Universidade de São Paulo
Instituto de Matemática e Estatística

Introdução à Teoria dos Números

Aluno: Almir Junior
Bolsista PIBIC do CNPq

Orientador: Dr. Konstyantin Iusenko
Departamento de Matemática

São Paulo
2021

Conteúdo

Introdução

Esse projeto foi guiado por um tipo de problema muito antigo mas que ainda sim é batante estudado, o problema consiste em determinar soluções para equações diofantinas. Essas equações são expressões polinomiais da forma $p(x_1, ..., x_n) = 0$ com coeficientes inteiros, e as soluções desejadas são aquelas dadas por números inteiros. Por exemplo: $x^2 + y^2 = z^2$ e $y^2 = x - 3$, são equações diofantinas, a trinca $(3, 4, 5)$ é um resultado para o primeiro exemplo. Podemos buscar soluções racionais para equações diofantinas e a partir delas encontrar soluções inteiras. O nome para esse tipo de equação vem de Diofanto de Alexandria, pois foi ele um dos primeiros a publicar um compilado de resultados sobre esse tipo de equação e propriedades envolvendo números inteiros.

Na primeira parte do projeto estudamos algumas estruturas algébricas, que nos permitem caracterizar de forma precisa certos tipos de conjuntos. A partir do capítulo três passamos a estudar conjuntos que possuem propriedades que possibilitam encontrar soluções para equações diofantinas, por exemplo os inteiros de Gauss $\mathbb{Z}[i]$. Vimos também que esses conjuntos possuem propriedade semelhantes ao conjunto dos números inteiros $\mathbb{Z}$, pois ambos são domínios euclidianos, para isso provamos que o algoritmo da divisão euclidiana é consistente em cada conjunto em questão. Após isso estudamos sobre ternas pitagóricas e soma de dois quadrados.

Na última parte do projeto, estudamos de forma introdutória a teoria das curvas elípticas. Essa teoria, por sua vez, possibilitou um resultado sobre a famosa equação diofantina $x^n + y^n = z^n$, teorema conhecido como *o último teorema de Fermat*. Nessa fase do projeto vimos que é possível escrever algumas equações diofantinas na forma de uma curva elíptica e que os pontos racionais de uma curva elíptica é um grupo abeliano finitamente gerado, resultado conhecido como teorema de Mordell-Weil. Também abordamos, num caso particular, a definição da operação que dá origem a esse grupo abeliano. Por final, vimos que o teorema da uniformização possibilita a interpretação de uma curva elíptica como um torus. Ao longo de cada secção, faremos menção aos principais livros utilizados.

Capítulo 1

Grupos

Neste capítulo abordaremos de forma introdutória um ramo importante da Álgebra. As principais referências usadas para esse assunto foram, [4, Abstract algebra] e[6, Introdução à álgebra]. Queremos usar uma operação entre dois elementos de um conjunto a fim de obter um terceiro objeto desse mesmo conjunto. Essa operação possue suas particularidades e define um tipo específico de conjunto, o qual chamamos de grupo. Vale ressaltar que, o símbolo que denotará tal operação é o mesmo utilizado para representar a multiplicação da aritmética usual, porém não se trata especificamente da multiplicação comum.

1.1 Grupos

Definição 1.1. Seja G um conjunto o qual possui uma operação binária denotada por:

$$\begin{aligned} \cdot : G \times G &\to G \\ (a, b) &\mapsto a \cdot b \end{aligned}$$

Dizemos que o par $(G, \cdot)$ é um grupo se satisfaz os seguintes axiomas:

(G1) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad, \forall a, b, c \in G$

(G2) $\exists e_G \in G : a \cdot e_G = e_G \cdot a = a \quad, \forall a \in G$

(G3) $\forall a \in G, \exists a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e_G$

Comentário 1.1. O axioma (G1) é a associatividade da operação $\cdot$ definida no conjunto, e o elemento e_G do axioma (G2) é a identidade do conjunto G, isto é, o elemento neutro da operação $\cdot$ em G. Se não houver ambiguidade na interpretação da identidade de um grupo, denotaremos e_G simplesmente por e. O axioma (G2) garante que um grupo é sempre não vazio. A notação a^{-1} não simboliza, necessariamente, a razão $1/a$, mas sim o inverso do elemento $a \in G$ em relação à operação definida em G.

Definição 1.2. Se G é um conjunto finito, dizemos que $(G, \cdot)$ é um grupo finito e a ordem de $(G, \cdot)$ é igual ao número de elemento de G, caso contrário dizemos que $(G, \cdot)$ é um grupo infinito.

Proposição 1.1. *Seja $(G, \cdot)$ um grupo. Então:*

(i) *A identidade e de G é única.*

(ii) *Para cada $a \in G$, a^{-1} é unicamente determinado.*

(iii) $(a^{-1})^{-1} = a, \forall a \in G$.

(iv) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

Demonstração. (i) Suponha que exista outra identidade em G, digamos f. Então pelo axioma (G2) temos $e = e \cdot f$. Pelo mesmo axioma vem $f = e \cdot f$. Portando, temos que $e = f$. Logo, a identidade é única.

(ii) Suponha que exista outro elemento $b \in G$ tal que $a \cdot b = b \cdot a = e$. Então temos que $a \cdot b = e$. Fazendo a operação com a^{-1} pela esquerda e usando os axiomas (G1) e (G2) obtemos:

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot e \implies (a^{-1} \cdot a) \cdot b = a^{-1} \implies b = a^{-1}$$

Portanto, a^{-1} é únicamente determinado.

(iii) Tome $a \in G$. Pelo axioma (G3) existe $a^{-1} \in G$ inverso de a e pelo mesmo axioma existe $(a^{-1})^{-1} \in G$ tal que $a^{-1} \cdot (a^{-1})^{-1} = e$. Então, fazendo a operação pela direita nessa igualdade e utilizando (G1) e (G2) segue que:

$$a \cdot [a^{-1} \cdot (a^{-1})^{-1}] = a \cdot e \implies (a \cdot a^{-1}) \cdot (a^{-1})^{-1} = a \implies (a^{-1})^{-1} = a.$$

(iv) Tome $a, b \in G$. Pelo axioma (G3) existem $a^{-1}, b^{-1} \in G$ inversos de a e b respectivamente. Também, $a \cdot b \in G$, novamente pelo (G3), existe $(a \cdot b)^{-1} \in G$ tal que $e = (a \cdot b)^{-1} \cdot (a \cdot b)$. Assim, fazendo a operação com b^{-1} pela direita e utilizando os axiomas (G1) e (G2) obtemos:

$$\begin{aligned} e \cdot b^{-1} &= [(a \cdot b)^{-1} \cdot (a \cdot b)] \cdot b^{-1} \\ &= (a \cdot b)^{-1} \cdot [(a \cdot b) \cdot b^{-1}] \\ &= (a \cdot b)^{-1} \cdot [a \cdot (b \cdot b^{-1})] \\ &= (a \cdot b)^{-1} \cdot a \end{aligned}$$

Logo $b^{-1} = (a \cdot b)^{-1} \cdot a$. Agora, fazendo o mesmo com a^{-1} obtemos:

$$\begin{aligned} b^{-1} \cdot a^{-1} &= [(a \cdot b)^{-1} \cdot a] \cdot a^{-1} \\ &= (a \cdot b)^{-1} \cdot (a \cdot a^{-1}) \\ &= (a \cdot b)^{-1} \end{aligned}$$

$\square$

Definição 1.3. Para qualquer grupo G, para quaisquer $x \in G$ e $n \in \mathbb{Z}^+$, definimos $x^n = x \cdots x(n$ termos), $x^{-n} = x^{-1} \cdots x^{-1}(n$ termos) e $x^0 = e$ sendo e a identidade de G.

Proposição 1.2. *Seja G um grupo e sejam $x \in G$ e $a, b \in \mathbb{Z}^+$. Então:*

(1) $x^{a+b} = x^a x^b$.

(2) $x^{ab} = (x^a)^b$.

(3) $(x^a)^{-1} = x^{-a} = (x^{-1})^a$.

Demonstração. (1) Se $a = b = 0$, temos que $x^a x^b = ee = e = x^{a+b}$. Suponha que ou $a \neq 0$ ou $b \neq 0$, digamos $a \neq 0$. Vamos fazer indução em b. Para o caso da base, suponha que $b = 0$. Assim temos que $x^{a+b} = x^a = x^a e = x^a x^b$. Suponha idutivamente que $x^{a+b} = x^a x^b$ para todo $0 \leq b \leq k$ para algum $k \in \mathbb{Z}^+$, vamos mostrar que vale para $b = k+1$. Fazendo $b = k+1$, temos que $x^{a+b} = x^{a+(k+1)} = x^{(a+k)+1} = x^{a+k}x$. Pela hipótese indutiva obtemos $x^{a+k}x = (x^a x^k)x = x^a(x^k x) = x^a x^{k+1} = x^a x^b$. O que finaliza a indução.
(2) Se $a = b = 0$, temos que $(x^a)^b = e^b = e = ee = x^{ab}$. Suponha que ou $a \neq 0$ ou $b \neq 0$, digamos $a \neq 0$.Vamos fazer indução em b. Para o caso da base, suponha que $b = 0$. Daí temos que $(x^a)^b = e = x^{ab}$. Suponha indutivamente que $(x^a)^b = x^{ab}$ para todo $0 \leq b \leq k$, para algum $k \in \mathbb{Z}^+$, vamos provar que vale para $b = k+1$. Considere $b = k+1$, daí temos que $(x^a)^b = (x^a)^{k+1}$, o que por (1) implica em $(x^a)^{k+1} = (x^a)^k x^a$. Pela hipótese indutiva e por (1) vem $(x^a)^k x^a = x^{ak}x^a = x^{ak+a} = x^{a(k+1)} = x^{ab}$. Assim, finalizamos a indução.
(3) Se $a = o$, temos que $(x^a)^{-1} = e^{-1} = e = x^{-a}$. Suponha $a \neq 0$. Fazendo $b = -1$ em (2) temos que $(x^a)^{-1} = x^{a(-1)} = x^{-a}$. Analogamente temos que $(x^{-1})^a = x^{-a}$. $\square$

Proposição 1.3. *Seja G um grupo e sejam $x \in G$ e $a, b \in \mathbb{Z}$. Então:*

(1) $x^{a+b} = x^a x^b$.

(2) $x^{ab} = (x^a)^b$.

Demonstração. Basta utililzar a parte (3) da **Proposição 1.2** na parte (1) e (2). □

Definição 1.4. Sejam G um grupo e $x \in G$. Definimos a ordem de x em relação a G como o menor inteiro positivo n tal que $x^n = e$ e denotamos por $\text{ord}_G(x) = n$. Se não existe n inteiro positivo tal que $x^n = e$, dizemos que x tem ordem infinita.

Proposição 1.4. *Seja G um grupo. Para qualquer $x \in G$ temos que* $\text{ord}_G(x) = \text{ord}_G(x^{-1})$.

Demonstração. Tome $x \in G$ arbitrário. Desde que G é um grupo, temos que $x^{-1} \in G$. Considere $\text{ord}_G(x) = n \in \mathbb{Z}^+$. Pela **Proposição 1.3**(2) obtemos $x^{-n} = (x^n)^{-1} = e^{-1} = e$. Então, $\text{ord}_G(x^{-1}) = n$. Reciprocamente, suponha que $\text{ord}_G(x^{-1}) = n \in \mathbb{Z}^+$. Segue que $x^n = x^{(-n)(-1)} = (x^{-n})^{-1} = [(x^{-1})^n]^{-1} = e^{-1} = e$. Portanto, $\text{ord}_G(x) = \text{ord}_G(x^{-1})$. □

Proposição 1.5. *Seja G um grupo e sejam $a, b \in G$. Então as equações $ax = b$ e $ya = b$ possuem solução única. Em particular temos que as duas implicações abaixo são consistentes G:*

$$au = av \implies u = v \qquad va = ua \implies v = u.$$

Demonstração. Para resolver a equação $ax = b$ basta multiplicar a equação à esquerda por a^{-1}, logo $x = a^{-1}b$. Como a^{-1} é unicamente determinado, temos que $x = a^{-1}b$ também o é. De forma análoga temos que $ya = b$, implica em $y = ba^{-1}$ com esse resultado unicamente determinado. Agora considere $au = av$. Multiplicando a equação por a^{-1} à esquerda obtemos $u = v$. Analogamente temos que $va = ua$ implica em $v = u$. □

Definição 1.5. Dizemos que um grupo $(G, \cdot)$ é um *grupo abeliano* quando:

$$a \cdot b = b \cdot a \quad , \forall a, b \in G$$

Ou seja, um grupo $(G, \cdot)$ é abeliano se a operação definida possui a propriedade comutativa.

Exemplo 1.1. O conjunto dos números inteiros $\mathbb{Z}$ juntamente com a operação de soma $+$ formam um grupo abeliano. Isto é, o par ordenado $(\mathbb{Z}, +)$ é um grupo abeliano no qual $e = 0$ e $a^{-1} = -a$. De forma mais geral, temos que $(\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ são grupos abelianos.

Exemplo 1.2. Os números racionais sem o elemento neutro aditivo(zero), que é denotado por $\mathbb{Q}^*$, com a operação de multiplicação $\cdot$ formam um grupo abeliano. Ou seja, o par ordenado $(\mathbb{Q}^*, \cdot)$ é um grupo abeliano onde $e = 1$ e $a^{-1} = 1/a$. Assim como $(\mathbb{R}, \cdot), (\mathbb{C}, \cdot)$ também são grupos abelianos.

Definição 1.6. Seja $S \subset G$ e G um grupo. Dizemos que G é um grupo gerado por S quando todo elemento de G pode ser escrito como produto finito de elementos de S em relação a operação $\cdot$ de G. Denotamos essa relação por $G = \langle S \rangle$.

Definição 1.7. Se G é um grupo gerado por S e S é um conjunto finito, dizemos que G é um grupo finitamente gerado.

Exemplo 1.3. Desde que $1 \in \mathbb{Z}$ e todo número inteiro pode ser escrito como soma finita de 1 e -1, temos que $(Z, +) = \langle 1 \rangle$. Também, como $\{1\}$ é um conjunto finito e é gerador de $(\mathbb{Z}, +)$, temos que $(\mathbb{Z}, +)$ é finitamente gerado.

Definição 1.8. Seja G um grupo. O conjunto $H \subset G$ é um subgrupo de G se $H \neq \varnothing$ e se H é fechado em relação ao inverso e em relação a operação $\cdot$ definida em G.

Comentário 1.2. A partir da definição acima, para mostrar que H é um subgrupo de G precisamos provar que:

1. $H \neq \varnothing$.
2. Dado qualquer $x \in H$, tem-se $x^{-1} \in H$.
3. Dados quaisquer $x, y \in H$, tem-se $x \cdot y \in H$.

Exemplo 1.4. Qualquer grupo G possui dois subgrupos $H = G$ e $H = e$, onde e é a identidade de G.

Exemplo 1.5. Temos que $\mathbb{Z} \leq \mathbb{Q}$ em relação a operação $+$ de adição.

Exemplo 1.6. Temos também que $\{2k \in \mathbb{Z}; k \in \mathbb{Z}\}$ e $\{2k + 1 \in \mathbb{Z}; k \in \mathbb{Z}\}$ são subgrupos de $\mathbb{Z}$ em relação a operação $+$ de adição.

Proposição 1.6 (Critério de subgrupo)**.** *Sejam G um grupo e $H \subset G$. Então $H \leq G$ se, e somente se:*

(1) $H \neq \varnothing$.

(2) $\forall x, y \in H$ tem-se $xy^{-1} \in H$.

Demonstração. $(\Rightarrow)$ Se $H \leq G$, segue direto da **Definição 1.7** que (1) e (2) são verificadas. $(\Leftarrow)$ Suponha que (1) e (2) são verificadas. Por (1) temos que $H \neq \varnothing$, então tome $x \in H$ qualquer. De (2) temos que $e = xx^{-1} \in H$, ou seja, H contém a identidade de G. Desde que $x, e \in H$, novamente por (2), temos que $ex^{-1} = x^{-1} \in H$. Agora tome $x, y \in H$, pelo o que acabamos de mostrar, temos que $y^{-1} \in H$. Logo, por (2) temos que $x(y^{-1})^{-1} \in H$, então $xy \in H$. Portanto, temos que $H \leq G$. $\square$

1.2 Homomorfismo de grupos e grupo quociente

Definição 1.9. Sejam $(G, \cdot)$ e $(H, \times)$ grupos. Chamamos de *homomorfismo de grupos* é uma função $\varphi : G \to H$ tal que:

$$\varphi(x \cdot y) = \varphi(x) \times \varphi(y), \forall x, y \in G.$$

Definição 1.10. Sejam $(G, \cdot)$ e $(H, \times)$ grupos. Dizemos que uma função $\varphi : G \to H$ é um *isomorfismo* quando φ é bijetiva e, também, um homomorfismo. Nesse caso, dizemos que G e H são isomorfos e escrevemos $G \cong H$.

Comentário 1.3. Dois grupo $(G, \cdot)$ e $(H, \times)$ são isomorfos entre si quando existe um bijeção entre eles que preserva a estrutura de grupo. Podemos intuitivamente observar G e H como o mesmo grupo com o detalhe de que a operação e os elementos são escritos de maneira diferente. Ou seja, qualquer propriedade de G em relação a $\cdot$ é consistente em H em relação a $\times$.

Observação 1.1. A relação $\cong$ que denota quando dois grupos são isomorfos entre si é uma relação de equivalência.

Exemplo 1.7. Temos que $(\mathbb{R}, +) \cong (\mathbb{R}^+, \times)$. De fato, a função $\exp : \mathbb{R} \to \mathbb{R}^+$ dada por $\exp(x) = e^x$, onde e é a a base do logaritmo natural, é tal que $\exp(x + y) = e^{x+y} = e^x e^y$. Desde que $\exp : \mathbb{R} \to \mathbb{R}^+$ é a inversa da função logaritmica $\ln : \mathbb{R}^+ \to \mathbb{R}$, temos exp bijetiva.

Definição 1.11. Sejam G e H grupos e seja φ um homomorfismo $\varphi : G \to H$. O *núcleo(kernel)* de φ é o conjunto

$$\ker \varphi := \{g \in G | \varphi(g) = e_H\}.$$

onde e_h é a identidade de H.

Proposição 1.7. *Sejam G e H grupos e φ um homomorfismo $\varphi : G \to H$.*

(1) $\varphi(e_G) = e_H$.

(2) $\varphi(g^{-1}) = \varphi(g)^{-1}, \forall g \in G$.

(3) $\varphi(g^n) = \varphi(g)^n, \forall n \in Z$

(4) $\ker \varphi \leq G$.

(5) $\mathrm{Im}\varphi \leq H$.

Demonstração. (1) Temos que $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$. Desde que H é um grupo e $\varphi(e_G) \in H$, vale a propriedade cancelativa. Assim $\varphi(e_G) = \varphi(e_G)\varphi(e_G)$, implica em $\varphi(e_G) = e_H$.
(2) Por (1) vem $e_H = \varphi(e_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$. Como $\varphi(g) \in H$, segue que $\varphi(g)^{-1} \in H$. Daí temos que $e_H = \varphi(g)\varphi(g^{-1})$ implica em $\varphi(g)^{-1} = \varphi(g^{-1})$.
(3) Vamos mostrar por indução que a igualdade vale para todo $n \in \mathbb{Z}^+$. Para o caso da base considere $n = 1$ e o resultado é direto. Suponha indutivamente que vale para algum $n \in \mathbb{Z}^+$. Assim, temos que $\varphi(g^{n+1}) = \varphi(g^n g) = \varphi(g^n)\varphi(g) = \varphi(g)^n\varphi(g) = \varphi(g)^{n+1}$, o que finaliza a indução. Agora utilizando (2) obtemos $\varphi(g^{-n}) = \varphi((g^n)^{-1}) = \varphi(g^n)^{-1} = [\varphi(g)^n]^{-1}\varphi(g)^{-n}$. O que finaliza a demonstração.
(4) Por (1) temos que $e_G \in \ker\varphi$, ou seja, $\ker\varphi \neq \varnothing$. Tome $x, y \in \ker\varphi$ arbitrários. Então $\varphi(x) = \varphi(y) = e_H$ e temos $\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = e_H e_H^{-1} = e_h$. Assim, $xy^{-1} \in \ker\varphi$. Portanto, pela **Proposição 1.6** temos que $\ker\varphi \leq G$.
(5) Como $e_H = \varphi(e_G) \in \mathrm{Im}\varphi$, segue que $\mathrm{Im}\varphi \neq \varnothing$. Tome $h_1, h_2 \in \mathrm{Im}\varphi$ quaisquer. Então existem $g_1, g_2 \in G$ tais que $\varphi(g_1) = h_1$ e $\varphi(g_2) = h_2$. Desde que $g_2 \in G$ e $\varphi(g_2) \in H$, temos que $g_2^{-1} \in G$ e $\varphi(g_2)^{-1} \in H$. Assim, como φ é um homomorfismo e por (2), obtemos $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} \in H$. Portanto, pela **Proposição 1.6** temos que $\mathrm{Im}\varphi \leq H$. $\square$

Proposição 1.8. *Sejam G um grupo, $H \leq G$ e $x, y, z \in G$. Então, $x \equiv y \mod H$ se, e somente se, $xy^{-1} \in H$ definie uma relação de equivalência em G.*

Demonstração. Desde que $xx^{-1} = e \in G$, temos $x \equiv x \mod H$. Logo, a relação é reflexiva. Como $x \equiv y \mod H$ se, e somente se, $xy^{-1} \in H$, segue que $yx^{-1} = (xy^{-1})^{-1} \in H$. Assim $y \equiv x \mod H$. Então a relação é simétrica. Agora, se $x \equiv y \mod H$ e $y \equiv x \mod H$, temos $xy^{-1} \in H$ e $yz^{-1} \in H$. Daí $xz^{-1} = (xy^{-1})(yz^{-1}) \in H$, logo $x \equiv z \mod H$. Assim. a relação é transitiva. Portanto é uma relação de equivalência. $\square$

Definição 1.12. Sejam G um grupo, H um subgrupo de G e $x \in G$. Dizemos que $\overline{x} = \{y \in G; y \equiv x \mod H\}$ é uma *classe de equivalência*.

Definição 1.13. Sejam G um grupo, $H \leq G$ e $g \in G$. Dizemos que $Hg := \{hg | h \in H\}$ é uma *classe lateral à direita* de H em G.

Observação 1.2. Temos que $\overline{g} = Hg$. De fato,

$$x \in \overline{g} \iff x \equiv g \mod H \iff xg^{-1} = h \in H \iff x = hg$$

para algum $h \in H$.

Definição 1.14. Definimos o conjunto quociente de G por H(dizemos também G módulo H) por $G/H := \{\overline{g}; g \in G\}$.

Proposição 1.9. *Seja G um grupo e $H \leq G$. Então, para quaisquer $g, h \in G$ tem-se que $\overline{g} \cdot \overline{h} = \overline{g \cdot h}$ define uma operação no conjunto G/H. Além disso, $(G/H, \cdot)$ é um grupo.*

Demonstração. Para provar que a operação do enunciado é uma operação em G/H, precisamos mostrar que a definição independe dos representantes das classes. Sejam $\overline{x} = \overline{a}$ e $\overline{y} = \overline{b}$. Vamos mostrar que $(xy)(ab)^{-1} \in H$. Desde que $xy \cdot (ab)^{-1} = xya^{-1}b^{-1}$ e $\overline{x} = \overline{a}, \overline{y} = \overline{b}$, temos que $xa^{-1}, yb^{-1} \in H$. Agora, se $xa^{-1} = h_1 \in H$ e $yb^{-1} = h_2 \in H$, então:

$$(xy)(ab)^{-1} = x(h_2)a^{-1} = (h_1a)(h_2)a^{-1} = h_1(ah_2a^{-1})$$

como $h_1, ah_2a^{-1} \in H$, segue que $(xy)(ab)^{-1} \in H$. Portanto, a definição independe dos representantes.
Vamos mostrar que $(G/H, \cdot)$ é grupo. Temos que $\overline{e_G} = He_G = H$. Desde que $\overline{e_G} \cdot \overline{g} = \overline{e_G \cdot g} = \overline{g}$ para qualquer $g \in G$, temos que $\overline{e_G}$ é a identidade de G/H. Também temos,

$$\begin{aligned}
\overline{x} \cdot (\overline{y} \cdot \overline{z}) &= \overline{x} \cdot \overline{y \cdot z} \\
&= \overline{x \cdot (y \cdot z)} \\
&= \overline{(x \cdot y \cdot) z} \\
&= \overline{x \cdot y} \cdot \overline{z} \\
&= (\overline{x} \cdot \overline{y}) \cdot \overline{z}.
\end{aligned}$$

Por final, se $\overline{g} \in G/H$, então $\overline{g^{-1}} \in G/H$. E segue que $\overline{g} \cdot \overline{g^{-1}} = \overline{g \cdot g^{-1}} = \overline{e_G}$. O que finaliza a demonstração. $\square$

Teorema 1.1. *Sejam G um grupo, $H \leq G$. Então, G/H é um grupo quociente se, e somente se, H é núcleo de algum homomorfismo.*

Demonstração. ($\Rightarrow$) Suponha que G/H é um grupo quociente. Considere a função $\pi : G \to G/H$ dada por $g \mapsto \pi(g) = \overline{g}$. Vamos mostrar que π é um homomorfismo. É evidente que π é sobrejetiva. Dados $g, h \in G$, temos $\pi(gh) = \overline{gh} = \overline{g} \cdot \overline{h} = \pi(g) \cdot \pi h$. Logo, π é um homomorfismo de grupo. Agora seja $g \in G$ tal que $\pi(g) = \overline{e_G}$. Temos que:

$$\pi(g) = \overline{e_G} \iff \overline{g} = \overline{e_G} \iff x \in H.$$

Portanto, $H = \ker \pi$.
($\Leftarrow$) Suponha que $H = \ker \varphi$ onde $\varphi : G \to F$ é um homomorfismo de

grupo. Assim, pela **Proposição 1.7**(1) temos que $\varphi(e_G) = e_F$, logo $e_G \in H$. Tome $f, g, h \in H$, então pela **Proposição 1.7**(4) temos que $\ker \varphi \leq G$ e, assim, $(fg)h = f(gh)$. Agora, seja $g \in H$. Daí, pela **Proposiçao 1.7**(1) e (2) temos:

$$\begin{aligned} e_F = \varphi(e_G) &= \varphi(gg^{-1}) \\ &= \varphi(g) \cdot \varphi(g^{-1}) \\ &= \varphi(g) \cdot \varphi(g)^{-1} \\ &= e_F \varphi(g)^{-1} = \varphi(g)^{-1} \end{aligned}$$

logo, $g^{-1} \in H$. O que mostra a existência de elemento oposto. Portanto H $\square$

Comentário 1.4. Dizemoque a função π acima é a *projeção canônica* de G em G/H.

