NOTAS DE AULA DE ELEMENTOS 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 19/dez.

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/elementos_algebra, e ela vai conter a ementa da disciplina, fotos das aulas 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

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

Aula 3

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:

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

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

Os termos da forma $(i\ \sigma(i)\ \ldots\ \sigma^p(i))$ 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 $\sigma = \mathrm{id}_{\{1,\ldots,n\}}$, então nós teríamos $\sigma = (n)(n-1)\ldots(2)(1)$, e nesse caso, nós denotamos σ simplesmente por (1).

Exemplo 3.1. 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 3.2. 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 3.3. Mostre que $|S_n| = n!$ e que a ordem de todo p-ciclo é p.

Exercício 3.4. 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:

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

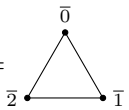
Observe que $\mathbb{H}$ é um grupo finito, $|\mathbb{H}| = 8$, e que não é abeliano. Observe também que $o(1) = 1$, $o(-1) = 2$ e $o(\pm i) = o(\pm j) = o(\pm k) = 4$.

1.2. Grupos diedrais

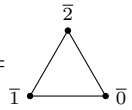
Para cada $n > 2$, denote por D_{2n} o conjunto formado por todas as simetrias de um n-ágono regular Δ_n (movimentos rígidos no espaço, ou seja, composições de translações, rotações e reflexões, que preservam Δ_n). Como toda simetria de Δ_n é uma função $f\colon \Delta_n \to \Delta_n$, defina a operação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

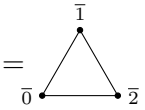
Exemplo 3.5. Considere o grupo D_6 de simetrias de um triângulo equilátero Δ_3. Para descrever as simetrias de Δ_3, vamos enumerar seus vértices com inteiros módulo 3:

$\Delta_3 =$ 

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:

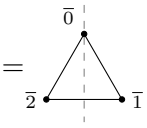
$r\,(\Delta_3)\ =$ 

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,

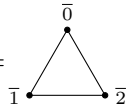
$r^2\,(\Delta_3)\ =$ 

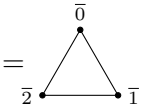
e que r^3 é a rotação de um ângulo de 2π, ou seja, $r^3 = \mathrm{id}_{\Delta_3}$. Com isso, concluímos que $o(r) = 3$.

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 $i \in \{1, \dots, n\}$, 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 $\mathrm{id}_{\Delta_n}, r, \dots, r^{n-1}$ são todas simetrias distintas. Verifique também que $o(s) = 2$ e que, para cada $i \in \{1, \dots, n\}$, 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 $\mathrm{id}_{\Delta_n}, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}$ 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

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

Exercício 3.6. Escreva o elemento $rsrsrsrs$ em termos de $\mathrm{id}_{\Delta_n}, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}$.

Aula 4

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

Exemplo 4.2. Uma presentação de $(\mathbb{Z}, +)$ é $\langle 1 \mid \emptyset \rangle$, ou simplesmente $\langle 1 \rangle$.

Exemplo 4.3. Uma presentação de $\mathbb{Z}_n$ é $\langle \overline{1} \mid n\overline{1} = \overline{0} \rangle$.

Exemplo 4.4. Uma presentação de $\mathbb{H} = Q_8$ é $\langle i, j \mid i^4 = 1, i^2 = j^2, iji = j \rangle$.

Exemplo 4.5. Uma presentação de S_n é

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

1.6. Homomorfismos e isomorfimos

Definição 4.6. 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:

(i) $f(m_G(g_1, g_2)) = m_H(f(g_1), f(g_2))$ para todos $g_1, g_2 \in G$,
(ii) $f(e_G) = e_H$.

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 4.7. *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, $f(g^{-1}) = f(g)^{-1}$ 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 $g \in G$. Se $n = 0$, então $f(g^0) = f(e_G) = e_H = f(g)^0$. 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 $n \geq 0$. 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 4.8. 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 4.9. 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 4.10. 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 4.11. 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 4.12. 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 4.13. 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 4.14. 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 4.15. 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.

Aula 5

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

1.7. Ações de grupos

Definição 5.1. 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 5.2. 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 5.3. 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 5.4. 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 5.5. 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 5.6. *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

$$\alpha_\phi(g_1, \alpha_\phi(g_2, x)) = \phi(g_1)(\phi(g_2)(x)) = (\phi(g_1) \circ \phi(g_2))(x) = \phi(g_1g_2)(x) = \alpha_\phi(g_1g_2, x)$$

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 5.7. *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 5.6(a), $\varphi_\alpha\colon H \to S_X$ é um homomorfismo de grupos dado por $\varphi_\alpha(h) = \alpha(h, -)$. Pelo Exercício 4.8(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 5.6(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 5.8. 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 5.9. Seja $n \geq 3$. Lembre do Exemplo 5.3 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 4.12 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 $\alpha_{(\varphi_\alpha \circ \vartheta)}$.

2.1. Definição e examplos de subgrupos

Definição 5.10. 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 5.11. 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 5.12. O grupo multiplicativo $(\mathbb{R} \setminus \{0\}, \cdot)$ **não** é um subgrupo do grupo aditivo $(\mathbb{R}, +)$. De fato, pela Definição 5.10, 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 5.13. 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 5.14. Dado qualquer grupo G, os subconjuntos $\{e_G\}$ e G são subgrupos de G.

Exemplo 5.15. Considere o grupo aditivo $\mathbb{Z}$. Vamos descrever todos os subgrupos $H \subseteq \mathbb{Z}$. Primeiro, temos pelo Exemplo 5.14 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 5.16. 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 5.17. 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 $\mathbb{Z}_2$.

Aula 6

Proposição 6.1. *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 5.10, 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 6.2. 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 6.3. *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 6.4. 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 6.5. 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 6.6. *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 6.7. *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 $g_1 g_2^{-1} \in \ker(f)$. (De fato, $f(g_1 g_2^{-1}) = f(g_1)f(g_2^{-1}) = f(g_1)f(g_2)^{-1} = f(g_1)f(g_1)^{-1} = e_G$.) Se $\ker(f) = \{e_G\}$, então $g_1 g_2^{-1} = e_G$, ou seja, $g_1 = g_2$. Isso mostra que f é injetora. □

Exercício 6.8. 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.

Definição 6.9. 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 6.10. *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 6.9 que $\ker(\alpha) = \bigcap_{x \in X} G_x$. Do Lema 6.3 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 6.3, 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. □

Aula 7

2.3. Grupos e subgrupos cíclicos

Definição 7.1. 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 7.2. *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 7.3. O grupo trivial é cíclico. De fato, $\langle e \rangle = \{e\}$.

Exemplo 7.4. 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 7.5. 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 7.6. Considere o grupo S_3. Se S_3 fosse cíclico, pelo Lema 7.2, S_3 seria abeliano. Mas no Exemplo 3.2 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 7.7. 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 7.8. *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 7.8 (parte $o(g)$ finita).

Corolário 7.9. *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 7.10. *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 7.8, 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 7.8, 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 7.11. *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 $o(g^k) = \frac{n}{\mathrm{mdc}(n,k)}$ 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 $n = \mathrm{mdc}(n,k)n'$, $k = \mathrm{mdc}(n,k)k'$. Queremos mostrar que $o(g^k) = n'$. Observe que, para cada $\ell \in \mathbb{Z}$, temos:

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

Como $o(g) = n$, segue do Corolário 7.9 que $(g^k)^\ell = e$ se, e somente se, $n \mid \mathrm{mdc}(k,n)(k'\ell)$, ou seja, $n' \mid k'\ell$. Como n' e k' não tem fatores em comum (se tivessem, eles seriam fatores do $\mathrm{mdc}(n,k)$), 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 7.12. *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 7.8, 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 7.11(b), $o(g^k) = o(g)$ se, e somente se, k é coprimo com n. Isso termina a demonstração. □

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

$$\langle X \rangle = \{(x_1)^{\epsilon_1}(x_2)^{\epsilon_2} \cdots (x_n)^{\epsilon_n} \mid n \geq 0, x_1, \ldots, x_n \in X, \epsilon_1, \ldots, \epsilon_n \in \{-1, 1\}\}.$$

Observe que, quando escolhemos $n = 0$ acima, obtemos $(x_1)^{\epsilon_1}(x_2)^{\epsilon_2} \cdots (x_n)^{\epsilon_n} = e_G$. 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 7.1).

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 6.3).

Proposição 7.14. *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 $(x_1)^{\epsilon_1}(x_2)^{\epsilon_2} \cdots (x_n)^{\epsilon_n} \in H$ para todos $n \geq 0$, $x_1, \ldots, x_n \in X$, $\epsilon_1, \ldots, \epsilon_n \in \{-1, 1\}$ 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 $\epsilon_1 = 1$). Agora observe que

$$(x_1)^{\epsilon_1}(x_2)^{\epsilon_2} \cdots (x_n)^{\epsilon_n}(y_1)^{\eta_1}(y_2)^{\eta_2} \cdots (y_m)^{\eta_m} \in \langle X \rangle$$

para todos $n, m \geq 0$, $x_1, \ldots, x_n, y_1, \ldots, y_m \in X$ e $\epsilon_1, \ldots, \epsilon_n, \eta_1, \ldots, \eta_m \in \{-1, 1\}$. Finalmente, observe que $((x_1)^{\epsilon_1}(x_2)^{\epsilon_2} \cdots (x_n)^{\epsilon_n})^{-1} = (x_n)^{-\epsilon_1} \cdots (x_2)^{-\epsilon_2}(x_1)^{-\epsilon_1} \in \langle X \rangle$ para todos $n \geq 0$, $x_1, \ldots, x_n \in X$ e $\epsilon_1, \ldots, \epsilon_n \in \{-1, 1\}$. 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 7.15. Lembre que $D_{2n} = \langle r, s \rangle$ para todo $n \geq 3$.

Exercício 7.16. Verifique que $S_n = \langle (1\ 2), (1\ 2\ \ldots\ n) \rangle$ para todo $n \geq 2$.

Exercício 7.17. 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 7.18. 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

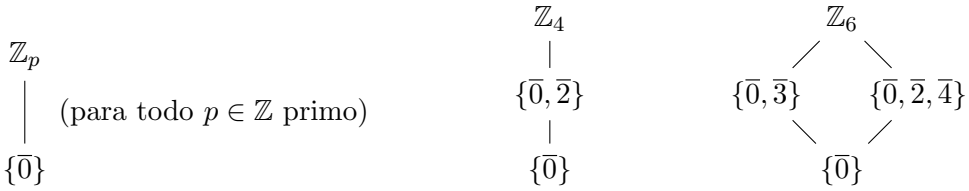
$$\tilde{X}_i = \{(x_1, \ldots, x_n) \in (G_1 \times \cdots \times G_n) \mid x_i \in X_i \text{ e } x_j = e_{G_j} \text{ para todo } j \neq i\}.$$

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 $H_1 \subsetneq H \subsetneq H_2$.

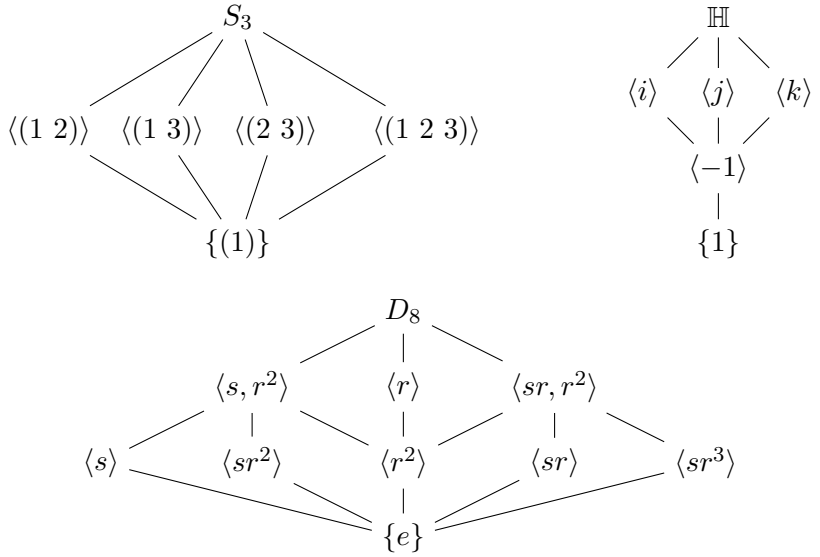
Exemplo 7.19. Pelos Lemas 7.8 e 7.11(b), podemos desenhar os retiiculados de subgrupos de $\mathbb{Z}_n$ para todo $n \geq 2$. Em particular, temos:



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

Exercício 7.20. 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.



