LECTURE 11
Euklidean and principal ideal domains

PAVEL RŮŽIČKA

Abstract. We study the relationship between divisibility in commutative domains and the ordering of their principal ideals. We define the notion of a principal ideal domain and we prove that greatest common divisors and least common multiples exist in principal ideal domains. We defined Euclidean domains and we prove that Euclidean domains are principal ideal domains. Finally we study the ring $\mathbb{Z}[i]$ of Gaussian integers and we prove that $\mathbb{Z}[i]$ is an Euclidean domain.

We restrict ourselves to commutative rings.

11.1. **Divisibility and ideals.** Ideals of a ring $\boldsymbol{R}$ are closed under arbitrary intersections. It follows that each subset $X \subseteq R$ possesses a least ideal containing X, namely the intersection of all ideals containing X. The ideal will be denoted by $(\boldsymbol{X})$ and call the *ideal generated* by the set X. Conversely, if $\boldsymbol{I}$ is an ideal of the ring $\boldsymbol{R}$ and $X \subseteq I$ is such that $\boldsymbol{I} = (\boldsymbol{X})$, then the set X is called the *set of generators of* (the ideal) $\boldsymbol{I}$.

An ideal generated by a single element is called *principal*. That is, a principal ideal is an ideal of the form $(\boldsymbol{a})$ for some $a \in \boldsymbol{R}$. It is straightforward to see that

$$(\boldsymbol{a}) = \{r \cdot a \mid r \in R\} = \{b \in R \mid a \mid b\},$$

i.e, the principal ideal $(\boldsymbol{a})$ consists of all elements of $\boldsymbol{R}$ that are divisible by the element a. It readily follows that

$$(\boldsymbol{a}) \subseteq (\boldsymbol{b}) \iff b \mid a, \tag{11.1}$$

and, consequently, $(\boldsymbol{a}) = (\boldsymbol{b})$ if and only if $a \sim b$.

Ideals of the ring $\boldsymbol{R}$ are ordered by inclusion. The greatest ideal contained in ideals $\boldsymbol{I}$, $\boldsymbol{J}$ is clearly the intersection $\boldsymbol{I} \cap \boldsymbol{J}$. The least ideal containing $\boldsymbol{I}$, $\boldsymbol{J}$ is

$$\boldsymbol{I} + \boldsymbol{J} := \{a + b \mid a \in I, b \in J\}.$$

It is straightforward from the definition that $\boldsymbol{I} + \boldsymbol{J}$ is an ideal. On the other hand, every ideal containing both $\boldsymbol{I}$ and $\boldsymbol{J}$, being closed under addition, contains $\boldsymbol{I} + \boldsymbol{J}$ as well.

The Lecture and the tutorial took place in Malá strana, room S11, on December 18, 2018.

11.2. **Principal ideal domains.** A ring $\boldsymbol{R}$ is an *integral domain* if

$$a \cdot b = 0 \implies a = 0 \text{ or } b = 0,$$

i.e., an integral domain is a commutative ring with no non-zero divisors of 0. A *principal ideal domain* (shortly *p.i.d.*) is an integral domain whose every ideal is principal.

Lemma 11.1. *Every pair of elements of a principal ideal domain has a greatest common divisor.*

Proof. Let $\boldsymbol{R}$ be a principal ideal domain and $a, b \in R$. The ideal $(\boldsymbol{a}) + (\boldsymbol{b})$ is principal, hence generated by some $d \in R$. Since $(\boldsymbol{d}) = (\boldsymbol{a}) + (\boldsymbol{b}) \supseteq (\boldsymbol{a})$, it follows from (11.1) that $d \mid a$. Similarly we get that $d \mid b$, and so d is a common divisor of a and b.

Let c be a common divisor of a, b. Again, by (11.1), we have that $(\boldsymbol{a}) \subseteq (\boldsymbol{c})$ and $(\boldsymbol{b}) \subseteq (\boldsymbol{c})$. It follows that $(\boldsymbol{a}) + (\boldsymbol{b}) \subseteq (\boldsymbol{c})$, hence $(\boldsymbol{d}) \subseteq (\boldsymbol{c})$, whence $c \mid d$, due to (11.1). We conclude that d is the greatest common divisor of a and b. □

Observe that, in the situation of the proof of Lemma 11.1, all generators of the ideal $(\boldsymbol{a}) + (\boldsymbol{b})$ form a block of $\sim$, corresponding to (a, b). Applying Theorem 11.12 we conclude that

Corollary 11.2. *Every irreducible element of a principal ideal domain is prime.*

Lemma 11.3. *Let $\boldsymbol{R}$ be a principal ideal domain. Let $a, b \in R$ and $d \in (a, b)$. Then there are $r, s \in R$ such that*

$$d = r \cdot a + s \cdot b. \tag{11.1}$$

Proof. It follows from $(\boldsymbol{d}) = (\boldsymbol{a}) + (\boldsymbol{b})$ that

$$d \in (\boldsymbol{a}) + (\boldsymbol{b}) = \{r \cdot a + s \cdot b \mid r, s \in R\}.$$

□

Lemma 11.3 states that in principal ideal domains, greatest common divisors are expressed as linear combinations of the elements. Equality (11.1) is called *Bézouts identity*.

