UNIVERSIDADE ESTADUAL PAULISTA
DEPARTAMENTO DE MATMÁTICA

ÁLGEBRA I

NEUZA KAKUTA
SÃO JOSÉ DO RIO PRETO - 2005

Conteúdo

CAPíTULO 1

Conjuntos

DEFINIÇÃO 0.1. *Sejam A e B conjuntos. Dizemos que A é subconjunto de B e escrevemos $A \subseteq B$ se $\forall x \in A \Rightarrow x \in B$.*

Claramente $\emptyset \subseteq A$ e $A \subseteq A$ para todo A.

DEFINIÇÃO 0.2. *Sejam A e B conjuntos. Dizemos que eles são iguais se $A \subseteq B$ e $B \subseteq A$. Neste caso escrevemos $A = B$.*

Operações entre conjuntos

Sejam X um conjunto universal e $A, B \subseteq X$.

DEFINIÇÃO 0.3. *A união de A com B é o conjunto*

$$A \cup B := \{x \in X \mid x \in A \text{ ou } x \in B\},$$

e interseção de A com B é

$$A \cap B := \{x \in X \mid x \in A \text{ e } x \in B\}.$$

PROPOSIÇÃO 0.4. *Sejam $A, B, C \subseteq X$. Então temos:*

(1) $A \subseteq A \cup B$ *e* $B \subseteq A \cup B$
(2) $A \cap B \subseteq A$ *e* $A \cap B \subseteq B$
(3) $A \cup B = B \cup A$ *e* $A \cap B = B \cap A$
(4) $A \cup \emptyset = A$ *e* $A \cap \emptyset = \emptyset$
(5) $A \cup (B \cup C) = (A \cup B) \cup C$ *e* $A \cap (B \cap C) = (A \cap B) \cap C$
(6) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *e* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

DEFINIÇÃO 0.5. *Sejam $A, B \subseteq X$. A diferença entre A e B é:*

$$A \setminus B := \{x \in X \mid x \in A \text{ e } x \notin B\}.$$

O conjunto $A^c := X \setminus A$ é chamado de complementar de A.

PROPOSIÇÃO 0.6. *Sejam $A, B \subseteq X$.*

(1) *Leis de Morgan:*
   (a) $(A \cup B)^c = A^c \cap B^c$
   (b) $(A \cap B)^c = A^c \cup B^c$
(2) $A \setminus B = A \cap B^c$.
(3) $(A^c)^c = A$
(4) $X^c = \emptyset$.
(5) $\emptyset^c = X$.
(6) $A \cap A^c = \emptyset$.
(7) $A \cup A^c = X$.

0.1. Exercícios. Sejam $A, B \subseteq X$. Prove que são equivalentes:

(1) $A \subseteq B$
(2) $A \cap B^c = \emptyset$
(3) $A \cup B = B$
(4) $B^c \subseteq A^c$
(5) $A \cap B = A$

Definição 0.7. *Sejam $A, B \subseteq X$. A diferença simétrica entre A e B é definida por*

$$A\Delta B := (A \setminus B) \cup (B \setminus A).$$

Proposição 0.8. *Sejam $A, B, C \subseteq X$. Então:*

(1) $A\Delta B = B\Delta A$
(2) $A\Delta A = \emptyset$
(3) $A\Delta\emptyset = A$
(4) $A\Delta B = (A \cap B^c) \cup (A^c \cap B)$
(5) $(A\Delta B)^c = (A^c \cap B^c) \cup (A \cap B)$
(6) $(A\Delta B) \cap C = (A \cap C)\Delta(B \cap C)$
(7) $(A\Delta B)\Delta C = A\Delta(B\Delta C)$

Demonstração. □

Definição 0.9. *(União e Interseção Generalizadas) Seja $\{A_i\}_{i\in I}$ uma família de subconjuntos de X. Por definição*

$$\bigcup_{i\in I} A_i = \{x \mid \exists i \text{ tal que } x \in A_i\}$$

e

$$\bigcap_{i\in I} A_i = \{x \mid \forall i, x \in A_i\}$$

DEFINIÇÃO 0.10. *Sejam A e B conjuntos. O produto cartesiano entre A e B é $A \times B := \{(a,b) \mid a \in A \text{ e } b \in B\}$. Se $\{A_i\}_{i\in I}$ uma família de conjuntos, então*

$$\prod_{i=1}^{n} A_i = \{(a_1, \ldots, a_n) \mid a_i \in A_i, \forall i = 1, \ldots, n\}$$

e

$$\prod_{i\in I} A_i = \{(a_i)_{i\in I} \mid a_i \in A_i, \forall i \in I\}.$$

DEFINIÇÃO 0.11. *Seja A um conjunto. Então o conjunto de todos os subconjuntos de A é chamado de partes de A. Este conjunto é denotado por $\wp(A) := \{Y \mid Y \subseteq A\}$.*

Claramente se $\#A = n$ então $\#\wp(A) = 2^n$.

PROPOSIÇÃO 0.12. *Sejam A e B conjuntos.*

(1) $\wp(A) \neq \emptyset$
(2) $A \subseteq B \Leftrightarrow \wp(A) \subseteq \wp(B)$

0.2. Exercícios.

(1) Se para todo $B \subseteq X$, $A \cap B = \emptyset$ então $A = \emptyset$.
(2) Se para todo $B \subseteq X$, $A \cup B = X$ então $A = X$.
(3) Sejam $A, B \subseteq X$. Prove que são equivalentes as afirmações
   (a) $A \subseteq B$
   (b) $A \cap B^c = \emptyset$
   (c) $A \cup (B \setminus A) \subseteq B$
(4) Sejam $A, B \subseteq X$. Mostre que
   (a) $\wp(A \cap B) = \wp(A) \cap \wp(B)$
   (b) $\wp(A) \cup \wp(B) \subseteq \wp(A \cup B)$
(5) Sejam $\{A_i\}_{i\in I}$ uma família de conjuntos e X um conjunto. Mostre que
   (a) $X \cap (\bigcup_{i\in I} A_i) = \bigcup_{i\in I}(X \cap A_i)$.
   (b) $X \cup (\bigcap_{i\in I} A_i) = \bigcap_{i\in I}(X \cup A_i)$.
   (c) $X \setminus (\bigcup_{i\in I} A_i) = \bigcap_{i\in I}(X \setminus A_i)$.
   (d) $X \setminus (\bigcap_{i\in I} A_i) = \bigcup_{i\in I}(X \setminus A_i)$.

(6) Sejam $A, B, C, D \subseteq X$. Prove:

(a) $A\Delta B = (A \cup B) \setminus (A \cap B)$.

(b) $(A \times C) \cup (B \times D) \subseteq (A \cup B) \times (C \cup D)$.

(c) $(C \times D) \setminus (A \times B) = (C \times (D \setminus B)) \cup ((C \setminus A) \times D)$.

CAPíTULO 2

A Aritmética dos Inteiros

A Teoria dos Números Inteiros se embasa em três princípios fundamentais: Princípio da Boa ordem e os Princípios da Indução Finita.

1. Princípio da Boa Ordem e Indução Finita

Princípio da Boa Ordem (P.B.O.) Todo subconjunto não vazio e limitado inferiormente de $\mathbb{Z}$, possui um mínimo.

O princípio acima é equivalente a:

(P.B.O.)' Todo subconjunto não vazio limitado superiormente de $\mathbb{Z}$, possui um máximo.

Isto segue do seguinte fato: S é limitado inferiormente se, e somente se, $-S$ é limitado superiormente, onde $-S = \{-x \in \mathbb{Z} \mid x \in S\}$.

Teorema 1.1. *(Primeiro Princípio da Indução Finita (PIF)) Dado $n_0 \in \mathbb{N}$, seja $P(n)$ uma sentença associada a cada $n \in \mathbb{N}$, com $n \geq n_0$. Se as condições abaixo são verificadas*

(1) *$P(n_0)$ é verdadeira.*

(2) *Se $P(k)$ é verdadeira para $k \geq n_0$, então $P(k+1)$ também é verdadeira.*

Então $P(n)$ é verdadeira para todo $n \in \mathbb{N}$ tal que $n \geq n_0$.

Demonstração. Veja Apêndice 1. □

Substituindo-se (2) por

(2)' Dado $r > n_0$, se $P(k)$ é verdadeira para todo k, $n_0 \leq k < r$, então $P(r)$ também é verdadeira.

O princípio se mantém verdadeiro e será chamado de *Segundo Princípio da Induçã Finita.*

1.1. Exercícios. Mostre que para todo $n \in \mathbb{N}$,

(1) $1 + \cdots + n = \frac{n(n+1)}{2}$

(2) $1 + 3 + \cdots + (2n-1) = n^2$

(3) $n^2 \geq n + 1$

(4) $1^3 + \cdots + n^3 = (1 + \cdots + n)^2$

(5) $1(1+1)+\ldots n(n+1)=\frac{n(n+1)(n+2)}{3}$

(6) $(1+\cdots+n)^2=\frac{n(n+1)(2n+1)}{6}$

2. Divisibilidade

DEFINIÇÃO 2.1. *Dados $a,b\in\mathbb{Z}$. Dizemos que a divide b se existe $q\in\mathbb{Z}$ tal que $b=a.q$. Neste caso escrevemos $a\mid b$. Caso contrário escrevemos $a\nmid b$.*

PROPOSIÇÃO 2.2. *Dados $a,b,c\in\mathbb{Z}$, então*

(1) *$a\mid 0$ e $a\mid a$.*

(2) *Se $a\mid b$ então $a\mid bc$.*

(3) *Se $a\mid b$ e $b\mid c$ então $a\mid c$.*

(4) *Se $a\mid b$ e $a\mid c$ então $a\mid b\pm c$.*

(5) *Se $a|b$ e $b|a$ então $a=\pm b$.*

DEFINIÇÃO 2.3. *Seja $p\in\mathbb{Z}$ tal que $p\neq 0,\pm 1$. Dizemos que p é um número primo se os únicos divisores de p são 1 e p.*

TEOREMA 2.4. *(Teorema Fundamental da Arimética (TFA)) Seja $a\in\mathbb{Z}$ tal que $a\neq 0,\pm 1$. Então existem únicos números primos positivos $p_1,\ldots,p_n$ (a menos da ordem) tais que $a=\pm p_1\cdots p_n$.*

DEMONSTRAÇÃO. Veja Apêndice 1. □

TEOREMA 2.5. *(Euclides) Existe um número infinito de números primos.*

DEMONSTRAÇÃO. Suponha por absurdo que existe um número finito de números primos, a saber: $p_1,\ldots,p_n$. Seja $a=p_1\cdots p_n+1$. Como $a\neq 0,\pm 1$ segue pelo TFA que

$$a={p_1}^{m_1}\cdots{p_n}^{m_n},m_1,\ldots,m_n\in\mathbb{N}$$

Sendo $a\neq\pm 1$, existe algum $m_i>0$ e portanto $p_i\mid p_1\cdots p_n+1$ e $p_i|p_1\cdots p_n$ então $p_i\mid 1$ (absurdo!). □

2.1. Exercícios. Sejam $a,b,c,d\in\mathbb{Z}$.

(1) Se $a\mid b$ e $c\mid d$. Então $ac\mid bd$.

(2) Se p um número primo tal que $p\mid ab$, então $p\mid a$ ou $p\mid b$.

(3) Para todo p número primo, $\sqrt{p}\notin\mathbb{Q}$.

TEOREMA 2.6. *(Algoritmo da Divisão de Euclides) Sejam $a, b \in \mathbb{Z}$ tais que $b \neq 0$. Então existem únicos $q, r \in \mathbb{Z}$ tais que $a = bq + r$ com $0 \leq r < |b|$.*

DEMONSTRAÇÃO. Se $a \geq 0$, existe $n \in \mathbb{N}$ tal que $n|b| \leq a < (n+1)|b|$ e então $0 \leq a - n|b| < |b|$. Tomando-se $r = a - n|b|$ temos que $a = n|b| + r$ com $0 \leq r < |b|$.

Se $a < 0$, existe $n \in \mathbb{N}$ tal que $-(n+1)|b| \leq a < -n|b|$ e então $0 \leq a + (n+1)|b| < |b|$. Tomando-se $r = a + (n+1)|b|$ temos que $a = -(n+1)|b| + r$ com $0 \leq r < |b|$.

Para a unicidade, suponha que $a = b.q + r$ e $a = b.q' + r'$, com $0 \leq r, r' < |b|$, então $b.q + r = b.q + r'$ ou seja $b(q - q') = r' - r$ então $b \mid r - r'$. Como $|r' - r| < |b|$ obtemos $r' - r = 0$, ou $r' = r$, logo $q = q'$. □

DEFINIÇÃO 2.7. *Dados $a, b \in \mathbb{Z}$. Um número inteiro d é o máximo divisor comum de a e b se*

(1) *$d \mid a$ e $d \mid b$,*
(2) *Se $d' \in \mathbb{Z}$ tal que $d' \mid a$ e $d' \mid b$ então $d' \mid d$,*
(3) *$d \geq 0$.*

Neste caso escrevemos $d = mcd(a, b)$.

DEFINIÇÃO 2.8. *Dizemos que a e b são primos entre si ou relativamente primos se $mcd(a, b) = 1$.*

DEFINIÇÃO 2.9. *Dados $a, b \in \mathbb{Z}$. Um número inteiro m é o mínimo múltiplo comum de a e b se*

(1) *$a \mid m$ e $b \mid m$,*
(2) *Se $m' \in \mathbb{Z}$ tal que $a \mid m'$ e $b \mid m'$ então $d \mid m'$,*
(3) *$m \geq 0$.*

Neste caso escrevemos $m = mmc(a, b)$.

Observações

(1) $mdc(0, 0) = 0$, $mmc(0, 0) = 0$.
(2) Para todo $a \neq 0$, $mdc(0, a) = |a|$.
(3) $mdc(a, b) = mdc(|a|, |b|)$ e $mmc(a, b) = mdc(|a|, |b|)$.

2.2. Exercícios. Sejam $a, b \in \mathbb{Z} \setminus \{0\}$ e $d = mdc(a, b)$.

(1) $mdc(\frac{a}{d}, \frac{b}{d}) = 1$.

(2) Se $m = mmc(a, b)$ então $ab = \pm dm$.

TEOREMA 2.10. *Sejam $a, b \in \mathbb{Z} \setminus \{0\}$. Seja r o resto da divisão de a por b. Então*

(1) $mdc(a, b) = |b|$ *se* $r = 0$,

(2) $mdc(a, b) = mdc(b, r)$ *se* $r > 0$.

DEMONSTRAÇÃO. Como r é o resto da divisão de a por b temos que $a = bq + r$, com $0 \leq r < b$. Se $r = 0$ então $b \mid a$ e $mdc(a, b) = |b|$. Se $r > 0$, sejam $d = mdc(a, b)$ e $d' = mdc(b, r)$. Temos

$$d \mid a \text{ e } d|b \Rightarrow d \mid a - bq \Rightarrow d \mid r \Rightarrow d|d'$$

e

$$d' \mid b \text{ e } d' \mid r \Rightarrow d' \mid bq \text{ e } d' \mid a - bq \Rightarrow d' \mid a \Rightarrow d'|d.$$

De $d, d' > 0$ com $d \mid d'$ e $d' \mid d$ segue que $d = d'$. □

2.3. Exercícios. Sejam $a, b \in \mathbb{Z} \setminus \{0\}$. Prove:

(1) Se p um número primo tal que $p \nmid a$ então $mdc(a, p) = 1$.

(2) Para todo $n \in \mathbb{Z}$, seja $n\mathbb{Z} := \{nx \mid x \in \mathbb{Z}\}$. Se $m = mmc(a, b)$, então $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

TEOREMA 2.11. *(Algoritmo de Euclides para cálculo de mdc) Sejam $a, b \in \mathbb{Z} \setminus \{0\}$. Suponha que $a = bq_1 + r_1, b = r_1q_2 + r_2, r_1 = r_2q_3 + r_3, \ldots, r_{n-1} = r_nq_{n+1} + r_{n+1}$ com $r_{n+1} = 0$. Então $mdc(a, b) = r_n$.*

DEMONSTRAÇÃO. Aplicando-se o teorema acima item (2) sucessivamente obtemos $mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2) = \cdots = mdc(r_{n-1}, r_n)$. Sendo $r_{n+1} = 0$ temos que $r_n \mid r_{n-1}$ e então pelo item (1) do teorema acima, $mdc(r_{n-1}, r_n) = r_n$. Donde segue que $mdc(a, b) = r_n$. □

TEOREMA 2.12. *(Identidade de Bézout) Sejam $a, b \in \mathbb{Z}$ e $d = mdc(a, b)$. Então existem $r, s \in \mathbb{Z}$ tais que $d = ra + sb$.*

DEMONSTRAÇÃO. Temos 3 casos:

Caso 1. $a = b = 0$. Neste caso $d = 0 = 0.a + 0.b$.

Caso 2. $b = 0$ e $a \neq 0$. Temos $d = |a| = \pm 1.a + 0.b$.

Caso 3. $b \neq 0$ e $a \neq 0$. Sendo $mdc(a, b) = mdc(|a|, |b|)$, podemos supor que $a > 0$ e $b > 0$. Seja $I = \{xa + yb \mid x, y \in \mathbb{Z}\} \cap \mathbb{N}$. Como $a = 1.a + 0.b$ segue que $I \neq \emptyset$ e I é limitado inferiormente pois $I \subseteq \mathbb{N}$. Assim pelo P.B.O., existe $\delta := \min I$. Então $\delta > 0$ e existem $r, s \in \mathbb{Z}$ tais que $\delta = ra + sb$. Mostremos que $\delta = d$.

Inicialmente provemos que $\delta \mid a$ e $\delta \mid b$. Como $\delta > 0$ e $a \in \mathbb{Z}$ então pelo algoritmo da divisão, $a = \delta q + r$, onde $0 \leq r < \delta$. Assim

$$r = a - \delta q = a - (ra + sb)q = (1 - rq)a + (-sq)b.$$

Sendo $\delta = \min I$ com $\delta > 0$ e $0 \leq r < \delta$ concluímos que $r = 0$. Portanto $a = \delta q$ ou seja $\delta \mid a$. Analogamente prova-se que $\delta \mid b$.