Capítulo 2

Anéis

Vimos que a teoria dos grupos possui suas propriedades baseadas em uma única operação binária. Neste capítulo abordaremos conjuntos que têm suas especificidades oriundas de duas operações binárias que chamamos de adição e multiplicação, além disso, são munidos pela lei distributiva. A leitura para essa secçaço foi baseada nos mesmos livros usados para o capítulo anterior, [4] e [6], e também utilizamos a dissertação de mestrado [5, Euclidean rings] para um melhor entendimento do último assunto desse capítulo.

2.1 Anéis e corpos

Definição 2.1. Seja R um conjunto munido de duas operações binárias, soma e multiplicação, respectivamente dadas por:

$$\begin{aligned} + : R \times R &\to R \\ (a,b) &\mapsto a+b \end{aligned} \quad \text{e} \quad \begin{aligned} \cdot : R \times R &\to R \\ (a,b) &\mapsto a \cdot b \end{aligned}$$

Dizemos que a tripla ordenada $(R, +, \cdot)$ é um anel quando são satisfeitos os seguintes axiomas:

(R1) $(R, +)$ é um grupo abeliano

(R2) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad, \forall a, b, c \in R$

(R3) $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a \quad, \forall a, b, c \in R$

Por simplicidade escreveremos ab ao invés de $a \cdot b$, para $a, b \in R$, quando não houver ambiguidade para interpretação. Também iremos nos referir a um anel $(R, +, \cdot)$ simplesmente pela notação de seu conjunto, ou seja, indicaremos o anel simplesmente por R. A identidade aditiva de um anel é denotado por 0 a o inverso aditivo de um elemento a é denotado por $-a$.

Definição 2.2. Seja R um anel.

(1) Dizemos que R é um *anel comutativo* se verificar $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ para quaisquer $a, b, c \in R$

(2) Dizemos que um R é um *anel com identidade* se existe $1_R \in R$ tal que $1_R \cdot a = a \cdot 1_R = a$ para todo $a \in R$

Proposição 2.1. *Seja $(R, +, \cdot)$ um anel. Então:*

(i) $0a = a0 = 0 \quad , \forall a \in R$

(ii) $(-a)b = a(-b) = -(ab) \quad , \forall a, b \in R$

(iii) $(-a)(-b) = ab \quad , \forall a, b \in R$

(iv) Se $(R, +, \cdot)$ tem identidade 1, então ela é única e $-a = (-1)a \quad , \forall a \in R$

Demonstração. (i) Tome $a \in R$ com $a \neq 0$. Vamos mostrar que $0 = 0a$, o caso $0 = a0$ é análogo. Pelo axioma (R3) temos:

$$0a = (0 + 0)a = a0 + 0a$$

Como $(R, +)$ é grupo, pela **Proposição 1.2.** ***(i)*** devemos ter $0 = 0a$. Agora vamos mostrar que $0 = 0 \cdot 0$. De fato, para $a \in R$ não nulo temos que:

$$0 \cdot 0 = 0 \cdot [a + (-a)] = 0a + 0(-a) = 0.$$

(ii) Tome $a, b \in R$. Utilizando (i) e (R3) temos:

$$-ab + ab = 0 = 0b = (-a + a)b = (-a)b + ab \implies -ab = (-a)b \tag{2.1}$$

onde a implicação segue da **Proposição 1.2.** ***(ii)***. Analogamente obtemos:

$$-ab + ab = 0 = a0 = a(-b + b) = a(-b) + ab \implies -ab = a(-b) \tag{2.2}$$

Portanto, de (1.1) e (1.2) temos que $-ab = (-a)b = a(-b)$.

(iii) Sejam $a, b \in R$ quaisquer. Utilizando (i), (ii) e (R3) segue que:

$$0 = (-a)0 = (-a)[b + (-b)] = (-a)b + (-a)(-b) = -ab + (-a)(-b)$$

Portanto, temos que $ab = (-a)(-b)$.

(iv) A demonstração da unicidade é idêntica a da **Proposição 1.2.**. Mostraremos que $-a = (-1)a$ para qualquer $a \in R$. Suponha que $a = 0$, desde que $0 + 0 = 0$, temos que $-0 = 0$. Daí segue de (i) que $-0 = 0 = (-1)0$. Agora suponha que $a \neq 0$, então por (i) e por (R3) assim:

$$0 = 0a = (-1+1)a = (-1)a + a$$

Logo, pela unicidade do elemento oposto devemos ter $-a = (-1)a$. □

Definição 2.3. Seja $(R, +, \cdot)$ um anel.

(1) Um elemento não nulo $a \in R$ é chamado *divisor de zero* se existe $b \in R$ não nulo tal que $ba = 0$ ou $ab = 0$.

(2) Assuma que $(R, +, \cdot)$ possui identidade $1 \neq 0$. Dizemos que $u \in R$ é uma *unidade* se existe $v \in R$ tal que $uv = vu = 1$. O conjunto das unidades de R é denotado por $R^{\times}$.

Comentário 2.1. Um divisor de zero nunca pode ser uma unidade. De fato, seja a um unidade em um anel R com identidade e suponha por absurdo que exista $b \in R$ não nulo tal que $ab = 0$. Então existe $a^{-1} \in R$ tal que $aa^{-1} = a^{-1}a = 1$. Segue que:

$$0 = a^{-1}0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b$$

Um absurdo, pois supomos $b \neq 0$. Analogamente, se $ba = 0$ para algum b não nulo, então a não é unidade.

Definição 2.4. Um anel comutativo R com unidade $1_R \neq 0_R$ é chamado de *domínio de integridade* se não possui divisores de zero.

Proposição 2.2. *Sejam $a, b, c \in R$ com a não divisor de zero e R um anel. Se $ab = ac$, então ou $a = 0$ ou $b = c$.*

Demonstração. Suponha que $ab = ac$ com a não divisor de zero. Então temos que $ab - ac = a(b - c) = 0$, logo devemos ter $a = 0$ ou $b - c = 0$ desde que a não é divisor de zero. Portanto, ou $a = 0$ ou $b = c$. □

Definição 2.5. Seja R um anel. Um subconjunto não vazio $S \subset R$ é chamado de *subanel* de R quando S é fechado sobre as operações de R.

Proposição 2.3. *Seja R um anel e seja $S \subset R$. Então, S é um subanel de R se, e somente se, as seguintes condições são verificadas:*

(i) $0_R \in S$.

(ii) $x, y \in S \implies x - y \in S$.

(iii) $x, y \in S \implies xy \in S$.

Demonstração. ($\Rightarrow$) Se S é um subanel de R os itens são verificados diretamente.
($\Leftarrow$) Suponhamos que $S \subset R$ e que os itens são verificados. Por (i) temos que $S \neq \varnothing$. Tome $x \in S$. Por (i) e (ii) temos que $-x = 0_R - x \in S$. Dado quaisquer $x, y \in S$, temos que $x + y = x - (-y) \in S$, logo S é fechado pela soma. Pelo item (iii) temos que S é fechado pelo produto. Portanto S é um subanel de R. $\square$

Definição 2.6. Um corpo(field) F é um anel comutativo com identidade $1 \neq 0$ para o qual todo elemento não nulo possui inverso multiplicativo, ou seja, $F = F^{\times} - \{0\}$. Em outras palavras, F satisfaz:

(C1) $\forall a \in F - 0, \exists a^{-1} \in F$ tal que $aa^{-1} = a^{-1}a = 1$

Observe que pelo **Comentário 1.10.** um corpo não possui divisores de zero.

Exemplo 2.1. O conjunto dos números reais $\mathbb{R}$ é um corpo, assim como o conjunto dos números racionais $\mathbb{Q}$ e o conjunto dos complexos $\mathbb{C}$.

Exemplo 2.2. Seja p um número primo positivo. Defina o conjunto $\mathbb{Q}\left[\sqrt{p}\right] := \left\{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\right\}$. com a operação de soma e produto dadas por:

$$
\begin{aligned}
(m + n\sqrt{p}) + (a + b\sqrt{p}) &:= (m + a) + (n + b)\sqrt{p} \\
(m + n\sqrt{p})(a + b\sqrt{p}) &:= (ma + nbp) + (mb + na)\sqrt{p}.
\end{aligned}
$$

Vamos verificar que $\mathbb{Q}\left[\sqrt{p}\right]$ é um corpo, para isso precisamos mostrar que $\mathbb{Q}\left[\sqrt{p}\right]$ é um anel comutativo com identidade e que todos seus elementos são unidades. Note que $\mathbb{Q} \subset \mathbb{Q}\left[\sqrt{p}\right]$, de fato, dado qualquer $a \in \mathbb{Q}$, podemos escrever $a = a + 0\sqrt{p} \in \mathbb{Q}\left[\sqrt{p}\right]$. Com isso é fácil ver que 0 é o elemento neutro da soma e 1 o elemento neutro da multiplicação. Agora vamos veirificar que $\mathbb{Q}\sqrt{p}$ é um anel. Tome $m + n\sqrt{p}, a + b\sqrt{p} \in \mathbb{Q}\sqrt{p}$ arbitrários, temos:

$$
\begin{aligned}
(m + n\sqrt{p}) + (a + b\sqrt{p}) &= (m + a) + (n + b)\sqrt{p} \\
&= (a + m) + (b + n)\sqrt{p} \\
&= (a + b\sqrt{p}) + (m + n\sqrt{p})
\end{aligned}
$$

Portanto, satisfaz a comutatividade da soma. Também temos que:

$$
\begin{aligned}
[(m + n\sqrt{p}) + (a + b\sqrt{p})] + (r + s\sqrt{p}) &= [(m + a) + (n + b)\sqrt{p}] + (r + s\sqrt{p}) \\
&= [(m + a) + r] + [(n + b) + s]\sqrt{p} \\
&= [m + (a + r)] + [n + (b + s)]\sqrt{p} \\
&= (m + n\sqrt{p}) + [(a + r) + (b + s)\sqrt{p}] \\
&= (m + n\sqrt{p}) + [(a + b\sqrt{p}) + (r + s\sqrt{p})]
\end{aligned}
$$

Logo, satisfaz a associatividade da soma. Agora tome $a + b\sqrt{p} \in \mathbb{Q}\sqrt{p}$ qualquer, temos que $-a - b\sqrt{p} \in \mathbb{Q}\sqrt{p}$ onde $-a$ e $-b$ são os inversos aditivos de a e b respectivamente, daí segue que:

$$
(a + b\sqrt{p}) + (-a - b\sqrt{p}) = (a - a) + (b - b)\sqrt{p} = 0
$$

Então todo elemento de $\mathbb{Q}\sqrt{p}$ possui inverso aditivo. Agora vamos verificar as propriedades em relação a multiplicação. Temos que:

$$\begin{aligned}(m+n\sqrt{p})(a+b\sqrt{p}) &= (ma+nbp)+(mb+na)\sqrt{p}\\ &= (am+bnp)+(bm+an)\sqrt{p}\\ &= (a+b\sqrt{p})(m+n\sqrt{p})\end{aligned}$$

então vale a comutatividade em relação a multiplicação. Também temos que:

$$\begin{aligned}[(m+n\sqrt{p})(a+b\sqrt{p})](r+s\sqrt{p}) &= [(ma+nbp)+(mb+na)\sqrt{p}](r+s\sqrt{p})\\ &= (ma+nbp)r+(mb+na)sp+[(ma+nbp)s+(mb+na)r]\sqrt{p}\\ &= mar+nbpr+mbsp+nasp+(mas+nbps+mbr+nar)\sqrt{p}\\ &= mar+mbsp+nasp+nbpr+(mas+mbr+nar+nbps)\sqrt{p}\\ &= m(ar+bsp)+n(as+br)p+[m(as+br)+n(ar+bsp)]\sqrt{p}\\ &= (m+n\sqrt{p})[(ar+bsp)+(as+br)\sqrt{p}]\\ &= (m+n\sqrt{p})[(a+b\sqrt{p})(r+s\sqrt{p})]\end{aligned}$$

Assim, vale a associatividade na multiplicação. Por final, sendo $a+b\sqrt{p}\in\mathbb{Q}$ um elemnto qualquer, queremos identificar o elemento x tal que $(a+b\sqrt{p})x=1$, daí:

$$\begin{aligned}(a+b\sqrt{p})x &= 1\\ \implies x &= \frac{1}{a+b\sqrt{p}}\\ &= \left(\frac{1}{a+b\sqrt{p}}\right)\left(\frac{a-b\sqrt{p}}{a-b\sqrt{p}}\right)\\ &= \frac{a-b\sqrt{p}}{a^2-b^2p}\\ &= \frac{a}{a^2-b^2p}-\frac{b}{a^2-b^2p}\sqrt{p}\end{aligned}$$

Como $a,b,p\in\mathbb{Q}$ e $\mathbb{Q}$ é um corpo, então:

$$\frac{a}{a^2-b^2p},\frac{b}{a^2-b^2p}\in\mathbb{Q}\implies\frac{a}{a^2-b^2p}-\frac{b}{a^2-b^2p}\sqrt{p}\in\mathbb{Q}\sqrt{p}$$

Portanto, todo elemento de $\mathbb{Q}\sqrt{p}$ é uma unidade.

2.2 Homomorfismo de anéis, ideais e anel quociente

Definição 2.7. Sejam R e S anéis.

1. Um *homomorfismo de anéis* é uma função $\varphi : R \to S$ que satisfaz:

   i $\varphi(a+b) = \varphi(a) + \varphi(b), \forall a, b \in R.$

   ii $\varphi(ab) = \varphi(a)\varphi(b), \forall a, b \in R$

2. O *kernel* de um homomorfismo de aneis φ é o conjunto de todos elementos $x \in R$ tais que $\varphi(x) = 0$. Denotamos esse conjunto por $\ker \varphi$.

3. Chamamos de *isomorfismo* um homomorfismo de anel $\varphi : R \to S$ que é bijetivo. Denotamos $R \cong S$ quando tal bijeção existir.

Proposição 2.4. *Sejam R e S anéis e $\varphi : R \to S$ um homomorfismo. Então:*

(1) $\varphi(0_R) = 0_S$.

(2) $\varphi(-a) = -\varphi(a), \forall a \in R.$

Demonstração. (i) Temos que $\varphi(O_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$. Desde que $\varphi(0_R) \in S$ e S é um anel, segue que $\varphi(O_R) = \varphi(0_R) + \varphi(0_R)$ implica em $\varphi(0_R) = 0_S$.
(ii) Temos que $\varphi(0_R) = \varphi(a + (-a)) = \varphi(a) + \varphi(-a)$. Pelo item (i) temos que $0_S = \varphi(a) + \varphi(-a)$. Portanto $\varphi(-a) = -\varphi(a)$. □

Proposição 2.5. *Sejam R e S anéis e seja $\varphi : R \to S$ um homomorfismo.*

1. $\mathrm{Im}(\varphi)$ *é um subanel de S.*

2. $\ker \varphi$ *é um subanel de R. Além disso, se $\alpha \in \ker \varphi$, então $r\alpha \in \ker \varphi$ para todo $r \in R$.*

Demonstração. (1) Pela **Proposição 2.4**$(1), 0_S \in \mathrm{Im}(\varphi)$. Tome $x, y \in \mathrm{Im}(\varphi)$. Então existem $r, s \in R$ tais que $\varphi(r) = x$ e $\varphi(s) = y$. Assim, pela **Proposição 2.4** $(2), x - y = \varphi(r) - \varphi(s) = \varphi(r) + \varphi(-s) = \varphi(r + (-s))$. Também temos que $xy = \varphi(r)\varphi(s) = \varphi(rs)$. Daí temos que $x - y, xy \in \mathrm{Im}(\varphi)$. Portanto, pela **Proposição 2.3** $\mathrm{Im}(\varphi)$ é um subanel de S.
(2) Pela **Proposição 2.4**(1) temos que $0_R \in \ker \varphi$. Sejam $x, y \in \ker \varphi$. Então $\varphi(x) = \varphi(y) = 0$. Segue que $\varphi(x - y) = \varphi(x) - \varphi(y) = 0$ e $\varphi(xy) = \varphi(x)\varphi(y) = 0$, logo $x - y \in \ker \varphi$ e $xy \in \ker \varphi$. Portanto, pela **Proposição 2.3** $\ker \varphi$ é um subanel de R. Analogamente, para qualquer $r \in R$ temos $\varphi(rx) = \varphi(r)\varphi(x) = \varphi(r)0 = 0$ e $\varphi(xr) = \varphi(x)\varphi(r) = 0\varphi(r) = 0$. Portanto $rx, xr \in \ker \varphi$. □

Definição 2.8. Seja R um anel, seja $I \subset R$.

1. Dizemos que I é um *ideal a esquerda* de R se $rx \in I$ para todo $r \in R$, ou seja, $R \cdot I \subset I$.

2. Dizemos que I é um *ideal a direita* de R se $xr \in I$ para todo $r \in R$, ou seja, $I \cdot R \subset I$.

3. Se I é um ideal simultaneamente a direita e a esquerda de R, dizemos que I é um *ideal* de R, isto é, $R \cdot I \subset I$ e $I \cdot R \subset I$.

Definição 2.9. Seja R um anel e seja $x \in R$.

1. O ideal $I = xR$ é dito *ideal principal* à esquerda gerado por x.

2. O ideal $I = Rx$ é dito *ideal principal* à direita gerado por x.

Definição 2.10. Seja R um anel e M um ideal de R. Dizemos que M é um *ideal maximal* de R se $M \neq R$ e se os únicos ideiais que contém M são M e R.

Definição 2.11. Um *Domínio Ideal Princial* é um domínio de integridade no qual todo ideal é principal.

Proposição 2.6. *Seja I um ideal do anel com unidade R.*

1. *$I = R$ se, e somente se, $u \in I$ com $u \in R$ uma unidade qualquer.*

2. *Seja R um anel comutativo. Então R é um corpo se, e somente se, seus únicos ideais são $\{0_R\}$ e R.*

Proposição 2.7. *(1)($\Rightarrow$) Suponha $I = R$. Então $1_R \in R = I$.*
($\Leftarrow$) Suponha que $u \in I$ é uma unidade com iverso v e tome $r \in R$. Assim, $r = r(vu) = (rv)u \in I$, logo $R \subset I$. E como $I \subset R$ temos, portanto, que $I = R$.
(2)($\Rightarrow$) Suponha que R é um corpo. Então todo elemento não nulo de R é uma unidade. Então qualquer ideal I de R contém unidades. Assim, por (1) temos que $I = R$.
($\Leftarrow$) Suponha que os únicos ideais de R são $\{0_R\}$ e R. Seja $u \in R$ não nulo e considere Ru o ideal principal gerado por u. Então $u \notin \{0_R\}$. Assim, por hipótese, temos que $Ru = R$. Daí $1_R \in Ru$, logo, existe $v \in R$ tal que $1_R = vu$. Portanto, R é um corpo.

Definição 2.12. Seja R um anel e seja I um ideal de R. Definimos a relação, se $r, s \in R$

$$r \equiv s \mod I \iff r - s \in I.$$

Observação 2.1. A relação $\equiv \mod I$ é de equivalência. De fato, dados quaisquer $r, s, t \in I$, temos

1. $r - r = 0_R \in I \iff r \equiv r \mod I$. A relação é reflexiva.

2. Se $r - s \in I$, então $-(r - s) = s - r \in I$. Logo $r \equiv s \mod I$, implica em $s \equiv s \mod I$. É uma relação simétrica.

3. Se $r \equiv s \mod I$ e $s \equiv t \mod I$, então $r - s, s - t \in I$. Assim, $r - t = (r - s) + (s - t) \in I$, logo $r \equiv r \mod I$. É uma relação transitiva.

Observação 2.2. Sejam R um anel e I um ideal de R. De forma análoga à **Definição 1.11**, o conjunto $\overline{r} := \{x \in R | x \equiv r \mod I\}$ é *classe de equivalência* de $r \in R$. Veja que, $r \equiv s \mod I$ se, e somente se, $r - s \in I$ e, por isso, também denotaremos $\overline{r} = r + I = \{r + s| \in I\}$. Assim como na **Definição 1.13**, $R/I := \{\overline{r} | r \in R\}$ é o *conjunto quociente* de R pelo ideal I.

Proposição 2.8. *Sejam R um anel e I um ideal de R. Se $r \equiv r' \mod I$ e $s \equiv s' \mod I$, então,*

(i) $r + s = r' + s' \mod I$.

(ii) $r \cdot s \equiv r' \cdot s' \mod I$.

Demonstração. Suponha válida a hipótese.
(i) Desde que $r \equiv r' \mod I$ e $s \equiv s' \mod I$, segue que $r - r', s - s' \in I$. Assim, $(r + s) - (r' + s') = (r - r') + (s - s') \in I$. Portanto, $r + s \equiv r' + s' \mod I$.
(ii) Sejam $a, b \in J, r = r' + a$ e $s = s' + b$. Assim,

$$\begin{aligned} rs - r's' &= (r' + a)(s' + b) - r's' \\ &= r's' + r'b + as' + ab - r's' \\ &= r'b + as' + ab. \end{aligned}$$

Portanto, como $a, b \in I$ e I é um ideal, concluimos que $rs - r's' \in I$. □

Corolário 2.8.1. *Sejam R um anel e I um ideal de R. Se $\overline{r} = \overline{r'}$ e $\overline{s} = \overline{s'}$, então,*

(i) $\overline{r + s} = \overline{r' + s'}$.

(ii) $\overline{r \cdot s} = \overline{r' \cdot s'}$.

Demonstração. Segue direto da **Proposição 2.8**. □

Proposição 2.9. *Seja R um anel e I um ideal de R. Se $\overline{r} = r + I$ e $R/I = \{\overline{r} : r \in R\}$, então:*

(1) $\begin{array}{rl} + : R/I \times R/I \to R/I \\ (\overline{r}, \overline{s}) \mapsto \overline{r+s} \end{array}$ *e* $\begin{array}{rl} \cdot : R/I \times R \to R/I \\ (\overline{a}, \overline{b}) \mapsto \overline{a \cdot b} \end{array}$

definem duas operações(soma e produto) em R/I.

(2) $(R/I, +, \cdot)$ *é um anel.*

(3) $\overline{1_R}$ *é a unidade de R/I.*

(4) Se R é comutativo, então R/I também o é.