Aula 8

3.1. Grupos quocientes e homomorfismos: Definições e exemplos

Vamos começar analisando um exemplo que nós já conhecemos.

Exemplo 8.1. Considere os grupos $\mathbb{Z}$ e $\mathbb{Z}_n$ ($n \geq 2$). Lembre do Exemplo 4.14 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 8.2. *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) $m(\overline{e_G}, \overline{g}) = \overline{(e_G g)} = \overline{g} = \overline{(g e_G)} = m(\overline{g}, \overline{e_G})$ 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 8.3. 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 $K(1\ 3) \neq (1\ 3)K$.

Proposição 8.4. *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 $g_1 g_2 \in G$ e $n_1, n_2 \in N$. Pela definição de m, temos que $\overline{g_1 g_2} = m(\overline{g_1}, \overline{g_2}) = m(\overline{g_1 n_1}, \overline{g_2 n_2}) = \overline{g_1 n_1 g_2 n_2}$ se, e somente se, $(g_1 g_2)^{-1}(g_1 n_1 g_2 n_2) \in N$. Como $n_2 \in N$ e N é um subgrupo de G, temos que:

$$m(\overline{g_1}, \overline{g_2}) = m(\overline{g_1 n_1}, \overline{g_2 n_2}) \quad \text{se, e somente se,} \quad g_2^{-1} n_1 g_2 \in N. \tag{8.1}$$

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, $g_2^{-1} n_1 g_2 \in N$. Daí segue que m está bem definida. Por outro lado, se $m(\overline{g_1}, \overline{g_2}) = m(\overline{g_1 n_1}, \overline{g_2 n_2})$ para todos $g_1, g_2 \in G$, $n_1, n_2 \in N$, então segue da equação (8.1) que $gN = Ng$ para todo $g \in G$ (tome $g_1 = e_G$, $g_2 = g^{-1}$ e varie $n_1 \in N$).

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, $f(g_1 g_2) = \overline{g_1 g_2} = m(\overline{g_1}, \overline{g_2}) = m(f(g_1), f(g_2))$. 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 8.5. Dado um grupo G, um subgrupo $N \subseteq G$ é dito normal quando $gN = Ng$ para todo $g \in G$.

Pela Proposição 8.4(a), $N \subseteq G$ é um subgrupo normal se, e somente se, $(G/N, m)$ for um grupo. Pelo Lema 8.2, 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 8.4(b) que todo subgrupo normal de G é o núcleo de um homomorfismo de grupos.

Exercício 8.6. 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, $N_G(N) = G$.

Exemplo 8.7. Para todo grupo G, verifique que o subgrupo trivial $\{e\} \subseteq G$ é um subgrupo normal e que $G/\{e\} \cong G$.

Exemplo 8.8. Para todo grupo G, verifique que $G \subseteq G$ é um subgrupo normal e que G/G é isomorfo ao grupo trivial.

Exemplo 8.9. 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 8.10. 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 8.11. Considere o grupo S_3. Explique por que $\langle(1\ 2)\rangle \subseteq S_3$ não é um subgrupo normal. (Lembre do Exemplo 8.3 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 8.12. 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.

Aula 9

3.2. Mais sobre classes laterais e Teorema de Lagrange

Definição 9.1. 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 9.2. *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 9.3. *Se G for um grupo finito, então $o(g)$ divide $|G|$ para todo $g \in G$. Em particular, $g^{|G|} = e_G$.*

Corolário 9.4. *Se $|G|$ for um número primo, então G é cíclico e $G \cong \mathbb{Z}_{|G|}$.*

Corolário 9.5. *Dados $a, p \in \mathbb{Z}$, se p for primo, então p divide $a^{p+1} - a$.*

Exemplo 9.6. 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 9.7. 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 $o(\sigma) = \mathrm{mmc}(p_1, \ldots, p_\ell)$. 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.

3.3. Teoremas de isomorfismo

O primeiro Teorema de Isomorfismo de grupos é o seguinte.

Teorema 9.8. *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 8.2 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 9.9. Dados um grupo G e subgrupos $H, K \subseteq G$, defina

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

Proposição 9.10. *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 9.11. 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 9.12. *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 $H/(H \cap K) = H/\ker(f) \cong \mathrm{im}(f) = HK/K$. □

Aula 10

3.3. Teoremas de isomorfismo

O terceiro Teorema de Isomorfismo de grupos é o seguinte.

Teorema 10.1. *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 $f(\overline{gh}) = \overline{\overline{gh}} = \overline{\overline{g}\,\overline{h}} = \overline{\overline{g}} = f(\overline{g})$, 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 10.2. *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:

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

Observação 10.3. 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, $N \subseteq \ker(F)$.

Aula 11

7.1. Introdução a anéis: definições e exemplos básicos

Definição 11.1. 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 11.2. 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 11.3. 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 11.4. 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 11.5. 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 11.6. 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 11.7. *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 11.8. 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 11.9. 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 7.12(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 11.10. 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 7.12(b) que $\mathbb{Z}_8^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$.

Exercício 11.11. Mostre que o anel $\mathbb{Z}_p$ é um corpo se, e somente se, p é primo.

Aula 12

7.1. Introdução a anéis: definições e exemplos básicos

Exemplo 12.1. 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 12.2. 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 12.3. *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 11.1(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 11.1, 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 12.4. *Todo domínio finito é um corpo.*

Demonstração. Suponha que D é um domínio e que $|D|$ é finita. Lembre que, pela Definição 11.8, 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 12.3(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 12.3(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 12.5. 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 12.6. 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 12.7. 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 12.5. 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 12.8. Considere o anel $\mathbb{Z}[\sqrt{2}]$ (do Exemplo 12.1) e o corpo $\mathbb{Q}(\sqrt{2})$ (do Exemplo 12.2). 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 11.4), segue que $\mathbb{Q}(\sqrt{2})$ é um subcorpo de $\mathbb{R}$.

Exercício 12.9. Considere os conjuntos dos números racionais ($\mathbb{Q}$), reais ($\mathbb{R}$) e complexos ($\mathbb{C}$) munidos de suas respectivas somas e multiplicações usuais. Mostre que $\mathbb{Q}$ é um subanel (subcorpo) de $\mathbb{R}$ e que $\mathbb{R}$ é um subanel (subcorpo) de $\mathbb{C}$.

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 12.10. 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.

Aula 13

Proposição 13.1. *Seja R um anel comutativo com identidade.*

(a) Se R for um domínio, então $\operatorname{grau}(p\cdot q) = \operatorname{grau}(p)+\operatorname{grau}(q)$ *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 $p = a_0+\cdots+a_n\bigstar^n \in R[\bigstar]$, $n = \operatorname{grau}(p)$, $q = b_0+\cdots+b_m\bigstar^m \in R[\bigstar]$ e $m = \operatorname{grau}(q)$. Por definição, $p\cdot q = (a_0b_0)+\cdots+(a_nb_m)\bigstar^{n+m}$. Como $\operatorname{grau}(p) = n$ (resp. $\operatorname{grau}(q) = m$), então $a_n \neq 0$ (resp. $b_m \neq 0$). Como R é um domínio, $a_nb_m \neq 0$, o que implica que $\operatorname{grau}(p\cdot q) = m+n$.

(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), $\operatorname{grau}(p)+\operatorname{grau}(q) = \operatorname{grau}(p\cdot q) = \operatorname{grau}(1) = 0$ se, e somente se, $\operatorname{grau}(p) = \operatorname{grau}(q) = 0$. 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 $\operatorname{grau}(p\cdot q) = \operatorname{grau}(p)+\operatorname{grau}(q)$ 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 12.5. 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 $c_k = \sum_{i=\max\{0,k-m\}}^{\min\{n,k\}} a_ib_{k-i} \in S$ 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:

$$s(a_1+b_1i+c_1j+d_1k,\ a_2+b_2i+c_2j+d_2k) = (a_1+a_2)+(b_1+b_2)i+(c_1+c_2)j+(d_1+d_2)k.$$

Exercício 13.2. 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 13.3. 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 13.4. 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 $i,j,k,\ell\in\{1,\dots,n\}$:

$$m(E_{i,j},E_{k,\ell})=E_{i,\ell},\quad \text{se } j=k \qquad \text{e} \qquad m(E_{i,j},E_{k,\ell})=0_{M_n(R)},\quad \text{se } j\neq k. \tag{13.2}$$

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 (13.2), temos que

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

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

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.

Aula 14

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 (13.2). 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 14.1. 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 14.2. 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 14.3. 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:

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

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 14.4. 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.

7.3. Homomorfimos de anéis e anéis quocientes

Definição 14.5. 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 14.6. 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 14.7. 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 14.8. 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:

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

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

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

Aula 15

Definição 15.1. 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 15.2. 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 15.3. Vamos verificar que $2\mathbb{Z}$ é um ideal (bilateral) de $\mathbb{Z}$.

(i) Lembre do Exemplo 12.6 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 15.4. 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 15.5. 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 15.6. Se $\Bbbk$ é um corpo, mostre que os únicos ideias (bilaterais) de $\Bbbk$ são $\{0_\Bbbk\}$ e $\Bbbk$.

Proposição 15.7. *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 12.5.

(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 12.5 (que é a condição (i) da Definição 15.1) e a condição (ii) da Definição 15.1.

- 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 15.8. 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 15.9. 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 15.10. *(a) Seja $f\colon R \to S$ um homomorfismo 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 15.7 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 15.11. *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 12.5 (que é a condição (i) da Definição 15.1) e a condição (ii) da Definição 15.1. 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 12.5 (que é a condição (i) da Definição 15.1) e a condição (ii) da Definição 15.1. 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 12.5 (que é a condição (i) da Definição 15.1) e a condição (ii) da Definição 15.1. 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 9.12 (Segundo Teorema de Isomorfismo de grupos), do Teorema 10.1 (Terceiro Teorema de Isomorfismo de grupos) e do Teorema 10.2 para anéis.

Teorema 15.12. *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 15.13. Use os isomorfismos explícitos dados nas demonstrações dos Teoremas 9.12, 10.1, 10.2 para demonstrar o Teorema 15.12.

Aula 16

7.4. Propriedades de ideais

Definição 16.1. 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 $(x_1, \ldots, x_n)$.
(b) 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 $\{r\}$.
(c) 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 16.2. 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 16.3. 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.

Exercício 16.4. Seja R um anel não-trivial com identidade. Mostre que, se $X \subseteq Y \subseteq R$, então $(X) \subseteq (Y)$.

Proposição 16.5. *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 15.11(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 16.6. 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 16.7. 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 16.8. 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 16.5, $(2, x) = \{2p + xq \mid p, q \in \mathbb{Z}[x]\} = \{2n + xr \mid n \in \mathbb{Z},\ r \in \mathbb{Z}[x]\}$. 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.

Exercício 16.9. 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 principal, gerado por $(\sigma - 1_R)$.

Proposição 16.10. *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 16.11. 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 16.10(c).