Como $\delta \mid a$ e $\delta \mid b$ e $d = mdc(a, b)$ segue que $\delta \mid d$.

Por outro lado

$$d = mdc(a, b) \Rightarrow d \mid a \text{ e } d \mid b \Rightarrow d \mid ra \text{ e } d \mid sb \Rightarrow d \mid ra + sb = \delta \Rightarrow d \mid \delta.$$

Das conclusões $d \mid \delta$ e $\delta \mid d$ com $\delta > 0$ e $d > 0$ segue que $\delta = d$. □

2.4. Exercícios. Sejam $a, b, c, m, n \in \mathbb{Z}$.

(1) Se $a \mid c$, $b \mid c$ e $mdc(a, b) = d$, então $ab \mid cd$.
(2) Se $mdc(a, b) = 1$ e $mdc(a, c) = d$ então $mdc(a, bc) = d$.
(3) Se existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$, então $mdc(a, b) = 1$.
(4) Seja p um número primo tal que $p \mid ab$ então $p \mid a$ ou $p \mid b$.
(5) Se p e q são dois números primos distintos tais que $p \mid a$ e $q \mid a$, mostre que $pq \mid a$.
(6) Sejam $m, n \in \mathbb{Z} \setminus \{0\}$ e $mdc(m, n) = 1$, então $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$
(7) $mdc(2n + 1, \frac{n(n+1)}{2}) = 1$.
(8) $mdc(ac, bc) = |c|.mdc(a, b)$.
(9) $mdc(a, b) = mdc(a + bc, a + b(c - 1))$.
(10) Se $mdc(b, c) = 1$ então $mdc(a, bc) = mdc(a, b).mdc(a, c)$.
(11) Se $mdc(a, 4) = mdc(b, 4) = 2$ então $mdc(a.b, 4) = 4$.
(12) $mdc(a + b, b) = 1 \Leftrightarrow mdc(a, b) = 1$.
(13) $mdc(a, b) = mdc(a + nb, b)$.

3. Equação Diofantina Linear

Toda equação do tipo $ax + by = c$, onde $a, b, c \in \mathbb{Z}$, é chamada de *equação diofantina linear em duas variáveis.*

Teorema 3.1. *Seja $a, b, c \in \mathbb{Z}$ e $mdc(a, b) = d$. A equação diofantina $ax + by = c$ tem solução inteira se e somente se $d \mid c$. Se (x_0, y_0) é uma solução, então todas as soluções são dadas por $x = x_0 + \frac{b}{d}t, y = y_0 - \frac{a}{d}t, t \in \mathbb{Z}$.*

DEMONSTRAÇÃO. Se (x_0, y_0) é uma solução de equação então $ax_0 + by_0 = c$. Como $d = mdc(a, b)$ obtemos $d \mid c$.

Agora seja $d \mid c$ então $c = dq$ para algum $q \in \mathbb{Z}$. Pela Identidade de Bézout, existem $r, s \in \mathbb{Z}$ tais que $d = ra + sb$. Então

$$c = dq = (ra + sb)q = (rq)a + (sq)b.$$

Ou seja (rq, sq) é uma solução.

Para obter todas as soluções, seja (x, y) uma outra solução, então

$$c = ax + by = ax_0 + by + 0 \Rightarrow a(x - x0) = b(y0 - y).$$

Como $d = mdc(a, b)$ existem $q, q' \in \mathbb{Z}$ tais que $a = dq$, $b = dq'$ e $mdc(q, q') = 1$. Então

$$dq(x - x_0) = dq'(y_0 - y) \Rightarrow q(x - x_0) = q'(y_0 - y) \Rightarrow$$

$$q \mid q'(y_0 - y) \text{ e } q' \mid q(x - x_0).$$

Como $mdc(q, q') = 1$ concluímos que $q|y_0 - y$ e $q' \mid x - x_0$. Daí existem $t, t' \in \mathbb{Z}$ tais que $x - x_0 = q't'$ e $y_0 - y = qt$, mas como $q(x - x_0) = q'(y_0 - y)$, temos $t = t'$ e obtemos $x = x_0 + \frac{b}{d}t$ e $y = y_0 - \frac{a}{d}t$. □

Exemplos.

(1) Determine todas as soluções da equação diofantina $172x + 20y = 1000$.

Como $mdc(172, 20) = 4$ e $4 \mid 1000$, a equação tem solução. Multiplicando $4 = 172.2 + 20.(-17)$ por $250 = 1000/4$ obtemos $1000 = 172.(500) + 20.(-4250)$. Então uma solução é $(500, -4250)$, portanto

$$x = 500 + (20/4)t, y = -4250 - (172/4)t, t \in \mathbb{Z}$$

é a solução geral da equação.

(2) Determine o menor inteiro positivo que dividido por 8 e por 15 deixa restos 6 e 13, respectivamente.

Seja $a \in \mathbb{Z}$ tal que $a = 8x + 6$ e $a = 15y + 13$. Então, $8x + 6 = 15y + 13$ ou seja $8x - 15y = 7$. Como $mdc(8, 15) = 1$, a equação diofantina $8x - 15y = 7$ tem solução. Claramente $(14, 7)$ é uma solução particular e $x = 14 - 15t$, $y = 7 - 8t$, $t \in \mathbb{Z}$ são todas as soluções. Para $t = 0$ temos que x é o menor inteiro tal que a $a > 0$ Assim, $a = 8x + 6 = 8.14 + 6 = 118$ é o número procurado.

4. Congruências

DEFINIÇÃO 4.1. *Seja $m \in \mathbb{Z}$, $m > 1$. Dizemos que $a, b \in \mathbb{Z}$ são congruentes e screvemos $a \equiv b(mod m)$ se $m|a - b$.*

PROPOSIÇÃO 4.2. *Sejam $a, b, c \in \mathbb{Z}$.*

(1) $a \equiv a(mod m)$.
(2) *Se* $a \equiv b(mod m)$ *então* $b \equiv a(mod m)$.
(3) *Se* $a \equiv b(mod m)$ *e* $b \equiv c(mod m)$ *então* $a \equiv c(mod m)$.
(4) *Se* $a \equiv b(mod m)$ *e* $c \equiv d(mod m)$ *então* $a + c \equiv b + d(mod m)$ *e* $ac \equiv bd(mod m)$. *(Em particular* $a \equiv b(mod m) \Rightarrow ac \equiv bc(mod m)$*)*
(5) *Se* $a \equiv b(mod m)$ *então* $a^n \equiv b^n(mod m)$, *para todo* $n \in \mathbb{N}$.
(6) *Se* $a \equiv b(mod m)$ *então os restos da divisão de* a *por* m *e de* b *por* m *são iguais.*

4.1. Exercícios.

(1) Determine o resto da divisão de 37^5 por 17.
(2) Mostre que para todo $n \in \mathbb{N}$
   (a) $2 \mid 3^n - 1$.
   (b) $3 \mid n(n^2 - 1)$.
   (c) $3^{2n+1} + 2^{n+2}$ é divisível por 7.
   (d) $3^{4n+2} + 2.4^{3n+1}$ é divisível por 17.
   (e) $2^{2n-1}3^{n+2} + 1$ é divisível por 11.
(3) Sejam $a, b, m, n \in \mathbb{Z}$. Prove:
   (a) $a \equiv b(mod m)$ e $mdc(c, m) = d$ então $a \equiv b(mod \frac{m}{d})$
   (b) Se $mdc(m, n) = 1$ então $a \equiv b(mod m)$ e $a \equiv b(mod n)$ se e somente se $a \equiv b(mod mn)$.
   (c) $a^3 \equiv a(mod 3)$.
   (d) $a \equiv b(mod 3) \Leftrightarrow a^3 \equiv b^3(mod 3)$.

4.2. Critérios de Divisibilidade. Seja $a = \overline{a_n a_{n-1} \cdots a_0} \in \mathbb{N}$. A expansão de a na base decimal é dada por

$$a = a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n, 0 \leq a_i < 9, i = 0, \ldots, n.$$

(1) a é divisível por $2 \Leftrightarrow 2 \mid a_0$.
(2) a é divisível por $3 \Leftrightarrow 3 \mid a_0 + a_1 + \cdots + a_n$.

4.3. Exercícios.

(1) (a) a é divisível por 9 se e somente se $9 \mid a_0 + a_1 + \cdots + a_n$.

(b) a é divisível por 5 se e somente se $a_0 = 0$ ou $a_0 = 5$.

(c) a é divisível por 10 se e somente se $a_0 = 0$.

(d) a é divisível por 4 se e somente se $4 \mid \overline{a_1 a_0} = a_0 + a_1 10$.

(e) a é divisível por 11 se e somente se $11 \mid a_0 - a_1 + a_2 - \cdots + (-1)^n a_n$.

(2) Exprima 100 como soma de dois inteiros positivos de modo que o primeiro seja divisível por 7 e o segundo divisível por 11.

(3) Determine $x, y \in \mathbb{Z}$ tais que $x + y$ seja o menor inteiro positivo que satisfaz $18x + 5y = 48$. (Resp: 1 e 6)

(4) Seja p um número primo. Prove que: se $p \nmid c$ e $ac \equiv bc(mod p)$ então $a \equiv b(mod p)$.

(5) Seja $a \in \mathbb{Z}$ tal que $mdc(a, 4) = 2$. Mostre que $a \equiv 2(mod 4)$.

(6) Determine $r, s \in \mathbb{Z}$ tais que $10 = 390r + 70s$.

(7) Ache o algarismo das unidades de 9^{9^9} e 7^{7^7}.

(8) Mostre que $6 \mid n(2n + 7)(7n + 1)$ e $30 \mid n(n^2 - 49)(n^2 + 49)$, para todo $n \in \mathbb{N}$.

(9) Sejam $a, b, c \in \mathbb{N}$ primos entre si, tais que $a^2 + b^2 = c^2$. Mostre que

(a) a ou b é par.

(b) a ou b é múltiplo de 3.

(10) Seja $a \in \mathbb{Z}$ tal que $5 \nmid a$. Mostre que $a^4 \equiv 1(mod 5)$.

(11) Num cassino existem duas espécies de fichas, uma de $62,00$ e outra de $11,00$ reais. De quantas e quais são as possíveis maneiras de se obter $788,00$ reais.

CAPíTULO 3

Relações de Equivalência e de Ordem

DEFINIÇÃO 0.3. *Sejam A e B conjuntos não vazios. Todo conjunto $R \neq \emptyset$, $R \subseteq A \times B$ é chamado de relação binária de A em B. Diremos que R é uma relação sobre A se $R \subseteq A \times A$.*

Notação. Escrevemos aRb em vez de $(a, b) \in R$ e diremos que a está relacionado com b. Caso $(a, b) \notin R$, escrevemos $a \not R b$.

DEFINIÇÃO 0.4. *Seja R é uma relação sobre A.*

(1) *R é reflexiva se $\forall a \in A, aRa$.*
(2) *R é simétrica se $aRb \Rightarrow bRa$.*
(3) *R é transitiva se aRb e $bRc \Rightarrow aRc$.*
(4) *R é anti-simétrica se aRb e $bRa \Rightarrow a = b$.*

DEFINIÇÃO 0.5. *Diremos que R é uma relação de equivalência se R é reflexiva, simétrica e transitiva; e que R é uma relação de ordem se R é reflexiva, anti-simétrica e transitiva.*

Exemplos.

(1) Seja $a, b, m \in \mathbb{Z}$, $m > 1$. A relação definida por

$$a \equiv b(mod m) \Leftrightarrow m \mid a - b$$

sobre $\mathbb{Z}$ é de equivalência.

(2) A relação de "divisibilidade"sobre $\mathbb{N}$ é uma relação de ordem.
(3) Sejam $a, b \in \mathbb{R}$. Define-se $a \leq b$ se existe $c \in \mathbb{R}^+$ tal que $b = a + c$. Esta relação é uma relação de ordem sobre $\mathbb{R}$, chamada de ordem "abitual","natural"ou "usual"sobre $\mathbb{R}$.
(4) Seja $\prod$ um plano e sejam as retas $r, s \in \prod$. Define-se

$$r \parallel s \text{ se } r = s \text{ ou } r \cap s = \emptyset.$$

A relação de "paralelismo"é uma relação de equivalência.

(5) Seja X um conjunto. A relação de inclusão sobre $\wp(X)$ é uma relação de ordem.

1. Relação de Equivalência

DEFINIÇÃO 1.1. *Seja R uma relação de equivalência sobre A. Para cada $a \in A$, define-se*

$$\bar{a} := \{x \in A \mid aRx\}.$$

Este conjunto é chamado de classe de equivalência de a.

PROPOSIÇÃO 1.2. *Seja R uma relação de equivalência sobre A. Sejam $a, b \in A$ então,*

(1) $\bar{a} \neq \emptyset$.
(2) $a \in \bar{b} \Leftrightarrow \bar{a} = \bar{b}$.
(3) $\bar{a} = \bar{b}$ *ou* $\bar{a} \cap \bar{b} = \emptyset$.
(4) $\bigcup_{a \in A} \bar{a} = A$.

DEFINIÇÃO 1.3. *Denotamos por $A/R := \{\bar{a} \mid a \in A\}$ o conjunto das classes de equivalência e será chamada de conjunto quociente, termo que justifica o fato que R "particiona"o conjunto A em subconjuntos não vazios e disjuntos.*

Exemplos.

(1) Seja a relação "$\equiv modm$" sobre $\mathbb{Z}$. Temos que

$$\bar{a} = \{b \in \mathbb{Z} \mid a \equiv b(modm)\}.$$

Seja r o resto da divisão de a por m então existe $q \in \mathbb{Z}$ tal que $a = mq + r$, $0 \leq r < m$. Assim, $a \equiv r(modm)$ com $0 \leq r < m$ ou seja $a \in \bar{r}$. Pela propriedade (2) temos que $\bar{a} = \bar{r}$ e pela propriedade (3), $\bar{0}, \ldots, \bar{m}$ são distintos. Assim, $\bar{a} \in \{\bar{0}, \ldots, \bar{m}\}$ e portanto, $\{\bar{a} \mid a \in \mathbb{Z}\} = \{\bar{0}, \ldots, \bar{m}\}$. O conjunto quociente será chamado de conjunto das classes dos restos módulo m e será denotado por $\mathbb{Z}_m := \{\bar{0}, \ldots, \bar{m}\}$.

(2) Sejam $u, v \in \mathbb{R}^2$ e defina $uRv \Leftrightarrow \exists \lambda \in \mathbb{R} \setminus \{0\}$ tal que $u = \lambda v$. Temos que R é uma relação de equivalência e

$$\bar{v} = \{u \in \mathbb{R}^2 \mid u = \lambda v \text{ para algum } \lambda \in \mathbb{R} \setminus \{0\}\}.$$

Note que $\bar{v} = \{(0,0)\}$ se $v = (0,0)$ e que se $v \neq (0,0)$, $\bar{v}$ é uma reta sem a origem, na direção do vetor v. Note que $\mathbb{R}^2$ é a reunião de todas essas retas paralelas com a origem.

2. Relação de Ordem

Seja $\preceq$ uma relação de ordem sobre A. Nesse caso diremos que $(A, \preceq)$ é *parcialmente ordenado*.

Quando $a \preceq b$ escrevemos também $b \succeq a$.

Diremos que A é *totalmente ordenado* se para quaisquer $a, b \in A$ uma das três alternativas abaixo ocorre:

$$a \prec b \text{ ou } a = b \text{ ou } b \prec a.$$

Ou seja, quaisquer dois elementos de A são comparáveis.

Exemplos.

(1) $(\mathbb{R}, \leq)$ é totalmente ordenado pela ordem usual.
(2) Seja $X = \{1, 2, 3\}$. Temos que $(\wp(X), \subseteq)$ é parcialmente ordenado, mas não é totalmente ordenado, pois $\{1, 2\}$ e $\{3\}$ não são comparáveis.

Definição 2.1. *Sejam $(A, \preceq)$ parcialmente ordenado e $\emptyset \neq X \subseteq A$. Dizemos que:*

(1) *X é limitado superiormente (resp. limitado inferiormente) se*

$$\exists a \in A \text{ tal que } x \preceq a, \forall x \in X (resp. a \preceq x, \forall x \in X).$$

Todo $a \in A$ tal que $x \preceq a$, para todo $x \in X$ (resp. $a \preceq x$, para todo $x \in X$) é chamado de limite superior de X ou majorante de X (resp. limite inferior de X ou minorante de X).

Denotamos por

$$\limsup X = \{a \in A \mid x \preceq a, \text{ para todo } x \in X\}$$

e

$$\liminf X = \{a \in A \mid a \preceq x, \text{ para todo } x \in X\}$$

(2) *Um elemento $a \in A$ é um máximo de X (resp. mínimo de X) se*

$$a \in X \cap \limsup X \text{ (resp. } a \in X \cap \liminf X).$$

Escrevemos $a := \max X$ (resp. $a := \min X$)

(3) *Um elemento $a \in A$ é o supremo de X (resp. ínfimo de X) se $a = \min \limsup X$ (resp. $a = \max \liminf X$). Escrevemos $a := \sup X$ (resp. $a := \inf X$).*

(4) *Um elemento $a \in X$ é um elemento maximal de X (resp. elemento minimal de X) se para todo $x \in A$ tal que $a \prec x$ (resp. $x \prec a$) tem-se que $x \notin X$. Denotamos por*

$$Elem.MaxX := \{ \text{ elementos maximais de } X\}$$

e

$$Elem.MinX := \{ \text{ elementos minimais de } X\}.$$

Observações.

• Tem-se que $\max X$ (resp. $\min X$) quando existe, é único.

• $\sup X$ e $\inf X$ podem não pertencer ao conjunto X.