Demonstração. (1) Pelo **Corolário 2.8.1** as regras $\overline{r} + \overline{s} = \overline{r+s}$ e $\overline{r} \cdot \overline{s} = \overline{r \cdot s}$ definem operações em R/I.
(2) Sejam $r, s, t \in R$. Vamos mostrar que $(R/I, +)$ é um grupo abeliano. Temos,

$$\begin{aligned}(\overline{r} + \overline{s})\overline{t} &= \overline{r+s} + \overline{t} \\ &= \overline{(r+s)+t} \\ &= \overline{r + (s+t)} \\ &= \overline{r} + \overline{s+t} = \overline{r} + (\overline{s} + \overline{t}).\end{aligned}$$

Logo, vale a associatividade. Também,

$$\overline{0_R} + \overline{r} = \overline{0_R + r} = \overline{r} = \overline{r + 0_R} = \overline{r} + \overline{0_R}.$$

Então, existe elemento neutro $\overline{O_R} \in R/I$.. Segue,

$$\overline{r} + \overline{-r} = \overline{r - r} = \overline{0_R} = \overline{-r + r} = \overline{-r} = \overline{r}.$$

Assim, existe elemento neutro para qualquer elemento em R/I. Por final,

$$\overline{r} + \overline{s} = \overline{r+s} = \overline{s+r} = \overline{s} + \overline{r}.$$

Portanto, vale a comutatividade. Agora vamos mostrar que vale as propriedade de anel em relação a multiplicação. Temos que,

$$\begin{aligned}(\overline{r} \cdot \overline{s}) \cdot \overline{t} &= \overline{r \cdot s} \cdot \overline{t} \\ &= \overline{(r \cdot s) \cdot t} \\ &= \overline{r \cdot (s \cdot t)} \\ &= \overline{r} \cdot \overline{s \cdot t} = \overline{r} \cdot (\overline{s} \cdot \overline{t}).\end{aligned}$$

Logo, vale a associtividade. Temos,

$$\begin{aligned}\overline{1_R} \cdot \overline{r} &= \overline{1_R \cdot r} \\ &= \overline{r} \\ &= \overline{r \cdot 1_R} = \overline{r} \cdot \overline{1_R}.\end{aligned}$$

Assim, $\overline{1_R}$ é o elemento neutro da multiplicação. Finalmente,

$$\begin{aligned}\overline{r}(\overline{s} + \overline{t}) &= \overline{r(s+t)} \\ &= \overline{rs + rt} \\ &= \overline{rs} + \overline{rt} = \overline{r} \cdot \overline{s} + \overline{r} \cdot \overline{t}.\end{aligned}$$

A demonstração da distributividade à direita é análoga, assim vale a distributividade em R/I. Portanto, R/I é um anel. (3)Temos que $\overline{1_R} \cdot \overline{r} = \overline{1_R \cdot r} = \overline{r \cdot 1_R \cdot} = \overline{r}$.
(4) Considere R um anel comutativo. Assim $\overline{r} \cdot \overline{s} = \overline{r \cdot s} = \overline{s \cdot r} = \overline{s} \cdot \overline{r}$. O que finaliza a demonstração. □

Teorema 2.1. *Sejam R um anel comutativo com unidade e I um ideal de R. Então I é um ideal maximal de R se, e somente se, R/I é um corpo.*

Demonstração. $(\Rightarrow)$ Suponha que I é um ideal maximal e seja $\overline{0} \neq \overline{r} \in R/I$. Se $J = Ra$ um ideal pricipal gerado por r. Como $a = 1_R \cdot a \in J \subset I + J := \{r+s : r \in I, s \in J\}$, temos que $I+J$ é um ideal tal que $I \subset I+J$ e $I+J \neq I$ e, além disso, $\overline{a} \neq \overline{0}$ se, e somente se, $a \notin I$. Como I é maximal, temos que $R = I + J$ e, assim, $1_R \in I + J$. Logo existem $u \in I$ e $v \in J$ tais que $u + v = 1_R$. Contudo, temos $J = Ra$, assim $v = ra$ para algum $r \in R$. Daí temos $1_R = u+v = u+ra$ e segue que $\overline{1_R} = \overline{u+ra} = \overline{u} + \overline{ra} = \overline{0} + \overline{ra} = \overline{ra}$. Portanto, existe elemento inverso para qualquer $\overline{a} \in R/I$ em relação a multiplicação.
$(Leftarrow)$ Suponha que R/I é um corpo. Desde que $\overline{1_R}, \overline{0_R} \in R/I$, temos $I \neq R$. Se $M \neq I$ é um ideal de R e $I \subset M \subset R$, então existe $m \in M, m \notin I$, isto é, $\overline{m} \neq \overline{0}, \overline{m} \in R/I$. Como R/I é um corpo, então existe $\overline{n} \in R/I$ tal que $\overline{mn} = \overline{1_R}$. Assim segue, $mn \equiv 1 \mod I$ se, e somente se,$ab - 1 \in I$, então existe $i \in I$ tal que $o = mn - 1_R$, logo, $1_R = mn - o$. Desde que $m \in M$ e $o \in I \subset M$ temos $mn, o \in M$. Então $1_R = mn - o \in M$. Portanto, pela **Proposição 2.6**(1), temos que $M = R$. □

Teorema 2.2. *Primeiro teorema de homomorfismo Sejam R e S anéis. Se $\varphi : R \to S$ um homomorfismo de anéis. Então,*

(1) $\mathrm{Im}\varphi$ *é um subanel de S.*

(2) $\ker\varphi$ *é um ideal de* R*.*

(3) φ *é injetiva se, e somente se,* $\ker\varphi = \{0_R\}$*.*

(4) $R/\ker\varphi \cong \text{Im}\varphi$*.*

Demonstração. (1) Desde que φ é um homomorfismo, pela **Proposição 2.4** temos que $\varphi(0_R) = 0_S$. Também, dados quaisquer $\varphi(r), \varphi(s) \in \text{Im}\varphi \subset S$, temos que $\varphi(r) - \varphi(s) = \varphi(r - s) \in \text{Im}\varphi$ e $\varphi(r)\varphi(s) = \varphi(rs) \in \text{Im}\varphi$. Portanto, pela **Proposição 2.3** concluimos que $\text{Im}\varphi$ é um subanel de R.
(2) Temos que $\varphi(0_R) = 0_S$. Dados quaisquer $a, b \in \ker\varphi$, temos $\varphi(a) = \varphi(b) = 0_S$ e segue que $\varphi(a - b) = \varphi(a) - \varphi(b) = 0_S - 0_S = 0_S$, logo $a - b \in \ker\varphi$. Agora tome $r \in R$ e $a \in \ker\varphi$, então $\varphi(ar) = \varphi(a)\varphi(r) = 0_S\varphi(r) = 0_S$. Analogamente temos $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0_S = 0_S$. Ou seja, $ar, ra \in \ker\varphi$. Portanto, $\ker\varphi$ é um ideal de R.
(3) ($\rightarrow$) Suponha que φ é injetiva. Então, desde que $\varphi(0_R) = 0_S$, temos $\text{Im}\varphi = 0_R$. ($\Leftarrow$) Suponha que $\text{Im}\varphi = 0_R$. Se $\varphi(r) = \varphi(s)$ com $r, s \in R$, segue que $\varphi(r) - \varphi(s) = \varphi(r - s) = 0_S$. Logo $r - s = 0_R$ e, então, $r = s$.
(4) Seja $I = \ker\varphi$. Defina uma função $f : R/\ker\varphi \rightarrow \text{Im}\varphi$ dada por $f(\overline{r}) = \varphi(r)$. Vamos mostrar que a função está bem definida:

$$\begin{aligned}
\overline{r} = \overline{s} &\iff r \equiv s \mod \ker\varphi \\
&\iff r - s \in \ker\varphi \\
&\iff \varphi(r - s) = 0_R \\
&\iff \varphi(r) - \varphi(s) = 0_R \\
&\iff \varphi(r) = \varphi(s) \\
&\iff f(\overline{r}) = \varphi(r) = \varphi(s) = f(\overline{s}).
\end{aligned}$$

E também temos:

$$\text{Im}f = \{f(r + I) : r + I \in R/I\} = \{\varphi(r) : r \in R\} = \text{Im}\varphi.$$

Portanto, $R/\ker\varphi \cong \text{Im}f$. $\square$

2.3 Domínios Euclidianos

As definições de 2.11 até 2.16 diz respeito a anéis, isto é, não possuem restrições para domínios euclidianos. Denotaremos o elemento neutro multiplicativo de um anel R por 1 e o elemento neutro aditivo de R por 0. Mas esses símbolos não se referem, necessariamente, aos números $1, 0 \in \mathbb{Z}$.

Definição 2.13. Seja R um anel comutativo e sejam $a, b \in R$ não nulos. Dizemos que a é múltiplo de b e escrevemos $b \mid a$ se existe $x \in R$ que satisfaz $a = bx$. Nesse caso, também dizemos que b *divide* a.

Definição 2.14. Seja R um anel comutativo. Um elemento $p \in R$ não nulo e não unidade é dito primo se $p = ab$ implicar em a ou b serem unidades em R.

Definição 2.15. Seja R um anel comutativo. Se um elemento de R é não nulo, não unidade e não primo, dizemos que esse elemento é um *elemento composto*.

Definição 2.16. Seja R um anel comutativo e sejam $a, b \in R$ não nulos. Dizemos que a e b são associados, e escrevemos $a \sim b$, se existe uma unidade $u \in R$ tal que $a = ub$.

Observação 2.3. A relação $\sim$ definida acima é uma relação de equivalência. De fato, considere $a, b, c, 1 \in R$ não nulos e 1 o elemento neutro multiplicativo de R. Temos que $a = 1a$ e temos que 1 é uma unidade. Então obtemos que $a \sim a$, logo a relação $\sim$ é reflexiva. Agora considere $a \sim b$, então existe uma unidade $u \in R$ tal que $a = ub$, logo $u^{-1}a = b$. Assim, temos que $b \sim a$, logo a relação $\sim$ é simétrica. Por final, considere $a \sim b$ e $b \sim c$, então existem unidades $u, v \in R$ tais que $a = bu$ e $b = cv$. Daí segue $a = bu = (cv)u = c(vu)$, onde vu é uma unidade pois $(vu)(v^{-1}u^{-1}) = (vv^{-1})(uu^{-1}) = 1 \cdot 1 = 1$. Portanto temos $a \sim c$, logo a relação $\sim$ é transitiva. Isso mostra que a relação é de equivalência.

Definição 2.17. Seja R um anel comutativo. Dizemos que R é um anel de fatoração quando todo elemento não nulo e não unidade $a \in R$ pode ser escrito como $a = \prod_{i=1}^{n} p_i$, com $p_i \in R$ primos para todo $i \in \{1, ..., n\}$.

Definição 2.18. Seja R um anel comutativo. Então R é chamado de anel de fatoração única se é um anel de fatoração e a fatoração é única no seguinte sentido: se $a = \prod_{i=1}^{n} p_i = \prod_{i=1}^{m} q_i$ com todos p_i e q_i primos, então $m = n$ e $p_i \sim q_j$ podendo ser $i \neq j$ ou $i = j$.

Agora vamos definir domínio euclidiano e provar algumas propriedades importantes sobre esse tipo de conjunto.

Definição 2.19. Seja E um anel comutativo. Dizemos que E é um *domínio euclidiano* se existe uma função $N : E \to \mathbb{N} \cup \{0\}$ que chamamos de *função norma*, de forma que:

1. Para quaisquer $a, b \in E$ não nulos $N(a) \leq N(ab)$.

2. Para quaisquer $a, b \in E$ não nulos, existem $q, r \in E$ tais que $a = bq+r$ com $N(r) < N(b)$ ou $r = 0$.

Comentário 2.2. Se $0_R \in R$ é o elemento neutro da soma, temos que $N(0_R) = 0$ e essa é a menor norma possível para os elementos de um anel R.

Teorema 2.3. *Seja E um domínio euclidiano.*

1. *E é um domínio de integridade.*

2. *Para todo $a \in E$ não nulo, se $ab = ac$, então $b = c$.*

3. *Para quaisquer elementos $a, b \in R$ não nulos, se $N(a) = N(ab)$, então b é uma unidade.*

Demonstração. 1. Precisamos mostrar que E não possui divisores de zero. Suponha por absurdo o contrário. Então existem $a, b \in E$ não nulos tais que $ab = 0$, então $0 < N(a), 0 < N(b)$ e $N(ab) = 0$. Logo $N(ab) < N(a)$ e $N(ab) < N(b)$, o que é um absurdo pois contradiz a **Definição 2.19**(2).
2. Suponha válidas as hipóteses. Por 1. temos que E é um domínio de integridade e, como $a \neq 0$, pela **Proposição 2.2** devemos ter $b = c$.
3. Suponha que $N(a) = N(ab)$. Pela **Definição 2.19**(3) existem $q, r \in E$ tais que $a = (ab)q + r$ com $N(r) < N(ab)$, daí podemos escrever $r = a - (ab)q = a(1 - bq)$. Por hipótese $a \neq 0$, se tivermos $(1 - bq) \neq 0$, pela **Definição 2.19**(2) obtemos $N(a) \leq N(a(1 - bq)) = N(r)$, o que não pode ocorrer pois $N(r) < N(ab) = N(a)$. Então $1 - bq = 0$, logo $1 = bq$. Portanto, b é uma unidade em E. $\square$

Teorema 2.4. *Seja E um domínio euclidiano, e sejam $a, b \in E$ não nulos e não unidades. Se $a \mid b$ e $b \mid a$, então $a \sim b$.*

Demonstração. Suponha válida a hipótese. Desde que $a \mid b$ e $b \mid a$, existem $x_1, x_2 \in E$ tais que $a = bx_1$ e $b = ax_2$. Assim, temos que $a = a1 = bx_1 = (ax_2)x_1 = a(x_1x_2)$, pelo **Teorema 2.3**$(2)$ obtemos $1 = x_1x_2$. Portanto, x_1 e x_2 são unidades e temos que $a \sim b$. $\square$

Definição 2.20. Sejam E um domínio euclidiano e $a, b \in E$. Dizemos que b é um divisor própio de a quando $a = bc$ com b e c não unidades.

Teorema 2.5. *Sejam E um domínio euclidiano e $a, b \in E$ não nulos. Se b é um divisor próprio de a, então $N(b) < N(a)$.*

Demonstração. Suponha que b é um divisor próprio de a. Então $a = bc$ com b e c não unidades, também, desde que a e b são não nulos e E é um domínio euclidiano, existem $q, r \in E$ tais que $b = aq + r$ com $N(r) < N(a)$ ou $r = 0$. Se $r = 0$, temos que $a \mid b$, logo $a \sim b$, o que contradiz a hipótese. Então devemos ter $r \neq 0$ e $N(r) < N(a)$. Dessa forma, desde que $b = aq+r$, obtemos $r = b - aq = b - (bc)q = b(1 - cq)$, logo $N(a) > N(r) = N(b(1 - cq)) \geq N(b)$. $\square$

Definição 2.21. Sejam E um domínio euclidiano e $a, b \in E$ não nulos. Dizemos que d é um *divisor comum* de a e b quando $d \mid a$ e $d \mid b$.

Definição 2.22. Sejam E um domínio euclidiano e $a, b \in E$ não nulos. Um elemento $d \in E$ é chamado de *maior divisor comum*(m.d.c.) de a e b quando satistaz:

- $d \mid a$ e $d \mid b$
- Se $d' \mid a$ e $d' \mid b$, então $d' \mid d$.

Denotamos $d = \text{mdc}(a, b)$ ou $d = (a, b)$.

Teorema 2.6. *Sejam E um anel euclidiano, $a, b \in E$ não nulos e $d = (a, b)$. Se $k = (a, b)$, então $d \sim k$, e todo elemento associado de d é maior divisor comum de a e b.*

Demonstração. Desde que d e k são m.d.c. de a e b, então, por definição, devemos ter $d \mid k$ e $k \mid d$. Daí, pelo **Teorema 2.4** temos que $d \sim k$. Agora considere $d = (a, b)$, e tome $m \in E$ tal que $d \sim m$. Então existe unidade $u \in E$ tal que $d = mu$. Assim, desde que $d \mid a$ e $d \mid b$, temos que $m \mid a$ e $m \mid b$, logo m é divisor comum de a e b. Tome $n \in E$ tal que $n \mid a$ e $n \mid b$. Então, por definição, temos que $n \mid d$, logo existe $w \in E$ tal que $d = nw$. Segue que $d = mu = nw$, logo $m = (nw)u^{-1} = n(wu^{-1})$, ou seja, $n \mid m$. Portanto, m é m.d.c. de a e b. $\square$

Teorema 2.7. *Sejam E um domínio euclidiano, $a, b \in E$ não nulos e $H := \{ax + by | x, y \in E\}$. Então um elemento $d \neq 0$ de H com menor norma é m.d.c. de a e b.*

Demonstração. Como a e b são não nulos, então H é não vazio e, também, contém um elemento d de menor norma. Além disso, como $a, b \in E$ são não nulos e E é um domínio euclidiano, existem $q, r \in E$ tais que $a = qd+r$

e $N(r) < N(d)$ ou $r = 0$. Desde que $d \in H$, existem $x_1, y_1 \in E$ tais que $d = ax_1 + by_1$, logo $r = a - qd = a - q(ax_1 + by_1) = a(1 - qx_1) + b(qy_1)$, e temos que $r \in H$. Como $d \in H$ é não nulo e é o elemento de menor norma, devemos ter $r = 0$ pois $N(r) < N(d)$, com isso vem que $d \mid a$. De forma análoga, mostra-se que $d \mid b$ e, então, d é divisor comum de a e b. Agora tome $c \in E$ tal que c é divisor comun de a e b. Então existem $k_1, k_2 \in E$ tais que $a = ck_1$ e $b = ck_2$. Logo podemos escrever $d = ax_1 + by_1 = ck_1x_1 + ck_2y_2 = c(k_1x_1 + k_2y_2)$, então $c \mid d$. Portanto, d é m.d.c. de a e b. $\square$

Teorema 2.8. *Seja E um domínio euclidiano. O subconjunto de E dos elementos que possuem a menor norma é o das unidades.*

Demonstração. Tome $u \in E$ uma unidade, tome também $b \in E$ não nulo. Então temos que $b = (bu^{-1})u = b(u^{-1}u)$, e $N(u) \leq N(b)$. Portanto, as unidades possuem a menor norma. Agora tome $b \in E$ não nulo de menor norma. Desde que b e 1 são não nulos e E é um domínio euclidiano, existem $q, r \in E$ tais que $1 = bq + r$ e $N(r) < N(b)$ ou $r = 0$. Desde que b tem menor norma, devemos ter $r = 0$, logo $1 = bq$. Portanto b é uma unidade. $\square$

Teorema 2.9. *Seja E um domínio euclidiano e seja $p \in E$ um elemento não nulo e não unidade de menor norma. Então p é primo.*

Demonstração. Suponha por absurdo que p é um elemento composto. Então existem $a, b \in E$ ambos não unidade tais que $p = ab$ e a e b divisores próprios de p. Pelo **Teorema 2.5** temos que $N(a) < N(p)$ e $N(b) < N(p)$, o que contradiz a hipótese, absurdo. Portanto p é primo. $\square$

Definição 2.23. Seja E um domínio euclidiano e sejam $a, b \in E$ ambos não nulo. Dizemos que a e b são relativamente primos se o m.d.c. de a e b for uma unidade.

Observação 2.4. Note que, se $u \in E$ é uma unidade tal que $u \sim 1$, temos que: se $(a, b) = u$, então $(a, b) = 1$. Ou seja, podemos também dizer que a e b são primos entre si quando $(a, b) = 1$.

Teorema 2.10 (Algoritmo de Euclides)**.** *Seja E um anel euclidiano. Sejam $a, b \in E$ não nulos, e sejam $q, r \in E$ tais que $b = aq + r$ com $N(r) < N(a)$ ou $r = 0$. Então o m.d.c. de a e b é também m.d.c. de a e r e vice-versa.*

Demonstração. Tome $d_1 \in E$ tal que $d_1 = (a, b)$ e tome $d_2 \in E$ tal que $d_2 = (a, r)$. Desde que $b = aq + r$, temos que $r = b - aq$ e como $d_1 = (a, b)$, existem $k_1, k_2 \in E$ tais que $a = d_1k_1$ e $b = d_1k_2$, assim $r = b - aq = d_1k_2 + (d_1k_1)q = d_1(k_2 + k_1q)$. Então temos que $d_1 \mid r$ e segue que d_1 é divisor comum de a e r. Logo, $d_1 \mid d_2$. Por outro lado, como $d_2 \mid r$ e $d_2 \mid a$, existem $m_1, m_2 \in E$ tais que $r = d_2m_1$ e $a = d_2m_2$. Com isso temos que $b = aq + r = (d_2m_2)q + d_2m_1 = d_2(m_2q + m_1)$, ou seja, $d_2 \mid b$ e segue que d_2 é divisor comum de a e b. Logo, $d_2 \mid d_1$. Assim, desde que $d_1 \mid d_2$ e $d_2 \mid d_1$, pelo **Teorema 2.4** temos que $d_1 \sim d_2$. Portanto, pelo **Teorema 2.6**, concluimos que $d_1 = (a, r)$ e $d_2 = (a, b)$. □

Teorema 2.11 (Bézout). *Seja E um anel euclidiano e seja $d = (a, b)$ onde $a, b \in E$. Então existem $x, y \in E$ tais que $d = ax + by$.*

Demonstração. Considere $H = \{ax+by|x, y \in E\}$ e tome $m = ax_1+by_1 \in H$ com menor norma. Então pelo **Teorema 2.7** temos que m é m.d.c. de a e b, e pelo **Teorema 2.6** temos que $d \sim m$. Assim, existe uma unidade $u \in E$ tal que $d = mu$ e segue que $d = um = u(ax_1 + by_1) = a(ux_1) + b(uy_1)$, onde $ux_1, uy_1 \in E$. Portanto, $d \in H$. □

Teorema 2.12. *Sejam E um domínio euclidiano, $a, b \in E$ não nulos e $u \in E$ uma unidade. Então, $(a, b) = u$ se, e somente se, existem $x, y \in E$ tais que $ax + by = u$.*

Demonstração. A ida segue direto do **Teorema 2.11**, vamos mostrar a volta. Seja $u \in E$ uma unidade e suponha que $ax + by = u$. Então $0_E \neq u \in H = \{ax + by; x, y \in E\}$. Assim, pelo **Teorema 2.8**, u possui menor norma, logo, pelo **Teorema 2.7**, u é m.d.c. de a e b. □

Teorema 2.13. *Sejam E um domínio euclidiano e $a, b, c, u \in E$ não nulos e u uma unidade. Se $a \mid bc$ e $(a, b) = u$, então $a \mid c$.*

Demonstração. Considere válida a hipótese. Desde que $(a, b) = u$, pelo **Teorema 2.12** existem $x, y \in E$ tais que $u = ax + by$, logo $1 = u^{-1}(ax + by)$ e segue que $c = cu^{-1}(ax + by) = acu^{-1}x + bcu^{-}1y$. Como $a \mid bc$, existe $k \in E$ tal que $bc = ak$. Segue que $c = acu^{-1}x + bcu^{-}1y = acu^{-1}x + (ak)u^{-}1y = a(cu^{-1}x + ku^{-1}y)$. Portanto, $a \mid c$. □

Teorema 2.14. *Seja E um domínio euclidiano, e sejam $p, b \in E$ ambos não nulos e p primo. Então ou $(b, p) = p$ ou $(b, p) = 1$ com d uma unidade.*

Demonstração. Seja $(b, p) = d$. Então $d \mid p$, logo existe $k \in E$ tal que $p = dk$. Como p é primo, então ou d ou k é unidade. Se d é uma unidade, então temos $d \sim 1$ e vem que $(b, p) = 1$. Caso constrário temos que k é unidade, logo $d \sim p$ e, pelo **Teorema 2.6**, $(b, p) = p$. □

Teorema 2.15. *Sejam E um domínio euclidiano, e $p, u \in E$ com p primo e u unidade. Então $pu \in E$ é um primo.*

Demonstração. Suponha por absurdo que pu não é primo. Então existem $a, b \in E$ ambos não unidades tais que $pu = ab$. Desde que u é unidade, temos que $p = p(uu^{-1}) = (pu)u^{-1} = (ab)u^{-1} = a(bu^{-1})$. Como a não é um unidade, temos que bu^{-1} é uma unidade, logo existe $k \in E$ tal que $k(bu^{-1}) = 1$, daí $b(ku^{-1}) = 1$ e temos que b é uma unidade. Absurdo, pois a e b não são unidades. $\square$

Teorema 2.16. *Seja E um anel euclidiano e sejam $p \in E$ primo e $a_1, ..., a_n \in E$ não nulos. Se $p \mid \prod_{i=1}^{n} a_i$, então $p \mid a_i$ para algum $i \in \{1, ..., n\}$.*

Demonstração. Vamos mostrar por indução em n. Para o caso da base considere $n = 1$, assim $p \mid \prod_{i=1}^{1} a_i = a_1$. Suponha indutivamente que a implicação vale para algum $n \in \mathbb{N}$. Agora suponha que $p \mid \prod_{i=1}^{n+1} a_i = (\prod_{i=1}^{n} a_i)a_{n+1}$. Pelo **Teorema 2.14** temos que $(a_{n+1}, p) = p$ ou $(a_{n+1}, p) = 1$. Se $(a_{n+1}, p) = p$, então $p \mid \prod_{i=1}^{n+1} a_i$. Se $(a_{n+1}, p) = 1$, então pelo **Teorema 2.13** temos que $p \mid \prod_{i=1}^{n} a_i$, logo, pela hipótese indutiva, $p \mid a_i$ para algum $i \in \{1, ..., n\}$, então $p \mid \prod_{i=1}^{n+1} a_i$. Em ambos os casos temos que $p \mid \prod_{i=1}^{n+1} a_i$ e, assim, finalizamos a indução. $\square$

Comentário 2.3. Fatorar um elemento é o mesmo que representá-lo como produto de elementos primos.

Teorema 2.17 (Fatoração única)**.** *Seja E um domínio euclidiano. Todo elemento não nulo e não unidade de E pode ser representado como produto de primos e essa representação é única.*

Demonstração. Vamos usar indução na norma. Para o caso da base tome $a \in E$ não nulo, não unidade e de menor norma. Então pelo **Teorema 2.8** temos que a é um elemento primo, logo sua representação em primos é trivial. Analogamente, se $a = \prod_{i=1}^{n} p_i = \prod_{i=1}^{m} q_i$, temos $n = m = 1$ e $p_1 \sim q_1$, desde que a é primo. Então a fatoração de a é única.

