K é o núcleo de um homomorfismo de grupos, G/K admite uma estrutura de grupo.

Lema 7.10. *Seja $f\colon G \to H$ um homomorfismo de grupos e denote $\ker(f)$ por K. O conjunto G/K é um grupo quando munido da operação*

$$m\colon (G/K)\times(G/K) \to (G/K) \quad \text{dada por} \quad m(\overline{g},\overline{h}) = \overline{gh}.$$

Demonstração. Primeiro vamos mostrar que m está bem definida. Dados $g,h \in G$ e $a,b \in K$, temos que $m(\overline{ga},\overline{hb}) = \overline{gahb} = \overline{gh}$ se, e somente se, $(gh)^{-1}(gahb) \in K = \ker(f)$. Como f é um homomorfismo de grupos e $a,b \in \ker(f)$, temos que:

$$f\left((gh)^{-1}(gahb)\right) = f(h^{-1}g^{-1}gahb) = f(h^{-1})f(a)f(h)f(b) = f(h)^{-1}f(h) = e.$$

Isso mostra que $m(\overline{ga},\overline{hb}) = m(\overline{g},\overline{h})$ para todos $g,h \in G$ e que m está bem definida.

Agora vamos mostrar que m satisfaz as condições (i)-(iii) da Definição 1.1:

(i) $m(\overline{a}, m(\overline{b},\overline{c})) = m(\overline{a},\overline{(bc)}) = \overline{(a(bc))} = \overline{((ab)c)} = m(m(\overline{a},\overline{b}),\overline{c})$ para todos $a,b,c \in G$.

(ii) $m(\overline{e_G},\overline{g}) = \overline{(e_G g)} = \overline{g} = \overline{(ge_G)} = m(\overline{g},\overline{e_G})$ para todo $g \in G$. Portanto $\overline{e_G}$ é o elemento neutro de G/K.

(iii) $m(\overline{g^{-1}},\overline{g}) = \overline{(g^{-1}g)} = \overline{e_G} = \overline{(gg^{-1})} = m(\overline{g},\overline{g^{-1}})$ para todo $g \in G$. Portanto $\overline{g^{-1}}$ é o elemento inverso de $\overline{g}$ em G/K. □

Observe que o lema anterior não é válido se substituirmos $\ker(f)$ por um subgrupo qualquer de G. De fato, m não está bem definida para todo subgrupo $K \subseteq G$.

Exemplo 7.11. Considere $G = S_3$ e $K = \langle(1\ 2)\rangle$. Observe que: $(1) \sim (1\ 2)$, $(1\ 3) \sim (1\ 2\ 3)$ e $(2\ 3) \sim (1\ 3\ 2)$. Logo $G/K = \{\overline{(1)}, \overline{(1\ 3)}, \overline{(2\ 3)}\}$. Se tentássemos definir

$$m\colon (G/K) \times (G/K) \to (G/K), \quad \text{dada por} \quad m(\overline{g}, \overline{h}) = \overline{gh},$$

teríamos $\overline{(1\ 2\ 3)} = \overline{(1\ 3)} = m(\overline{(1)}, \overline{(1\ 3)}) = m(\overline{(1\ 2)}, \overline{(1\ 3)}) = \overline{(1\ 3\ 2)}$. Isso mostra que m não estaria bem definida, pois ela dependeria da escolha do representante. Observe que o problema, nesse caso, é que $(1\ 2\ 3)K = (1\ 3)K \neq (1\ 2)K(1\ 3)K$, ou mais especificamente, o problema é que $K(1\ 3) \neq (1\ 3)K$.

Aula 8

3.1. Grupos quocientes e homomorfismos: Definições e exemplos

Sejam G um grupo e $H \subseteq G$ um subgrupo. Lembre que G/K denota o conjunto de classes de equivalência da relação

$$g_1 \sim g_2 \quad \text{se, e somente se,} \quad (g_2)^{-1}g_1 \in H. \tag{8.1}$$

Denote por $\overline{g} \in G/K$ a classe de equivalência a qual o elemento $g \in G$ pertence, e por gK (resp. Kg) o subconjunto $\{gk \in G \mid k \in K\}$ (resp. $\{kg \in G \mid k \in K\}$). O conjunto gK (resp. Kg) é chamado de classe lateral de g à esquerda (resp. classe lateral de g à direita). (Observe que $\overline{h} = \overline{g}$ para todo $h \in gK$. Ou seja, os elementos da classe lateral de g à esquerda são os representantes da classe de equivalência $\overline{g}$.)

Proposição 8.1. *Seja G um grupo e $N \subseteq G$ um subgrupo.*

(a) Munido da operação $m\colon (G/N)\times(G/N) \to (G/N)$ dada por $m(\overline{g},\overline{h}) = \overline{gh}$, o conjunto G/N é um grupo se, e somente se, $gN = Ng$ para todo $g \in G$.
(b) Se $gN = Ng$ para todo $g \in G$, então a função $f\colon G \to G/N$ dada por $f(g) = \overline{g}$ é um homomorfismo de grupos e $\ker(f) = N$.

Demonstração. (a) Vamos mostrar que m está bem definida se, e somente se, $gN = Ng$ para todo $g \in G$. Considere $g_1g_2 \in G$ e $n_1, n_2 \in N$. Pela definição de m, temos que $\overline{g_1g_2} = m(\overline{g_1},\overline{g_2}) = m(\overline{g_1n_1},\overline{g_2n_2}) = \overline{g_1n_1g_2n_2}$ se, e somente se, $g_2^{-1}n_1g_2n_2 = (g_1g_2)^{-1}(g_1n_1g_2n_2)$ pertence a N.

Se $gN = Ng$ para todo $g \in G$, então em particular, $(g_2^{-1})n_1 = n(g_2^{-1})$ para algum $n \in N$, ou seja, $g_2^{-1}n_1g_2 \in N$. Daí segue que $g_2^{-1}n_1g_2n_2 \in N$ e portanto m está bem definida. Por outro lado, se m está bem definida, ou seja, $m(\overline{g_1},\overline{g_2}) = m(\overline{g_1n_1},\overline{g_2n_2})$ para todos $g_1, g_2 \in G$, $n_1, n_2 \in N$, então $g_2^{-1}n_1g_2n_2 \in N$. Em particular, para $n_2 = e_G$, segue que $g_2Ng_2^{-1} \subseteq N$ para todo $g_2 \in G$. Tomando $g_2 = e_G$, concluímos que $gNg^{-1} = N$ para todo $g \in G$. Agora observe que $gNg^{-1} = N$ se, e somente se, $gN = Ng$.

Para terminar a demonstração do item(a), verifique que, quando m é bem definida, ela satisfaz as condições (i)-(iii) da Definição 1.1.

(b) Pelo item(a), se $gN = Ng$ para todo $g \in G$, então $(G/N, m)$ é um grupo. Nesse caso, por construção, $f(g_1g_2) = \overline{g_1g_2} = m(\overline{g_1},\overline{g_2}) = m(f(g_1), f(g_2))$. Portanto f é um homomorfismo de grupos. Além disso,

$$\ker(f) = \{g \in G \mid f(g) = \overline{e}\} = \{g \in G \mid \overline{g} = \overline{e}\} = \{g \in G \mid g \in N\} = N. \qquad \square$$

A proposição anterior motiva a próxima definição.

Definição 8.2. Dado um grupo G, um subgrupo $N \subseteq G$ é dito normal quando $gN = Ng$ para todo $g \in G$.

Pela Proposição 8.1(a), $N \subseteq G$ é um subgrupo normal se, e somente se, $(G/N, m)$ for um grupo. Pelo Lema 7.10, segue que, para todo homomorfismo de grupos $f\colon G \to H$, $\ker(f)$ é um subgrupo normal de G. Por outro lado, segue da Proposição 8.1(b) que todo subgrupo normal de G é o núcleo de um homomorfismo de grupos.

Exercício 8.3. Seja G um grupo e $N \subseteq G$ um subgrupo. Mostre que N é normal se, e somente se, $gNg^{-1} = N$ para todo $g \in G$ se, e somente se, $N_G(N) = G$. Conclua que, se G é abeliano, então todo subgrupo $N \subseteq G$ é normal.

Exemplo 8.4. Para todo grupo G, verifique que o subgrupo trivial $\{e\} \subseteq G$ é um subgrupo normal e que $G/\{e\} \cong G$.

Exemplo 8.5. Para todo grupo G, verifique que $G \subseteq G$ é um subgrupo normal e que G/G é isomorfo ao grupo trivial.

Exemplo 8.6. Considere o grupo aditivo $G = \mathbb{Z}$. Verifique que $\langle n \rangle \subseteq \mathbb{Z}$ é um subgrupo normal e que $\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$ para todo $n \geq 2$.

Exemplo 8.7. Considere o grupo $\mathbb{Z}_6$. Verifique que $\langle \overline{2} \rangle \subseteq \mathbb{Z}_6$ e $\langle \overline{3} \rangle \subseteq \mathbb{Z}_6$ são subgrupos normais. Verifique também que $\mathbb{Z}/\langle \overline{2} \rangle \cong \mathbb{Z}_2$ e $\mathbb{Z}/\langle \overline{3} \rangle \cong \mathbb{Z}_3$.

Exemplo 8.8. Considere o grupo S_3. Explique por que $\langle (1\ 2) \rangle \subseteq S_3$ não é um subgrupo normal. (Lembre do Exemplo 7.11 que $S_3/\langle (1\ 2) \rangle$ não é um grupo.) Verifique que $\langle (1\ 2\ 3) \rangle \subseteq S_3$ é um subgrupo normal e que $S_3/\langle (1\ 2\ 3) \rangle \cong \mathbb{Z}_2$.

Exemplo 8.9. Considere $n \geq 3$ e $G = D_{2n}$. Verifique que $\langle r \rangle \subseteq D_{2n}$ é um subgrupo normal e que $D_{2n}/\langle r \rangle \cong \mathbb{Z}_2$. Determine se $\langle s \rangle \subseteq D_{2n}$ é um subgrupo normal.

3.2. Mais sobre classes laterais e Teorema de Lagrange

Definição 8.10. Dados um grupo G e um subgrupo $H \subseteq G$, defina o índice de H em G, $|G\colon H|$, como a quantidade de classes laterais (à esquerda) de H em G.

Teorema 8.11 (de Lagrange)**.** *Seja G um grupo e $H \subseteq G$ um subgrupo. Se $|G|$ for finita, então $|H|$ divide $|G|$ e $|G\colon H| = |G|/|H|$.*

Demonstração. Primeiro vamos mostrar que $g_1H \cap g_2H \neq \emptyset$ $(g_1, g_2 \in G)$ se, se somente se, $g_1H = g_2H$ e, depois, que $|gH| = |H|$ para todo $g \in G$. Como $G = \bigcup_{g \in G} gH$, segue que $|G| = |H||G\colon H|$.

Suponha que $g_1, g_2 \in G$ sejam tais que $g_1H \cap g_2H \neq \emptyset$. Isso significa que existem $k_1, k_2 \in H$ tais que $g_2k_2 = g_1k_1$. Denote $k_1k_2^{-1} \in H$ por k. Então $g_2H = \{g_2h \mid h \in H\} = \{g_1kh \mid h \in H\}$. Como $k \in H$, então $kh \in H$ para todo $h \in H$. Além disso, para todo $h' \in H$, existe $h = (k^{-1}h') \in H$ e $kh = h'$. Isso mostra que $kH = H$ e implica que $g_2H = \{g_1(kh) \mid h \in H\} = \{g_1h \mid h \in H\} = g_1H$.

Agora fixe $g \in G$ e defina uma função $l_g\colon H \to G$ da seguinte forma $l_g(h) = gh$ para todo $h \in H$. Observe que l_g é injetora, pois $l_g(h_1) = l_g(h_2)$ se, e somente se, $gh_1 = gh_2$ se, e somente se, $h_1 = h_2$. Além disso, $\mathrm{im}(l_g) = gH$. Portanto l_g é uma bijeção entre H e gH. Isso implica que $|H| = |gH|$ e termina a demonstração. □

A volta do Teorema de Lagrange não é válido em geral. Dois resultados parciais nessa direção são o Teorema de Cauchy e os Teoremas de Sylow, que nós também veremos nesse curso.

Corolário 8.12. *Se G for um grupo finito, então $o(g)$ divide $|G|$ para todo $g \in G$. Em particular, $g^{|G|} = e_G$.*

Corolário 8.13. *Se $|G|$ for um número primo, então G é cíclico e $G \cong \mathbb{Z}_{|G|}$.*

Corolário 8.14. *Dados $a, p \in \mathbb{Z}$, se p for primo, então p divide $a^{p+1} - a$.*

Exemplo 8.15. Lembre que, se $G = \langle g \rangle$ for cíclico $(\cong \mathbb{Z}_n)$, então $o(g^k) = \frac{n}{\mathrm{mdc}(k,n)}$. Lembre também que todo subgrupo $H \subseteq \mathbb{Z}_n$ é cíclico, ou seja, $H = \langle g^k \rangle$ para algum k. Portanto, as ordens dos subgrupos de G dividem $|G|$. Além disso, o índice de $\langle g^k \rangle$ em G é igual a $\mathrm{mdc}(k, n)$.

Exemplo 8.16. Considere $n \geq 2$ e $G = S_n$. Lembre que, para todo p-ciclo $\sigma \in S_n$, $o(\sigma) = p$. Como $|S_n| = n!$ e $p \in \{1, \ldots, n\}$, então $o(\sigma) \mid |S_n|$.

Além disso, lembre que todo $\sigma \in S_n$ admite uma decomposição $\sigma = \sigma_1 \cdots \sigma_\ell$ em ciclos disjuntos. Para cada $i \in \{1, \ldots, \ell\}$, denote por p_i a ordem de σ_i (ou seja, σ_i é um p_i-ciclo). Então $o(\sigma) = \text{mmc}(p_1, \ldots, p_\ell)$. Como $p_1, \ldots, p_\ell \in \{1, \ldots, n\}$ e $|S_n| = n!$, então $o(\sigma) \mid n!$.

Em particular (para $n = 3$), lembre que todo subgrupo de S_3 é cíclico. Como $|\langle\sigma\rangle| = o(\sigma)$ para todo $\sigma \in S_3$, então as ordens dos subgrupos de S_3 são:

- 1: $\{(1)\}$,
- 2: $\langle(1\ 2)\rangle$, $\langle(1\ 3)\rangle$ e $\langle(2\ 3)\rangle$,
- 3: $\langle(1\ 2\ 3)\rangle$,
- 6: S_3.

Aula 9

3.3. Teoremas de isomorfismo

O primeiro Teorema de Isomorfismo de grupos é o seguinte.

Teorema 9.1. *Para todo homomorfismo de grupos $f\colon G \to H$, existe um isomorfismo de grupos $G/\ker(f) \cong \mathrm{im}(f)$.*

Demonstração. Lembre do Lema 7.10 que $\ker(f)$ é um subgrupo normal de G. Então considere o grupo $G/\ker(f)$ e defina uma função $F\colon G/\ker(f) \to \mathrm{im}(f)$ da seguinte forma $F(\overline{g}) = f(g)$ para todo $\overline{g} \in G/\ker(f)$. Vamos mostrar que F é um isomorfismo de grupos.

Primeiro, observe que F está bem definida. De fato, $F(\overline{gk}) = f(gk) = f(g)f(k) = f(g)$ para todos $g \in G$, $k \in \ker(f)$. Além disso, $F(\overline{g_1 g_2}) = f(g_1 g_2) = f(g_1)f(g_2) = F(\overline{g_1})F(\overline{g_2})$ para todos $g_1, g_2 \in G$. Isso mostra que F é um homomorfismo de grupos. Observe também que, por construção, $\mathrm{im}(F) = \mathrm{im}(f)$, ou seja, F é sobrejetora. Agora vamos calcular o núcleo de F:

$$\ker(F) = \{\overline{g} \in G/\ker(f) \mid F(\overline{g}) = f(g) = e_H\} = \{\overline{g} \in G/\ker(f) \mid g \in \ker(f)\} = \overline{e_G}.$$

Isso mostra F é injetora e termina a demonstração. □

Para enunciar o segundo Teorema de Isomorfismo de grupos, nós precisamos de algumas definições e resultados preliminares.

Definição 9.2. Dados um grupo G e subgrupos $H, K \subseteq G$, defina

$$HK = \{hk \in G \mid h \in H, k \in K\}.$$

Proposição 9.3. *Seja G um grupo e $H, K \subseteq G$ subgrupos.*

(a) Se H e K são subgrupos finitos, então

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

(b) HK é um subgrupo de G se, e somente se, KH é um subgrupo de G.

Demonstração. (a) Primeiro observe que $HK = \bigcup_{h \in H} hK$, e lembre (da demonstração do Teorema de Lagrange) que $|hK| = |K|$ para todo $h \in H$. Vamos mostrar que o número de classes laterais hK distintas é $|H|/|H \cap K|$. Primeiro lembre (também da demonstração do Teorema de Lagrange) que $h_1 K = h_2 K$ se, e somente se, $h_2^{-1} h_1 \in K$. Como $h_1, h_2 \in H$ e H é um subgrupo, então $h_2^{-1} h_1 \in (H \cap K)$. Isso mostra que $h_1 K = h_2 K$ se, e somente se, $h_1(H \cap K) = h_2(H \cap K)$, e consequentemente, que existem $|H|/|H \cap K|$ classes laterais hK distintas.

(b) Como a afirmação é simétrica em H e K, basta mostrar que HK é um subgrupo de G se KH é um subgrupo de G. Dados $k_1, k_2 \in K$ e $h_1, h_2 \in H$, se KH for um subgrupo de G, então $(k_2^{-1} h_2^{-1})(k_1^{-1} h_1^{-1}) = kh$ para alguns $k \in K$ e $h \in H$. Logo $(h_1 k_1)(h_2 k_2) = h^{-1} k^{-1} \in HK$. Além disso, se KH for um subgrupo de G, então, para todos $h \in H$ e $k \in K$, temos que $(k^{-1} h^{-1})^{-1} = k'h'$ para alguns $h' \in H$ e $k' \in K$. Isso implica que $(hk)^{-1} = (k'h')^{-1} = (h')^{-1}(k')^{-1} \in HK$. □

Definição 9.4. Dados um grupo G e um subgrupo $H \subseteq G$, dizemos que um subconjunto $X \subseteq G$ normaliza H (resp. centraliza H) quando $X \subseteq N_G(H)$ (resp. $X \subseteq C_G(H)$).

O segundo Teorema de Isomorfismo de grupos é o seguinte.

Teorema 9.5. *Sejam G um grupo e $H, K \subseteq G$ subgrupos. Se H normaliza K, então: HK é um subgrupo de G, K é normal em HK, $(H \cap K)$ é normal em H e existe um isomorfismo de grupos $HK/K \cong H/(H \cap K)$.*

Demonstração. Se H normaliza K, então $hKh^{-1} = K$ para todo $h \in H$. Logo, para todos $h_1, h_2 \in H$ e $k_1, k_2 \in K$, temos que $(h_1k_1)(h_2k_2) = h_1h_2^{-1}k'k_2$ para algum $k' \in K$. Em particular, $(h_1k_1)(h_2k_2) \in HK$. Além disso, para todos $h \in H$ e $k \in K$, temos que $(hk)^{-1} = k^{-1}h^{-1} = hk'$ para algum $k' \in K$. Em particular, $(hk)^{-1} \in HK$. Isso mostra que HK é um subgrupo de G.

Agora, se $hKh^{-1} = K$ para todo $h \in H$, então $(hk)K(hk)^{-1} = h(kKk^{-1})h^{-1} = hKh^{-1} = K$ para todos $h \in H$ e $k \in K$. Isso mostra que K é normal em HK. A demonstração de que $(H \cap K)$ é normal em H é similar. (Verifique.)

Agora, vamos construir um isomorfismo entre HK/K e $H/(H \cap K)$. Considere a função $f\colon H \to HK/K$ dada por $f(h) = \overline{h}$. Primeiro, observe que $f(h_1h_2) = \overline{h_1h_2} = \overline{h_1h_2} = f(h_1)f(h_2)$ para todos $h_1, h_2 \in H$. Ou seja, f é um homomorfismo de grupos. O núcleo de f é:

$$\ker(f) = \{h \in H \mid f(h) = \overline{e}\} = \{h \in H \mid h \in K\} = (H \cap K).$$

Além disso, para todo $h \in H$ e $k \in K$, temos que $h^{-1}(hk) \in K$, ou seja, $\overline{hk} = \overline{h} \in HK/K$. Como $\overline{h} = f(h)$ para todo $h \in H$, então f é sobrejetora. Usando o primeiro Teorema de Isomorfismo de grupos, concluímos que $H/(H \cap K) = H/\ker(f) \cong \mathrm{im}(f) = HK/K$. □

O terceiro Teorema de Isomorfismo de grupos é o seguinte.

Teorema 9.6. *Seja G um grupo. Se $H \subseteq K \subseteq G$ são subgrupos normais, então $K/H \subseteq G/H$ é um subgrupo normal e*

$$\frac{G/H}{K/H} \cong G/K.$$

Demonstração. Denote os elementos de G/H por $\overline{g}$ e os elementos de G/K por $\overline{\overline{g}}$ $(g \in G)$. Vamos usar o primeiro Teorema de Isomorfismo de grupos para mostrar que $(G/H)/(K/H)$ é isomorfo a G/K. Considere a função $f\colon G/H \to G/K$ dada por $f(\overline{g}) = \overline{\overline{g}}$. Primeiro observe que f está bem definida. De fato, para todos $g \in G$ e $h \in H$, temos que $f(\overline{gh}) = \overline{\overline{gh}} = \overline{\overline{g}\,\overline{h}} = \overline{\overline{g}}$, pois $h \in H \subseteq K$.

Agora vamos verificar que $\ker(f) = K/H$. De fato,

$$\ker(f) = \{\overline{g} \in G/H \mid f(\overline{g}) = \overline{\overline{g}} = \overline{\overline{e}}\} = \{\overline{g} \in G/H \mid g \in K\} = K/H.$$

Para terminar, obsereve que $\mathrm{im}(f) = G/K$. De fato, para todo $\overline{\overline{g}} \in G/K$, temos que $\overline{\overline{g}} = f(\overline{g})$. Usando o primeiro Teorema de Isomorfismo de grupos, concluímos que $G/K = \mathrm{im}(f) \cong (G/H)/\ker(f) = (G/H)/(K/H)$. □

O próximo resultado descreve uma relação entre os subgrupos normais de um grupo e os subgrupos normais de seus quocientes.

Teorema 9.7. *Sejam G um grupo e $N \subseteq G$ um subgrupo normal. Existe uma bijeção (que preserva inclusão) entre o conjunto de subgrupos normais de G/N e o conjunto de subgrupos normais de G que contem N.*

Demonstração. Dados subgrupos normais $N \subseteq K \subseteq G$, pela primeira parte do terceiro Teorema de Isomorfismos de grupos, temos que K/N é um subgrupo normal de G/N. Denote por A o conjunto de subgrupos normais de G que contem N e por B o conjunto de subgrupos normais

de G/N. Vamos mostrar que a função $q\colon A \to B$ dada por $q(K) = K/N$, é uma bijeção. De fato, vamos construir uma inversa explícita para ela.

Defina a função $l\colon B \to A$ por $l(H) = \{g \in G \mid \overline{g} \in H\}$. Observe que, de fato, $N \subseteq l(H)$, pois $\overline{n} = \overline{e} \in H$ para todo $n \in N$. Além disso, por construção, $q(l(H)) = l(H)/N = H$ (ou seja, l é uma inversa à direita de q). Para terminar a demonstração, vamos mostrar que l também é uma inversa à esquerda de q:

$$l(q(K)) = \{g \in G \mid \overline{g} \in K/N\} = \{g \in G \mid g \in NK\} = NK = K. \qquad \square$$

Aula 10

Observação 10.1. Seja G, H dois grupos, $N \subseteq G$ um subgrupo normal e $f\colon (G/N) \to H$ um homomorfismo de grupos. Denote por $\pi\colon G \to G/N$ a projeção canônica, $\pi(g) = \overline{g}$. Observe que $(f \circ \pi)\colon G \to H$ é um homomorfismo de grupos.

Agora, nós podemos fazer a pergunta contrária. Dado um homomorfismo de grupos $F\colon G \to H$, sob que condições existe um homomorfismo de grupos $f\colon (G/N) \to H$ tal que $(f \circ \pi) = F$? A resposta é: se, e somente se, $N \subseteq \ker(F)$.

Se $N \subseteq \ker(F)$, então a função $f\colon G/N \to H$ definida por $f(\overline{g}) = F(g)$ é um homomorfismo de grupos. Primeiro vamos verificar que f está bem definida. Para todo $n \in N$, como $N \subseteq \ker(F)$, temos que: $f(\overline{gn}) = F(gn) = F(g)F(n) = F(g)$. Agora vamos verificar que f é de fato um homomorfismo de grupos: $f(\overline{g_1}\,\overline{g_2}) = f(\overline{g_1 g_2}) = F(g_1 g_2) = F(g_1)F(g_2) = f(\overline{g_1})f(\overline{g_2})$ para todos $g_1, g_2 \in G$. Além disso, por definição, $f \circ \pi = G$.

Por outro lado, se um homomorfismo de grupos $f\colon G/N \to H$ satisfaz $(f \circ \pi) = F$, então $F(n) = (f \circ \pi)(n) = f(\overline{n}) = f(\overline{e}) = e_H$ para todo $n \in N$. Ou seja, $N \subseteq \ker(F)$.

3.4. Composição em série e Teorema de Jordan-Hölder e grupos solúveis

Proposição 10.2. *Se G for um grupo abeliano finito e p for um primo que divide $|G|$, então existe $g \in G$ tal que $o(g) = p$.*

Demonstração. Escreva $|G| = pm$. Nós vamos usar indução em m. Primeiro, se $m = 1$, então $|G| = p$. Em particular, $G \setminus \{e_G\}$ é não-vazio. Além disso, pelo Teorema 8.11 (de Lagrange), para todo $g \in G \setminus \{e_G\}$, temos que $o(g) = p$.

Agora suponha que $m > 1$ e que o resultado seja válido para todo grupo de ordem pk, $k \in \{1, \dots, m-1\}$. Considere $x \in G \setminus \{e_G\}$. Se $o(x) = pk$ para algum $k \in \{1, \dots, m\}$, então tomando $g = x^k$, temos que $o(g) = p$ pelo Lemma 6.14(b). Caso contrário, se $p \nmid o(x)$, então pelo Teorema 8.11 (de Lagrange), $|G/\langle x\rangle| = pk$ para algum $k \in \{1, \dots, m-1\}$. Pela hipótese de indução, existe $\overline{y} \in G/\langle x\rangle$ tal que $o(\overline{y}) = p$, ou seja, existe algum $y \in G \setminus \langle x\rangle$ tal que $y^p \in \langle x\rangle$. Em particular, $y \notin \langle y^p\rangle$. Consequentemente, $p \mid o(y)$. De fato, se $p \nmid o(y)$, então como p é primo (ou seja, p seria coprimo com $o(y)$), existiriam $a, b \in \mathbb{Z}$ tais que

$$y = y^{o(y)a+pb} = (y^{o(y)})^a y^{pb} = (y^p)^b \in \langle y^p\rangle.$$

Ou seja, $o(y) = pk$ para algum $k \in \{1, \dots, m\}$. Tomando $g = y^k$, temos que $o(g) = p$. □

Definição 10.3. Um grupo G é dito simples quando G é não-trivial e não existe nenhum subgrupo normal próprio e não-trivial de G. (Ou seja, $|G| > 1$ e $N \subseteq G$ é um subgrupo normal se, e somente se, $N = \{e\}$ ou $N = G$.) Dado um grupo G, uma composição em série de G é uma cadeia de subgrupos normais

$$\{e\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_{k-1} \subsetneq N_k = G,$$

tal que N_i/N_{i-1} é simples para todo $i \in \{1, \dots, k\}$. Nesse caso, os grupos simples N_i/N_{i-1} ($i \in \{1, \dots, k\}$) são chamados de fatores da composição de G.