• Se $x \in A$ tal que $x \prec \sup X$ (resp. $\inf X \prec x$) então existe $x_0 \in X$ tal que $x_0 \prec x$ (resp. $x \prec x_0$.)

Exemplos.

(1) Seja $\mathbb{R}$ ordenado pela relação de ordem habitual e seja $X = [0, 1)$. Temos $\limsup X = [1, +\infty)$, $\liminf X = (-\infty, 0]$, Elem.Max = Elem.Min = $\{0\}$, $\nexists \max X$, $\min X = 0$, $\sup X = 1$ e $\inf X = 0$.

(2) Seja $\wp(\mathbb{R}^3)$ ordenado pela relação de inclusão.

(a) Seja $X = \{S \subseteq \mathbb{R}^3 \mid S \text{ é L.I.}\}$, então

$$Elem.MaxX = \{ \text{ bases do } \mathbb{R}^3\}.$$

De fato se B é uma base de $\mathbb{R}^3$ então B é L.I. e portanto $B \in X$. Se $B \subsetneq S$ então S é L.D. e portanto $S \notin X$. (todo subconjunto do $\mathbb{R}^3$ com mais de 3 vetores é L.D.)

(b) Seja $X = \{S \subseteq \mathbb{R}^3 \mid S \text{ gera } \mathbb{R}^3\}$, então

$$Elem.MinX = \{ \text{ bases do } \mathbb{R}^3\}.$$

Se se B é uma base de $\mathbb{R}^3$ então B gera $\mathbb{R}^3$ e portanto, $B \in X$. Se $S \subsetneq B$ temos que S não gera $\mathbb{R}^3$ e portanto $S \notin X$. (todo subconjunto de $\mathbb{R}^3$ com menos que 3 vetores não gera o $\mathbb{R}^3$.)

2.1. Exercícios.

(1) Determine $\limsup X, \liminf X$, Elem.Max X, Elem.Min X, $\max X$, $\min X$, $\sup X$ e $\inf X$ caso existam.

(a) Sejam $\mathbb{N}$ ordenado pela relação de "divisibilidade"e seja $X = \{2, 3, 5, 6, 10, 15, 18\}$.

(b) Sejam $A = \wp(\{a, b, c\})$ ordenado pela inclusão e $X = \{\{a\}, \{b\}, \{b, c\}, \{a, b, c\}\}$.

(2) Seja $f : X \to Y$ uma função. Sobre X defina a relação

$$xRx' \Leftrightarrow f(x) = f(x').$$

Prove que R é uma relação de equivalência.

(3) Seja $f : [0, 1] \to \mathbb{R}$ uma função estritamente decrescente e $S = Imf$. Mostre que $f(0) = \max S$ e $f(1) = \min S$.

(4) Prove que as relações R abaixo são de equivalência.

(a) Sobre $\mathbb{R}$ definida por $xRy \Leftrightarrow x = y$ ou $x = -y$.

(b) Sobre $\mathbb{C}$ definida por $(x + yi)R(z + ti) \Leftrightarrow x^2 + y^2 = z^2 + t^2$.

(5) Mostre que a relação $\preceq$ definida sobre $\mathbb{N} \times \mathbb{N}$ por

$$(a, b) \preceq (c, d) \Leftrightarrow a \mid c \text{ e } b \leq d$$

é uma relação de ordem. Seja $A = \{(1, 2), (2, 1)\}$. Determine $\limsup A$, $\liminf A$, $\max A$, $\min A$, $\sup A$, $\inf A$, Elem.Max A e Elem.Min A.

(6) Mostre que a relação sobre $\mathbb{N}$ definida por

$$a \leq b \Leftrightarrow \exists x \in \mathbb{N} \text{ tal que } b = a + x,$$

é uma ordem total.

(7) Seja $A = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$ ordenado pela relação de "divisibilidade". Seja $B = \{3, 6, 9\}$. Determine $\limsup B$, $\limsup B$, Elem.Max B, Elem.Min B e caso existam, determine $\max B$, $\min B$, $\sup B$ e $\inf B$.

(8) Mostre que a relação $x \sim y \Leftrightarrow xy > 0$ sobre $\mathbb{R} \setminus \{0\}$ é uma relação de equivalência e determine $\mathbb{R} \setminus \{0\}/\sim$.

(9) Seja R a relação definida sobre $\mathbb{N} \times \mathbb{N}$ por

$$(a, b)R(c, d) \Leftrightarrow a + d = b + c.$$

(a) Mostre que R é uma relação de equivalência. Represente geometricamente $\overline{(0, 0)}$ e $\overline{(1, 0)}$.

(b) Sejam $x = \overline{(a, b)}$ e $y = \overline{(c, d)}$ e defina

$$x \preceq y \Leftrightarrow a + d \leq b + c.$$

Mostre que $\preceq$ é de ordem total.

(10) Seja R a relação definida sobre $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ por

$$(a, b)R(c, d) \Leftrightarrow ad = bc.$$

(a) Mostre que R é uma relação de equivalência. Represente geometricamente $\overline{(0, 1)}$ e $\overline{(1, 1)}$.

(b) Sejam $x = \overline{(a, b)}$ e $y = \overline{(c, d)}$ e defina

$$x \preceq y \Leftrightarrow ad \leq bc.$$

Mostre que

(i) A relação $\preceq$ é de ordem total.

(ii) $\overline{(a, b)} = \overline{(-a, -b)}$.

(c) Seja R uma relação sobre A tal que R é reflexiva e satisfaz a seguinte propriedade:

$$\forall x, y, z \in A, xRy \text{ e } yRz \Rightarrow zRx.$$

Mostre que R é uma relação de equivalência.

(d) Seja $A = \{a_1, \ldots, a_n\} \subset \mathbb{N}$ ordenado pela relação de divisibilidade. Se $d = mdc(a_1, \ldots, a_n)$ e $m = mmc(a_1, \ldots, a_n)$, mostre que $d = \inf A$ e $m = \sup A$.

(e) Mostre que a relação R definida sobre $\mathbb{Q}$ por

$$xRy \Leftrightarrow x - y \in \mathbb{Z},$$

é uma relação de equivalência e determine $\bar{1}$.

CAPíTULO 4

Operações

DEFINIÇÃO 0.2. *Seja $\mathcal{A}$ um conjunto. Toda função $* : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ é chamada de operação sobre $\mathcal{A}$.*

DEFINIÇÃO 0.3. *Sejam $\mathcal{A}$ uma conjunto munido de operação $*$ e $\mathcal{B} \subseteq \mathcal{A}$. Dizemos que $\mathcal{B}$ é fechado para a operação se $a * b \in \mathcal{B}$, para todo $a, b \in \mathcal{B}$.*

Exemplo. Sejam $m \in \mathbb{Z}_m, m > 1$ e $\mathbb{Z}_m := \{\bar{a} \mid a \in \mathbb{Z}\}$, onde $\bar{a} = \{x \in \mathbb{Z} \mid x \equiv a(modm)\}$. As operações de adição e multiplicação sobre $\mathbb{Z}_m$ são dadas por

$$\bar{a} \oplus \bar{b} := \overline{a+b} \text{ e } \bar{a} \odot \bar{b} := \overline{ab}.$$

Mostremos que as operações estão bem definidas.

Suponha que $(\bar{a}, \bar{b}) = (\bar{c}, \bar{d})$, então

$$\bar{a} = \bar{c}, \bar{b} = \bar{d} \Rightarrow a \equiv c(modm), b \equiv d(modm)$$

Logo, $a + b \equiv c + d(modm)$ e $ab \equiv cd(modm)$. Então $\overline{a+b} = \overline{c+d}$ e $\overline{ac} = \overline{bd}$, portanto $\bar{a} \oplus \bar{b} = \bar{c} \oplus \bar{d}$ e $\bar{a} \odot \bar{b} = \bar{c} \odot \bar{d}$.

DEFINIÇÃO 0.4. *Seja $* : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ uma operação. Dizemos que:*

(1) *A operação é associativa se $\forall a, b, c \in \mathcal{A}, (a * b) * c = a * (b * c)$.*

(2) *A operação é comutativa se $\forall a, b \in \mathcal{A}, a * b = b * a$.*

(3) *$\mathcal{A}$ admite um elemento neutro para a operação se*

$$\exists e \in \mathcal{A} \text{ tal que } \forall a \in \mathcal{A}, e * a = a = a * e.$$

(4) *Suponha que $\mathcal{A}$ admite um elemento neutro e. Um elemento $a \in \mathcal{A}$ é simetrizável com relação a operação se existe $a' \in \mathcal{A}$ tal que $a * a' = e = a' * a$. O elemento a' é chamado de simétrico de a com respeito a operação.*

(5) *Um elemento $a \in \mathcal{A}$ é regular para a operação se satisfizer as seguintes condições:*

$$x * a = y * a \Rightarrow x = y \text{ (regular à direita)},$$

$$a * x = a * y \Rightarrow x = y \text{ (regular à esquerda)}.$$

Exemplos.

(1) Seja $\mathcal{F}(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid$ f é uma função $\}$. As operações adição, multiplicação e composição sobre $\mathcal{F}(\mathbb{R})$ são definidas respectivamente por: $(f+g)(x) := f(x) + g(x)$, $(f \cdot g)(x) := f(x).g(x)$ e $(f \circ g)(x) := f(g(x))$.
   (a) $\{f \in \mathcal{F}(\mathbb{R}) | f(x) = f(-x), \forall x \in \mathbb{R}\}$ é fechado para a adição.
   (b) $\{f \in \mathcal{F}(\mathbb{R}) | f(x) = -f(-x), \forall x \in \mathbb{R}\}$ é fechado para a adição, mas não é fechado para a multiplicação.
   (c) $\{f \in \mathcal{F}(\mathbb{R}) | f$ é bijetora$\}$ é fechado para a composição.
   (d) $\{f \in \mathcal{F}(\mathbb{R}) | f$ é derivável$\}$ é fechado para a multiplicação.

(2) Seja $\mathbf{M}_n(\mathbb{R}) = \{(a_{ij})_{n\times n} \mid a_{ij} \in \mathbb{R}\}$.
   (a) $\{A \in \mathbf{M}_n(\mathbb{R}) | A = A^t\}$ é fechado para a adição.
   (b) $\{A \in \mathbf{M}_n(\mathbb{R}) | A$ é inversível e $A^{-1} = A^t\}$ é fechado para a multiplicação.

0.2. Exercícios.

(1) Seja $*$ uma operação definida sobre $\mathcal{A}$, que é associativa. Prove que:
   (a) $a \in \mathcal{A}$ é regular à esquerda se e somente se $f : \mathcal{A} \to \mathcal{A}$ dada por $f(x) = a * x$ é injetora.
   (b) $\mathcal{B} = \{a \in \mathcal{A} | a$ é regular$\}$ é fechado para a operação $*$.

(2) Seja $*$ uma operação definida sobre $\mathcal{A}$, que é associativa e tem um neutro e. Defina o *centro* de $\mathcal{A}$ como sendo

$$Z(\mathcal{A}) := \{x \in \mathcal{A} \mid a * x = x * a, \forall a \in \mathcal{A}\}.$$

Mostre que $Z(\mathcal{A})$ é fechado com relação à operação $*$.

(3) Mostre que $\mathcal{A} = \left\{ \begin{pmatrix} \cos a & \sin a \\ -\sin a & \cos a \end{pmatrix} \mid a \in \mathbb{R} \right\}$ é fechado para a multiplicação.

(4) Seja $*$ uma operação sobre $\mathcal{A}$ com elemento neutro e. Mostre que esta operação é associativa e comutativa se e somente se $\forall a, b, c, d \in \mathcal{A}, (a*b)*(c*d) = (a*c)*(b*d)$.

(5) Seja $*$ uma operação sobre $\mathcal{A}$. Mostre que

$$\mathcal{S} := \{a \in \mathcal{A} \mid a * (x * y) = (a * x) * y, \forall x, y \in \mathcal{A}\}$$

é fechado para a operação $*$.

(6) Definem-se a adição e multiplicação de duas seqüências numéricas por: $(x_n) + (y_n) = (x_n + y_n)$ e $(x_n).(y_n) = (x_n y_n)$. Mostre que os conjuntos abaixo são fechados com relação essas operações.

(a) $\{(x_n) \mid (x_n) \text{ é convergente}\}$

(b) $\{(x_n) \mid (x_n) \text{ é limitada}\}$

Tábua de uma Operação sobre um Conjunto Finito

Seja $\mathcal{A} = \{a_1, \ldots, a_n\}$ munido da operação $*$. A tábua de $(\mathcal{A}, *)$ é construída como na tabela abaixo. A primeira linha é chamada de *linha fundamental* e a primeira coluna à esquerda é chamada de *coluna fundamental*.

$*$	a_1	$\ldots$	$\ldots$	a_i	$\ldots$	a_j	$\ldots$	$\ldots$	a_n
a_1	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
a_i	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$a_i * a_j$	$\ldots$	$\ldots$	$\ldots$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
a_j	$\ldots$	$\ldots$	$\ldots$	$a_j * a_i$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$a_j * a_n$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
a_n	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$a_n * a_j$	$\ldots$	$\ldots$	$\ldots$

Listaremos algumas propriedades da operação:

• A operação $*$ é comutativa se a tábua é simétrica em relação ao diagonal principal.

• Existe um elemento neutro, se existirem uma linha e uma coluna idênticas às fundamentais.

• Seja L_i a linha iniciada por a_i. Se nesta linha o elemento neutro e, se situa na coluna C_j então o simétrico de a_i' inicia coluna C_j, ou seja no cruzamento da linha L_i com a coluna C_j se encontra o elemento neutro e.

• Um elemento a_k é regular para a operação $*$, se na linha L_k e na coluna C_k não tem elementos repetidos. Na coluna C_k da tábua acima figuram os elementos $a_i * a_k$ e $a_j * a_k$ que devem ser distintos, pois caso contrário implicaria em $a_i = a_j$.

0.3. Exercícios.

(1) Faça a tábua para $(\mathbb{Z}_6, \oplus)$, $(\mathbb{Z}_6^*, \odot)$ e $(\mathbb{Z}_5^*, \odot)$.

(2) Sejam $G = \{f_1, f_2, f_3, f_4\}$, $f_i : \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$ dadas por $f_1(x) = x$, $f_2(x) = -x$, $f_3(x) = \frac{1}{x}$ e $f_4(x) = -\frac{1}{x}$. Faça a tábua para $(G, \circ)$.

(3) Sejam $G = \{f_1, f_2, f_3, f_4\}$, $f_i : \mathbb{R}^2 \to \mathbb{R}^2$ dadas por

$$f_1(x, y) = (x, y), f_2(x, y) = (-x, y),$$

$$f_3(x, y) = (x, -y), f_4(x, y) = (-x, -y).$$

Faça a tábua para $(G, \circ)$.

CAPíTULO 5

Grupos

DEFINIÇÃO 0.5. *Seja $* : G \times G \to G$ uma operação. Dizemos que G é um grupo se satisfaz as seguintes condições:*

(1) *A operação é associativa: $\forall a, b, c \in G; (a * b) * c = a * (b * c)$.*

(2) *Existe um elemento neutro $e \in G$: $\forall a \in G; e * a = a * e = a$.*

(3) *$\forall a \in G, \exists a' \in G$, simétrico de a tal que $a * a' = a' * a = e$.*

DEFINIÇÃO 0.6. *Se além disso, $\forall a, b \in G; a * b = b * a$, diremos que G é um grupo abeliano.*

Notações: Seja $(G, *)$ um grupo. Quando G é um grupo aditivo (resp. multipliucativo) usaremos " $+$ " (resp " $\cdot$ ") para a operação, "0" (resp. "1") para o elemento neutro e " $-a$" (resp. "a^{-1}") para o elmento simétrico.

PROPOSIÇÃO 0.7. *Seja $(G, *)$ é um grupo. Então*

(1) *O elemento neutro é único.*

(2) *Para cada $a \in G$, o simétrico de a é único e $(a')' = a$.*

(3) *$\forall a, b \in G; (a * b)' = b' * a'$.*

(4) *Todo elemento de G é regular.*

DEMONSTRAÇÃO. (de item (4)) Suponha que $x * a = y * a$, com $x, y \in G$. Então:

$$(x * a) * a' = (y * a) * a' \Rightarrow x * (a * a') = y * (a * a') \Rightarrow x * e = y * e \Rightarrow x = y.$$

Analogamente prova-se que $a * x = a * y$, com $x, y \in G$ implica que $x = y$. □

DEFINIÇÃO 0.8. *Seja $(G, *)$ um grupo e $H \subseteq G$. Dizemos que H é um subgrupo de G se $(H, *)$ é um grupo. Neste caso escrevemos $H \leqslant G$.*

PROPOSIÇÃO 0.9. *Seja $\emptyset \neq H \subseteq G$. Então $H \leqslant G$ se e somente se $\forall a, b \in H; a * b' \in H$.*

Exemplos.

(1) $(\mathbb{Z}, +)$ e $(\mathbb{Q}, +)$ são grupos abelianos.(Veja Apêndice 2)

(2) $(\mathbb{C}, +)$ é um grupo abeliano e $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são subgrupos de $\mathbb{C}$.

(3) $(\mathbb{C}^*, \cdot)$ é um grupo abeliano e $\mathbb{Q}^*$ e $\mathbb{R}^*$ são subgrupos de $\mathbb{C}^*$.

(4) $(\mathbb{Z}_n, \oplus)$ é um grupo abeliano.

(5) Seja $(G, +)$ um grupo abeliano. O conjunto $\mathcal{F}(X) = \{f \mid f : X \to X \text{ é uma função}\}$ munido de operação soma de funções é um grupo abeliano.

(6) $S_X := \{f : X \to X \mid f \text{ é uma função bijetora}\}$. Se $\#X > 2$, $(S_X, \circ)$ é um grupo não abeliano, chamado de*grupo das permutações sobre* X. Se $X = \{1, \cdots, n\}$ então S_X será denotado por S_n e todo $\sigma \in S_n$ será denotado por

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

$(S_n, \circ)$ é chamado de *grupo de permutações de grau* n. Por exemplo

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}.$$

(7) $\mathbf{M}_{m\times n}(\mathbb{R}) = \{(a_{ij}) \mid a_{ij} \in \mathbb{R}\}$ é um grupo aditivo abeliano.