Considere $a \in E$ não nulo e não unidade com $N(a) = k$ para algum $k \in \mathbb{N}$, e suponha indutivamente que todo elemento $x \in E$ não nulo e não unidade com $N(x) < k$ possui fatoração em primos única. Se tivermos a um elemento primo, então voltamos para o caso da base e a possui fatoração única. Se a é não primo, então é composto e existem $b, c \in E$ não nulos e não unidades tais que $a = bc$. Daí temos que b e c são divisores próprios de a, logo, pelo **Teorema 2.5** temos que $N(b) < N(a) = k$ e $N(c) < N(a) = k$. Assim, pela hipótese indutiva, temos que b e c possuem fatoração única em primos, isto é, $b = \prod_{i=1}^{n} p_i'$ e $c = \prod_{i=1}^{m} q_i'$. Com isso temos que $a = (\prod_{i=1}^{n} p_i')(\prod_{i=1}^{m} q_i')$.

Agora vamos mostrar que a fatoração é única. Assuma que $a = \prod_{i=1}^{r} p_i = \prod_{i=1}^{s} q_i$ são duas fatorações em primos. Desde que $p_r \mid \prod_{i=1}^{s} q_i$, pelo **Teorema 2.16** temos que $p_r \mid q_j$ para algum $j \in \{1, ..., s\}$, e como q_j é primo temos que $p_r \sim q_j$. Daí existe uma unidade $u \in E$ tal que $p_r = uq_j$, então temos que:

$$\left(\prod_{i=1}^{r-1} p_i\right) p_r = \left(\prod_{i=1}^{r-1} p_i\right) uq_j = \prod_{i=1}^{s} q_i \implies \prod_{i=1}^{r-1} p_i = \left(\prod_{i=1}^{j-1} q_i\right) \left(\prod_{i=j+1}^{s} q_i\right)$$

Mas temos que $\prod_{i=1}^{r-1} p_i$ é divisor próprio de a, então pelo **Teorema 2.5** vem que $N(\prod_{i=1}^{r-1} p_i) < N(a) = k$ e pela hipótese indutiva temos que essa fatoração é única. Desde que é única temos que $r - 1 = s - 1$, e devemos ter $p_i \sim q_j$ de forma que podemos ter $i = j$ ou $i \neq j$ para os associados. Assim, temos que a fatoração é única e completamos a indução. $\square$

Teorema 2.18. *Todo ideal de um domínio euclidiano é um ideal principal. Mais precisamente, se $0 \neq I$ é um ideal qualquer de um domínio euclidiano E, então I é gerado por $d \in I$ onde d é um elemento de menor norma.*

Demonstração. Suponha que $I \neq 0$ e tome um $d \in I$ não nulo de norma mínima. De fato, d existe pois $\{N(a); a \in I\}$ possue elemento mínimo pela Boa Ordenação de $\mathbb{Z}$. Desde que $d \in I$, temos $dE \subseteq I$. Reciprocamente, tome $a \in I$ arbitrariamente. Pelo algoritmo da divisão existem $q, r \in I$ com $N(r) < N(d)$ tais que $a = dq + r$. Assim podemos escrever $r = a - dq$. Desde que $a, qd \in I$, então $r \in I$. Como d possue menor norma, obtemos $r = 0$. Logo, $a = dq \in dR$ e, então, $I \subseteq dR$. Portanto temos $dR = I$. $\square$

Capítulo 3

Inteiros módulo *n*

O Conjunto dos números inteiros $\mathbb{Z}$ pode ser definido de forma axiomática tendo as propriedades da **Definição 2.1** e da **Definição 2.2** como seus axiomas. Assim, o conjunto $\mathbb{Z}$ é um anel comutativo com unidade. Com isso, todas as proposições para esse tipo de anel são consistentes em $\mathbb{Z}$.

3.1 Conjunto dos Inteiros

Definição 3.1. O conjunto dos números inteiros $\mathbb{Z}$ é um anel comutativos com unidade.

Proposição 3.1 (Pricípio da Boa Ordem)**.** *Todo conjunto não vazio de inteiros não negativos contém um elemento mínimo.*

Proposição 3.2. *Seja* $a \in \mathbb{Z}$ *tal que* $0 \leq a \leq 1$*. Então, ou* $a = 0$ *ou* $a = 1$

Demonstração. Considere $A := \{a \in \mathbb{Z}; 0 < a < 1\}$. Tome $a \in \mathbb{Z}$ com $0 \leq a \leq 1$ e suponha por absurdo que $a \neq 0$ ou $a \neq 1$. Dessa maneira temos que $A \neq \varnothing$, pelo Princípio da Boa Ordem existe $b \in \mathbb{Z}$ tal que $b = \min A$. Desde que $b \in A$, temos $0 < b < 1$, então $0 < b^2 < b < 1$. O que é um absurdo, pois b é o elemento mínimo de A. $\square$

Proposição 3.3. *Todo conjunto não vazio de inteiros limitado inferiormente possui um elemento mínimo.*

Demonstração. Seja $A \neq \varnothing$ um conjunto de inteiros e seja k uma cota inferior de A, ou seja, $k \leq a$ para todo $a \in A$. Defina o conjunto $A_k = \{a - k; a \in A\}$. Como $A \neq \varnothing$, então $A_k \neq \varnothing$. Também, desde que $k \leq a$ para todo $a \in A$, temos que $0 \leq a - k$, isto é, os elementos de A_k

são não negativos. Pelo Princípio de Boa Ordem existe $m = \min A_k$, então podemos escrever $m = a_m - k$ para algum $a_m \in A$.

Vamos mostrar que a_m é elemento mínimo em A. Sabemos que $a_m \in A$. Suponha por absurdo que exista algum $b \in A$ tal que $b < a_m$. Daí segue $b-k < a_m-k = m$ e $b-k \in A_k$, o que é um absurdo desde que $m = \min A_k$. Portanto, $a_m = \min A$. $\square$

Proposição 3.4 (Princípio da Indução Finita 1)**.** *Seja $a \in Z$. Se para cada inteiro $n \geq a$ tivermos uma proposição $P(n)$ de forma que:*

(i) $P(a)$ é verdadeira.

(ii) Se $P(n)$ é verdadeira para cada $n \geq a$, então $P(n+1)$ é verdadeira.

Então $P(n)$ vale para todo $n \in \mathbb{Z}$ tal que $a \leq n$.

Demonstração. Pode ser encontrada em [1, Cap.1, pg.21] $\square$

Proposição 3.5 (Princípio da Indução Finita 2)**.** *Seja $a \in Z$. Se para cada inteiro $n \geq a$ tivermos uma proposição $P(n)$ de forma que:*

(i) $P(a)$ é verdadeira.

(ii) Se $P(n)$ é verdadeira para cada k inteiro tal que $a \leq k \leq n$, então $P(k+1)$ é verdadeira.

Então $P(n)$ vale para todo $n \in \mathbb{Z}$ tal que $a \leq n$.

Demonstração. Pode ser encontrada em [1, Cap.1, pg.26] $\square$

Proposição 3.6. *O conjunto $\mathbb{Z}$ é um domínio de integridade.*

Demonstração. Sejam $a, b \in \mathbb{Z}$ tais que $ab = 0$. Se tivermos $a \neq 0$, então temos que $ab = 0 = ab - (ab) = a(b-b) = a0$, pela propriedade cancelativa vem que $b = 0$. Fazendo o mesmo para b obtemos $a = 0$. Portanto, se $ab = 0$, devemos ter ou $a = 0$ ou $b = 0$. $\square$

Proposição 3.7. *Sejam $a, b, c \in \mathbb{Z}$. A equação $ax+by = c$ adimite solução inteira se, e somente se, $(a, b) \mid c$.*

Demonstração. $(\Rightarrow)$Suponha que a equação possua solução inteira $x_0, y_0 \in \mathbb{Z}$. Seja $(a, b) = d \in \mathbb{Z}$. Temos que $d \mid a$ e $d \mid b$, portanto $d \mid ax_0 + by_0 = c$.
$(\Leftarrow)$ Agora suponha que $(a, b) = d \mid c$. Assim temos que $c = dk$ para algum $k \in \mathbb{Z}$. Pelo **Teorema 2.11**, existem $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = d$. Multiplicando a equação por k, obtemos $a(kx_0) + b(ky_0) = dk = c$. Assim, $kx_0, ky_0 \in \mathbb{Z}$ é solução da equação do enunciado. $\square$

Lema 3.1. *Sejam $a, b \in \mathbb{Z}$ tais que $0 \leq a$ e $0 < b$. Então, existem $q, r \in \mathbb{Z}$ tais que $a = bq + r$ e $0 \leq r < b$.*

Demonstração. Defina $A = \{a - bx \in \mathbb{Z}; x \in \mathbb{Z}, 0 \leq a - bx\}$. Fazenso $x = 0$, temos $a - bx = a \in S$, assim $A \neq \varnothing$. Utilizando o Princípio da Boa Ordem, existe $r = \min A$. Vamos mostrar que $0 \leq r < b$. De fato, desde que $r \in A$, podemos escrever $r = a - bq \geq 0$ para algum $q \in \mathbb{Z}$. Agora, suponha por absurdo que $b \leq r$, então $0 \leq r - b$ e segue que,

$$r > r - b = a - bq - b = a - b(q + 1) \geq 0.$$

Daí $r - b \in A$ e $r - b < \min A = r$, o que é uma contradição. Portanto, devemos ter $r < b$. $\square$

Teorema 3.2. *O conjutno dos inteiros $\mathbb{Z}$ é um domínio euclidiano.*

Demonstração. A função $N : \mathbb{Z} \to \mathbb{N}$ dada por $N(a) = |a| = a$ se $0 \leq a$ e $N(a) = |a| = -a$ se $a < 0$, é a função norma em $\mathbb{Z}$. E pelas propriedades do valor absoluto, temos que $N(ab) = N(a)N(b)$; $N(a) = 0$ se, e somente se, $a = 0$. Também, dados $a, b \in \mathbb{Z}$ não nulos, temos $N(ab) = N(a)N(b) \geq N(a)$.

Vamos mostrar que existem $q, r \in \mathbb{Z}$ satisfazendo as condições do enunciado quando $0 < b$ e $a \in \mathbb{Z}$. Pelo lema anterior, o caso para $0 \leq a$ está provado. Suponha que $a < 0$. Assim, $0 \leq |a|$. Pelo lema anterior, existem $q_1, r_1 \in \mathbb{Z}$ tais que $|a| = bq_1 + r_1$ e $0 \leq r_1 < b$. Se $r_1 = 0$, temos $-|a| = a = b(-q_1 - 1) + 0$, daí basta tomar $q = q_1, r = 0$. Se $0 < r_1$, então,

$$a = -|a| = b(-q_1) - r_1 = b(-q_1) - b + b - r_1 = b(-q_1 - 1) + b - r_1.$$

Como $0 \leq r_1 < b$, temos $0 < b - r_1 < b$, então basta tomar $q = (-q_1 - 1)$ e $r = b - r_1$.

Agora mostraremos que exitem $q, r \in \mathbb{Z}$ para $0 < b$. Tome $a \in \mathbb{Z}$. Pelo o que acabamos de mostrar, existem $q_1, r_1 \in \mathbb{Z}$ tais que $a = |b|q_1 + r_1$ e $0 \leq r_1 < |b|$. Para $0 < b$, temos $a = bq_1 + r_1$ e, para $b < 0$, temos $a = (-b)q_1 + r_1 = b(-q_1) + r_1$. De forma que, fazendo $q = -q_1$ e $r = r_1$, as condições do teorema estão satisfeitas.

Por final, vamos mostrar que $q, r \in \mathbb{Z}$ satisfazendo as condições do enunciado são unicamente determinados. De fato, suponha que

$$a = qb + r = q_1 b + r_1 \tag{3.1}$$

e suponha que $r_1 \leq r$. Assim, $r_1 - r = q_1 b - qb = (q - q_1)b$. Desde que $r_1 - r < |b|$, podemos escrever $(q - q_1)b < |b|$. Pelas propriedades do valor absoluto, vem que $0 \leq |q - q_1||b| < |b|$, logo $0 \leq |q - q_1| < 1$. Como que $|q - q_1| \in \mathbb{Z}$, pela **Proposição 3.2** devemos ter $|q - q_1| = 0$, portanto, $q = q_1$. Com isso, usando a propriedade cancelativa em (3.1), obtemos $r = r_1$. $\square$

Corolário 3.3. *Todo ideal I de $\mathbb{Z}$ é principal.*

Demonstração. Como $\mathbb{Z}$ é um domínio euclidiano, o resultado segue direto do **Teorema 2.18**. $\square$

Teorema 3.4. *Seja $p \in \mathbb{Z}$. Então p é primo se, e somente se, o ideal $p\mathbb{Z}$ é maximal.*

Demonstração. ($\Rightarrow$) Seja $p \in \mathbb{Z}$ um primo e considere $I_p = p\mathbb{Z}$ o ideal gerado por p. Vamos mostrar que I_P satisfaz as condições da **Definição 2.11**. Seja I_n um ideal de $\mathbb{Z}$ tal que $I_p \subset I_n \subset \mathbb{Z}$. Pela proposição acima, I_n é um ideal principal, ou seja, $I_n = n\mathbb{Z}$ para algum $n \in \mathbb{Z}$; também temos que $p \in p\mathbb{Z}$, logo $p \in n\mathbb{Z}$. Dessa forma, existe $m \in n\mathbb{Z}$ tal que $p = nm$. Ou seja, $n \mid p$, então $n = \pm 1$ ou $n = \pm p$. Se tivermos $n = \pm 1$, então $I = \mathbb{Z}$; se tivermos $n = \pm p$, então $I_n = I_p$. Portanto, os únicos ideais que contém I_p é ele mesmo e $\mathbb{Z}$.
($\Leftarrow$) Seja $I_p = p\mathbb{Z}$ um ideal maximal. Suponha que $n \mid p$ com $n \in \mathbb{Z}$, ou seja, existe $k \in \mathbb{Z}$ tal que $p = nk$. Considere o ideial $I_n = n\mathbb{Z}$. Desde que $n \mid p$, temos $p \in I_n$. Daí, como I_p é maximal, devemos ter $I_n = I_p$ ou $I_n = \mathbb{Z}$. Se $I_n = I_p$, então $n = \pm p$ e pela propriedade cancelativa temos que $p = nk = \pm pk$, resultada em $k = \pm 1$; se $I_n = \mathbb{Z}$, então $n = \pm 1$ e vem que $p = nk = \pm k$. Portanto, temos que p é um inteiro primo. $\square$

3.2 Anel dos inteiros módulo *n*

Sendo $\mathbb{Z}$ um domínio euclidiano, todas as proposições, teoremas e definições da **secção 2.3** se aplicam no conjunto dos inteiros. Os elementos irredutíveis em $\mathbb{Z}$ são chamados de números primos e, conforme a **Definição 2.14** os números primos $p \in \mathbb{Z}$ são tais que $p = p \cdot 1 = (-p)(-1)$.

Vamos destacar que pelo **Teorema 2.18**, todo ideal de $\mathbb{Z}$ é principal, assim, os ideais de $\mathbb{Z}$ são da forma $n\mathbb{Z} = \{nd \in \mathbb{Z}; d \in \mathbb{Z}\}$ para um $n \in \mathbb{Z}$ fixo. Ou seja, $n\mathbb{Z}$ é o conjunto dos inteiros múltiplos de n. Dessa forma, seguindo a **Definição 2.12** temos:

$$a \equiv b \mod n\mathbb{Z} \iff a - b \in n\mathbb{Z} \iff a - b = nk, k \in \mathbb{Z} \iff n \mid a - b$$

escreveremos, simplesmente, $a \equiv b \mod n$ ao invés de $a \equiv b \mod n\mathbb{Z}$. A partir da **Proposição 2.9**, o conjunto $\mathbb{Z}/n\mathbb{Z}$ é um anel comutativo com unidade, às vezes denotado simplesmente por $\mathbb{Z}_n$. Por exemplo $\mathbb{Z}/2\mathbb{Z}$ é o anel dos inteiros pares, isto é, dos inteiros múltiplos de 2. Agora note que, se $\overline{a_1} = \overline{a_2}$, temos

$$a_1 \equiv a_2 \mod n \iff n \mid a_1 - a_2.$$

Pela divisão euclidiana, desde que $n > 0$, temos que existem únicos $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ com $0 \leq r_1, r_2 < n$ tais que $a_1 = q_1 n + r_1$ e $a_2 = q_2 n + r_2$, daí,

$$a_1 - a_2 = q_1 n - q_2 n + r_1 - r_2 = n(q_1 - q_2) + (r_1 - r_2).$$

Então, $n \mid a_1 - a_2$ se, e somente se,$r_1 - r_2 = 0$, ou seja, $r_1 = r_2$. Com isso, podemos usar como representante das classes de equivalência os possíveis restos $r \in \mathbb{Z}$ na divísão por n os quais satisfazem $0 \leq r < n$. Dessa forma temos que,

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-2}, \overline{n-1}\}.$$

Vamos ver algumas propriedades sobre o anel $\mathbb{Z}_n$.

Proposição 3.8. *Sejam $a, n \in \mathbb{Z}$ com $0 < n$. Então existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \mod n$ se, e somente se, $(a, n) = 1$.*

Demonstração. Note que $ab \equiv 1 \mod n$ se e somente se $ab - 1 = nk$ para algum $k \in \mathbb{Z}$, que é equivalente a $ab + n(-k) = 1$ de forma que $n, -k \in \mathbb{Z}$ é solução para equação $ax + ny = 1$. O que, pelo **Teorema 2.12**, acontece se, e somente se, $1 = (a, n)$. $\square$

Proposição 3.9. *Seja $n \in \mathbb{Z}$ com $0 < n$. Então $\mathbb{Z}/n\mathbb{Z}$ é um corpo se, e somente se, n é primo.*

Demonstração. Segue direto da **Teorema 3.4** e do **Teorema 2.1**. $\square$

Lema 3.5. *Se $p \in \mathbb{Z}$ é um primo, então as únicas soluções de $x^2 \equiv 1 \mod p$ são ± 1.*

Demonstração. Segue que,

$$\begin{aligned} x^2 \equiv 1 \mod p &\iff p \mid x^2 - 1 = (x+1)(x-1) \\ &\iff p \mid x+1 \text{ ou } p \mid x - 1 \\ &\iff x \equiv 1 \mod p \text{ ou } x \equiv -1 \mod p \end{aligned}$$

$\square$

3.2.1 A função φ de Euler e o Teorema de Euler-Fermat

Definição 3.2. Sejam $a, b \in \mathbb{Z}$. Se $a \equiv b \mod n$, dizemos que b é um *resíduo* de a módulo n.

Definição 3.3. Seja $n \in \mathbb{Z}$ com $0 < n$. Dizemos que um conjunto de n inteiros $a_1, ..., a_n$ forma um *sistema completo de resíduos módulo n* quando

(i) $\mathbb{Z}/n\mathbb{Z} = \{\overline{a_1}, ..., \overline{a_n}\}$ e $\overline{a_i} \neq \overline{a_j}$ para todos $i, j \in \{1, ..., n\}$ com $i \neq j$.

(ii) Para todo $n \in \mathbb{Z}$ existe a_i tal que $\overline{n} = \overline{a_i}$.

Teorema 3.6. *Se m inteiros $r_1, ..., r_k$ formam um sistema completo de resíduos módulo n, então $k = n$.*

Demonstração. Afirmamos que $0, 2, ..., n-1$ é um sistemas completo de resíduos módulo n. De fato, dado $a \in \mathbb{Z}$, pela divisão euclidiana existe únicos $q, r \in \mathbb{Z}$ tais que $a = nq + r$ com $0 \leq r \leq n$. Então $a \equiv r \mod n$ e devemos ter $r \in \{0, ..., n-1\}$. Agora tome $t_i, t_j \in \{1, ..., n-1\}$. Desde que $0 \leq t_i, t_j \leq n-1$, pela propriedade do valor absoluto temos $|t_i - t_j| \leq n-1 < n = |n|$. Daí pela contrapositiva do **Teorema 2.5**, temos que $n \nmid t_i - t_j$ para $i \neq j$, ou seja, $t_i \not\equiv t_j \mod n$ para $i \neq j$. Portanto $\{0, ..., n-1\}$ é um sistema completo de resíduos. Assim cada $r_i \in \{r_1, ..., r_k\}$ é congruente a exatamente um $b \in \{1, ..., n-1\}$, logo $k \leq n$. Como $\{r_1, ..., r_k\}$ é um sistema completo de resíduos por hipótese, cada $b \in \{0, ..., n-1\}$ é congruente a exatamente um $r_i \in \{r_1, ..., r_k\}$, logo $n \leq k$. Portanto $k = n$. □

Teorema 3.7. *Se $\{r_1, ..., r_n\}$ é um sistema completo de resíduos módulo n e $a, b \in \mathbb{Z}$ com $(a, n) = 1$, então $ar_1 + b, ar_2 + b, ..., ar_n + b$ é um sistema completo de resíduos módulo n.*

Demonstração. Considerando o teorema acima, basta mostrar que os $ar_i + b \not\equiv ar_j + b \mod n$ para $i \neq j$. Suponha que $ar_i + b \equiv ar_j + b \mod n$. Disso obtemos $ar_i \equiv ar_j \mod n$. Desde que $(a, n) = 1$, a partir da **Proposição 3.8** obtemos $r_i \equiv r_j \mod n$. Como $\{r_1, ..., r_n\}$ é um sistema completo de resíduos módulo n, devemos ter $i = j$. □

Definição 3.4. A função $\varphi(n) := |\{U(\mathbb{Z}/n\mathbb{Z})\}|$ é chamada de *função phi de Euler*.

Comentário 3.1. A função φ recebe como argumento um inteiro positivo n e retorna a quantidade de unidades no anel $\mathbb{Z}/n\mathbb{Z}$.

Proposição 3.10. *Se $p \in \mathbb{Z}$ é primo, então $\varphi(p^\alpha) = p^\alpha - p^{-\alpha}$.*

Demonstração. Desde que os divisíveis por p que são positivos e menores que p^α formam um conjunto de $p^{\alpha-1}$ elementos e existem p^α inteiros de 1 a p^α, obtemos $p^\alpha - p^{\alpha-1}$ inteiros relativamente primos com p^α, o que por definição é igual a $\varphi(p^\alpha)$. Daí podemos escrever

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p^\alpha}\right)$$

$\square$

Teorema 3.8. *Sejam $m, n \in \mathbb{Z}$ com $0 < m, n$. Se $(m, n) = 1$ então, $\varphi(mn) = \varphi(m)\varphi(n)$.*

Demonstração. Seja $(m, n) = 1$. Queremos encontrar todos os elementos de 1 a mn que são primos com mn, e sabemos que existem $\varphi(mn)$ elementos primos com mn pela definição da função φ. Vamos escrever os números de 1 a mn na forma de uma matriz com m linhas e com a primeira coluna m até a última coluna mn:

$$\begin{array}{ccccccc}
1 & m+1 & 2m+1 & 3m+1 & \cdots & (n-2)m+1 & (n-1)m+1 \\
2 & m+2 & 2m+2 & 3m+2 & \cdots & (n-2)m+2 & (n-1)m+2 \\
3 & m+3 & 2m+3 & 3m+3 & \cdots & (n-2)m+3 & (n-1)m+3 \\
4 & m+4 & 2m+4 & 3m+4 & \cdots & (n-2)m+4 & (n-1)m+4 \\
m-1 & m+(m-1) & 2m+(m-1) & 3m+(m-1) & \cdots & (n-2)m+(m-1) & (n-1)m+(m-1) \\
 & & & & \vdots & & \\
m & 2m & 3m & 4m & \cdots & (n-1)m & nm
\end{array}$$

Considere uma linha qualquer l onde $1 \leq l \leq m$. Se tivermos $(l, m) = d \neq 1$, então $d \mid km + l$ desde que $d \mid l$ e $d \mid m$. Assim, como os termos da linha l são da forma $km+l$ com $0 < k < n$, nenhum deles será primo com mn pois $d \mid mn$ já que $d \mid m$. Então, para encontrar os elementos primos com mn que estão na tabela, precisamos olhar para as linhas l tais que $(l, m) = 1$. Pela função φ de Euler, existem exatamente $\varphi(m)$ linhas l com $(l, m) = 1$.

Depois disso precisamos localizar os elementos dessas $\varphi(m)$ linhas l que são primos com n. Como $(m, l) = (m, n) = 1$, então pelo **Teorema 3.7**, $l, m + l, 2m + l, ..., (n - 1)m + l$ forma um sistema completo de resíduos módulo n. Com isso, em cada linha l temos exatamente $\varphi(n)$ elementos que são primos com n, os quais são também primos com m, o que implica que esses elementos são primos com mn. Dessa maneira temos $\varphi(m)\varphi(n)$ elementos primos com mn. Portanto $\varphi(mn) = \varphi(m)\varphi(n)$. $\square$

Corolário 3.10.1. *Se $n = \prod_{i=1}^{k} p_i$ com cada $p_i \in \mathbb{Z}$ primos distintos para todo $1 \leq i \leq k$, então,*

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Demonstração. Seja $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Pelo teorema e pela proposição acima temos,

$$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{k} p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

$\square$

Teorema 3.9. *Euler-Fermat Sejam $a, n \in \mathbb{Z}$ com $0 < n$ e $(a, n) = 1$. Então*

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Demonstração. Sejam $r_1, ..., r_{\varphi(n)}$ um sistema completo de resíduos módulo n. Desde que $(a, n) = 1$, fazendo $b = 0$, pelo **Teorema 3.7**, temos que $ar_1, ..., ar_{\varphi(n)}$ é um sistema completo de resíduos. Assim, cada ar_i é congruente a exatamente um r_j e disso vem,

$$\prod_{i=1}^{\varphi(n)} (ar_i) \equiv \prod_{i=1}^{\varphi(n)} r_i \mod n \iff a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} r_i \equiv \prod_{i=1}^{\varphi(n)} r_i \mod n. \tag{3.2}$$

Desque $(r_i, n) = 1$ para cada $i \in \{1, ..., \varphi(n)\}$, então $\left(\prod_{i=1}^{\varphi(n)} r_i, n\right) = 1$. Portanto, pela **Proposição 3.8**, segue de (3.2) que $a^{\varphi(n)} \equiv 1 \mod n$. □

Teorema 3.10. *Pequeno Teorema de Fermat Sejam $a, p \in \mathbb{Z}$ com $0 < a$ e p primo. Então $a^p \equiv a \mod p$.*

Demonstração. Considere válida a hipótes. Se $p \mid a$, então o resultado é direto. Suponha que $(a, p) = 1$. Assim pelo teorema acima e pela **Proposição 3.10** temos que $a^{\varphi(p)} = a^{p-1} \equiv 1 \mod p$. Multiplicando por a obtemos $a^p \equiv a \mod p$. □

3.2.2 Equações lineares módulo *n*

Chamamos de *congruência linear* módulo m uma congruência da forma $ax \equiv b \mod m$ a qual pode ou não ter solução.