Teorema 10.4 (de Jordan-Hölder)**.** *Seja G um grupo finito não-trivial. Existe uma composição em série de G e o conjunto de fatores da composição de G é único (não depende da composição em série).*

Definição 10.5. Um grupo G é dito solúvel quando existe uma cadeia de subgrupos normais

$$\{e\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_{k-1} \subsetneq N_k = G,$$

tal que N_i/N_{i-1} é abeliano para todo $i \in \{1, \dots, k\}$.

Lema 10.6. *Sejam G um grupo e $N \subseteq G$ um subgrupo normal. G é solúvel se, e somente se, N e G/N são solúveis.*

Demonstração. Primeiro suponha que G é solúvel, ou seja, que existe uma cadeia de subgrupos normais $\{e\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_{k-1} \subsetneq N_k = G$ tal que N_i/N_{i-1} é abeliano para todo $i \in \{1, \ldots, k\}$. Verifique que

$$\{e\} = (N_0 \cap N) \subsetneq (N_1 \cap N) \subsetneq \cdots \subsetneq (N_{k-1} \cap N) \subsetneq (N_k \cap N) = N$$

é uma cadeia de subgrupos normais de N e que $(N_i \cap N)/(N_{i-1} \cap N)$ é abeliano para todo $i \in \{1, \ldots, k\}$. Verifique também que

$$\{e\} = (N_0/N) \subsetneq (N_1/N) \subsetneq \cdots \subsetneq (N_{k-1}/N) \subsetneq (N_k/N) = G/N$$

é uma cadeia de subgrupos normais de G/N e observe que $(N_i/N)/(N_{i-1}/N) \cong N_i/N_{i-1}$ é abeliano para todo $i \in \{1, \ldots, k\}$ pelo Teorema 9.6.

Agora suponha que N e G/N são grupos solúveis, ou seja, que existem cadeias de subgrupos normais

$$\{e\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_{k-1} \subsetneq N_k = N \quad \text{e}$$
$$\{\overline{e}\} = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_{\ell-1} \subsetneq K_\ell = G/N,$$

tais que N_i/N_{i-1} e K_j/K_{j-1} são abelianos para todos $i \in \{1, \ldots, k\}$ e $j \in \{1, \ldots, \ell\}$. Pelo Teorema 9.7, existem subgrupos normais $N_{k+1}, \ldots, N_{k+\ell} \subseteq G$ que contem N e tais que $N_{k+j}/N \cong K_j$ para todo $j \in \{1, \ldots, \ell\}$. Além disso, pelo Teorema 9.6, $N_{k+j}/N_{k+j-1} \cong K_j/K_{j-1}$ é abeliano para todo $j \in \{1, \ldots, \ell\}$. Portanto

$$\{e\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_k \subsetneq \cdots \subsetneq N_{k+\ell} = G$$

é uma cadeia de subgrupos normais tal que N_i/N_{i-1} é abeliano para todo $i \in \{1, \ldots, k+\ell\}$. □

Aula 11

3.5. Transposições e Grupo Alternado

Definição 11.1. Dado $n \geq 2$, os elementos $(i\ j) \in S_n$ são chamados de transposiçõoes para todos $i, j \in \{1, \ldots, n\}$ distintos.

Proposição 11.2. *Seja $n \geq 2$. Para todo $\sigma \in S_n$, existem transposições $\tau_1, \ldots, \tau_\ell \in S_n$ tais que $\sigma = \tau_1 \cdots \tau_\ell$.*

Demonstração. Fixe $\sigma \in S_n$. Lembre que existem ciclos disjuntos $\sigma_1, \ldots, \sigma_k \in S_n$ tais que $\sigma = \sigma_1 \cdots \sigma_k$. Para cada $i \in \{1, \ldots, k\}$, denote $o(\sigma_i) = p_i$. Então, para cada $i \in \{1, \ldots, k\}$, existem $a_1, \ldots, a_{p_i} \in \{1, \ldots, n\}$ distintos tais que $\sigma_i = (a_1\ a_2\ \ldots\ a_{p_i})$. Agora observe que:

$$(a_1\ a_2\ \ldots\ a_{p_i}) = (a_1\ a_{p_i}) \cdots (a_1\ a_2). \qquad \square$$

Observe que a decomposição de uma permutação em transposições não é única. Por exemplo, $(1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(2\ 3) = (2\ 3)(1\ 3)$. Mas existe um invariante em todas essas decomposições. Para mostrar isso, nós vamos precisar da seguinte construção.

Dados $n \geq 2$ e $\sigma \in S_n$, considere a matriz $I_\sigma \in M_n(\mathbb{R})$ cuja i-ésima linha é a $\sigma(i)$-ésima linha da matriz identidade. Por exemplo, se $n = 3$, então:

$$I_{(1)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad I_{(1\ 2\ 3)} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad I_{(1\ 3\ 2)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

$$I_{(1\ 2)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad I_{(1\ 3)} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad I_{(2\ 3)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Agora, para cada $\sigma \in S_n$, defina o sinal de σ como $\varepsilon(\sigma) = \det(I_\sigma)$. Observe que $\varepsilon(\sigma) \in \{-1, 1\}$, pois trocando as linhas de I_σ (o que só muda o sinal do determinante), obtemos a matriz identidade (cujo determinante é 1).

Finalmente, observe que o conjunto $\{-1, 1\}$ munido da multiplicação usual de números é um grupo isomorfo a $\mathbb{Z}_2$. (De fato, verifique que $f\colon \mathbb{Z}_2 \to \{-1, 1\}$ dada por $f(\overline{0}) = 1$ e $f(\overline{1}) = -1$ é um isomorfismo de grupos.) Nós temos portanto o seguinte resultado.

Lema 11.3. *Para todo $n \geq 2$, a função $\varepsilon\colon S_n \to \{-1, 1\}$ é um homomorfismo sobrejetor de grupos.*

Demonstração. Fixe $n \geq 2$ e considere a base canônica $\{E_{ij} \mid i, j \in \{1, \ldots, n\}\}$ de $M_n(\mathbb{R})$. (Lembre que E_{ij} é a matriz cuja entrada (i, j) é 1 e todas as outras entradas são 0. Lembre também que $E_{ij}E_{k\ell} = \delta_{jk}E_{i\ell}$ para todos $i, j, k, \ell \in \{1, \ldots, n\}$). Agora observe que $I_\sigma = E_{1,\sigma(1)} + E_{2,\sigma(2)} + \cdots + E_{n,\sigma(n)}$ para todo $\sigma \in S_n$. Portanto

$$\begin{aligned}
\varepsilon(\rho)\varepsilon(\sigma) &= \det(I_\rho)\det(I_\sigma) \\
&= \det(I_\sigma)\det(I_\rho) \\
&= \det(I_\sigma I_\rho) \\
&= \det\left((E_{1,\sigma(1)} + E_{2,\sigma(2)} + \cdots + E_{n,\sigma(n)})(E_{1,\rho(1)} + E_{2,\rho(2)} + \cdots + E_{n,\rho(n)})\right) \\
&= \det\left((E_{1,\sigma(1)} + E_{2,\sigma(2)} + \cdots + E_{n,\sigma(n)})(E_{\sigma(1),\rho(\sigma(1))} + E_{\sigma(2),\rho(\sigma(2))} + \cdots + E_{\sigma(n),\rho(\sigma(n))})\right) \\
&= \det(E_{1,\rho(\sigma(1))} + E_{2,\rho(\sigma(2))} + \cdots + E_{n,\rho(\sigma(n))}) \\
&= I_{\rho\sigma}.
\end{aligned}$$

Isso mostra que ε é um homomorfismo de grupos. Além disso, $\varepsilon(1) = 1$ e $\varepsilon(1\ 2) = -1$. Portanto ε é sobrejetora. □

Definição 11.4. Dado $n \geq 2$, uma permutação $\sigma \in S_n$ é dita par quando $\varepsilon(\sigma) = 1$ e ímpar quando $\varepsilon(\sigma) = -1$. O grupo alternado é definido como o subgrupo de S_n dado por

$$A_n = \{\sigma \in S_n \mid \sigma \text{ é par}\}.$$

Observe que $A_n = \ker(\varepsilon)$. Portanto $A_n \subseteq S_n$ é normal. Além disso, $|S_n : A_n| = 2$, pois $\varepsilon\colon S_n \to \{-1, 1\}$ induz um isomorfismo de grupos $S_n/A_n \cong \mathbb{Z}_2$.

4.1. Ações de grupos e representações por permutações

Sejam G um grupo e X um conjunto não-vazio. Lembre que S_X denota o grupo de permutações (bijeções) de X. Lembre também (da Proposição 4.16) que toda ação de G em X induz um homomorfismo de grupos $G \to S_X$, e que todo homomorfismo de grupos $G \to S_X$ induz uma ação de G em X.

Definição 11.5. Sejam G um grupo e X um conjunto não-vazio. Uma representação por permutações de G em X é um homomorfismo de grupos $\varphi\colon G \to S_X$. A ação $\alpha_\varphi\colon G \times X \to X$ dada por $\alpha_\varphi(g, x) = \varphi(g)(x)$ é dita induzida. O núcleo de α_φ é definido como o núcleo do homomorfismo φ. A ação α_φ é dita fiel quando seu núcleo é trivial ($\ker(\varphi) = \{e_G\}$). A órbita de um elemento $x \in X$ por uma ação $\alpha\colon G \times X \to X$ é o subconjunto $G \cdot x = \{\alpha(g, x) \in X \mid g \in G\}$.

Exemplo 11.6. Seja $n \geq 3$. Lembre que D_{2n} é o grupo de simetrias de um n-ágono regular e que, enumerando os vértices desse n-ágono com os elementos de $\mathbb{Z}_n$, obtemos uma ação de D_{2n} em $\mathbb{Z}_n$, $\alpha\colon D_{2n} \times \mathbb{Z}_n \to \mathbb{Z}_n$, onde $\alpha(\sigma, \bar{i}) = \sigma(\bar{i})$ é a imagem do vértice $\bar{i}$ pela simetria σ.

Como $\mathbb{Z}_n$ é um conjunto com n elementos, $S_{\mathbb{Z}_n} = S_n$. Assim, $\varphi_\alpha\colon D_{2n} \to S_n$ é dada por $\varphi_\alpha(\sigma) = \alpha(\sigma, -) = \sigma$. Ou seja, φ_α é a inclusão de D_{2n} em S_n. Em particular, essa ação é fiel. Agora observe que $D_{2n} \cdot \bar{i} = \mathbb{Z}_n$ para todo $\bar{i} \in \mathbb{Z}_n$. De fato, $r^{j-i}(\bar{i}) = \bar{j}$ para todo $\bar{j} \in \mathbb{Z}_n$. Portanto essa ação tem apenas uma órbita.

Exemplo 11.7. Considere um grupo G e tome $X = G$. Lembre que $m\colon G \times G \to G$ é uma ação de G em G. Neste caso, $\varphi_m\colon G \to S_G$ é a função tal que $\varphi_m(g)\colon G \to G$, para cada $g \in G$, é a multiplicação à esquerda por g, $\varphi_m(g)(h) = gh$. (Observe que $\varphi_m(g)$ é uma permutação cuja inversa é $\varphi_m(g^{-1})$.)

Para mostrar que m é uma ação fiel, vamos mostrar que o núcleo de φ_m é trivial. De fato, se $g \in G$ é tal que $\varphi_m(g) = \mathrm{id}_G$, então $gh = h$ para todo $h \in H$. Logo $g = e_G$. Uma consequência do fato de m ser fiel é o fato de que $\mathrm{im}(\varphi_m)$ é um subgrupo de S_G isomorfo a G. Ou seja, G é isomorfo a um subgrupo de um grupo de permutações (Teorema de Cayley).

Para terminar, vamos mostrar que $G \cdot g = G$ para todo $g \in G$. De fato, $h = (hg^{-1})g$ para todo $h \in G$. Ou seja, todo elemento $h \in G$ está na órbita $G \cdot g$. Portanto essa ação também tem apenas uma órbita.

Exemplo 11.8. Considere o grupo multiplicativo $\mathbb{R} \setminus \{0\}$ em $X = \mathbb{R}^2$ (ou poderia se qualquer outro $\mathbb{R}$-espaço vetorial). Lembre que a multiplicação escalar $\alpha\colon (\mathbb{R} \setminus \{0\}) \times \mathbb{R}^2 \to \mathbb{R}^2$, $\alpha(\lambda, v) = \lambda v$ é uma ação. Neste caso, $\varphi_\alpha\colon \mathbb{R} \setminus \{0\} \to S_{\mathbb{R}^2}$ é a função tal que $\varphi_\alpha(\lambda)\colon \mathbb{R}^2 \to \mathbb{R}^2$ é a multiplicação pelo escalar λ.

Essa ação também é fiel. De fato, $\varphi_\alpha(\lambda) = \mathrm{id}_{\mathbb{R}^2}$ se, e somente se, $\lambda(x, y) = (x, y)$ para todo $(x, y) \in \mathbb{R}^2$. Mas isso ocorre se, e somente se, $\lambda = 1 = e_{\mathbb{R}\setminus\{0\}}$. Agora observe que $(\mathbb{R} \setminus \{0\}) \cdot (0, 0) = \{(0, 0)\}$ (só um ponto) e que $(\mathbb{R} \setminus \{0\}) \cdot (x, y) = \{(\lambda x, \lambda y) \mid \lambda \in \mathbb{R} \setminus \{0\}\}$ (é uma reta sem a origem) para todo $(x, y) \neq (0, 0)$.

Exemplo 11.9. Considere o conjunto $M_n(\mathbb{R})$ e o grupo multiplicativo $GL_n(\mathbb{R})$, formado pelas matrizes em $M_n(\mathbb{R})$ que são invertíveis. Defina $\alpha\colon GL_n(\mathbb{R}) \times M_n(\mathbb{R}) \to M_n(\mathbb{R})$ por $\alpha(A, B) = ABA^{-1}$. (Verifique que α é uma ação.) Nesse caso, $\varphi_\alpha(A)\colon M_n(\mathbb{R}) \to M_n(\mathbb{R})$ é a conjugação pela matriz A ($\varphi_\alpha(A)(B) = ABA^{-1}$).

Observe que essa ação não é fiel. De fato, $\varphi_\alpha = \mathrm{id}_{M_n(\mathbb{R})}$ se e somente se, $ABA^{-1} = B$ para toda $B \in M_n(\mathbb{R})$. Isso ocorre se, e somente se, $AB = BA$ para toda $B \in M_n(\mathbb{R})$. Agora, as matrizes de $GL_n(\mathbb{R})$ que comutam com todas as matrizes de $M_n(\mathbb{R})$ são da forma $\lambda \mathrm{Id}_n$, com $\lambda \in \mathbb{R}\backslash\{0\}$. Portanto o núcleo dessa ação é o conjunto de matrizes escalares, $\{\lambda \mathrm{Id}_n \mid \lambda \in \mathbb{R}\backslash\{0\}\}$.

Usando a linguagem de órbitas, podemos definir matrizes semelhantes como aquelas que estão na mesma órbita por essa ação. Além disso, matrizes diagonalizáveis são aquelas cujas órbitas contém alguma matriz diagonal (não necessariamente escalar). Observe que essa ação tem infinitas órbitas distintas. De fato, se $A \in GL_n(\mathbb{R}) \cdot B$, então $\det(A) = \det(B)$. Como existe pelo menos uma matriz com determinante d para cada $d \in \mathbb{R}$ e $|\mathbb{R}|$ é infinita, segue que existem pelo menos $|\mathbb{R}|$ órbitas distintas.

Observação 11.10. Nos exemplos acima, a maioria das ações é fiel. O motivo para isso é que é mais natural pensar em ações fiéis. De fato, pelo Primeiro Teorema de Isomorfismo, toda ação $\alpha\colon G \times X \to X$ induz uma ação $\tilde{\alpha}\colon G/\ker(\varphi_\alpha) \times X \to X$, dada por $\tilde{\alpha}(\overline{g}, x) = \alpha(g, x)$, que é fiel.

Por outro lado, para toda ação $\alpha\colon H \times X \to X$ e todo homomorfismo de grupos $\psi\colon G \to H$, temos que $(\varphi_\alpha \circ \psi)\colon G \to S_X$ também é um homomorfismo de grupos. Consequentemente, tomando um subgrupo normal $N \subseteq G$, $H = G/N$ e $\psi = \pi$ a projeção canônica, obtemos uma ação $\alpha_{(\varphi_\alpha \circ \psi)}$ de G em X cujo núcleo contem N. Em particular, isso nos permite construir uma ação não-fiel a partir de uma ação fiel.

Lembre (da Definição 6.2 e Proposição 6.3) que, dada uma ação $\alpha\colon G \times X \to X$ de um grupo G em um conjunto não-vazio X, o estabilizador de $x \in X$ é o subgrupo

$$G_x = \{g \in G \mid \alpha(g, x) = x\} \subseteq G.$$

Proposição 11.11. *Seja G um grupo agindo em um conjunto não-vazio X. A relação em X definida por*

$$x \sim y \quad \text{se, e somente se,} \quad x \in G \cdot y$$

é uma relação de equivalência. Além disso, $|G \cdot x| = |G\colon G_x|$.

Demonstração. Primeiro vamos mostrar que $\sim$ é uma relação de equivalência.

- $x \sim x$, pois $\alpha(e_G, x) = x$ para todo $x \in X$.
- Se $x \sim y$, então existe $g \in G$ tal que $x = \alpha(g, y)$. Consequentemente,

  $$\alpha(g^{-1}, x) = \alpha(g^{-1}, \alpha(g, y)) = \alpha(g^{-1}g, y) = \alpha(e_G, y) = y.$$

  Logo $y \in G \cdot x$, ou seja, $y \sim x$.
- Se $x \sim y$ e $y \sim z$, então existem $g, h \in G$ tais que $x = \alpha(g, y)$ e $y = \alpha(h, z)$. Consequentemente, $x = \alpha(g, \alpha(h, z)) = \alpha(gh, z)$. Logo $x \in G \cdot z$, ou seja, $x \sim z$.

Para mostrar a segunda parte, considere a função $f\colon G/G_x \to X$ dada por $f(\overline{g}) = \alpha(g, x)$. Primeiro, vamos mostrar que f é bem definida. Dados $g \in G$ e $h \in G_x$, temos que $f(\overline{gh}) = \alpha(gh, x) = \alpha(g, \alpha(h, x)) = \alpha(g, x) = f(\overline{g})$. Agora vamos mostrar que f é injetora. De fato, se $g, h \in G$ são tais que $f(\overline{g}) = f(\overline{h})$, então $\alpha(h^{-1}g, x) = \alpha(h^{-1}, \alpha(g, x)) = \alpha(h^{-1}, \alpha(h, x)) = x$. Logo $h^{-1}g \in G_x$, ou seja, $\overline{g} = \overline{h}$. Para terminar, observe que $\mathrm{im}(f) = \{\alpha(g, x) \mid g \in G\} = G \cdot x$. Como $|G\colon G_x| = |G/G_x|$ e f induz uma bijeção entre G/G_x e $G \cdot x$, segue que $|G\colon G_x| = |G \cdot x|$. □

Definição 11.12. Uma ação de um grupo G em um conjunto não-vazio X é dita transitiva quando $G \cdot x = X$ para algum $x \in X$.

Observe que, se $G \cdot x = X$ para algum $x \in X$, então $G \cdot y = X$ para todo $y \in X$. De fato, se $G \cdot x = X$, então $y \sim x$ para todo $y \in X$, ou seja, $x \in G \cdot y$ para todo $y \in X$. Segue daí que $X = G \cdot x \subseteq G \cdot y \subseteq X$, e consequentemente, $G \cdot y = X$, para tdodo $y \in X$. Ou seja, uma ação é transitiva quando existe apenas uma órbita.

Seja G um grupo finito e X um conjunto não-vazio. Pela Proposição 11.11, se X é infinito, ele não admite nenhuma ação transitiva de G. Ainda mais, pelo Teorema 8.11 (de Lagrange), se X admite uma ação transitiva de G, então $|X| \mid |G|$.

Exemplo 11.13. Observe que a ação de D_{2n} em $\mathbb{Z}_n$ (dada no Exemplo 11.6) e a ação de G em G dada por multiplicação à esquerda (Exemplo 11.7) são transitivas. Mas a ação de $\mathbb{R} \setminus \{0\}$ em $\mathbb{R}^2$ por multiplicação escalar (Exemplo 11.8) e a ação de $GL_n(\mathbb{R})$ em $M_n(\mathbb{R})$ por conjugação (Exemplo 11.9) não são transitivas.

Aula 12

4.2. Grupos agindo em si mesmos por multiplicação e Teorema de Cayley

Sejam G um grupo e $g \in G$. Lembre que, para todo subconjunto $X \subseteq G$, (gXg^{-1}) denota o subconjunto $\{gxg^{-1} \in G \mid x \in X\}$. Além disso, se $H \subseteq G$ for um subgrupo, então $gHg^{-1} \subseteq G$ é um subgrupo e $gH \subseteq G$ é um subconjunto chamado classe lateral à esquerda (classe de equivalência pela relação (8.1)) associada a g.

Lema 12.1. *Sejam G um grupo e $H \subseteq G$ um subgrupo. Denote por A o conjunto de classes laterais à esquerda $A = \{gH \mid g \in G\}$. A função $\alpha\colon G \times A \to A$ dada por $\alpha(g, aH) = (ga)H$ é uma ação de G em A.*

Demonstração. Vamos verificar as duas condições da Definição 4.11.

(i) Dados $g_1, g_2 \in G$ e $aH \in A$, temos que $\alpha(g_1, \alpha(g_2, aH)) = \alpha(g_1, (g_2a)H) = (g_1(g_2a))H = ((g_1g_2)a)H = \alpha(g_1g_2, aH)$.
(ii) Dado $aH \in A$, temos que $\alpha(e_G, aH) = (e_Ga)H = aH$. □

No caso em que $H = \{e_G\}$, o conjunto A do lema acima se identifica a G e a ação acima se identifica à ação dada por multiplicação à esquerda de G em G.

Lema 12.2. *Sejam G um grupo e $H \subseteq G$ um subgrupo. Então $\bigcap_{g\in G} gHg^{-1}$ é o maior subgrupo normal de G que está contido em H.*

Demonstração. Primeiro lembre que, como $H \subseteq G$ é um subgrupo, então $gHg^{-1} \subseteq G$ é um subgrupo para todo $g \in G$. Depois, observe que $e_GHe_G^{-1} = H$. Portanto $\bigcap_{g\in G} gHg^{-1}$ é um subgrupo de G contido em H. Além disso, para todos $a \in G$ e $x \in \bigcap_{g\in G} gHg^{-1}$, temos que $axa^{-1} \in (ag)H(ag)^{-1}$ para todo $g \in G$. Portanto $\bigcap_{g\in G} gHg^{-1}$ é um subgrupo normal de G.

Agora suponha que N seja um subgrupo normal de G contido em H. Então $N = gNg^{-1} \subseteq gHg^{-1}$ para todo $g \in G$. Isso implica que $N = \bigcap_{g\in G} gNg^{-1} \subseteq \bigcap_{g\in G} gHg^{-1}$. Logo $\bigcap_{g\in G} gHg^{-1}$ é o maior subgrupo normal de G que está contido em H. □

Teorema 12.3. *Sejam G um grupo e $H \subseteq G$ um subgrupo. Denote por A o conjunto de classes laterais à esquerda, $A = \{gH \mid g \in G\}$, por $\alpha\colon G \times A \to A$ a ação dada por $\alpha(g, aH) = (ga)H$, e por $\pi_H\colon G \to S_A$ o homomorfismo de grupos φ_α, induzido da ação α.*

(a) A ação de G em A é transitiva.
(b) O estabilizador de e_GH é $G_{e_GH} = H$.
(c) $\ker(\pi_H) = \bigcap_{g\in G} gHg^{-1}$. Consequentemente, $\ker(\pi_H)$ é o maior subgrupo normal de G que está contido em H.

Demonstração. (a) Lembre que a ação de G em A é transitiva se, para quaisquer $g_1H, g_2H \in A$, existe $g \in G$ tal que $\alpha(g, g_1H) = g_2H$. Tomando $g = g_2g_1^{-1}$, temos

$$\alpha(g, g_1H) = ((g_2g_1^{-1})g_1)H = g_2H.$$

(b) Lembre (da Definição 6.2) que $G_{e_GH} = \{g \in G \mid \alpha(g, e_GH) = e_GH\}$. Como $e_GH = \alpha(g, e_GH) = g(e_GH) = gH$ se, e somente se, $g \in H$, segue que $G_{e_GH} = H$.
(c) Por definição, $\ker(\pi_H) = \{g \in G \mid \alpha(g, aH) = aH\}$ para todo $a \in G$. Fixe $a \in G$. Observe que $g(aH) = aH$ se, e somente se, $gah \in aH$ para todo $h \in H$, ou seja, para todo $h \in H$,

existe $h' \in H$ tal que $gah = ah'$. Neste caso, $g = a(h'h^{-1})a^{-1} \in aHa^{-1}$. Por outro lado, se $g \in aHa^{-1}$, então $(ga)H = ((aha^{-1})a)H = aH$. Isso mostra que

$$\ker(\pi_H) = \{g \in G \mid g \in aHa^{-1} \text{ para todo } a \in G\} = \bigcap_{a \in G} aHa^{-1}.$$

O fato de que $\ker(\pi_H)$ é o maior subgrupo normal de G que está contido em H segue direto do Lema 12.2. □

Um caso particular do teorema anterior, o caso em que $H = \{e_G\}$, mostra que todo grupo é um subgrupo de algum grupo de simetrias.

Teorema 12.4 (de Cayley)**.** *Se G for um grupo de ordem $n \geq 1$, então G é isomorfo a um subgrupo de S_n.*

Demonstração. Considere o subgrupo $H = \{e_G\}$. Pelo Teorema 12.3, $\ker(\pi_H) = H = \{e_G\}$. Logo, $\pi_H \colon G \to S_G$ é um homomorfismo injetor de grupos. Portanto, pelo Primeiro Teorema de Isomorfismo de grupos, G é isomorfo a $\mathrm{im}(\pi_H)$, que é um subgrupo do grupo de permutações $S_G \cong S_n$. □

Corolário 12.5. *Se G for um grupo finito e p for o menor primo que divide $|G|$, então todo subgrupo de G de índice p é normal.*

Demonstração. Lembre que um subgrupo $N \subseteq G$ é normal se, e somente se, $gNg^{-1} = N$ para todo $g \in G$. Denote por A o conjunto de classes laterais à esquerda $A = \{gN \mid g \in G\}$. Usando o Teorema 12.3(c), temos que $N \subseteq G$ é normal se, e somente se, o núcleo da ação $\alpha \colon G \times A \to A$ dada por $\alpha(g, aN) = (ga)N$ é igual a N. Lembre que $|G \colon N|$ é a quantidade de classes laterais distintas da forma gN, $g \in G$; ou seja, $|A| = |G \colon N| = p$ (por hipótese). Pelo Teorema de Lagrange, $p | N \colon \ker(\varphi_\alpha)| = |G \colon \ker(\varphi_\alpha)| = |\mathrm{im}(\varphi_\alpha)|$ divide $|S_A| = p!$. Como p é o menor primo que divide $|G|$, então $|N \colon \ker(\varphi_\alpha)| = 1$. Ou seja, $N = \ker(\varphi_\alpha)$. □

4.3. Grupos agindo em si mesmos por conjugação e a Equação de Classe

Seja G um grupo. Lembre que $\mathcal{P}(G)$ denota o conjunto de subconjuntos de G.

Proposição 12.6. *Seja G um grupo. A função $\alpha \colon G \times \mathcal{P}(G) \to \mathcal{P}(G)$ dada por $\alpha(g, X) = gXg^{-1}$ é uma ação.*

Demonstração. Vamos verificar as duas condições da Definição 4.11.

