Estruturas Algébricas

Aula 4

Divisão Euclidiana

Abramo Hefez

2025

Os aneis que possuem uma divisão com resto pequeno, termos que vamos definir a seguir, possuem propriedades algébricas notáveis que exploraremos nas próximas aulas.

Divisão Euclidiana nos inteiros

A divisão nos inteiros nem sempre é exata. Poder efetuar a divisão de dois inteiros com resto pequeno é uma propriedade importante, responsável por propriedades algébricas notáveis que os inteiros possuem.

Lema(Propriedade Arquimediana) Dados dois inteiros a e b, com $b \neq 0$, existe $n \in \mathbb{Z}$ tal que $n \cdot b \geq a$.

Prova Como $b \neq 0$, temos que $|b| \geq 1$, logo

$$|b| \cdot |a| = |b \cdot a| \geq |a| \geq a.$$

Se $b > 0$, tome $n = |a|$ e se $b < 0$, tome $n = -|a|$, e o resultado decorre da desigualdade acima.

Teorema(Divisão Euclidiana) Dados inteiros d e D com $d \neq 0$, existem inteiros q e r tais que

$$D = d \cdot q + r \quad \text{e} \quad 0 \leq r < |d|.$$

Além disso, q e r são unicamente determinados pelas condições acima.

Prova Considere o conjunto

$$S = \{x \in \mathbb{N} \cup \{0\}\,;\ \ x = D - d \cdot n \text{ para algum } n \in \mathbb{Z}\}.$$

Esse conjunto é limitado inferiormente (por 0) e não vazio, pois, pela Propriedade Arquimediana dos inteiros, existe um inteiro m tal que $m \cdot (-d) \geq -D$. Portanto, $a = D - m \cdot d \in S$.

Pelo Princípio da Boa Ordem, segue-se que S possui um menor elemento r. Logo $r = D - d \cdot q$, para algum $q \in \mathbb{Z}$. É claro que $r \geq 0$, pois $r \in S$.

Vamos agora provar que $r < |d|$.

Suponha por absurdo que $r \geq |d|$, logo $r = |d| + s$ para algum inteiro s tal que $0 \leq s < r$.

Portanto,

$$D = d \cdot q + |d| + s = d(q \pm 1) + s,$$

e, consequentemente,

$$s = D - d \cdot (q \pm 1) \in S.$$

Como $s \in S$ e $s < r$, temos uma contradição, pois r era o menor elemento de S.

Para provar a unicidade, suponha que

$$D = d \cdot q_1 + r_1 = d \cdot q_2 + r_2\,,$$

com $0 \leq r_1 < |d|$ e $0 \leq r_2 < |d|$.

Logo $0 \leq r_1 < |d|$ e $-|d| < -r_2 \leq 0$ e, portanto,

$-|d| < r_1 - r_2 < |d|$, ou seja, $|r_1 - r_2| < |d|$.

Como

$$d(q_1 - q_2) = r_2 - r_1,$$

segue-se que

$$|d| \cdot |q_1 - q_2| = |r_2 - r_1| < |d|.$$

Isto só é possível se $q_1 = q_2$ e $r_2 = r_1$.

Portanto, o teorema nos garante que em $\mathbb{Z}$ é sempre possível efetuar a divisão de um número D por outro número $d \neq 0$ com resto pequeno. Os números D, d, q e r são chamados, respectivamente, de **dividendo**, **divisor**, **quociente** e **resto**.

Divisão Euclidiana nos polinômios

Vamos mostrar que é possível efetuar *de modo único* uma divisão com *resto controlado* em $A[x]$, sempre que o divisor tiver coeficiente líder invertível em A.

Recorde que se $f(x)$ e $g(x)$ em $A[x]$ e se existe $h(x) \in A[x]$ tal que $f(x) = g(x) \cdot h(x)$, dizemos que $f(x)$ é **múltiplo** de $g(x)$ ou que $g(x)$ **divide** $f(x)$.

É claro por esta definição que qualquer $f(x) \in A[x]$ divide 0.

Exemplo $x^2 - 2x + 2$ divide $x^4 + 4$ em $\mathbb{Z}[x]$, assim como $x^2 + 2x + 2$ divide $x^4 + 4$, conforme visto em exemplo anterior.

O seguinte resultado é uma consequência da propriedade multiplicativa do grau em $A[x]$.