Corolário 16.12. *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 16.10(b), $\ker(f) = \{0_D\}$ ou $\ker(f) = D$. No primeiro caso, f é injetor, e no segundo caso, f é trivial. □

Definição 16.13. 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 16.14 (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 16.15. *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 16.10(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. $\square$

Aula 17

7.4. Propriedades de ideais

Proposição 17.1. *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 16.10, R/m é um corpo se, e somente se, seus únicos ideais são $\{0_{R/\mathsf{m}}\}$ e R/m. Pelo Teorema 15.12(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 17.2. 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 17.3. 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 17.1, 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 16.8). Como $\mathbb{Z}_2$ é um corpo (Corolário 12.4), então segue da Proposição 17.1 que $(2, x)$ é maximal.

Exercício 17.4. Mostre que o ideal de aumento em $\mathbb{R}[G]$ é maximal.

Definição 17.5. 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 17.6. 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 17.7. *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 17.5, isso mostra que P é primo. □

Corolário 17.8. *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 17.1 e 17.7. □

Exemplo 17.9. Lembre do Exemplo 17.3 que (x) é um ideal de $\mathbb{Z}[x]$ tal que $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. Então segue da Proposição 17.7, que (x) é um ideal primo. Mas, pelo que foi mostrado no Exemplo 17.3, (x) não é maximal. De fato, $(x) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$.

7.5. Corpo de frações

Exemplo 17.10. 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 17.11. 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 18

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 18.1. Dado um domínio D, o corpo (Q,s,m) é chamado de corpo de frações de D.

Lema 18.2. *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 18.3. Mostre que existe um único homomorfismo de anéis $f\colon \mathbb{Z} \to \mathbb{Z}_6$ satisfazendo $f(1) = \overline{3}$.

Teorema 18.4. *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 18.2, $f(1_R) = 1_Q$. 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 18.5. 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 18.6. Considere o anel $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ do Exemplo 12.1 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 12.2 é isomorfo a Q. Primeiro lembre do Exemplo 12.2 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 18.4, 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 18.7. Se R for um corpo, mostre que o corpo de frações de R é o próprio R.

7.3. Teorema chinês dos restos

Exercício 18.8. 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 18.9. Dado R um anel não-trivial, comutativo e com identidade, dois ideais $I, J \subseteq R$ são ditos comaximais quando $I + J = R$.

Exemplo 18.10. 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 5.15 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 18.11. 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 18.12 (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 18.13. *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 18.10, $p_i^{k_i}\mathbb{Z}$ 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 18.12. □

Aula 19

8.1. Domínios Euclidianos

Nesta seção todos os anéis serão domínios.

Definição 19.1. Dado um domínio D, uma norma em D é uma função $N\colon D \to \mathbb{N}$ tal que $N(0) = 0$. Um domínio D munido de uma norma N é dito Euclidiano quando, para quaisquer $a \in D$ e $b \in D \setminus \{0_D\}$, existem $q, r \in D$ tais que

$$a = qb + r, \quad \text{onde } r = 0 \text{ ou } N(r) < N(b).$$

Exemplo 19.2. Dado um corpo $\Bbbk$, observe que $a = (ab^{-1})b$ para quaisquer $a, b \in \Bbbk$. Portanto, $\Bbbk$ é um domínio Euclidiano com qualquer norma $N\colon \Bbbk \to \mathbb{N}$; em particular, podemos tomar a norma dada por $N(a) = 0$ para todo $a \in \Bbbk$.

Exemplo 19.3. Considere o domínio $\mathbb{Z}$. Observe que a função $N\colon \mathbb{Z} \to \mathbb{N}$ dada por$N(a) = |a|$ é uma norma em $\mathbb{Z}$. De fato, $N(0) = |0| = 0$ e $N(a) = |a| \geq 0$ para todo $a \in \mathbb{Z}$. Agora lembre que, usando o algoritmo de divisão, para quaisquer $a \in \mathbb{Z}$ e $b \in \mathbb{Z} \setminus \{0\}$, existem $q, r \in \mathbb{Z}$ tais que

$$a = qb + r, \quad \text{onde } r = 0 \text{ ou } |r| < |b|.$$

Isso mostra que $(\mathbb{Z}, |\cdot|)$ é um domínio Euclidiano.

Exemplo 19.4. Considere o corpo dos números reais $\mathbb{R}$ e lembre que o anel de polinômios em uma variável $\mathbb{R}[x]$ é um domínio. Observe que $\operatorname{grau}\colon \mathbb{R}[x] \to \mathbb{N}$ é de fato uma norma em $\mathbb{R}[x]$. Lembre que, usando o algoritmo de divisão de polinômios, para quaisquer $a \in \mathbb{R}[x]$ e $b \in \mathbb{Z}[x] \setminus \{0\}$, existem polinômios $q, r \in \mathbb{R}[x]$ tais que

$$a = qb + r, \quad \text{onde } r = 0 \text{ ou } \operatorname{grau}(r) < \operatorname{grau}(b).$$

Isso mostra que $(\mathbb{R}[x], \operatorname{grau})$ é um domínio Euclidiano.

Verifique que, para qualquer corpo $\Bbbk$, o domínio $\Bbbk[x]$ munido da norma grau também é um domínio Euclidiano. (Pois um algoritmo de divisão similar ao de $\mathbb{R}[x]$ funciona em $\Bbbk[x]$.)

Proposição 19.5. *Todo ideal de um domínio Euclidiano é principal.*

Demonstração. Considere um domínio Euclidiano (D, N) e $I \subseteq D$ um ideal. Se $I = \{0_D\}$, então $I = (0_D)$ é principal. Então assuma que $I \neq \{0_D\}$. Como $\{N(i) \mid i \in I \setminus \{0_D\}\}$ é um subconjunto não-vazio de $\mathbb{N}$, existe $i \in I \setminus \{0_D\}$ tal que $N(i) \leq N(j)$ para todo $j \in I \setminus \{0_D\}$. Vamos mostrar que $I = (i)$.

Como $i \in I$, então $(i) \subseteq I$. Logo, basta mostrar que $I \subseteq (i)$. Se $a = 0_D$, então $a \in (i)$. Então assuma que $a \in I \setminus \{0_D\}$. Como D é um domínio Euclidiano, existem $q, r \in D$ tais que

$$a = qi + r, \quad \text{onde } r = 0 \text{ ou } N(r) < N(i).$$

Como $r = a - qi$, então $r \in I$. Como $N(i) \leq N(j)$ para todo $j \in I \setminus \{0_D\}$, então $r = 0_D$. Isso implica que $a = qi$, ou seja, $a \in (i)$. □

Exemplo 19.6. Lembre do Exemplo 16.8 que o ideal $(2, x) \subseteq \mathbb{Z}[x]$ não é um ideal principal. Portanto, segue da Proposição 19.5 que $\mathbb{Z}[x]$ não é um domínio Euclidiano. Vamos verificar que $\mathbb{Z}[x]$ munido, por exemplo, da norma $N\colon \mathbb{Z}[x] \to \mathbb{N}$ dada por $N(p) = \operatorname{grau}(p)$ não é um domínio Euclidiano. Se fosse, existiriam $q, r \in \mathbb{Z}[x]$ tais que

$$x = 2q + r, \quad \text{onde } r = 0 \text{ (pois } \operatorname{grau}(2) = 0).$$

Mas não existe $q \in \mathbb{Z}[x]$ tal que $x = 2q$.

Definição 19.7. Seja R um anel comutativo. Dados $a \in R$ e $b \in R \setminus \{0_R\}$, dizemos que a é múltiplo de b quando existe $r \in R$ tal que $a = rb$. Neste caso, dizemos também que b é um divisor de a, e denotamos $b \mid a$. Dados $r, s \in R$, um elemento $d \in R \setminus \{0_R\}$ é dito mdc de r e s quando satisfaz as seguintes condições:

(i) $d \mid r$, $d \mid s$,
(ii) se $d' \mid r$ e $d' \mid s$, então $d' \mid d$.

O mdc entre dois elementos não-nulos de um anel comutativo R nem sempre existe. O próximo lema mostra, em particular, que, no caso de domínios Euclidianos, o mdc sempre existe.

Lema 19.8. *Sejam R um anel comutativo e $a, b \in R \setminus \{0_R\}$. Se existe $d \in R$ tal que $(a, b) = (d)$, então d é um mdc de a e b.*

Demonstração. Como $(a, b) = (d)$, então $a, b \in (d)$. Portanto $d \mid a$ e $d \mid b$. Agora suponha que $d' \in R$ seja tal que $d' \mid a$ e $d' \mid b$, ou seja, tal que existam $r, s \in R$ satisfazendo $a = rd'$ e $b = sd'$. Isso implica que todo elemento em (a, b) é da forma $xa + yb = xrd' + ysd' = (xr + ys)d'$ para alguns $x, y \in R$. Como $(a, b) = (d)$, então existem $x, y \in R$ tais que $d = xa + yb = (xr + ys)d'$. Isso mostra que $d' \mid d$. Portanto d é um mdc de a e b. □

O próximo lema mostra, em particular, que, quando existirem, os mdcs são únicos a menos de multiplos por unidades.

Lema 19.9. *Sejam D um domínio e $d_1, d_2 \in D \setminus \{0_D\}$. Se $(d_1) = (d_2)$, então $d_1 = ud_2$ para algum $u \in D^\times$. Em particular, se d_1, d_2 forem mdcs de a, b, então $d_1 = ud_2$ para algum $u \in D^\times$.*

Demonstração. Se $(d_1) \subseteq (d_2)$, então existe $u \in R$ tal que $d_1 = ud_2$. Se $(d_2) \subseteq (d_1)$, então existe $v \in R$ tal que $d_2 = vd_1$. Portanto $d_1 = ud_2 = u(vd_1) = (uv)d_1$, ou seja, $d_1(1_D - uv) = 0_D$. Como D é um domínio e $d_1 \neq 0_D$, então $uv = 1_D$. Isso mostra que $u, v \in D^\times$.

Se $d_1, d_2 \in D$ são mdcs de a e b, então $d_1 \mid d_2$ e $d_2 \mid d_1$, ou seja, $(d_2) \subseteq (d_1)$ e $(d_1) \subseteq (d_2)$. Isso implica que $(d_1) = (d_2)$. Pela primeira parte desse lema, existe $u \in D^\times$ tal que $d_1 = ud_2$. □

Sejam (D, N) um domínio Euclidiano e $a, b \in D \setminus \{0_D\}$. Os dois lemas acima mostram que um mdc de a, b existe e que ele é único a menos de uma unidade de D. Para calcular explicitamente um mdc entre a e b, podemos usar o seguinte algoritmo. Existem $q_1, r_1 \in D$ tais que

$$a = q_1 b + r_1, \quad \text{onde } r_1 = 0_D \text{ ou } N(r_1) < N(b).$$

Se $r_1 = 0_D$, então $b \mid a$. Neste caso, $\text{mdc}(a, b) = b$. (De fato, se $d \mid a$ e $d \mid b$, então $d \mid b$.) Caso contrário, existem $q_2, r_2 \in D$ tais que

$$b = q_2 r_1 + r_2, \quad \text{onde } r_2 = 0_D \text{ ou } N(r_2) < N(r_1).$$

Se $r_2 = 0_D$, então $b = q_2 r_1$ e $a = q_1 b + r_1 = (q_1 q_2) r_1 + r_1 = (q_1 q_2 + 1) r_1$. Neste caso, $\text{mdc}(a, b) = r_1$. (De fato, se $d \mid a$ e $d \mid b$, então $d \mid r_1$.) Caso contrário, existem $q_3, r_3 \in D$ tais que

$$r_1 = q_3 r_2 + r_3, \quad \text{onde } r_3 = 0_D \text{ ou } N(r_3) < N(r_2).$$

Se $r_3 = 0_D$, então $b = (q_2 q_3) r_2$ e $a = q_1 b + r_1 = (q_1 q_2 q_3) r_2 + q_3 r_2 = (q_1 q_2 + 1) q_3 r_2$. Neste caso, $\text{mdc}(a, b) = r_2$. (De fato, se $d \mid a$ e $d \mid b$, então $d \mid r_1$, e consequentemente, $d \mid r_2$.) E assim sucessivamente. Observe que $\text{mdc}(a, b) = r_n$, onde n é o menor inteiro positivo tal que $r_{n+1} = 0$. Observe que esse algoritmo sempre para, pois $N(b) > N(r_1) > N(r_2) > \cdots > N(r_n) > \cdots$.