Proposição 3.11. *A congruência $ax \equiv b \mod m$ possui solução se, e somente se, $(a, m) \mid b$. Nesse caso há (a, m) soluções distintas módulo m.*

Demonstração. $(\Rightarrow)$ Suponha que a congruência possua solução $x_0 \in \mathbb{Z}$ e seja $(a, m) = d$. Se $d = 1$, o resultado segue direto. Suponha $1 < d$. Desde que $ax_0 \equiv b \mod m$, então $ax_0 - b = mk$ para algum $k \in \mathbb{Z}$, logo $ax_0 - mk = b$. Como $d \mid a$ e $d \mid m$, então $d \mid ax_0 - mk = b$.
$(\Leftarrow)$ Agora suponha que $(a, m) = d \mid b$, então $b = dk$ para algum $k \in \mathbb{Z}$ também podemos escrever $a = da_0$ e $m = dm_0$ com $(a_0, m_0) = 1$. Pelo **Teorema 2.12** existem $x, y \in \mathbb{Z}$ tais que $ax + my = b$. Multiplicando por $k \in \mathbb{Z}$, vem que $a(xk)+m(yk) = dk = b$. Disso segue que, $x_0 = xk$ e $y_0 = yk$ são soluções para $ax - my = b$. Por outro lado,

$$\begin{aligned} b = a(xk) - m(yk) &= a(xk) + \frac{am}{d}k - m(yk) - \frac{am}{d}k \\ &= a\left(xk + \frac{m}{d}k\right) - m\left(yk + \frac{a}{d}k\right). \end{aligned}$$

Assim, existem infitas soluções na forma $x' = x_0 - k(m/d)$ com $k \in \mathbb{Z}$.

Agora sejam $x_1, x_2 \in \mathbb{Z}$ duas soluções. Assim podemos escrever $x_1 = x_0 - k_1(m/d)$ e $x_2 = x_0 - k_2(m/d)$. Se tivermos x_1 e x_2 congruentes entre si, então,

$$\begin{aligned} x_0 - k_1\frac{m}{d} \equiv x_0 - k_2\frac{m}{d} \mod m &\implies k_1\frac{m}{d} \equiv k_2\frac{m}{d} \mod m \\ \implies k_1\frac{m}{d} - k_2\frac{m}{d} = \frac{m}{d}(k_1 - k_2) &= mk_m = \frac{m}{d}(dk_m), k_m \in \mathbb{Z} \\ \implies k_1 - k_2 = dk_m &\implies k_1 \equiv k_2 \mod d. \end{aligned}$$

Isso mostra que as soluções incongruentes serão obtidas se tomarmos $x' = x_0 - k_1(m/d)$ com k percorrendo um sistema completo de resíduos módulo d. □

Teorema 3.11. *Teorema Chinês do Resto Se* $(a_i, m_i) = (m_i, m_j) = 1$ *para* $i \neq j$ *e* $c_i \in \mathbb{Z}$ *para cada* $i \in \{1, ..., k\}$*, então:*

$$\begin{aligned} a_1x &\equiv c_1 \mod m_1 \\ a_2x &\equiv c_2 \mod m_2 \\ a_3x &\equiv c_3 \mod m_3 \\ &\vdots \\ a_kx &\equiv c_r \mod m_k \end{aligned}$$

possui única solução $m = \prod_{i=1}^{r} m_i$*.*

Demonstração. Como $(a_i, m_i) = 1$ para todo i, pela proposição acima, temos que $a_ix \equiv c_i \mod m_i$ possui uma única solução b_i módulo m_i. Desde que $(m_i, m_j) = 1$ para $i \neq j$, então sendo $n_i = m/m_i$ temos $(n_i, m_i) = 1$. Daí, mais uma vez pela proposição acima, temos que $n_ix \equiv 1 \mod m_i$ possui única solução d_i. Seja $x_0 = \sum_{i=1}^{k} b_in_id_i$. Se $i \neq j$, então $m_i \mid n_j$, logo $n_jd_j \equiv 0 \mod m_i$. Juntando esse último resultado com o fato de $n_id_i \equiv 1 \mod m_i$ e $a_ib_i \equiv c_i \mod m_i$ obtemos,

$$a_ix_0 = a_i\sum_{i=1}^{k} b_in_id_i \equiv a_ib_in_id_i \equiv a_ib_i \equiv c_i \mod m_i.$$

ou seja, x_0 é solução do sistema. Agora, se x_1 é outra solução, temos que $x_0 \equiv x_1 \mod m_i$ se, e somente se, $m_i \mid x_0 - x_1$ para cada m_i, mas $(m_i, m_j) = 1$ para $i \neq j$, daí o resultado anterior consiste se, e somente se, $m \mid x_0 - x_1$, que é equivalente a $x_0 \equiv x_1 \mod m$. O que mostra que a solução é única módulo m. □

3.2.3 Resíduos Quadráticos e símbolo de Legendre

Seja $p \in \mathbb{Z}$ um primo ímpar e sejam $a, b, c \in \mathbb{Z}$ com $(a, p) = 1$. Desejamos resolver equações do tipo $ax^2 + bx + c \equiv 0 \mod p$. Desde que $(a, p) = (4, p) = 1$, multiplicando a congruência por $4a$ e somando b^2 obtemos:

$$4a^2x^2 + 4abx + 4ac + b^2 \equiv b^2 \mod p \implies (2ax + b)^2 \equiv b^2 - 4ac \mod p.$$

Tomando $x' = (2ax + b)^2$ e $d = b^2 - 4ac$ temos $x^2 \equiv d \mod p$. Se essa equação admite sólução, dizemos que d é um *resíduo quadrático*. Vamos ver alguns resutados envolvendo resíduos quadráticos.

Teorema 3.12. *Seja $p \in \mathbb{Z}$ um primo ímpar e seja $a \in \mathbb{Z}$ com $(a, p) = 1$. Então se a equação $x^2 \equiv a \mod p$ tiver solução, tem duas soluções incongruentes módulo p.*

Demonstração. Seja $x_0 \in \mathbb{Z}$ uma solução da equação. Desde que $(-x_0)^2 = x_0^2$,$-x_0$ também é solução da equação. Note, desde que $x_0^2 \equiv a \mod p$, podemos escrever $x^2 - pk = a$ para algum $k \in \mathbb{Z}$, então devemos ter $p \nmid x_0$ caso contrário ocorreira $p \mid a$, o que não pode acontecer. Agora suponha por absurdo que $x_0 \equiv -x_1 \mod p$. Então $2x_1 \equiv 0 \mod p$, logo $p \mid 2x_0$, o que é um absurdo pois $p \nmid 2$ e $p \nmid x_0$. Portanto $x_0 \not\equiv -x_0 \mod p$.

Agora suponha que $x_1 \in \mathbb{Z}$ é também uma solução da equação. Assim, $x_0^2 \equiv x_1^2 \mod p$ desde que x_0^2 e x_1^2 são congruntes a a módulo p. Daí segue que,

$$\begin{aligned}
&x_0^2 - x_1^2 = (x_0 - x_1)(x_0 + x_1) \equiv 0 \mod p \\
\implies &p \mid (x_0 - x_1)(x_0 + x_1) \\
\implies &p \mid (x_0 - x_1) \text{ ou } p \mid (x_0 + x_1) \\
\implies &x_0 \equiv x_1 \mod p \text{ ou } x_0 \equiv -x_1 \mod p.
\end{aligned}$$

Portanto qualquer outra solução é congruente a x_0 ou a $-x_0$. □

Teorema 3.13. *Seja $p \in Z$ um primo ímpar. Considere o conjunto $P = \{1, ..., p-1\}$. Assim, exatamente $(p-1)/2$ elementos de P são resíduos quadráticos e $(p-1)/2$ não o são.*

Demonstração. Considere os quadrados $1^2, 2^2, ..., (p-1)^2/2$. Afirmamos que esses quadrados são incongruentes módulo p. De fato, sejam $x_1, x_2 \in \mathbb{Z}$ com $1 \leq x_1 \leq (p-1)/2$ e $1 \leq x_2 \leq (p-1)/2$ e suponha que $x_1^2 \equiv x_2^2 \mod p$. Daí vem que $x + y \leq p - 1 < p$, e também obtemos que $(x_1 - x_2)(x_1 + x_2) \equiv 0 \mod p$, logo $p \mid (x_1 - x_2)(x_1 + x_2)$. Assim, desde que $x_1 + x_2 < p$, devemos ter $p \mid (x_1 - x_2)$. Mas como $x_1 < p$ e $x_2 < p$, segue que $x_1 = x_2$. Portanto, os quadrados são incongruentes módulo p. Agora note que, se $a \in \{1, ..., (p-1)/2\}$, temos que

$$p - a \in \left\{\frac{p+1}{2}, \frac{p+2}{2}, ..., p-1\right\}.$$

Dessa forma, desde que $p^2 - 2pa + a^2 = (p-a)^2 \equiv a^2 \mod p$, temos que os resíduos quadráticos denotados por a pertencem ao conjunto $\{1, ..., (p-1)/2\}$. Portanto, há $(p-1)/2$ resíduos quadráticos em P de forma que os outros $(p-1)/2$ elementos desse conjunto não são resíduos quadráticos. $\square$

Definição 3.5. Sejam $p, a \in \mathbb{Z}$ com p primo ímpar e $(a,p) = 1$. Definimos o *Símbolo de Legendre* por,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } a \text{ é um resíduo quadrático módulo } p \\ -1 & \text{se } a \text{ não é um resíduo quadrático módulo } p \end{cases}$$

Lema 3.14. *Seja $p \in \mathbb{Z}$ primo. A equação $x^{(p-1)/2} \equiv 1 \mod p$ possui no máximo $(p-1)/2$ raízes. Sendo essas os números $\{1^2, 2^2, ..., [(p-1)/2]^2\}$*

Demonstração. Como para todo $x \in \{1, ..., (p-1)/2\}$ temos $x < p$, então $(x,p) = 1$. Assim, pelo teorema de Euler-Fermat, vem que $x^{p-1} \equiv 1 \mod p$, logo $(x^2)^{(p-1)/2} \equiv 1 \mod p$. Portanto, os números $\{1^2, 2^2, ..., [(p-1)/2]^2\}$ são raízes da equação. Agora note que podemos escrever a equação na forma $\overline{x}^{(p-1)/2} - \overline{1} = \overline{0}$, onde $\overline{x}^{(p-1)/2} - \overline{1} \in \mathbf{F_p}[x]$. Pela **Proposição 3.9** sabemos que $\mathbf{F_p}$ é um corpo, então, pela **Proposição 4.2**, $\overline{x}^{(p-1)/2} - \overline{1}$ possui no máximo $(p-1)/2$ raízes. $\square$

Teorema 3.15. *Critério de Euler Se $p, a \in \mathbb{Z}$ com p primo ímpar e $(a,p) = 1$, então,*

$$\left(\frac{a}{b}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

Demonstração. Desde que $(a,p) = 1$, pelo teorema de Euler-Fermat temos $a^{p-1} \equiv 1 \mod p$. Assim, obtemos,

$$\begin{aligned} & a^{p-1} \equiv 1 \mod p \\ \Longleftrightarrow\ & a^{p-1} - 1 \equiv 0 \mod p \\ \Longleftrightarrow\ & (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \mod p \\ \Longleftrightarrow\ & a^{\frac{p-1}{2}} \equiv 1 \mod p \ \text{ ou } \ a^{\frac{p-1}{2}} \equiv -1 \mod p \end{aligned}$$

Vamos mostrar que $a^{\frac{p-1}{2}} \equiv 1 \mod p$ se, e só se, a é um resíduo quadrático. Seja a uma solução da equação $x^2 \equiv a \mod p$. Pelo lema acima, a é solução da equação se, e somente se, $a \in \{1^2, 2^2, ..., [(p-1)/2]^2\}$. $\square$

Proposição 3.12. *Sejam $p, a, b \in \mathbb{Z}$ com p primo ímpar e $(a,p) = (b,p) = 1$. Então,*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Demonstração. A partir do Critério de Euler,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{b}\right)\left(\frac{b}{p}\right) \mod p. \tag{3.3}$$

Como o Símbolo de Legendre assume os valores 1 e -1, os quais são incongruentes módulo p, segue de (3.3) que

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

como queríamos. □

Teorema 3.16. *Lei da Reciprocidade Quadrática Sejam $p, q \in \mathbb{Z}$ primos ímpares distintos. Então,*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Demonstração. A demonstração dada por Eisenstein, a qual utiliza argumentos geométricos, pode ser encontrada em [3, Cap. 5, pg. 107]. Uma demonstração baseada nas funções seno e cosseno, a qual em seu argumento utiliza relações entre números complexos como a identidade de Euler, pode ser encontrada em [9, Cap. 2, pg. 95]. □

3.2.4 Ordem e raízes primitivas

Definição 3.6. Chamamos de *ordem de a módulo m* e denotamos por $\text{ord}_m a$ o menor inteiro positivo k para o qual $a^k \equiv 1 \mod m$ com $(a,m) = 1$.

Proposição 3.13. *Temos $a^t \equiv 1 \mod m$ se, e somente se, $\text{ord}_m a \mid t$.*

Demonstração. ($\Rightarrow$) Seja $\text{ord}_m a = k$ e seja $t \in \mathbb{Z}$ tal que $a^t \equiv 1 \mod m$. Pelo algoritmo da divisão, existem únicos $q, r \in \mathbb{Z}$ tais que $t = kq + r$ com $0 \leq r < k$. Daí temos que,

$$a^t = (a^k)^q a^r \equiv 1 \mod m \implies a^r \equiv 1 \mod r$$

mas $0 \leq r < k = \text{ord}_m a$, então devemos ter $r = 0$. Assim, $t = kq$, ou seja $\text{ord}_m a = k \mid t$.
($\Leftarrow$) Agora seja $k = \text{ord}_m a$ e suponha que $k \mid t$. Assim $t = km$ para algum $m \in \mathbb{Z}$. Dessa maneira temos que

$$a^k \equiv 1 \mod m \implies (a^k)^m \equiv 1 \mod m \implies a^t \equiv 1 \mod m.$$

□

Corolário 3.13.1. $\text{ord}_m a \mid \varphi(m)$.

Demonstração. Temos que $(a, m) = 1$ para que $a^{\text{ord}_m a} \equiv 1 \mod m$. Assim, a partir do teorema de Euler-Fermat temos que $a^{\varphi(m)} \equiv 1 \mod m$. Logo, pelo teorema acima, devemos ter $\text{ord}_m a \mid \varphi(m)$. □

Proposição 3.14. *Seja $k = \text{ord}_m a$. Então, $a^t \equiv a^h \mod m$ se, e somente se, $t \equiv h \mod k$.*

Demonstração. ($\Rightarrow$)Suponha que $a^t \equiv a^h \mod m$ e suponha, sem perda de generealidade, que $h \leq t$. Daí temos que $a^h \equiv a^h \equiv a^h a^{t-h} \mod m$. Veja que $(a^h, m) = 1$ desde que $(a, m) = 1$. Assim, cancelando a^h na congruência, obtemos $a^{t-h} \equiv 1 \mod m$. Com isso, a partir do **Proposição 3.13**, temos que $k \mid t - h$, ou seja $t \equiv h \mod m$.
($\Leftarrow$)Suponha que $t \equiv h \mod k$ onde $k = \text{ord}_m a$. Assim podemos escrever $t = h + km$ para algum $m \in \mathbb{Z}$. Note que pelo algoritmo da divisão m é unicamente determinado. Como $k = \text{ord}_m a$, segue que:

$$a^k \equiv 1 \mod m \implies (a^k)^m \equiv 1 \mod m \implies (a^k)^m a^h = a^t \equiv a^h \mod m.$$

□

Corolário 3.14.1. *Seja $k = \text{ord}_m a$. Então $1, a, a^2, ..., a^{k-1}$ são incongruentes módulo m.*

Demonstração. Tome dois elementos em $1, a, a^2, ..., a^{k-1}$, digamos a^t e a^h, e suponha que $a^t \equiv a^h \mod m$. Assim, pela **Proposição 3.14** temos que $t \equiv h \mod k$, ou seja $k \mid t - h$. Mas como $0 \leq t < k$ e $0 \leq h < k$, então $t \equiv h \mod m$ ocorre quando $t = h$. Portanto, os elementos $1, a, a^2, ..., a^{k-1}$ são incongruentes. □

Definição 3.7. Dizemos que a é uma *raiz primitiva módulo m* se $\text{ord}_m a = \varphi(m)$.

Teorema 3.17. *Se a é uma raiz primitiva módulo m, então $a, a^2, a^3, ..., a^{\varphi(m)}$ forma um sistema reduzido de resíduos módulo m.*

Demonstração. Temos que $\text{ord}_m a = \varphi(m)$ desde que a é uma raiz primitiva módulo m. Assim, pelo **Corolário 3.14.1**, $1, a, a^2, ..., a^{\varphi(m)-1}$ são incongruentes entre si. Então, pelo **Teorema**, $\{a, a^2, ..., a^{\varphi(m)}\}$ é um sistema reduzido de rezíduos módulo m. $\square$

Proposição 3.15. *Se a é uma raiz primitiva módulo p, então $a+p$ também é.*

Demonstração. Desde que a é raiz primitiva módulo p temos $(a, p) = 1$, logo $(a+p, p) = 1$. Do teorema de Euler-Fermat, temos $(a+p)^{\varphi(p)} \equiv 1 \mod p$. Vamos mostrar que não há expoente n menor que $\varphi(p)$ com $a^n \equiv 1 \mod p$. Suponha que $(a+p)^n \equiv 1 \mod p$ com $n < \varphi(p)$. Note que $(a+p)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} p^i$, assim $(a+p)^n \equiv a^n \mod p$. Daí vem que $a^n \equiv 1 \mod p$, o que não pode ocorrer, pois a é raiz primitiva módulo p. $\square$

Capítulo 4

Polinômios e Inteiros Algébricos

Neste capítulo vamos mostrar que alguns anéis são bastante úteis para a resolver equações diofantinas. Em particular esses anéis são domínios euclidianos, assim, todos os resultados do capítulo 2.3 são aplicados para esses anéis. Por esse motivo, a estrutura algébrica desses conjuntos são semelhantes a estrutura algébrica do conjunto dos números inteiros.

4.1 Polinômios

Definição 4.1. Seja R um anel comutativo com unidade.

1. Definimos o anel dos polinômios sobre R como o conjuto $R[x]$ dos elementos da forma $p(x) = \sum_{i=0}^{n} a_i x^i$ onde $a_i \in R$ para todo $i \in \{0, ..., n\}$. Dizemos que $p(x)$ é um polinômio sobre R em uma indeterminada x e chamamos cada $a_i \in R$ de coeficientes.

2. Chamamos de *termo líder* de $p(x) = \sum_{i=0}^{n} a_i x^i$ a parcela $a_i x^i$ de maior i com $a_i \neq 0$ $p(x)$. Nesse caso, dizemos que a_i é o *coeficiente líder*.

3. Um polinômio $p(x) = \sum_{i=0}^{n} a_i x^i$ é dito *mônico* quando seu coeficiente líder é igual a 1.

4. Definimos o grau de $p(x) = \sum_{i=0}^{n} a_i x^i$ como sendo i maior i tal que $a_i \neq 0$ e denotamos por $\deg p(x) = i$.

Definição 4.2. Seja R um anel comutativo e sejam $p(x) = \sum_{i=0}^{n} a_i x^i, q(x) = \sum_{i=0}^{m} b_i x^i \in R[x]$.

1. Temos que $p(x) = q(x)$ quando $m = n$ e $a_i = b_i$ para todo $i \in \{1, ..., n\}$.

2. Chamaremos de *polinômio identicamente nulo* o polinômio $p(x) = \sum_{i=0}^{n} a_i x^i$ que possue $a_i = 0$ para todo $i \in \{0, ..., n\}$. Denotaremos simplesmente por $p(x) = 0$.

3. Seja $a \in R$ não nulo. Indicaremos por $p(x) = a$ o polinôimo $p(x) = \sum_{i=0}^{n} a_i x^i$ tal que $a_o x^0 = a_0 = a \in R$ e $a_i = 0$ para todo $i \in \{1, ..., n\}$.

Observação 4.1. A partir da definição acima, é fácil ver que $R \subset R[x]$.

Comentário 4.1. Note que x é chamado de indeterminada e não de variável, pois não abordamos, exatamente, um polinômio como uma função, ou seja, não estamos necessariamente interessados em estudar o comportamento de $p(x)$ para certos valores da indeterminada x. Porém, desejamos evidenciar os valores de x para os quais $p(x) = 0$, o que vem na seguinte definição.

Definição 4.3. Seja R um anel comutativo. Considere $p(x) \in R[x]$. Dizemos que $\alpha \in R$ é raiz do polinômio $p(x)$ quando $p(\alpha) = 0$.

Definição 4.4. Definimos indutivamente a soma e a multiplicação de dois polinômios $p(x), q(x) \in R[x]$ com $\deg p(x) = n$ e $\deg q(x) = m$ por:

$$p(x) + q(x) := \sum_{i=0}^{n+m} (a_i + b_i) x^i$$

E também:

$$p(x)q(x) := \sum_{k}^{n+m} c_k x^k \quad \text{,com } c_k = \sum_{i+j=k}^{n+m} a_i b_j$$

Observação 4.2. Note que $\deg(p(x) + q(x)) \leq \max\{\deg p(x), \deg q(x)\}$. Também, temos que as operações acima fazem de $R[x]$ um anel comutativo.

Proposição 4.1. *Seja R um domínio de integridade. Então,*

1. $\deg(p(x)q(x)) = \deg p(x) + \deg q(x)$.