11.3. **Euclidean domains.** Let $\boldsymbol{R}$ be an integral domain. An *Euclidean norm* on $\boldsymbol{R}$ is a map $N \colon \boldsymbol{R} \setminus \{0\} \to \mathbb{N}_0$ such that for all $a, b \in R$, $b \neq 0$, there are $c, r \in R$ such that

(i) $a = b \cdot c + r$,
(ii) $r = 0$ or $N(r) < N(b)$.

An *Euclidean domain* is a domain having an Euclidean norm.

Lemma 11.4. *Every Euclidean domain is a principal ideal domain.*

Proof. Let $\boldsymbol{R}$ be an Euclidean domain with an Euclidean norm $N\colon R\backslash\{0\} \to \mathbb{N}_0$ and $\boldsymbol{I}$ an ideal of $\boldsymbol{R}$. If $\boldsymbol{I} = \boldsymbol{(0)}$, then $\boldsymbol{I}$ is principal. Suppose that $\boldsymbol{I}$ contains a non-zero element and pick a non-zero $b \in I$ with $N(b)$ smallest possible. Then clearly $\boldsymbol{(b)} \subseteq \boldsymbol{I}$. We prove that the equality holds true. Suppose that there is $a \in \boldsymbol{I} \setminus \boldsymbol{(b)}$. Since $\boldsymbol{R}$ is an Euclidean domain, there are $c, r \in R$ such that $a = b \cdot c + r$ and $r = 0$ or $N(r) < N(b)$. Since $a \notin \boldsymbol{(b)}$, we have that $r \neq 0$, and so $N(r) < N(b)$. Since $r = a - b \cdot c$, we have that $r \in I$. This contradicts the choice of b with $N(b)$ smallest possible in I. □

Observe that common divisors of a and b corresponds to common divisors of a and r. We can thus compute the greatest common divisor of a, b using the *Euclidean algorithm*:

Euclidan algorithm: Compute the greates common divisor

```
procedure GCD
input elements $a, b$
loop A:
  until $b = 0$ do
  find $c, r$ such that $a = b \cdot c + r$ and $r = 0$ or $N(r) < N(b)$
  a := b
  b := r
  goto loop A
return a
```

Example 11.5. *For an integer a put $N(a) = |a|$; the absolute value of a. The ring $\boldsymbol{Z}$ of all integers is an Euclidean domain with the Euclidean norm $N\colon \mathbb{Z} \setminus \{0\} \to \mathbb{N}$. Observe that the Euclidean norm is multiplicative, i.e, $N(a \cdot b) = N(a) \cdot N(b)$, for all $a, b \in \mathbb{Z} \setminus \{0\}$.*

Let $\boldsymbol{F}$ be a field and $\boldsymbol{F}[x]$ the ring of all polynomials with coefficients in $\boldsymbol{T}$. For a polynomial $f(x) = a_n \cdot x^n + \cdots + a_1 \cdot x + a_0$, with $a_n \neq 0$, put $N(f) = n$ be the degree of f. It is well known that $N\colon \boldsymbol{F}[x] \setminus \{0\} \to \mathbb{N}_0$ is an Euclidean norm on $\boldsymbol{F}[x]$. In this case however the Euclidean norm is not multiplicative. Instead we have that $N(f \cdot g) = N(f) + N(g)$ for every pair of non-zero polynomials f, g.

11.4. **Gaussian integers.** Put

$$\boldsymbol{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}\},$$

and observe that $\boldsymbol{Z}[i]$ is a subring of the field $\boldsymbol{C}$ of all complex numbers. Indeed $(a + ib) - (c + id) = (a - c) + i(b - d) \in \boldsymbol{Z}[i]$ and $(a + ib) \cdot (c + id) = (a \cdot c - b \cdot d) + i(a \cdot d + b \cdot c) \in \boldsymbol{Z}[i]$. Elements of the ring $\boldsymbol{Z}[i]$ are called *Gaussian integers*.

Let $\xi = x + iy$ be a complex number. We denote by $\overline{\xi} := x - iy$ the conjugate of ξ and we put

$$N(\xi) := \xi \cdot \overline{\xi} = (x + iy) \cdot (x - iy) = x^2 + y^2.$$

Thus $N(\xi)$ is the square of the *complex norm* of ξ. Observe that

$$N(\xi\cdot\eta) = (\xi\cdot\eta)\cdot\overline{(\xi\cdot\eta)} = \xi\cdot\eta\cdot\overline{\xi}\cdot\overline{\eta} = N(\xi)\cdot N(\eta). \tag{11.1}$$