(i) Dados $g_1, g_2 \in G$ e $X \in \mathcal{P}(G)$, temos que

$$\alpha(g_1, \alpha(g_2, X)) = \alpha(g_1, (g_2 X g_2^{-1})) = g_1(g_2 X g_2^{-1})g_1^{-1} = (g_1 g_2)X(g_1 g_2)^{-1} = \alpha(g_1 g_2, X).$$

(ii) Dado $X \in \mathcal{P}(G)$, temos que $\alpha(e_G, X) = e_G X e_G^{-1} = X$. □

Definição 12.7. Dado um grupo G, dois subconjuntos $X, Y \subseteq G$ são ditos conjugados quando existe $g \in G$ tal que $X = gYg^{-1}$. (Em particular, dois elementos $a, b \in G$ são ditos conjugados quando $\{a\}$ e $\{b\}$ são conjugados.) Para cada $x \in G$, a órbita $\{gxg^{-1} \in G \mid g \in G\}$ é chamada de classe de conjugação de x em G.

Exemplo 12.8. Se um grupo G é abeliano, então $gxg^{-1} = x$ para todos $g, x \in G$. Consequentemente $gXg^{-1} = X$ para todos $g \in G$ e $X \in \mathcal{P}(G)$. Ou seja, neste caso, a ação de G em $\mathcal{P}(G)$ definida via conjugação é trivial.

Exemplo 12.9. Se $|G| > 1$, então a ação de G em $\mathcal{P}(G)$ definida via conjugação não é transitiva. De fato, $ge_Gg^{-1} = e_G$ para todo $g \in G$. Portanto a órbita de $\{e_G\}$ contem apenas $\{e_G\}$. Como $G \neq \{e_G\}$, então existe $X \in \mathcal{P}(G)$ que não é conjugado a $\{e_G\}$, a saber, $X = G$.

Exemplo 12.10. As classes de conjugação em S_3 são:

- $\{(1)\}$. De fato, $\sigma(1)\sigma^{-1} = (1)$ para todo $\sigma \in S_3$.
- $\{(1\ 2), (1\ 3), (2\ 3)\}$. De fato,
$$(1\ 3)(1\ 2)(1\ 3) = (2\ 3) = (1\ 2\ 3)(1\ 2)(1\ 3\ 2)$$
$$(2\ 3)(1\ 2)(2\ 3) = (1\ 3) = (1\ 3\ 2)(1\ 2)(1\ 2\ 3).$$
- $\{(1\ 2\ 3), (1\ 3\ 2)\}$. De fato,
$$(1\ 3\ 2) = (1\ 2)(1\ 2\ 3)(1\ 2) = (2\ 3)(1\ 2\ 3)(2\ 3) = (1\ 3)(1\ 2\ 3)(1\ 3).$$

Proposição 12.11. *Seja G um grupo. Dado um subconjunto $X \subseteq G$, a quantidade de subconjuntos de G conjugados a X é $|G\colon N_G(X)|$. Em particular, para todo $x \in G$, a quantidade de elementos de G conjugados a x é $|G\colon C_G(x)|$.*

Demonstração. Considere a função $f\colon G/N_G(X) \to \mathcal{P}(X)$ dada por $f(\overline{g}) = gXg^{-1}$. Vamos verificar que f está bem definida. De fato, $f(\overline{gn}) = (gn)X(gn)^{-1} = g(nXn^{-1})g^{-1} = gXg^{-1} = f(\overline{g})$ para todos $g \in G$ e $n \in N_G(X)$. Agora observe que $\mathrm{im}(f) = \{gXg^{-1} \mid g \in G\}$. Em particular, $|\mathrm{im}(f)|$ é a quantidade de subconjuntos de G conjugados a X. Finalmente, observe que f é injetora. De fato, se $f(\overline{g_1}) = f(\overline{g_2})$, então $g_1Xg_1^{-1} = g_2Xg_2^{-1}$. Logo $(g_2^{-1}g_1)X(g_2^{-1}g_1)^{-1} = X$, ou seja, $g_2^{-1}g_1 \in N_G(X)$. Isso significa que $\overline{g_1} = \overline{g_2}$. Portanto f induz uma bijeção entre $G/N_G(X)$ e $\mathrm{im}(f)$. Em particular, $|G\colon N_G(X)| = |\mathrm{im}(f)|$ é a quantidade de subconjuntos de G conjugados a X. Em particular, quando $X = \{x\}$, então $N_G(X) = C_G(x)$, e a segunda parte segue. □

Usando a decomposição de G em classes de conjugação, nós obtemos a chamada *Equação de Classe*.

Teorema 12.12. *Sejam G um grupo finito e $g_1, \ldots, g_n \in G$ representantes de cada uma das diferentes classes de conjugação de G. Suponha que $g_1, \ldots, g_r \in G \setminus Z(G)$ e $g_{r+1}, \ldots, g_n \in Z(G)$ para algum $r \in \{1, \ldots, n\}$. Então*
$$|G| = |Z(G)| + \sum_{i=1}^{r} |G\colon C_G(g_i)|.$$

Demonstração. Lembre (da Proposição 11.11) que uma ação de G em um conjunto decompõe esse conjunto em órbitas (as classes de equivalência) disjuntas. Em particular, considere a ação de G em G dada por $\alpha\colon G \times G \to G$, $\alpha(g, x) = gxg^{-1}$. Neste caso, a órbita de $x \in G$ é a classes de conjugação de x em G. Pela Proposição 12.11, a cardinalidade da classe de conjugação de x é $|G\colon C_G(x)|$. Em particular, se $z \in Z(G)$, então $gzg^{-1} = z$ para todo $g \in G$. O resultado segue. □

Proposição 12.13. *Se p é um primo e G um grupo tal que $|G| = p^n$, $n \geq 1$, então $Z(G) \neq \{e_G\}$.*

Demonstração. Sejam $g_1, \ldots, g_n \in G$ representantes de cada uma das diferentes classes de conjugação de G. Como $|G\colon H|$ divide $|G| = p^n$ para todo subgrupo $H \subseteq G$, então existem $0 < k_1, \ldots, k_n < n$ tais que $|G\colon C_G(g_i)| = p^{k_n}$ para cada $i \in \{1, \ldots, n\}$. Observe que $k_i = 0$ se, e somente se, $g_i \in Z(G)$. Usando a Equação de Classe, obtemos que $|Z(G)| = p^n - \sum_{i=1}^{r} p^{k_i}$. Como p divide o lado direito e $|Z(G)| \geq 1$, então p divide $|Z(G)|$. Logo $Z(G) \neq \{e_G\}$. □

Aula 13

4.3. Grupos agindo em si mesmos por conjugação e a Equação de Classe

Corolário 13.1. *Se p é primo e $|G| = p^2$, então G é abeliano e isomorfo a $\mathbb{Z}_{p^2}$ ou $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Demonstração. Como $|G| = p^2$, pela Proposição 12.13, $Z(G) \neq \{e_G\}$. Como, pelo Teorema 8.11 (de Lagrange), $|Z(G)|$ divide $|G| = p^2$, então $|Z(G)| \in \{p, p^2\}$. Suponha, primeiro, que $|Z(G)| = p$. Nesse caso, $|G/Z(G)| = p$. Portanto $Z(G)$ e $G/Z(G)$ são grupos cíclicos. Escolha $z, g \in G$ tais que $Z(G) = \{e_G, z, \ldots, z^{p-1}\}$ e $G/Z(G) = \{\overline{e_G}, \overline{g}, \ldots, \overline{g}^{p-1}\}$. Consequentemente, $G = \{g^i z^j \mid i, j \in \{0, \ldots, p-1\}\}$. Como $g(g^i z^j) = (g^{i+1} z^j) = (g^i z^j)g$, então $g \in Z(G)$, o que é uma contradição. Ou seja, $|Z(G)| = p^2$ e G é abeliano.

Agora observe que todo elemento de G tem ordem 1, p, ou p^2. Se existir um elemento de ordem p^2, então G é cíclico, isomorfo a $\mathbb{Z}_{p^2}$. Caso contrário, todo elemento $g \in G \setminus \{e_G\}$ tem ordem p. Neste caso, tome $x, y \in G$ tais que $x \notin \langle y \rangle$. Vamos mostrar que a função $f\colon \mathbb{Z}_p \times \mathbb{Z}_p \to G$ dada por $f(\overline{i}, \overline{j}) = x^i y^j$ é um isomorfismo de grupos. Como $o(x) = o(y) = p$, então f está bem definida. Como G é abeliano, então f é um homomorfismo de grupos. Vamos calcular o núcleo de f:

$$\ker(f) = \{(\overline{i}, \overline{j}) \in \mathbb{Z}_p \times \mathbb{Z}_p \mid x^i y^j = e_G\} = \{(\overline{i}, \overline{j}) \in \mathbb{Z}_p \times \mathbb{Z}_p \mid x^i = y^{-j}\}.$$

Como $o(x) = o(y) = p$ é primo e $x \notin \langle y \rangle$, então $x^i = y^{-j}$ se, e somente se, $i = j = 0$. Isso mostra que $\ker(f) = \{(\overline{0}, \overline{0})\}$, ou seja, f é injetora. Como $|\mathbb{Z}_p \times \mathbb{Z}_p| = p^2 = |G|$ e f é injetora, então f também é sobrejetora. Portanto f é um isomorfismo de grupos. □

Conjugação em S_n

O próximo resultado é um análogo ao fato de que conjugação de matrizes corresponde a mudança de base de uma transformação linear.

Proposição 13.2. *Sejam $n \geq 2$, $\tau \in S_n$ e $\sigma = (i_1 \ \cdots \ i_p) \in S_n$ um p-ciclo, $p \leq n$. Então*

$$\tau\sigma\tau^{-1} = (\tau(i_1) \ \cdots \ \tau(i_p)).$$

Demonstração. Vamos mostrar que $\tau \circ (i_1 \ \cdots \ i_p) = (\tau(i_1) \ \cdots \ \tau(i_p)) \circ \tau$. Observe que:

$$(\tau \circ (i_1 \ \cdots \ i_p))(i_j) = \tau(i_{j+1}) = ((\tau(i_1) \ \cdots \ \tau(i_p)) \circ \tau)(i_j) \quad \text{para todo } j \in \{1, \ldots, p-1\},$$
$$(\tau \circ (i_1 \ \cdots \ i_p))(i_p) = \tau(i_1) = ((\tau(i_1) \ \cdots \ \tau(i_p)) \circ \tau)(i_p).$$

Agora, se $i \notin \{i_1, \ldots, i_p\}$, então $\tau(i) \notin \{\tau(i_1), \ldots, \tau(i_p)\}$. Neste caso,

$$(\tau \circ (i_1 \ \cdots \ i_p))(i) = \tau(i) = ((\tau(i_1) \ \cdots \ \tau(i_p)) \circ \tau)(i).$$ □

Lema 13.3. *Sejam $n \geq 2$, $\sigma = (i_1 \ \cdots \ i_p)$ um p-ciclo e $\tau = (k_1 \ \cdots \ k_q)$ um q-ciclo, $p, q \leq n$. Se σ e τ são ciclos disjuntos, então $\tau\sigma = \sigma\tau$.*

Demonstração. Se σ e τ são disjuntos, então $\{i_1, \ldots, i_p\} \cap \{k_1, \ldots, k_q\} = \emptyset$. Logo, para todo $x \in \{i_1, \ldots, i_p\}$, $\tau(\sigma(x)) = \sigma(x)$ e $\sigma(\tau(x)) = \sigma(x)$. Analogamente, se $y \in \{k_1, \ldots, k_q\}$, então $\sigma(\tau(y)) = \tau(y) = \tau(\sigma(y))$. Se $z \notin \{i_1, \ldots, i_p\} \cup \{k_1, \ldots, k_q\}$, então $\tau(\sigma(z)) = z = \sigma(\tau(z))$. □

Lembre que todo elemento $\sigma \in S_n$ pode ser escrito como produto de ciclos disjuntos $\sigma = \sigma_1 \cdots \sigma_r$. Pelo lema anterior, esses ciclos σ_i, $i \in \{1, \ldots, r\}$, comutam, e portanto eles podem ser ordenados de acordo com seu comprimento: $o(\sigma_1) \leq \cdots \leq o(\sigma_r)$. Além disso, lembre que o conjunto $\{\sigma_1, \ldots, \sigma_r\}$, dos ciclos que aparecem na decomposição de σ, é único.

Definição 13.4. Dado $n > 0$, uma partição de n é uma sequência finita $n_1, \dots, n_r$, tal que $0 < n_1 \leq n_2 \leq \cdots \leq n_r$ e $n_1 + \cdots + n_r = n$. Dado $\sigma \in S_n$, o tipo cíclico de σ é definido como a (única) partição $n_1, \dots, n_r$ de n tal que $\sigma = \sigma_1 \cdots \sigma_r$ (incluindo os 1-ciclos) é uma decomposição de σ em ciclos disjuntos e $o(\sigma_1) = n_1, \dots, o(\sigma_r) = n_r$.

Proposição 13.5. *Seja $n \geq 2$. Dois elementos de S_n são conjugados se, e somente se, eles tem o mesmo tipo cíclico. Além disso, o número de classes de conjugação distintas em S_n é igual ao número de partições de n.*

Demonstração. Suponha que $\sigma, \tau \in S_n$ são conjugados. Considere uma decomposição $\sigma = \sigma_1 \cdots \sigma_r$ em ciclos disjuntos (incluindo os 1-ciclos) e tais que $o(\sigma_1) \leq \cdots \leq o(\sigma_r)$. Como σ e τ são conjugados, então existe $g \in S_n$ tal que $\tau = g\sigma g^{-1} = (g\sigma_1 g^{-1}) \cdots (g\sigma_r g^{-1})$. Pela Proposição 13.2, $(g\sigma_1 g^{-1}), \dots, (g\sigma_r g^{-1})$ são ciclos disjuntos e tais que $o(g\sigma_1 g^{-1}) \leq \cdots \leq o(g\sigma_r g^{-1})$. Pela unicidade do tipo cíclico, segue que o tipo cíclico de τ é o mesmo de σ.

Suponha agora que $\sigma, \tau \in S_n$ tem o mesmo tipo cíclico; ou seja, existem ciclos disjuntos $\sigma_1, \dots, \sigma_r \in S_n$ e ciclos disjuntos $\tau_1, \dots, \tau_r \in S_n$ tais que $\sigma = \sigma_1 \cdots \sigma_r$, $\tau = \tau_1 \cdots \tau_r$, e $o(\sigma_i) = o(\tau_i)$ para todo $i \in \{1, \dots, r\}$. Para cada $i \in \{1, \dots, r\}$, denote $o(\sigma_i) = p_i$, $\sigma_i = (k_1 \ \cdots \ k_{p_i})$ e $\tau_i = (\ell_1 \ \cdots \ \ell_{p_i})$. Defina $g_i \in S_n$ da seguinte forma $g(k_j) = \ell_j$ para $j \in \{1, \dots, p_i\}$ e $g_i(x) = x$ para todo $x \notin \{k_1, \dots, k_{p_i}\}$. Pela Proposição 13.2, $(g_i \sigma_i g_i^{-1}) = \tau_i$ e $g_i \sigma_j g_i^{-1} = \sigma_j$ para todo $j \neq i$. Considere $g = g_1 \circ \cdots \circ g_r \in S_n$ e observe que

$$g\sigma g^{-1} = (g\sigma_1 g^{-1}) \cdots (g\sigma_r g^{-1}) = (g_1 \sigma_1 g_1^{-1}) \cdots (g_r \sigma_r g_r^{-1}) = \tau_1 \cdots \tau_r = \tau.$$

Isso mostra que σ e τ são conjugados, e termina a demonstração. □

Exemplo 13.6. É fácil ver que em S_2, as classes de conjugação são: $\{(1)\}$ e $\{(1\ 2)\}$. Além disso, as únicas partições de 2 são: $2 = 2$ e $2 = 1 + 1$. A primeira corresponde ao 2-ciclo $(1\ 2)$ e a segunda corresponde ao produto de 1-ciclos $(1) = (1)(2)$.

Exemplo 13.7. Nós vimos no Exemplo 12.10 que as classes de conjugação de S_3 são:

- $\{(1)\}$, que corresponde à partição $3 = 1 + 1 + 1$;
- $\{(1\ 2), (1\ 3), (2\ 3)\}$, que corresponde a partição $3 = 1 + 2$;
- $\{(1\ 2\ 3), (1\ 3\ 2)\}$, que correponde a partição $3 = 3$.

Observe que $3 = 3$, $3 = 1 + 2$ e $3 = 1 + 1 + 1$ são todas as possíveis partições de 3.

Exemplo 13.8. Vamos calcular todas as possíveis partições de 4 e depois verificar que elas correspondem às classes de conjugação em S_4. As possíveis partições de 4 são: $4 = 4$, $4 = 1 + 3$, $4 = 2 + 2$, $4 = 1 + 1 + 2$ e $4 = 1 + 1 + 1 + 1$.

O 4-ciclo $(1\ 2\ 3\ 4)$ corresponde à partição $4 = 4$. Além disso, todo 4 ciclo é conjugado a $(1\ 2\ 3\ 4)$. De fato, pela Proposição 13.2, $(i_1\ i_2\ i_3\ i_4) = \tau(1\ 2\ 3\ 4)\tau^{-1}$ para $\tau \in S_4$ dada por $\tau(j) = i_j$. Como $|C_{S_4}(1\ 2\ 3\ 4)| = 4$ (verifique!), pela Proposição 12.11, existem 6 distintos 4-ciclos.

O 3-ciclo $(2\ 3\ 4) = (1)(2\ 3\ 4)$ corresponde à partição $4 = 1 + 3$. Além disso, todo 3-ciclo é conjugado a $(2\ 3\ 4)$. De fato, pela Proposição 13.2, $(i_1)(i_2\ i_3\ i_4) = \tau(2\ 3\ 4)\tau^{-1}$ para $\tau \in S_4$ dada por $\tau(j) = i_j$. Como $|C_{S_4}(1\ 2\ 3)| = 3$ (verifique!), pela Proposição 12.11, existem 8 distintos 3-ciclos.

O elemento $(1\ 2)(3\ 4)$ corresponde à partição $4 = 2 + 2$. Além disso, todo elemento da forma $(i_1\ i_2)(i_3\ i_4)$ é conjugado a $(1\ 2)(3\ 4)$. De fato, pela Proposição 13.2, $\tau(1\ 2)(3\ 4)\tau^{-1} = (\tau(1\ 2)\tau^{-1})(\tau(3\ 4)\tau^{-1}) = (i_1\ i_2)(i_3\ i_4)$ para $\tau \in S_4$ dada por $\tau(j) = i_j$. Como $|C_{S_4}((1\ 2)(3\ 4))| = 8$ (verifique!), pela Proposição 12.11, existem 3 elementos da forma $(i_1\ i_2)(i_3\ i_4)$ distintos.

O 2-ciclo $(3\ 4) = (1)(2)(3\ 4)$ corresponde à partição $4 = 1 + 1 + 2$. Além disso, todo 2-ciclo é conjugado a $(3\ 4)$. De fato, pela Proposição 13.2, $(i_1)(i_2)(i_3\ i_4) = \tau(3\ 4)\tau^{-1}$ para $\tau \in S_4$ dada por $\tau(j) = i_j$. Como $|C_{S_4}(3\ 4)| = 4$ (verifique!), pela Proposição 12.11, existem 6 distintos 2-ciclos.

A identidade $(1) = (1)(2)(3)(4)$ é o único elemento correspondente à partição $4 = 1+1+1+1$.

Teorema 13.9. *A_5 é um grupo simples.*

Demonstração. Existem cinco classes de conjugação distintas em A_5 e elas tem respectivamente 1, 12, 12, 15 e 20 elementos (ver os detalhes no livro). Agora, seja $N \subseteq A_5$ um subgrupo normal. Por definição $gng^{-1} \in N$ para todo $n \in N$. Ou seja, para todo $n \in N$, a classe de conjugação de n está toda contida em N. Como a única classe de conjugação que é um subgrupo é $\{(1)\}$, se N é um subgrupo não-trivial, então N é a união de duas ou mais classes de conjugação. Ou seja, $|N| \in \{13, 16, 21, 25, 28, 33, 36, 40, 45, 48, 60\}$. Mas, como $|N|$ divide $|A_5| = |S_5|/2 = 5!/2 = 60$, então $|N| \in \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$. Observe que os únicos subgrupos possíveis são $N = \{e_G\}$ ou $N = A_5$. Isso mostra que A_5 é simples. □

Aula 14

4.4. Automorfismos

Definição 14.1. Seja G um grupo. Um automorfismo de G é um isomorfismo de grupos $f\colon G \to G$. O conjunto de todos os automorfismos de G é denotado por $\mathrm{Aut}(G)$.

Exercício 14.2. Dado um grupo G, o conjunto $\mathrm{Aut}(G)$ munido da composição de funções é um grupo.

Proposição 14.3. *Sejam G um grupo e $N \subseteq G$ um subgrupo normal. A função definida por $\alpha\colon G \times N \to N$, $\alpha(g,n) = gng^{-1}$ é uma ação de G em N. Além disso, $\varphi_\alpha\colon G \to \mathrm{Aut}(N)$ é um homomorfismo de grupos com núcleo $C_G(N)$.*

Demonstração. Primeiro, como N é um subgrupo normal, $gng^{-1} \in N$ para todos $g \in G$, $n \in N$. O fato de α satisfazer as condições (i) e (ii) segue da Proposição 12.6. Logo, pela Proposição 4.16(a), $\varphi_\alpha\colon G \to S_N$ é um homomorfismo de grupos. Vamos mostrar que, para cada $g \in G$, $\varphi_\alpha(g)\colon N \to N$ é também um homomorfismo de grupos. Fixe $g \in G$ e denote $\varphi_\alpha(g) \in S_N$ por f_g. Por definição, para todos $n_1, n_2 \in N$, temos que $f_g(n_1)f_g(n_2) = (gn_1g^{-1})(gn_2g^{-1}) = g(n_1n_2)g^{-1} = f_g(n_1n_2)$. Isso mostra que $\varphi_\alpha\colon G \to \mathrm{Aut}(N)$ é um homomorfismo de grupos. Para terminar a demonstração, observe que

$$\ker(\varphi_\alpha) = \{g \in G \mid \varphi_\alpha(g) = \mathrm{id}_N\} = \{g \in G \mid gng^{-1} = n \text{ para todo } n \in N\} = C_G(N). \qquad \square$$

Corolário 14.4. *Sejam G um grupo e $H \subseteq G$ um subgrupo. Para todo $g \in G$ existe um isomorfismo de grupos $H \cong gHg^{-1}$. Em particular, elementos conjugados e subgrupos conjugados tem a mesma ordem.*

Demonstração. Para cada $g \in G$, considere a função $f_g\colon G \to G$ dada por $f_g(h) = ghg^{-1}$, a conjugação por g. Pela Proposição 14.3, $f_g \in \mathrm{Aut}(G)$. Em particular, f_g induz um isomorfismo de grupos entre H e $f_g(H) = gHg^{-1}$. Como conjugações $(f_g, g \in G)$ são isomorfismos de grupos e como grupos isomorfos (e elementos correspondentes) tem a mesma ordem, então subgrupos e elementos conjugados tem a mesma ordem. $\square$

Definição 14.5. Dado um grupo G, um automorfismo $f \in \mathrm{Aut}(G)$ é dito interno quando existe $g \in G$ tal que $f(x) = gxg^{-1}$ para todo $x \in G$. O conjunto de todos os automorfismos internos de G é denotado por $\mathrm{Inn}(G)$

Corolário 14.6. *Sejam G um grupo e $H \subseteq G$ um subgrupo. O grupo $N_G(H)/C_G(H)$ é isomorfo a um subgrupo de $\mathrm{Aut}(H)$. Em particular, $G/Z(G)$ é isomorfo ao subgrupo $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$.*

Demonstração. Considere o grupo $N_G(H)$. Pela Definição 6.2, $H \subseteq N_G(H)$ é um subgrupo normal. Pela Proposição 14.3, $\varphi_\alpha\colon N_G(H) \to H$ é um homomorfismo de grupos com núcleo

$$\begin{aligned} C_{N_G(H)}(H) &= \{g \in N_G(H) \mid ghg^{-1} = h \text{ para todo } h \in H\} \\ &= \{g \in G \mid ghg^{-1} = h \in H \text{ para todo } h \in H\} \\ &= C_G(H). \end{aligned}$$

Pelo Primeiro Teorema de Isomorfismo de grupos, segue que $N_G(H)/C_G(H) = N_G(H)/\ker(\varphi_\alpha)$ é isomorfo a $\mathrm{im}(\varphi_\alpha)$, que é um subgrupo de $\mathrm{Aut}(H)$. Isso mostra a primeira parte. Para mostrar a segunda parte, observe que, se $H = G$, então $N_G(G) = G$, $C_G(G) = Z(G)$ e $\mathrm{im}(\varphi_\alpha) = \mathrm{Inn}(G)$. Isso termina a demonstração. (Observe que, em geral, $\mathrm{Inn}(H) \subsetneq \mathrm{im}(\varphi_\alpha)$, pois $\mathrm{im}(\varphi_\alpha)$ inclui conjugações por elementos de $N_G(H)$, não só por elementos de H.) $\square$

4.5. Teorema de Sylow

Definição 14.7. Dado um primo $p \geq 2$, um grupo G é dito um p-grupo quando $|G| = p^k$ para algum $k > 0$. Dados um grupo G e um primo $p \geq 2$, um p-subgrupo de G é um subgrupo $H \subseteq G$ tal que $|H| = p^k$ para algum $k > 0$. Dados um grupo G e um primo $p \geq 2$, um p-subgrupo de Sylow de G é um subgrupo $H \subseteq G$ tal que $|H| = p^k$ e $|G| = p^k m$ para algum $m > 0$ tal que $p \nmid m$. Dados um grupo G e um primo $p \geq 2$, denote por $\mathrm{Syl}_p(G)$ o conjunto de p-subgrupos de Sylow de G.

O principal objetivo desta seção é provar o Teorema de Sylow. Vamos começar com um lema técnico.

Lema 14.8. *Seja G um grupo finito. Se $P \in \mathrm{Syl}_p(G)$ e Q é um p-subgrupo de G (não necessariamente de Sylow), então $Q \cap N_G(P) = Q \cap P$.*

Demonstração. Denote $|G| = p^k m$, onde $k, m > 0$ e $p \nmid m$. Por hipótese $|P| = p^k$ e $|Q| = p^\ell$, $\ell \in \{1, \ldots, k\}$. Como $P \subseteq N_G(P)$, então $(Q \cap P) \subseteq (Q \cap N_G(P))$. Logo, para mostrar o resultado, basta provar que $(Q \cap N_G(P)) \subseteq (Q \cap P)$. Como $(Q \cap N_G(P)) \subseteq Q$, na verdade, basta provar que $(Q \cap N_G(P)) \subseteq P$.

Como $(Q \cap N_G(P))$ normaliza P, pela Proposição 9.3 e pelo Segundo Teorema de Isomorfismo de grupos (Teorema 9.5), temos que $(Q \cap N_G(P))P$ é um subgrupo de G e

$$|(Q \cap N_G(P))\, P| = \frac{|Q \cap N_G(P)|\,|P|}{|Q \cap N_G(P) \cap P|} = \frac{|Q \cap N_G(P)|\,|P|}{|Q \cap P|}.$$

Pelo Teorema 8.11 (de Lagrange), $(Q \cap N_G(P))$ e $(Q \cap P)$ são p-subgrupos, ou seja, o lado direito da equação acima é uma potência de p. Como $(Q \cap N_G(P))P$ contem P essa potência é $\geq p^k$. Mas, como P é um p-subgrupo de Sylow, $|(Q \cap N_G(P))P| = p^k = |P|$. Logo $(Q \cap N_G(P))P = P$, ou seja, $(Q \cap N_G(P)) \subseteq P$. □

Agora vamos provar o Teorema de Sylow.

Teorema 14.9 (de Sylow)**.** *Seja G um grupo e seja $p \geq 2$ um primo tal que $|G| = p^k m$ para alguns $k, m > 0$ com $p \nmid m$. Então:*

(a) $\mathrm{Syl}_p(G) \neq \emptyset$.
(b) Se $P \in \mathrm{Syl}_p(G)$ e Q é um p-subgrupo de G (não necessariamente de Sylow), então existe $g \in G$ tal que $gQg^{-1} \subseteq P$. Em particular, se $P, Q \in \mathrm{Syl}_p(G)$, então P e Q são conjugados (e portanto isomorfos).
(c) $|\mathrm{Syl}_p(G)| = |G : N_G(P)| \equiv 1 \pmod p$ *para qualquer* $P \in \mathrm{Syl}_p(G)$. *Em particular,* $|\mathrm{Syl}_p(G)|$ *divide* m.