2. *As unidade de $R[x]$ são as mesma de R.*

3. *$R[x]$ é um domínio de integridade.*

Demonstração. Sejam $p(x), q(x) \in R[x]$ polinômios não identicamente nulos com os monômios líderes $a_n x^n$ e $b_m x^m$, respectivamente. Assim, o monômio líder de $p(x)q(x)$ é $a_n b_m x^{n+m}$ com $a_n b_m \neq 0$. Então $\deg(p(x)q(x)) = n + m$ e $p(x)q(x) \neq 0$. Isso prova (1) e (3). Agora suponha que $p(x)$ é uma unidade de forma que $p(x)q(x) = 1$. Daí, $\deg p(x) + \deg q(x) = \deg(p(x)q(x)) = \deg(1) = 0$. Então $\deg p(x) = \deg q(x) = 0$. Portanto, temos que $p(x) \in R$. Isso prova (2). □

Teorema 4.1 (Algoritmo da divisão)**.** *Seja K um corpo. Se $a(x), b(x) \in K[x]$ com $b(x) \neq 0$, então existem $q(x), r(x) \in K[x]$, unicamente determinados, tais que*

$$a(x) = q(x)b(x) + r(x) \quad \textit{com} \quad \deg r(x) < \deg b(x)$$

Demonstração. Sejam $\deg a(x) = n$ e $\deg b(x) = m$. Usaremos indução em n para mostrar a existência de $q(x), r(x)$. Se tivermos $n < m$, basta fazer $q(x) = 0$ e $a(x) = r(x)$. Assim, suponha que $m \leq n$. Para o caso da base considere $n = 0$, então $m = 0$ e $a(x) = a$ e $b(x) = b$ para algum $a, b \in K$. Daí fazemos $q(x) = a/b$ e $r(x) = 0$. Suponha indutivamente que para todo $p(x) \in R[x]$ com $\deg p(x) \leq n \in N$ existem $q(x), r(x) \in K[x]$ satisfazendo o teorema. Seja $a(x) = a_n x^n + a_1(x)$ e $b(x) = b_m x^m + b_1(x)$ com $a_n \neq 0, b_m \neq 0$ e $\deg a_1(x) < n, \deg b_1(x) < m$. Assim, temos que $a(x) - \frac{a_n}{b_m} x^{n-m} b(x) = a_1(x) - \frac{a_n}{b_m} x^{n-m} b_1(x)$ possui grau menor que n. Então, pela hipótese indutiva, existem $q_1(x)$ e $r(x)$ tais que,

$$a(x) - \frac{a_n}{b_m} b(x) = q_1(x)b(x) + r(x) \quad \text{com} \quad \deg r(x) < \deg b(x).$$

Assim, segue que,

$$a(x) = \left(\frac{a_n}{b_m} x^{n-m} + q_1(x) \right) b(x) + r(x).$$

Agora basta tomar $q(x) = \left(\frac{a_n}{b_m} x^{n-m} + q_1(x) \right)$ e concluimos que $a(x) = q(x)b(x) + r(x)$, como queríamos.
Agora vamos provar que $q(x)$ e $r(x)$ são unicamente determinados. Suponha por absurdo que,

$$a(x) = q(x)b(x) + r(x) = q_1(x)b(x) + r_1(x)$$

com $q(x) \neq q_1(x)$ e $\deg r(x), \deg r_1(x) < \deg g(x)$. Então, $r_1(x) - r(x) = (q(x) - q_1(x))b(x) \neq 0$ é múltiplo de $g(x)$ com grau menor do que $g(x)$, o que é um absurdo. □

Corolário 4.2. *Seja K um corpo e sejam $p(x) \in K[x], \alpha \in K$. Então, $x-\alpha \mid p(x)$ se, e somente se, $p(\alpha) = 0$.*

Demonstração. Se $p(x)$ é identicamente nulo, o resultado é direto. Seja $p(x) \neq 0$.
($\Rightarrow$) Suponha que $x-\alpha \mid p(x)$. Assim, existe $g(x)$ tal que $p(x) = (x-\alpha)g(x)$. Então, $p(\alpha) = (\alpha - \alpha)g(\alpha) = 0g(\alpha) = 0$.
($\Leftarrow$) Suponha que $p(\alpha) = 0$. Pelo **Teorema 4.1**, existem $q(x), r(x) \in K[x]$ tais que $p(x) = q(x)(x - \alpha) + r(x)$ com $\deg r(x) < \deg(x - \alpha) = 1$. Assim, $\deg r(x) = 0$ e temos que $r(x) = r \in K$. Daí $p(x) = q(x)(x - \alpha) + r$, implica,

$$p(\alpha) = q(\alpha)(\alpha - \alpha) + r = q(\alpha)0 + r = r \implies 0 = r.$$

Com isso vem que $p(x) = q(x)(x - \alpha) + r = q(x)(x - \alpha)$. Portanto, $x - \alpha \mid p(x)$. $\square$

Teorema 4.3. *Seja K um corpo. Então $R[x]$ é um domínio euclideano sob a norma $N(p(x)) = \deg p(x), p(x) \neq 0$.*

Demonstração. Precisamos mostrar que $K[x]$ satisfaz as condições (1) e (2) da **Proposição 2.19**. De fato, dados $p(x), q(x) \in K[x]$ não nulos, pela **Definição 4.1** e pela **Proposição 4.1**, temos que $\deg(p(x)q(x)) = \deg p(x) + \deg q(x) > \deg p(x)$. O que prova (1). E a parte (2) segue direto do **Teorema 4.1**. $\square$

Comentário 4.2. Desde que $K[x]$, para K um corpo, forma um domínio euclidiano, todos os teoremas e definições para domínios euclidianos são aplicáveis em $K[x]$. Inclusive, a definição de divisor, a existência de m.d.c. e a existência de elementos irredutíveis em $K[x]$ os quais chamamos de polinômios irredutíveis, também a fatoração única ocorre em $K[x]$.

Definição 4.5. Seja K um corpo. Um polinômio $p(x)$ em $K[x]$ é dito irredutível se $p(x)$ não é produto de polinômios em $K[x]$ de graus estritamente menores que $\deg p(x)$.

Teorema 4.4. *Fatoração única Seja K um corpo. Todo polinômio não nulo em $K[x]$ pode ser fatorado de modo único como produto de polinômios irredutíveis em $K[x]$ a menos da ordem dos fatores.*

Demonstração. Segue direto do **Teorema 4.3** e do **Teorema 2.17**. $\square$

Proposição 4.2. *Seja K um corpo. Um polinômio $p(x) \in K[x]$ não nulo de grau n possui no máximo n raízes em K.*

Demonstração. Vamos provar por indução em $\deg p(x) = n$. Para o caso da base considere $n = 0$ e $n = 1$, e o resultado é direto. Suponha indutivamente que $p(x)$ com $\deg p(x) = n$ possui nomáximo n raízes para algum $n \in N$. Se $p(x)$ tivesse $n+1$ raízes distintas $\alpha_1, ..., \alpha_n$, então $p(x) = (x - \alpha_{n+1})g(x)$ pelo corolário anterior, onde $\deg g(x) = n - 1$ desde que $\deg p(x) = n$ e $\deg(x - \alpha_{n+1}) = 1$. Com isso, para $i \neq n+1$ segue,

$$p(\alpha_i) = (\alpha_i - \alpha_{n+1})g(\alpha_i) = 0 \implies g(\alpha_i) = 0$$

pois $\alpha_i - \alpha_{n+1} \neq 0$. Então $g(x)$ teria n raízes distintas $\alpha_1, ..., \alpha_n$. Absurdo, pois contradiz a hipótese indutiva desde que $\deg g(x) = n - 1$. $\square$

Definição 4.6. Um polinômio não nulo $f(x) \in \mathbb{Z}[x]$ é dito primitivo se o m.d.c. de seus coeficientes é igual a 1.

Teorema 4.5. *Critério de Eisenstein Seja* $p(x) = \sum_{i=0}^{n} a_i \in \mathbb{Z}[x]$ *um polinômio primitivo não constante. Se existir um primo* $p \in \mathbb{Z}$ *tal que* $p \nmid a_n$ *e* $p \mid a_i$ *para todo* $0 \leq i < n$*, então* $p(x)$ *é irredutível em* $\mathbb{Z}[x]$.

Demonstração. Suponha por absurdo que $p(x) = \sum_{i=0}^{n} a_i \in \mathbb{Z}[x]$ é irredutível. Assim, existem $m(x), n(x) \in \mathbb{Z}[x]$ tais que $p(x) = m(x)n(x)$ com $0 < \deg m(x), \deg n(x) < n$. Fazendo $\overline{p(x)} = \overline{m(x)n(x)} \in \mathbb{Z}/p\mathbb{Z}$, isto é, reduzindo os coeficientes módulo p. Como, por hipótese, $p \mid a_i$ para todo $0 \leq i < n$, temos $\overline{p(x)} = \overline{a_n}x^n$ e, assim, pelo **Teorema 4.5** temos $m(x) = \bar{b}x^i$ e $n(x) = \bar{c}x^j$ com $0 < i, j < n, i + j = n$ e $\bar{b}\bar{c} = \overline{a_n}$. O que implica que que os coeficientes de x^0 em $m(x)$ e $n(x)$ são múltiplos de p. Como $p(x) = m(x)n(x)$, obtemos que a_0 é múltiplo de p^2, o que é um absurdo. $\square$

Proposição 4.3. *O produto de dois polinômios primitivos é um polinômio primitivo.*

Demonstração. Sejam $g(x)$ e $h(x)$ dois polinômios primitivos. Seja p um primo e suponha por absurdo que p divida todos coeficientes de $g(x)h(x) = \sum_{i=0}^{n} a_i$. Dessa forma temos que temos que $a_i \equiv 0 \mod p$ para todo $i = \{1, ..., n\}$. Portanto, em $\mathbb{Z}/p\mathbb{Z}[x]$, temos que $\overline{g(x)h(x)} = \overline{g(x)}\overline{h(x)} = \overline{0}$, onde a a barra denota o polinômio obtido reduzindo seus coeficientes a módulo p. Desde que $g(x)$ e $h(x)$ são primitivos, temos que p não divide todos os coeficientes $g(x)$ e $h(x)$. Então $\overline{g(x)} \neq \overline{0}$ e $\overline{p(x)} \neq \overline{0}$. Absurdo, pois $\mathbb{Z}/p\mathbb{Z}[x]$ é um domínio de integridade pelo **Teorema** e **Proposição 4.1**. $\square$

Teorema 4.6. *Lema de Gauss Seja* $p(x) \in \mathbb{Z}[x]/Z$ *um polinômio primitivo. Então* $p(x)$ *é irredutível em* $\mathbb{Q}[x]$ *se, e somente se,* $p(x)$ *é irredutível em* $\mathbb{Z}[x]$.

Demonstração. ($\Rightarrow$) Basta observar que qualquer $p(x) \in \mathbb{Q}[x]$ pode ser escrito como $mp(x) \in Z$ onde m =m.m.c. dos denominadores dos coeficientes de $p(x)$.
($\Leftarrow$) Suponha por absurdo que $p(x)$ seja irredutível em $\mathbb{Z}[x]$ onde $p(x) = q(x)r(x)$ com $q(x), r(x) \in \mathbb{Q}[x]/\mathbb{Q}$. Podemos multiplicar última igualdade por algum $k \in \mathbb{Z}^+$ de forma que,

$$kp(x) = nq_0(x)r_0(x)$$

onde $n \in Z^+$ e $q_0(x), r_0(x) \in \mathbb{Z}[x]$ são primitivos. Pela proposição anterior temos que $q_0(x)r_0(x)$ é primitivo e, por hipótese, $p(x)$ é primitivo. Assim, k é o m.d.c. dos coeficientes de $kp(x)$ e n é o m.d.c. dos coeficientes de $nq_0(x)r_0(x)$. Então temos que $k = n$ e, assim, $p(x) = q_0(x)r_0(x)$ é irredutível em $\mathbb{Z}[x]$, o que é um absurdo. $\square$

Definição 4.7. Seja L/K uma extensão de corpos.

1. Um elemento $\alpha \in L$ é chamdo de *algébrico* sobre K se existe um polinômio $p(x) \in K[x]$ tal que $p(\alpha) = 0$. Um número $\alpha \in \mathbb{Q}$ é algébrico se ele é algébrico sobre $\mathbb{Q}$.

2. Se $\alpha \in L$ é algébrico, então um polinômio mônico $p(x) \in K[x]$ de grau mínimo tal que $p(\alpha) = 0$ é chamado de *polinômio minimal* de α sobre K.

Teorema 4.7. *Seja L/K uma extensão de corpos e $\alpha \in L$ algébrico sobre K com polinômio minimal $p(x) \in K[x]$. Então se $g(x) \in K[x]$,*

$$g(\alpha) = 0 \iff p(x) \mid g(x).$$

Isso mostra que α possui um único polinômio minimal.

Demonstração. ($\Leftarrow$) Se $p(x) \mid g(x)$, então podemos escrever $g(x) = p(x)q(x)$ para algum $q(x) \in K[x]$. Como α é raiz de $p(x)$, segue que $g(\alpha) = p(\alpha)q(\alpha) = 0$.
($\Rightarrow$) Suponha que $g(\alpha) = 0$. Pelo algoritmo da divisão existem únicos $q(x), r(x) \in K[x]$ tais que $g(x) = p(x)q(x) + r(x)$ com $0 \leq \deg r(x) < \deg p(x)$. Daí, desde que $g(\alpha) = p(\alpha) = 0$, segue que,

$$g(\alpha) = p(\alpha)q(\alpha) + r(\alpha) \implies r(\alpha) = 0.$$

Como $p(x)$ é polinômio minimal de α, então $r(x)$ é o polinômio nulo. Assim, $g(x) = p(x)q(x)$, ou seja, $p(x) \mid g(x)$.

Agora suponha que houvesse $p_1(x), p_2(x) \in K[x]$ ambos polinômios minimais de α. A partir do que provamos acima, vem que $p_1(x) \mid p_2(x)$ e $p_2(x) \mid p_1(x)$. Porém, ambos são mônicos, com isso devemos ter $p_1(x) = p_2(x)$. $\square$

Definição 4.8. Sejam L/K uma extensão de corpos e $\alpha \in L$ algébrico sobre K com polinômio minimal $p(x) \in K[x]$. As raízes de $p(x)$ em L são chamadas de conjugados de α.

Corolário 4.8. *Sejam L/K uma extensão de corpos, $\alpha \in L$ algébrico sobre é K e α_i os conjugados de α. Se $g(x) \in K[x]$ é tal que $g(\alpha) = 0$, então $g(\alpha_i) = 0$ para todo i*

Demonstração. O resultado segue direto do teorema acima. □

Definição 4.9. Seja R um anel comutativo. O anel de polinômios em n variáveis denotado por $R[x_1, ..., x_n] = R[x - 1, ..., x_{n-1}][x_n]$ é o conjunto dos polinômios com n variáveis $p(x_1, ..., x_n)$ com coeficientes em R.

Comentário 4.3. Essa definição nos diz que podemos considerar um polinômio $p(x_1, ..., x_n) \in R[x_1, ..., x_n]$ como um polinômio em uma variável cujo os coeficientes são polinômios em $n - 1$ variáveis. Temos assim que um polinômio $p \in \mathbb{R}[x_1, ..., x_n]$ é uma soma finita de monômios da forma $ax_1^{e_1} \cdots x_n^{e_n}$, onde $e_i \in \mathbb{Z}^+$ é chamado de grau de x_i. E temos que o grau do monômio é $e = \sum_{i=1}^{n} e_i$.

Definição 4.10. Seja R um anel comutativo com unidade. O grau de um polinômio não nulo $p(x_1, ..., x_n) \in R[x_1, ..., x_n]$ é o grau do monômio de maior grau.

Definição 4.11. Seja R um anel comutativo com unidade. Dizemos que um polinômio $p(x_1, ..., x_n) \in R[x_1, ..., x_n]$ é *homogêneo* quando todos monômios possuem o mesmo grau.

Definição 4.12. Um polinômio $p(x_1, ..., x_n)$ é dito *polinômio simétrico* se é invariante por qualquer permutação das variáveis $x_1, ..., x_n$.

Definição 4.13. Chamamos de *polinômios simétricos elementares* os polinômios p_i da forma:

$$\begin{aligned}
p_1(x_1, ..., x_n) &= x_1 + x_2 + ... + x_n \\
p_2(x_1, ..., x_n) &= x_1x_2 + x_1x_3 + ... + x_1x_n + x_2x_3 + ... + x_2x_n + ... + x_{n-1}x_n \\
p_3(x_1, ..., x_n) &= x_1x_2x_3 + ... + x_{n-2}x_{n-1}x_n \\
&\vdots \\
p_n(x_1, ..., x_n) &= x_1 \cdots x_n
\end{aligned}$$

Teorema 4.9. *Todo polinômio simétrico $p(x_1, ..., x_n)$ pode ser escrito como uma combinação de polinômios simétricos elementares.*

Demonstração. Uma demonstração para esse teorema pode ser encontrada em [9, Cap. 6; pg. 268]. □

Definição 4.14. Dizemos que $\alpha \in \mathbb{C}$ é algébrico quando para algum $p(x) \in \mathbb{Z}[x]$ tivermos $p(\alpha) = 0$.

4.2 Inteiros de Gauss

Definição 4.15. Os inteiros de de Gauss é o conjunto:

$$\mathbb{Z}[i] := \{m + ni \in \mathbb{C} | m, n \in \mathbb{Z} \text{ e } i^2 = -1\},$$

que é um subanel de $\mathbb{C}$.

Definição 4.16. A norma de um elemento C é uma função $N : \mathbb{C} \to \mathbb{N} \cup \{0\}$ dada por $z = a + bi \mapsto N(z) = |z|^2 = |z||\overline{z}| = a^2 + b^2 \geq 0$.

Observação 4.3. Desde que $|x||y| = |xy|$, temos que a função N é multiplicativa, ou seja $N(x)N(y) = N(xy)$.

Comentário 4.4. Para a próxima demonstração, usaremos o fato de que dado qualquer racional p/q, o inteiro mais próximo de p/q é n tal que $|n - p/q| \leq 1/2$. E temos que n é unicamente determinado.

Teorema 4.10. *Os inteiros de Gauss $\mathbb{Z}[i]$ é um domínio euclidiano.*

Demonstração. Temos $\mathbb{Z}[i] \subset \mathbb{C}$. Então a função norma $N : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$ está bem definida. Dados $\alpha = a_1 + a_2 i, \beta = b_1 + b_2 i \in \mathbb{Z}[i]$ não nulos, temos $0 < N(\alpha), N(\beta)$ $N(\alpha\beta) = N(\alpha)N(\beta) \geq N(\alpha)$.
Agora tome $\alpha, \beta \in \mathbb{Z}[i]$ com $\beta \neq 0$. Assim podemos escrever $\alpha/\beta = x + yi$ com $x, y \in \mathbb{Q}$. Sejam, m e n os inteiros mais próximos de x e y, respectivamente, ou seja, $|x - m| \leq 1/2$ e $|y - n| \leq 1/2$. Agora considere $\gamma = m + ni$ e $\lambda = \alpha - \beta\gamma$. Então temos que $\gamma, \lambda \in \mathbb{Z}[i]$ e $\alpha = \gamma\beta + \lambda$. E segue que,

$$\begin{aligned}
|\frac{\alpha}{\beta} - \gamma|^2 &= |x + yi - (m + ni)| \\
&= |(x - m) + (y - n)i|^2 \\
&= (x - m)^2 + (y - n)^2 \leq \frac{1}{4} + \frac{1}{4} < 1
\end{aligned}$$

$$\begin{aligned}
\implies \left|\frac{\alpha}{\beta} - \gamma\right|^2 |\beta|^2 < 1|\beta|^2 \\
\implies |\alpha - \gamma\beta|^2 < |\beta|^2 \\
\implies N(\lambda) < N(\beta).
\end{aligned}$$

Portanto, a **Definição 2.19** é satisfeita. □

Comentário 4.5. O teorema acima nos permite utilizar todas as definições e propriedades para domínios euclidianos. Assim, existem elementos irredutíveis em $\mathbb{Z}[i]$ e, também, m.d.c. entre dois elementos. Também, todo elemento em $\mathbb{Z}[i]$ pode ser fatorado de maneira única a menos de uma unidade e da ordem.

Proposição 4.4. *As unidades em $\mathbb{Z}[i]$ são ± 1 e $\pm i$.*

Demonstração. Vamos verificar que ± 1 e $\pm i$ são unidades em $\mathbb{Z}[i]$. O caso para ± 1 é direto. Para $\pm i$ basta ver que $i \cot(-i) = -i^2 = -(-1) = 1$. Agora vamos mostrar que não existe nenhum unidade além dessas. Seja $u = m + ni \in Z[i]$ um unidade, de forma que $uv = 1$. Assim, temos que $N(uv) = N(u)N(v) = 1$. Desde que $0 < N(u), N(v) \in \mathbb{Z}$, devemos ter $N(u) = N(v) = 1$, então $N(u) = m^2 + n^2 = 1$. Como $m, n \in \mathbb{Z}$, devemos ter $(m^2, n^2) = (1, 0)$ ou $(m^2, n^2) = (0, 1)$. Portanto $u \in \{\pm 1, \pm i\}$. $\square$

Observação 4.4. Pelo **Teorema 2.8** temos que $N(\pm 1) = N(\pm i) = 1$.

Proposição 4.5. *Se $\pi \in \mathbb{Z}[i]$ é tal que $N(\pi)$ é um inteiro primo, então π é irredutível.*

Demonstração. Suponha que a hipótese é satisfeita. Se tivermos $\pi = \alpha\beta$, então $N(\pi) = N(\alpha\beta) = N(\alpha)N(\beta)$. Desde que $N(\pi)$ é um inteiro primo, por definição vem que ou $N(\alpha) = 1$ ou $N(\beta) = 1$. Então ou α é unidade ou β o é. Portanto, temos que π é um irredutível. $\square$

Proposição 4.6. *Se $p \in \mathbb{Z}$ é um primo tal que $p \equiv 3 \mod 4$, então p é irredutível em $Z[i]$.*

Demonstração. Seja $p \equiv 3 \mod 4$ e suponha que $p = \alpha\beta \in \mathbb{Z}[i]$ tal que α, β não são unidades. Então $N(\alpha\beta) = N(\alpha)N(\beta) = N(\beta) = p^2$ e $1 \neq N(\alpha), N(\beta)$. Assim, devemos ter $N(\alpha) = N(\beta) = p$. Seja $\alpha = m + ni$, segue que $N(\alpha) = m^2 + n^2 = p$. Daí vem $m^2 + n^2 \equiv 3 \mod 4$, o que contradiz o **Teorema**. $\square$

Teorema 4.11. *Seja $p \in \mathbb{Z}$ um primo tal que $p \equiv 1 \mod 4$. Então $p = (m + ni)(m - ni) = m^2 + n^2$ com $m, n \in \mathbb{Z}$.*

Demonstração. Seja $p \in \mathbb{Z}$ satisfazendo a hipótese. Assim, pelo **Teorema** temos que $x^2 \equiv -1 \mod p$ possui solução. Seja p é irredutível em $\mathbb{Z}[i]$. Então $p \mid x^2 + 1 = (x + i)(x - i)$ o que implica em $p \mid x + i$ ou $p \mid x - i$. O que não pode ocorrer, porque $p(a + bi) = pa + pbi$ com $a, b \in \mathbb{Z}$. Logo, p é redutível.
Dessa maneira, existem $\alpha, \beta \in \mathbb{Z}[i]$ não unidades tais que $p = \alpha\beta$. Então $N(p) = N(\alpha)N(\beta)$, logo $p^2 = n(\alpha)N(\beta)$, então $N(\alpha) = N(\beta) = p$. Sendo $\alpha = m + ni \in \mathbb{Z}[i]$, segue que $p = m^2 + n^2 = (m + ni)(m - ni)$. $\square$

Definição 4.17. Defina $\xi(\mu) := |\{\alpha \in \mathbb{Z}[i]/(\mu) | \alpha \text{ é unidade}\}|$. Ou seja, $\xi(\mu)$ é quantidade de unidades em $\mathbb{Z}[i]/\mu\mathbb{Z}[i]$.

Proposição 4.7. *Sejam $\alpha, \gamma \in \mathbb{Z}[i], n > 0$. Então, existe $\beta \in \mathbb{Z}[i]$ com $\alpha\beta \equiv 1 \mod \gamma$ se, e somente se, $(\alpha, \beta) = 1$.*

Proposição 4.8. ($\Rightarrow$) *Suponha que exista $\beta \in \mathbb{Z}[i]$ com $\alpha\beta \equiv 1 \mod \gamma$. Então $\alpha\beta - 1 = \gamma\lambda$ para algum $\lambda \in \mathbb{Z}[i]$, logo $\alpha\beta - \gamma\lambda = 1$. Desde que $\mathbb{Z}[i]$ é um domínio euclidiano, segue pelo **Teorema 2.12** que $(\alpha, \gamma) = 1$.*
($\Leftarrow$) *Seja $(\alpha, \gamma) = 1$. Novamente, pelo **Teorema 2.12**, existem $\beta, \lambda \in \mathbb{Z}[i]$ tais que $\alpha\beta + \gamma\lambda = 1$. Assim, $\alpha\beta - 1 = (-\lambda)\gamma$, portanto $\alpha\beta \equiv 1 \mod \gamma$.*

Teorema 4.12. *Se $\alpha, \mu \in \mathbb{Z}[i]$ são primos entre si, então $\alpha^{\xi(\mu)} \equiv 1 \mod \mu$.*

Demonstração. Sejam $\gamma_1, ..., \gamma_{\xi(\mu)}$ um sistema completo de invertíveis módulo μ e seja $(\alpha, \mu) = 1$. Daí, pela proposição anterior temos que $(\gamma_i, \alpha) = 1$ para todo $1 \leq i \leq \xi(\mu)$, e assim $(\alpha\gamma_i, m) = 1$ para todo $1 \leq i \leq \xi(\mu)$. Logo, $\alpha\gamma_1, ..., \alpha\gamma_{\xi(\mu)}$ também forma um sistema completo de resíduos módulo μ. Com isso, temos que $\alpha\gamma_i \equiv \alpha\gamma_j \mod \xi(\mu)$, logo $\gamma_i \equiv \gamma_j \mod \mu$ o que implica em $i = j$. O que implica que $\alpha\gamma_i \equiv \gamma_i \mod \xi(\mu)$, portanto,

$$\prod_{i=1}^{\xi(\mu)} (\alpha\gamma_i) \equiv \prod_{i=1}^{\xi(\mu)} \gamma_i \mod \mu \iff \alpha^{\xi(\mu)} \prod_{i=1}^{\xi(\mu)} \gamma_i \equiv \prod_{i=1}^{\xi(\mu)} \gamma_i \mod \mu.$$

Como cada γ_i é invertível módulo μ, basta simplificar a última congruência e obtemos, portanto $\alpha^{\xi(\mu)} \equiv 1 \mod \mu$ como desejado. □

4.3 Inteiros de Eisenstein

Definição 4.18. Seja $\omega = \frac{1}{2}(-1 + i\sqrt{3}) \in \mathbb{C}$. Os Inteiros de Eisenstein é o conjunto

$$\mathbb{Z}[\omega] := \{a + b\omega \in \mathbb{C} | a, b \in \mathbb{C}\}.$$

o qual é uma subanel de $\mathbb{C}$.