Proposição Sejam A um anel, $f(x)$, $g(x) \in A[x]\backslash\{0\}$. Se $g(x)$ tem coeficiente líder invertível e divide $f(x)$, então $\mathrm{grau}(g(x)) \leqslant \mathrm{grau}(f(x))$.

Prova Como $g(x)$ divide $f(x)$ e ambos são não nulos, então existe $h(x) \in A[x]\backslash\{0\}$ tal que $f(x) = g(x)h(x)$. Pela propriedade multiplicativa do grau, temos

$$\begin{aligned} \mathrm{grau}(f(x)) &= \mathrm{grau}(g(x)h(x)) \\ &= \mathrm{grau}(g(x)) + \mathrm{grau}(h(x)) \geqslant \mathrm{grau}(g(x)). \end{aligned}$$

A divisão em $A[x]$, conhecida como **divisão euclidiana**, será apresentada no resultado a seguir.

Teorema(Divisão Euclidiana) Seja A um anel comutativo e sejam $f(x), g(x) \in A[x]$, com $g(x) \neq 0$ e coeficiente líder invertível em A. Então, existem $q(x)$ e $r(x)$ em $A[x]$, unicamente determinados, tais que

$$f(x) = g(x)q(x) + r(x),$$

onde $r(x) = 0$ ou $\mathrm{grau}(r(x)) < \mathrm{grau}(g(x))$.

Prova da existência Seja $g(x) = b_0 + b_1x + \cdots + b_mx^m$, com $b_m \in A^*$.

Se $f(x) = 0$, então tome $q(x) = r(x) = 0$.

Se $f(x) \neq 0$, podemos escrever $f(x) = a_0 + a_1x + \cdots + a_nx^n$, com $a_n \neq 0$.

Se $n < m$, então tome $q(x) = 0$ e $r(x) = f(x)$.

Podemos supor $n \geqslant m$. A demonstração é por indução sobre $n = \mathrm{grau}(f(x))$.

Se $n = 0$, então $0 = n \geqslant m = \mathrm{grau}(g(x))$, logo $m = 0$, $f(x) = a_0 \neq 0$, $g(x) = b_0$, com $b_0^{-1} \in A$.

Assim, $f(x) = g(x)a_0b_0^{-1}$, com $q(x) = a_0b_0^{-1}$ e $r(x) = 0$.

Suponhamos o resultado válido para polinômios com grau menor do que $n = \mathrm{grau}(f(x))$. Vamos mostrar que vale para $f(x)$.

Seja $f_1(x)$ o polinômio definido por $r_1(x) = f(x) - g(x)q_1(x)$, onde $q_1(x) = a_nb_m^{-1}x^{n-m}$. O polinômio $g(x)a_nb_m^{-1}x^{n-m}$ tem grau n e coeficiente líder a_n. Logo, $\mathrm{grau}(r_1(x)) < \mathrm{grau}(f(x))$. Por hipótese de indução, existem $q_2(x)$ e $r_2(x)$ em $A[x]$ tais que

$$r_1(x) = g(x)q_2(x) + r_2(x),$$

com $r_2(x) = 0$ ou $\mathrm{grau}(r_2(x)) < \mathrm{grau}(g(x))$.

Logo,

$$\begin{aligned} f(x) &= r_1(x) + g(x)a_nb_m^{-1}x^{m-n} \\ &= (g(x)q_2(x) + r_2(x)) + g(x)a_nb_m^{-1}x^{m-n} \\ &= g(x)(q_2(x) + a_nb_m^{-1}x^{m-n}) + r_2(x). \end{aligned}$$

Tomamos $q(x) = q_2(x) + a_nb_m^{-1}x^{m-n}$ e $r(x) = r_2(x)$.

Prova da unicidade Sejam $q_1(x), r_1(x), q_2(x), r_2(x)$ tais que

$$f(x) = g(x)q_1(x) + r_1(x) \overset{(1)}{=} g(x)q_2(x) + r_2(x), \text{ onde}$$

$$(2) \begin{cases} r_1(x) = 0 \text{ ou } \operatorname{grau}(r_1(x)) < \operatorname{grau}(g(x)) \text{ e} \\ r_2(x) = 0 \text{ ou } \operatorname{grau}(r_2(x)) < \operatorname{grau}(g(x)). \end{cases}$$

De (1), segue que $g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$.