(8) $\mathbf{GL}_n(\mathbb{R}) = \{A \in \mathbf{M}_n(\mathbb{R}) \mid A \text{ é invertível}\}$ é um grupo multiplicativo não abeliano.

0.4. Exercício.

(1) Sejam H_1 e H_2 subgrupos de G. Prove que $H_1 \cup H_2$ é um subgrupo de G se e somente se $H_1 \subseteq H_2$ ou $H_1 \subseteq H_2$.

(2) Seja $(H_i)_{i\in I}$ é uma família de subgrupos de G. Então $\bigcap_{i\in I} H_i$ é um subgrupo de G.

(3) $Z(G) = \{a \in G \mid a * x = x * a, \forall x \in G\}$ é um subgrupo de G, chamado de *centro* de G.

Definição 0.10. *Sejam $(G, *)$ um grupo e $a \in G$. Para cada $n \in \mathbb{Z}$, denotaremos por $a^0 = e, a^n = a * (a^{n-1})$ se $n > 0$ e $a^n = (a')^{-n}$ se $n < 0$. Definamos $[a] := \{a^n \mid n \in \mathbb{Z}\}$. Se G é um grupo aditivo, escrevemos* na *em vez de a^n e $[a] = \{na \mid n \in \mathbb{Z}\}$.*

Proposição 0.11. *Seja G um grupo e $a \in G$. Então $[a]$ é um subgrupo de G, chamado de subgrupo gerado por a.*

Definição 0.12. *Seja G um grupo e $a \in G$. Se existe $m \in \mathbb{Z}$ tal que $a^m = e$ dizemos que a é de ordem finita. O menor $m \in \mathbb{Z}$, $m > 0$ tal que $a^m = e$ é chamado de ordem de a. Se $m = 0$ é o único natural $a^m = e$, diremos que a ordem de a é zero. Usaremos $o(a)$ para ordem de a.*

Observação. Alguns autores escrevem $o(a) = \infty$, em vez de $o(a) = 0$.

0.5. Exercícios.

(1) Seja $(G, *)$ um grupo e $a \in G$.
   (a) Se $o(a) = n > 0$ e $a^m = e$ então $n \mid m$.
   (b) Se $\forall a \in G; a * a = e$, então $a = a'$ e G é abeliano.
   (c) Prove que $o(a) = o(a')$.

(2) Sejam $(G, *)$ um grupo abeliano e $H = \{x \in G \mid x * x = e\}$. Mostre que
   (a) H é um subgrupo de G.
   (b) Se $\forall a, b, c \in G; a * b = c$ e $a * c = b$, então $H = G$.

(3) Dado o grupo $(\mathbb{Z}, *)$, onde $a * b = a + b - 3$. Mostre que $3\mathbb{Z}$ é um subgrupo de $(\mathbb{Z}, *)$.

(4) Sejam $G = \mathbb{R} \times \mathbb{R}^*$ e $*$ uma operação definida sobre G por $(a, b) * (c, d) = (ad + bc, bd)$. Mostre que
   (a) $(G, *)$ é um grupo abeliano.
   (b) $H = \{(a, 1) \mid a \in \mathbb{R}\}$ é um subgrupo de G.

(5) Seja X um conjunto. Mostre que
   (a) $(\wp(X), \Delta)$ é um grupo abeliano.(Δ é a diferença simétrica)
   (b) Seja $B \subseteq X$. Então $H = \{A \in \wp(X) \mid A \cap B = \emptyset\}$ é um subgrupo de $(\wp(X), \Delta)$.

(6) Seja $G = \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = ax + b, a \neq 0\}$. Prove que $(G, \circ)$ é um subgrupo de $S_{\mathbb{R}}$

(7) Seja $G = \{e, a, b, c\}$ munido de operação definada pela tábua abaixo.

$*$	e	a	b	c
e	e	a	b	c
a	e	e	c	b
b	b	c	e	a
c	c	b	a	e

Determine $[e]$, $[a]$, $[b]$, $[c]$ e a ordem de cada elemento.

1. Homomorfismo de Grupos

Definição 1.1. *Sejam $(G_1, *)$ e $(G_2, \circ)$ dois grupos. Uma função $f : G_1 \to G_2$ é um homomorfismo de grupos se $\forall a, b \in G; f(a * b) = f(a) \circ f(b)$.*

Proposição 1.2. *Seja $f : G_1 \to G_2$ um homomorfismo de grupos.*

(1) *Se e_1 e e_2 são os neutros de G_1 e G_2 respectivamente então $f(e_1) = e_2$.*
(2) *$\forall a \in G_1; f(a') = (f(a))'$.*

1.1. Exercício. Seja $f : G_1 \to G_2$ um homomorfismo de grupos.

(1) Se $H_1 \leqslant G_1$ então $f(H_1) \leqslant G_2$.
(2) Se $H_2 \leqslant G_2$ então $f^{-1}(H_2) \leqslant G_1$.

Definição 1.3. *Seja $f : G_1 \to G_2$ um homomorfismo de grupos e e_2 o elemento neutro de G_2. O núcleo de f é*

$$\ker f := \{a \in G_1 \mid f(a) = e_2\}$$

e a imagem de f é

$$\mathrm{Im} f := \{f(a) \mid a \in G_1\}.$$

Definição 1.4. *Um homomorfismo $f : G_1 \to G_2$ é dito monomorfismo se f é injetora, epimorfismo se f é sobrejetora e isomorfismo se f é bijetora. Um isomorfismo f é um automorfismo se $G_1 = G_2$. Dizemos que G_1 e G_2 são isomorfos se $f : G_1 \to G_2$ um isomorfismo e escrevemos $G_1 \simeq G_2$.*

Proposição 1.5. *Seja $f : G_1 \to G_2$ um homomorfismo de grupos.*

(1) $\ker f \leqslant G_1$.
(2) $\mathrm{Im} f \leqslant G_2$.
(3) *f é um monorfismo se* $\ker f = \{e_1\}$.

1.2. Exercícios. Mostre que f é um homomorfismo e determine o $\ker f$.

(1) $f : \mathbb{R} \to \mathbb{C}^*$ tal que $f(\theta) = \cos(\theta) + i \sin(\theta)$.
(2) $f : \mathbb{Z} \to \mathbb{Z}_m$ tal que $f(x) = \bar{x}$

Proposição 1.6. *Sejam $f : G_1 \to G_2$ e $g : G_2 \to G_3$ homomorfismos de grupos. Então;*

(1) *$g \circ f$ é um homomorfismo.*
(2) *Se f é um isomorfismo então f^{-1} é um isomorfismo.*

1.3. Exercício.

(1) Seja $Aut(G) = \{f : G \to G \mid f$ é um automorfismo$\}$. Mostre que $(Aut(G), \circ)$ é um grupo.
(2) Seja $f : G \to H$ um homomorfismo. Prove:
   (a) Para todo $a \in G$; $o(f(a)) \mid o(a)$.
   (b) Se f é um monomorfismo então $o(f(a)) = o(a)$.

(3) Seja $f : G \to G$ definida por $f(x) = x^{-1}$. Mostre que: f é um homomorfismo se e somente se G é abeliano.

(4) Se $(G, \cdot)$ é abeliano e $a, b \in G$ tais que $mdc(o(a), o(b)) = 1$ então $o(a \cdot b) = o(a)o(b)$.

(5) Seja $f : \mathbb{Z}_4 \to \mathbb{C}^*$ tal que $f(\bar{n}) = i^n$. Prove que f é um monomorfismo.

(6) Sejam $(G, \cdot)$ um grupo, $a \in G$ e $f_a : G \to G$ definida por $f_a(x) = a \cdot x \cdot a^{-1}$. Mostre que;

(a) f_a é um automorfismo.

(b) $f_a \circ f_b = f_{a \cdot b}$.

(c) $o(x) = o(a \cdot x \cdot a^{-1})$.

(d) $\mathcal{I}(G) := \{f_a \mid a \in G\}$ é um subgrupo de $Aut(G)$, chamado de *grupo dos automorfismos internos* de G.

(e) $\varphi : G \to \mathcal{I}(G)$ dada por $\varphi(a) = f_a$ é um homomorfismo e $\ker \varphi = Z(G)$.

(7) Sejam $(G, +)$ e $(J, \cdot)$ grupos e $f : G \to J$ um homomorfismo. Prove por indução que para todo $n \in \mathbb{Z}$ que $f(nx) = (f(x))^n$.

(8) Sejam $(G, *)$ e $(J, \circ)$ grupos e defina sobre $G \times J$ a operação dada por $(a, b) + (c, d) := (a * c, b \circ d)$. Mostre que;

(a) $(G \times J, +)$ é um grupo.

(b) $f : G \times J \to G$ tal que $f(x, y) = x$ é um homomorfismo e determine $\ker f$.

(9) Mostre que;

(a) $G = \{A \in \mathbf{M}_{2\times 2}(\mathbb{R}) \mid A \text{ é invertível e } A^{-1} = A^t\}$ é um grupo.

(b) $H = \left\{ \begin{pmatrix} \cos a & -\sin a \\ \sin a & \cos a \end{pmatrix} \mid a \in \mathbb{R} \right\} \leqslant G$.

(c) $f : \mathbb{R} \to H$ dada por $f(a) = \begin{pmatrix} \cos a & -\sin a \\ \sin a & \cos a \end{pmatrix}$ é um homomorfismo de determine o $\ker f$.

(10) Seja $f : \mathbb{Z}_6 \to \mathbb{Z}_2$ dada por $f(\bar{x}) = \bar{r}$, onde r é o resto da divisão de x por 2. Verifique se

(a) f está bem definida?

(b) f é um homomorfismo?

(c) f é injetora?

(d) f é sobrejetora?

(11) Sejam $(G, *)$ um grupo, $H \leqslant G$ e $a \in G$. Prove:

(a) $a * H * a^{-1} := \{a * x * a^{-1} \mid h \in H\}$ é um subgrupo de G.

(b) Se $f : G \to G$ é um homomorfismo e G é abeliano então $H := \{a^{-1} * f(a) \mid a \in G\}$ é um subgrupo de G.

(c) Seja R uma relação sobre G definida por

$$xRy \Leftrightarrow \exists a \in G \text{ tal que } y = a * x * a^{-1},$$

então R é uma relação de equivalência.

(12) Seja $f : \mathbb{C}^* \to \mathbb{C}^*$ tal que $f(z) = z^n$. Mostre que f é um homomorfismo e determine $\ker f$.

2. Grupos Cíclicos

DEFINIÇÃO 2.1. *Seja G é um grupo. Dizemos que G é cíclico se existe $a \in G$ tal que $G = [a]$.*

Exemplos.

(1) $\mathbb{Z} = [1] = [-1]$.

(2) $\mathbb{Z}_m = [\bar{1}]$.

(3) Se $H = \{z \in \mathbb{C} \mid z^n = 1\}$ então $H = [\omega]$ onde $\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

PROPOSIÇÃO 2.2. *Se G é cíclico e $H \leqslant G$ então H é cíclico.*

DEMONSTRAÇÃO. Sejam $G = [a]$ e $n := \min\{k \mid k > 0, a^k \in H\}$. Mostramos que $H = [a^n]$.

Temos que $[a^n] \subseteq H$. Seja $x \in H$. Então $x = a^m$ para algum $m \in \mathbb{Z}$. Como H é subgrupo podemos supor $m > 0$. Pela minimalidade de n temos $m \geq n$. Pelo algoritmo de divisão seja $m = nq + r$, onde $r, q \in \mathbb{Z}$ e $0 \leq r < n$. Então $a^r = a^{m-nq}$ que claramente é um elemento de H. Mas pela minimalidade de n, obtemos que $r = 0$ ou seja $m = nq$ e $x \in [a^n]$. □

PROPOSIÇÃO 2.3. *Seja $G = [a]$. Então:*

(1) *Se $o(a) = n > 0$ então $G \simeq \mathbb{Z}_n$.*

(2) *Se $o(a) = 0$ então $G \simeq \mathbb{Z}$.*

DEMONSTRAÇÃO. (1) Seja $f : \mathbb{Z}_n \to G$ dada por $f(\bar{x}) = a^x$. Temos claramente que f é um homomorfismo sobre. Seja $\bar{x} \in \ker f$, então

$$f(\bar{x}) = e \Leftrightarrow a^x = e \Leftrightarrow n \mid x \Leftrightarrow \bar{x} = \bar{0}.$$

Ou seja f é injetora, portanto f é um isomorfismo e temos $G \cong \mathbb{Z}_n$.

(2) Seja $f : \mathbb{Z} \to G$ dada por $f(n) = a^n$. Temos claramente que f é um homomorfismo sobre. Seja $n \in \ker f$, então

$$f(n) = e \Leftrightarrow a^n = e \Leftrightarrow n = 0.$$

Ou seja f é injetora, portanto f é um isomorfismo e temos $G \cong \mathbb{Z}$. □

COROLÁRIO 2.4. (1) *Se $H \leqslant \mathbb{Z}$ então $H = [m]$ para algum $m \in \mathbb{Z}$.*

(2) *Se $H \leqslant \mathbb{Z}_n$ então $H = [\bar{m}]$ para algum $m \in \mathbb{Z}$.*

DEMONSTRAÇÃO. Exercício! □

PROPOSIÇÃO 2.5. *Seja $G = [a]$ com $o(a) = n > 0$. Então $G = [a^m]$ se e somente se $mdc(n, m) = 1$.*

DEMONSTRAÇÃO. Seja $G = [a^m]$. Como $a \in G$ existe $m \in \mathbb{Z}$ tal que $a = (a^m)^q$. Então $a = a^{mq}$, portanto $a^{mq-1} = e$ e $n \mid mq - 1$. Então existe $q' \in \mathbb{Z}$ tal que $mq - 1 = nq'$; ou $mq - nq' = 1$. Pela identidade de Bézout $mdc(n, m) = 1$. Para a recíproca seja $mdc(n, m) = 1$, então pela identidade de Bézout existem $r, s \in \mathbb{Z}$ tais que $rn + sm = 1$. Como $[a^m] \subseteq [a]$, basta mostrar que $[a] \subseteq [a^m]$. Sendo $a = a^{rn+sm} = a^{nr}a^{sm} = (a^m)^s$ concluímos que $a \in [a^m]$. Logo $[a] \subseteq [a^m]$. □

Exemplos. Utilizando o Corolário 2.4 acima temos:

(1) $\mathbb{Z}_4 = [\bar{1}] = [\bar{3}]$.

(2) Sejam $\omega = \exp(\frac{2\pi i}{8})$ e $G = [\omega]$. Então $G = [\omega^3] = [\omega^5] = [\omega^7]$.

Observações.

A função de *Euler* $\phi : \mathbb{N} \to \mathbb{N}$ é definida por

$$\phi(n) := \#\{m \in \mathbb{N} \mid 1 \leq m \leq n \text{ e } mdc(n, m) = 1\}.$$

(1) Se $n = p_1^{n_1} \cdots p_r^{n_r}$, onde $p_1, \ldots, p_r$ são números primos distintos então

$$\phi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r}).$$

(Veja apêndice 2)

(2) O número de geradores de $G = [a]$ quando $o(a) = n > 0$ é $\phi(n)$.

(3) Segundo a equivalência

$$\bar{a} \text{ é invertível em } \mathbb{Z}_n \Leftrightarrow mdc(a, n) = 1,$$

temos também que o número de elementos invertíveis em $\mathbb{Z}_n$ é $\phi(n)$.

2.1. Exercícios.

(1) Seja $f : G \to J$ um epimorfismo de grupos. Prove que:

  (a) Se G é abeliano então J é abeliano.

  (b) Se G é cíclico então J é cíclico.

(2) Se $G \neq \{e\}$ é um grupo tal que os únicos subgrupos de G são os triviais então G é cíclico.

(3) Se G é um grupo cíclico infinito e $G = [a] = [b]$ então $b = a$ ou $b = a^{-1}$.

(4) Sabendo-se que $G = \{e, a, b, c, d, f\}$ é um grupo isomorfo ao grupo $(\mathbb{Z}_6, \oplus)$ pede-se:

(a) Construir uma tábua para G.

(b) Verificar se G é cíclico, e no caso afirmativo determinar os seus geradores.

(5) Seja $H=\left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\right\}$ um subgrupo de S_4. Determine a ordem de cada elemento de H. Verifique se H é cíclico e se H pode ser isomorfo a $\mathbb{Z}_4$.

(6) Seja

$$H=\left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}\right\}.$$

Mostre que H é cíclico.

(7) Sejam $a, b \in \mathbb{Z}$ e $H = \{ax + by \mid x, y \in \mathbb{Z}\}$. Mostre que:

(a) $H \leqslant \mathbb{Z}$.

(b) Se $d = mdc(a, b)$ então $H = [d]$.

(8) Dado $n \in \mathbb{N}$ seja $H = \{z \in \mathbb{C} \mid z^n = 1\}$. Prove que:

(a) $H \leqslant \mathbb{C}^*$ cíclico gerado por $w = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$.

(b) $f : \mathbb{Z}_n \to H$ dada por $f(\bar{x}) = \cos(\frac{2\pi x}{n}) + i\sin(\frac{2\pi x}{n})$ é um isomorfismo.

3. Grupo Gerado por um Conjunto

Definição 3.1. *Sejam $(G, \cdot)$ um grupo e $\emptyset \neq S \subseteq G$. Define-se $[S] = \{a_1^{n_1} \cdots a_r^{n_r} \mid a_1, \ldots, a_r \in S$ e $n_1, \ldots, n_r \in \mathbb{Z}\}$. Este conjunto é um subgrupo de G e será chamado de grupo gerado por S.*

Quando G é um grupo aditivo, define-se $[S] = \{n_1a_1 + \cdots + n_ra_r \mid a_1, \ldots, a_r \in S$ e $n_1, \ldots, n_r \in \mathbb{Z}\}$

Exemplos.