Observação 4.5. Seguindo a **Definição 4.12** a norma de um elemento $a + b\omega \in \mathbb{Z}[\omega]$ é

$$\begin{aligned} |a + b\omega|^2 &= \left[a + b\left(\frac{-1 + i\sqrt{3}}{2}\right)\right]\left[a + b\left(\frac{-1 - i\sqrt{3}}{2}\right)\right] \\ &= a^2 - \frac{ab}{2} - \frac{abi\sqrt{3}}{2} - \frac{ab}{2} + \frac{abi\sqrt{3}}{2} + b^2 \\ &= a^2 - ab + b^2. \end{aligned}$$

Teorema 4.13. *Os Inteiros de Eisenstein é um domínio euclidiano.*

Demonstração. Desde que $\mathbb{Z}[\omega] \subset \mathbb{C}$, a função norma de $\mathbb{C}$ restrita ao conjunto $\mathbb{Z}[\omega]$,isto é, $N : \mathbb{Z}[\omega] \to \mathbb{N}$ dada por $a + b\omega \mapsto a^2 - ab + b^2$, está bem definida e é uma norma. Sejam $\alpha = a + b\omega, \beta = m + n\omega \in \mathbb{Z}[\omega]$ não nulos. Assim $\mathbb{N}(\beta) > 0$, logo $N(\alpha\beta) = N(\alpha)N(\beta) = (a^2 - ab + b^2)(m^2 - mn + n^2) \geq a^2 - ab + b^2 = N(\alpha)$.
Agora vamos mostrar que vale a divisão euclidiana. Tome $\alpha, \beta \in \mathbb{Z}[\omega]$. Podemos escrever $\alpha/\beta = x + y\omega$ com $x, y \in \mathbb{Z}[w]$. Tome $m, n \in \mathbb{Z}$ tais que $|x - m| \leq 1/2$ e $|y - n| \leq 1/2$. Considere $\gamma = m + n\omega$ e $\pi = \alpha - \gamma\beta$. Daí, pela desigualdade triangular, obtemos

$$\left|\frac{\alpha}{\beta} - \gamma\right| = |(x - m) + (y - n)| \leq |x - m| + |y - n| \leq \frac{1}{2} + \frac{1}{2} = 1 \quad (4.1)$$
$$\implies \left|\frac{\alpha}{\beta} - \gamma\right| |\beta| \leq 1|\beta| \implies |\alpha - \gamma\beta| \leq |\beta| \implies |\alpha - \gamma\beta|^2 \leq |\beta|^2.$$

Note que não existem $r_1, r_2 \in \mathbb{R}^*$ tais que $r_1 \cdot 1 + r_2 \cdot \omega = 0$, logo a primeira desigualdade ede (4.1) é estrita exceto para $x - m = 0$ e $y - n = 0$. Mas, em ambos os casos a segunda desigualdade de (4.1) é estrita. Portanto, obtemos $N(\pi) < N(\beta)$. Com isso, temos que a **Definição 2.19** é válida. $\square$

Comentário 4.6. Desde que $\mathbb{Z}[\omega]$ é um domínio euclidiano, a existência de elementos irredutíveis consiste em $\mathbb{Z}[\omega]$ assim como a fatoração única a menos de unidade e da ordem dos fatores. Com isso, $Z[\omega]$ possui uma estrura muito semelhante ao conjunto dos inteiros $\mathbb{Z}$. Além do mais, assim como em $Z[i]$, alguns elementos irredutíveis em $\mathbb{Z}$ podem ser redutíveis em $Z[\omega]$, por exemplo, o inteiro 3.

Proposição 4.9. *As unidade em* $\mathbb{Z}[\omega]$ *são* $\{\pm 1, \pm\omega, \pm\omega^2\}$.

Demonstração. Para verificar que esses elementos são unidades bastar ver que

$$\begin{aligned}
\omega^2\omega &= \left(\frac{-1 + i\sqrt{3}}{2}\right)^3 \\
&= \frac{-1 + 3i\sqrt{3} - 3(i\sqrt{3})^2 - 3i\sqrt{3}}{8} \\
&= \frac{-1 - 3(-1)3}{8} = 1
\end{aligned}$$

e o caso ± 1 é direto. Agora tome $\alpha = a + b\omega \in \mathbb{Z}[w]$ unidade. Assim, para $\beta \in \mathbb{Z}[\omega]$, temos $\alpha\beta = 1$. Então $N(\alpha\beta) = N(\alpha)N(\beta) = 1$, e segue que $N(\alpha) = N(\beta) = 1$. Com isso vem

$$N(\alpha) = a^2 - ab + b^2 = 1 \implies (a-b)^2 + ab - 1 = 0. \tag{4.2}$$

Desde que $a, b \in \mathbb{Z}$, temos $a - b, ab \in Z$. Daí, as soluções de (4.2) são $(a, b) \in \{(\pm 1, 0), (0, \pm 1)(\pm 1, \pm 1)\}$ e o resultado segue substituindo esses valores de a e b em α. □

Lema 4.14. *Se $\alpha \in \mathbb{Z}[\omega]$ e $N(\alpha)$ é um inteiro primo, então α é irredutível em $\mathbb{Z}[w]$.*

Demonstração. Sejam $\alpha = \gamma\beta \in \mathbb{Z}[\omega]$ e $N(\alpha)$ um inteiro primo. Assim $N(\alpha) = N(\gamma\beta) = N(\gamma)N(\beta)$. Desde que $N(\alpha)$ é primo, devemos ter ou $N(\gamma) = 1$ ou $N(\beta) = 1$. Assim, como $\mathbb{Z}[\omega]$ é um domínio euclidiano, pelo **Teorema 2.8** temos que ou $N(\gamma)$ é uma unidade ou $N(\beta)$ o é. □

Teorema 4.15. *Seja p um inteiro primo. Então:*

(1) Se $p = 3$, então $1 - \omega \in \mathbb{Z}[\omega]$ é irredutível e $3 = -\omega^2(1-\omega)^2$.

(2) Se $p \equiv 1 \mod 3$, então existe um irredutível $\gamma \in \mathbb{Z}[\omega]$ tal que $p = \gamma\overline{\gamma}$ e $\gamma \not\sim \overline{\gamma}$.

(3) Se $p \equiv 2 \mod 3$, então p é irredutível em $\mathbb{Z}[\omega]$.

Demonstração. Vamos mostrar somente (1), mas uma demonstração completa para esse teorema pode ser encontrada em [2, Cap. 4, pg. 169]. Desde que $N(1-\omega) = 1^2 - 1(-1) + (-1)^2 = 3$, pelo **Lema 4.11** temos que $1 - \omega$ é irredutível em $\mathbb{Z}[\omega]$. □

4.4 Extensões Quadráticas

Definição 4.19. Seja $d \in \mathbb{Z}$ não quadrado perfeito. O conjunto

$$\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} \quad | \quad a, b \in \mathbb{Z}\}$$

é chamado de extensão quadrática.

Observação 4.6. O conjunto $\mathbb{Z}[\sqrt{d}]$ é fechado pela soma e produto e forma um anel. Algumas propriedades aritméticas definidas em $\mathbb{Z}[i]$ e em $\mathbb{Z}[\omega]$ podem ser extendidas para $\mathbb{Z}[\sqrt{d}]$, como a divisibilidade:

$$\beta \mid \alpha \iff \exists\gamma \in \mathbb{Z}[\sqrt{d}]; \alpha = \gamma\beta.$$

E de forma análoga ao anéis $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$ definimos, também, a relação de congruência

$$\alpha \equiv \beta \mod \lambda \iff \lambda \mid \alpha - \beta.$$

Teorema 4.16. *Seja $p \in \mathbb{Z}$ um número primo tal que $p \neq 2$ e $p \nmid d$. Então, para todo $\alpha \in \mathbb{Z}[\sqrt{d}]$,*

$$\alpha^{p^2} \equiv \alpha \mod p.$$

Demonstração. Seja $\alpha = a + b\sqrt{d}$ com $a, b \in \mathbb{Z}$. Desde que $p \mid \binom{p}{i}$ para $i = 1, ..., p-1$ segue que,

$$\alpha^p = (a + b\sqrt{d})^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i}(b\sqrt{d})^i \equiv a^p + b^p(\sqrt{d})^p \mod p.$$

Pelo pequeno teorema de Fermat temos que $a^p \equiv a \mod p$ e $b^p \equiv b \mod p$, logo $\alpha^p \equiv a^p + b^p(\sqrt{d})^p \mod p$. Elevando a última congruência a p, obtemos,

$$\alpha^{p^2} \equiv (a + b\sqrt{d}^p)^p \equiv a + b(\sqrt{d})^{p^2} = a + b(d^{p-1})^{\frac{p-1}{2}})\sqrt{d} \mod p. \tag{4.3}$$

Por hipótese temos que $p \neq 2$ e $p \nmid d.$, daí $(p+1)/2 \in \mathbb{Z}$ e $(d, p) = 1$.Então novamente pelo pequeno teorema de Fermat, vem que e pelo cancelamento, temos,

$$\left(d^{\frac{p+1}{2}}\right)^p \equiv d \mod p \implies \left(d^{\frac{p+1}{2}}\right)^{p-1} \equiv 1 \mod p. \tag{4.4}$$

Portanto, de (4.3) e (4.4) obtemos $\alpha^{p^2} \equiv \alpha \mod p$. □

Proposição 4.10. *Seja $p \in \mathbb{Z}$ primo com $p \nmid d$. Então $\mathbb{Z}[\sqrt{d}]/pZ$ é um corpo se, e somente se, $\left(\frac{d}{p}\right) = -1$.*

Demonstração. $(\Rightarrow)$ Vamos mostrar a contrapositiva. Suponha que $\left(\frac{d}{p}\right) = 1$ onde $a^2 \equiv d \mod p$ com $a \in \mathbb{Z}$. Assim, desde que $(a + \sqrt{d})(a - \sqrt{d} = a^2 - d \equiv 0 \mod p$, temos $a \pm \sqrt{d}$ não nulos, logo são divisores de zero. Portanto, $\mathbb{Z}[\sqrt{d}]/pZ$ não é um corpo.
$(\Leftarrow)$ Sejam $\left(\frac{d}{p}\right) = -1$ e $a + b\sqrt{d} \not\equiv 0 \mod p$. Assim, ou $p \nmid a$ ou $p \nmid b$. Vamos mostrar que nessas condições temos $a^2 + b^2 d$ inversível módulo p. Se $p \nmid a$ então devemos ter $p \mid b$. Daí $a \not\equiv 0 \mod p$ e $b \equiv 0 \mod p$, então

$$a^2 + b^2 d \equiv a^2 \equiv 0 \mod p$$

o que não pode ocorrer pois $p \nmid a$. Se $p \nmid b$, então $p \mid a$. Daí vem que

$$a^2 + b^2 d \equiv 0 \mod p \iff \left(\frac{a}{b}\right)^2 \equiv d \mod p$$

o que também não pode ocorrer pois $\left(\frac{d}{p}\right) = -1$. Em ambos os casos temos que $a^2 + b^2 d \not\equiv 0 \mod p$, portanto é inversível módulo p. Portanto, $\mathbb{Z}[\sqrt{d}]/pZ$ é um corpo. $\square$

Comentário 4.7. Para alguns valores de d o conjunto $\mathbb{Z}[\sqrt{d}]$ é um domínio euclidiano.

Capítulo 5

Triplas pitagóricas e soma de dois quadrados

Veremos alguns resultados sobre triplas pitagóricas que são soluções para a equação diofantina $x^2+y^2=z^2$, as quais correspondem aos lados de triângulos retângulos de comprimentos inteiros. Também veremos alguns resultados sobre soma de dois quadrados.

5.1 Soma de dois quadrados

Teorema 5.1. *Seja $p \in \mathbb{Z}$ um número primo. Então a equação $x^2+y^2=p$ possui solução inteira se, e somente se, $p=2$ ou $p \equiv 1 \mod 4$.*

Demonstração. ($\Rightarrow$) Primeiramente, fazendo $x=y=1$ obtemos $p=2$. Considere $p \in \mathbb{Z}$ um primo ímpar. Desde que os resíduos módulo 4 são $0,1,2,3$ temos que $p \not\equiv 0 \mod 4$, pois se fosse o contrário teríamos $4 \mid p$ e p seria um número par, também devemos ter $p \not\equiv 2 \mod 4$, caso contrário $p=2+4k$ para algum $k \in \mathbb{Z}$ e vem que $2 \mid p$, ou seja, p seria par. Dsde que p é ímpar, temos que $p-1$ é par e, então, podemos ter $p \equiv 1 \mod 4$. De forma análoga, sendo p ímapar, temos $p-1$ par, assim $(p-1)-2=p-3$ também é par e podemos ter $p \equiv 3 \mod 4$. Portanto, se $p \in \mathbb{Z}$ é um primo ímpar, devemos ter $p \equiv 1 \mod 4$ ou $p \equiv 3 \mod 4$. Agora note que se $x \in \mathbb{Z}$, então x é congruente a 0, ou 1, ou 2, ou 3 módulo 4, segue:

$$\begin{aligned}
x \equiv 0 \mod 4 &\implies x^2 \equiv 0 \mod 4 \\
x \equiv 1 \mod 4 &\implies x^2 \equiv 1 \mod 4 \\
x \equiv 2 \mod 4 &\implies x^2 \equiv 4 \equiv 0 \mod 4 \\
x \equiv 3 \mod 4 &\implies x^2 \equiv 9 \equiv 1 \mod 4
\end{aligned}$$

então temos que $x^2 \equiv 1 \mod 4$ ou $x^2 \equiv 0 \mod 4$ e o mesmo vale para y. Com isso vem que $x^2 + y^2 \equiv 0 \mod 4$ ou $x^2 + y^2 \equiv 1 \mod 4$. Agora suponha que $x^2 + y^2 = p$ com $p \in \mathbb{Z}$ primo ímpar, juntando os resultados acima devemos ter $p \equiv 1 \mod 4$.
($\Leftarrow$) Se tivermos $p = 2$, $x = y = 1$ é uma solução da equação. Agora suponha que $p \equiv 1 \mod 4$, então pelo **Teorema 5.11** existem $x, y \in \mathbb{Z}$ com $x^2 + y^2 = p$. □

Teorema 5.2. *Os únicos números n que podem se expressar como soma de dois quadrados são da forma $n = 2^s d^2 l$ onde $s \in \mathbb{N}$ e $l \in \mathbb{Z}$ é livre de quadrados com fatores primos $p \in \mathbb{Z}$ tais que $p \equiv 1 \mod 4$.*

Demonstração. Uma demonstração para esse teorema pode ser encontrada em [9, Cap. 4, pg.136]. □

5.2 Triplas pitagóricas

Definição 5.1. As triplas de números (a, b, c) que satisfazem a equação $x^2 + y^2 = z^2$ são chamada de *triplas pitagóricas.* Se a, b e c forem dois a dois primos entre si, dizemos que a terna (a, b, c) é uma *tripla pitagórica primitiva.*

Proposição 5.1. *As ternas pitagóricas primitivas (a, b, c) são da forma*

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2$$

com $(m, n) = 1$ e $m + n$ ímpar.

Demonstração. Suponha que $p \in \mathbb{Z}$ é um primo tal que $p \mid (a, b)$. Então $p \mid a^2 + b^2 = c^2$, logo $p \mid c$. Daí temos que $(a/p, b/p, c/p)$ também é uma trilpa pitagórica. Com isso, suponha que (a, b, c) é um tripla pitagórica primitiva. Assim, temos que a e b não podem ambos serem pares ao mesmo tempo, suponhamos que a é ímpar. Como um número quadrado é congruente a 0 ou a 1 módulo 4 e $(2k + 1)^2 \equiv 1 \mod 4$, devemos ter b um número par, senão $c^2 = b^2 + a^2 \equiv 2 \mod 4$, o que não pode ocorrer. Com isso vem que c é ímpar. Também temos que $b^2 = (c + a)(c - a) = c^2 + a^2$ e, como $(a, c) = 1$, então $(a + c, c) = 1$, temos $a + c$ 4 $a - c$ números pares, logo $(2c, c + a) = (c - a, a + c) = 2$. Daí, desde que b é par, vem que $(c + a)/2$ e $(c - a)/2$ são primos entre si tais que

$$\frac{c-a}{2}\frac{c+a}{2} = \frac{c^2 - a^2}{4} = \frac{b^2}{4} = \left(\frac{b}{2}\right)^2 = k^2 \quad , k \in \mathbb{Z}.$$

Então, pelo teorema Fundamental da Aritmética $(c+a)/2 = m^2$ e $(c-a)/2 = n^2$ para algum $m, n \in \mathbb{Z}$ e vem que $b = 2mn$. Portanto temos que,

$$m^2 - n^2 = \frac{c+a}{2} - \frac{c-a}{2} = a \quad \text{e} \quad m^2 + n^2 = \frac{c+a}{2} + \frac{c-a}{2} = c.$$

$\square$

Teorema 5.3 (Legendre). *Sejam $a, b, c \in \mathbb{Z}$ livres de quadrados, dois a dois primos entre si e não todos com o mesmo sinal. A equação $ax^2 + by^2 + cz^2 = 0$ tem solução não trivial inteira se, e somente se, $m^2 \equiv -bc \mod a, n^2 \equiv -ac \mod b$ e $k^2 \equiv -ab \mod c$.*

Demonstração. Uma demonstração para esse teorema pode ser encontrada em [9, Cap. 4, pg. 139]. $\square$

Teorema 5.4. *As soluções racionais (x, y) da equação diofantina $x^2 + y^2 = 1$ são da forma $(x, y) = (1, 0)$ e*

$$(x, y) = \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right) \quad , t \in \mathbb{Q}.$$

Demonstração. Temos que $(1, 0)$ é solução da equação e sabemos que essa equação produz uma circunferência C de raio 1 no plano cartesiano. Considere $t \in \mathbb{Q}^*$ e o ponto $(0, t)$. A reta d l que passa por $(1, 0)$ e $(0, t)$ é dada pela equação $y = -tx + t$. Sendo $0 \neq t$, a reta l não é paralela ao *eixo-y* e portanto não é tangente a circunferência. Dessa maneira, temos que l intersecta a circunferência C em dois pontos. Assim, como $x^2 + y^2 = 1$ e $y = -tx + t$, segue que

$$x^2 + (t - tx)^2 = 1 \implies (t^2+1)x^2 - 2t^2x + t^2 - 1 = 0 \implies x = \frac{2t^2 \pm 2}{2(t^2+1)}.$$

Então temos $x_1 = 1$ e $x_2 = (t^2-1)/(t^2+1)$. Aplicando esses valores de x na equação da reta l, obtemos $y_1 = t - tx_1 = t - t = 0$ e

$$y_2 = t - tx_2 = t - t\frac{t^2-1}{t^2+1} = \frac{t(t^2+1)}{t^2+1} - \frac{t(t^2-1)}{t^2+1} = \frac{2t}{t^2+1}.$$

Desde que $t \in \mathbb{Q}$, o par $\left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right)$ é racional. Tome um ponto $Q = (x_q, y_q) \in C$ racional com $Q \neq (1, 0)$. Então a reta $r : y = \alpha x + \beta$ que contém Q e $(1, 0)$ é dada por

$$\alpha = \frac{y_q - 0}{x_q - 1} \implies y = \left(\frac{y_q - 0}{x_q - 1}\right)x_q + b \implies b = y - \left(\frac{y_q}{x_q - 1}\right)x_q.$$

Substituindo $x = x_q$ e $y = y_q$ temos que $b \in \mathbb{Q}$. possui coeficientes racionais, logo intersexta o *eixo-y* em algum ponto racional $(0, b)$. Portanto,

$$(0,1) \mapsto \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right) \tag{5.1}$$

estabele uma bijeção entre pontos racionais do *eixo-y* e os pontos racionais da circunferência. O que finaliza a demonstração. $\square$

Capítulo 6

Curvas elípticas

As referênciais principais para esse capítulo foram [8], [7], [11] e [10]. Apresentaremos as definições e os resultados fundamentais que utilizamos durante os estudos.

6.1 Curvas elípticas como curvas projetivas

Seja K um corpo. O *espaço projetivo* $\mathbb{P}^n_K$ é o conjunto de todas as retas em K^{n+1} que passam pela origem. Um ponto não nulo $(x_0, ..., x_n)$ em K^{n+1} pode ser entendido como um vetor. Dois vetores $(x_0, ..., x_n)$ e $(y_0, ..., y_n)$ definem uma mesma reta que passa pela origem quando $(x_0, ..., x_n) = \lambda(y_0, ..., y_n) = (\lambda y_0, ..., \lambda y_n)$ para algum $\lambda \in K$. Dessa forma, esses vetores correspondem a um mesmo ponto em $\mathbb{P}^n_K$ e, então, podemos definir o espaço projetivo da seguinte maneira:

Definição 6.1. Seja K um corpo e $n \in \mathbb{N}$ com $1 \leq n$. Chamamos de *espaço projetivo* de dimensão n sobre o corpo K o conjunto quociente:

$$\mathbb{P}^n_K = \frac{K^{n+1}\backslash\{0\}}{\sim}$$

para o qual $\sim$ é uma relação de equivalência entre pontos que estão numa mesma reta, assim temos que

$$(x_0, ..., x_n) \sim (y_0, ..., y_n) \iff \exists\lambda \in K^*; (x_0, ..., x_n) = (\lambda y_0, ..., \lambda y_n).$$

Os elementos de $\mathbb{P}^n_K$ são as classes de equivalência dadas por

$$(x_0 : ... : x_n) = \{(\lambda x_0, ..., \lambda x_n) | \lambda \in K^*\}.$$

Observação 6.1. O mapa $\sigma : K^n \to \mathbb{P}^n_K$, definido de forma que $(x_0, ..., x_{n-1}) \mapsto (x_0 : ... : x_{n-1} : 1)$, é injetivo. E com isso temos que $\text{Im}(\sigma) = \{(x_0 : ... : x_n) | x_n \neq 0\}$ é uma cópia de K^n em $\mathbb{P}^n_K$.

Definição 6.2. Chamamos de pontos no infinito os elementos do conjunto

$$H_\infty = \mathbb{P}^n_K \backslash \text{Im}(\sigma).$$

Observação 6.2. Com a definição acima temos $\mathbb{P}^n_K = \text{Im}(\sigma) \cup H_\infty$. Veja que existe também a função $\psi : \text{Im}(\sigma) \to K^n$ dada por $(x_0 : ... : x_n) \mapsto \left(\frac{x_0}{x_n}, ..., \frac{x_{n-1}}{x_n}\right)$. Assim, $\sigma \circ \psi = id_{\text{Im}(\sigma)}$ e $\psi \circ \sigma = id_{K^n}$. Então podemos visualizar os objetos de K^n em $\mathbb{P}^n_K$ e observar os objetos no espaço projetivo como união de seus pontos no infinito com o seu complementar, que é sua *parte a fim*.

Definição 6.3. Seja K um corpo e seja $p(x, y) \in K[x, y]$ um polinômio não constante. O subconjunto $C \subset K^2$ dado por,

$$C = \{(a, b) \in K^2 | p(a, b) = 0\}$$

é chamado de *curva algébrica*. Nesse caso diremos que $p(x, y) = 0$ é uma equação para a curva C.

Definição 6.4. Seja K um corpo. Um subconjunto $X \subset K^2$ é chamado de *curva plana projetiva* se existe um polinômio homogêneo $p(x, y) \in K[x, y, z]$ não constante tal que $X = \{(a : b : c) \in \mathbb{P}^2_K | p(a, b, c) = 0\}$.

Exemplo 6.1. Seja K um corpo e seja $C_1 = \{(x, y) | ax + by + c = 0\} \in K^2$, isto é, $C_1 : ax + by + c = 0$. A fim de encontrar $\sigma(C_1)$, precisamos fazer $x \mapsto x/z$ e $y \mapsto y/z$. Daí temos a equação $a(x/z) + b(y/z) + c = 0$ que implica em $ax + by + cz = 0$, que é um polinômio homogêneo e, então, define um curva em $\mathbb{P}^3_K$ dada por $C_1 = \{(a : b : c) | ax + by + cz = 0\}$. Para encontrar $\mathcal{O}$ tomamos $z = 0$, daí vem que $ax + by = 0$, logo $x = -b$ e $y = a$. Então, $\mathcal{O} = (-b : a : 0)$.

Exemplo 6.2. Seja K um corpo e seja $C : y - x^2 = 0$. Daí para encontrar $\sigma(C_2)$ fazemos $y \mapsto y/z$ e $x \mapsto x/z$. Obtemos $y/z - (x/z)^2 = 0$ que implica em $yz - x^2 = 0$. Assim, $\sigma(C_2) = \{(a : b : c) | yz - x^2 = 0\}$. Agora fazendo $z = 0$, segue que $x^2 = 0$, logo $x = 0$. E com isso vem que $y = 1$. Portanto, $\mathcal{O} = (0 : 1 : 0)$.

Definição 6.5. Sejam K um corpo e $C \subset \mathbb{P}^n_K$ uma curva projetiva, seja $P \in C$ um ponto. Dizemos que P é um *ponto singular* da curva $C : p(x_: ... : x_n) = 0$ se tivermos,

$$\frac{\partial p}{\partial x_i}(P) = 0 \quad , \forall i \in \{0, ..., n\}.$$

Caso contrário diremos que P é um ponto *suave* de C ou um ponto *não singular* de C.

Definição 6.6. Dizemos que uma curva C é uma *curva suave* ou *não singular* se todos os pontos em C são suaves.

Definição 6.7. Seja K um corpo de característica diferente de 2 e 3. Uma curva projetiva plana suave definida pela equação

$$y^2 z = x^3 + axz^2 + bz^3, \quad a, b \in K,$$

é chamda de *curva elíptica* sobre K.