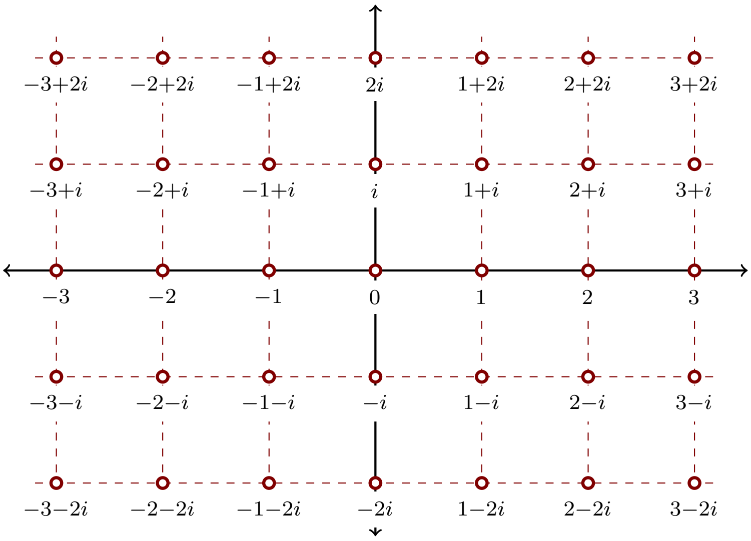

FIGURE 1. The ring $\boldsymbol{Z}[i]$

Lemma 11.6. *The restiction $N\restriction(\boldsymbol{Z}[i]\setminus\{0\})\colon \boldsymbol{Z}[i]\setminus\{0\}\to\mathbb{N}$ is an Euclidean norm on the ring $\boldsymbol{Z}[i]$ of Gaussian integers.*

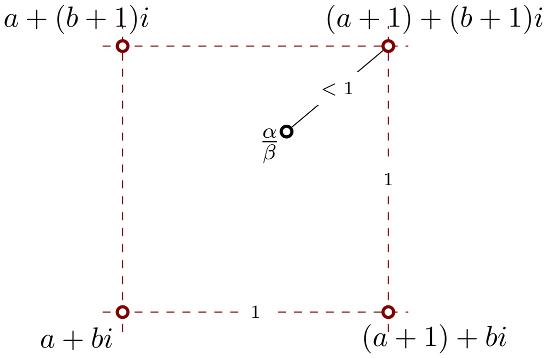

FIGURE 2. Fouding γ

Proof. Let $\alpha,\beta\in\boldsymbol{Z}[i]$ be such that $\beta\neq 0$. We are looking for $\gamma,\rho\in\boldsymbol{Z}[i]$ such that $\alpha=\beta\cdot\gamma+\rho$ and either $\rho=0$ or $N(\rho)<N(\beta)$.

Elements of the ring $\boldsymbol{Z}[i]$ form a lattice in the complex plane (see Figure 1). The lattice consists of squares with sides of size 1. Since $\beta\neq 0$, we can form the complex fraction $\frac{\alpha}{\beta}$. The fraction lies inside a square of the lattice. Since the side of the square has length 1, there is a vertex γ of the square (not necessarily unigue) such that $|\frac{\alpha}{\beta} - \gamma| < 1$ (see Figure 2). It follows that

$$N(\frac{\alpha}{\beta} - \gamma) = |\frac{\alpha}{\beta} - \gamma|^2 < 1. \tag{11.2}$$

We set $\rho = \alpha - \beta \cdot \gamma$. It follows from (11.1) and (11.2) that

$$N(\rho) = N((\frac{\alpha}{\beta} - \gamma) \cdot \beta) = N(\frac{\alpha}{\beta} - \gamma) \cdot N(\beta) < N(\beta).$$

□

Exercises

Exercise 11.1. *Let $\boldsymbol{R}$ be a ring and $\boldsymbol{I}$ a proper ideal of $\boldsymbol{R}$. Prove that*

(i) *$\boldsymbol{I}$ is a prime ideal if and only if the factor-ring $\boldsymbol{R} \,/\, \boldsymbol{I}$ is an integral domain.;*

(ii) *the ideal $\boldsymbol{I}$ is maximal if and only if the factor ring $\boldsymbol{R} \,/\, \boldsymbol{I}$ is a field.*

Exercise 11.2. *List all ideals of the rings $\mathbb{Z}$and $\mathbb{Z}_{p^n}$ where p is a prime and n is a positive integer.*

Exercise 11.3. *Decide, whether there is a multiplicative Euclidean norm on the ring $\boldsymbol{F}[x]$ of all polynomials with coefficients in a field $\boldsymbol{F}$.*

For a ring $\boldsymbol{R}$ let $\boldsymbol{R}^*$ denote the multiplicative group of all invertible elements of $\boldsymbol{R}$.

Exercise 11.4. *Prove that*

(i) $\mathbb{Z}^* = \{1, -1\}$*;*

(ii) $\mathbb{Z}_n^* = \{i \in \mathbb{Z}_n \mid (i, n) = 1\}$ *for every* $n \in \mathbb{N}$*;*

(iii) $\boldsymbol{R}[x] = \boldsymbol{R}$ *for every ring* $\boldsymbol{R}$.

Exercise 11.5. *Prove that $\alpha \in \mathbb{Z}[i]^*$ if and only if $N(\alpha) = 1$. List all elements of $\mathbb{Z}[i]^*$.*