Se $q_1(x) \neq q_2(x)$, então $r_2(x) - r_1(x) \neq 0$, logo obtemos

$$\operatorname{grau}(\underbrace{g(x)}_{\text{divisor}}) \leq \operatorname{grau}(r_2(x) - r_1(x)) \overset{(2)}{<} \operatorname{grau}(g(x)),$$

uma contradição.

Portanto, $q_1(x) = q_2(x)$, logo $r_1(x) = r_2(x)$.

Sejam $f(x), g(x), q(x)$ e $r(x)$ como no Teorema. Chamamos $f(x)$ de **dividendo**, $g(x)$ de **divisor**, $q(x)$ de **quociente** e $r(x)$ de **resto**.

Corolário Seja K um corpo. Dados $f(x), g(x) \in K[x]$, com $g(x) \neq 0$, existem $q(x)$ e $r(x)$ em $K[x]$, univocamente determinados, tais que

$$f(x) = g(x)q(x)+r(x), \text{ com } r(x) = 0, \text{ ou } \mathrm{grau}(r(x)) < \mathrm{grau}(g(x)).$$

Prova Basta aplicar o teorema, observando que em $K[x]$ todo polinômio não nulo tem coeficiente líder invertível.

Se o coeficiente líder do divisor não for invertível, a divisão com resto pode não ser possível. Por exemplo, não se pode dividir $x^2 + 1$ por $2x + 1$ em $\mathbb{Z}[x]$.

A determinação do monômio de maior grau do quociente só depende dos monômios de maior grau do dividendo e do divisor.

Na divisão de polinômios devemos prestar atenção nos graus do dividendo, do divisor e do resto. Agora vamos armar e efetuar a divisão, seguindo passo a passo a demonstração do Teorema.

Armamos e resolvemos a divisão seguindo o modelo

$$\begin{array}{r|l} f(x) & g(x) \\ \hline \vdots & \\ \hline r(x) & q(x) \end{array}$$

Exemplo Sejam $f(x) = 2x + 5$ e $g(x) = x^2 + 2x + 4$ em $\mathbb{Z}[x]$.

(Passo 1) Temos $\mathrm{grau}(f(x)) = 1 < 2 = \mathrm{grau}(g(x))$. Nada a fazer.

(Passo 2) O quociente é $q(x) = 0$ e o resto é $r(x) = f(x) = 2x + 5$.

$$\begin{array}{rcr|l} 2x & + & 5 & x^2 + 2x + 4 \\ & - & 0 & \hline 0 \\ \hline 2x & + & 5 & \end{array}$$

Exemplo Sejam $f(x) = 2x^2 + 3x + 3$ e $g(x) = x^2 + 2x + 2$ em $\mathbb{Q}[x]$.

(Passo 1) O monômio de maior grau de $f(x)$ é $2x^2$ e o monômio de maior grau de $g(x)$ é x^2. O quociente da divisão de $2x^2$ por x^2 é $q_1(x) = 2$.

(Passo 2) Fazemos o cálculo:
$r_1(x) = f(x) - q_1(x)g(x) = (2x^2 + 3x + 3) - 2x^2 - 4x - 4 = -x - 1$.

$$\begin{array}{rrrrrrr|rrrrrr} & 2x^2 & + & 3x & + & 3 & & x^2 & + & 2x & + & 2 \\ \cline{8-12} - & 2x^2 & - & 4x & - & 4 & & 2 & & & & \\ \cline{1-6} & & - & x & - & 1 & & & & & & \end{array}$$

(Passo 3) Como $1 = \text{grau}(r_1(x)) < \text{grau}(g(x)) = 2$, não podemos continuar a divisão. Paramos os cálculos.

(Passo 4) Obtemos $q(x) = q_1(x) = 2$ e $r(x) = r_1(x) = -x - 1$.

Exemplo Faremos a divisão euclidiana de $f(x) = 3x^4 + 5x^3 + 2x^2 + x - 3$ por $g(x) = x^2 + 2x + 1$ em $\mathbb{Z}[x]$.

(Passo 1) O monômio de maior grau de $f(x)$ é $3x^4$ e o monômio de maior grau de $g(x)$ é x^2. O quociente da divisão de $3x^4$ por x^2 é $q_1(x) = 3x^2$.