Aula 20

8.2. Domínio de ideais principais

Definição 20.1. Um domínio D é dito de ideais principais quando todo ideal $I \subseteq D$ é principal, ou seja, quando existe $d \in D$ tal que $I = (d)$.

Exemplo 20.2. Considere um corpo $\Bbbk$. Lembre que $\Bbbk$ é um domínio e que os únicos ideais de $\Bbbk$ são $\{0_\Bbbk\}$ e $\Bbbk$. Como $\{0_\Bbbk\} = (0_\Bbbk)$ e $\Bbbk = (1_\Bbbk)$, então $\Bbbk$ é um domínio de ideais principais.

Exemplo 20.3. Pela Proposição 19.5, todo domínio Euclidiano é de ideais principais. Em particular, pelo Exemplo 19.3, $\mathbb{Z}$ é um domínio de ideais principais, e pelo Exemplo 19.4, se $\Bbbk$ é um corpo, então $\Bbbk[x]$ é um domínio de ideais principais.

Exemplo 20.4. Lembre do Exemplo 16.8 que $(2, x) \subseteq \mathbb{Z}[x]$ não é um ideal principal. Portanto $\mathbb{Z}[x]$ não é um domínio de ideais pricipais.

O próximo resultado mostra que mdcs existem e são únicos (a menos de unidades) em domínios de ideais principais.

Proposição 20.5. *Sejam D um domínio de ideais principais e $a, b \in D \setminus \{0_D\}$. Se $d \in D$ é tal que $(a, b) = (d)$, então:*

(a) d é um mdc de a e b;
(b) existem $x, y \in D$ tais que $d = ax + by$;
(c) se $d' \in D$ é tal que $(d') = (a, b)$, então existe $u \in D^\times$ tal que $d' = ud$.

Demonstração. A parte (a) segue do Lema 19.8. A parte (b) segue do fato de $d \in (a, b)$. A parte (c) segue do Lema 19.9. □

Lembre que todo ideal maximal é primo (Corolário 17.8). Lembre também que $(x) \subseteq \mathbb{Z}[x]$ é um ideal primo que não é maximal, pois $(x) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$ (Exemplo 17.3).

Proposição 20.6. *Se D for um domínio de ideais principais, então todo ideal primo não-nulo é maximal.*

Demonstração. Seja $(p) \subseteq D$ um ideal primo, $p \in D \setminus \{0_D\}$. Se $d \in D$ é tal que $(p) \subseteq (d)$, então $p = xd$ para algum $x \in D$. Como (p) é primo, então $x \in (p)$ ou $d \in (p)$. No primeiro caso, $x = py$ para algum $y \in D$. Logo $p = xd = (py)d$. Como D é um domínio e $p \neq 0_D$, então $yd = 1_D$. Isso mostra que $d \in D^\times$. Logo $(d) = D$. No segundo caso, $d \in (p)$. Logo $(d) = (p)$. Isso mostra que (p) é maximal. □

Corolário 20.7. *Dado um anel comutativo R. Se $R[x]$ for um domínio de ideais principais, então R é um corpo.*

Demonstração. Pela Proposição 13.1(c), $R[x]$ é um domínio se, e somente se, R é um domínio. Então, como $R[x]/(x) \cong R$, segue da Proposição 17.7 que $(x) \subseteq R[x]$ é um ideal primo. Se $R[x]$ for um domínio de ideais principais, segue da Proposição 20.6 que $(x) \subseteq R[x]$ é um ideal maximal. Então, segue da Proposição 17.1 que $R \cong R[x]/(x)$ é um corpo. □

Exemplo 20.8. Lembre do Exemplo 20.3 que, se $\Bbbk$ for um corpo, então $\Bbbk[x]$ é um domínio de ideais principais. E lembre do Exemplo 20.4 que, $\mathbb{Z}[x]$ não é um domínio de ideais principais.

Exemplo 20.9. Considere duas variáveis, $\bigstar_1$ e $\bigstar_2$. Agora considere o anel $(R[\bigstar_1])[\bigstar_2]$, que consiste de polinômios na variável $\bigstar_2$ com coeficientes no anel $R[\bigstar_1]$. Denote $(R[\bigstar_1])[\bigstar_2]$ por $R[\bigstar_1, \bigstar_2]$ e observe que os elementos de $R[\bigstar_1, \bigstar_2]$ têm a forma

$$a_{0,0} + a_{1,0}\bigstar_1 + a_{0,1}\bigstar_2 + a_{1,1}\bigstar_1\bigstar_2 + \cdots + a_{n,m}\bigstar_1^n\bigstar_2^m,$$

onde $n, m \geq 0$ e $a_{i,j} \in R$ para todos $i \in \{1, \ldots, n\}$, $j \in \{1, \ldots, m\}$.

Lembre da Proposição 13.1 que $\mathbb{R}[\bigstar_1]$ é um domínio, mas não é um corpo. Portanto, pelo Corolário 20.7, $R[\bigstar_1, \bigstar_2]$ é um domínio, mas não é de ideais principais. De fato, o ideal $(\bigstar_1, \bigstar_2)$ não é principal.

8.3. Domínios de fatoração única

Definição 20.10. Seja D um domínio.

(a) Um elemento $d \in D \setminus (D^\times \cup \{0_D\})$ é dito redutível quando existem $a, b \in D \setminus D^\times$ tais que $d = ab$. Um elemento $d \in D \setminus (D^\times \cup \{0_D\})$ é dito irredutível quando, para todos $a, b \in D$ tais que $d = ab$, temos que $a \in D^\times$ ou $b \in D^\times$.
(b) Um elemento $p \in D \setminus (D^\times \cup \{0_D\})$ é dito primo quando, para todos $a, b \in D$ tais que $p \mid ab$, temos que $p \mid a$ ou $p \mid b$.
(c) Dois elementos $a, b \in D$ são ditos associados quando existe $u \in D^\times$ tal que $a = ub$.

Exemplo 20.11. Considere o domínio $\mathbb{Z}$. Observe que, como $\mathbb{Z}^\times = \{-1, 1\}$, então $a, b \in \mathbb{Z}$ são associados se, e somente se $a \in \{-b, b\}$. Agora, lembre que um elemento $p \in \mathbb{Z}$ é primo se, e somente se, para todos $a, b \in D$ tais que $p \mid ab$, temos que $p \mid a$ ou $p \mid b$. Então a definição de elemento primo de um domínio generaliza a definição de número inteiro primo.

Um elemento $z \in D$ é redutível quando existem $a, b \in \mathbb{Z} \setminus \{-1, 1\}$ tais que $z = ab$, ou seja, quando z é composto. Logo, um elemento $z \in \mathbb{Z}$ é irredutível quando z é primo. Ou seja, em $\mathbb{Z}$ as noções de elemento primo e irredutível são as mesmas. Nós veremos a seguir que isso não ocorre em geral.

Proposição 20.12. *Seja D for um domínio de ideais principais. Um elemento $d \in D \setminus (D^\times \cup \{0_D\})$ é irredutível se, e somente se, o ideal $(d) \subseteq D$ é maximal.*

Demonstração. "Somente se": Suponha que $d \in D \setminus (D^\times \cup \{0_D\})$ é irredutível. Se $a \in D$ é tal que $(d) \subseteq (a) \subseteq D$. Então $d \in (a)$ implica que existe $b \in D$ tal que $d = ab$. Como d é um elemento irredutível, então segue que $a \in D^\times$ ou $b \in D^\times$. No primeiro caso, $(a) = D$ e, no segundo caso, $(a) = (d)$.

"Se": Suponha que $(d) \subseteq D$ é um ideal maximal. Se $a, b \in D$ são tais que $d = ab$, então $(d) \subseteq (a)$. Como (d) é maximal, então $(a) = D$ ou $(a) = (d)$. No primeiro caso, segue da Proposição 16.10(a) que $a \in D^\times$; no segundo caso, segue do Lema 19.9 que $b \in D^\times$. □

Exemplo 20.13. Considere o ideal $\mathbb{Z}[x]$. Lembre que $(x) \subseteq \mathbb{Z}[x]$ não é um ideal maximal. Mas observe que $x \in \mathbb{Z}[x]$ é um elemento irredutível. De fato, se $p, q \in \mathbb{Z}[x]$ são tais que $x = pq$, então $\text{grau}(p) + \text{grau}(q) = \text{grau}(x) = 1$. Como $\mathbb{Z}[x]$ é comutativo, sem perda de generalidade, podemos supor que $\text{grau}(p) = 0$ e $\text{grau}(q) = 1$. Ou seja, existem $a, b, c \in \mathbb{Z}$ tais que $p = a$ e $q = bx + c$. Como $pq = x$, então $ab = 1$ e $ac = 0$. Isso mostra que $a = b \in \{-1, 1\} = \mathbb{Z}^\times$ e $c = 0$. Em particular, $p \in \mathbb{Z}[x]^\times$.

Esse exemplo mostra que, se D não for um domínio de ideais principais, mesmo que $d \in D \setminus D^\times$ seja irredutível, $(d) \subseteq D$ não necessariamente é um ideal maximal.

Proposição 20.14. *Seja D um domínio.*

(a) Um elemento $p \in D$ é primo se, e somente se, $(p) \subseteq D$ é um ideal primo.
(b) Se $p \in D$ for primo, então p é irredutível.
(c) Se D for um domínio de ideais principais, então p é primo se, e somente se, p é irredutível.

Demonstração. (a) Lembre que $(p) \subseteq D$ é um ideal primo se, e somente se, para todos $a, b \in D$ tais que $ab \in (p)$, temos que $a \in (p)$ ou $b \in (p)$. Ou seja, para todos $a, b \in D$ tais que $p \mid ab$, temos que $p \mid a$ ou $p \mid b$. Pela Definição 20.10, p é primo se, e somente se, para todos $a, b \in D$ tais que $p \mid ab$, temos que $p \mid a$ ou $p \mid b$.

(b) Suponha que p é primo e sejam $a, b \in D$ tais que $p = ab$. Como $p \mid ab$ e p é primo, então $p \mid a$ ou $p \mid b$. Isso significa que existe $x \in D$ tal que $a = px$ ou $b = px$. Como D é comutativo, sem perda de generalidade, podemos supor que $a = px$. Neste caso, $p = ab = (px)b = p(xb)$. Como D é um domínio, segue que $xb = 1_D$, ou seja, $b \in D^\times$. Isso mostra que p é irredutível.

(c) Pelo item (b), se p for primo, então p é irredutível. Por outro lado, se D é um domínio de ideais principais e p for irredutível, segue da Proposição 20.12 que $(p) \subseteq D$ é um ideal maximal. Então, segue da Corolário 17.8 que $(p) \subseteq D$ é um ideal primo. Daí, segue do item (a) que, $p \in D \setminus D^\times$ é um elemento primo. □

Exemplo 20.15. Lembre que $\mathbb{Z}$ é um domínio de ideais principais e que, de fato, todos os ideais de $\mathbb{Z}$ são da forma $n\mathbb{Z}$ para algum $n \in \mathbb{Z}$. Lembre também que $p\mathbb{Z} \subseteq \mathbb{Z}$ é maximal se, e somente se, $p\mathbb{Z} \subseteq \mathbb{Z}$ é primo se, e somente se, $p \in \mathbb{Z}$ é irredutível se, e somente se, $p \in \mathbb{Z}$ é primo.

Aula 21

Lembre que nós provamos o seguinte resultado no fim da aula passada.