(1) Considere $\mathbb{Z}_2 \times \mathbb{Z}_2$. Este grupo é chamado de grupo de Klein. Pondo $a = (\bar{1}, \bar{0})$ e $b = (\bar{0}, \bar{1})$. Temos que $\mathbb{Z}_2 \times \mathbb{Z}_2 = [a, b]$.

(2) Considere S_3. Sejam $\sigma = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ e $\tau = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$. Temos $\tau \circ \sigma^2 = \sigma \circ \tau$ e $S_3 = [\sigma, \tau]$.

(3) Seja $\sigma, \tau \in S_4$ dadas por $\sigma = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$ e $\tau = \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}$. Temos $\tau \circ \sigma^3 = \sigma \circ \tau$ e $\tau \circ \sigma^2 = \sigma^2 \circ \tau$. Cosidere $D_4 := [\sigma, \tau]$. este grupo é chamado de grupo de Diedral de ordem 8. Este grupo pode ser visto como o grupo de permutações de um quadrado.

Os sugrupos de D_4 são: $[\sigma] \simeq \mathbb{Z}_4$, $K_4 = \{\mathbf{1}, \tau \circ \sigma, \tau \circ \sigma^3, \sigma^2\}$ e $V_4 = \{\mathbf{1}, \tau, \tau \circ \sigma^2, \sigma^2\}$, onde $\mathbf{1}$ é a permutação identidade. Temos $K_4 \simeq V_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

(4) Seja Q_3 o grupo dos Quatérnios de ordem 8. Isto é:

$$Q_3 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \right\}.$$

Sejam $A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ e $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Temos $AB = BA^3$ e $Q_3 = [A, B]$.

4. Classes Laterais e Teorema de Lagrange

Sejam G um grupo finito e $H \leqslant G$. O nosso objetivo nessa seção é obter uma relação entre $\#H$ e $\#G$. Primeiro definiremos as *classes laterias* e estudaremos as suas propriedades básicas. Vale a pena observar que estas definições e propriedades não dependem da finitude de G.

Definição 4.1. *Sejam $(G, \cdot)$ um grupo e $H \leqslant G$. Para cada $a \in G$, definamos a classe lateral de a à esquerda por $a \cdot H := \{a \cdot h \mid h \in H\}$ e a classe lateral de a à direita por $H \cdot a := \{h \cdot a \mid h \in H\}$.*

Proposição 4.2. *Sejam $(G, \cdot)$ um grupo, $H \leqslant G$ e $a, b \in G$. Então:*

(1) *$a \cdot H = b \cdot H \Leftrightarrow b^{-1} \cdot a \in H$. Em particular $a \cdot H = H \Leftrightarrow a \in H$.*

(2) *$f_a : H \to a \cdot H$ tal que $f_a(h) = a \cdot h$ é bijetora. Em particular $|H| = |a \cdot H|$.*

(3) *Seja*

$$\varphi : \{\textit{classes laterais à esquerda}\} \to \{\textit{classes laterais à direita}\}$$
$$a \cdot H \mapsto H \cdot a^{-1},$$

então φ é bijetora.

(4) *Considere a relação dada por $a \sim b \Leftrightarrow a \cdot H = b \cdot H$. Esta relação é uma relação de equivalência. Segue daí que:*

(a) *$a \cdot H \neq \emptyset$.*

(b) *$a \cdot H = b \cdot H$ ou $(a \cdot H) \cap (b \cdot H) = \emptyset$.*

(c) *$G = \bigcup_{a \in G} (a \cdot H)$.*

Demonstração. Exercício! □

Notação. Denotaremos por $(G : H)$ o número de classes laterais à esquerda que é igual ao número de classes laterais à direita, pelo item (3) da proposição acima.

Observação. Analogamente,

$$a \sim b \Leftrightarrow H \cdot a = H \cdot b,$$

é uma relação de equivalência.

TEOREMA 4.3. *(Lagrange) Se G é um grupo finito e $H \leqslant G$, então $|G| = |H|(G : H)$. Em particular $|H|$ divide $|G|$ e $\frac{|G|}{|H|} = (G : H)$.*

DEMONSTRAÇÃO. Pelo item (4) da proposição acima podemos escrever

$$G = (a_1 \cdot H) \bigcup (a_2 \cdot H) \bigcup \cdots \bigcup (a_r \cdot H),$$

com $(a_i \cdot H) \bigcap (a_j \cdot H) = \emptyset$, para $i \neq j$. Assim $r = (G : H)$. Sendo, $|a_i \cdot H| = |a_j \cdot H| = |H|$, segue que:

$$|G| = |a_1 \cdot H| + |a_2 \cdot H| + \cdots + |a_r \cdot H| = r.|H| = (G : H)|H|.$$

Portanto $\frac{|G|}{|H|} = (G : H)$. □

COROLÁRIO 4.4. *Sejam G é um grupo finito e $a \in G$, então $o(a)$ divide $|G|$. Em particular $a^{|G|} = e$.*

DEMONSTRAÇÃO. Como $[a] \leqslant G$ e $|[a]| = o(a)$, pelo teorema de Lagrange temos que $o(a)$ divide $|G|$. Assim exsite $q \in \mathbb{Z}$ tal que $|G| = q.o(a)$, então $a^{|G|} = (a^{o(a)})^q = e$. □

COROLÁRIO 4.5. *Todo grupo de ordem prima é cíclico.*

DEMONSTRAÇÃO. Suponha que $|G| = p$, onde p é um número primo. Seja $a \in G \setminus \{e\}$ então $o(a) \mid p$ e daí $o(a) = 1$ ou p. Como $a \neq e$, temos que $o(a) = p$. Portanto $G = [a]$. □

COROLÁRIO 4.6. *(Pequeno Teorema de Fermat) Seja p um número primo então para todo $\bar{a} \in \mathbb{Z}_p^*$ temos $\bar{a}^{p-1} = \bar{1}$.*

DEMONSTRAÇÃO. Como $(\mathbb{Z}_p^*, \odot)$ é um grupo e $|\mathbb{Z}_p^*| = p-1$ então pelo corolário (4.4) temos $\bar{a}^{p-1} = \bar{1}$. □

COROLÁRIO 4.7. *Para todo $\bar{a} \in \mathbb{Z}_p$ temos $\bar{a}^p = \bar{a}$; i.é, todos os elementos de $\mathbb{Z}_p$ são raízes do polinômio $f(x) = x^p - x$.*

DEMONSTRAÇÃO. Exercício! □

4.1. Exercícios.

(1) Seja $f : G \to G$ um homomorfismo e $H = \ker f$. Mostre que $a \cdot H = b \cdot H$ se e somente se $f(a) = f(b)$.

(2) Sejam H_1 e H_2 subgrupos de G. Prove se $|H_1| = m$ e $|H_2| = n$ e $mdc(m, n) = 1$ então $H_1 \cap H_2 = \{e\}$.

(3) Se um grupo G tem ordem prima então os únicos subgrupos de G são os triviais.

(4) Para todo $\bar{a}, \bar{b} \in \mathbb{Z}_p$, temos $(\bar{a} \oplus \bar{b})^p = \bar{a}^p \oplus \bar{b}^p$.

5. Subgrupos Normais

Definição 5.1. *Sejam $(G, \cdot)$ um grupo e H um subgrupo de G. Dizemos que H é um subgrupo normal de G se para todo $a \in G$, $a \cdot H = H \cdot a$. Neste caso escrevemos $H \trianglelefteq G$.*

Exemplos.

(1) Os subgrupos triviais $\{e\}$ e G são subgrupos normais de G.

(2) Se G é um grupo abeliano então todos os subgrupos de G são normais.

(3) Se G é um grupo H é um subgrupo de G tal que $(G : H) = 2$, então $H \trianglelefteq G$.

Proposição 5.2. *Sejam $(G, \cdot)$ um grupo e H um subgrupo de G. Então $H \trianglelefteq G$ se e somente se para todo $a \in G$, $a \cdot H \cdot a^{-1} \subseteq H$.*

Demonstração. Sejam $H \trianglelefteq G$ e $x \in a \cdot H \cdot a^{-1}$. Então existe $h \in H$ tal que $x = a \cdot h \cdot a^{-1}$. Portanto

$$x \cdot a = a \cdot h \Rightarrow x \cdot a \in a \cdot H = H \cdot a \Rightarrow \exists h_1 \in H \ni x \cdot a = h_1 \cdot a \Rightarrow x = h_1 \Rightarrow x \in H.$$

Para a recíproca, mostremos que $H \cdot a \subseteq a \cdot H$. Seja $x \in H \cdot a$. Então exsite $h \in H$ tal que $x = h \cdot a$. Daí

$$x = (a \cdot a^{-1}) \cdot h \cdot a \Rightarrow x = a \cdot (a^{-1} \cdot h \cdot a).$$

Como pela hipótese, $a^{-1} \cdot h \cdot a \in H$, segue que $x \in a \cdot H$. Analogamente, prova-se que $a \cdot H \subseteq H \cdot a$. □

5.1. Exercícios.

(1) Sejam $(G_1, \cdot)$ e $(G_2, \circ)$ grupos e $f : G_1 \to G_2$ um homomorfismo. Então $\ker f \trianglelefteq G_1$.

(2) Seja $(G_1, \cdot)$ um grupo. Então

$$Z(G) := \{x \in G \mid a \cdot x = x \cdot a \text{ para todo } a \in G\}$$

é um subgrupo normal de G chamado de centro de G.

6. Grupo das Permutações

DEFINIÇÃO 6.1. *Seja X um conjunto(finito ou infinito) e considere $S_X := \{\sigma : X \to X \mid \sigma$ é bijetora$\}$. Esse conjunto munido de composição de funções é um grupo, chamado de grupo das permutações sobre X. Se $X = \{1, \cdots, n\}$ denotaremos S_X por S_n e $\sigma \in S_n$ por* $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$.

TEOREMA 6.2. *(Cayley) Seja G é um grupo finito tal que $|G| = n$, então G é isomorfo a um subgrupo de S_n.*

DEMONSTRAÇÃO. Seja $\Phi : G \to S_G = S_n$ dada por $\Phi(x) = \Phi_x$, onde $\Phi_x : G \to G$ é dada por $\Phi_x(a) = xa$. Mostremos que é um homomorfismo injetor. Sejam $x, y \in G$ tais que $\Phi(x) = \Phi(y)$. Então:

$$\Phi_x = \Phi_y \Rightarrow \forall a \in G, \Phi_x(a) = \Phi_y(a) \Rightarrow xa = ya \Rightarrow x = y.$$

Ou seja Φ é injetora. Seja $\mathcal{G} := \text{Im}\Phi$. Pela proposição (1.5), $\mathcal{G} \leqslant S_n$ e claramente $G \simeq \mathcal{G}$. □

DEFINIÇÃO 6.3. *Uma permutação $\sigma \in S_n$ é um r-ciclo, $r \geq 2$, se existem $a_1, \cdots, a_r \in \{1, \ldots, n\}$ tais que $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, $\ldots$, $\sigma(a_r) = a_1$ e $\sigma(i) = i$, para todo $i \notin \{a_1, \ldots, a_r\}$. Um 2-ciclo é chamado de uma transposição.*

Notação. Denotamos um r-ciclo por $(a_1, a_2, \ldots, a_r) = (a_2, a_3, \ldots, a_r, a_1) = \cdots = (a_r, a_1, \ldots, a_{r-1})$.

Exemplos.

(1) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 4 & 2 & 6 & 7 \end{pmatrix} = (235)$, é um 3-ciclo.

(2) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$, é produto(composição) de duas transposições.

Obsevações.

- Se σ é um r-ciclo então $o(\sigma) = r$.
- Se σ é uma transposição então $\sigma = \sigma^{-1}$.

DEFINIÇÃO 6.4. *Dizemos que dois ciclos σ e τ em S_n são ciclos disjuntos, se $\sigma(i) \neq i \Rightarrow \tau(i) = i$ e $\tau(j) \neq j \Rightarrow \sigma(j) = j$, para todo $i, j \in \{1, \ldots, n\}$.*

6.1. Exercícios. Se $\sigma = \alpha \circ \beta$, onde α e β são ciclos disjuntos, então $\sigma = \beta \circ \alpha$ e $o(\sigma) = mmc(o(\alpha), o(\beta))$.

Exemplos.

(1) $S_3 = \{(1), (123), (132), (12), (13), (23)\}$.

(2) $D_4 = \{(1), (1234), (13)(24), (1432), (12)(34), (14)(23), (24), (13)\}$.

(3) $S_4 = \{(1), (34), (23), (243), (234), (24), (12), (12)(34), (123), (1234), (1243), (124), (132), (1342), (13), (134), (13)(24), (1324), (1432), (142), (143), (14), (1423), (14)(23)\}$.

DEFINIÇÃO 6.5. *Seja* $p = \prod_{1\leq i<j\leq n}(x_i - x_j) \in \mathbb{Z}[x_1, \cdots, x_n]$. *Para cada* $\sigma \in S_n$, *seja* $p^\sigma := \prod_{1\leq i<j\leq n}(x_{\sigma(i)} - x_{\sigma(j)})$.

Tem-se que $p^\sigma = \pm p$. *Diremos que* σ *é uma permutação par se* $p^\sigma = p$ *e é uma permutação ímpar se* $p^\sigma = -p$.

PROPOSIÇÃO 6.6. *Sejam* $\sigma, \tau \in S_n$.

(1) *Se* σ *é ma transposição então* $p^\sigma = -p$.

(2) $p^{\sigma\circ\tau} = (p^\tau)^\sigma$.

TEOREMA 6.7. *Seja* $\sigma \in S_n$, $\sigma \neq (\mathbf{1})$. *Então existem* $\sigma_1, \ldots, \sigma_m$, *ciclos disjuntos tais que* $\sigma = \sigma_1 \circ \cdots \circ \sigma_m$.

DEMONSTRAÇÃO. Seja $X = \{1, \cdots, n\}$. Sendo $\sigma \neq (\mathbf{1})$, existe $i_1 \in X$ tal que $\sigma(i_1) \neq i_1$. Como $X_1 := \{i_1, \sigma(i_1), \sigma^2(i_1), \cdots\} \subseteq X$, então X_1 é finito, daí existe r_1 tal que $\sigma^{r_1}(i_1) = i_1$. Logo $\sigma_1 := (i_1\sigma(i_1)\cdots\sigma^{r_1-1}(i_1))$ é um r_1-ciclo. Se $\sigma = \sigma_1$, acabou a demonstração. Se $\sigma \neq \sigma_1$, então $X \neq X_1$ e daí existe $i_2 \in X \setminus X_1$ tal que $\sigma(i_2) \neq i_2$. Então r_2 tal que $\sigma^{r_2}(i_2) = i_2$ e assim $\sigma_2 = (i_2\sigma(i_2)\cdots\sigma^{r_2-1}(i_2))$ é um r_2-ciclo. Se $\sigma = \sigma_1 \circ \sigma_2$, acabou a demonstração, caso contrário $X \neq X_1 \cup X_2$, onde $X_2 = \{i_2, \sigma_2(i_2), \cdots, \sigma^{r_2-1}(i_2)\}$. Usando o mesmo argumento acima sucessivamente, podemos encontrar $r_1, r_2, \cdots, r_m$ e $X_1, \cdots, X_m$ disjuntos tais que $X = X_1 \cup \cdots \cup X_m$ e $\sigma = \sigma_1 \circ \cdots \circ \sigma_m$, onde σ_i é r_i-ciclo, $i = 1, \cdots, m$. □

COROLÁRIO 6.8. *Se* $\sigma \in S_n$. *Então existem transposições* $\sigma_1, \cdots, \sigma_m$ *tais que* $\sigma = \sigma_1 \circ \cdots \circ \sigma_m$ *ou seja* S_n *é gerado por transposições.*

DEMONSTRAÇÃO. Se $\sigma = (\mathbf{1})$ então $\sigma = (ab) \circ (ab)$. Se $\sigma \neq (\mathbf{1})$ então existem ciclos disjuntos $\sigma_1, \ldots, \sigma_m$, tais que $\sigma = \sigma_1 \circ \cdots \circ \sigma_m$. Agora, todo r-ciclo $(a_1, \ldots, a_r)$ pode ser escrito como $(a_1a_r) \circ (a_1a_{r-1}) \circ \cdots \circ (a_1a_2)$. Agora utilize o teorema acima. □

DEFINIÇÃO 6.9. *A função sinal* $sgn : S_n \to \{-1, +1\}$ *é definida por:*

$$sgn(\sigma) := \begin{cases} +1, \text{ se } \sigma \text{ é par}; \\ -1, \text{ se } \sigma \text{ é ímpar.} \end{cases}$$

PROPOSIÇÃO 6.10. *A função sinal é um homomorfismo de grupos, i.é.*

DEMONSTRAÇÃO. Sejam $\sigma, \tau \in S_n$. Então $p^\sigma = (sgn\sigma)p$ e $p^\tau = (sgn\tau)p$. Como,

$$p^{\sigma\circ\tau} = (p^\sigma)^\tau = ((sgn\tau)p)^\sigma = (sgn(\tau))p^\sigma = (sgn(\tau)sgn(\sigma))p,$$

segue que $sgn(\sigma \circ \tau) = sgn(\sigma).sgn(\tau)$. Logo, sgn é um homomorfismo. □

6.2. Exercícios.

(1) Mostre que
   (a) Se σ é um transposição então $sgn(\sigma) = -1$
   (b) Se $\sigma = (a_1 \cdots a_r)$ então $sgn(\sigma) = (-1)^{r-1}$.
(2) Determine as ordens e os sinais dos elementos de D_4.
(3) Se $\sigma = (135)(12)$ e $\tau = (1579)$, determine $\sigma \circ \tau \circ \sigma^{-1}$.

DEFINIÇÃO 6.11. *O grupo alternado de grau n é* $A_n := \ker(sgn) = \{\sigma \in S_n \mid \sigma \text{ é par}\}$.