(Passo 2) Fazemos o cálculo:
$r_1(x) = f(x) - q_1(x)g(x) =$
$(3x^4 + 5x^3 + 2x^2 + x - 3) - 3x^4 - 6x^3 - 3x^2 = -x^3 - x^2 + x - 3.$

$$\begin{array}{rcrcrcrcr|l|l}
3x^4 & + & 5x^3 & + & 2x^2 & + & x & - & 3 & x^2 + 2x + 1 & \\
\cline{10-10}
-3x^4 & - & 6x^3 & - & 3x^2 & & & & & 3x^2 & \\
\cline{1-9}
 & - & x^3 & - & x^2 & + & x & - & 3 & & \\
\end{array}$$

(Passo 3) Como $3 = \mathrm{grau}(r_1(x)) > \mathrm{grau}(g(x)) = 2$ devemos continuar, dividindo $r_1(x)$ por $g(x)$, pois $r_1(x)$ não é o resto da divisão euclidiana.

(Passo 4) O monômio de maior grau de $r_1(x)$ é $-x^3$ e o monômio de maior grau de $g(x)$ é x^2. O quociente da divisão de $-x^3$ por x^2 é $q_2(x) = -x$.

(Passo 5) Fazemos o cálculo:
$r_2(x) = r_1(x) - q_2(x)g(x) = (-x^3 - x^2 + x - 3) + x^3 + 2x^2 + x = x^2 + 2x - 3$.

$$
\begin{array}{rcrcrcrcr|l}
3x^4 & + & 5x^3 & + & x^2 & + & x & - & 3 & x^2 + 2x + 1 \\
\cline{10-10}
-3x^4 & - & 6x^3 & - & 3x^2 & & & & & 3x^2 - x \\
\cline{1-9}
 & - & x^3 & - & x^2 & + & x & - & 3 & \\
 & & x^3 & + & 2x^2 & + & x & & & \\
\cline{3-9}
 & & & & x^2 & + & 2x & - & 3 &
\end{array}
$$

(Passo 6) Como $2 = \mathrm{grau}(r_2(x)) = \mathrm{grau}(g(x)) = 2$, podemos continuar, calculando a divisão de $r_2(x)$ por $g(x)$, pois $r_2(x)$ não é o resto da divisão euclidiana.

(Passo 7) O monômio de maior grau de $r_2(x)$ é x^2 e o monômio de maior grau de $g(x)$ é x^2. O quociente da divisão de x^2 por x^2 é $q_3(x) = 1$.

(Passo 8) Fazemos o cálculo:

$r_3(x) = r_2(x) - q_3(x)g(x) = (x^2 + 2x - 3) - x^2 - 2x - 1 = -4.$

$$
\begin{array}{rcrcrcrcr|l}
3x^4 & + & 5x^3 & + & 2x^2 & + & x & - & 3 & x^2 + 2x + 1 \\
\cline{10-10}
-3x^4 & - & 6x^3 & - & 3x^2 & & & & & 3x^2 - x + 1 \\
\cline{1-9}
 & - & x^3 & - & x^2 & + & x & - & 3 & \\
 & & x^3 & + & 2x^2 & + & x & & & \\
\cline{2-8}
 & & & & x^2 & + & 2x & - & 3 & \\
 & & & - & x^2 & - & 2x & - & 1 & \\
\cline{4-9}
 & & & & & & & - & 4 &
\end{array}
$$

(Passo 9) Como $0 = \mathrm{grau}(r_3(x)) < \mathrm{grau}(g(x)) = 2$, terminamos o algoritmo, pois $r_3(x)$ é o resto da divisão euclidiana.

(Passo 10) Obtemos
$q(x) = 3x^2 - x + 1 = q_1(x) + q_2(x) + q_3(x)$ e $r(x) = r_3(x) = -4$.

Domínios Euclidianos

Um **domínio euclidiano** é um domínio $(D, +, \cdot)$ no qual está definida uma função

$$\varphi \colon D \setminus \{0\} \to \mathbb{N} \cup \{0\},$$

satisfazendo a:

i) Para todos $a, b \in D$ com $b \neq 0$, existem $q, r \in D$ tais que

$$a = qb + r \quad \text{com} \quad \begin{cases} r = 0, \text{ ou} \\ \varphi(r) < \varphi(b) \end{cases}$$

ii) Para todos $a, b \in D \setminus \{0\}$, $\varphi(a) \leq \varphi(ab)$.