Proposição 21.1. *Seja D um domínio.*

(a) Um elemento $p \in D$ é primo se, e somente se, $(p) \subseteq D$ é um ideal primo.
(b) Se $p \in D$ for primo, então p é irredutível.
(c) Seja D for um domínio de ideais principais. Um elemento $d \in D \setminus (D^\times \cup \{0_D\})$ é irredutível se, e somente se, o ideal $(d) \subseteq D$ é maximal.
(d) Se D for um domínio de ideais principais, então p é primo se, e somente se, p é irredutível.

Exemplo 21.2. Considere o elemento $\sqrt{-5} \in \mathbb{C}$, e observe que o conjunto

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$$

é um subanel de $\mathbb{C}$, quando munido das operações dadas por

$$s\colon \mathbb{Z}[\sqrt{-5}] \times \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}[\sqrt{-5}], \qquad s(a + b\sqrt{-5}, c + d\sqrt{-5}) = (a + c) + (b + d)\sqrt{-5} \quad \text{e}$$
$$m\colon \mathbb{Z}[\sqrt{-5}] \times \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}[\sqrt{-5}], \qquad m(a + b\sqrt{-5}, c + d\sqrt{-5}) = (ac - 5bd) + (ad + bc)\sqrt{-5}.$$

Como $\mathbb{C}$ é um domínio (um corpo), então $\mathbb{Z}[\sqrt{-5}]$ é um domínio. Vamos usar a proposição anterior para mostrar que $\mathbb{Z}[\sqrt{-5}]$ não é um domínio de ideais principais.

Primeiro, vamos determinar quais são as unidades de $\mathbb{Z}[\sqrt{-5}]$. Pela definição de m, temos que $(a + b\sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]^\times$ se, e somente se, existem $c, d \in \mathbb{Z}$ tais que $ac = 5bd + 1$ e $ad = -bc$. Resolvendo essas equações para $a, b \in \mathbb{Z}$, obtemos que $a \in \{-1, 1\}$ e $b = 0$.

Observe que $3 \in \mathbb{Z}[\sqrt{-5}]$ é um elemento irredutível. De fato, se $(a + b\sqrt{-5}), (c + d\sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]^\times$ são tais que $m(a + b\sqrt{-5}), c + d\sqrt{-5}) = 3$, então $ac = 5bd + 3$ e $ad = -bc$. Resolvendo essas equações para $a, b \in \mathbb{Z}$, obtemos que $a \in \{-3, -1, 1, 3\}$ e $b = 0$. Mas não é um elemento primo. De fato, como $m(2 + \sqrt{-5}, 2 - \sqrt{-5}) = 9 = 3^2$, então $3 \mid m(2 + \sqrt{-5}, 2 - \sqrt{-5})$, mas $3 \nmid (2 + \sqrt{-5})$ e $3 \nmid (2 - \sqrt{-5})$.

Como nem todo elemento irredutível de $\mathbb{Z}[\sqrt{-5}]$ é um elemento primo, então $\mathbb{Z}[\sqrt{-5}]$ não é um domínio de ideais principais. (Em particular, $\mathbb{Z}[\sqrt{-5}]$ não é um domínio Euclidiano.)

Exercício 21.3. Seja D um domínio e $u \in D^\times$. Mostre que, se $d \in D \setminus (D^\times \cup \{0_D\})$ for irredutível, então $ud \in D \setminus (D^\times \cup \{0_D\})$ é irredutível.

Definição 21.4. Um domínio D é dito de fatoração única quando todo $d \in D \setminus (D^\times \cup \{0_D\})$ admite uma única (a menos de associados) fatoração em irredutíveis, ou seja:

(i) existem $n > 0$ e elementos irredutíveis $p_1, \ldots, p_n \in D$ (não necessáriamente distintos), tais que $d = p_1 \cdots p_n$;
(ii) se $m > 0$ e $q_1, \ldots, q_m \in D$ forem elementos irredutíveis tais que $d = q_1 \cdots q_m$, então $m = n$ e q_i é associado a p_i para todo $i \in \{1, \ldots, n\}$.

Exemplo 21.5. Considere o domínio $\mathbb{Z}$. Lembre que todo elemento $z \in \mathbb{Z} \setminus \{-1, 0, 1\}$ admite uma decomposição primária $z = p_1 \cdots p_n$, onde $p_1, \ldots, p_n \in \mathbb{Z}$ são os primos (portanto elementos irredutíveis em $\mathbb{Z}$) que dividem z. Lembre ainda que essa decomposição primária é única a menos de sinal (ou seja, a menos de associados).

Exemplo 21.6. Lembre que $\Bbbk$ é um corpo se, e somente se, $\Bbbk^\times = \Bbbk \setminus \{0_\Bbbk\}$. Portanto, por vacuidade ($\Bbbk \setminus (\Bbbk^\times \cup \{0_\Bbbk\}) = \emptyset$), todo corpo é um domínio de fatoração única.

Exercício 21.7. Considere o domínio $\mathbb{Z}[\sqrt{-5}]$ do Exemplo 21.2.

(a) Mostre que $2, 3, (1 + \sqrt{-5}), (1 - \sqrt{-5})$ são elementos irredutíveis de $\mathbb{Z}[\sqrt{-5}]$.

(b) Mostre que 2 não é associado a $(1+\sqrt{-5}), (1-\sqrt{-5})$ e que 3 também não é associado a $(1+\sqrt{-5}), (1-\sqrt{-5})$.
(c) Mostre que 6 admite mais de uma fatoração em irredutíveis, e conclua que $\mathbb{Z}[\sqrt{-5}]$ não é um domínio de fatoração única.

Proposição 21.8. *Se D for um domínio de fatoração única, então todo elemento irredutível em D é primo.*

Demonstração. Seja $d \in D$ um elemento irredutível e considere $a, b \in D$ tais que $d = ab$. Suponha (por contradição) que $a, b \in D^\times$. Como D é um domínio de fatoração única, então existem $n, m > 0$ e $p_1, \ldots, p_n, q_1, \ldots, q_m \in D$ irredutíveis tais que $a = p_1 \cdots p_n$ e $b = q_1 \cdots q_m$. Por hipótese $d = p_1 \cdots p_n q_1 \cdots q_m$ são duas decomposições irredutíveis de d. Então $m + n = 1$, ou seja, temos que $m = 0$ e $n = 1$ ou que $m = 1$ e $n = 0$. Em ambos os casos, temos uma contradição com o fato de $n, m > 0$. Isso mostra que $a \in D^\times$ ou $b \in D^\times$, e portanto que d é um elemento primo. □

Proposição 21.9. *Sejam D um domínio de fatoração única e $a, b \in D \setminus \{0_D\}$. Se uma decomposição de a e b em fatores irredutíveis é dada por*

$$a = up_1^{k_1} \cdots p_n^{k_n} \quad \text{e} \quad b = vp_1^{\ell_1} \cdots p_n^{\ell_n}$$

onde $p_1, \ldots, p_n \in D \setminus (D^\times \cup \{0_D\})$ são irredutíveis distintos, $u, v \in D^\times$ e $k_1, \ell_1, \ldots, k_n, \ell_n \in \mathbb{N}$, então $\operatorname{mdc}(a, b) = p_1^{\min\{k_1,\ell_1\}} \cdots p_n^{\min\{k_n,\ell_n\}}$.

Demonstração. Denote $p_1^{\min\{k_1,\ell_1\}} \cdots p_n^{\min\{k_n,\ell_n\}}$ por d. Como $\min\{k_i, \ell_i\} \leq k_i$ e $\min\{k_i, \ell_i\} \leq \ell_i$ para todo $i \in \{1, \ldots, n\}$, então $d \mid a$, $d \mid b$. Agora suponha que $d' \mid a$ e $d' \mid b$, ou seja, que existem $x, y \in D$ tais que $xd' = up_1^{k_1} \cdots p_n^{k_n}$ e $yd' = vp_1^{\ell_1} \cdots p_n^{\ell_n}$. Se $d' = q_1^{i_1} \cdots q_m^{i_m}$, pela unicidade (a menos de associados) das decomposições em irredutíveis de a e b, segue que $m = n$ e, sem perda de generalidade, $q_1 = p_1, i_1 \leq k_1, i_1 \leq \ell_1, \ldots, q_n = p_n, i_n \leq k_n, i_n \leq \ell_n$. Isso implica que $d' \mid d$. □

Teorema 21.10. *Se D for um domínio de ideais principais, então D é um domínio de fatoração única.*

Demonstração. Considere $d \in D \setminus (D^\times \cup \{0_D\})$. Queremos mostrar que d admite uma decomposição como produto de elementos irredutíveis em D e que essa decomposição é única a menos de associados.

Se d for irredutível, então $d = d$ é uma decomposição de d em irredutíveis. Caso contrário, se d for redutível, então existem $d_1, d_2 \in D \setminus (D^\times \cup \{0_D\})$ tais que $d = d_1 d_2$. Se d_1, d_2 forem irredutíveis, então $d = d_1 d_2$ é uma decomposição de d em irredutíveis. Caso contrário, se d_1 for redutível, então existem $d_{11}, d_{12} \in D \setminus (D^\times \cup \{0_D\})$ tais que $d_1 = d_{11} d_{12}$, e se d_2 for redutível, então existem $d_{21}, d_{22} \in D \setminus (D^\times \cup \{0_D\})$ tais que $d_2 = d_{21} d_{22}$. Esse processo continua até que todos os fatores $d_{i_1 \cdots i_m}$ sejam irredutíveis.

Para mostrar que esse critério de parada é satisfeito, vamos supor que existam elementos $d_{i_1}, d_{i_1 i_2}, \ldots, d_{i_1 \cdots i_m}, \ldots \in D \setminus (D^\times \cup \{0_D\})$ tais que $d_{i_1 \cdots i_k i_{k+1}} \mid d_{i_1 \cdots i_k}$ para todo $k > 1$, ou seja, tais que

$$(d_{i_1}) \subseteq (d_{i_1 i_2}) \subseteq \ldots \subseteq (d_{i_1 \cdots i_k}) \subseteq \cdots \subsetneq D.$$

Defina $I = \bigcup_{k \geq 1} (d_{i_1 \cdots i_k})$ e observe que I é um ideal próprio de D (compare com a demonstração da Proposição 16.15). Como, por hipótese, D é um domínio de ideais principais, então existe $a \in D \setminus (D^\times \cup \{0_D\})$ tal que $(a) = I$. Como, em particular, $a \in \bigcup_{k \geq 1} (d_{i_1 \cdots i_k})$, então $a \in (d_{i_1 \cdots i_k})$ para algum $k \geq 1$. Ou seja, $(a) \subseteq (d_{i_1 \cdots i_k}) \subseteq I = (a)$ para algum $k \geq 1$. Logo $I = (d_{i_1 \cdots i_k})$ para

algum $k \geq 1$. Em particular, isso mostra que a é associado a $d_{i_1 \cdots i_k}$, que é associado a $d_{i_1 \cdots i_\ell}$ para todo $\ell > k$. Consequentemente, $d_{i_1 \cdots i_k}$ é irredutível.