PROPOSIÇÃO 6.12. $A_n \trianglelefteq S_n$.

Aplicação. Seja $\mathbf{M}_{n\times n}(\mathbb{R}) = \{(a_{ij}) \mid a_{ij} \in \mathbb{R}\}$. A função determinante sobre $\mathbf{M}_{n\times n}(\mathbb{R})$ é definida por:

$$\begin{aligned} \det : \mathbf{M}_{n\times n}(\mathbb{R}) &\to \mathbb{R} \\ (a_{ij}) &\to \sum_{\sigma\in S_n} sgn(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}\ldots a_{n\sigma(n)}. \end{aligned}$$

CAPíTULO 6

Anéis e Corpos

DEFINIÇÃO 0.13. *Seja $A \neq \emptyset$ um conjunto munido de duas operações $+ : A \times A \to A$ e $\cdot : A \times A \to A$. Dizemos que A é um anel se as seguintes condições são satisfeitas:*

(1) $(A, +)$ *é um grupo abeliano.*

(2) $\forall a, b, c \in A; (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(3) $\forall a, b, c \in A; a \cdot (b + c) = a \cdot b + a \cdot c$ *e* $(b + c) \cdot a = b \cdot a + c \cdot a$.

Se além disso, $a \cdot b = b \cdot a$ para todo $a, b \in A$, diremos que A é um anel comutativo. Se existe $1 \in A$ tal que $\forall a \in A; a \cdot 1 = a = 1 \cdot a$, diremos que A é um anel com unidade 1.

Notação. Durante este capítulo, $(A, +, \cdot)$ denotará um anel e $0 = 0_A$, o elemento neutro da adição.

Observação. Se $0 = 1$, então $A = \{0\}$; de fato para todo $x \in A$, temos $x = x \cdot 1 = x \cdot 0 = 0$.

Exemplos.

(1) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ e $(\mathbb{Z}_m, \oplus, \odot)$, $m > 1$ são anéis comutativos com unidades.

(2) $\mathbb{R}[x] := \{\sum_{i=1}^{n} a_i x^i \mid a_i \in \mathbb{R}, n \in \mathbb{N}\}$ é um anel comutativo com unidade.

(3) $\mathbf{M}_n(\mathbb{R}) = \{(a_{ij}) \mid a_{ij} \in \mathbb{R}\}$ é um anel não comutativo com unidade I_n.

(4) Seja $\mathcal{F}(\mathbb{R}, \mathbb{R}) := \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ é uma função}\}$. Este conjunto munido de soma e produto dde funções é um anel comutativo com unidade $1_{\mathcal{F}(\mathbb{R},\mathbb{R})} = 1$. $(1(x) = 1$ para todo $x \in \mathbb{R}$.) Observe que não teremos um anel se considerarmos composição em lugar de produto, pois em geral

$$f \circ (g + h) \neq f \circ g + f \circ h.$$

(5) Seja $\mathcal{L}(\mathbb{R}^n) := \{T : \mathbb{R}^n \to \mathbb{R}^n \mid T \text{ é uma transformação linear}\}$. Este conjunto munido de soma e composição é um anel *não* comutativo com unidade $1_{\mathcal{L}(\mathbb{R}^n)} = id_{\mathbb{R}^n}$

DEFINIÇÃO 0.14. *Sejam $(A, +, \cdot)$ um anel e $\emptyset \neq B \subseteq A$. Dizemos que B é um subanel de A se $(B, +, \cdot)$ é um anel. Neste caso escrevemos $B \leqslant A$.*

PROPOSIÇÃO 0.15. *Sejam A um anel e $\emptyset \neq B \subseteq A$. Então B é um subanel de A se e somente se, para todo $a, b \in B; a - b \in B$ e $a \cdot b \in B$.*

DEFINIÇÃO 0.16. *Seja $(K, +, \cdot)$ um anel comutativo com unidade 1. Dizemos que K é um corpo se para todo $a \in K \setminus \{0\}$, existe $a^{-1} \in K$, tal que $a \cdot a^{-1} = 1$.*

Observação. Se $(K, +, \cdot)$ é um corpo então $(K \setminus \{0\}, +, \cdot)$ é um grupo abeliano.

DEFINIÇÃO 0.17. *Seja $(K, +, \cdot)$ um corpo e $\emptyset \neq L \subseteq K$. Dizemos que L é um subcorpo de K se $(L, +, \cdot)$ é um corpo.*

PROPOSIÇÃO 0.18. *Sejam K um corpo e $\emptyset \neq L \subseteq K$. Então, L é um subcorpo de K se e somente se, para todo $a, b \in L; a - b$ e $a \cdot b \in L$ e para todo $a \in L \setminus \{0\}; a^{-1} \in L$.*

Exemplos.

(1) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são corpos.
(2) $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$ é um subanel de $\mathbb{C}$, chamado de anel dos inteiros de Gauss.
(3) $\mathbb{Q}[i] := \{a + bi \mid a, b \in \mathbb{Q}\}$ é um subcorpo de $\mathbb{C}$.
(4) $Q[\sqrt{p}] = \{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\}$ é um subcorpo de $\mathbb{R}$ se $p > 0$ e é um subcorpo de $\mathbb{C}$ se $p < 0$.

1. Domínios e Corpo de Frações

1.1. Domínios.

DEFINIÇÃO 1.1. *Seja $(A, +, \cdot)$ um anel comutativo com unidade. Dizemos que A é um anel de integridade ou domínio de integridade ou simplesmente domínio se A satisfaz a seguinte condição:*

$$a \cdot b = 0 \Rightarrow a = 0 \text{ ou } b = 0.$$

Se A não é um domínio então existem $a, b \in A$ tais que $a \cdot b = 0$, mas $a \neq 0$ e $b \neq 0$. Tais elementos são chamados de divisores próprios do zero.

Exemplos.

(1) Todo corpo é um domínio.
(2) $\mathbb{Z}_m$ é um domínio, se o somente e m é um número primo.
(3) Se A é um domínio então $A[x] = \{\sum_{i=1}^{n} a_i x^i \mid a_i \in A, n \in \mathbb{N}\}$ é um domínio. (Anel dos Polinômios com coeficientes em A na variável x)

1.2. Exercícios.

(1) Num anel de integridade, resolva as equações $x^2 = x$ e $x^2 = 1$.

(2) Sejam $f, g : \mathbb{R} \to \mathbb{R}$ tais que $f(x) = x + |x|$ e $g(x) = x - |x|$. Mostre que f e g são divisores próprios do zero.

(3) Seja A um anel e $0 \neq a \in A$. Mostre que $(a, 0)$ e $(0, a)$ são divisores próprios do zero de $A \times A$.

(4) Seja $(A, +, \cdot)$ um anel. Verifique se

(a) $B = \{x \in A \mid \forall y \in A; x \cdot y = y \cdot x\}$ é um subanel de A.

(b) $B = \{x \in A \mid x^2 = x\}$ é um subanel de A.

(5) Quais são os divisores de zero e os elementos invertíveis de $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_3$.

(6) Defina $a * b = a + b - 1$ e $a \circ b = a + b - ab$. Mostre que $(\mathbb{Z}, *, \circ)$ é um domínio e $(\mathbb{Q}, *, \circ)$ é um corpo.

(7) Seja p um número primo. Mostre que $A = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$ é um subanel, mas não é um subcorpo de $\mathbb{Q}$.

1.3. Corpo de Frações. Seja $(A, +, \cdot)$ um domínio. Definimos a seguinte relação sobre $A \times A \setminus \{0\}$;

$$(a, b) \sim (c, d) \Leftrightarrow a \cdot d = b \cdot c$$

Claramente esta relação é uma relação de equivalência. Denotamos a classe de (a, b) por $\frac{a}{b}$ e seja $K = (A \times A \setminus \{0\})/\sim$. Agora definimos as seguintes operações sobre K;

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd} \text{ e } \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

Essas operações estão bem definidas e $(K, +, \cdot)$ é um corpo.

Definição 1.2. *Sejam A um domínio, o corpo obtido na construção acima é chamado de corpo de frações de A, denotado por $cf(A)$.*

Observações.

• Via aplicação injetora $f : A \to K$, $a \mapsto \frac{a}{1}$, os elementos de A podem ser identificados como os elementos da $\mathrm{Im}f$ e podemos dizer que A é um *subconjunto* de K.

• O corpo de frações de A é o menor corpo *contendo* A.

Exemplos.

(1) $cf(\mathbb{Z}) = \mathbb{Q}$.

(2) Seja $\mathbb{Z}[\sqrt{n}] := \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$, onde n é livre de quadrados. Então $cf(\mathbb{Z}[\sqrt{n}]) = \mathbb{Q}[\sqrt{n}]$.

2. Ideais de um Anel Comutativo

DEFINIÇÃO 2.1. *Sejam A um anel comutativo e $\emptyset \neq I \subseteq A$. Dizemos que I é um ideal de A se*

$$\forall x, y \in I, x - y \in I \text{ e } \forall a \in A, x \in I, ax \in I.$$

Observações. Seja A um anel comutativo com unidade 1.

• Se $1 \in I$ então $I = A$.

• Todo ideal é um subanel, mas a recíproca não vale; por exemplo $\{\sum_{i=0}^{n} a_i x^{2i} \mid a_i \in \mathbb{Z}, n \in \mathbb{N}\}$ é subanel de $\mathbb{Z}[x]$ mas *não* é ideal.

Exemplos.

(1) $\{0\}$ e A são ideais de A, chamados de ideais *triviais* de A.

(2) Sejam $x_1, \ldots, x_n \in A$. O conjunto

$$(x_1, \ldots, x_n) := \{a_1 x_1 + \ldots + a_n x_n \mid a_1, \ldots, a_n \in A\}$$

é um ideal de A, chamado de *ideal gerado* por $x_1, \ldots, x_n$. Quando $n = 1$, este ideal é chamado de ideal *principal gerado* por x_1.

2.1. Exercícios.

(1) Seja K um domínio. Mostre que K é um corpo se e somente se os únicos ideais de K são os triviais.

(2) Sejam A um anel comutativo com unidade e I, J ideais de A. Mostre que $I \cap J$ é o maior ideal de A contido em I e J. Define-se $I + J := \{x + y \mid x \in I, y \in J\}$. Mostre que $I + J$ é o menor ideal de A contendo I e J.

(3) Seja $A = \{f : \mathbb{R} \to \mathbb{R} \mid \forall x \in \mathbb{R}, f(x) \in \mathbb{Q}\} \subset \mathcal{F}(\mathbb{R}, \mathbb{R})$ Mostre que A é um subanel de $\mathcal{F}(\mathbb{R}, \mathbb{R})$, mas não é um ideal de $\mathcal{F}(\mathbb{R}, \mathbb{R})$.

(4) Seja p um número primo. Mostre que $I = \{\frac{a}{b} \in \mathbb{Q} \mid p \mid a, p \nmid b\}$ é um ideal de $\mathbb{Q}$.

(5) Dados $(A, +, \cdot)$ um anel comutativo com unidade e $a \in A$. Mostre que:

(a) $B = \{x \in A \mid \forall a \in A, a \cdot x = x \cdot a\}$ é um subanel de A.

(b) $I = \{x \in A \mid a \cdot x = 0\}$ é um ideal de A.

(6) Em cada item, verifique se o conjunto dado é subanel ou ideal de $\mathbb{Z}[x]$.
   (a) $\{\sum_{i=1}^{n} a_i x^i \in \mathbb{Z}[x] \mid a_0 \in 2\mathbb{Z}, n \in \mathbb{N}\}$.
   (b) $\{\sum_{i=1}^{n} a_i x^i \in \mathbb{Z}[x] \mid a_0 = 0, n \in \mathbb{N}\}$.
   (c) $\{\sum_{i=1}^{n} a_i x^i \in \mathbb{Z}[x] \mid a_0 + a_1 = 0, n \in \mathbb{N}\}$.

(7) Sejam A um anel comutativo com unidade e I é um ideal de A. Seja $J := \{x \in A \mid \forall a \in A, xa \in I\}$. Mostre que $J \trianglelefteq A$ e $I \subseteq J$.

(8) Sejam A um anel comutativo com unidade e I um ideal de A. Mostre que $\sqrt{I} := \{a \in A \mid \exists n \in \mathbb{N}, a^n I\}$ é um ideal de A e $I \subseteq \sqrt{I}$. (Este ideal é chamado de ideal *radical* de I.)

3. Homomorfismos de Anéis

Definição 3.1. *Sejam A e B anéis. Uma função $f : A \to B$ é um homomorfismo de anéis se*

$$\forall x, y \in A; f(x + y) = f(x) + f(y) \text{ e } f(xy) = f(x)f(y).$$

O núcleo de f é $\ker f := \{x \in A \mid f(x) = 0_B\}$.

Dizemos que f é monomorfimo (resp. epimorfismo) se f é injetora (resp. sobrejetora). Se f for uma bijeção, diremos que f é um isomorfismo e escrevemos $A \simeq B$.

Proposição 3.2. *Seja $f : A \to B$ um homomorfismo de anéis.*

(1) $\ker f \trianglelefteq A$ *e* $\mathrm{Im} f \leqslant B$.
(2) f *é injetora se e somente se* $\ker f = \{0_A\}$.

3.1. Exercícios.

(1) Seja $f : A \to B$ um homomorfismo de anéis comutativos com unidades 1_A e 1_B respectivamente.
   (a) Se f é um epimorfismo então $f(1_A) = 1_B$.
   (b) Se $I \trianglelefteq A$ então $f(I)$ não é necessariamente um ideal de B.
   (c) Se $J \trianglelefteq B$ então $f^{-1}(J) \trianglelefteq A$.

(2) Sejam A um anel e $Aut(A) := \{f : A \to A \mid f \text{ é um isomorfismo}\}$. Prove que $(Aut(A), \circ)$ é um grupo.

(3) Seja $f : A \to B$ um homomorfismo de anéis comutativos com unidade. Se B é um domínio e $f \neq 0$, então $f(1_A) = 1_B$.

(4) Verificar se as seguintes aplicações são homomorfismo de anéis e no caso afirmativo determine o núcleo.
   (a) $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ dada por $f(x, y) = y$.
   (b) $f : \mathbb{C} \to \mathbb{C}$ dada por $f(a + bi) = a - bi$.
   (c) $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ dada por $f(x, y) = (0, y)$.
   (d) $f : \mathbb{Z} \to \mathbb{Z}$ dada por $f(x) = 2x$.

(5) Mostrar que $L = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \leqslant \mathbf{M}_2(\mathbb{R})$, comutativo e com unidade. Mostre que não existe um isomorfismo de anéis $f : \mathbb{C} \to L$.(Dica: Usar $f(-1) = -f(1)$ e $f(-1) = f(i.i)$)

4. Anéis Quocientes e Teorema de Isomorfismo

4.1. Anéis Quocientes. Sejam A um anel comutativo e $I \trianglelefteq A$. Seja $A/I := \{a+I \mid a \in A\}$ e defina:

$$(a + I) + (b + I) := (a + b) + I \text{ e } (a + I) \cdot (b + I) := (ab) + I.$$

Essas operações estão bem definidas e A/I munido dessas operações é um anel comuttivo, chamado de *anel quociente de A por I*. Se A é um anel com unidade então A/I é com unidade, $1_{A/I} = 1_A + I$.

Notação. Em lugar de $a + I$, escrevemos $\bar{a}$.

4.2. Teorema de Isomorfiso.

TEOREMA 4.1. *Seja $f : A \to B$ um homomorfismo de anéis, então $A/\ker f \simeq \mathrm{Im} f$.*

DEMONSTRAÇÃO. Seja $\bar{f} : A/\ker f \to \mathrm{Im} f$ tal que $\bar{f}(\bar{x}) = f(x)$. Primeiro mostremos que $\bar{f}$ está bem definida e injetora;

$$\bar{x} = \bar{y} \Leftrightarrow x - y \in \ker f \Leftrightarrow f(x - y) = 0_B \Leftrightarrow f(x) = f(y) \Leftrightarrow \bar{f}(\bar{x}) = \bar{f}(\bar{y}).$$

Claramente $\bar{f}$ é sobrejetora e temos

$$\bar{f}(\bar{x} + \bar{y}) = f(x + y) = f(x) + f(y) = \bar{f}(\bar{x}) + \bar{f}(\bar{y})$$

e

$$\bar{f}(\bar{x}\bar{y}) = \bar{f}(\overline{xy}) = f(xy) = f(x)f(y) = \bar{f}(\bar{x})\bar{f}(\bar{y})$$

Portanto, f é um isomorfismo de anéis.

□

Exemplos.

(1) $\mathbb{Z}/(n) \simeq \mathbb{Z}_n$.
(2) $\mathbb{Z}[x]/(x) \simeq \mathbb{Z}$.
(3) $\mathbb{R}[x,y] = \{\sum_{i=0}^{n}\sum_{j=0}^{m} a_{ij}x^iy^j \mid a_{ij} \in \mathbb{R}; n,m \in \mathbb{N}\}$. Então, $\mathbb{R}[x,y]/(x) \simeq \mathbb{R}[y]$.
(4) $\mathbb{Z}[x]/(m,x) \simeq \mathbb{Z}_m$.