Um domínio euclidiano será denotado por $(D, +, \cdot, \varphi)$.

Portanto, conforme vimos nas aulas anteriores, temos que $(\mathbb{Z}, +, \cdot, |\ \ |)$ e $(K[x], +, \cdot, \mathrm{grau})$ são domínios euclidianos.

Outros exemplos de domínios euclidianos são dados por $(K, +, \cdot, 0)$, onde $(K, +, \cdot)$ é um corpo e φ é a função constante igual a zero.

Além de $\mathbb{Z}$, de $K[x]$ e de um corpo K, existem inúmeros anéis euclidianos, vários relacionados com a Teoria dos Números. O exemplo que damos a seguir é um dos mais emblemáticos.

Proposição O domínio $(\mathbb{Z}[i], +, \cdot, N)$ dos inteiros Gaussiano, junto com a função norma é um domínio euclidiano.

Prova Vimos anteriormente que a função norma satisfaz a propriedade (ii) da definição de domínio euclidiano.

O resultado estará provado se mostrarmos a seguinte afirmação: Dados $\alpha, \beta \in \mathbb{Z}[i]$ com $\beta \neq 0$, existem $q, \rho \in \mathbb{Z}[i]$ tais que

$$\alpha = \beta q + \rho, \quad \text{com} \quad N(\rho) < N(\beta).$$

Trata-se portanto de achar um inteiro Gaussiano q tal que

$$N(\alpha - \beta q) < N(\beta).$$

Como

$$N(\alpha - \beta q) = N(\beta) N(\alpha/\beta - q), \tag{1}$$

onde $\alpha/\beta \in \mathbb{Q}(i)$, devemos então achar q tal que $N(\alpha/\beta - q) < 1$.

Escrevamos $\alpha/\beta = a + bi$, com $a, b \in \mathbb{Q}$, e sejam r e s inteiros tais que

$$|a - r| \leq 1/2 \quad \text{e} \quad |b - s| \leq 1/2. \tag{2}$$

Observe que tais pares de inteiros r e s existem e são em número de 1, 2 ou 4.
Tome $q = r + si$, onde (r, s) é uma solução de (2) e ponha $\rho = \alpha - \beta q$. Logo, de (1) e (2), temos que

$$\begin{aligned} N(\rho) &= N(\beta) \cdot N(\alpha/\beta - q) = N(\beta) \cdot N(a - r + (b - s)i) \\ &= N(\beta)\left[(a - r)^2 + (b - s)^2\right] \leq N(\beta)[1/4 + 1/4] \\ &= \frac{1}{2} N(\beta) < N(\beta). \end{aligned}$$

□

Damos a seguir um exemplo em que há quatro soluções para os pares (q, ρ).

Tome $\alpha = 4 + 5i$ e $\beta = 1 + i$, logo

$$\alpha/\beta = a + bi = (9 + i)/2.$$

Portanto, r e s devem satisfazer

$$|9/2 - r| \leq 1/2 \quad \text{e} \quad |1/2 - s| \leq 1/2.$$

Então $r \in \{4, 5\}$ e $s \in \{0, 1\}$.

Portanto, são as seguintes as soluções para os pares (q, ρ):

$$(4, i), \quad (4 + i, 1), \quad (5, -1) \quad (5 + i, -i).$$

Em domínios euclidianos, as unidades se comportam de modo bem particular com relação à função φ, como podemos ver no que se segue

Lema Seja $(D, +, \cdot, \varphi)$ um domínio euclidiano. Para $u \in D \setminus \{0\}$, são equivalentes as seguintes afirmações:

i) Existe $a \in D \setminus \{0\}$ tal que $\varphi(ua) = \varphi(a)$;

ii) $u \in D^*$;

iii) $\forall a \in D \setminus \{0\}$, tem-se que $\varphi(ua) = \varphi(a)$.