Agora vamos usar indução para mostrar que, para todo $d \in D \setminus (D^\times \cup \{0_D\})$, a menos de associados, existe uma única decomposição de d em irredutíveis. Suponha que existam $m, n > 0$, $v \in D^\times$ e $p_1, \ldots, p_n, q_1, \ldots, q_m \in D \setminus (D^\times \cup \{0_D\})$ irredutíveis (não necessariamente distintos) tais que $d = p_1 \cdots p_n = v q_1 \cdots q_m$. Como p_1 é irredutível e $q_1, \ldots, q_m \in D \setminus (D^\times \cup \{0_D\})$, no caso $n = 1$, $p_1 = v q_1 \cdots q_m$ se, e somente se, $m = 1$ e $p_1 = v q_1$. Isso mostra o caso $n = 1$. Suponha agora (por hipótese de indução) que a unicidade é válida para $n - 1$ ($n > 1$). Como $p_1 \mid d = v q_1 \cdots q_m$ e p_1 é irredutível, então $p_1 \mid q_j$ para algum $j \in \{1, \ldots, m\}$. Como D é comutativo, sem perda de generalidade, podemos supor que $p_1 \mid q_1$. Como q_1 é irredutível, então existe $u_1 \in D^\times$ tal que $q_1 = u_1 p_1$. Consequentemente, $p_1 p_2 \cdots p_n = v q_1 q_2 \cdots q_m = v u_1 p_1 q_2 \cdots q_m$. Como D é um domínio, então $p_2 \cdots p_n = v u_1 q_2 \cdots q_m$. Pela hipótese de indução, concluímos que $m = n$ e que existem $u_2, \ldots, u_n \in D^\times$ tais que $p_2 = u_2 q_2, \ldots, p_n = u_n q_n$. Isso termina a demonstração. □

Exemplo 21.11. Considere $D = \mathbb{Z}$. Neste caso, o Teorema 21.10 é conhecido como Teorema Fundamental da Aritmética. De fato, neste caso, o resultado afirma que todo número inteiro admite uma decomposição em fatores primos e que essa decomposição é única a menos de escolha de sinal dos fatores primos.

Aula 22

9.1. Anéis de polinômios: definições e propriedades básicas

A partir de agora, assuma que R é um anel não-trivial, comutativo e com identidade. Lembre que o anel $R[x]$, de polinômios na variável x com coeficientes em R, é um anel não-trivial, comutativo e com identidade, cujos elementos são da forma

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

Lembre também que $0_{R[x]} = 0$ e $1_{R[x]} = 1 + 0x$. Lembre ainda, da Proposição 13.1, que:

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

Dado um ideal $I \subseteq R$, lembre que I é, em particular, um subanel de R. Portanto, pelo item (d) acima, $I[x]$ (os polinômios na variável x com coeficientes em I) é um subanel de $R[x]$.

Proposição 22.1. *Sejam R um anel não-trivial, comutativo, com identidade e $I \subseteq R$ um ideal.*

(a) $I[x] \subseteq R[x]$ é um ideal.
(b) $R[x]/I[x] \cong (R/I)[x]$.
(c) $P \subseteq R$ é um ideal primo se, e somente se, $P[x] \subseteq R[x]$ é um ideal primo.

Demonstração. (a) Lembre que $I[x] \subseteq R[x]$ é um subanel. Além disso, como $I \subseteq R$ é um ideal, se $i_0 + i_1 x + \cdots + i_n x^n \in I[x]$ e $r_0 + r_1 x + \cdots + r_m x^m \in R[x]$, então

$$i \cdot r = \sum_{k=0}^{n+m} \left(\sum_{\ell=\max\{0,k-m\}}^{\min\{n,k\}} i_\ell r_{k-\ell} \right) x^k \in I[x].$$

(b) Considere a função $f\colon R[x] \to (R/I)[x]$ dada por

$$f(a_0 + a_1 x + \cdots + a_n x^n) = \overline{a_0} + \overline{a_1} x + \cdots + \overline{a_n} x^n.$$

Observe que f é um homomorfismo de anéis. Além disso,

$$\begin{aligned} \ker(f) &= \{a_0 + a_1 x + \cdots + a_n x^n \in R[x] \mid \overline{a_0} + \overline{a_1} x + \cdots + \overline{a_n} x^n = 0_{(R/I)[x]}\} \\ &= \{a_0 + a_1 x + \cdots + a_n x^n \in R[x] \mid \overline{a_0} + \overline{a_1} x + \cdots + \overline{a_n} x^n = \overline{0} + \overline{0} x\} \\ &= \{a_0 + a_1 x + \cdots + a_n x^n \in R[x] \mid a_0, a_1, \ldots, a_n \in I\} \\ &= I[x]. \end{aligned}$$

Como, para todo $a \in R/I$, existe $x \in R$ tal que $\overline{x} = a$, então f é sobrejetora. Do Primeiro Teorema de Isomorfismo de anéis segue que $R[x]/I[x] = R[x]/\ker(f) \cong \operatorname{im}(f) = (R/I)[x]$.

(c) Lembre do Proposição 17.7 que $P \subseteq R$ é primo se, e somente se, R/P é um domínio. Agora, segue da Proposição 13.1(b) que R/P é domínio se, e somente se, $(R/P)[x]$ é domínio. Pela parte (b) desta proposição, $(R/P)[x] \cong R[x]/P[x]$. Então, segue novamente do Proposição 17.7 que $(R/P)[x]$ é um domínio se, e somente se, $P[x] \subseteq R[x]$ é primo. □

Exemplo 22.2. Dado um corpo $\Bbbk$, lembre que $\Bbbk[x]$ é um domínio, mas não é um corpo. (De fato, $x \in \Bbbk[x]$ é um elemento não-zero que não tem inverso.) Como $\Bbbk$ é um corpo, então $\mathsf{m} = \{0_\Bbbk\} \subseteq \Bbbk$ é um ideal maximal. Mas $\mathsf{m}[x] = \{0_{\Bbbk[x]}\} \subseteq \Bbbk[x]$ não é maximal (apesar de ser primo).

Exemplo 22.3. Considere o domínio $\mathbb{Z}[x]$ e o ideal $I = n\mathbb{Z} \subseteq \mathbb{Z}$. Observe que, neste caso, $I[x] = n\mathbb{Z}[x]$ é o conjunto formado por polinômios cujos coeficientes são inteiros múltiplos de n. (Como multiplicando inteiros por múltiplos de n obtem-se múltiplos de n, nós vemos que $n\mathbb{Z}[x] \subseteq \mathbb{Z}[x]$ é, de fato, um ideal.) Em particular, observe que $nx^i \in n\mathbb{Z}[x]$ para todo $i \in \mathbb{N}$. Então $\overline{nx^i} = \overline{0} \in \mathbb{Z}[x]/n\mathbb{Z}[x]$ para todo $i \in \mathbb{N}$. Logo, em $\mathbb{Z}[x]/n\mathbb{Z}[x]$, podemos reduzir todos os coeficientes módulo n, ou seja, $\mathbb{Z}[x]/n\mathbb{Z}[x] \cong \mathbb{Z}_n[x]$ de fato.

Agora, lembre que $\mathbb{Z}_n[x]$ é um domínio se, e somente se, $\mathbb{Z}_n$ é um domínio. Como todo domínio finito é um corpo (Corolário 12.4), então $\mathbb{Z}_n[x]$ é um domínio se, e somente se, $\mathbb{Z}_n$ é um corpo. Como $\mathbb{Z}_n$ é um corpo se, e somente se, n é primo, então: $\mathbb{Z}_n[x]$ é um domínio se, e somente se, n é primo. Ou seja, de fato, $n\mathbb{Z}[x] \subseteq \mathbb{Z}[x]$ é primo se, e somente se, n é primo.

Definição 22.4. Considere R um anel não-trivial, comutativo, com identidade, e $x_1, \ldots, x_n$ ($n > 0$) variáveis. Defina o anel $R[x_1, x_2, \ldots, x_n]$ indutivamente da seguinte forma:

$$R[x_1, x_2, \ldots, x_n] = (R[x_1, x_2, \ldots, x_{n-1}])\,[x_n].$$

Um elemento de $R[x_1, \ldots, x_n]$ da forma $x_1^{d_1} \cdots x_n^{d_n}$, onde $d_1, \ldots, d_n \geq 0$, é chamado de monômio. (Observe que todo polinômio é uma soma de produtos de elementos de R por monômios.) Dado um elemento da forma $rx_1^{d_1} \cdots x_n^{d_n}$, onde $r \in R$ e $d_1, \ldots, d_n \geq 0$, o seu grau é definido como $d = d_1 + \cdots + d_n$ e seu multigrau é definido como $(d_1, \ldots, d_n) \in \mathbb{N}^n$. O grau de um polinômio é o maior dentre os graus de seus termos. Um polinômio é dito homogêneo (ou uma forma) quando todos os seus termos têm o mesmo grau.

Exemplo 22.5. Considere $\mathbb{Z}[x_1, x_2]$. Observe que seus elementos têm a forma

$$(a_{00} + \cdots + a_{i0}x_1^i) + (a_{01} + \cdots + a_{j1}x_1^j)x_2 + \cdots + (a_{0m} + \cdots + a_{km}x_1^k)x_2^m$$
$$= a_{00} + a_{10}x_1 + a_{01}x_2 + \cdots + a_{km}x_1^k x_2^m,$$

onde $i, j, k, m \geq 0$ e $a_{rs} \in \mathbb{Z}$ para todos $r \in \{0, \ldots, k\}$ e $s \in \{0, \ldots, m\}$. O elemento $x_1^3 x_2$ é um monômio de grau 4 e multigrau $(3, 1)$. O elemento $x_1^2 x_2 + 17x_1 x_2^2 - x_2^3$ é um polinômio homogêneo de grau 3, que não é um monômio. O polinômio $x_1^3 + 2x_1 x_2 + 3x_2^2 + 4x_1 x_2 + 5$ também é um polinômio de grau 3, mas não é homogêneo.

Aula 23

9.3. Anéis de polinômios que são domínios de fatoração única

Lembre que, quando $\Bbbk$ é um corpo, $\Bbbk[x]$ é um domínio Euclidiano (com a norma dada pelo grau). Como consequência, $\Bbbk[x]$ é um domínio principal e de fatoração única. O objetivo desta seção é determinar para quais anéis R, o anel de polinômios $R[x]$ é um domínio de fatoração única.

Vamos começar caracterizando polinômios (ir)redutíveis em $R[x]$. Denote o corpo de frações de R por Q, e lembre que existe um subanel de Q isomorfo a R. Consequentemente, existe uma imagem isomorfa de $R[x]$ dentro de $Q[x]$.

Proposição 23.1 (Lema de Gauss)**.** *Sejam D um domínio de fatoração única, $p \in D[x]$ e denote por Q o corpo de frações de D. Se a imagem de p em $Q[x]$ for redutível, então p é redutível em $D[x]$.*

Demonstração. Suponha que a imagem de p em $Q[x]$ é redutivel, ou seja, existem $a = a_0 + \cdots + a_n x^n \in Q[x] \setminus (Q[x]^\times \cup \{0\})$ e $b = b_0 + \cdots + b_m x^m \in Q[x] \setminus (Q[x]^\times \cup \{0\})$ tais que $p = ab$. Denote por $d_a \in D$ (resp. $d_b \in D$) o produto dos denominadores dos elementos $a_0, \ldots, a_n$ (resp. $b_0, \ldots, b_m$), e observe que $(d_a d_b)p = (d_a a)(d_b b)$, onde $d_a a, d_b b \in D[x] \setminus (D[x]^\times \cup \{0\})$. Como D é um domínio de fatoração única e $d_a d_b \in D$, existem elementos irredutíveis $q_1, \ldots, q_k \in D$ tais que $d_a d_b = q_1 \cdots q_k$. Fixe $i \in \{1, \ldots, k\}$. Como q_i é irredutível e D é um domínio de fatoração única, segue das Proposições 21.1(c) e 22.1(c) que $(q_i) \subseteq D[x]$ é um ideal primo. Como $d_a a d_b b \in (q_i)$, então $d_a a \in (q_i)$ ou $d_b b \in (q_i)$. Isso mostra que: ou $q_i \mid a_j$ para todo $j \in \{0, \ldots, n\}$, ou $q_i \mid b_j$ para todo $j \in \{0, \ldots, m\}$. Sem perda de generalidade, suponha que $q_i \mid a_j$ para todo $j \in \{0, \ldots, n\}$. Como $D[x]$ é um domínio, segue que $d_a a / q_i \in D[x]$. Fazendo isso para cada $i \in \{1, \ldots, n\}$ sucessivamente, concluímos que p é redutível em $D[x]$. □

Corolário 23.2. *Sejam D um domínio de fatoração única, e denote por Q o corpo de frações de D. Um polinômio $p \in D[x]$ é irredutível em $D[x]$ se, e somente se, 1_D for um mdc dos coeficientes de p e p for irredutível em $Q[x]$.*

Demonstração. "Somente se": Pelo Lema de Gauss (contrapositiva da Proposição 23.1), se p for irredutível em $D[x]$, então p é irredutível em $Q[x]$.