Demonstração. (a) Vamos usar indução em $|G|$. O caso base é $|G| = p$. Nesse caso (e sempre que $|G| = p^k$, $k > 0$), G é um p-subgrupo de Sylow de G. A hipótese de indução é que $\mathrm{Syl}_p(H) \neq \emptyset$ para todo grupo H tal que $p \leq |H| < p^k m = |G|$.

Primeiro, suponha que p divide $|Z(G)|$. Como $Z(G)$ é um grupo abeliano, pela Proposição 10.2, existe $z \in Z(G)$ tal que $|\langle z \rangle| = p$. Por indução $G/\langle z \rangle$ tem um subgrupo $\overline{P}$ de ordem p^{k-1}. Escolha $g_1, \ldots, g_{p^{k-1}} \in G$ tais que $\{\overline{g_i} \mid i \in \{1, \ldots, p^{k-1}\}\} = \overline{P}$. O subconjunto $P = \{g_i z^j \mid i \in \{1, \ldots, p^{k-1}\},\ j \in \{0, \ldots, p-1\}\} \subseteq G$ é um subgrupo (verifique!) de ordem p^k. Portanto P é um p-subgrupo de Sylow de G.

Agora suponha que p não divide $|Z(G)|$. Pelo Teorema 12.12 (Equação de Classe) temos que (usando a mesma notação do teorema):

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G\colon C_G(g_i)| \qquad (g_i \in G \setminus Z(G) \text{ não conjugados}).$$

Como estamos supondo que p não divide $|Z(G)|$, então existe $i \in \{1, \ldots, r\}$ tal que p não divide $|G\colon C_G(g_i)|$, ou seja, $|C_G(g_i)| = p^k m'$, onde $m' < m$. (Se $m' = m$, então $C_G(g_i) = G$ e g_i estaria em $Z(G)$.) Pela hipótese de indução, $C_G(g_i)$ tem um p-subgrupo de Sylow, ou seja, existe um subgrupo $P \subseteq C_G(g_i) \subseteq G$ tal que $|P| = p^k$. Observe que P também é um p-subgrupo de Sylow de G.

(b) Considere $P \in \mathrm{Syl}_p(G)$ e denote $\mathcal{S} = \{gPg^{-1} \mid g \in G\} = \{P_1, \ldots, P_r\}$, onde $r = |G\colon N_G(P)|$ (pela Proposição 12.11). Agora considere um p-subgrupo $Q \subseteq G$. A ação de Q por conjugação em $\mathcal{S}$ induz uma decomposição em órbitas $\mathcal{S} = \mathcal{O}_1 \dot\cup \cdots \dot\cup \mathcal{O}_s$, onde $s \leq r$ e (sem perda de generalidade, podemos supor que) $\mathcal{O}_1 = \{qP_1q^{-1} \mid q \in Q\}, \ldots, \mathcal{O}_s = \{qP_sq^{-1} \mid q \in Q\}$. Observe que, pela Proposição 12.11 e pelo Lema 14.8, $|\mathcal{O}_i| = |Q\colon N_Q(P_i)| = |Q\colon (Q \cap P_i)|$ para cada $i \in \{1, \ldots, s\}$. Além disso,

$$|G\colon N_G(P)| = r = |\mathcal{O}_1| + \cdots + |\mathcal{O}_s| = |Q\colon N_Q(P_1)| + \cdots + |Q\colon N_Q(P_s)|.$$

Como Q é um p-subgrupo arbitrário e r não depende da escolha de Q, podemos escolher $Q = P_1$. Neste caso, $|\mathcal{O}_1| = |P_1\colon N_{P_1}(P_1)| = 1$. Além disso, como P_1 é um p-subgrupo, segue que p divide $|\mathcal{O}_i| = |P_1\colon N_{P_1}(P_i)|$ para todo $i \in \{2, \ldots, r\}$. Logo $r \equiv 1 \ (mod\ p)$.

Como $r \equiv 1 \ (mod\ p)$, para todo p-subgrupo $Q \subseteq G$, existe $i \in \{1, \ldots, r\}$ tal que p não divide $|Q\colon N_Q(P_i)|$. Como Q é um p-subgrupo, ou seja, $|Q| = p^\ell$ para algum $0 < \ell \leq k$, pelo Teorema 8.11 (de Lagrange), temos que $|Q\colon N_Q(P_i)| = 1$. Logo, pelo Lema 14.8, $Q = (Q \cap N_Q(P_i)) \subseteq (Q \cap N_G(P_i)) = (Q \cap P_i)$. Isso implica que $Q \subseteq P_i$.

(c) Pelo item (b), quaisquer dois p-subgrupos de Sylow são conjugados. Então, para qualquer $P \in \mathrm{Syl}_p(G)$, temos que $\mathrm{Syl}_p(G) = \{gPg^{-1} \mid g \in G\} = \{P_1, \ldots, P_r\}$, onde $r = |G\colon N_G(P)|$, e ainda $r \equiv 1 \ (mod\ p)$. Além disso, $P \subseteq N_G(P)$ e portanto $|G\colon N_G(P)|$ divide m. □

Aula 15

4.5. Teorema de Sylow

Lembre o enunciado do Teorema de Sylow.

Teorema 15.1 (de Sylow)**.** *Seja G um grupo e seja $p \geq 2$ um primo tal que $|G| = p^k m$ para alguns $k, m > 0$ com $p \nmid m$. Então:*

(a) $\mathrm{Syl}_p(G) \neq \emptyset$.
(b) Se $P \in \mathrm{Syl}_p(G)$ e Q é um p-subgrupo de G (não necessariamente de Sylow), então existe $g \in G$ tal que $gQg^{-1} \subseteq P$. Em particular, se $P, Q \in \mathrm{Syl}_p(G)$, então P e Q são conjugados (e portanto isomorfos).
(c) $|\mathrm{Syl}_p(G)| = |G\colon N_G(P)| \equiv 1 \pmod p$ para qualquer $P \in \mathrm{Syl}_p(G)$. Em particular, $|\mathrm{Syl}_p(G)|$ divide m.

Uma aplicação desse resultado é a seguinte.

Corolário 15.2. *Sejam G um grupo finito e $p \geq 2$ um primo tal que $|G| = p^k m$ para alguns $k, m > 0$ com $p \nmid m$. As seguintes afirmações são equivalentes:*

(a) P é o único p-subgrupo de Sylow de G,
(b) $P \in \mathrm{Syl}_p(G)$ é normal em G,
(c) Se $X \subseteq G$ é um subconjunto tal que $o(x)$ é uma potência de p para todo $x \in X$, então $\langle X \rangle$ é um p-subgrupo de G.

Demonstração. Vamos mostrar $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$.

$(a) \Rightarrow (b)$**:** Se P for o único p-subgrupo de Sylow de G, então $|\mathrm{Syl}_p(G)| = 1$. Pelo Teorema de Sylow (Teorema 14.9(c)), $|G\colon N_G(P)| = |\mathrm{Syl}_p(G)| = 1$. Logo $N_G(P) = G$, ou seja, P é normal em G.

$(b) \Rightarrow (c)$**:** Suponha que $P \in \mathrm{Syl}_p(G)$ é um subgrupo normal de G e que $X \subseteq G$ é um subconjunto tal que $o(x) = p^\ell$ (algum $\ell \in \{0, \ldots, k\}$) para todo $x \in X$. Fixe $x \in X$. Por hipótese, $\langle x \rangle$ é um p-subgrupo de G para todo $x \in X$. Pelo Teorema 14.9(b), existe $g \in G$ tal que $gxg^{-1} \in P$, ou seja, tal que $x \in g^{-1}Pg$. Como P é normal por hipótese, $x \in P = g^{-1}Pg$. Como P é um subgrupo de G, isso mostra que $\langle X \rangle \subseteq P$. Pelo Teorema 8.11 (de Lagrange), $|\langle X \rangle|$ divide $|P|$, logo $\langle X \rangle$ é um p-subgrupo de G.

$(c) \Rightarrow (a)$**:** Considere $X = \{g \in G \mid o(g) = p^\ell \text{ para algum } \ell \in \{0, \ldots, k\}\}$ e denote $\langle X \rangle$ por Q. Suponha que Q seja um p-subgrupo de G. Vamos mostrar que Q é o único p-subgrupo de Sylow de G. Como, pelo Teorema 14.9(a), $\mathrm{Syl}_p(G) \neq \emptyset$, então podemos tomar $P \in \mathrm{Syl}_p(G)$. Pelo Teorema 8.11, para todo $g \in P$, temos que $o(g) \mid |P| = p^k$, ou seja, $o(g) = p^\ell$ para algum $\ell \in \{0, \ldots, k\}$. Isso implica que $P \subseteq Q$. Por outro lado, pelo Teorema 14.9(b), existe $g \in G$ tal que $gQg^{-1} \subseteq P$. Em particular, $|Q| = |gQg^{-1}| \leq |P| \leq |Q|$. Isso mostra que $P = Q$ e que $\mathrm{Syl}_p(G) = \{Q\}$. □

Exemplo 15.3. Sejam p um primo e G um grupo de ordem p^n, $n > 0$. Observe que G é o único p-subgrupo de Sylow de G. Em particular, $|\mathrm{Syl}_p(G)| = 1 \equiv 1 \pmod p$. Além disso, pelo Teorema 8.11 (de Lagrange), todo subgrupo de G é um p-subgrupo. Logo, todo p-subgrupo de G está contido em G. Observe ainda que G é normal em G e que a ordem de todo elemento de G é uma potência de p. Portanto todo subgrupo de G é um p-subgrupo e é gerado por elementos cujas ordens são potências de p.

Exemplo 15.4. Sejam G um grupo abeliano finito e p um primo tal que p divide $|G|$. Como todo subgrupo de G é normal, pelo Corolário 15.2, existe um único p-subgrupo de Sylow $P \subseteq G$.

Pelo Teorema 14.9(b), esse subgrupo P contem todos os p-subgrupos de G e, consequentemente, todos os elementos de G cujas ordens são potências de p. Pelo Teorema de Lagrange, todos os elementos de P tem ordem potência de p. Portanto:

$$P = \{g \in G \mid o(g) = p^k,\ k \geq 0\}.$$

Exemplo 15.5. Considere $G = S_3$. Observe que $|S_3| = 2 \cdot 3$. Vamos considerar primeiro $p = 2$. Lembre que S_3 tem 3 subgrupos de ordem 2 (que são os 2-subgrupos de Sylow): $\langle(1\ 2)\rangle$, $\langle(1\ 3)\rangle$ e $\langle(2\ 3)\rangle$. Observe que $N_{S_3}(1\ 2) = \langle(1\ 2)\rangle$, $N_{S_3}(1\ 3) = \langle(1\ 3)\rangle$ e $N_{S_3}(2\ 3) = \langle(2\ 3)\rangle$. Observe ainda que $|S_3 \colon N_{S_3}(1\ 2)| = |S_3 \colon N_{S_3}(1\ 3)| = |S_3 \colon N_{S_3}(2\ 3)| = 3 \equiv 1\ (mod\ 2)$.

Agora considere $p = 3$. Lembre que S_3 tem apenas 1 subgrupo de ordem 3: $\langle(1\ 2\ 3)\rangle$. Lembre também que esse subgrupo é normal e contem todos os elementos de orderm 3 em S_3.

Exemplo 15.6. Seja G um grupo de oredm pq, onde $p < q$ são primos. Considere $P \in \mathrm{Syl}_p(G)$, $Q \in \mathrm{Syl}_q(G)$. Observe que $|P| = p$ e $|Q| = q$, logo P, Q são cíclicos (abelianos) e existem $x \in P$ e $y \in Q$ tais que $P = \langle x\rangle$, $Q = \langle y\rangle$.

Primeiro vamos mostrar que Q é normal em G. Pelo Corolário 15.2, isso é equivalente a mostrar que $|\mathrm{Syl}_q(G)| = 1$. Pelo Teorema 14.9(c), $|\mathrm{Syl}_q(G)|$ divide p (logo $|\mathrm{Syl}_q(G)| \in \{1, p\}$) e $|\mathrm{Syl}_q(G)| \in \{1 + nq \mid n \in \mathbb{Z}\}$. Como $p < q$, segue que $|\mathrm{Syl}_q(G)| = 1$.

Usando um argumento análogo ao usado no parágrafo anterior, podemos ver que:

- ou $|\mathrm{Syl}_p(G)| = 1$ e P é normal em G,
- ou $q \equiv 1\ (mod\ p)$ e $|\mathrm{Syl}_p(G)| = q$. (Nesse caso, pelo Corolário 15.2, $P \subseteq G$ não é normal.)

No caso em que P é normal, $N_G(P) = G$. Considere $C_G(P)$. Como P é abeliano, então $P \subseteq C_G(P)$. Em particular, $|C_G(P)| \geq p$. Como $|G| = pq$ e $C_G(P) \subseteq G$ é um subgrupo, então pelo Teorema 8.11 (de Lagrange), $C_G(P) = P$ ou $C_G(P) = G$. Pelo Corolário 14.6, $N_G(P)/C_G(P)$ é um subgrupo de $\mathrm{Aut}(P)$. Como $|\mathrm{Aut}(P)| = p - 1 < q = |G/P|$ (verifique!), então $C_G(P) = G$, ou seja, $P \subseteq Z(G)$. Como $x \in P \subseteq Z(G)$, então $o(xy) = pq$. De fato, $(xy)^n = x^n y^n = e_G$ se, e somente se, $x^n = y^{-n}$. Como p e q são coprimos, pelo Teorema 8.11 (de Lagrange), $P \cap Q = \{e_G\}$. Portanto $x^n = e_G = y^n$, ou seja, $p \mid n$ e $q \mid n$. Isso mostra que $o(xy) = pq$ e que G é cíclico (gerado por xy), ou seja, $G \cong \mathbb{Z}_{pq}$.

5.1. Produto direto de grupos

Definição 15.7. Para cada $i \in \mathbb{N}$, seja (G_i, m_i) um grupo. Para cada $n > 0$, defina o produto direto $G_1 \times \cdots \times G_n$ como sendo o conjunto $G_1 \times \cdots \times G_n$ munido da operação binária

$$\begin{array}{rccl} m\colon & (G_1 \times \cdots \times G_n) \times (G_1 \times \cdots \times G_n) & \longrightarrow & (G_1 \times \cdots \times G_n)\,, \\ & ((g_1, \ldots, g_n), (h_1, \ldots, h_n)) & \longmapsto & (m_1(g_1, h_1), \ldots, m_n(g_n, h_n))\,. \end{array}$$

Analogamente, defina o produto direto $\prod_{i\in\mathbb{N}} G_i$ como sendo o conjunto $\prod_{i\in\mathbb{N}} G_i$ munido da operação binária

$$\begin{array}{rccl} m\colon & \left(\prod_{i\in\mathbb{N}} G_i\right) \times \left(\prod_{i\in\mathbb{N}} G_i\right) & \longrightarrow & \left(\prod_{i\in\mathbb{N}} G_i\right), \\ & ((g_i)_{i\in\mathbb{N}},\ (h_i)_{i\in\mathbb{N}}) & \longmapsto & (m_i(g_i, h_i))_{i\in\mathbb{N}}\,. \end{array}$$

Exemplo 15.8. Considere $G_1 = \mathbb{Z}$ (grupo aditivo), $G_2 = GL_2(\mathbb{R})$ (munido da multiplicação de matrizes) e $G_3 = S_3$ (munido da composição de permutações). Então o grupo $G_1 \times G_2 \times G_3$ consiste do conjunto $\mathbb{Z} \times GL_2(\mathbb{R}) \times S_3$ munido da operação binária

$$m\left((a, A, \sigma), (b, B, \rho)\right) = (a + b,\ AB,\ \sigma \circ \rho).$$

Exemplo 15.9. Considere $G_i = \mathbb{R}$ (grupo aditivo) para todo $i \in \mathbb{N}$. Então o produto $\prod_{i\in\mathbb{N}} G_i$ é o conjunto de sequências reais $\mathbb{R}^{\mathbb{N}} = \{(a_i)_{i\in\mathbb{N}} \mid a_i \in \mathbb{R} \text{ para todo } i \in \mathbb{N}\}$ munido da operação binária

$$m\left((a_i)_{i\in\mathbb{N}}, (b_i)_{i\in\mathbb{N}}\right) = (a_i + b_i)_{i\in\mathbb{N}}\,.$$

Exercício 15.10. Para cada $i \in \mathbb{N}$, seja (G_i, m_i) um grupo. Verifique que $G_1 \times \cdots \times G_n$ e $\prod_{i\in\mathbb{N}} G_i$ como definidos acima são de fato grupos. Verifique também que, se G_i é finito para todo $i \in \mathbb{N}$, então $|G_1 \times \cdots \times G_n| = |G_1| \cdots |G_n|$ para todo $n > 0$. Se G_i é infinito para algum $i \in \mathbb{N}$, então $G_1 \times \cdots \times G_n$ é infinito para todo $n \geq i$.

Apesar das operações binárias dos diferentes grupos G_i poderem ser distintas, em geral, nós vamos supor que as operações estão claras do contexto, omití-las e, para cada i, denotar $m_i(g_i, h_i)$ simplesmente por $g_i h_i$.

Aula 16

Proposição 16.1. *Para cada $i \in \mathbb{N}$, seja G_i um grupo. Denote o grupo $\prod_{i\in\mathbb{N}} G_i$ por G.*

(a) Para todo $k \in \mathbb{N}$, a função $\iota_k \colon G_k \to G$ dada por $\iota_k(g) = (e_{G_1}, \dots, e_{G_{k-1}}, g, e_{G_{k+1}}, \dots)$ é um homomorfismo injetor de grupos. Consequentemente, para todo $k \in \mathbb{N}$, $\iota_k(G_k) \subseteq G$ é um subgrupo isomorfo a G_k.
(b) Para todos $k, \ell \in \mathbb{N}$, $k \neq \ell$, $g_k \in G_k$ e $g_\ell \in G_\ell$, temos que $\iota_k(g_k)\iota_\ell(g_\ell) = \iota_\ell(g_\ell)\iota_k(g_k) \in G$.
(c) Para todo $n \in \mathbb{N}$, $(G_1 \times \cdots \times G_n) = \iota_1(G_1)\cdots\iota_n(G_n)$. Consequentemente, para todo $k \leq n \in \mathbb{N}$, $\iota_k(G_k)$ é um subgrupo normal de $(G_1 \times \cdots \times G_n)$.
(d) Para todo $k \in \mathbb{N}$, a função $\pi_k \colon G \to G_k$ dada por $\pi_k(g_i)_{i\in\mathbb{N}} = g_k$ é um homomorfismo sobrejetor de grupos.

Demonstração. (a) Fixe $k \in \mathbb{N}$. Primeiro vamos verificar que ι_k é um homomorfismo de grupos. Para quaisquer $g, h \in G_k$, temos que

$$\begin{aligned}\iota_k(gh) &= (e_{G_1}, \dots, e_{G_{k-1}}, gh, e_{G_{k+1}}, \dots)\\ &= (e_{G_1}, \dots, e_{G_{k-1}}, g, e_{G_{k+1}}, \dots)(e_{G_1}, \dots, e_{G_{k-1}}, h, e_{G_{k+1}}, \dots)\\ &= \iota_k(g)\iota_k(h).\end{aligned}$$

Agora vamos verificar que ι_k é injetor, calculando seu núcleo:

$$\ker(\iota_k) = \{g \in G_k \mid (e_{G_1}, \dots, e_{G_{k-1}}, g, e_{G_{k+1}}, \dots) = (e_{G_1}, \dots, e_{G_k}, \dots)\} = \{e_{G_k}\}.$$

Isso mostra que ι_k é um homomorfismo injetor de grupos. Pelo Primeiro Teorema de Isomorfismo de grupos, segue que $\iota_k(G_k) \subseteq G$ é um subgrupo isomorfo a G_k.

(b) Sem perda de generalidade, fixe $k < \ell \in \mathbb{N}$. Para quaisquer $g_k \in G_k$ e $g_\ell \in G_\ell$, temos que

$$\begin{aligned}\iota_k(g_k)\iota_\ell(g_\ell) &= (e_{G_1}, \dots, e_{G_{k-1}}, g_k, e_{G_{k+1}}, \dots, e_{G_\ell}, \dots)(e_{G_1}, \dots, e_{G_k}, \dots, e_{G_{\ell-1}}, g_\ell, e_{G_{\ell+1}}, \dots)\\ &= (e_{G_1}, \dots, e_{G_{k-1}}, g_k, e_{G_{k+1}}, \dots, e_{G_\ell - 1}, g_\ell, e_{G_{\ell+1}}, \dots)\\ &= (e_{G_1}, \dots, e_{G_k}, \dots, e_{G_{\ell-1}}, g_\ell, e_{G_{\ell+1}}, \dots)(e_{G_1}, \dots, e_{G_{k-1}}, g_k, e_{G_{k+1}}, \dots, e_{G_\ell}, \dots)\\ &= \iota_\ell(g_\ell)\iota_k(g_k).\end{aligned}$$

(c) Pela parte (a) (tomando $G_i = \{e\}$ para todo $i > n$), segue que $\iota_k(G_k)$ é um subgrupo de $(G_1 \times \cdots \times G_n)$ para todo $k \leq n$. Além disso, para quaisquer $g_1 \in G_1, \dots, g_n \in G_n$, temos que $(g_1, \dots, g_n) = \iota_1(g_1)\cdots\iota_n(g_n)$. Isso mostra a primeira afirmação. Usando essa afirmação junto com a parte (b), segue que $\iota_k(G_k)$ é normal em $(G_1 \times \cdots \times G_n)$.

(d) Fixe $k \in \mathbb{N}$. Primeiro vamos verificar que π_k é um homomorfismo de grupos. Para quaisquer $(g_1, g_2, \dots), (h_1, h_2, \dots) \in G$, temos que

$$\pi_k\left((g_1, g_2, \dots)(h_1, h_2, \dots)\right) = \pi_k(g_1h_1, g_2h_2, \dots) = g_kh_k = \pi_k(g_1, g_2, \dots)\pi_k(h_1, h_2, \dots).$$

Agora observe que, para todo $g \in G_k$, $\pi_k(e_{G_1}, \dots, e_{G_{k-1}}, g, e_{G_{k+1}}, \dots) = g$. Isso mostra que π_k é um homomorfismo sobrejetor de grupos. □

5.2. Teorema fundamental dos grupos abelianos finitamente gerados

Definição 16.2. Um grupo G é dito finitamente gerado quando existe um subconjunto finito $X \subseteq G$ tal que $\langle X \rangle = G$. Para cada $r \in \mathbb{N}$, o grupo $\mathbb{Z}^r := \prod_{i=1}^r \mathbb{Z}$ é chamado de grupo abeliano livre de posto r.

O próximo resultado é conhecido como Teorema fundamental dos grupos abelianos finitamente gerados. (Nós não vamos demonstrar esse teorema.)

Teorema 16.3. *Seja G um grupo abeliano finitamente gerado. Então existem inteiros $r, s \geq 0$, $n_1, \ldots, n_s > 1$, tais que $n_{i+1} \mid n_i$ para todo $i \in \{1, \ldots, s-1\}$ e*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}.$$

5.5. Produto semidireto de grupos

Considere um grupo G e dois subgrupos $H, N \subseteq G$ tais que $N \subseteq G$ é normal e $H \cap N = \{e\}$. Lembre que $NH \subseteq G$ é um subgrupo. De fato, dados $n_1, n_2 \in N$ e $h_1, h_2 \in H$, temos que

$$(n_1h_1)(n_2h_2) = n_1(h_1n_2h_1^{-1})h_1h_2 = (n_1n')(h_1h_2)$$

para algum $n' \in N$, já que N é normal em G. Observe que, como $H \cap N = \{e\}$, a função $f\colon (N \times H) \to NH$ dada por $f(n,h) = nh$ é uma bijeção (entre os conjuntos). De fato, $(n_1h_1) = f(n_1,h_1) = f(n_2,h_2) = (n_2h_2)$ se, e somente se, $n_2^{-1}n_1 = h_2h_1^{-1} \in (N \cap H) = \{e_G\}$, ou seja, $n_1 = n_2$ e $h_1 = h_2$. Mas f nem sempre é um isomorfismo de grupos, pois:

$$f\left((n_1,h_1)(n_2,h_2)\right) = f(n_1n_2, h_1h_2) = (n_1n_2)(h_1h_2)$$
$$\text{e} \quad f(n_1,h_1)f(n_2,h_2) = (n_1(h_1n_2h_1^{-1}))(h_1h_2).$$

Observe que a diferença entre $f\left((n_1,h_1)(n_2,h_2)\right)$ e $f(n_1,h_1)f(n_2,h_2)$ aparece quando $(h_1n_2h_1^{-1})$ é diferente de n_2. Ou seja, quando a conjugação por h_1 (que é um automorfismo de N, já que N é normal) é não trivial.

O produto semidireto é uma generalização do produto direto que incorpora esse automorfismo em um de seus termos.

Definição 16.4. Sejam H, N dois grupos e $\varphi\colon H \to \mathrm{Aut}(N)$ um homorfismo de grupos. Defina o produto semidireto $N \rtimes_\varphi H$ como sendo o conjunto $N \times H$ munido da seguinte operação binária

$$\begin{array}{rcl} m\colon (N \times H) \times (N \times H) & \longrightarrow & (N \times H) \\ ((n_1,h_1),(n_2,h_2)) & \longmapsto & (n_1\,\varphi(h_1)(n_2),\ h_1h_2)\,. \end{array}$$

Exercício 16.5. Sejam H, N dois grupos e $\varphi\colon H \to \mathrm{Aut}(N)$ um homomorfismo de grupos. Mostre que $(N \rtimes_\varphi H, m)$ é um grupo, com $e_{N \rtimes_\varphi H} = (e_N, e_H)$ e $(n,h)^{-1} = (\varphi(h^{-1})(n^{-1}), h^{-1})$. Mostre também que $|N \rtimes_\varphi H| = |N||H|$ e que, quando φ é trivial (ou seja, $\varphi(h) = \mathrm{id}_N$ para todo $h \in H$), existe um isomorfismo de grupos $(N \rtimes_\varphi H) \cong (N \times H)$.

Exemplo 16.6. Considere os grupos aditivos $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ e $\mathbb{Z}_3 = \{\overline{\overline{0}}, \overline{\overline{1}}, \overline{\overline{2}}\}$. Primeiro vamos tentar criar um produto semidireto $\mathbb{Z}_2 \rtimes_\varphi \mathbb{Z}_3$ (onde $\mathbb{Z}_2$ é normal). Para isso, precisamos escolher um homomorfismo de grupos $\varphi\colon \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_2)$. Como $\mathrm{Aut}(\mathbb{Z}_2) = \{\mathrm{id}_{\mathbb{Z}_2}\}$ (verifique!), então a única opção é $\varphi(\overline{\overline{a}}) = \mathrm{id}_{\mathbb{Z}_2}$ para todo $\overline{\overline{a}} \in \mathbb{Z}_3$. Nesse caso, temos

$$m\left((\overline{a_1}, \overline{\overline{b_1}}), (\overline{a_2}, \overline{\overline{b_2}})\right) = \left(\overline{a_1}\,\varphi(\overline{\overline{b_1}})(\overline{a_2}),\ \overline{\overline{b_1}}\,\overline{\overline{b_2}}\right) = \left(\overline{a_1}\,\overline{a_2},\ \overline{\overline{b_1}}\,\overline{\overline{b_2}}\right).$$

Ou seja, $\mathbb{Z}_2 \rtimes_\varphi \mathbb{Z}_3 = \mathbb{Z}_2 \times \mathbb{Z}_3$. Além disso, como $|\mathbb{Z}_2 \times \mathbb{Z}_3| = 6 = o\left(\overline{1}, \overline{\overline{1}}\right)$, então $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. Em particular, $\mathbb{Z}_2 \rtimes_\varphi \mathbb{Z}_3$ é um grupo abeliano.