4.3. Exercícios.

(1) Seja $f : \mathbb{Z}_m \to \mathbb{Z}_n$ tal que $n \mid m$, definida por $f(\bar{x}) = \bar{y}$, se $x \equiv y(mod n)$. Mostre que f é um homomorfismo de anéis.
(2) Seja $f : \mathbb{C} \to \mathbf{M}_2(\mathbb{R})$ dada por $f(a+bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Mostre que f é um monomorfismo.
(3) Sejam A um domínio, $0 \neq a \in A$ e $f : A \to A$ tal que $f(x) = ax$. Mostre que f é injetora. Quando f é um homomorfismo de anéis?
(4) Mostre que $f : \mathbb{Z} \to \mathbb{Z}_p$ dada por $f(a) = \bar{a}^p$ é um homomorfismo de anéis.
(5) Seja $f : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ definida por $f(a+b\sqrt{2}) = a - b\sqrt{2}$. Mostre que f é um isomorfismo de anéis.
(6) Se p, q são números primos e $p \neq q$ então $\mathbb{Q}[\sqrt{p}]$ e $\mathbb{Q}[\sqrt{q}]$ não são isomorfos.
(7) Mostre $Aut(\mathbb{Q}[\sqrt{p}]) = \{id_{\mathbb{Q}[\sqrt{p}]}, \sigma\}$, onde $\sigma(a+b\sqrt{p}) = a - b\sqrt{p}$.
(8) Sejam A um corpo e $f : A \to B$ um homomorfismo de anéis. Prove f é um monomorfismo ou f é nulo.
(9) Seja $(\mathbb{Z}\times\mathbb{Z}, +, \cdot)$ um anel, onde $(a,b)+(c,d) = (a+c, b+d)$ e $(a,b)\cdot(c,d) = (ac, ad+bc)$. Mostre que
   (a) $\mathbb{Z} \times 2\mathbb{Z} \leqslant \mathbb{Z} \times \mathbb{Z}$.
   (b) Se $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times 2\mathbb{Z}$ tal que $f(x,y) = (x, 2y)$, então f é um epimorfismo.
(10) Seja A um anel e $a \in A$ invertível. Seja $f_a : A \to A$ tal que $f_a(x) = axa^{-1}$. Mostre que f_a é um isomorfismo e determine a sua inversa.
(11) Mostre que $(\mathbb{Q}, *, \circ)$ é um corpo, onde $a * b := a + b + 1$ e $a \circ b = a + b + ab$. Seja $f : (\mathbb{Q}, +, \cdot) \to (\mathbb{Q}, *, \circ)$ tal que $f(x) = x - 1$. Mostre que f é um isomorfismo.
(12) Considere o epimorfismo de anéis $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ dado por $f(x,y) = y$. Determinar o $\ker f$ e prove que $(\mathbb{Z} \times \mathbb{Z})/\ker f \simeq \mathbb{Z}$.
(13) Mostre que $\mathbb{Z}[x]/(m) \simeq \mathbb{Z}_m[x]$ e $\mathbb{Z}[\sqrt{2}]/(\sqrt{2}) \simeq \mathbb{Z}_2$.

5. Domínios Principais

DEFINIÇÃO 5.1. *Um domínio A é principal se todo ideal de A é principal; i.é, se I é um ideal de A então $I = (a)$, para algum $a \in A$.*

5.1. Exercícios. Tente definir os conceitos de *divisibilidade, maior divisor comum* e *menos múltiplo comum* em um domínio qualquer.

(1) Sejam A um domínio e $a, b \in A \setminus \{0\}$. Então $a \mid b \Leftrightarrow (b) = (a)$.

(2) $a \mid b$ e $b \mid a \Leftrightarrow (a) = (b) \Leftrightarrow a = ub$, para algum u invertível em A.

TEOREMA 5.2. *Se A é um domínio principal e $a, b \in A$, então $(a) + (b) = (d)$, onde $d = mdc(a, b)$.*

DEMONSTRAÇÃO. Como A é pincipal, existe $d \in A$ tal que $(a) + (b) = (d)$. Mostremos que $d = mdc(a, b)$.

Temos

$$a \in (a) \subseteq (a) + (b) = (d) \Rightarrow d \mid a.$$

Da mesma forma $d \mid b$. Por outro lado

$$d \in (d) = (a) + (b) \Rightarrow \exists r, s \in A \ni d = ar + bs.$$

Agora se $d' \in A$ tal que $d' \mid a$ e $d' \mid b$, então $d' \mid ar+bs$ ou seja $d' \mid d$. Portanto $d = mdc(a, b)$. □

Observação. Se $d = mdc(a, b)$ então $d = ar + bs$. Essa igualdade é chamada de identidade de *Bézout*.

TEOREMA 5.3. *O anel dos inteiros $\mathbb{Z}$ é um domínio principal.*

DEMONSTRAÇÃO. Seja $I \trianglelefteq \mathbb{Z}$. Se $I = \{0\}$ então $I = (0)$. Se $I \neq \{0\}$ então $a \in I$ tal que $a \neq 0$. Podemos supor que $a > 0$, pois caso contrário consideramos $-a \in I$. Então $I \cap \mathbb{N} \neq \emptyset$ e limitado inferiormente. Assim, pelo PBO, existe $d = \min I$. Mostremos que $I = (d)$.

Como, $d \in I$ segue que $(d) \subseteq I$. Agora seja $x \in I$. Pelo algoritmo da divisão que $x = dq + r$, onde $0 \leq r < d$. Como $r = x - dq \in I$ e $d = \min I$, temos que $r = 0$, portanto, $x = dq$. Daí, $x \in (d)$. Então $I = (d)$. □

6. Anel de Polinômios sobre um Corpo

Outro exemplo muito importante de domínios principais é o anel de polinômios sobre um corpo. A seguir estudamos este exemplo.

Seja K um corpo e considere $K[x] = \{\sum_{i=0}^{n} a_i x^i \mid a_i \in K; n \in \mathbb{N}\}$. Este anel é um domínio.

A função grau é definida por

$$\begin{aligned} &\deg : K[x] \to \mathbb{N} \\ &\sum_{i=0}^{n} a_i x^i \mapsto n, \text{ onde n é o maior inteiro tal que } a_n \neq 0. \end{aligned}$$

Teorema 6.1. *(Algoritmo da Divisão) Sejam $f, g \in K[x]$ tal que $g \neq 0$. Então existem $q, r \in K[x]$ tais que $f = g.q + r$, onde $r = 0$ ou $\deg r < \deg g$.*

Corolário 6.2. *Sejam $f \in K[x] \setminus K$ e $a \in K$. Então $f(a) = 0$ se e somente se $x - a \mid f$.*

Definição 6.3. *Um corpo K é dito algebricamente fechado se todo $f \in K[x] \setminus K$ admite todas as raízes em K.*

Teorema 6.4. *(Teorema Fundamental da Álgebra) O corpo dos números compleos é um corpo algebricamente fechado.*

Teorema 6.5. *Seja K um corpo. Então $K[x]$ é um domínio principal.*

Demonstração. Seja $I \trianglelefteq K[x]$. Se $I = \{0\}$ então $I = (0)$. Se $I \neq \{0\}$, então existe $p \in I$, $p \neq 0$ tal que $\deg p$ é mínimo em I. Mostremos que $I = (p)$.

Claramente $(p) \in I$, pois $p \in I$. Agora se $f \in I$, pelo algoritmo da divisão existem $q, r \in K[x]$ tais que $f = p.q + r$, onde $r = 0$ ou $\deg r < p$. Como $r = f - pq \in I$, então pela minimalidade do grau de p, temos que $r = 0$ ou seja $f = pq$. Portanto $f \in (p)$. Daí concluímos que $I = (p)$. Logo $K[x]$ é principal. □

Exemplos.

(1) $\mathbb{Q}[x], \mathbb{R}[x]$ e $\mathbb{C}[x]$ são principais.
(2) $\mathbb{Z}[x]$ não é principal. Por exemplo o ideal gerado por 2 e x não é principal.
(3) Seja K um corpo, então $K[x, y]$ não é principal. Por exemplo o ideal (x, y) não é principal,

7. Raízes de um Polinômio

Durante essa seção K reresenta um subcorpo de $\mathbb{C}$.

DEFINIÇÃO 7.1. *Um elemento $\alpha \in \mathbb{C}$ é uma raiz de multiplicidade k, $k \geq 1$ se k é o maior interiro tal que $(x-\alpha)^k \mid f$. Neste caso escrevemos $(x-\alpha)^k \parallel f$. Se $k=1$, $k=2$, $k=3$, etc. diremos respectivamente que α é uma raiz simples, dupla, tripla, etc.*

DEFINIÇÃO 7.2. *Seja $f = a_0 + a_1 x + \cdot + a_n x_n \in K[x]$. A derivada de f é definida e denotada por $f' = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$.*

PROPOSIÇÃO 7.3. *$\alpha \in \mathbb{C}$ é uma raiz simples de f se e somente se $f'(\alpha) \neq 0$.*

DEMONSTRAÇÃO. Temos

$$f(\alpha) = 0 \Leftrightarrow x - \alpha \mid f \Leftrightarrow \exists q \in K[x] \text{ tal que } f = (x-\alpha)q$$

Agora $f' = (x-\alpha)q' + q$, então $f'(\alpha) = q(\alpha)$. Logo, α é uma raiz simples de f se e somente se $f(\alpha) = 0$ e $q(\alpha) \neq 0$ ou seja $f'(\alpha) \neq 0$. □

Exemplos.

(1) Seja $f = x^n - 1 \in \mathbb{C}[x]$. Temos que $f(\omega^r) = 0, r = 0, \ldots, n-1$, onde $\omega = e^{\frac{2\pi i}{n}}$. Como $f' = nx^{n-1}$ e $f'(\omega^r) \neq 0$, seque que $1, \omega, \omega^2, \ldots, \omega^{n-1}$ são raízes simples de f.
(2) Em geral todas as raízes de $f = x^n - \alpha \in \mathbb{C}[x]$, $\alpha > 0$, são $\sqrt[n]{\alpha}$, $\sqrt[n]{\alpha}\omega$, $\sqrt[n]{\alpha}\omega^2, \ldots, \sqrt[n]{\alpha}\omega^{n-1}$, onde $\omega = e^{\frac{2\pi i}{n}}$.

8. Polinômios Irredutíveis

Durante essa seção, sempre K representa um corpo.

DEFINIÇÃO 8.1. *Seja $0 \neq f \in K[x]$. Dizemos que f é irredutível em K, se $f \notin K$ e se $f = gh$ com $g, h \in K[x]$ então $g \in K$ ou $h \in K$; i.é, f não admite nenhum divisor g tal que $0 < \deg g < \deg f$.*

Observações.

(1) Se $\deg f = 1$, então f é irredutível.
(2) Se $\deg f = 2$ ou $\deg f = 3$ tal que f não tem raízes em K então f é irredutível em K.
(3) Seja $f \in \mathbb{R}[x]$ então f é irredutível se e somente se $\deg f = 1$ ou $f = ax^2 + bx + c$ tal que $a \neq 0$ e $\Delta = b^2 - 4ac < 0$.
(4) Seja $f \in \mathbb{C}[x]$, então f é irredutível se e somente se $\deg f = 1$.

8.1. Critérios de Irredutibilidade.

DEFINIÇÃO 8.2. *Seja $f = a_0 + a_1x + \cdots + a_nx_n \in \mathbb{Z}[x]$. O número $c(f) = mdc(a_0, a_1, \ldots, a_n)$ é chamado de conteúdo de f. Se $c(f) = 1$, diremos que f é primitivo.*

Admitiremos o seguinte lema[1].

LEMA 8.3. *(Gauss) Seja $f \in \mathbb{Z}[x]$ com $c(f) = 1$. Se f é irredutível sobre $\mathbb{Z}$ então f é irredutível sobre $\mathbb{Q}$.*

8.1.1. *Critério de Eisenstein (C.E.).* Seja $f = a_0 + \cdots + a_nx_n \in \mathbb{Z}[x]$. Se existir p um número primo tal que para todo $0 \leq i \leq n-1$, $p \mid a_i$, $p \nmid a_n$ e $p^2 \nmid a_0$. Então f é irredutível sobre $\mathbb{Q}$.

DEMONSTRAÇÃO. Podemos supor que $mdc(a_0, a_1, \ldots, a_n) = 1$, pois colocando em evidência $mdc(a_0, a_1, \ldots, a_n)$ os seus coeficientes satisfazem as condições acima. Assim, pelo lema de Gauss basta provarmos que f é irredutível sobre $\mathbb{Z}$.

Suponha que f seja redutível; i.é, $f = gh$ com $g, h \in \mathbb{Z}[x]$ com $1 \leq \deg g < \deg f$ e $1 \leq \deg h < \deg f$. Pondo $g = \sum_{i=0}^{r} b_ix_i$ e $h = \sum_{i=0}^{s} c_ix^i$ temos que $a_k = \sum_{i+j=k} b_ic_j$. Como $p \mid a_0 = b_0c_0$ temos $p \mid b_0$ ou $p \mid c_0$ e não ambos pois $p^2 \nmid a_0$. Sem perder generalidade, suponha que $p \mid c_0$ e $p \nmid b_0$. Temos ainda $p \nmid a_n = b_rc_s$, então $p \nmid b_r$ e $p \nmid c_s$. Assim, $p \mid c_0$ e $p \nmid c_s$ então existe o menor t tal que tal que $p \nmid c_t$.

Se $t < n$ então $b_0c_t = a_t - (b_1c_{t-1} + \cdots + b_tc_0)$. Pela escolha de t temos que $p \mid (b_1c_{t-1} + \cdots + b_tc_0)$ e por hipótese $p \mid a_t$, destes fatos segue que $p \mid b_0c_t$, e isto não ocorre pois $p \nmid b_0$ e $p \nmid c_t$. Logo, $t = n$. Sendo $s \leq n = t \leq s$ concluímos que $n = s$. Daí, $\deg h = \deg f$ e então $\deg g = 0$. Portanto, f é irredutível em $\mathbb{Z}$. □

Exemplos.

(1) Dado $f = x^5 - 6x^3 + 12x^2 - 4x + 6 \in \mathbb{Z}[x]$. Tome $p = 2$. Temos as condições do C.E. satisfeitas e portanto f é irredutível sobre $\mathbb{Q}$.
(2) $f = x^n - p$, onde p um número primo, é irredutível sobre $\mathbb{Q}$ pelo C.E.

8.1.2. Sejam $f \in K[x]$ e $a \in K$. Então f é irredutível sobre K se e somente se $f(x + a)$ é irredutível sobre K.

[1]Este lema será provado em Álgebra II, em domínios chamados de Domínios Fatoriais.

DEMONSTRAÇÃO. Claramente $\phi_a : K[x] \to K[x]$ tal que $\phi_a(f(x)) = f(x+a)$ é um isomorfismo. Suponha $f = gh$, $g, h \in K[x]$ então $\phi_a(f) = \phi_a(g)\phi_a(h)$. Como $\forall p \in K[x]; \deg p = \deg(\phi_a(p))$, segue que f é irredutível sobre K se e somente se $\phi_a(f)$ é irredutível sobre K. □

Exemplo. Seja $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, onde p é um número primo. Temos que Φ_p é irredutível sobre $\mathbb{Q}$. De fato, $\Phi_p(x) = \frac{x^p-1}{x-1}$, então

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \begin{pmatrix} p \\ 1 \end{pmatrix} x^{p-2} + \cdots + \begin{pmatrix} p \\ p-2 \end{pmatrix} x + \begin{pmatrix} p \\ p-1 \end{pmatrix}.$$

Como, $p \mid \begin{pmatrix} p \\ i \end{pmatrix}$, para todo $1 \leq i \leq p-1$ e $p^2 \nmid p = \begin{pmatrix} p \\ p-1 \end{pmatrix}$ segue pelo C.E. que $\Phi_p(x+1)$ é irredutível sobre $\mathbb{Q}$ e portanto p é irredutível sobre $\mathbb{Q}$.

8.1.3. Sejam p um número primo e $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ definida por

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

Suponha que $p \nmid a_n$ e f é irredutível sobre $\mathbb{Z}_p$ então f é irredutível sobre $\mathbb{Z}$.

DEMONSTRAÇÃO. Claramente φ é um homomorfismo. Suponha que $f = gh$ com $g, h \in \mathbb{Z}[x]$. Então $\overline{f} = \overline{g}\overline{h}$. Pondo $g = \sum_{i=0}^{r} b_i x_i$ e $h = \sum_{i=0}^{s} c_i x^i$ temos que $a_n = b_r c_s$. Como $p \nmid a_n$, $p \nmid b_r$ e $p \nmid c_s$, daí $\deg \overline{g} = \deg g$ e $\deg \overline{h} = \deg h$. Da irredutibilidade de $\bar{f}$ sobre $\mathbb{Z}_p$ concluímos que $\deg \overline{g} = 0$ ou $\deg \overline{h} = 0$. Daí $\deg g = 0$ ou $\deg h = 0$, e com isto concluímos que f é irredutível sobre $\mathbb{Z}$. □

Exemplos.

(1) Seja $f = x^3 + 6x^2 + 5x + 25 \in \mathbb{Z}[x]$. Tomando $p = 3$ obtemos $\bar{f} = x^3 + \overline{2}x + \overline{1} \in \mathbb{Z}_3[x]$. Como, $\overline{f}(\overline{0}) = \overline{f}(\overline{1}) = \overline{f}(\overline{2}) = \overline{1}$ e $\deg \overline{f} = 3$, segue que $\overline{f}$ é irredutível sobre $\mathbb{Z}_3$. Logo, f é irredutível sobre $\mathbb{Z}$.

(2) Seja $f = x^4 + 10x^3 + 15x^2 + 2 \in \mathbb{Z}[x]$. Tomando $p = 5$, $\overline{f} = x^4 + \overline{2} \in \mathbb{Z}_5[x]$. Como $\overline{f}(\overline{0}) = \overline{2}, \overline{f}(\overline{1}) = \overline{f}(\overline{2}) = \overline{f}(\overline{3}) = \overline{f}(\overline{4}) = \overline{3}$, $\overline{f}$ não tem raízes em $\mathbb{Z}_5$ ou seja não pode ser decomposto em produto de polinômios de grau 1 e 3. Suponha que $\overline{f} = (x2 + \overline{a}x + \overline{b})(x^2 + \overline{c}x + \overline{d})$ temos então

$$\begin{cases} \overline{a}+\overline{c}=\overline{0}, & \text{(i)} \\ \overline{a}\overline{d}+\overline{b}\overline{c}=\overline{0}, & \text{(ii)} \\ \overline{d}+\overline{ac}+\overline{b}=\overline{0}, & \text{(iii)} \\ \overline{bd}=\overline{2}, & \text{(iv)} \end{cases}$$

De (ii) e (iii) concluímos $\overline{a}=\overline{0}$ ou $\overline{b}=\overline{d}$.