"Se": Suponha que p é irredutível em $Q[x]$. Se $a, b \in D[x]$ forem tais que $p = ab$, então $a \in Q[x]^\times$ ou $b \in Q[x]^\times$. Como $Q[x]^\times = Q \setminus \{0\}$, então $a \in D \setminus \{0\}$ ou $b \in D \setminus \{0\}$. Como 1_D é um mdc dos coeficientes de p e todos os seus mdcs são associados, então $a \in D^\times$ ou $b \in D^\times$. Isso mostra que p é irredutível em $D[x]$. □

Teorema 23.3. *Um domínio D é de fatoração única se, e somente se, $D[x]$ é um domínio de fatoração única.*

Demonstração. "Se": Como $D \subseteq D[x]$ é um subanel, toda fatoração em irredutíveis em $D[x]$ induz uma fatoração em irredutíveis em D. Além disso, como $D^\times = D[x]^\times$, dois elementos irredutíveis de D são associados em $D[x]^\times$ se, e somente se, eles são associados em $D^\times$.

"Somente se": Suponha que D é um domínio de fatoração única. Dado $p = a_0 + a_1 x + \cdots + a_n x^n \in D[x] \setminus (D[x]^\times \cup \{0\})$, denote $d = \mathrm{mdc}(a_1, \ldots, a_n) \in D$. Observe que $q = \frac{a_0}{d} + \frac{a_1}{d} x + \cdots + \frac{a_n}{d} x^n \in D[x] \setminus (D[x]^\times \cup \{0\})$, $p = dq$ e $\mathrm{mdc}(\frac{a_0}{d}, \frac{a_1}{d}, \ldots, \frac{a_n}{d}) = 1$. Como D é um domínio de fatoração única, basta mostrarmos que é possível fatorar q em um único (a menos de associados) produto de irredutíveis.

Se q for irredutível em $D[x]$, então o resultado está provado. Caso contrário, ou seja, se q for redutível em $D[x]$, então q é redutível em $Q[x]$. Como Q é um corpo, $Q[x]$ é um domínio de fatoração única. Pelo Lema de Gauss (Proposição 23.1), existem $q_1, \ldots, q_r \in D[x]$ tais que $q = q_1 \cdots q_r$. Como o mdc dos coeficientes de q é 1, então para cada $i \in \{1, \ldots, r\}$, o mdc dos coeficientes de q_i também é 1. Pelo Corolário 23.2, q_i é irredutível para todo $i \in \{1, \ldots, r\}$. Além disso, a escolha de $q_1, \ldots, q_r$ é única a menos de múltiplos por elementos em $Q^\times$. Fixe $i \in \{1, \ldots, r\}$, tome $a \in D$, $b \in D \setminus \{0\}$ e $q_i' = [a, b]q_i$. Como o mdc dos coeficientes de q_i é 1, para que o mdc dos coeficientes de q_i' seja 1, temos que ter $[a, b] \in D^\times$. Isso mostra que a escolha de $q_1, \ldots, q_r$ é única a menos de múltiplos por elementos em $D^\times$. □

O próximo resultado segue direto do teorema anterior.

Corolário 23.4. *Se R for um domínio de fatoração única, então $R[x_1, \ldots, x_n]$ é um domínio de fatoração única.*

Exemplo 23.5. Lembre do Exemplo 19.3 que $\mathbb{Z}$ é um domínio Euclidiano. Então, pela Proposição 19.5 e pelo Teorema 21.10, $\mathbb{Z}$ é um domínio de fatoração única. Logo, pelo corolário acima, $\mathbb{Z}[x]$ também é um domínio de fatoração única. Mas lembre do Exemplo 16.8 que $\mathbb{Z}[x]$ não é um domínio de ideais principais.

Exercício 23.6. Dado um corpo $\Bbbk$, para todo $n > 1$, mostre que $\Bbbk[x_1, \ldots, x_n]$ é um domínio de fatoração única, mas não é um domínio de ideais principais.

9.4. Critérios de irredutibilidade

Proposição 23.7. *Seja $\Bbbk$ um corpo. Um polinômio $p \in \Bbbk[x]$ tem um fator de grau 1 se, e somente se, p tem uma raiz em $\Bbbk$.*

Demonstração. *"Se"*: Suponha que $\alpha \in \Bbbk$ é tal que $p(\alpha) = 0$. Lembre que $\Bbbk[x]$ é um domínio Euclidiano. Então existem $q, r \in \Bbbk[x]$ tais que $p = q \cdot (x - \alpha) + r$, onde $r = 0$ ou $\text{grau}(r) = 0$ (ou seja, $r \in \Bbbk$). Como $0 = p(\alpha) = q(\alpha) \cdot 0 + r = r$, então $r = 0$. Isso mostra que $(x - \alpha)$ divide p.

"Somente se": Suponha que $\alpha x - \beta \in \Bbbk[x]$ seja um fator de grau 1 de p. Em particular, $\alpha \in \Bbbk \setminus \{0\}$. Então, existe $q \in \Bbbk[x]$ tal que $p = q \cdot (\alpha x - \beta)$. Como $p(\alpha^{-1}\beta) = q(\alpha^{-1}\beta) \cdot 0 = 0$, então $\alpha^{-1}\beta \in \Bbbk$ é uma raiz de p. □

Corolário 23.8. *Seja $\Bbbk$ um corpo. Um polinômio $p \in \Bbbk[x]$ de grau 2 ou 3 é redutível se, e somente se, p tem uma raiz em $\Bbbk$.*

Demonstração. *"Se"*: Suponha que p tem uma raiz em $\Bbbk$. Segue da Proposição 23.7 (parte *se*) que p é redutível em $\Bbbk[x]$.

"Somente se": Um polinômio $p \in \Bbbk[x]$ é redutível se, e somente se, existem $a, b \in \Bbbk[x] \setminus \Bbbk$ tais que $p = a \cdot b$. Neste caso, como $\Bbbk$ é um corpo, $\text{grau}(p) = \text{grau}(a) + \text{grau}(b)$. Como $\text{grau}(a), \text{grau}(b) > 0$, se $\text{grau}(p) \in \{2, 3\}$, então $\text{grau}(a) = 1$ ou $\text{grau}(b) = 1$. Pela Proposição 23.7 (parte *somente se*), isso significa que p tem uma raiz em $\Bbbk$. □

Exemplo 23.9. Considere o polinômio $p = x^3 - 3x - 1 \in \mathbb{Z}[x]$. Como $\text{mdc}(1, -3, -1) = 1$, então segue do Corolário 23.2 que p é redutível em $\mathbb{Z}[x]$ se, e somente se, p é redutível em $\mathbb{Q}[x]$. Então, segue do Corolário 23.8 que p é redutível em $\mathbb{Q}[x]$ se, e somente se, p admite uma raiz em $\mathbb{Q}$.

Suponha que $a \in \mathbb{Z}$ e $b \in \mathbb{Z} \setminus \{0\}$ são tais que $\text{mdc}(a, b) = 1$ e $\frac{a^3}{b^3} - 3\frac{a}{b} - 1 = 0$. Então $a^3 - 3ab^2 - b^3 = 0$. Dessa equação seguem que $a^3 = b(3ab - b^2)$ e $b^3 = a(a^2 - 3b^2)$. Como $\text{mdc}(a, b) = 1$, então $a, b \in \mathbb{Z}^\times = \{-1, 1\}$. Como $p(1) = -3 \neq 0$ e $p(-1) = 1 \neq 0$, então p não admite raízes em $\mathbb{Q}$. Com isso, concluímos que p é irredutível em $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$.

Exercício 23.10. Mostre que $x^3 - p$ e $x^2 - p$ são irredutíveis em $\mathbb{Q}[x]$ para todo $p \in \mathbb{Z}$ primo.

Aula 24

9.4. Critérios de irredutibilidade

Definição 24.1. Dado um anel R não-trivial, comutativo e com identidade, um polinômio $a_0 + \cdots + a_n x^n \in R[x]$ de grau $n \geq 0$ é dito mônico quando $a_n = 1_R$.

Proposição 24.2. *Seja $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$. Se $r/s \in \mathbb{Q}$ for uma raiz de $p(x)$ e $\mathrm{mdc}(r, s) = 1$, então $r \mid a_0$ e $s \mid a_n$. Em particular, se $p(x) \in \mathbb{Z}[x]$ for mônico e $r/s \in \mathbb{Q}$ for uma raiz de $p(x)$, então $s = 1$ (ou seja, $r/s \in \mathbb{Z}$) e $r \mid p(0)$.*

Demonstração. Se r/s for raiz de $p(x)$, então $p(r/s) = 0$. Como $s \neq 0$, isso significa que:

$$s^n a_0 + s^{n-1} r a_1 + \cdots + s r^{n-1} a_{n-1} + r^n a_n = 0.$$

Em particular, $s^n a_0 = -r(s^{n-1} a_1 + \cdots + s r^{n-2} a_{n-1} + r^{n-1} a_n)$. Isso implica que $r \mid s^n a_0$. Como $r \nmid s$, então $r \mid a_0$. Analogamente, $r^n a_n = -s(s^{n-1} a_0 + s^{n-2} r a_1 + \cdots + r^{n-1} a_{n-1})$. Isso implica que $s \mid r^n a_n$. Como $s \nmid r$, então $s \mid a_n$. □

Proposição 24.3. *Sejam D um domínio, $I \subsetneq D$ um ideal próprio e $p \in D[x]$ um polinômio mônico não-constante. Se p for redutível em $D[x]$, então existem $\overline{a}, \overline{b} \in (D/I)[x]$ tais que $\mathrm{grau}(\overline{a}), \mathrm{grau}(\overline{b}) < \mathrm{grau}(p)$ e $\overline{p} = \overline{a}\,\overline{b} \in (D/I)[x]$.*

Demonstração. Suponha que $p = p_0 + \cdots + p_{n-1} x^{n-1} + x^n \in D[x]$ é redutível. Isso significa que existem $a = a_0 + \cdots + a_k x^k \in D[x] \setminus (D[x]^\times \cup \{0\})$ e $b = b_0 + \cdots + b_\ell x^\ell \in D[x] \setminus (D[x]^\times \cup \{0\})$ tais que $p = a \cdot b = a_0 b_0 + \cdots + (a_k b_\ell) x^{k+\ell}$. Como D é um domínio, temos que $k + \ell = n$ e $a_k b_\ell = 1_D$. Em particular, $a_k, b_\ell \in D^\times$ e $k, \ell > 0$. Como $I \subsetneq D$ é próprio, então $\overline{a_k}, \overline{b_\ell} \neq \overline{0}_{D/I}$. Logo $0 < \mathrm{grau}(\overline{a}) = k < n$ e $0 < \mathrm{grau}(\overline{b}) = \ell < n$. Além disso, $\overline{p} = \overline{a}\,\overline{b} \in (D/I)[x]$. □

Exemplo 24.4. Considere $D = \mathbb{Z}$ e $x^3 + x + 1 \in \mathbb{Z}[x]$. Pela proposição anterior, se $x^3 + x + 1$ fosse redutível, então existiriam $\overline{a}, \overline{b} \in \mathbb{Z}_2[x]$ polinômios de grau 1 e 2 respectivamente, tais que $\overline{a} \cdot \overline{b} = x^3 + x + \overline{1} \in \mathbb{Z}_2[x]$. Em particular, $x^3 + x + \overline{1}$ teria uma raiz em $\mathbb{Z}_2$. Como $\overline{0}^3 + \overline{0} + \overline{1} = \overline{1}$ e $\overline{1}^3 + \overline{1} + \overline{1} = \overline{1}$, isso mostra que $x^3 + x + \overline{1}$ não tem raiz em $\mathbb{Z}_2$. Logo $x^3 + x + 1 \in \mathbb{Z}[x]$ é irredutível.