Agora vamos tentar criar um produto semidireto $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_2$ (onde $\mathbb{Z}_3$ é normal) e tal que φ é não-trivial. Observe que $\mathrm{Aut}(\mathbb{Z}_3) = \{\mathrm{id}_{\mathbb{Z}_3}, \sigma\}$, onde $\sigma(\overline{\overline{0}}) = \overline{\overline{0}}$, $\sigma(\overline{\overline{1}}) = \overline{\overline{2}} = -\overline{\overline{1}}$ e $\sigma(\overline{\overline{2}}) = \overline{\overline{1}} = -\overline{\overline{2}}$.

Portanto $\mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$, e existe um único homomorfismo de grupos $\varphi\colon \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$ não-trivial, explicitamente, $\varphi(\overline{0}) = \mathrm{id}_{\mathbb{Z}_3}$ e $\varphi(\overline{1}) = \sigma$. Usando esse φ, obtemos

$$m\left((\overline{\overline{a_1}}, \overline{0}), (\overline{\overline{a_2}}, \overline{b})\right) = \left(\overline{\overline{a_1}} + \varphi(\overline{0})(\overline{\overline{a_2}}),\, \overline{0} + \overline{b}\right) = \left(\overline{\overline{a_1 + a_2}},\, \overline{b}\right)$$

e

$$m\left((\overline{\overline{a_1}}, \overline{1}), (\overline{\overline{a_2}}, \overline{b})\right) = \left(\overline{\overline{a_1}} + \varphi(\overline{1})(\overline{\overline{a_2}}),\, \overline{1} + \overline{b}\right) = \left(\overline{\overline{a_1 - a_2}},\, \overline{b+1}\right),$$

para todos $\overline{\overline{a_1}}, \overline{\overline{a_2}} \in \mathbb{Z}_3$ e $\overline{b} \in \mathbb{Z}_2$. Observe que, nesse caso, $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_2$ não é um grupo abeliano. De fato, $m((\overline{\overline{1}}, \overline{0}), (\overline{\overline{0}}, \overline{1})) = (\overline{\overline{1}}, \overline{1}) \neq (\overline{\overline{2}}, \overline{1}) = m((\overline{\overline{0}}, \overline{1}), (\overline{\overline{1}}, \overline{0}))$.

Exercício 16.7. Mostre que existe um único homomorfismo de grupos $f\colon \mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_2 \to S_3$ satisfazendo $f(\overline{\overline{0}}, \overline{1}) = (1\ 2)$ e $f(\overline{\overline{1}}, \overline{0}) = (1\ 2\ 3)$. Mostre ainda que f é um isomorfismo.

Proposição 16.8. *Sejam H, N dois grupos e $\varphi\colon H \to \mathrm{Aut}(N)$ um homomorfismo de grupos.*

(a) A função $\iota_H\colon H \to (N \rtimes_\varphi H)$ dada por $\iota_H(h) = (e_N, h)$ e a função $\iota_N\colon N \to (N \rtimes_\varphi H)$ dada por $\iota_N(n) = (n, e_H)$ são homomorfismos injetores de grupos. Consequentemente H e N são isomorfos a subgrupos de $N \rtimes_\varphi H$.
(b) $\iota_N(N)$ é um subgrupo normal de $N \rtimes_\varphi H$.
(c) $\iota_N(N) \cap \iota_H(H) = \{(e_N, e_H)\}$.
(d) $\iota_H(H)$ é um subgrupo normal de $N \rtimes_\varphi H$ se, e somente se, φ é trivial.

Demonstração. (a) Vamos mostrar que $\iota_H\colon H \to (N \rtimes_\varphi H)$ dada por $\iota_H(h) = (e_N, h)$ é um homorfismo injetor de grupos. O caso ι_N é análogo, pois $\varphi(e_H) = \mathrm{id}_N$. Primeiro vamos mostrar que ι_H é um homomorfismo de grupos. Dados $h_1, h_2 \in H$, temos que

$$\iota_H(h_1h_2) = (e_N, h_1h_2) = (e_N, h_1)(e_N, h_2) = \iota_H(h_1)\iota_H(h_2).$$

Agora vamos mostrar que ι_H é injetora, calculando seu núcleo:

$$\ker(\iota_H) = \{h \in H \mid \iota_H(h) = (e_N, e_H)\} = \{h \in H \mid (e_N, h) = (e_N, e_H)\} = \{e_H\}.$$

Isso mostra que ι_H é um homorfismo injetor de grupos. Pelo Primeiro Teorema de Isomorfismos de grupos, segue que H é isomorfo a $\mathrm{im}(\iota_H) = \iota_H(H)$, que é um subgrupo de $N \rtimes_\varphi H$.

(b) Pelo item (a), $\iota_N(N)$ é um subgrupo de $N \rtimes_\varphi H$. Vamos mostrar que $\iota_N(N)$ é normal. Dados $(n_1, h_1) \in N \rtimes_\varphi H$ e $n \in N$, temos que

$$\begin{aligned}(n_1, h_1)(n, e_H)(n_1, h_1)^{-1} &= (n_1\, \varphi(h_1)(n),\ h_1)(\varphi(h_1^{-1})(n_1^{-1}), h_1^{-1}) \\ &= (n_1\, \varphi(h_1)(n)\, \varphi(h_1)(\varphi(h_1^{-1})(n_1^{-1})),\ e_H) \in \iota_N(N).\end{aligned}$$

(c) $\iota_N(N) \cap \iota_H(H) = \{(n, e_H) \mid n \in N\} \cap \{(e_N, h) \mid h \in H\} = \{(e_N, e_H)\}$.

(d) Se φ for trivial, pelo Exercício 16.5, existe um isomorfismo de grupos $N \rtimes_\varphi H \cong N \times H$. Da Proposição 16.1(c), segue que $\iota_H(H) \subseteq N \times H$ é um subgrupo normal.

Por outro lado, se $\iota_H(H)$ é um subgrupo normal de $N \rtimes_\varphi H$, então, para todos $n \in N$ e $h \in H$, temos que

$$\begin{aligned}(n, e_H)(e_N, h)(n, e_H)^{-1} &= (n\, \varphi(e_H)(e_N),\ h)(\varphi(e_H^{-1})(n^{-1}), e_H) \\ &= (ne_N\, \varphi(h)(n^{-1}),\ h) \\ &= (n\, \varphi(h)(n^{-1}),\ h) \in \iota_H(H).\end{aligned}$$

Ou seja, $\varphi(h)(n^{-1}) = n^{-1}$ para todos $n \in N, h \in H$. Isso mostra que φ é trivial. □

Teorema 16.9. *Seja G um grupo e $H, N \subseteq G$ subgrupos. Se $G = NH$, $N \subseteq G$ é normal e $N \cap H = \{e_G\}$, então $G \cong N \rtimes_\varphi H$ para $\varphi\colon H \to \mathrm{Aut}(N)$ dado por $\varphi(h)(n) = hnh^{-1}$ para todos $h \in H$, $n \in N$.*

Demonstração. Considere a função $f\colon (N \rtimes_\varphi H) \to G$ dada por $f(n,h) = nh$. Como $G = NH$ por hipótese, então f é sobrejetora. Como $N \cap H = \{e_G\}$, então f é injetora. De fato, suponha que sejam tais que $f(n_1,h_1) = f(n_2,h_2)$, ou seja, tais que $n_1h_1 = n_2h_2$. Isso ocorre se, e somente se, $n_2^{-1}n_1 = h_2h_1^{-1} \in (N \cap H) = \{e_G\}$, ou seja, e, e somente se, $n_1 = n_2$ e $h_1 = h_2$. Com isso, concluímos que f é uma bijeção.

Agora vamos mostrar que f é um homomorfismo de grupos. Para todos $n_1, n_2 \in N$ e $h_1, h_2 \in H$, temos que

$$\begin{aligned} f\left((n_1,h_1)(n_2,h_2)\right) &= f\left(n_1\,\varphi(h_1)(n_2),\ h_1h_2\right) \\ &= (n_1(h_1n_2h_1^{-1}))(h_1h_2) \\ &= (n_1h_1)(n_2h_2) \\ &= f(n_1,h_1)f(n_2,h_2). \end{aligned}$$

Isso mostra que f é um isomorfismo de grupos, e termina a demonstração. □

Aula 17

7.1. Introdução a anéis: definições e exemplos básicos

Definição 17.1. Um anel R é um conjunto munido de duas operações binárias

$$s\colon R\times R\to R \quad \text{e} \quad m\colon R\times R\to R,$$

satisfazendo as seguintes condições:

(i) (R,s) é um grupo abeliano.
(ii) $m(a,m(b,c))=m(m(a,b),c)$ para todos $a,b,c\in R$.
(iii) $m(s(a,b),c)=s(m(a,c),m(b,c))$ para todos $a,b,c\in R$.
(iv) $m(a,s(b,c))=s(m(a,b),m(a,c))$ para todos $a,b,c\in R$.

O elemento neutro do grupo (R,s) será denotado por 0_R. Um anel (R,s,m) é dito comutativo quando

$$m(a,b)=m(b,a) \qquad \text{para todos } a,b\in R.$$

Um anel (R,s,m) é dito com identidade quando existir $1_R\in R$ tal que

$$m(1_R,a)=a=m(a,1_R) \qquad \text{para todo } a\in R.$$

Um anel (R,s,m) é dito de divisão quando (R,s,m) é um anel com identidade e $(R\setminus\{0_R\},m)$ é um grupo (ou seja, todo elemento de R diferente de 0_R tem inverso com relação a m). Um anel (R,s,m) é dito um corpo quando (R,s,m) é um anel de divisão comutativo (em particular, (R,s) e $(R\setminus\{0_R\},m)$ são grupos abelianos).

Exemplo 17.2. Considere um conjunto com um único elemento, $\{\clubsuit\}$, e considere as (únicas) operações binárias

$$s\colon \{\clubsuit\}\times\{\clubsuit\}\to\{\clubsuit\} \quad \text{dada por} \quad s(\clubsuit,\clubsuit)=\clubsuit,$$
$$m\colon \{\clubsuit\}\times\{\clubsuit\}\to\{\clubsuit\} \quad \text{dada por} \quad m(\clubsuit,\clubsuit)=\clubsuit.$$

Vamos verificar que $(\{\clubsuit\},s,m)$ é um anel.

(i) $(\{\clubsuit\},s)$ é o grupo trivial.
(ii) $m(\clubsuit,m(\clubsuit,\clubsuit))=m(\clubsuit,\clubsuit)=\clubsuit$ e $m(m(\clubsuit,\clubsuit),\clubsuit))=m(\clubsuit,\clubsuit)=\clubsuit$.
(iii) $m(s(\clubsuit,\clubsuit),\clubsuit)=m(\clubsuit,\clubsuit)=\clubsuit$ e $s(m(\clubsuit,\clubsuit),m(\clubsuit,\clubsuit))=s(\clubsuit,\clubsuit)=\clubsuit$.
(iv) $m(\clubsuit,s(\clubsuit,\clubsuit))=m(\clubsuit,\clubsuit)=\clubsuit$ e $s(m(\clubsuit,\clubsuit),m(\clubsuit,\clubsuit))=m(\clubsuit,\clubsuit)=\clubsuit$.

Observe que $0_{\{\clubsuit\}}=\clubsuit$. Além disso, $\{\clubsuit\}$ é um anel comutativo com identidade $1_{\{\clubsuit\}}=\clubsuit$. De fato, $m(\clubsuit,\clubsuit)=\clubsuit=m(\clubsuit,\clubsuit)$. Mas $\{\clubsuit\}$ não é um anel de divisão (e, consequentemente, não é um corpo), pois $\{\clubsuit\}\setminus\{0_{\{\clubsuit\}}\}=\emptyset$ não é um grupo.

Esse anel é chamado de anel trivial e $\clubsuit$, em geral, é denotado por 0.

Exemplo 17.3. Considere o conjunto $\mathbb{Z}$ (dos números inteiros) munido das operações binárias

$$s\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z} \quad \text{dada por} \quad s(a,b)=a+b,$$
$$m\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z} \quad \text{dada por} \quad m(a,b)=ab.$$

Vamos verificar que $(\mathbb{Z},s,m)$ é um anel.

(i) Nós já vimos que $(\mathbb{Z},s)$ é um grupo.
(ii) $m(a,m(b,c))=m(a,bc)=a(bc)=(ab)c=m(ab,c)=m(m(a,b),c))$ para todos $a,b,c\in\mathbb{Z}$.
(iii) $m(s(a,b),c)=m(a+b,c)=(a+b)c=ac+bc=s(ac,bc)=s(m(a,c),m(b,c))$ para todos $a,b,c\in\mathbb{Z}$.
(iv) $m(a,s(b,c))=m(a,b+c)=a(b+c)=ab+ac=s(ab,ac)=s(m(a,b),m(a,c))$.

Observe que $0_{\mathbb{Z}} = 0$. Além disso, $\mathbb{Z}$ é um anel comutativo com identidade $1_{\mathbb{Z}} = 1$. De fato, $m(a,b) = ab = ba = m(b,a)$ e $m(1,a) = a = m(a,1)$ para todos $a, b \in \mathbb{Z}$. Mas $\mathbb{Z}$ não é um anel de divisão (e, consequentemente, não é um corpo). De fato, $m(2,a) = 1$ se, e somente se, $a = \frac{1}{2}$. Como $\frac{1}{2} \notin \mathbb{Z}$, $2 \in \mathbb{Z} \setminus \{0\}$ não tem inverso com relação a m.

Exercício 17.4. Mostre que os conjuntos $\mathbb{Q}$ (dos números racionais), $\mathbb{R}$ (dos números reais) e $\mathbb{C}$ (dos números complexos) são corpos quando munidos da soma (s) e multiplicação (m) usuais.

Exercício 17.5. Sejam A um anel e X um conjunto não-vazio. Considere o conjunto $\mathcal{F}(X,A) = \{f\colon X \to A \mid f \text{ é uma função}\}$ e as operações binárias $s\colon \mathcal{F}(X,A) \times \mathcal{F}(X,A) \to \mathcal{F}(X,A)$ e $m\colon \mathcal{F}(X,A) \times \mathcal{F}(X,A) \to \mathcal{F}(X,A)$ dadas por

$$s(f,g)(x) = f(x) + g(x) \qquad \text{e} \qquad m(f,g)(x) = f(x)g(x) \qquad \text{para todo } x \in X.$$

(a) Mostre que $\mathcal{F}(X,A)$ é um anel.
(b) Se A tiver identidade, mostre que $\mathcal{F}(X,A)$ tem identidade (a função "constante" $1_{\mathcal{F}(X,A)}(x) = 1_A$ para todo $x \in X$).
(c) Se A for comutativo, mostre que $\mathcal{F}(X,A)$ é comutativo.
(d) Se A for um anel de divisão, mostre que $\mathcal{F}(X,A)$ é um anel de divisão.
(e) Se A for um corpo, mostre que $\mathcal{F}(X,A)$ é um corpo.

Observação 17.6. Em geral, vamos denotar a operação s por $+$, chamá-la de adição, denotar a operação m por $\cdot$, e chamá-la multiplicação. Além disso, o elemento inverso de $r \in R$ com relação à adição será denotado por $-r$ e chamado de inverso aditivo. Quando existir, o elemento inverso de $r \in R$ com relação à multiplicação será denotado por r^{-1} e chamado de inverso multiplicativo.

Proposição 17.7. *Seja R um anel.*

(a) $0_R \cdot r = 0_R = r \cdot 0_R$ *para todo* $r \in R$.
(b) $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$ *para todos* $a, b \in R$.
(c) $(-a) \cdot (-b) = ab$ *para todos* $a, b \in R$.
(d) Se R for um anel com identidade, então 1_R *é único.*
(e) Se R for um anel com identidade, então $(-1_R) \cdot r = -r$ *para todo* $r \in R$.

Demonstração. (a) Para todo $r \in R$, temos que

$$0_R = (0_R \cdot r) - (0_R \cdot r) = ((0_R + 0_R) \cdot r) - (0_R \cdot r) = ((0_R + 0_R) - 0_R) \cdot r = 0_R \cdot r.$$

(b) Considere $a, b \in R$. Observe que $((-a) \cdot b) + (a \cdot b) = (-a + a) \cdot b = 0_R \cdot b = 0_R$ pelo item (a). Logo $(-a) \cdot b = -(a \cdot b)$. Analogamente, $(a \cdot (-b)) + (a \cdot b) = a \cdot (-b + b) = a \cdot 0_R = 0_R$ pelo item (a). Logo $a \cdot (-b) = -(a \cdot b)$.
(c) Considere $a, b \in R$. Pelo item (b), temos que $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = (a \cdot b)$.
(d) Se R for um anel com unidade, então existe $1_R \in R$. Suponha que exista $u \in R$ tal que $u \cdot r = r = r \cdot u$ para todo $r \in R$. Então $u = u \cdot 1_R = 1_R$.
(e) Observe que $r + ((-1_R) \cdot r) = (1_R \cdot r) + ((-1_R) \cdot r) = (1_R - 1_R) \cdot r = 0_R \cdot r = 0_R$ para todo $r \in R$. Logo $((-1_R) \cdot r) = -r$. □

Definição 17.8. Dado um anel R, um elemento $a \in R$, $a \neq 0_R$, é dito um divisor de zero quando existe $b \in R$, $b \neq 0_R$, tal que $a \cdot b = 0_R$ ou $b \cdot a = 0_R$. Dado um anel não-trivial com unidade R, um elemento $u \in R$ é dito uma unidade quando existe $r \in R$ tal que $u \cdot r = 1_R = r \cdot u$. Neste caso, o conjunto de unidades de R é denotado por $R^\times$. Um anel R é dito um domínio (integral) quando R é não-trivial, comutativo, com unidade, e não tem nenhum divisor de zero.

Exemplo 17.9. Observe que $(\mathbb{Z}, +, \cdot)$ é um domínio. De fato, $a \cdot b = 0$ se, e somente se, $a = 0$ ou $b = 0$. Além disso, segue da Proposição 6.15(a) que $\mathbb{Z}^\times = \{-1, 1\}$. Observe que, em particular, $2 \in \mathbb{Z}$ não é nem uma unidade, nem um divisor de zero.

Exemplo 17.10. Observe que $(\mathbb{Z}_8, +, \cdot)$ não é um domínio, pois $\overline{2}, \overline{4}, \overline{6} \in \mathbb{Z}_8$ são divisores de zero. De fato, $\overline{2} \cdot \overline{4} = \overline{0} = \overline{6} \cdot \overline{4}$. Além disso, segue da Proposição 6.15(b) que $\mathbb{Z}_8^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$.

Exercício 17.11. Mostre que o anel $\mathbb{Z}_p$ é um corpo se, e somente se, p é primo.

Exemplo 17.12. Considere o conjunto $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ munido das funções $s\colon \mathbb{Z}[\sqrt{2}] \times \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ e $m\colon \mathbb{Z}[\sqrt{2}] \times \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ dadas por:

$$s(a + b\sqrt{2},\ c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \quad \text{(soma usual de números reais)} \quad \text{e}$$

$$m(a + b\sqrt{2},\ c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2} \quad \text{(produto usual de números reais)}.$$

Verifique que $\big(\mathbb{Z}[\sqrt{2}], s, m\big)$ é um anel comutativo com identidade $1_{\mathbb{Z}[\sqrt{2}]} = 1 + 0\sqrt{2}$. Mas $\mathbb{Z}[\sqrt{2}]$ não é um anel de divisão, e portanto não é um corpo. De fato, $m(2, c + d\sqrt{2}) = 1$ se, e somente se, $2c = 1$ e $2d = 0$, ou seja, $c = \frac{1}{2}$ e $d = 0$. Como $\frac{1}{2} \notin \mathbb{Z}$, então não existe um inverso multiplicativo para $2 \neq 0_{\mathbb{Z}[\sqrt{2}]}$ em $\mathbb{Z}[\sqrt{2}]$.

Exemplo 17.13. Considere o conjunto $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ munido das funções $s\colon \mathbb{Q}(\sqrt{2}) \times \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$, dada pela soma usual de números reais, e $m\colon \mathbb{Q}(\sqrt{2}) \times \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$, dada pelo produto usual de números reais. Verifique que $\big(\mathbb{Q}(\sqrt{2}), s, m\big)$ é um anel comutativo com identidade $1_{\mathbb{Q}(\sqrt{2})} = 1 + 0\sqrt{2}$. Além disso, $\mathbb{Q}(\sqrt{2})$ é um corpo. De fato, dado $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2}) \setminus \{0_{\mathbb{Q}(\sqrt{2})}\}$, temos $m\left(a + b\sqrt{2},\ \left(\frac{a}{a^2 - 2b^2}\right) + \left(\frac{-b}{a^2 - 2b^2}\right)\sqrt{2}\right) = 1_{\mathbb{Q}(\sqrt{2})}$. Além disso, $\left(\frac{a}{a^2 - 2b^2}\right) + \left(\frac{-b}{a^2 - 2b^2}\right)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. De fato, $a^2 = 2b^2$ se, e somente se, $a = \pm b\sqrt{2}$. Agora, como $b \in \mathbb{Q} \setminus \{0\}$, então $\pm b\sqrt{2} \notin \mathbb{Q}$. Ou seja, $a^2 - 2b^2 \neq 0$ para todos $a, b \in \mathbb{Q}$ não ambos nulos.

Proposição 17.14. *Seja (R, s, m) um anel não-trivial com unidade.*

(a) Se $r \in R$ for um divisor de zero, então $r \notin R^\times$. Equivalentemente, se $r \in R^\times$, então r não é um divisor de zero.
(b) $(R^\times, m)$ é um grupo.
(c) R é um anel de divisão se, e somente se, $R^\times = R \setminus \{0_R\}$.
(d) Se $a \in R$ não é um divisor de zero (em particular, se R for um domínio) e $m(a, b) = m(a, c)$, então $a = 0_R$ ou $b = c$. Analogamente, se $a \in R$ não é um divisor de zero e $m(b, a) = m(c, a)$, então $a = 0_R$ ou $b = c$.

Demonstração. (a) Vamos mostrar que, se $r \in R^\times$, então r não é um divisor de zero. Por definição, $R^\times = \{r \in R \mid \text{existe } u \in R \text{ tal que } m(u, r) = 1_R = m(r, u)\}$. Suponha que $r \in R^\times$ e tome $u \in R$ tal que $m(u, r) = 1_R = m(r, u)$. Se $a \in R$ for tal que $m(r, a) = 0_R$, então $0_R = m(u, 0_R) = m(u, m(r, a)) = m(m(u, r), a) = m(1_R, a) = a$. Analogamente, se $a \in R$ for tal que $m(a, r) = 0_R$, então $0_R = m(0_R, u) = m(m(a, r), u) = m(a, m(r, u)) = m(a, 1_R) = a$. Isso mostra que r não é um divisor de zero.

(b) Primeiro, vamos mostrar que $m(a, b) \in R^\times$ para todos $a, b \in R^\times$. Se $a, b \in R^\times$, então existem $u, v \in R$ tais que $m(a, u) = m(u, a) = m(b, v) = m(v, b) = 1_R$. Consequentemente,

$$\begin{aligned} m(m(a,b), m(v,u)) &= m(m(m(a,b), v), u) \\ &= m(m(a, m(b,v)), u) \\ &= m(m(a, 1_R), u) \\ &= m(a, u) \\ &= 1_R, \end{aligned} \qquad \begin{aligned} m(m(v,u), m(a,b)) &= m(v, m(u, m(a,b))) \\ &= m(v, m(m(u,a), b)) \\ &= m(v, m(1_R, b)) \\ &= m(v, b) \\ &= 1_R. \end{aligned}$$

Isso mostra que $m(a, b) \in R^\times$. Agora vamos verificar as condições $(i) - (iii)$ da Definição 1.1.

(i) Pela Definição 17.1(ii), $m(a, m(b, c)) = m(m(a, b), c)$ para todos $a, b, c \in R$.

(ii) Pela definição de 1_R, $m(1_R, a) = 1_R = m(a, 1_R)$ para todo $a \in R$. Logo, pela definição de $R^\times$, $e_{R^\times} = 1_R \in R^\times$.
(iii) Pela definição de $R^\times$, para todo $r \in R^\times$, existe $u \in R$ tal que $m(r, u) = 1_R = m(u, r)$. Portanto $u = r^{-1} \in R^\times$.

(c) Pela Definição 17.1, R é um anel de divisão se, e somente se, para todo $r \in R \setminus \{0_R\}$, existe $u \in R$ tal que $m(r, u) = 1_R = m(u, r)$. Ou seja, R é um anel de divisão se, e somente se, $R^\times = R \setminus \{0_R\}$.

(d) Suponha que $a \in R$ não é um divisor de zero e que $m(a, b) = m(a, c)$. Então $m(a, s(b, -c)) = s(m(a, b), -m(a, c)) = 0_R$. Como a não é um divisor de zero, então $s(b, -c) = 0_R$ ou $a = 0_R$. Ou seja, $a = 0_R$, ou $b = c$. A demonstração do outro caso é completamente análoga. □

Corolário 17.15. *Todo domínio finito é um corpo.*

Demonstração. Suponha que D é um domínio e que $|D|$ é finita. Lembre que, pela Definição 17.8, D é um anel comutativo com identidade e sem divisores de zero. Vamos mostrar que, para todo $a \in D \setminus \{0_D\}$, existe $b \in D$ tal que $a \cdot b = 1_D = b \cdot a$. Dado $a \in D \setminus \{0_D\}$, considere a função $f_a \colon D \to D$ dada por $f_a(b) = a \cdot b$. Pela Proposição 17.14(d), f_a é injetora. Como $|D|$ é finita, segue que f_a é sobrejetora. Em particular, existe $b \in D$ tal que $a \cdot b = f_a(b) = 1_R$.

Analogamente, considere a função $g_a \colon D \to D$ dada por $g_a(c) = c \cdot a$. Pela Proposição 17.14(d), g_a é injetora. Como $|D|$ é finita, segue que g_a é sobrejetora. Em particular, existe $c \in D$ tal que $c \cdot a = g_a(c) = 1_R$. Para terminar, observe que $c = c \cdot 1_R = c \cdot (a \cdot b) = (c \cdot a) \cdot b = 1_R \cdot b = b$. □

Definição 17.16. Dado um anel $(R, +, \cdot)$, um subanel de R é um subconjunto não-vazio $S \subseteq R$ tal que, para todos $a, b \in S$:

(i) $a + b \in S$,
(ii) $-a \in S$,
(iii) $a \cdot b \in S$.

Ou seja, um subanel é um subconjunto (não-vazio) de um anel que, quando munido das restrições da soma e multiplicação do anel, é também um anel.

Exemplo 17.17. Considere o anel $(\mathbb{Z}, +, \cdot)$ e o subconjunto $2\mathbb{Z} = \{2z \in \mathbb{Z} \mid z \in \mathbb{Z}\}$. Observe que:

(i) Para todos $z_1, z_2 \in \mathbb{Z}$, $2z_1 + 2z_2 = 2(z_1 + z_2) \in 2\mathbb{Z}$,
(ii) Para todo $z \in \mathbb{Z}$, $-(2z) = 2(-z) \in 2\mathbb{Z}$,
(iii) Para todos $z_1, z_2 \in \mathbb{Z}$, $(2z_1) \cdot (2z_2) = 2(2z_1 z_2) \in 2\mathbb{Z}$.

Portanto $2\mathbb{Z}$ é um subanel de $\mathbb{Z}$. Observe também que $2\mathbb{Z}$ munido da soma e multiplicação usual também é um anel (por si só, independente de $\mathbb{Z}$). Além disso, $2\mathbb{Z}$ é comutativo e sem identidade.

Exemplo 17.18. Considere um anel não-trivial R. O subconjunto $R^\times$ não é um subanel de R, pois $R^\times$ não satisfaz a condição (i) da Definição 17.16. De fato, $1_R \in R^\times$ e $-1_R \in R^\times$, pois $(-1_R) \cdot (-1_R) = -(-1_R) \cdot 1_R = -(-1_R) = 1_R$. Mas $-1_R + 1_R = 0_R \notin R^\times$.