Prova *i*) $\Rightarrow$ *ii*) Dividindo a por ua, temos

$$a = uaq + r, \quad \text{com} \quad r = 0 \quad \text{ou} \quad \varphi(r) < \varphi(ua).$$

Mostremos que $r = 0$. De fato, se $r \neq 0$, então $r = a(1 - uq)$, logo

$$\varphi(r) = \varphi(a(1 - uq)) \geq \varphi(a) = \varphi(ua),$$

o que é uma contradição. Logo, $a = uaq$ e cancelando $a \neq 0$, temos que $uq = 1$ e, consequentemente, $u \in D^*$.

ii) $\Rightarrow$ *iii*) Suponha que $u \in D^*$, logo

$$\forall a \in D \setminus \{0\}, \ \varphi(a) \leq \varphi(ua) \leq \varphi(u^{-1}au) = \varphi(a).$$

logo $\varphi(ua) = \varphi(a)$.

iii) $\Rightarrow$ *i*) Óbvio. $\square$

Corolário Em um domínio euclidiano, temos que

$$u \in D^* \iff \varphi(u) = \varphi(1).$$

Prova Suponha $u \in D^*$, logo por $ii) \Rightarrow iii)$ temos que $\varphi(u) = \varphi(u \cdot 1) = \varphi(1)$.

Inversamente, se $\varphi(u) = \varphi(1)$, por $i) \Rightarrow ii)$ temos que $u \in D^*$.

□

Note que se tem $\varphi(1) = \min\{\varphi(a);\ a \in D \setminus \{0\}\}$.

Os Anéis de Kummer

Kummer estudou os anéis da forma

$$D = \mathbb{Z}[\sqrt{\delta}] = \{a + b\sqrt{\delta};\ a, b \in \mathbb{Z}\},$$

com $\delta \in \mathbb{Z} \setminus \{0, 1\}$ e livre de quadrados.

É um exercício mostrar que o corpo de frações deste anel é

$$\mathbb{Q}(\sqrt{\delta}) = \{x + y\sqrt{\delta};\ x, y \in \mathbb{Q}\}.$$

Em $\mathbb{Z}[\sqrt{\delta}]$ definimos a função *norma absoluta* dada por

$$\begin{array}{rccc} N: & D & \to & \mathbb{N} \cup \{0\} \\ & a + b\sqrt{\delta} & \mapsto & |a^2 - \delta b^2| \end{array}$$

Note que se $\delta < 0$, então $N(a + b\sqrt{\delta}) = a^2 - \delta b^2 \geq 0$.

Além disso, para todo $\delta \in \mathbb{Z} \setminus \{0, 1\}$ e livre de quadrados,

$$N(a + b\sqrt{\delta}) = 0 \iff a = b = 0.$$

Isto é claro se $\delta < 0$ e segue para $\delta > 0$ pelo fato de δ ser livre de quadrados.

Lema É um homomorfismo de anéis a função

$$\begin{array}{rccc} h\colon & D & \to & D. \\ & a+b\sqrt{\delta} & \mapsto & a-b\sqrt{\delta} \end{array}$$

Prova A única propriedade não trivial a ser provada é que h é multiplicativa.

De fato,

$$\begin{aligned} h((a+b\sqrt{\delta})(c+d\sqrt{\delta})) &= h(ac+bd\delta+(ad+bc)\sqrt{\delta}) \\ &= ac+\delta bd-(ad+bc)\sqrt{\delta} \\ &= (a-b\sqrt{\delta})(c-d\sqrt{\delta}) \\ &= h(a+b\sqrt{\delta})h(c+d\sqrt{\delta}). \end{aligned}$$

Proposição A função norma absoluta N de $D=\mathbb{Z}[\sqrt{\delta}]$ é multiplicativa.

Prova De fato, para todo $z\in D$, tem-se que $N(z)=|zh(z)|$. Sejam $z,z'\in D$, logo

$$N(zz')=|zz'h(zz')|=|zh(z)z'h(z')|=|zh(z)|\,|z'h(z')|=N(z)N(z').$$

Note que da proposição acima, temos que, se $z' \neq 0$ e z é qualquer, como $N(z') \geq 1$, segue-se que $N(zz') = N(z)N(z') \geq N(z)$.

Lema Em $D = \mathbb{Z}[\sqrt{\delta}]$ tem-se que u é uma unidade se, e somente se, $N(u) = 1$.

Prova De fato, se u é uma unidade, então

$$1 = N(1) = N(uu^{-1}) \geq N(u).$$

Como $N(u) \geq 1$, temos que $N(u) = 1$.

Reciprocamente, se $u = a + b\sqrt{\delta}$, então $N(u) = 1$ implica que $(a + b\sqrt{\delta})(a - b\sqrt{\delta}) = \pm 1$, o que implica que u é invertível.