Exemplo 24.5. Observe que a volta da Proposição 24.3 não é válida. De fato, como não existe $r \in \mathbb{Z}$ tal que $r^2 = -1$, então pela Proposição 24.2, $x^2 + 1$ é irredutível em $\mathbb{Z}[x]$. No entanto, como $(x + \overline{1})^2 = x^2 + \overline{1}$, então $x^2 + \overline{1} \in \mathbb{Z}_2[x]$ é redutível.

Proposição 24.6 (Critério de Eisenstein)**.** *Sejam D um domínio, $P \subsetneq D$ um ideal primo e $p(x) = a_0 + \cdots + a_{n-1} x^{n-1} + x^n \in D[x]$, $\mathrm{grau}(p(x)) \geq 1$. Se $a_0, \ldots, a_{n-1} \in P$ e $a_0 \notin P^2$, então $p(x)$ é irredutível em $D[x]$.*

Demonstração. Suponha que $r(x) = r_0 + \cdots + r_k x^k \in D[x]$ e $s(x) = s_0 + \cdots + s_\ell x^\ell \in D[x]$ são tais que $p(x) = r(x)s(x) = r_0 s_0 + \cdots + (r_k s_\ell) x^{k+\ell}$. Queremos concluir que $r(x) \in D[x]^\times$ ou $s(x) \in D[x]^\times$. Observe que, como $p(x)$ é mônico, então $r_k, s_\ell \in D^\times$. Portanto, se $\mathrm{grau}(r(x)) = 0$, então $r(x) \in D[x]^\times$, e se $\mathrm{grau}(s(x)) = 0$, então $s(x) \in D[x]^\times$.

Agora suponha que $\mathrm{grau}(r(x)), \mathrm{grau}(s(x)) \geq 1$. Como $r_0 s_0 = a_0 \in P$ e $P \subsetneq R$ é um ideal primo, então $r_0 \in P$ ou $s_0 \in P$. Como D é comutativo, sem perda de generalidade, podemos supor que $r_0 \in P$. Como $r_0 s_0 = a_0 \notin P^2$, então $s_0 \notin P$. Em particular, $s_0 \neq 0_D$. Além disso, como $\mathrm{grau}(s(x)) \geq 1$, então $n = k + \ell > k$. Isso implica que, para todo $i \in \{1, \ldots, k\}$, temos $r_0 s_i + \cdots + r_i s_0 = a_i \in P$. Supondo indutivamente, que $r_0, \ldots, r_{i-1} \in P$, como $s_0 \notin P$, concluímos que $r_i \in P$ para todo $i \in \{1, \ldots, k\}$. Em particular, $r_k \in P \cap D^\times$. Isso implica que $P = D$, o que contradiz o fato de P ser um ideal primo. □

O próximo resultado é um caso particular do Critério de Eisenstein.

Corolário 24.7. *Seja $p = a_0 + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbb{Z}[x]$. Se existe $p \in \mathbb{Z}$ primo tal que $p \mid a_0, \ldots, p \mid a_{n-1}$ e $p^2 \nmid a_0$, então p é irredutível.* □

Exemplo 24.8. Considere $D = \mathbb{Z}$ e $x^4 + 10x + 5 \in \mathbb{Z}[x]$. Como $5 \mid 5$, $5 \mid 10$ e $25 \nmid 5$, então pelo Corolário 24.7, $x^4 + 10x + 5$ é irredutível em $\mathbb{Z}[x]$

Exemplo 24.9. Considere $D = \mathbb{Z}$, $p \in \mathbb{Z}$ um primo, e $\xi_p(x) = 1 + x + \cdots + x^{p-1}$. Esse polinômio é chamado de ciclotômico. Observe que $\xi_p(x) = \dfrac{x^p - 1}{x - 1}$. Observe também que

$$\xi_p(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{k=1}^{p} \binom{p}{k} x^{k-1}.$$

Como $p \mid \binom{p}{k} =: a_{k-1}$ para todo $1 \leq k \leq p-1$, e $p^2 \nmid p = a_0$, então pelo Corolário 24.7, $\xi_p(x+1)$ é irredutível em $\mathbb{Z}[x]$.

Agora, vamos mostrar que $\xi_p(x)$ é irredutível. Suponha que existam $a(x), b(x) \in \mathbb{Z}[x]$ tais que $\xi_p(x) = a(x)b(x)$. Então $a(x+1), b(x+1) \in \mathbb{Z}[x]$ são tais que $a(x+1)b(x+1) = \xi_p(x+1)$. Como $\xi_p(x+1)$ é irredutível, então $a(x+1) \in \{-1, 0, 1\}$ ou $b(x) \in \{-1, 0, 1\}$. No primeiro caso, $a(x) \in \{-2, -1, 0\}$. Como $\xi_p(x)$ é mônico, então $a(x) = -1 \in \mathbb{Z}[x]^\times$. No segundo caso, $b(x) \in \{-2, -1, 0\}$. Como $\xi_p(x)$ é mônico, então $b(x) = -1 \in \mathbb{Z}[x]^\times$. Isso mostra que $\xi_p(x)$ é irredutível em $\mathbb{Z}[x]$.

9.5. Anéis de polinômios sobre corpos

Nesta seção, denote por $\Bbbk$ um corpo. Lembre que $\Bbbk[x]$ é um domínio Euclidiano, de ideais principais e de fatoração única.

Proposição 24.10. *Um ideal $\mathfrak{m} \subseteq \Bbbk[x]$ é maximal se, e somente se, $\mathfrak{m} = (p)$ para algum $p \in \Bbbk[x]$ irredutível.*

Demonstração. Como $\Bbbk[x]$ é um domínio de ideais principais, segue da Proposição 21.1(c) que $\mathfrak{m} \subseteq \Bbbk[x]$ é maximal se, e somente se, $\mathfrak{m} = (p)$ para algum $p \in \Bbbk[x]$ irredutível. □

Exemplo 24.11. Considere um polinômio $p \in \mathbb{C}[x]$ com $\text{grau}(p) = n > 0$. Lembre que p tem n raízes em $\mathbb{C}$. Então, segue da Proposição 23.7 que p é irredutível se, e somente se, $\text{grau}(p) = 1$. Ou seja, os polinômios irredutíveis em $\mathbb{C}[x]$ são da forma $\alpha x + \beta$, onde $\alpha \in \mathbb{C} \setminus \{0\}$ e $\beta \in \mathbb{C}$. Agora, segue da Proposição 24.10 que $\mathbb{C}[x]/(\alpha x + \beta)$ é um corpo. Mostre que existe um isomorfismo de anéis $\mathbb{C}[x]/(\alpha x + \beta) \cong \mathbb{C}$.

Exemplo 24.12. Considere o polinômio $q = x^2 - 2 \in \mathbb{Z}[x]$. Como p é mônico, $2 \mid -2$ e $4 \nmid -2$, segue do Corolário 24.7 que q é irredutível em $\mathbb{Z}[x]$. Como $\mathbb{Z}$ é um domínio de fatoração única e $\mathbb{Q}$ é seu corpo de frações, segue do Lema de Gauss (Proposição 23.1) que q é irredutível em $\mathbb{Q}[x]$. Então, segue da Proposição 24.10 que $\mathbb{Q}[x]/(x^2 - 2)$ é um corpo. Mostre que existe um isomorfismo de anéis $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$.

Exemplo 24.13. Considere o polinômio $r(x) = x^2 + 1 \in \mathbb{R}[x]$. Como $\text{grau}(r) = 2$, segue do Corolário 23.8 que r é redutível se, e somente se, $r(x)$ tem uma raiz em $\mathbb{R}$. Como $r(a) = a^2 + 1 > 0$ para todo $a \in \mathbb{R}$, então $r(x)$ não tem nenhuma raiz em $\mathbb{R}$. Consequentemente, $r(x)$ é irredutível em $\mathbb{R}[x]$. Pela Proposição 24.10, $\mathbb{R}[x]/(x^2 + 1)$ é um corpo. Mostre que existe um isomorfismo de anéis $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Proposição 24.14. *Seja $p \in \Bbbk[x]$ um polinômio tal que* $\operatorname{grau}(p) > 0$. *Se uma fatoração de p em irredutíveis for dada por $p = p_1^{n_1} \cdots p_k^{n_k}$, onde $p_1, \ldots, p_k \in \Bbbk[x]$ são irredutíveis distintos, então existe um isomorfismo de anéis*

$$\frac{\Bbbk[x]}{(p)} \cong \frac{\Bbbk[x]}{(p_1^{n_1})} \times \cdots \times \frac{\Bbbk[x]}{(p_k^{n_k})}.$$

Demonstração. Primeiro, vamos mostrar que $(p_i^{n_i})$ e $(p_j^{n_j})$ são comaximais, ou seja, $(p_i^{n_i}, p_j^{n_j}) = (1)$, para todos $i \neq j \in \{1, \ldots, k\}$. Como $\Bbbk[x]$ é um domínio Euclidiano, então existe $d \in \Bbbk[x]$ tal que $(p_i^{n_i}, p_j^{n_j}) = (d)$. Em particular, $d \mid p_i^{n_i}$ e $d \mid p_j^{n_j}$. Como p_i e p_j são irredutíveis distintos, $d \in \Bbbk[x]^\times$.

Agora, vamos usar o Teorema Chinês dos Restos (Teorema 18.12). Como $(p_i^{n_i})$ e $(p_j^{n_j})$ são comaximais para todos $i \neq j \in \{1, \ldots, k\}$, e $(p) = (p_1^{n_1}) \cdots (p_n^{n_k})$, então existe um isomorfismo de anéis

$$\frac{\Bbbk[x]}{(p)} \cong \frac{\Bbbk[x]}{(p_1^{n_1})} \times \cdots \times \frac{\Bbbk[x]}{(p_k^{n_k})}. \qquad \square$$

Proposição 24.15. *Seja $p(x) \in \Bbbk[x]$ um polinômio de grau $n > 0$. Se $\alpha_1, \ldots, \alpha_k \in \Bbbk$ são raízes de p com multiplicidades $m_1, \ldots, m_k$ respectivamente, então $(x - \alpha_1)^{m_1} \cdots (x - \alpha_k)^{m_k}$ é um fator de $p(x)$. Além disso, $p(x)$ tem no máximo n raízes (contando suas multiplicidades).*

Demonstração. Lembre que $\alpha \in \Bbbk$ é uma raiz de $p(x)$ de multiplicidade m quando $(x - \alpha)^m \mid p$ e $(x - \alpha)^{m+1} \nmid p$. Como $x - \alpha_i$ e $x - \alpha_j$ são irredutíveis distintos (se $i \neq j$), então

$$(x - \alpha_1)^{m_1} \mid p \ , \ (x - \alpha_2)^{m_2} \mid \frac{p}{(x - \alpha_1)^{m_1}} \ , \ \cdots \ , \ (x - \alpha_k)^{m_k} \mid \frac{p}{(x - \alpha_1)^{m_1} \cdots (x - \alpha_{k-1})^{m_{k-1}}}.$$

Isso mostra que $(x - \alpha_1)^{m_1} \cdots (x - \alpha_k)^{m_k}$ é um fator de $p(x)$. Além disso, como $\Bbbk[x]$ é um domínio Euclidiano, se $(x - \alpha_1)^{m_1} \cdots (x - \alpha_k)^{m_k} \mid p(x)$, então $m_1 + \cdots + m_k \leq n = \operatorname{grau}(p)$. $\square$