Exemplo 17.19. Considere o anel $\mathbb{Z}[\sqrt{2}]$ (do Exemplo 17.12) e o corpo $\mathbb{Q}(\sqrt{2})$ (do Exemplo 17.13). Como as operações binárias s e m em $\mathbb{Z}[\sqrt{2}]$ são restrições das respectivas operações em $\mathbb{Q}(\sqrt{2})$, então $\mathbb{Z}[\sqrt{2}]$ é um subanel de $\mathbb{Q}(\sqrt{2})$. Mais do que disso, as operações binárias s e m em $\mathbb{Q}(\sqrt{2})$ são restrições da soma e multiplicação usuais de $\mathbb{R}$. Como $\mathbb{R}$ munido dessas operações também é um corpo (Exercício 17.4), segue que $\mathbb{Q}(\sqrt{2})$ é um subcorpo de $\mathbb{R}$.

Exercício 17.20. Considere os conjuntos dos números inteiros ($\mathbb{Z}$), racionais ($\mathbb{Q}$), reais ($\mathbb{R}$), complexos ($\mathbb{C}$) e quatérnios ($\mathbb{H}$) munidos de suas respectivas somas e multiplicações usuais. Mostre que $\mathbb{Z}$ é um subanel de $\mathbb{Q}$, que é um subanel (subcorpo) de $\mathbb{Q}(\sqrt{2})$, que é um subanel (subcorpo) de $\mathbb{R}$, que $\mathbb{R}$ é um subanel (subcorpo) de $\mathbb{C}$, que é um subanel de $\mathbb{H}$.

Aula 18

7.2. Exemplos: Anéis de polinômios, matrizes e anéis de grupos

Anéis de polinômios

Considere um anel comutativo com identidade R e uma variável $\bigstar$. Um polinômio em $\bigstar$ com coeficientes em R é um elemento da forma

$$r_0 + r_1\bigstar + \cdots + r_n\bigstar^n, \qquad \text{onde } n \geq 0 \text{ e } r_0, \ldots, r_n \in R.$$

(Observe que um polinômio em $\bigstar$ com coeficientes em R não é uma função, não é um número, não é nada além do símbolo representado por essa soma formal.) Denote o conjunto de todos os polinômios em $\bigstar$ com coeficientes em R por $R[\bigstar]$. Dois polinômios, $a_0 + \cdots + a_n\bigstar^n \in R[\bigstar]$ e $b_0 + \cdots + b_m\bigstar^m \in R[\bigstar]$, são ditos iguais quando:

- $n = m$ e $a_i = b_i$ para todo $i \in \{0, \ldots, n\}$, ou
- $n > m$, $a_i = b_i$ para todo $i \in \{0, \ldots, n\}$ e $b_j = 0$ para todo $j \in \{n+1, \ldots, m\}$, ou
- $m > n$, $a_i = b_i$ para todo $i \in \{0, \ldots, m\}$ e $a_j = 0$ para todo $j \in \{m+1, \ldots, n\}$.

Defina duas operações binárias $s\colon R[\bigstar] \times R[\bigstar] \to R[\bigstar]$ e $m\colon R[\bigstar] \times R[\bigstar] \to R[\bigstar]$ da seguinte forma:

$$s(a_0 + \cdots + a_n\bigstar^n,\ b_0 + \cdots + b_n\bigstar^n) = (a_0 + b_0) + \cdots + (a_n + b_n)\bigstar^n,$$

$$m(a_0 + \cdots + a_n\bigstar^n,\ b_0 + \cdots + b_m\bigstar^m) = c_0 + \cdots + c_{m+n}\bigstar^{m+n}, \qquad c_k = \sum_{i=\max\{0,k-m\}}^{\min\{n,k\}} a_i b_{k-i}.$$

Exercício 18.1. Verifique que $(R[\bigstar], s, m)$ é um anel comutativo com identidade.

Considere um polinômio $p = r_0 + \cdots + r_n\bigstar^n \in R[\bigstar]$. Se $r_i \neq 0$ para algum $i \in \{0, \ldots, n\}$, defina o grau de p como sendo $\text{grau}(p) = \max\{i \mid r_i \neq 0\}$. (Se $p = 0_R$, não definimos o grau de p.) Quando $p \neq 0_R$ e $\text{grau}(p) = 0$, o polinômio p é chamado de polinômio constante. Se o grau de p for $d \geq 0$, definimos o termo líder de p como sendo $r_d\bigstar^d$ e o coeficiente líder de p como sendo r_d. O polinômio p é dito mônico quando seu coeficiente líder é 1.

Proposição 18.2. *Seja R um anel comutativo com identidade.*

(a) Se R for um domínio, então $\text{grau}(p \cdot q) = \text{grau}(p) + \text{grau}(q)$ para todos $p, q \in R[\bigstar] \setminus \{0_{R[\bigstar]}\}$.
(b) Se R for um domínio, então $R[\bigstar]^\times = R^\times$.
(c) $R[\bigstar]$ é um domínio se, e somente se, R é um domínio.
(d) Se $S \subseteq R$ é um subanel, então $S[\bigstar] \subseteq R[\bigstar]$ é um subanel.

Demonstração. (a) Sejam $p = a_0 + \cdots + a_n\bigstar^n \in R[\bigstar]$, $n = \text{grau}(p)$, $q = b_0 + \cdots + b_m\bigstar^m \in R[\bigstar]$ e $m = \text{grau}(q)$. Por definição, $p \cdot q = (a_0 b_0) + \cdots + (a_n b_m)\bigstar^{n+m}$. Como $\text{grau}(p) = n$ (resp. $\text{grau}(q) = m$), então $a_n \neq 0$ (resp. $b_m \neq 0$). Como R é um domínio, $a_n b_m \neq 0$, o que implica que $\text{grau}(p \cdot q) = m + n$.

(b) Primeiro observe que $R^\times \subseteq R[\bigstar]^\times$. Agora suponha que $p \in R[\bigstar]^\times$, ou seja, existe $q \in R[\bigstar]$ tal que $p \cdot q = 1$. Pela parte (a), $\text{grau}(p) + \text{grau}(q) = \text{grau}(p \cdot q) = \text{grau}(1) = 0$ se, e somente se, $\text{grau}(p) = \text{grau}(q) = 0$. Isso mostra que $p, q \in R$. Além disso, como $p \cdot q = 1$, temos que $p, q \in R^\times$.

(c) Se $R[\bigstar]$ for um domínio, então, em particular, para quaisquer $p, q \in R$ tais que $p \cdot q = 0$, temos que ter $p = 0$ ou $q = 0$. Por outro lado, se R for um domínio, então $\text{grau}(p \cdot q) = \text{grau}(p) + \text{grau}(q)$ para todos $p, q \in R[\bigstar] \setminus \{0\}$ pela parte (a). Em particular, isso mostra que $p \cdot q \neq 0$. Logo $R[\bigstar]$ é um domínio.

(d) Vamos verificar as condições (i)-(iii) da Definição 17.16. Sejam $p = a_0 + \cdots + a_n\bigstar^n$, $q = b_0 + \cdots + b_m\bigstar^m \in S[\bigstar]$ e (sem perda de generalidade), suponha que $n \leq m$:
   (i) $p + q = (a_0 + b_0) + \cdots + (a_n + b_n)\bigstar^n + b_{n+1}\bigstar^{n+1} + \cdots + b_m\bigstar^m \in S[\bigstar]$, pois, como $S \subseteq R$ é um subanel, $(a_0 + b_0), \ldots, (a_n + b_n) \in S$.
   (ii) $-p = (-a_0) + \cdots + (-a_n)\bigstar^n \in S[\bigstar]$, pois $S \subseteq R$ é um subanel e $(-a_0), \ldots, (-a_n) \in S$.
   (iii) $p \cdot q = c_0 + \cdots + c_{n+m}$, onde $c_k = \sum_{i=\max\{0,k-m\}}^{\min\{n,k\}} a_i b_{k-i} \in S$ para todo $k \in \{0, \ldots, m+n\}$, pois $S \subseteq R$ é um subanel. □

Conjunto dos números quatérnios

Considere três símbolos i, j, k e o conjunto $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$. Defina uma operação binária $s\colon \mathbb{H} \times \mathbb{H} \to \mathbb{H}$ por:

$$s(a_1 + b_1 i + c_1 j + d_1 k,\ a_2 + b_2 i + c_2 j + d_2 k) = (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k.$$

Exercício 18.3. Mostre que $(\mathbb{H}, s)$ é um grupo abeliano e que $0_{\mathbb{H}} = 0 + 0i + 0j + 0k$.

Agora defina $m\colon \mathbb{H} \times \mathbb{H} \to \mathbb{H}$ como a única operação binária associativa que satisfaz:

$$\begin{gathered}
m(s(x, y), z) = s(m(x, z), m(y, z)) \quad \text{para todos } x, y, z \in \mathbb{H}, \\
m(x, s(y, z)) = s(m(x, y), m(x, cz)) \quad \text{para todos } x, y, z \in \mathbb{H}, \\
m(\alpha, a + bi + cj + dk) = (\alpha a) + (\alpha b)i + (\alpha c)j + (\alpha d)k = m(a + bi + cj + dk, \alpha), \\
m(i, i) = -1, \quad m(i, j) = k, \quad m(i, k) = -j, \\
m(j, i) = -k, \quad m(j, j) = -1, \quad m(j, k) = i, \\
m(k, i) = j, \quad m(k, j) = -i, \quad m(k, k) = -1.
\end{gathered}$$

Ou seja, nós construímos $\mathbb{H}$, s e m de modo que $(\mathbb{H}, s, m)$ é um anel.

Observe que $\mathbb{H}$ é um anel com identidade $1_{\mathbb{H}} = 1 + 0i + 0j + 0k$. Observe ainda que $\mathbb{H}$ não é um anel comutativo. Por exemplo, $m(i, j) = k = -m(j, i)$. Além disso, $\mathbb{H}$ é um anel de divisão. De fato, para todo $a + bi + cj + dk \in \mathbb{H}$, temos que

$$\begin{aligned}
m(a + bi + cj + dk, a - bi - cj - dk) &= a^2 - (ab)i - (ac)j - (ad)k \\
&\quad + (ab)i + b^2 - (bc)j + (bd)k \\
&\quad + (ac)j + (bc)k + c^2 - (cd)i \\
&\quad + (ad)k - (bd)j + (cd)i + d^2 \\
&= a^2 + b^2 + c^2 + d^2.
\end{aligned}$$

Portanto, para todo $a + bi + cj + dk \in \mathbb{H} \setminus \{0_{\mathbb{H}}\}$, temos que $a^2 + b^2 + c^2 + d^2 > 0$ e

$$m\left(a + bi + cj + dk, \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}\right) = 1_{\mathbb{H}}.$$

Mas, como $\mathbb{H}$ não é comutativo, ele não é um corpo.

Exercício 18.4. Mostre que $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são subanéis de $\mathbb{H}$.

Anel de matrizes

Considere $n > 0$, R um anel não-trivial e o conjunto $M_n(R)$ formado por matrizes de ordem $n \times n$ e entradas em R. Defina $s\colon M_n(R) \times M_n(R) \to M_n(R)$ como $s(A, B) = A + B$, a soma usual de matrizes (entrada-a-entrada), e $m\colon M_n(R) \times M_n(R) \to M_n(R)$ como $m(A, B) = AB$, o produto usual de matrizes (linha por coluna).

Exercício 18.5. Mostre que $M_n(R)$ é um anel e que $0_{M_n(R)}$ é a matriz cujas entradas são todas iguais a 0_R.

Vamos mostrar que o anel $M_n(R)$ é comutativo se, e somente se, $n = 1$ e R é comutativo. De fato, $M_1(R) = \{(r) \mid r \in R\}$ com $m((a),(b)) = (ab)$ para todos $(a),(b) \in M_1(R)$. Se R é um anel comutativo, então $m((a),(b)) = (ab) = (ba) = m((b),(a))$ para todos $a, b \in R$. Logo $M_1(R)$ é comutativo. Por outro lado, se $n = 1$ e R não for comutativo, então existem $a, b \in R$ tais que $m((a),(b)) = (ab) \neq (ba) = m((b),(a))$. Logo $M_1(R)$ não é comutativo. Além disso, se $n > 1$ (qualquer R não-trivial), então existem $a, b \in R$ tais que $a \cdot b \neq 0_R$. Considere as matrizes A, cuja entrada $(1,2)$ é a e todas as outras são 0_R, e B cuja entrada $(2,1)$ é b e todas as outras são 0_R. Temos que $m(A,B)$ é a matriz cuja entrada $(1,1)$ é $a \cdot b$ e todas as outras são 0_R e $m(B,A)$ é a matriz cuja entrada $(2,2)$ é $b \cdot a$ e todas as outras são 0_R. Isso mostra que $m(A,B) \neq m(B,A)$ e que $M_n(R)$ não é comutativo.

Agora vamos mostrar que, se R tem identidade ($n > 0$), então $M_n(R)$ tem identidade. Para isso, denote por $E_{i,j}$ a matriz em $M_n(R)$ cuja entrada (i,j) é 1_R e todas as outras entradas são 0_R. Observe que, para todos $i, j, k, \ell \in \{1, \ldots, n\}$:

$$m(E_{i,j}, E_{k,\ell}) = E_{i,\ell}, \quad \text{se } j = k \qquad \text{e} \qquad m(E_{i,j}, E_{k,\ell}) = 0_{M_n(R)}, \quad \text{se } j \neq k. \tag{18.2}$$

Agora observe que, para todo $A \in M_n(R)$, existem $a_{i,j} \in R$ tais que $A = \sum_{i=1}^n \sum_{j=1}^n a_{ij} E_{i,j}$. Denote por I_n a matriz $I_n = E_{1,1} + \cdots + E_{n,n} \in M_n(R)$. Por (18.2), temos que

$$\begin{aligned}
m(A, I_n) &= \sum_{i=1}^n \sum_{j=1}^n a_{ij} m(E_{i,j}, E_{1,1}) + \cdots + \sum_{i=1}^n \sum_{j=1}^n a_{ij} m(E_{i,j}, E_{n,n}) \\
&= \sum_{i=1}^n a_{i1} E_{i,1} + \cdots + \sum_{i=1}^n a_{in} E_{i,n} \\
&= A, \\
m(I_n, A) &= \sum_{i=1}^n \sum_{j=1}^n a_{ij} m(E_{1,1}, E_{i,j}) + \cdots + \sum_{i=1}^n \sum_{j=1}^n a_{ij} m(E_{n,n}, E_{i,j}) \\
&= \sum_{j=1}^n a_{1j} E_{1,j} + \cdots + \sum_{j=1}^n a_{nj} E_{n,j} \\
&= A,
\end{aligned}$$

para toda $A = \sum_{i=1}^n \sum_{j=1}^n a_{ij} E_{i,j} \in M_n(R)$. Isso mostra que $I_n = 1_{M_n(R)}$ é a identidade de $M_n(R)$.

Se R é um anel comutativo, então $M_n(R)^\times = \{A \in M_n(R) \mid \det(A) \in R^\times\}$. Esse conjunto é chamado de grupo geral linear e denotado por $GL_n(R)$. De fato, por um lado, se $A \in M_n(R)^\times$, então existe $B \in M_n(R)$ tal que $AB = I_n = BA$. Como $1_R = \det(I_n) = \det(AB) = \det(A)\det(B)$ e $1_R = \det(I_n) = \det(BA) = \det(B)\det(A)$, então $\det(A) \in R^\times$ (e $\det(A)^{-1} = \det(B)$). Por outro lado, se $\det(A) \in R^\times$, vamos construir uma matriz B tal que $AB = I_n = BA$. Primeiro denote $A = \sum_{i=1}^n \sum_{j=1}^n a_{ij} E_{i,j}$, e para cada $i, j \in \{1, \ldots, n\}$, defina $A^{(i,j)}$ como sendo a matriz em $M_{n-1}(R)$ obtida da matriz A apagando a i-ésima linha e j-ésima coluna. Defina $B = \sum_{i=1}^n \sum_{j=1}^n b_i j E_{i,j}$ com $b_{ij} = \frac{(-1)^{i+j} \det(A^{(i,j)})}{\det(A)}$. Verifique que $m(A,B) = I_n = m(B,A)$.

Pelo que mostramos acima, $M_n(R)$ é um corpo se, e somente se, $n = 1$ e R é um corpo.

Anel de matrizes

Lembre que, para todo anel R, $M_n(R)$ é um anel, e que $M_n(R)$ tem identidade, se R tiver identidade. Além disso, $M_n(R)$ é um domínio se, e somente se, $n = 1$ e R é um domínio.

De fato, $M_1(R) = \{(r) \mid r \in R\}$ com $m((a),(b)) = (ab)$ (para todos $a, b \in R$) é um domínio se, e somente se, R é um domínio. Por outro lado, se $n \geq 2$ (qualquer R não-trivial), então $m(aE_{1,1}, bE_{2,2}) = 0_{M_n(R)}$ pela equação (18.2). Isso mostra que $aE_{1,1} \in M_n(R) \setminus \{0_{M_n(R)}\}$ é um divisor de zero para todo $a \neq 0_R$.

Observe que, se $S \subseteq R$ é um subanel, então $M_n(S) \subseteq M_n(R)$ é um subanel. Outros exemplos de subanéis de $M_n(R)$ são os seguintes:

- Matrizes triangulares superiores: $\{A = (a_{ij}) \mid a_{ij} = 0 \text{ para todo } i > j\}$;
- Matrizes triangulares inferiores: $\{A = (a_{ij}) \mid a_{ij} = 0 \text{ para todo } i < j\}$;
- Matrizes diagonais: $\{A = (a_{ij}) \mid a_{ij} = 0 \text{ para todo } i \neq j\}$.

Anel de grupo

Dados um anel não-trivial $(R, +, \cdot)$ e um grupo G, considere o conjunto

$$R[G] = \{r_1 g_1 + \cdots + r_n g_n \mid n \geq 0,\ r_1, \ldots, r_n \in R,\ g_1, \ldots, g_n \in G\}.$$

Observe que todo elemento em $R[G]$ pode ser escrito da forma $\sum_{g \in G} r_g g$, onde $r_g \in G$ para todo $g \in G$ e $r_g \neq 0_R$ apenas para uma quantidade finita de $g \in G$. Usando essa notação, defina uma operação binária $s\colon R[G] \times R[G] \to R[G]$ como

$$s\left(\sum_{g \in G} a_g g,\ \sum_{g \in G} b_g g\right) = \sum_{g \in G} (a_g + b_g) g.$$

Observe que $(R[G], s)$ é um grupo abeliano com elemento neutro $0_{R[G]} = \sum_{g \in G} 0_R g$. Agora defina uma operação binária $m\colon R[G] \times R[G] \to R[G]$ como

$$m\left(\sum_{g \in G} a_g g,\ \sum_{g \in G} b_g g\right) = \sum_{g \in G} c_g g, \qquad \text{onde } c_g = \sum_{h \in G} (a_h \cdot b_{h^{-1}g}).$$

Exercício 18.6. Sejam R um anel não-trivial e G um grupo.

(a) Mostre que $(R[G], s, m)$ é um anel.
(b) Mostre que, se R e G forem comutativos, então $R[G]$ é comutativo.
(c) Mostre que, se R tiver identidade, então $R[G]$ tem identidade $1_{R[G]} = 1_R e_G$.
(d) Mostre que o conjunto $\{re_G \mid r \in R\}$ é um subanel de $R[G]$. Dessa forma, podemos identificar R como um subanel de $R[G]$, explicitamente, identificando o elemento $r \in R$ com o elemento $re_G \in R[G]$. Use essa identificação para mostrar que $R^\times \subseteq R[G]^\times$.
(e) Para todo $g \in G$, mostre que $1_R g \in R[G]^\times$.

Exemplo 18.7. Considere $R = \mathbb{R}$ e $G = \mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$. Por definição,

$$\mathbb{R}[\mathbb{Z}_2] = \{r_0\overline{0} + r_1\overline{1} \mid r_0, r_1 \in R\} = \mathbb{R}^2 \qquad \text{(como conjunto)},$$
$$s(a_0\overline{0} + a_1\overline{1},\ b_0\overline{0} + b_1\overline{1}) = (a_0 + b_0)\overline{0} + (a_1 + b_1)\overline{1} \qquad \text{(soma coordenada-a-coordenada)},$$
$$m(a_0\overline{0} + a_1\overline{1},\ b_0\overline{0} + b_1\overline{1}) = (a_0b_0 + a_1b_1)\overline{0} + (a_0b_1 + a_1b_0)\overline{1}.$$

Observe que, dados $a, b \in \mathbb{R}$, existem $x, y \in \mathbb{R}$ tais que $m(a\overline{0} + b\overline{1},\ x\overline{0} + y\overline{1}) = 1$ se, e somente se, $ax + by = 1$ e $ay + bx = 0$. Agora, o sistema linear

$$\begin{cases} ax + by = 1 \\ bx + ay = 0 \end{cases}$$

tem solução única se, e somente se, $a \notin \{-b, b\}$. De fato, se $a \notin \{-b, b\}$, então

$$m\left(a\overline{0} + b\overline{1},\ \frac{a}{a^2 - b^2}\overline{0} + \frac{-b}{a^2 + b^2}\overline{1}\right) = 1.$$

Caso contrário, $m((a\overline{0}+a\overline{1}),(a\overline{0}-a\overline{1}))=0$. Ou seja, $(a\overline{0}+a\overline{1})$, $(a\overline{0}-a\overline{1})$ são divisores de zero para todo $a\in\mathbb{R}\setminus\{0\}$; e $(a\overline{0}+b\overline{1})\in\mathbb{R}[\mathbb{Z}_2]^\times$ para todos $a,b\in\mathbb{R}$ tais que $a\notin\{-b,b\}$.

Exemplo 18.8. Considere $R=\mathbb{Q}$ e $G=\mathbb{Z}$. Para não confundirmos os elementos de $\mathbb{Q}$ com os elementos de $\mathbb{Z}$, vamos denotar os elementos do grupo $\mathbb{Z}$ por x^z $(z\in\mathbb{Z})$. Observe que, usando essa notação, a operação binária do grupo $\mathbb{Z}$ se torna $(x^a)(x^b)=x^{a+b}$ (que é a regra usual de expoentes). Usando essa notação, temos:

$$\mathbb{Q}[\mathbb{Z}]=\{a_{-n}x^{-n}+\cdots+a_0x^0+\cdots+a_mx^m\mid -n\leq 0\leq m,\ a_{-n},\ldots,a_m\in\mathbb{Q}\}.$$

Além disso, observe que s se identifica com a soma usual de polinômios e m se identifica com o produto usual de polinômios. Esse anel é chamado de anel de polinômios de Laurent em x com coeficientes em $\mathbb{Q}$, e denotado por $\mathbb{Q}[x,x^{-1}]$.

Observe que $\mathbb{Q}[\mathbb{Z}]$ é um domínio, mas não é um anel de divisão. De fato, considere $p=a_{-n}x^{-n}+\cdots+a_mx^m\in\mathbb{Q}[\mathbb{Z}]$ com $a_{-n},a_m\neq 0$ e $q=b_{-k}x^{-k}+\cdots+b_\ell x^\ell\in\mathbb{Q}[\mathbb{Z}]$ com $b_{-k},b_\ell\neq 0$. Como $\mathbb{Q}$ é um domínio (um corpo), então $p\cdot q=(a_{-n}b_{-k})x^{-n-k}+\cdots+(a_mb_\ell)x^{m+\ell}\neq 0$. Em particular, $x^2\notin\mathbb{Q}[\mathbb{Z}]^\times$.

Exemplo 18.9. Considere $R=\mathbb{Z}_2$ e $G=S_3$. Observe que $\mathbb{Z}_2[S_3]$ tem 64 $(=2^6)$ elementos. De fato, cada $\sigma\in S_3$ pode ter coeficiente $\overline{0}$ ou $\overline{1}$. O anel $\mathbb{Z}_2[S_3]$ não é comutativo. Por exemplo,

$$m(\overline{1}(1\ 2),\overline{1}(1\ 3))=\overline{1}(1\ 3\ 2)\neq\overline{1}(1\ 2\ 3)=m(\overline{1}(1\ 3),\overline{1}(1\ 2)).$$

Mas $\mathbb{Z}_2[S_3]$ é um anel com unidade $1_{\mathbb{Z}_2[S_3]}=\overline{1}(1)$. Além disso, $\mathbb{Z}_2[S_3]$ também não é um domínio. Por exemplo, $m(\overline{1}+(1\ 2),\ \overline{1}-(1\ 2))=\overline{0}$. Logo $\mathbb{Z}_2[S_3]$ não é um anel de divisão, nem um corpo.

Aula 19

7.3. Homomorfimos de anéis e anéis quocientes

Definição 19.1. Sejam R e S dois anéis. Uma função $f\colon R \to S$ é dita um homomorfismo de anéis quando, para todos $r_1, r_2 \in R$, temos:

(i) $f(r_1 +_R r_2) = f(r_1) +_S f(r_2)$,
(ii) $f(r_1 \cdot_R r_2) = f(r_1) \cdot_S f(r_2)$.

Um homomorfismo de anéis $f\colon R \to S$ é dito um isomorfismo de anéis quando f for bijetor. Dois anéis R e S são ditos isomorfos quando existe um isomorfismo de anéis $f\colon R \to S$. O núcleo de um homomorfismo de anéis $f\colon R \to S$ é definido como sendo $\ker(f) = \{r \in R \mid f(r) = 0_S\}$.

Observe que todo homomorfismo de anéis $f\colon R \to S$ é um homomorfismo de grupos entre os grupos abelianos $(R, +_R)$ e $(S, +_S)$. Além disso, o núcleo do homomorfismo de anéis $f\colon R \to S$ é exatamente o núcleo desse homomorfismo de grupos.

Exemplo 19.2. Lembre que, se $f\colon \mathbb{Z} \to \mathbb{Z}$ é um homomorfismo de grupos, então $f(n) = nf(1)$ para todo $n \in \mathbb{Z}$. Portanto f é da forma $f(n) = nk$ para algum $k(= f(1)) \in \mathbb{Z}$. Fixe $k \in \mathbb{Z}$. Como $f(a)f(b) = (ak)(bk)$ e $f(ab) = (ab)k$ para todos $a, b \in \mathbb{Z}$, então os únicos homomorfismos de anéis $f\colon \mathbb{Z} \to \mathbb{Z}$ são: a identidade e o homomorfismo trivial.

Como id_R é uma bijeção para todo anel R, então id_R é um isomorfismo de anéis. Já o homomorfismo trivial, não é nem injetor nem sobrejetor (portanto não é um isomorfismo).

Exemplo 19.3. Lembre que não existem homomorfismos não-triviais de grupos $f\colon \mathbb{Z}_3 \to \mathbb{Z}$ (pois nenhum elemento de $\mathbb{Z} \setminus \{0\}$ tem ordem finita. Logo não existe nenhum homomorfismo não-trivial de anéis $f\colon \mathbb{Z}_3 \to \mathbb{Z}$.

Exemplo 19.4. Considere dois grupos G, H e um anel R. Dado um homomorfismo de grupos $f\colon G \to H$, vamos mostrar que a função $F\colon R[G] \to R[H]$ dada por $F(r_1 g_1 \cdots + r_n g_n) = r_1 f(g_1) + \cdots + r_n f(g_n)$ é um homomorfismo de anéis:

$$\begin{aligned} &F\left(\sum_{g\in G} a_g g,\ \sum_{g\in G} b_g g\right) \\ &= F\left(\sum_{g\in G} (a_g + b_g) g\right) \\ &= \sum_{g\in G} (a_g + b_g) f(g) \\ &= \sum_{g\in G} a_g f(g) + \sum_{g\in G} b_g f(g) \\ &= F\left(\sum_{g\in G} a_g g\right) + F\left(\sum_{g\in G} b_g g\right), \end{aligned}$$

$$\begin{aligned} &F\left(\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right)\right) \\ &= F\left(\sum_{g\in G}\left(\sum_{h\in G} a_h b_{h^{-1}g}\right) g\right) \\ &= \sum_{g\in G}\left(\sum_{h\in G} a_h b_{h^{-1}g}\right) f(g) \\ &= \left(\sum_{g\in G} a_g f(g)\right)\left(\sum_{g\in G} b_g f(g)\right) \\ &= F\left(\sum_{g\in G} a_g g\right) F\left(\sum_{g\in G} b_g g\right). \end{aligned}$$

(a) Mostre que, se f for injetora, então F é injetora.
(b) Mostre que, se f for sobretora, então F é sobretora.