Proposição Se $D = \mathbb{Z}[\sqrt{\delta}]$, com $\delta < 0$, então

i) $D^* = \{\pm 1, \pm i\}$, se $\delta = -1$;

ii) $D^* = \{\pm 1\}$, se $\delta < -1$.

Prova (i) Suponha que $\delta = -1$. Temos que $a + b\sqrt{-1}$ é invertível se, e somente se,

$$1 = N(a + b\sqrt{-1}) = (a^2 + b^2),$$

cujas soluções são $a = \pm 1$, $b = 0$ ou $a = 0$ e $b = \pm 1$, o que prova a proposição neste caso.

(ii) Suponha $\delta < -1$, logo $1 = N(a + b\sqrt{\delta}) = (a^2 + |\delta|b^2)$, cujas únicas soluções são $a = \pm 1$ e $b = 0$.

Quando $\delta > 1$, a situação é bem diferente, podendo $\mathbb{Z}[\sqrt{\delta}]^*$ ser infinito, como pode se ver no exemplo a seguir.

Exemplo As unidades de $D = \mathbb{Z}[\sqrt{2}]$.

Note que $N(1 \pm \sqrt{2}) = |1^2 - 2 \cdot (\pm 1)^2| = 1$, logo $1 \pm \sqrt{2}$ são unidades. Note também que $(1 + \sqrt{2})^{-1} = 1 - \sqrt{2}$. Isso nos fornece as seguintes unidades de D:

As potências com expoentes inteiros de $1 + \sqrt{2}$ e os seus simétricos.

Vamos mostrar que essas são todas as unidades de D. Seja u uma unidade de $\mathbb{Z}[\sqrt{2}]$. Como u, $1/u$, $-u$ e $-1/u$ são também unidades, podemos supor que $u > 1$ e depois tomar $\pm u$ e $\pm 1/u$.

Como a sequência $(1 + \sqrt{2})^k$ para $k \geq 0$ é crescente e ilimitada, existe um $n \geq 1$ tal que

$$(1 + \sqrt{2})^n \leq u < (1 + \sqrt{2})^{n+1},$$

logo

$$1 \leq u(1+\sqrt{2})^{-n} < 1+\sqrt{2}.$$

Como $u(1+\sqrt{2})^{-n}$ é uma unidade e $1+\sqrt{2}$ é a menor unidade maior do que 1, devemos ter que $u(1+\sqrt{2})^{-n} = 1$, ou seja, $u = (1+\sqrt{2})^n$ para algum $n \geq 1$.

Usando o mesmo argumento que foi usado na prova de que $\mathbb{Z}[i]$ é um domínio euclidiano, mostra-se que o anel $\mathbb{Z}[\sqrt{\delta}]$ é um domínio euclidiano com a norma absoluta se, e somente se, dados $a, b \in \mathbb{Q}$, existem $r, s \in \mathbb{Z}$ tais que

$$N(a-r+\delta(b-s)) = |(a-r)^2 - \delta(b-s)^2| < 1.$$

Como aplicação temos que $\mathbb{Z}[\sqrt{2}]$ e $\mathbb{Z}[\sqrt{-2}]$ são euclidianos com a norma absoluta, pois tomando $r, s \in \mathbb{Z}$ tais que $|a-r| \leq 1/2$ e $|b-s| \leq 1/2$, pela desigualdade triangular, temos que

$$\begin{aligned} N((a-r)+(b-s)\sqrt{\pm 2}) &= |(a-r)^2 \mp 2(b-s)^2| \\ &\leq (a-r)^2 + 2(b-s)^2 \\ &\leq 1/4 + 2(1/4) = 3/4 < 1. \end{aligned} \tag{3}$$

Observação Prova-se que $\mathbb{Z}[\sqrt{3}]$ é um domínio euclidiano com a norma absoluta, tomando r e s inteiros tais que $|a-r| \leq 1/2$ e $|b-s| \leq 1/2$ e substituindo (3) pela seguinte desigualdade:

$$\begin{aligned} N((a-r)+(b-s)\sqrt{3}) &= |(a-r)^2 - 3(b-s)^2| \\ &\leq \max\{(a-r)^2, 3(b-s)^2\} \\ &\leq \max\{1/4, 3/4\} < 1. \end{aligned}$$

Note que esse argumento não funciona para $\mathbb{Z}[\sqrt{-3}]$.

FIM DA AULA 4