- $\overline{a}=\overline{0} \Rightarrow \overline{c}=\overline{0} \overset{iii}{\Rightarrow} \overline{d}=-\overline{b} \overset{iv}{\Rightarrow} \overline{b}^2=-\overline{2}=\overline{3}$.
- $\overline{b}=\overline{d} \overset{iv}{\Rightarrow} \overline{b}^2=\overline{2}$.

Mas como não existe $x \in \mathbb{Z}_5$ tal que $x^2=\overline{2}$ ou $x^2=\overline{3}$, segue que $\overline{f}$ não pode ser decomposto em produto de polinômios de grau 2. Logo $\overline{f}$ é irredutível em $\mathbb{Z}_5$ e portanto f é irredutível em $\mathbb{Z}$.

Definição 8.4. *Sejam $K \subseteq L$ corpos e $\alpha \in L$. Dizemos que α é algébrico sobre K se existe $0 \neq f \in K[x]$ tal que $f(\alpha)=0$. Caso contrário α é dito transcendente sobre K. O polinômio mônico $0 \neq p \in K[x]$ de menor grau tal que $p(\alpha)=0$ é chamado de polinômio minimal de α sobre K, denotado por $irr\alpha|_K$*

Observação. Temos claramente que $irr\alpha|_K$ é irredutível sobre K.

Exemplos.

(1) Seja $\alpha=\sqrt[3]{2}$. Temos que $\alpha^3=2$ e portanto para $p=x^3-2 \in \mathbb{Q}[x]$ temos $p(\alpha)=0$. Pelo C.E., p é irredutível e assim, $p=irr\alpha|_{\mathbb{Q}}$.

(2) Seja $\alpha=\sqrt{1+\sqrt{5}}$. Temos

$$\alpha^2=1+\sqrt{5} \Rightarrow (\alpha^2-1)^2=5 \Rightarrow \alpha^4-2\alpha^2-4=0.$$

Então $p=x^4-2x^2-4 \in \mathbb{Q}[x]$ tal que $p(\alpha)=0$. Mostremos que $p=irr\alpha|_{\mathbb{Q}}$. Para isso utilizamos o critério (8.1.3). Tome $p=3$, entãp $\overline{p}=x^4-\overline{2}x^2-\overline{1} \in \mathbb{Z}_3[x]$. Como $\overline{p}$ não admite raízes em Z_3, não tem fatores de grau 1 ou 3. Suponha que $\overline{p}=(x^2+\overline{a}x+\overline{b})(x^2+\overline{c}x+\overline{d})$. Então

$$\begin{cases} \overline{a}+\overline{c}=\overline{0} \\ \overline{a}\overline{d}+\overline{b}\overline{c}=\overline{0} \\ \overline{d}+\overline{ac}+\overline{b}=\overline{1} \\ \overline{bd}=\overline{2} \end{cases}$$

Este sistema não tem solução em $\mathbb{Z}_3$; i.é, $\overline{p}$ não se fatora em produto de polinômios de graus 2. Assim, $\overline{p}$ é irredutível em $\mathbb{Z}_3[x]$. Então p é irredutível sobre $\mathbb{Z}$ e pelo lema de Gauss é irredutível sobre $\mathbb{Q}$.

8.2. Exercícios.

(1) Mostre que os polinômios abaixo são irredutíveis sobre $\mathbb{Q}$.
   (a) $f = x^n - p$, p é um primo.
   (b) $f = x^3 + 6x^2 + 5x + 25$ (Dica : use $\mathbb{Z}_3[x]$)
   (c) $f = x^3 + 6x + 1$ (Dica: use $f(x-1)$)
   (d) $f = x^4 + x^3 + x^2 + x + 1$.

(2) Seja $f \in K[x]$, irredutível. Mostre que:
   (a) Se $0 \neq g \in K[x]$ e $f \nmid g$ então $mdc(f, g) = 1$.
   (b) Se $g, h \in K[x]$ tais que $f \mid gh$ então $f \mid g$ ou $f \mid h$.

(3) Seja $f \in \mathbb{Q}[x]$, irredutível. Seja $\alpha \in \mathbb{C}$ tal que $f(\alpha) = 0$. Mostre se $g \in \mathbb{Q}[x]$ tal que $g(\alpha) = 0$ então $g \in (f)$.

(4) Mostre que todo elemento de $\mathbb{Z}_p$ é raiz do polinômio $f = x^p - x$.

(5) Determine o polinômio minimal de $\sqrt{2} + \sqrt{3}$, $\sqrt[p]{p}$ e $e^{\frac{2\pi i}{p}}$, sobre $\mathbb{Q}$. (p é um primo.)

Apêndice 1

Indução Finita

Dado $a \in \mathbb{N}$, seja $P(n)$ uma sentença associada a cada $n \in \mathbb{N}$, com $n \geq a$. Se as condições abaixo são verificadas:

(1) $P(a)$ é verdadeira.

(2) Se $P(k)$ é verdadeira para $k \geq a$, então $P(k+1)$ também é verdadeira.

Então $P(n)$ é verdadeira para todo $n \geq \mathbb{N}$ tal que $n \geq a$.

DEMONSTRAÇÃO. Seja $S := \{x \in \mathbb{N} \mid x \geq a \text{ e } P(x) \text{ seja falsa}\}$. Mostremos que $S = \emptyset$. Se $S \neq \emptyset$, como S é limitado inferiormente então pelo PBO, existe $b = \min S$. Como por (1), $P(a)$ é verdadeira, temos que $b > a$. Sendo, $b = \min S$ concluímos que $P(x)$ é verdadeira para todo $x \in \mathbb{Z}$ tal que $a \leq x < b$. Então por (2) segue que $P(b)$ é verdadeira, o que é um absurdo pois $b \in S$. □

Observação. Substituindo-se (2) por

(2)' Dado $r > a$, se $P(k)$ é verdadeira para todo k, $a \leq k < r$, então $P(r+1)$ também é verdadeira.

o teorema se mantém verdadeiro.

Teorema Fundamental da Aritmética

Seja $a \in \mathbb{Z}$, $a \neq 0, \pm 1$. Então existem únicos números primos positivos $p_1, \ldots, p_n$ (a menos da ordem) tais que $a = \pm p_1 \cdots p_n$.

DEMONSTRAÇÃO. Provaremos o teorema usando a indução. Se a é um número primo, nada há para provar. Suponha então que a não seja um número primo. Seja $S = \{x \in \mathbb{Z} \mid x > 1, x \mid a\}$. Temos que $S \neq \emptyset$, pois $a \in S$ ou $-a \in S$. Como S é limitado inferiormente, então pelo PBO, existe $p = \min S$. Calaramente p é um número primo. Assim, $p \mid a$, então existe $q \in \mathbb{Z}$ tal que $a = bp$ com $0 < |b| < |a|$. Pela hipótese da indução, existem únicos números primos positivos $p_1, \ldots, p_r$ tais que $b = \pm p_1 \cdots p_r$ e daí, $a = bp = \pm p_1 \cdots p_n$.

Para a unicidade; se existem números primos positivos $q_1, \ldots, q_m$ tais que $a = \pm q_1 \cdots q_m$, então $p_1 \cdots p_n = q_1 \cdots q_m$, então $p_1 \mid q_1 \cdots q_m$, daí existe i tal que $p_1 \mid q_i$ ou $q_i = p_1$. Reordenando os q_i's, podemos supor que $i = 1$ e daí, $p_2 \cdots p_n = q_2 \cdots q_m$. Usando o argumento acima repetidas vezes, concluímos que $n = m$ e $q_i = p_i$, $i = 1, \cdots, n$. □

Apêndice 2

Função de Euler

Como já vimos a função de Euler é uma função $\phi : \mathbb{N} \to \mathbb{N}$ dada por

$$\varphi(n) = \#\{m \in \mathbb{N} \mid 1 \leq m < n \text{ tal que } mdc(m,n) = 1\}.$$

TEOREMA 8.5. *Se $mdc(m,n) = 1$ então $\phi(mn) = \phi(m)\phi(n)$.*

DEMONSTRAÇÃO. Considere os números de 1 até mn dispostos como na tabela abaixo.

1	$m+1$	$2m+1$	$\cdots$	$\cdots$	$(n-1)m+1$
2	$m+2$	$2m+2$	$\cdots$	$\cdots$	$(n-1)m+2$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
r	$m+r$	$2m+r$	$\cdots$	$\cdots$	$(n-1)m+r$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
m	$2m$	$3m$	$\cdots$	$\cdots$	mn

Cada elemento x dessa tabela é da forma $x = km + r$, $0 \leq k \leq n-1$ e $1 \leq r \leq m$.

Afirmação 1. Se $mdc(x,m) = 1$ então $mdc(r,m) = 1$.

De fato,

$$d = mdc(r,m) \Rightarrow d \mid r, d \mid m \Rightarrow d \mid km + r, d \mid m \Rightarrow d \mid x, d \mid m \Rightarrow d = 1.$$

Como, $1 \leq r \leq m$, então da afirmação temos que $\phi(m)$ é o número de linhas tais que todo x nessas linhas têm $mdc(x,m) = 1$.

Afirmação 2. $\{\overline{r}, \overline{m+r}, \ldots, \overline{(n-1)m+r}\} = \{\overline{0}, \ldots, \overline{n-1}\}$.

Para provarmos a afirmação, bata provarmos que os elementos de $\{\overline{r}, \overline{m+r}, \ldots, \overline{(n-1)m+r}\}$ são distintos ou seja se $x = im + r$ e $y = jm + r$, $i \neq j$ então $\overline{x} \neq \overline{y}$. Suponha que $\overline{x} = \overline{y}$ então $x \equiv y(modn)$ e daí,

$$n \mid x - y \Rightarrow n \mid (i-j)m \Rightarrow n \mid (i-j) \Rightarrow i = j \Rightarrow x = y,$$

que é absurdo.

Afirmação 3. Se $mdc(x,n) = 1$ e $x \equiv s(mod n)$ com $0 \leq s < n$ então $mdc(s,n) = 1$.

De fato,

$$x \equiv s(mod n) \Rightarrow s = x + nq, q \in \mathbb{Z}$$

e

$$d = mdc(s,n) \Rightarrow d \mid s, d \mid n \Rightarrow d \mid s - nq, d \mid n \Rightarrow d \mid x, d \mid n \Rightarrow d = 1.$$

Como $0 \leq s < n$ então das afirmações 2 e 3 temos que existem $\phi(n)$ elementos em cada uma das $\phi(m)$ linhas tais que $mdc(x,n) = 1$.

Assim, existem $\phi(m)\phi(n)$ elementos x na tabela tais que $mdc(x,m) = 1$ e $mdc(x,n) = 1$. Como $mdc(m,n) = 1$, temos que $mdc(x,mn) = 1$, $mdc(x,m) = 1$ e $mdc(x,n) = 1$ e portanto, $\phi(m)\phi(n) = \phi(mn)$. □

LEMA 8.6. *Se p é um número primo então $\phi(p^n) = p^n - p^{n-1}$.*

DEMONSTRAÇÃO. Se $mdc(x,p^n) \neq 1$ temos $x = p^r$ para algum $r = 1, \ldots, n-1$ então $\phi(p^n) = p^n - p^{n-1}$. □

COROLÁRIO 8.7. *Seja $n = p_1^{n_1} \ldots p_r^{n_r}$, onde p_i 's são primos distintos e $n_i \in \mathbb{N}$. Então $\phi(n) = n\Pi_{i=1}^{r}(1 - \frac{1}{p_i})$.*

DEMONSTRAÇÃO. Exercício! □

Apêndice 3

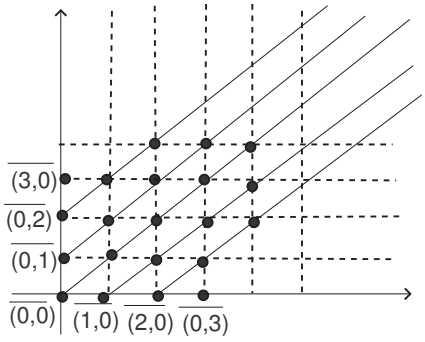
Construção do Anel dos Inteiros

Seja R uma relação definida sobre $\mathbb{N} \times \mathbb{N}$ por

$$(a,b)R(c,d) \Leftrightarrow a+d = b+c.$$

Claramente R é uma relação de equivalência.(veja exercício 9 em Exercícios 2.1)

Sejam $x = \overline{(a,b)}, y = \overline{(c,d)} \in (\mathbb{N} \times \mathbb{N})/R$;



- $x = y \Leftrightarrow a+d = b+c$,
- Definimos a *adição* como sendo

$$x + y := \overline{(a+c, b+d)}$$

e a *multiplicação* por

$$x \cdot y := \overline{(ac+bd, ad+bc)}$$

Essas operações estão bem definidas, comutativas e temos:

- $\overline{(a,b)} + \overline{(0,0)} = \overline{(a,b)}$ ou seja $\overline{(0,0)}$ é o elemento neutro da adição,
- $\overline{(a,b)} + \overline{(b,a)} = \overline{(0,0)}$ ou seja $\overline{(b,a)}$ é a inversa de $\overline{(a,b)}$.

Pela definição de adição temos

$$\overline{(a,b)} = \overline{(a,0)} + \overline{(0,b)}.$$

Denotamos $\overline{(a,0)}$ por a, observamos que $\overline{(b,0)} + \overline{(0,b)} = \overline{(0,0)}$, então denotamos $\overline{(0,b)}$ por $-b$.

O **conjunto dos inteiros** é definido como sendo $\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

Teorema. O conjuntos dos inteiros munido de adição e multiplicação definidas acima é um anel comoutativo com unidade.

Ordem em $\mathbb{Z}$

Considere a seguinte relação sobre $\mathbb{Z}$;

$$x \preceq y \Leftrightarrow a + d \leq b + c.$$

Essa relação é uma relação de ordem total e é compatível com a adição; i.e, se $x \preceq y$ então $x + z \preceq y + z$.

Dizemos que $x \in \mathbb{Z}$ é *positivo* (resp. *negativo*) se $0 \prec x$ (resp. $x \prec 0$).

Teorema. A aplicação $f : \mathbb{N} \to \mathbb{Z}$ definida por $f(a) = \overline{(a, 0)}$ é injetiva e ainda $f(a + b) = f(a) + f(b)$ e $f(ab) = f(a)f(b)$.

Esse teorema permite identificar $\mathbb{N}$ como *subconjunto* de $\mathbb{Z}$. De fato $\mathbb{N}$ é o conjunto dos *inteiros positivos*. Então podemos escrever $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N}) \cup \{0\}$.

Regra de Sinais

Para quaisquer $a, b \in \mathbb{N}$,

(1) $a + b, ab \in \mathbb{N}$.

(2) Se $a \geq b$ então $a - b \in N$.

(3)

Finalmente temos

Teorema. O anel $\mathbb{Z}$ é um anel de integridade.

Apêndice 4

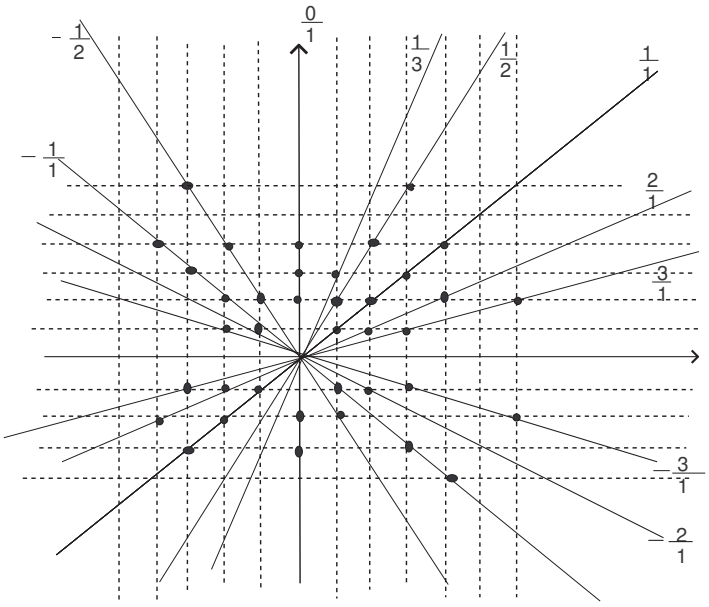
Construção do Corpo dos Racionais

Seja $\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$ e considere a seguinte relação sobre $\mathbb{Z} \times \mathbb{Z}^*$:

$$(a, b)R(c, d) \Leftrightarrow ad = bc.$$

Claramente R é uma relação de equivalênica. Escrevemos $\frac{a}{b}$ para a classe $\overline{(a, b)}$ e consideramos o conjunto quociente $\mathbb{Z}\times\mathbb{Z}^*/R$. Este conjunto é chamado do **conjunto dos números racionais**:

$$\mathbb{Q} := \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z}^*\}.$$



Definimos a adição e multiplicação em $\mathbb{Q}$ por:

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

Essas operações estão bem definidas e temos:

Teorema. O conjunto dos números racinais munido das operações definidas acima é um corpo.

Ordem em $\mathbb{Q}$

Sejam $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, define-se

$$\frac{a}{b} \preceq \frac{c}{d} \Leftrightarrow ad \leq bc.$$

Temos que " $\preceq$ " é uma relação de ordem total em $\mathbb{Q}$ e é *compatível com a adição:*

$$\frac{a}{b} \preceq \frac{c}{d} \Rightarrow \frac{a}{b} + \frac{e}{f} \preceq \frac{c}{d} + \frac{e}{f}.$$

Teorema. A aplicação $f : \mathbb{Z} \to \mathbb{Q}$ definida por $f(a) = \frac{a}{1}$ é injetiva e ainda $f(a+b) = f(a) + f(b)$ e $f(ab) = f(a)f(b)$.

Esse teorema permite identificar $\mathbb{Z}$ como *subanel* de $\mathbb{Q}$.