Definição 19.5. Dado um anel R, um ideal à esquerda (resp. ideal à direita) de R é um subconjunto $I \subseteq R$ satisfazedo:

(*i*) I é um subanel de R,
(*ii*) $ri \in I$ (resp. $ir \in I$) para todos $r \in R$ e $i \in I$.

Um ideal bilateral é um subconjunto $I \subseteq R$ que é um ideal à esquera e à direita de R.

Exemplo 19.6. Para todo anel R, o sunconjunto $\{0_R\}$ é um ideal bilateral de R. De fato:

- $0_R + 0_R = 0_R \in \{0_R\}$,
- $-0_R = 0_R \in \{0_R\}$,
- $0_R \cdot 0_R = 0_R \in \{0_R\}$,
- $r \cdot 0_R = 0_R = 0_R \cdot r \in \{0_R\}$ para todo $r \in R$.

Além disso, R também é um ideal bilateral de R. De fato:

- $r + s \in R$ para todos $r, s \in R$,
- $-r \in R$ para todo $r \in R$,
- $r \cdot s \in R$ para todos $r, s \in R$,
- $r \cdot s \in R$ para todos $r, s \in R$.

Exemplo 19.7. Vamos verificar que $2\mathbb{Z}$ é um ideal (bilateral) de $\mathbb{Z}$.

(*i*) Lembre do Exemplo 17.17 que $2\mathbb{Z}$ é um subanel de $\mathbb{Z}$.
(*ii*) Além disso, para todos $a, b \in \mathbb{Z}$, temos que $a(2b) = 2(ab) = (2b)a \in 2\mathbb{Z}$.

Exemplo 19.8. Observe que, apesar de $\mathbb{Z}$ ser um subanel de $\mathbb{R}$ (e de $\mathbb{Q}$), $\mathbb{Z}$ não é um ideal de $\mathbb{R}$ (nem de $\mathbb{Q}$). De fato, $2 \in \mathbb{Z}$, $\frac{4}{3} \in \mathbb{R}$ (e $\frac{4}{3} \in \mathbb{Q}$), mas $2\frac{4}{3} = \frac{8}{3} \notin \mathbb{Z}$.

Exemplo 19.9. Vamos verificar que o subconjunto $S = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ é um ideal à esquerda, mas não é um ideal à direita de $M_2(\mathbb{R})$. Primeiro vamos verificar que S é um subanel:

(i) Para todos $a_1, b_1, a_2, b_2 \in \mathbb{R}$, temos que
$$\begin{pmatrix} 0 & a_1 \\ 0 & b_1 \end{pmatrix} + \begin{pmatrix} 0 & a_2 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} 0 & a_1 + a_2 \\ 0 & b_1 + b_2 \end{pmatrix} \in S.$$

(ii) Para todos $a, b \in \mathbb{R}$, temos que
$$-\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & -a \\ 0 & -b \end{pmatrix} \in S.$$

(iii) Para todos $a_1, b_1, a_2, b_2 \in \mathbb{R}$, temos que
$$\begin{pmatrix} 0 & a_1 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} 0 & a_2 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} 0 & a_1 b_2 \\ 0 & b_1 b_2 \end{pmatrix} \in S.$$

Agora vamos mostrar que S é fechado pela multiplicação à esquerda por elementos de $M_2(\mathbb{R})$. Para todos $x, y, z, w, a, b \in \mathbb{R}$, temos que
$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & xa + yb \\ 0 & za + wb \end{pmatrix} \in S.$$
Isso mostra que S é um ideal à esquerda de $M_2(\mathbb{R})$. Mas como
$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \notin S,$$
então S não é um ideal à direita de $M_2(\mathbb{R})$.

Exercício 19.10. Se $\Bbbk$ é um corpo, mostre que os únicos ideias (bilaterais) de $\Bbbk$ são $\{0_\Bbbk\}$ e $\Bbbk$.

Proposição 19.11. *Sejam $f\colon R \to S$ um homomorfismo de anéis.*

(a) $\operatorname{im}(f)$ *é um subanel de* S.
(b) $\ker(f)$ *é um ideal bilateral de* R.

Demonstração. (a) Vamos verificar que $\operatorname{im}(f)$ satisfaz as condições (i)-(iii) da Definição 17.16.
(i) Se $s_1, s_2 \in \operatorname{im}(f)$, então existem $r_1, r_2 \in R$ tais que $f(r_1) = s_1$ e $f(r_2) = s_2$. Consequentemente, $f(r_1 + r_2) = f(r_1) + f(r_2) = (s_1 + s_2) \in \operatorname{im}(f)$.
(ii) Se $s \in \operatorname{im}(f)$, então existe $r \in R$ tal que $f(r) = s$. Consequentemente, $f(-r) = -f(r) = -s \in \operatorname{im}(f)$.
(iii) Se $s_1, s_2 \in \operatorname{im}(f)$, então existem $r_1, r_2 \in R$ tais que $f(r_1) = s_1$ e $f(r_2) = s_2$. Consequentemente, $f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2) = (s_1 \cdot s_2) \in \operatorname{im}(f)$.
(b) Vamos verificar que $\ker(f)$ satisfaz as condições (i)-(iii) da Definição 17.16 (que é a condição (i) da Definição 19.5) e a condição (ii) da Definição 19.5.
- Se $r_1, r_2 \in \ker(f)$, então $f(r_1) = f(r_2) = 0_S$. Consequentemente, $f(r_1 + r_2) = f(r_1) + f(r_2) = 0_S + 0_S = 0_S$. Logo $(r_1 + r_2) \in \ker(f)$.
- Se $r \in \ker(f)$, então $f(r) = 0_S$. Consequentemente, $f(-r) = -f(r) = -0_S = 0_S$. Logo $(-r) \in \ker(f)$.
- Se $r_1, r_2 \in \ker(f)$, então $f(r_1) = f(r_2) = 0_S$. Consequentemente, $f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2) = 0_S \cdot 0_S = 0_S$. Logo $(r_1 \cdot r_2) \in \ker(f)$.
- Se $r \in R$ e $k \in \ker(f)$, então $f(r \cdot k) = f(r) \cdot f(k) = f(r) \cdot 0_S = 0_S$ e $f(k \cdot r) = f(k) \cdot f(r) = 0_S \cdot f(r) = 0_S$. Logo $(r \cdot k), (k \cdot r) \in \ker(f)$. □

Definição 19.12. Sejam $(R, +\cdot)$ um anel e $I \subseteq R$ um ideal bilateral. Considere R como grupo (abeliano), $I \subseteq R$ como subgrupo (normal) e defina R/I como o grupo quociente, ou seja, munido da operação bilinear $s\colon (R/I) \times (R/I) \to (R/I)$ dada por $s(\overline{a}, \overline{b}) = \overline{a + b}$ para todos $\overline{a}, \overline{b} \in R/I$. Agora defina o anel quociente R/I como o grupo abeliano $(R/I, s)$ munido da operação bilinear $m\colon (R/I) \times (R/I) \to (R/I)$ dada por $m(\overline{a}, \overline{b}) = \overline{a \cdot b}$ para todos $\overline{a}, \overline{b} \in R/I$.

Exercício 19.13. Verifique que $((R/I), s, m)$ é de fato um anel.

O próximo resultado é a versão do Primeiro Teorema de Isomorfismo para anéis.

Teorema 19.14. *(a) Seja* $f\colon R \to S$ *um homorfismo de anéis. Existe um isomorfismo de anéis* $R/\ker(f) \cong \operatorname{im}(f)$.
(b) Sejam R *um anel e* $I \subseteq R$ *um ideal bilateral. A função* $\pi_I\colon R \to R/I$ *dada por* $\pi_I(r) = \overline{r}$ *é um homomorfismo sobrejetor de anéis.*

Demonstração. (a) Lembre da Proposição 19.11 que $\ker(f) \subseteq R$ é um ideal bilateral e $\operatorname{im}(f) \subseteq S$ é um subanel. Portanto $R/\ker(f)$ e $\operatorname{im}(f)$ são anéis. Lembre também que $f\colon R \to S$ é um homomorfismo de grupos abelianos $(R, +) \to (S, +)$. Portanto, do Teorema de Isomorfismo de grupos, segue que existe um isomorfismo de grupos abelianos $F\colon R/\ker(f) \to \operatorname{im}(f)$. Explicitamente, F é dado por $F(\overline{r}) = f(r)$ para todo $r \in R$. Vamos verificar que F é também um homomorfismo de anéis. Para todos $r_1, r_2 \in R$, temos

$$F(\overline{r_1} \cdot \overline{r_2}) = F(\overline{r_1 \cdot r_2}) = f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2) = F(\overline{r_1}) \cdot F(\overline{r_2}).$$

Isso termina a demonstração da parte (a).
(b) Primeiro vamos verificar que π_I é um homomorfismo de anéis. Para todos $r_1, r_2 \in R$, temos:

$$\pi_I(r_1 + r_2) = \overline{r_1 + r_2} = \overline{r_1} + \overline{r_2} = \pi_I(r_1) + \pi_I(r_2),$$
$$\pi_I(r_1 \cdot r_2) = \overline{r_1 \cdot r_2} = \overline{r_1} \cdot \overline{r_2} = \pi_I(r_1) \cdot \pi_I(r_2).$$

Isso mostra que π_I é um homomorfismo de anéis. Além disso, para todo $\overline{r} \in R/I$ existe $r \in R$ tal que $\pi_I(r) = \overline{r}$. Isso mostra que π_I é sobrejetor. □

Pelo resultado anterior, o núcleo de um homomorfismo de anéis é um ideal bilateral, e todo ideal bilateral é o núcleo de um homomorfismo de anéis.

Lema 19.15. *Sejam R um anel e $I, J \subseteq R$ ideais à esquerda (resp. à direita, resp. bilateral).*

(a) $I + J := \{i + j \mid i \in I,\ j \in J\}$ *é um ideal à esquerda (resp. à direita, resp. bilateral) de R.*
(b) $IJ := \{\sum_{k=1}^{n} i_k \cdot j_k \mid n \geq 0,\ i_1, \cdots, i_n \in I,\ j_1, \cdots, j_n \in J\}$ *é um ideal à esquerda (resp. à direita, resp. bilateral) de R. Em particular, $I^n = I \cdots I$ (n vezes) é um ideal à esquerda (resp. à direita, resp. bilateral) de R para todo $n > 0$.*
(c) $(I \cap J)$ *é um ideal à esquerda (resp. à direita, resp. bilateral) de R e $IJ \subseteq (I \cap J)$.*

Demonstração. Vamos provar apenas o caso *à esquerda*, já que o caso *à direita* é análogo e o caso *bilateral* segue dos casos *à esquerda* e *à direita*.

(a) Vamos verificar que $I + J$ satisfaz as condições (i)-(iii) da Definição 17.16 (que é a condição (i) da Definição 19.5) e a condição (ii) da Definição 19.5. Para isso, lembre que I e J são ideais à esquerda de R. Então temos que:
- $(i_1 + j_1) + (i_2 + j_2) = (i_1 + i_2) + (j_1 + j_2) \in (I + J)$ para todos $i_1, i_2 \in I$ e $j_1, j_2 \in J$;
- $-(i + j) = (-i) + (-j) \in (I + J)$ para todos $i \in I$ e $j \in J$;
- $(i_1 + j_1) \cdot (i_2 + j_2) = ((i_1 + j_1) \cdot i_2) + ((i_1 + j_1) \cdot j_2) \in (I + J)$ para todos $i_1, i_2 \in I$ e $j_1, j_2 \in J$;
- $r \cdot (i + j) = (r \cdot i) + (r \cdot j) \in (I + J)$ para todos $r \in R$, $i \in I$ e $j \in J$.

(b) Vamos verificar que IJ satisfaz as condições (i)-(iii) da Definição 17.16 (que é a condição (i) da Definição 19.5) e a condição (ii) da Definição 19.5. Para isso, lembre que I e J são ideais à esquerda de R. Então temos que:
- $(i_1 \cdot j_1) + (i_2 \cdot j_2) \in IJ$ para todos $i_1, i_2 \in I$ e $j_1, j_2 \in J$;
- $-(i \cdot j) = (-i) \cdot j \in IJ$ para todos $i \in I$ e $j \in J$;
- $(i_1 \cdot j_1) \cdot (i_2 \cdot j_2) = ((i_1 \cdot j_1) \cdot i_2) \cdot j_2) \in IJ$ para todos $i_1, i_2 \in I$ e $j_1, j_2 \in J$;
- $r \cdot (i \cdot j) = (r \cdot i) \cdot j \in IJ$ para todos $r \in R$, $i \in I$ e $j \in J$.

(c) Vamos verificar que $I \cap J$ satisfaz as condições (i)-(iii) da Definição 17.16 (que é a condição (i) da Definição 19.5) e a condição (ii) da Definição 19.5. Para isso, lembre que I e J são ideais à esquerda de R. Então temos que:
- Se $r_1, r_2 \in (I \cap J)$, então $r_1, r_2 \in I$ e $r_1, r_2 \in J$. Consequentemente, $(r_1 + r_2) \in I$ e $(r_1 + r_2) \in J$. Portanto $(r_1 + r_2) \in (I \cap J)$.
- Se $r \in (I \cap J)$, então $r \in I$ e $r \in J$. Consequentemente, $-r \in I$ e $-r \in J$. Portanto $-r \in (I \cap J)$.
- Se $r_1, r_2 \in (I \cap J)$, então $r_1, r_2 \in I$ e $r_1, r_2 \in J$. Consequentemente, $r_1 \cdot r_2 \in I$ e $r_1 \cdot r_2 \in J$. Portanto $r_1 \cdot r_2 \in (I \cap J)$;
- Se $s \in (I \cap J)$, então $s \in I$ e $s \in J$. Consequentemente, $r \cdot s \in I$ e $r \cdot s \in J$ para todo $r \in R$. Portanto $r \cdot s \in (I \cap J)$ para todo $r \in R$. □

O próximo resultado é uma versão do Teorema 9.5 (Segundo Teorema de Isomorfismo de grupos), do Teorema 9.6 (Terceiro Teorema de Isomorfismo de grupos) e do Teorema 9.7 para anéis.

Teorema 19.16. *Sejam R um anel e $I \subseteq R$ um ideal bilateral.*

(a) Para todo subanel $S \subseteq R$, temos que $(S + I) = \{s + i \in R \mid s \in S,\ i \in I\} \subseteq R$ é um subanel, $(S \cap I) \subseteq S$ é um ideal bilateral, e existe um isomorfismo de anéis

$$\frac{(S + I)}{I} \cong \frac{S}{(S \cap I)}.$$

(b) Para todo ideal bilateral $J \subseteq R$ tal que $J \subseteq I$, temos que $(I/J) \subseteq (R/J)$ é um ideal bilateral e existe um isomorfismo de anéis

$$\frac{R/J}{I/J} \cong \frac{R}{I}.$$

(c) Existe uma bijeção entre o conjunto de subanéis (resp. ideais bilaterais) de R/I e o conjunto de subanéis (resp. ideais bilaterais) de R que contem I.

Exercício 19.17. Use os isomorfismos explícitos dados nas demonstrações dos Teoremas 9.5, 9.6, 9.7 para demonstrar o Teorema 19.16.

7.4. Propriedades de ideais

Definição 19.18. Seja R um anel não-trivial com identidade.

(a) Dado um subconjunto $X \subseteq R$, o ideal à esquerda (resp. à direita, resp. bilateral) gerado por X é definido como o único ideal $I \subseteq R$ tal que $X \subseteq I$ e, se $J \subseteq R$ é um ideal tal que $X \subseteq J$, então $I \subseteq J$. (Ou seja, o menor ideal de R que contém X). Denote o ideal bilateral de R gerado por X por (X). Quando X for um conjunto finito, $X = \{x_1, \ldots, x_n\}$, denote (X) por $(x_1, \ldots, x_n)$.

Exercício 19.19. Seja R um anel não-trivial com identidade. Mostre que, se $X \subseteq Y \subseteq R$, então $(X) \subseteq (Y)$.

Proposição 19.20. *Sejam R um anel não-trivial com identidade e $X \subseteq R$ um subconjunto.*

(a) O ideal à esquerda (resp. à direita, resp. bilateral) gerado por X é a intersecção de todos os ideais à esquerda (resp. à direita, resp. bilaterais) que contem X.

(b) O ideal à esquerda gerado por X é igual a

$$RX = \{r_1x_1 + \cdots + r_nx_n \mid n > 0,\ r_1, \ldots, r_n \in R, x_1, \ldots, x_n \in X\}.$$

O ideal à direita gerado por X é igual a

$$XR = \{x_1r_1 + \cdots + x_nr_n \mid n > 0,\ r_1, \ldots, r_n \in R, x_1, \ldots, x_n \in X\}.$$

Consequentemente,

$$(X) = RXR = \{r_1x_1s_1 + \cdots + r_nx_ns_n \mid n > 0,\ r_1, s_1, \ldots, r_n, s_n \in R, x_1, \ldots, x_n \in X\}.$$

Demonstração. Vamos provar apenas os casos *à esquerda*, pois os casos *à direita* e *bilateral* são análogos.

(a) Denote por $\mathfrak{I}$ o conjunto formado por todos os ideais à esquerda $I \subseteq R$ que contem X. Como $X \subseteq I$ para todo $I \in \mathfrak{I}$, então $X \subseteq \bigcap_{I\in\mathfrak{I}} I$. Como $\bigcap_{I\in\mathfrak{I}} I$ é um ideal à esquerda (ver Lema 19.15(c)) que contém X, então $\left(\bigcap_{I\in\mathfrak{I}} I\right) \in \mathfrak{I}$. Além disso, se $J \in \mathfrak{I}$, então $\left(\bigcap_{I\in\mathfrak{I}} I\right) \subseteq J$. Isso mostra que $\bigcap_{I\in\mathfrak{I}} I$ é o menor ideal à esquerda de R que contém X, ou seja, $\bigcap_{I\in\mathfrak{I}} I$ é o ideal à esquerda gerado por X.

(b) Primeiro observe que RX é um ideal de R e que, como R tem identidade, então $X \subseteq RX$. Isso mostra que o ideal à esquerda gerado por X está contido em RX. Para mostrar a outra inclusão, observe que, se $I \subseteq R$ for um ideal à esquerda que contém X, então $x_1 \in I$, logo $r_1x_1 \in I$, e portanto $r_1x_1 + \cdots + r_nx_n \in I$ para todos $n > 0$, $r_1, \ldots, r_n \in R$, $x_1, \ldots, x_n \in X$. Isso mostra que $RX \subseteq I$ para todo ideal à esquerda $I \subseteq R$ que contém X. Do item (a), segue que RX está contido no ideal à esquerda gerado por X. □

Observação 19.21. Lembre que, quando R é um anel comutativo com identidade, todo ideal à esquerda é um ideal à direita e bilateral. Portanto, nesse caso, para todo subconjunto $X \subseteq R$, temos que $RX = XR = (X)$.

Exemplo 19.22. Considere o anel $\mathbb{Z}$. Lembre que todo ideal de $\mathbb{Z}$ é da forma $n\mathbb{Z}$ para algum $n \in \mathbb{Z}$.

Exercício 19.23. Considere um anel não-trivial, comutativo, com identidade R e um grupo G. O ideal bilateral gerado por $\{g - 1_R \mid g \in G\}$ é chamado de ideal de aumento de G. Mostre que, se G for um grupo cíclico gerado por σ, então o ideal de aumento de $R[G]$ é gerado por $(\sigma - 1_R)$.

Proposição 19.24. *Sejam R um anel não-trivial com identidade e $I \subseteq R$ um ideal à esquerda (resp. à direita, resp. bilateral).*

(a) $I = R$ se, e somente se, I contém uma unidade de R.
(b) Se R for um anel de divisão, então $I = \{0_R\}$ ou $I = R$.
(c) Se os únicos ideais à esqueda e os únicos ideais à direita de R forem $\{0_R\}$ e R, então R é um anel de divisão.

Demonstração. Vamos provar apenas os casos *à esquerda* dos itens (a) e (b), pois os respectivos casos *à direita* e *bilateral* são análogos.

(a) Se $I = R$, então $1_R \in I$. Logo I contém um a unidade de R. Por outro lado, suponha que I é um ideal à esquerda que contém uma unidade $u \in R^\times$. Como $u \in R^\times$, existe $v \in R$ tal que $vu = 1_R$. Como I é um ideal à esquerda de R, para todo $r \in R$, temos que $r = (rv)u \in I$. Isso mostra que $R = I$.
(b) Se R for um anel de divisão e $I \subseteq R$ for um ideal à esquerda, $I \neq \{0_R\}$, então I contém alguma unidade de R. Pelo item (a), segue que $I = R$.
(c) Dado $r \in R \setminus \{0_R\}$, vamos mostrar que existe $u \in R$ tal que $ur = 1_R = ru$. Como os únicos ideais à esquerda de R são $\{0_R\}$ e R, então $R\{r\} = R$. Em particular, existe $u_1 \in R$ tal que $1_R = u_1 r$. Como os únicos ideais à direita de R são $\{0_R\}$ e R, então $\{r\}R = R$. Em particular, existe $u_2 \in R$ tal que $1_R = ru_2$. Além disso,

$$u_1 = u_1 1_R = u_1(ru_2) = (u_1 r)u_2 = 1_R u_2 = u_2.$$

Isso mostra que $ur = 1_R = ru$ para $u = u_1 = u_2$. □

Exercício 19.25. Considere o anel $M_2(\mathbb{R})$. Lembre que $M_2(\mathbb{R})$ não é um anel de divisão. (De fato, toda matriz $A \in M_2(\mathbb{R})$ tal que $\det(A) = 0$ não admite inversa.)

(a) Mostre que todo ideal $\{0\} \neq I \subseteq M_2(\mathbb{R})$ contém os elementos $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ e $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.
(b) Mostre que o único ideal bilateral $\{0\} \neq I \subseteq M_2(\mathbb{R})$ é $I = M_2(\mathbb{R})$.
(c) Conclua que $M_2(\mathbb{R})$ é um anel (não-comutativo) cujos únicos ideais bilaterais são $\{0\}$ e $M_2(\mathbb{R})$, mas que $M_2(\mathbb{R})$ não é um anel de divisão. Explique por que isso não contradiz a Proposição 19.24(c).

Aula 20

Corolário 20.1. *Se D for um anel de divisão, então todo homomorfismo de anéis $f\colon D \to S$ é trivial ou injetor.*

Demonstração. Se $f\colon D \to S$ é um homomorfismo de anéis, então $\ker(f) \subseteq D$ é um ideal bilateral. Pela Proposição 19.24(b), $\ker(f) = \{0_D\}$ ou $\ker(f) = D$. No primeiro caso, f é injetor, e no segundo caso, f é trivial. □

Definição 20.2. Seja R um anel não-trivial com identidade.

(a) Um ideal à esquerda (resp. à direita, resp. bilateral) $I \subseteq R$ é dito principal quando existe $r \in R$ tal que I é o ideal à esquerda (resp. à direita, resp. bilateral) gerado por $\{r\}$.
(b) Um ideal à esquerda (resp. à direita, resp. bilateral) $I \subseteq R$ é dito finitamente gerado quando existe um subconjunto finito $X \subseteq R$ tal que I é o ideal à esquerda (resp. à direita, resp. bilateral) gerado por X.

Observação 20.3. Observe que todo ideal principal é finitamente gerado, mas que nem todo ideal finitamente gerado é principal. Por exemplo, mostre que $(x, y) \subseteq \mathbb{R}[x, y]$ não é principal. Mas, pela construção, (x, y) é finitamente gerado (por dois elementos).

Exemplo 20.4. Seja R um anel não-trivial com identidade. Lembre que $\{0_R\} \subseteq R$ é um ideal bilateral. Observe que $\{0_R\} = (0_R)$. Portanto $\{0_R\}$ é um ideal principal. Lembre também que $R \subseteq R$ é um ideal bilateral. Além disso, observe que $R = (1_R)$. Portanto R é um ideal principal.

Exemplo 20.5. Considere o anel $\mathbb{Z}$. Lembre que todo ideal de $\mathbb{Z}$ é da forma $n\mathbb{Z}$ para algum $n \in \mathbb{Z}$. Portanto, todo ideal de $\mathbb{Z}$ é principal.

Exemplo 20.6. Considere o anel comutativo $\mathbb{Z}[x]$. Vamos mostrar que o ideal $(2, x) \subseteq \mathbb{Z}[x]$ não é principal. Primeiro, lembre que $\mathbb{Z}[x]$ é um anel comutativo. Pela Proposição 19.20, $(2, x) = \{2p + xq \mid p, q \in \mathbb{Z}[x]\} = \{2n + xr \mid n \in \mathbb{Z},\ r \in \mathbb{Z}[x]\}$. Se $(2, x)$ fosse principal, então existiria $g \in \mathbb{Z}[x]$ tal que $(2, x) = (g)$. Em particular, existiriam $h_1, h_2 \in \mathbb{Z}[x]$ tais que $2 = gh_1$ e $x = gh_2$. Da primeira igualdade, segue que $g \in \mathbb{Z}$ divide 2. Como $1 \notin (2, x) = (g)$, então $g = 2$. Agora, da segunda igualdade, segue que $x = 2h_2$. Isso é um absurdo.

Definição 20.7. Seja R um anel não-trivial com identidade. Um ideal à esquerda (resp. à direita, resp. bilateral) $\mathsf{m} \subseteq R$ é dito maximal quando $\mathsf{m} \neq R$ e os únicos ideais à esquerda (resp. à direita, resp. bilaterais) $I \subseteq R$ tais que $\mathsf{m} \subseteq I$ são $I = \mathsf{m}$ e $I = R$. (Ou seja, m é um dos maiores ideais próprios de R.)

Lembre que um conjunto X é dito parcialmente ordenado quando X é munido de uma relação $\leq$ satisfazendo as seguintes propriedades:

(*i*) $x \leq x$ para todo $x \in X$;
(*ii*) Se $x, y, z \in X$, $x \leq y$ e $y \leq z$, então $x \leq z$;
(*iii*) Se $x, y \in X$, $x \leq y$ e $y \leq x$, então $x = y$.

Lema 20.8 (de Zorn)**.** *Seja $(X, \leq)$ um conjunto parcialmente ordenado não-vazio. Se toda cadeia $x_1 \leq x_2 \leq \cdots \leq x_n \leq \cdots$ admite um elemento máximo (ou seja, se existe um elemento $y \in X$ tal que $x_i \leq y$ para todo $i \in \mathbb{N}$), então X admite um elemento maximal (ou seja, existe $z \in X$ tal que $z \leq x$, somente se $z = x$).*

O Lema de Zorn é equivalente ao Axioma da Escolha e portanto nós não iremos demonstrá-lo. Mas nós vamos usá-lo para provar o próximo resultado.

Proposição 20.9. *Todo anel não-trivial com identidade admite um ideal maximal à esquerda (resp. à direita, resp. bilateral).*

Demonstração. Vamos mostrar apenas o caso *à esquerda*, pois os casos *à direita* e *bilateral* são análogos.