Comentário 6.1. Observe que a curva projetiva acima é curva algébrica definida pela equação $y^2 = x^4 + ax + b$ para $z \neq 0$, juntamente com o ponto no infinito $\mathcal{O}(0 : 1 : 0)$. Para nos refirmos a uma curva E definida sobre um corpo K escreveremos E/K ou simplesmente $E(K)$.

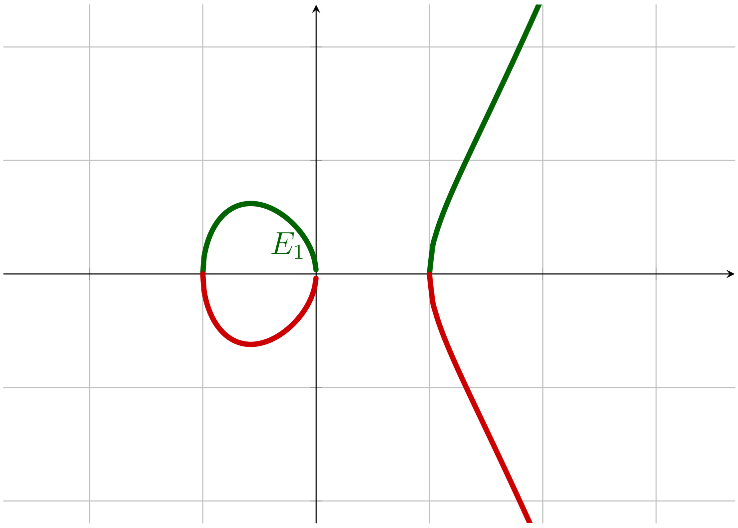
Observação 6.3. Podemos definir uma curva elíptica sobre um corpo K de característica diferente de 2 e 3 como o conjunto dos pontos (x, y) que satisfazem a equação $y^2 = x^3 + ax + b$, onde $p(x) = x^3 + ax + b$ não possui raízes múltiplas, juntamente do ponto no infinito $\mathcal{O}$. Para que $p(x)$ não possua raízes múltiplas é necessário que a condição $4a^3 + 27b^2 \neq 0$ seja satisfeita. O motivo para tal restrição pode ser encontrado em [10, Cap.3, pg. 45].

Comentário 6.2. A equação mais geral para uma curva elíptica sobre um corpo K de característica qualquer é a equação de Weierstrass:

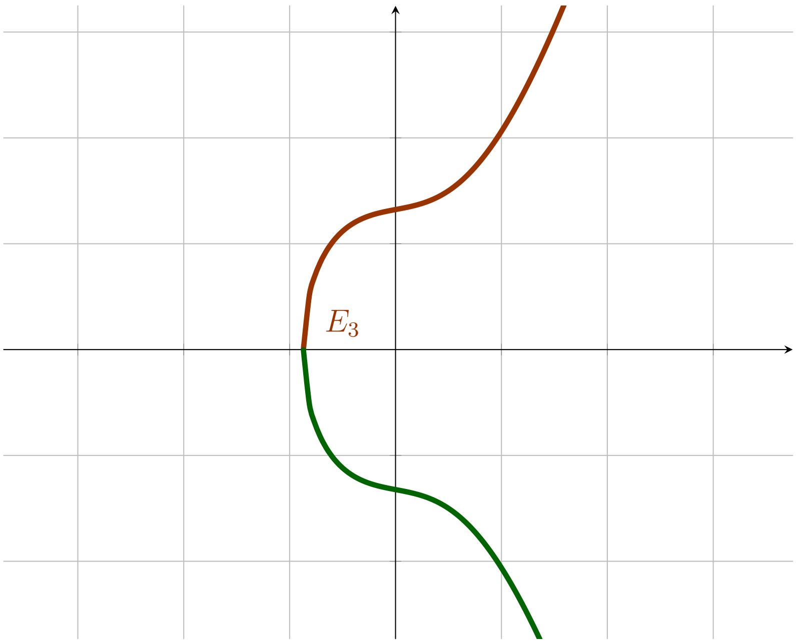
$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Dependendo da característica do corpo K, podemos manipular a equação acima a fim de simplicá-la e obter, portanto, uma expressão mais fácil de trabalhar. Estaremos interessados em curvas eliticas com coeficientes racionais e, portanto, a próxima definição será de maior apoio.

Exemplo 6.3. $E_1(\mathbb{R}) : y^2 = x^3 - x$ é uma curva elíptica sobre o corpo dos números reais.



Exemplo 6.4. $E_3(\mathbb{R}) : y^2 = x^3 + x + 7$ é outra curva elíptica sobre $\mathbb{R}$.



6.2 Lei da corda tangente

Vamos trabalhar com curvas elípticas dadas por equações na forma $y^2 = x^3 + ax + b$. Para que essa curva seja não singular é necessário que tenhamos $4a^3 + 27b^2 \neq 0$. Sendo satisfeita essa condição podemos definir um grupo a partir da curva $E : y^2 = x^3 + ax + b$ juntamente com seu ponto no infinito $\mathcal{O}$. Denotaremos a operação desse grupo por $+$ e a chamaremos de adição, o ponto $\mathcal{O}$ será o elemento neutro dessa operação. O caso da equação geral de Weierstrass pode ser consultado em [10, Cap. 3, pg.52].

Definição 6.8. Seja E uma curva elíptica dada pela equação de Weierstrass $y^2 = x^3 + ax + b$ com $4a^3 + 27b^2 \neq 0$ e com $\mathcal{O}$ o ponto no infinito. Sejam $P, Q \in E$. Definimos o oposto de P, que é denotado por -P, e a soma $P + Q = S$ pelas seguintes regras:

(i) Se $P = \mathcal{O}$, então $-P = \mathcal{O}$ e $P + Q = Q$.

Agora suponha que $P \neq \mathcal{O}$ e $Q \neq \mathcal{O}$ e sejam $P = (x_p, y_p)$ e $Q = (x_q, y_q)$.

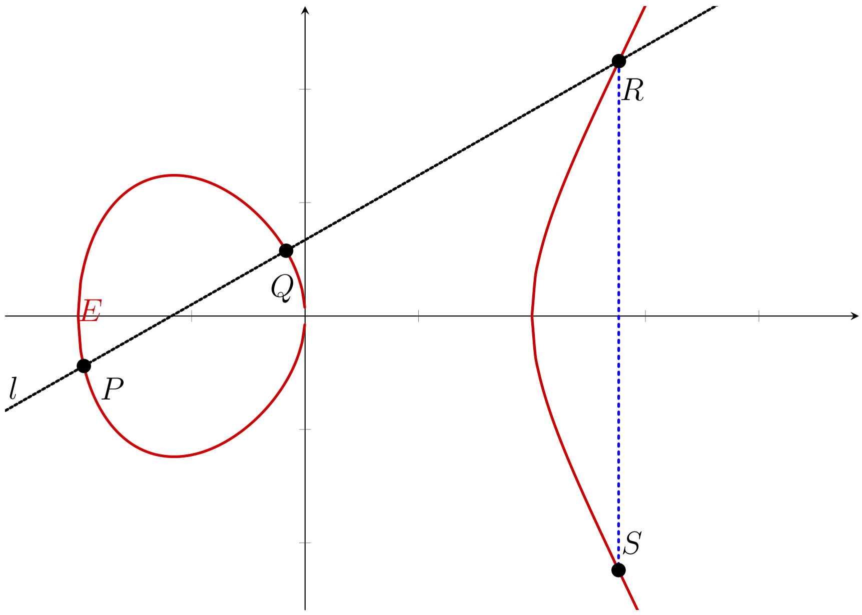
(1) O oposto de P é dado por $-P = (x_p, -y_p)$.

(2) Se $x_p \neq x_q$, então a reta l que passa pelos pontos P e Q não é paralela ao *eixo-y*, logo l intersecta a curva em um ponto R além de P e Q. Portanto, definimos $P + Q = S = -R$.

(3) Se $Q = -P$, então $P + Q = \mathcal{O}$.

(4) Se $P = Q$, então a reta l que passa por P e Q é uma reta tangente à curva E em P. Daí definimos o ponto $P + Q = S = -R$ onde R é o segundo ponto de intersecção de l com E. Se nesse caso tivermos $y_p = y_q = 0$, então a reta l é vertical, daí $P + Q = \mathcal{O}$.

Observação 6.4. A figura abaixo representa o pensamento geométrico por trás da definição acima.



Vamos ver algebricamente o porquê da definição acima. Mostraremos que existe um terceito ponto S de intersecção da reta l que passa por P e Q, e vamos deduzir as coordenadas do ponto $S = P + Q$.

Sejam $P = (x_p, y_p), Q = (x_q, y_q)$ e $S = (x_s, y_s)$. Se tivermos $x_p \neq x_q$, estaremos no caso (2). Suponha que $l = \alpha x + \beta$ é a reta que contém P e Q. Temos que l não é paralela ao *eixo-y* pois $x_p \neq x_q$. Desde que $P, Q \in l$, temos $\alpha x_p + \beta = y_p$ e $\alpha x_q + \beta = y_q$, dessa maneira podemos escrever $\alpha = (y_q - y_p)/(x_q - x_p)$ e $\beta = y_p - \alpha x_p$. Agora veja que um ponto qualquer $X = (x, y) \in l$, onde $y = \alpha x + \beta$, pertence à curva $E : y^2 = x^3 + ax + b$ se, e somente se, $(\alpha x + \beta)^2 = x^3 + ax + b$. Ou seja, esse ponto deve ser raiz da equação $x^3 - (\alpha x + \beta)^2 + ax + b = 0$. Como a equação possui no máximo três raízes, existem no máximo três pontos de intersecção entre a reta l e a curva E. Podemos reescrever a equação:

$$x^3 - (\alpha x + \beta)^2 + ax + b = x^3 - \alpha^2 x^2 + (a - 2\alpha\beta)x + b - \beta^2 = 0.$$

Como P e Q pertencem a curva E, então x_p e x_q são raízes da equação, também, como a soma das raízes de um polinômio mônico é igual ao coeficiente da variável da indeterminada de segundo maior grau, temos que $x_p + x_q + x_s = \alpha^2$, logo $x_s = \alpha^2 - x_p - x_q$. Agora, como $P + Q = S \in l$, devemos ter $y_s = \alpha x_s + \beta$. Portanto, temos que:

$$x_s = \left(\frac{y_q - y_p}{x_q - x_p}\right)^2 - x_p - x_q \quad \text{e} \quad y_s = -y_p + \left(\frac{y_q - y_p}{x_q - x_p}\right)(x_p - x_s). \tag{6.1}$$

Suponhamos que $P = Q$ com $y_p \neq 0$. Então, l é uma reta não vertical tangente à curva E e podemos encontrar o coeficiente angular de l derivando a equação $y^2 = x^3 + ax + b$. Para isso devemos interpretar $y = f(x)$, e derivar a igualdade em relação à variável x, no lado esquerdo teremos a derivada de um função composta, segue:

$$y^2 = x^3 + ax + b \implies 2y\frac{dy}{dx} = 3x^2 + a \implies \alpha = \frac{dy}{dx} = \frac{3x^2 + a}{2y}.$$

Então, no ponto P temos $\alpha = (3x_p^2 + a)/2y_p$ e vem que:

$$x_s = \left(\frac{3x_p^2 + a}{2y_p}\right)^2 - 2x_p \quad \text{e} \quad y_s = -y_p + \left(\frac{3x_p^2 + a}{2y_p}\right)(x_p - x_s). \tag{6.2}$$

Teorema 6.1. *Os ponto de adição de uma curva elíptica E dada pela equação $y^2 = x^3 + ax + b$ forma um grupo abeliano $(E, +)$ onde o ponto $\mathcal{O}$ é o elemento neutro.*

Demonstração. Uma demonstração para esse teorema pode ser encontrada em [12, Cap. 2, pg. 15]. □

Comentário 6.3. O teorema acima nos garante que encontrado um par de pontos racionais numa curva elíptica, podemos encontrar um terceiro ponto racional. Pois, como suas coordenadas são racionais e o conjunto dos racionais é um corpo, a partir das fórmulas em (5.1) e (5.2) sabemos que o terceiro ponto será racional também.

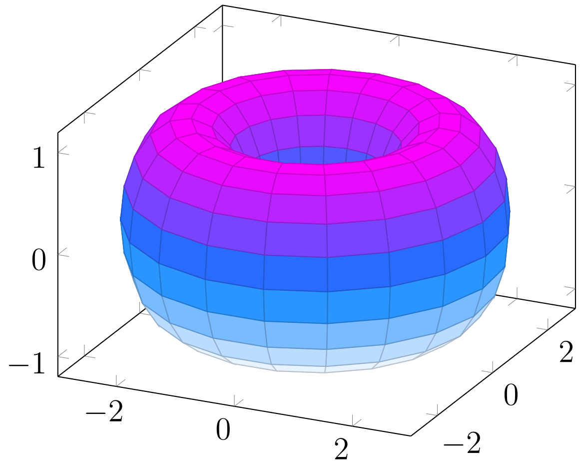
Teorema 6.2 (Mordell-Weil)**.** *O conjunto dos pontos racionais de um curva elíptica $E(\mathbb{Q})$ é um grupo abeliano finitamente gerado. Em outras palavras, existem finitos pontos $P_1, ..., P_n$ tais que qualquer outro ponto $Q \in E(\mathbb{Q})$ pode ser escrito como combinação linear dos P_i, onde $i \in \{1, ..., n\}$:*

$$Q = a_1P_1 + a_2P_2 + ... + a_nP_n \quad , a_i \in \mathbb{Z}.$$

Demonstração. Uma demonstração para esse teorema pode ser encontrada em [11, Cap. 3, pg. 83] □

6.3 Curvas elípticas sobre $\mathbb{C}$

Abordaremos, agora, algumas definições e propriedades que nos permitem visualizar curvas elípticas como um torus(rosquiha).



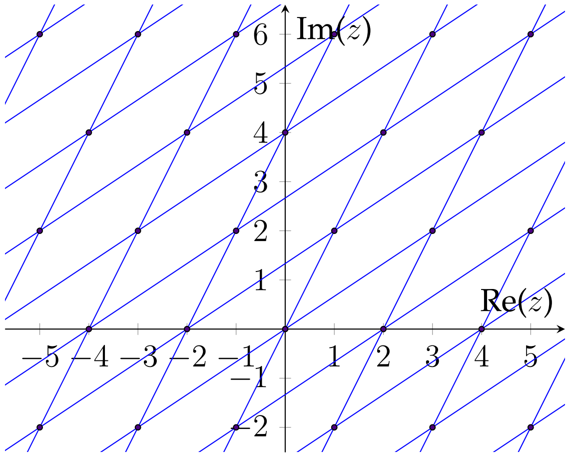
As demonstrações das proposições e dos teoremas desta seção serão omitidas, mas podem ser consultadas em [10] e [12].

Definição 6.9. Sejam $w_1 = u_1 + v_1 i$ e $w_2 = u_2 + v_2 i$ números complexos não nulos tais que os vetores (u_1, v_1) e (u_2, v_2) são linearmente independentes em $\mathbb{R}^2$, isto é, $(u_1, v_1) \neq \lambda(u_2, v_2)$ para qualquer $0 \neq \lambda \in \mathbb{R}$. Chamamos de retículado(do inglês, *lattice*) o conjunto:

$$L = \{mw_1 + nw_2 : m, n \in \mathbb{Z}\}.$$

O reticulado gerado por w_1 e w_2 é denotado por $\langle w_1, w_2 \rangle$. Também exigimos que a base do reticulado possua *orientação positiva*, isto é, $w_1/w_2 \in \mathbb{H} = \{a + bi \in \mathbb{C} : 0 < b\}$.

Exemplo 6.5. Abaixo temos os pontos do reticulado $\langle 1+2i, 3+2i\rangle$ no plano complexo:



Exemplo 6.6. Os inteiros de Gauss $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$ é um reticulado. De fato, temos que $a + bi = aw_1 + bw_2$ onde $w_1 = 1 \in \mathbb{C}$ e $w_2 = i \in \mathbb{C}$, daí temos que $\mathbb{Z}[i] = \langle 1, i\rangle$.

Definição 6.10. Seja L um reticulado gerado por $w_1, w_2 \in \mathbb{C}$. Definimos $\mathbb{C}/L$ pela relação de equivalência:

$$z_1 \equiv z_2 \mod L \iff z_1 - z_2 \in L.$$

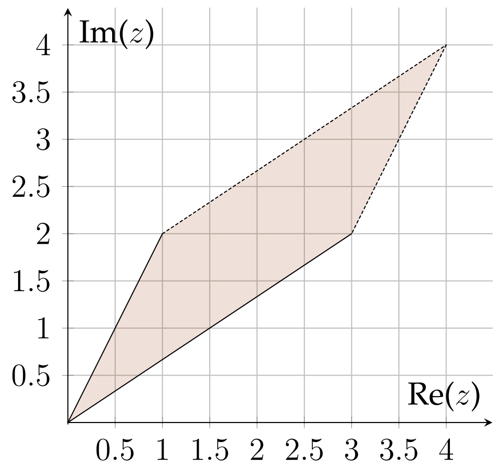
Então C/L é o conjunto das classes de equivalência de $\mathbb{C}$ módulo L.

Definição 6.11. Seja L um reticulado tal que $\langle w_1, w_2\rangle$. O *domínio fundamental* de $\mathbb{C}/L$ é o conjunto

$$\mathcal{F} := \{\lambda w_1 + \mu w_2; 0 \leq \lambda, \mu < 1\}.$$

$\mathcal{F}$ forma um paralelogramo no plano complexo.

Exemplo 6.7. O conjunto $\mathcal{F} = \{\lambda(1 + 2i) + \mu(3 + 2i); 0 \leq \lambda, \mu < 1\}$ é o domínio fundamental de $\mathbb{C}/\langle 1 + 2i, 3 + 2i\rangle$.



Proposição 6.1. *Sejam $L = \langle w_1, w_2 \rangle$ e $L' = \langle w_1', w_2' \rangle$ reticulados com $w_1/w_2, w_1'/w_2' \in \mathbb{H}$.*

1. *$L = L'$ se, e somente se, existe $M \in SL(2, \mathbb{Z})$ tal que $\left(\begin{smallmatrix} w_1' \\ w_2' \end{smallmatrix}\right) = M\left(\begin{smallmatrix} w_1 \\ w_2 \end{smallmatrix}\right)$.*

2. *Existe um isomorfismo complexo e analítico entre $\mathbb{C}/L$ e $\mathbb{C}/L'$ se, e somente se, $L' = \alpha L$ para algum $\alpha \in \mathbb{C}$.*

Corolário 6.1.1. *Sejam $L = \langle w_1, w_2 \rangle$ e $L' = \langle w_1', w_2' \rangle$ reticulados com $w_1/w_2, w_1'/w_2' \in \mathbb{H}$, tais que existe um isomorfismo complexo e analítico de grupos abelianos $\mathbb{C}/L \cong \mathbb{C}/L'$. Então existe um $a \in \mathbb{C}$ não nulo e $M \in \mathrm{SL}(2, \mathbb{Z})$ tais que $\left(\begin{smallmatrix} w_1' \\ w_2' \end{smallmatrix}\right) = \alpha M\left(\begin{smallmatrix} w_1 \\ w_2 \end{smallmatrix}\right)$.*

Proposição 6.2. *Seja $L = \langle w_1, w_2 \rangle$ um reticulado em $\mathbb{C}$.*

1. *Existe um $\tau \in \mathbb{H}$ tal que $\mathbb{C}/L \cong \mathbb{C}/\langle \tau, 1 \rangle$.*

2. *Sejam $\tau, \tau' \in \mathbb{H}$. Então $\mathbb{C}/\langle \tau, 1 \rangle \cong \mathbb{C}/\langle \tau', 1 \rangle$ se, e somente se, existem $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z})$ tal que:*

$$\tau' = M\tau = \frac{a\tau + b}{c\tau + d}.$$

Definição 6.12. Seja L um reticulado. A função $\wp$ de Weierstrass relativa a L é a função

$$\wp(z, L) = \frac{1}{z^2} + \sum_{0 \neq w \in L} \left(\frac{1}{(z-w)^2} + \frac{1}{w^2} \right).$$

Definição 6.13. Sejam $2 \leq k \in \mathbb{Z}$ e L um reticulado. A série de Eisenstein de L com comprimento $2k$ é a série

$$G_2k(L) = \sum_{0 \neq w \in L} \frac{1}{w^{2k}}.$$

Proposição 6.3. *Sejam L um reticulado e $\wp$ a função de Weierstrass relativa a L. Então temos que $\wp(z, L) = \wp(z + v, L)$ para todo $v \in L$.*

Comentário 6.4. Não estamos interessados, necessariamente, na convergência das séries, mas, a saber, $G_2k(L)$ é absolutamente convergente para todo $k > 1$ e $\wp(z, L)$ converge uniformemente em todo subconjunto compacto de $\mathbb{C} - L$.

Definição 6.14. A série de Laurent de uma função complexa $f(z)$ sobre um ponto a é uma série infinita da forma

$$f(z) = \sum_{n=1}^{\infty} \frac{b_n}{(z-a)^n} + \sum_{n=0}^{\infty} c_n (z-a)^n$$

onde b_n, c_n são coeficientes complexos. É possível combinar essas duas séries e obter

$$f(z) = \sum_{n=-\infty}^{\infty} a_n (z-a)^n$$

onde

$$a_n = \begin{cases} b_{-n}, & \text{se } n \leq -1 \\ c_n, & \text{se } n \geq 0 \end{cases}$$

A saber, além da configuração acima, $a_n \in \mathbb{C}$ é dado por uma integral de linha.

Teorema 6.3. *Seja L um reticulado.*

1. *A série de Laurent de $\wp(z, L)$ sobre $z = 0$ é dada por*

$$\wp(z, L) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2k+1) G_(2k+2)(L) z^{2k}.$$

2. *Seja $\wp'(z, L)$ a derivada de $\wp$ em z. Então para todo $z \in \mathbb{C} - L$, temos*

$$\left(\frac{\wp'(z, L)}{2} \right)^2 = \wp(z, L)^3 - 15 G_4(L) \wp(z, L) - 35 G_6(L).$$

Observação 6.5. O **Teorema 5.3** mostra que existe o mapa,

$$\phi : \mathbb{C}/L \to E_L(\mathbb{C}), \quad z \mod L \mapsto \left(\wp(z, L), \frac{\wp'(z, L)}{2}\right). \tag{6.3}$$

Comentário 6.5. Em outras palavras, temos que $(\wp(z, L), \wp'(z, L)/2)$ é um ponto em $E_L(\mathbb{C})$, onde $E_L(\mathbb{C}) : y^2 = x^3 - 15G_4(L)x - 35G_6(L)$.

Teorema 6.4 (Teorema da Uniformização)**.** *Seja L um reticulado.*

1. *A equação $y^2 = x^3 - 15G_4(L)x - 35G_6(L)$ é não-singular e define um curva elíptica. Além disso, a função $\phi : \mathbb{C}/L \to E_L(\mathbb{C})$ definida em (5.3) é complexa, analítica e um isomorfismo de grupo abeliano.*

2. *Seja $E/\mathbb{Q} : y^2 = x^3 + Ax + B$ uma curva elíptica. Então existe um reticulado $L \subset \mathbb{C}$ tal que $A = -15G_4(L), B = -35G_6(L)$ e $C/L \cong E(\mathbb{C})$ via ϕ.*

Comentário 6.6. O teorema acima diz que todo reticulado L determina um curva elíptica $E_L(\mathbb{C})$ e, reciprocamente, para toda curva $E(\mathbb{C})$ existe um reticulado L que produz E. Em outras palavras, $E(\mathbb{C}) \cong \mathbb{C}/L$. Agora, a **Proposição 5.2** diz que é possível encontrar um reticulado da forma $\langle \tau, 1 \rangle$ com $\tau \in \mathbb{H}$ tal que $E(\mathbb{C}) \cong \mathbb{C}/\langle \tau, 1 \rangle$. Mas a escolha de τ não é única, fato que segue, também, da **Proposição 5.2**. Assim, podemos visualizar um curva elíptica como um torus para um reticulado conveniente, pois cada lado do domínio fundamental $\mathcal{F}$ do reticulado L é identificado com o lado oposto módulo L.

Bibliografia

[1] Sônia Pitta COELHO and C Polcino Milies. Números: uma introdução à matemática. *São Paulo, EDUSP*, 2003.

[2] David A Cox. *Primes of the form x2+ ny2: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011.

[3] José Plínio de Oliveira Santos. *Introdução à teoria dos números*. Instituto de Matemática Pura e Aplicada, 1998.

[4] David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.

[5] Ralph Michael. Euclidean Rings Fecke. Euclidean rings, 1974.

[6] Adilson Gonçalves. *Introdução à álgebra*. Impa, 1979.

[7] Neal Koblitz. *A course in number theory and cryptography*, volume 114. Springer Science & Business Media, 1994.

[8] Álvaro Lozano-Robledo and Alvaro Lozano-Robledo. *Elliptic curves, modular forms, and their L-functions*. American Mathematical Society Providence, RI, 2011.

[9] FB MARTINEZ, CG MOREIRA, N SALDANHA, and Eduardo Tengan. Teoria dos números: um passeio com primos e outros números. *IMPA, Rio de Janeiro, 5ª edição*, 2018.

[10] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[11] Joseph H Silverman and John Torrence Tate. *Rational points on elliptic curves*, volume 9. Springer, 1992.

[12] Lawrence C Washington. *Elliptic curves: number theory and cryptography*. CRC press, 2008.