Considere o conjunto $\mathfrak{I}$ formado por todos os ideais à esquerda $I \subseteq R$, $I \neq R$, e considere a ordem parcial em $\mathfrak{I}$ dada da seguinte forma: $I \leq J$, quando $I \subseteq J$. Vamos usar o Lema de Zorn para mostrar que $\mathfrak{I}$ tem algum elemento maximal. Lembre que $\{0_R\} \in \mathfrak{I}$. Em particular, $\mathfrak{I} \neq \emptyset$. Agora considere uma cadeia de ideais $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots \subseteq R$ tal que $I_k \neq R$ para todo $k \in \mathbb{N}$. Vamos mostrar que $\left(\bigcup_{k\in\mathbb{N}} I_k\right) \in \mathfrak{I}$:

- Se $r_1, r_2 \in \bigcup_{k\in\mathbb{N}} I_k$, então existem $k, \ell \in \mathbb{N}$ tais que $r_1 \in I_k$ e $r_2 \in I_\ell$. Consequentemente, $r_1, r_2 \in I_{k+\ell}$. Como $I_{k+\ell}$ é um ideal à esquerda de R, então $r_1 + r_2 \in I_{k+\ell}$. Portanto $r_1 + r_2 \in \bigcup_{k\in\mathbb{N}} I_k$.
- Se $r \in \bigcup_{k\in\mathbb{N}} I_k$, então existe $k \in \mathbb{N}$ tal que $r \in I_k$. Como I_k é um ideal à esquerda de R, então $-r \in I_k$. Portanto $-r \in \bigcup_{k\in\mathbb{N}} I_k$.
- Se $r \in R$ e $i \in \bigcup_{k\in\mathbb{N}} I_k$, então existe $k \in \mathbb{N}$ tal que $i \in I_k$. Como I_k é um ideal à esquerda de R, então $ri \in I_k$. Portanto $ri \in \bigcup_{k\in\mathbb{N}} I_k$. Isso mostra que $\bigcup_{k\in\mathbb{N}} I_k$ é um ideal de R.
- Agora vamos mostrar que $\left(\bigcup_{k\in\mathbb{N}} I_k\right) \neq R$. Como $I_k \neq R$, então $I_k \cap R^\times = \emptyset$ para todo $k \in \mathbb{N}$ (ver Proposição 19.24(b)). Em particular, $1_R \notin I_k$ para todo $k \in \mathbb{N}$. Consequentemente, $1_R \notin \bigcup_{k\in\mathbb{N}} I_k$. Isso mostra que $\left(\bigcup_{k\in\mathbb{N}} I_k\right) \neq R$ e, consequentemente, que $\left(\bigcup_{k\in\mathbb{N}} I_k\right) \in \mathfrak{I}$.

Como toda cadeia ascendente admite um elemento máximo, então, pelo Lema de Zorn, o conjunto $\mathfrak{I}$ admite um elemento maximal. Ou seja, existe um ideal à esquerda maximal. □

Proposição 20.10. *Seja R um anel não-trivial, comutativo e com identidade. Um ideal $\mathsf{m} \subseteq R$ é maximal se, e somente se, R/m é um corpo.*

Demonstração. Pela Proposição 19.24, R/m é um corpo se, e somente se, seus únicos ideais são $\{0_{R/\mathsf{m}}\}$ e R/m. Pelo Teorema 19.16(c), existe uma bijeção entre o conjunto de ideais de R/m e o conjunto de ideais de R que contem m. Através dessa bijeção, $\{0_{R/\mathsf{m}}\}$ corresponde a m e R/m corresponde a R. Por definição, $\mathsf{m} \subseteq R$ é maximal se, e somente se, os únicos ideais de R que contem m são m e R. □

Exemplo 20.11. Considere o anel $\mathbb{Z}$. Lembre que todo ideal de $\mathbb{Z}$ é da forma $n\mathbb{Z}$ para algum $n \in \mathbb{Z}$. Vamos mostrar que $n\mathbb{Z}$ é maximal se, e somente se, n é primo. Primeiro, observe que, se $m \mid n$, então $n\mathbb{Z} \subseteq m\mathbb{Z}$. De fato, como $m \mid n$, então existe $k \in \mathbb{Z}$ tal que $n = mk$. Consequentemente, $nz = m(kz) \in m\mathbb{Z}$ para todo $z \in \mathbb{Z}$. Isso mostra que, se n for um número composto, então $n\mathbb{Z}$ não é maximal. Ou seja, que se $n\mathbb{Z}$ é maximal, então n é primo.

Por outro lado, vamos mostrar que, se $n\mathbb{Z} \subseteq m\mathbb{Z}$, então $m \mid n$. De fato, $n \in m\mathbb{Z}$ somente se $n = mz$ para algum $z \in \mathbb{Z}$. Ou seja, m divide n. Isso mostra que, se p for primo, então $p\mathbb{Z}$ é maximal.

Exemplo 20.12. Considere o anel $\mathbb{Z}[x]$. Vamos mostrar que o ideal $(x) \subseteq \mathbb{Z}[x]$ não é maximal. Uma forma de ver isso é lembrar que $(x) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$. Outra forma de ver isso é mostrar que $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. Considere a função $\mathrm{ev}_0 \colon \mathbb{Z}[x] \to \mathbb{Z}$ dada por $\mathrm{ev}_0(p) = p(0)$. Verifique que ev_0 é um homomorfismo de anéis. Observe que $p = a_0 + \cdots + a_n x^n \in \ker(\mathrm{ev}_0)$ se, e somente se, $a_0 = 0$. Isso mostra que $(x) = \ker(\mathrm{ev}_0)$. Como $z = \mathrm{ev}_0(z)$ para todo $z \in \mathbb{Z}$, então ev_0 é sobrejetor. Do Primeiro Teorema de Isomorfismo de anéis, segue que $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. Como $\mathbb{Z}$ não é um corpo, da Proposição 20.10, segue que (x) não é maximal.

Agora vamos mostrar que $(2, x) \subseteq \mathbb{Z}[x]$ é maximal. Para isso, considere a função $f\colon \mathbb{Z}[x] \to \mathbb{Z}_2$ dada por $f(p) = \overline{p(0)}$. Verifique que f é um homomorfismo de anéis. Observe que $p = a_0 + \cdots + a_n x^n \in \ker(f)$ se, e somente se, $2 \mid a_0$. Isso mostra que $\ker(f) = (2, x)$ (compare com o Exemplo 20.6). Como $\mathbb{Z}_2$ é um corpo (Corolário 17.15), então segue da Proposição 20.10 que $(2, x)$ é maximal.

Exercício 20.13. Mostre que o ideal de aumento em $\mathbb{R}[G]$ é maximal.

Definição 20.14. Dado um anel R não-trivial, comutativo e com identidade, um ideal $P \subseteq R$ é dito primo quando $P \neq R$ e, para todos $a, b \in R$ satisfazendo $ab \in P$, temos $a \in P$ ou $b \in P$.

Exemplo 20.15. Lembre que os ideais de $\mathbb{Z}$ são da forma $n\mathbb{Z}$ para algum $n \in \mathbb{Z}$. Vamos mostrar que $n\mathbb{Z}$ é um ideal primo se, e somente se, n é um número primo. Primeiro observe que, se $n = n_1 n_2$, para alguns $n_1, n_2 \in \mathbb{Z} \setminus \{-1, 0, 1\}$ (ou seja, n é composto), então $n_1 n_2 \in n\mathbb{Z}$, mas $n_1 \notin n\mathbb{Z}$ e $n_2 \notin n\mathbb{Z}$. Por outro lado, se p for primo e $ab \in p\mathbb{Z}$, então $ab = pm$; ou seja, $p \mid ab$. Como p é primo, então $p \mid a$ ou $p \mid b$. Isso mostra que $a \in p\mathbb{Z}$ ou $b \in p\mathbb{Z}$. Portanto, nesse caso, $p\mathbb{Z}$ é um ideal primo.

Proposição 20.16. *Seja R um anel não-trivial, comutativo e com identidade. Um ideal $P \subseteq R$ é primo se, e somente se, R/P é um domínio.*

Demonstração. Suponha que $P \subseteq R$ é um ideal primo e considere $\overline{a}, \overline{b} \in R/P$. Se $\overline{a}\overline{b} = \overline{0}$, então $ab \in P$. Como P é primo, então $a \in P$ ou $b \in P$; ou seja, $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$. Isso mostra que R/P é um domínio. Por outro lado, suponha que R/P é um domínio e considere $a, b \in R$. Se $ab \in P$, então $\overline{ab} = \overline{0}$. Como R/P é um domínio, então $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$; ou seja, $a \in P$ ou $b \in P$. Pela Definição 20.14, isso mostra que P é primo. □

Corolário 20.17. *Se R é um anel não-trivial, comutativo e com identidade, então todo ideal maximal de R é primo.*

Demonstração. Lembre que todo corpo é um domínio. Então o resultado do corolário segue das Proposições 20.10 e 20.16. □

Exemplo 20.18. Lembre do Exemplo 20.12 que (x) é um ideal de $\mathbb{Z}[x]$ tal que $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. Então segue da Proposição 20.16, que (x) é um ideal primo. Mas, pelo que foi mostrado no Exemplo 20.12, (x) não é maximal. De fato, $(x) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$.

7.5. Corpo de frações

Exemplo 20.19. Vamos lembrar como nós construímos o corpo $\mathbb{Q}$ a partir do anel $\mathbb{Z}$. Os elementos de $\mathbb{Q}$ são da forma a/b, onde $a \in \mathbb{Z}$ e $b \in \mathbb{Z} \setminus \{0\}$. Lembre que dois elementos $a/b, c/d \in \mathbb{Q}$ são ditos iguais quando $ad = bc$. Ou seja, na verdade, cada elemento de $\mathbb{Q}$ é uma classe de equivalência.

A soma em $\mathbb{Q}$ é definida a partir da soma $+$ em $\mathbb{Z}$ da seguinte forma:

$$s\colon \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad s(a/b, c/d) = (ad + bc)/(bd).$$

Além disso, a multiplicação em $\mathbb{Q}$ é definida a partir da multiplicação $\cdot$ em $\mathbb{Z}$ da seguinte forma:

$$m\colon \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad m(a/b, c/d) = (a \cdot c)/(b \cdot d).$$

Lembre que essas operações, s e m, são bem definidas, ou seja, não dependem da escolha de representante das classes de equivalência de a/b e c/d.

Lembre ainda que $\mathbb{Z}$ é isomorfo ao subanel $\{z/1 \mid z \in \mathbb{Z}\}$ de $\mathbb{Q}$. Por fim, observe que $\mathbb{Q}$ é o menor corpo que contém um subanel isomorfo a $\mathbb{Z}$. De fato, se $\mathbb{F}$ fosse um corpo e $f\colon \mathbb{Z} \to \mathbb{F}$

fosse um homomorfismo injetor de anéis, então $f(a)f(b)^{-1} \in \mathbb{F}$ para todos $a \in \mathbb{Z}$ e $b \in \mathbb{Z} \setminus \{0\}$. Logo a função $F\colon \mathbb{Q} \to \mathbb{F}$ dada por $F(a/b) = f(a)f(b)^{-1}$ é um homomorfismo injetor de anéis. (Verifique!) Isso mostra que $\mathbb{F}$ contém um subcorpo isomorfo a $\mathbb{Q}$.

Vamos construir um corpo a partir de outros anéis, além de $\mathbb{Z}$. Seja D um domínio (ou seja, um anel não-trivial, comutativo, com identidade e sem divisores de zero). Considere a seguinte relação de equivalência no conjunto $D \times (D \setminus \{0\})$:

$$(a, b) \sim (c, d) \quad \text{se, e somente se,} \quad ad = bc.$$

Denote por $[a, b]$ a classe de equivalência que contém (a, b) e por Q o conjunto formado pelas classes de equivalência $[a, b]$, onde $a \in D$ e $b \in D \setminus \{0\}$.

Defina $s\colon Q \times Q \to Q$ da seguinte forma:

$$s([a, b], [c, d]) = [ad - bc, bd].$$

Observe que s está bem definida. De fato, como D é um domínio e $b, d \neq 0$, então $bd \neq 0$. Além disso, se $a' \in D$ e $b' \in D \setminus \{0\}$ são tais que $ab' = a'b$, então $(a'd - b'c)(bd) = (a'bd^2 - b'bcd) = (ab'd^2 - bb'cd) = (ad - bc)(b'd)$. Portanto $s([a', b'], [c, d]) = [a'd - b'c, b'd] = [ad - bc, bd] = s([a, b], [c, d])$.

Agora defina $m\colon Q \times Q \to Q$ da seguinte forma:

$$m([a, b], [c, d]) = [ac, bd].$$

Observe que m também está bem definida. De fato, como D é um domínio e $b, d \neq 0$, então $bd \neq 0$. Além disso, se $a' \in D$ e $b' \in D \setminus \{0\}$ são tais que $ab' = a'b$, então $(a'c)(bd) = a'bcd = (ab'cd) = (ac)(b'd)$. Portanto $m([a', b'], [c, d]) = [a'c, b'd] = [ac, bd] = m([a, b], [c, d])$.

Exercício 20.20. Mostre que (Q, s, m) é um corpo com $0_Q = [0_D, 1_D]$, $1_Q = [1_D, 1_D]$ e $[a, b]^{-1} = [b, a]$ para todo $a \neq 0_D$.

Aula 21

7.5. Corpo de frações

Dado um domínio D, lembre que nós construímos Q como o conjunto formado pelas classes de equivalência $[a,b]$, onde $a \in D$ e $b \in D \setminus \{0\}$ e

$$[a,b] = [c,d] \quad \text{se, e somente se,} \quad ad = bc.$$

Além disso, nós definimos uma soma $s\colon Q \times Q \to Q$ por:

$$s([a,b],[c,d]) = [ad - bc, bd],$$

e uma multiplicação $m\colon Q \times Q \to Q$ por:

$$m([a,b],[c,d]) = [ac, bd].$$

Definição 21.1. Dado um domínio D, o corpo (Q,s,m) é chamado de corpo de frações de D.

Lema 21.2. *Sejam R, S anéis com identidade e $f\colon R \to S$ um homomorfismo não-trivial de anéis. Se $f(1_R) \in S$ não for um divisor de zero, então $f(1_R) = 1_S$.*

Demonstração. Denote $f(1_R)$ por s. Vamos mostrar que $s = 1_S$. Como f é um homomorfismo de anéis, então $s = f(1_R) = f(1_R \cdot 1_R) = s^2$. Consequentemente, $s \cdot (s - 1_S) = 0_S$. Como s não é um divisor de zero, então $s = 0_S$ ou $s = 1_S$. Como f seria trivial se $s = 0_S$, então $s = 1_S$. □

Exercício 21.3. Mostre que existe um único homomorfismo de anéis $f\colon \mathbb{Z} \to \mathbb{Z}_6$ satisfazendo $f(1) = \overline{3}$.

Teorema 21.4. *Seja R um domínio e denote por Q seu corpo de frações.*

(a) A função $\iota_R\colon R \to Q$ dada por $\iota_R(r) = [r, 1_R]$ é um homomorfismo injetor de anéis.
(b) Para todo anel comutativo com identidade S e todo homomorfismo de anéis $f\colon R \to S$ tal que $f(r) \in S^\times$ para todo $r \in R \setminus \{0\}$, existe um homomorfismo injetor de anéis $F\colon Q \to S$ tal que $f = F \circ \iota_R$.
(c) Se $\mathbb{F}$ for um corpo que contém um subanel isomorfo a R, então existe um subcorpo de $\mathbb{F}$ isomorfo a Q.

Demonstração. (a) Primeiro vamos mostrar que ι_R é um homomorfismo de anéis. Para quaisquer $a, b \in R$, temos:

- $\iota_R(a+b) = [a+b, 1_R] = s([a,1_R],[b,1_R]) = s(\iota_R(a), \iota_R(b))$.
- $\iota_R(a \cdot b) = [a \cdot b, 1_R] = m([a,1_R],[b,1_R]) = m(\iota_R(a), \iota_R(b))$.

Agora vamos verificar que ι_R é injetor, calculando seu núcleo:

$$\ker(\iota_R) = \{r \in R \mid \iota_R(r) = [r,1_R] = 0_Q\} = \{r \in R \mid [r,1_R] = [0_R,1_R]\} = \{0_R\}.$$

(b) Defina a função $F\colon Q \to S$ da seguinte forma $F([a,b]) = f(a)f(b)^{-1}$. Vamos verificar, primeiro, que F está bem definida. Como $b \in R \setminus \{0\}$, então $f(b) \in S^\times$ por hipótese. Além disso, se $[a,b] = [c,d]$, ou seja, se $ad = bc$, então

$$\begin{aligned} F([a,b]) &= f(a)f(b)^{-1} \\ &= f(a)f(d)f(b)^{-1}f(d)^{-1} \\ &= f(ad)f(b)^{-1}f(d)^{-1} \\ &= f(bc)f(b)^{-1}f(d)^{-1} \\ &= f(c)f(d)^{-1} \\ &= F([c,d]). \end{aligned}$$

Isso mostra que F está bem definida. Além disso, por definição $F \circ \iota_R(r) = F([r, 1_R]) = f(r)f(1_R)^{-1}$. Como Q é um corpo e f é não-trivial, pelo Lema 21.2, $f(1_R) = 1_Q$. Como $1_Q^{-1} = 1_Q$, concluímos que $F \circ \iota_R(r) = f(r)$ para todo $r \in R$. Por fim, observe que, como f é não-trivial e $F[r, 1_R] = f(r)$ para todo $r \in R$, então F é não-trivial. Como o domínio de F é Q, um corpo, e $\ker(F) \subseteq Q$ é um ideal, então $\ker(F) = Q$ ou $\ker(F) = \{0_Q\}$. No primeiro caso, F seria trivial. Isso mostra que $\ker(F) = \{0_Q\}$, ou seja, F é injetor.

(c) Se $\mathbb{F}$ tem um subanel S isomorfo a R, então existe um homomorfismo injetor de anéis $\phi\colon R \to \mathbb{F}$, cuja imagem é S. Como $\mathbb{F}$ é um corpo e ϕ é injetor, então $\phi(r) \in \mathbb{F}^\times$ para todo $r \in R \setminus \{0_R\}$. Pelo item (b), existe um homomorfismo injetor de anéis $\varphi\colon Q \to \mathbb{F}$ tal que $\phi = \varphi \circ \iota_R$. Portanto $\mathrm{im}(\varphi) \subseteq \mathbb{F}$ é um subcorpo isomorfo a Q. □

Exemplo 21.5. Considere o anel de polinômios com coeficientes reais, $\mathbb{R}[x]$. Lembre que, como $\mathbb{R}$ é um domínio (de fato, é um corpo), então $\mathbb{R}[x]$ é um domínio. Como conjunto, o corpo de frações de $\mathbb{R}[x]$ pode ser representado por

$$\left\{ \frac{p}{q} \mid p \in \mathbb{R}[x],\ q \in \mathbb{R}[x] \setminus \{0\} \right\}.$$

Usando essa notação, a soma e a multiplicação no corpo de frações de $\mathbb{R}[x]$ são dadas por:

$$s\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) = \frac{p_1q_2 + q_1p_2}{q_1q_2} \quad \text{e} \quad m\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) = \frac{p_1p_2}{q_1q_2}.$$

Em geral, o corpo de frações de $\mathbb{R}[x]$ é denotado por $\mathbb{R}(x)$.

Exemplo 21.6. Considere o anel $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ do Exemplo 17.12 e denote seu corpo de frações por Q. Vamos mostrar que $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ do Exemplo 17.13 é isomorfo a Q. Primeiro lembre do Exemplo 17.13 que $\mathbb{Q}(\sqrt{2})$ é um corpo. Além disso, observe que a função $f\colon \mathbb{Z}[\sqrt{2}] \to \mathbb{Q}(\sqrt{2})$ dada por $f(a + b\sqrt{2}) = a + b\sqrt{2}$ é um homomorfismo injetor de anéis. Pelo Teorema 21.4, a função $F\colon Q \to \mathbb{Q}(\sqrt{2})$ dada por

$$F[a + b\sqrt{2}, c + d\sqrt{2}] = f(a + b\sqrt{2})f(c + d\sqrt{2})^{-1} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2}$$

é um homomorfismo injetor de anéis. Vamos verificar que F é sobrejetor. Dados quaisquer $a = \frac{p_a}{q_a}$, $b = \frac{p_b}{q_b} \in \mathbb{Q}$, temos que

$$F[(p_aq_b) + (p_bq_a)\sqrt{2},\ q_aq_b] = \frac{(p_aq_b) + (p_bq_a)\sqrt{2}}{q_aq_b} = \frac{p_a}{q_a} + \frac{p_b}{q_b}\sqrt{2} = a + b\sqrt{2}.$$

Isso mostra que F é um isomorfismo de anéis entre Q e $\mathbb{Q}(\sqrt{2})$.

Exercício 21.7. Se R for um corpo, mostre que o corpo de frações de R é o próprio R.

7.3. Teorema chinês dos restos

Exercício 21.8. Sejam $n > 0$ e $(R_1, s_1, m_1), \ldots, (R_n, s_n, m_n)$ anéis. Considere o conjunto $R = (R_1 \times \cdots \times R_n)$ e as seguintes operações binárias

$$\begin{aligned} s\colon (R_1 \times \cdots \times R_n) \times (R_1 \times \cdots \times R_n) &\longrightarrow (R_1 \times \cdots \times R_n) \\ ((a_1, \ldots, a_n), (b_1, \ldots, b_n)) &\longmapsto (s_1(a_1, b_1), \ldots, s_n(a_n, b_n)), \\ m\colon (R_1 \times \cdots \times R_n) \times (R_1 \times \cdots \times R_n) &\longrightarrow (R_1 \times \cdots \times R_n) \\ ((a_1, \ldots, a_n), (b_1, \ldots, b_n)) &\longmapsto (m_1(a_1, b_1), \ldots, m_n(a_n, b_n)). \end{aligned}$$

Mostre que (R, s, m) é um anel. Esse anel é chamado de produto direto dos anéis $R_1, \ldots, R_n$.

Definição 21.9. Dado R um anel não-trivial, comutativo e com identidade, dois ideais $I, J \subseteq R$ são ditos comaximais quando $I + J = R$.

Exemplo 21.10. Lembre que todo ideal do anel $\mathbb{Z}$ é da forma $n\mathbb{Z}$ para algum $n \in \mathbb{Z}$. Em particular, lembre do Exemplo **??** que $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$ onde $d = \mathrm{mdc}(n, m)$. Então dois ideais $n\mathbb{Z}, m\mathbb{Z} \subseteq \mathbb{Z}$ são comaximais se, e somente se, n, m são coprimos. Em particular, observe que, se $p, q \in \mathbb{Z}$ são primos distintos, então $p^k\mathbb{Z}$ e $q^\ell\mathbb{Z}$ são comaximais para todos $k, \ell > 0$.

Exemplo 21.11. Considere o anel $\mathbb{R}[x]$ e dois pontos distintos $a, b \in \mathbb{R}$. Vamos verificar que os ideais $(x-a), (x-b) \subseteq \mathbb{R}[x]$ são comaximais. Para isso, observe que, para todo $p \in \mathbb{R}[x]$,

$$\frac{p}{b-a}(x-a) + \frac{p}{a-b}(x-b) = p\left(\frac{x-a}{b-a} - \frac{x-b}{b-a}\right) = p$$

pertence ao ideal $(x-a) + (x-b)$. Isso mostra que $(x-a) + (x-b) = \mathbb{R}[x]$

Teorema 21.12 (Chinês dos Restos)**.** *Sejam R um anel não-trivial, comutativo, com identidade, e $I_1, \ldots, I_n \subseteq R$ ideais. A função $f\colon R \to R/I_1 \times \cdots \times R/I_n$ dada por*

$$f(r) = (r + I_1, \ldots, r + I_n), \quad r \in R,$$

é um homomorfismo de anéis com núcleo $I_1 \cap \cdots \cap I_n$. Se I_k, I_ℓ forem comaximais para todos $k, \ell \in \{1, \ldots, n\}$, então f é sobrejetor e $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$. Neste caso, existe um isomorfismo de anéis

$$R/(I_1 \cdots I_n) \cong (R/I_1) \times \cdots \times (R/I_n)\,.$$

Demonstração. Primeiro, vamos mostrar que f é um homomorfismo de anéis. Dados $a, b \in R$, temos:

$$\begin{aligned} f(a+b) &= ((a+b) + I_1, \ldots, (a+b) + I_n) \\ &= (a + I_1, \ldots, a + I_n) + (b + I_1, \ldots, b + I_n) \\ &= f(a) + f(b), \\ f(a \cdot b) &= ((a \cdot b) + I_1, \ldots, (a \cdot b) + I_n) \\ &= (a + I_1, \ldots, a + I_n) \cdot (b + I_1, \ldots, b + I_n) \\ &= f(a) \cdot f(b). \end{aligned}$$

Agora vamos calcular o núcleo de f.

$$\begin{aligned} \ker(f) &= \{r \in R \mid f(r) = (r + I_1, \ldots, r + I_n) = (0 + I_1, \ldots, 0 + I_n)\} \\ &= \{r \in R \mid r \in I_1, \ \ldots, \ r \in I_n\} \\ &= I_1 \cap \cdots \cap I_n. \end{aligned}$$

Agora suponha que I_k, I_ℓ sejam comaximais para todos $k, \ell \in \{1, \ldots, n\}$. Fixe $k \in \{1, \ldots, n\}$. Para cada $\ell \in \{1, \ldots, n\} \setminus \{k\}$, existem $x_\ell \in I_k$ e $y_\ell \in I_\ell$ tais que $x_\ell + y_\ell = 1_R$. Consequentemente $(x_1+y_1)\cdots(x_{k-1}+y_{k-1})(x_{k+1}+y_{k+1})\cdots(x_n+y_n) = 1_R \cdots 1_R = 1_R$. Usando a distributividade, vemos que

$$1_R = (x_1 + y_1)\cdots(x_{k-1} + y_{k-1})(x_{k+1} + y_{k+1})\cdots(x_n + y_n) \in I_k + (I_1 \cdots I_{k-1} I_{k+1} \cdots I_n).$$

Isso mostra que I_k e $(I_1 \cdots I_{k-1} I_{k+1} \cdots I_n)$ também são comaximais. Em particular, para cada $k \in \{1, \ldots, n\}$, podemos escolher $i_k \in I_k$ e $j_k \in (I_1 \cdots I_{k-1} I_{k+1} \cdots I_n)$ tais que $i_k + j_k = 1_R$.

Vamos usar os elementos i_k, j_k para mostrar que f é sobrejetora (no caso em que I_k, I_ℓ são comaximais para todos $k, \ell \in \{1, \ldots, n\}$). Dado $y \in (R/I_1) \times \cdots \times (R/I_n)$, escolha $r_1, \ldots, r_n \in R$ tais que $(r_1 + I_1, \ldots, r_n + I_n) = y$. Como $r_k j_k \in (I_1 \cdots I_{k-1} I_{k+1} \cdots I_n)$ e $r_k = r_k j_k + r_k i_k \in (r_k j_k + I_k)$, então

$$f(r_k j_k) = (0 + I_1, \ \ldots, \ 0 + I_{k-1}, \ r_k + I_k, \ 0 + I_{k+1}, \ \ldots, \ 0 + I_n) \quad \text{para todo } k \in \{1, \ldots, n\}.$$

Consequentemente, $f(r_1 j_1 + \cdots + r_n j_n) = y$.

Agora vamos usar indução em n para mostrar que $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$, se I_k, I_ℓ são comaximais para todos $k, \ell \in \{1, \ldots, n\}$. Primeiro, observe que $I_1 \cdots I_n \subseteq I_1 \cap \cdots \cap I_n$. Então basta mostrar que $I_1 \cap \cdots \cap I_n \subseteq I_1 \cdots I_n$. O caso $n = 1$ é óbvio. Então suponha (por hipótese de indução) que $I_2 \cap \cdots \cap I_n = I_2 \cdots I_n$ e tome $r \in (I_1 \cap I_2 \cap \cdots \cap I_n) = I_1 \cap (I_2 \cdots I_n)$. Como $i_1 + j_1 = 1_R$, então $r = ri_1 + rj_1 \in I_1 I_2 \cdots I_n$. Isso mostra que $I_1 \cap \cdots \cap I_n \subseteq I_1 \cdots I_n$.

O isomorfismo $R/(I_1 \cdots I_n) \cong (R/I_1) \times \cdots \times (R/I_n)$ segue do Primeiro Teorema de Isomorfismo de anéis, do fato de f ser sobrejetor e do fato de $\ker(f) = (I_1 \cap \cdots \cap I_n) = (I_1 \cdots I_n)$. □

Corolário 21.13. *Seja $m \in \mathbb{Z}$ com decomposição primária $m = p_1^{k_1} \cdots p_n^{k_n}$. Então existe um isomorfismo de anéis*

$$\mathbb{Z}/n\mathbb{Z} \cong \left(\mathbb{Z}/p_1^{k_1}\mathbb{Z}\right) \times \cdots \times \left(\mathbb{Z}/p_n^{k_n}\mathbb{Z}\right).$$

Demonstração. Pelo Exemplo 21.10, $p_i^{k_i}\mathbb{Z}$ e $p_j^{k_j}\mathbb{Z}$ são comaximais para quaisquer $i, j \in \{1, \ldots, n\}$. O resultado segue do Teorema Chinês dos Restos 21.12. □