LECTURE 10
Rings, ideals, and divisibility

PAVEL RŮŽIČKA

Abstract. We define rings and we show some examples. Namely the examples of the ring of integers, fields, and the constructions of polynomial and matrix rings. We introduce the notion of an ideal of a ring. We prove that ideals correspond to kernels of ring homomorphisms. Finally we study divisibility in commutative cancellative monoids.

10.1. **Rings.** A *ring* $\boldsymbol{R}$ consists of a set, R, and a pair of binary operations $+$ and $\cdot$ respectively of addition and multiplication such that

(i) $(R,+)$ is an Abelian group,
(ii) $(R,\cdot)$ is a monoid,
(iii) the *distributive law* holds true, that is,

$$(a+b)\cdot c = a\cdot c + b\cdot c \quad \text{and} \quad c\cdot(a+b) = c\cdot a + c\cdot b,$$

for all $a,b,c\in R$.

The unit of the Abelian group $(R,+)$ is usually denoted by 0 and called the zero of the ring $\boldsymbol{R}$ while the unit of the monoid $(R,\cdot)$ is usually denote by 1 and it is called the unit of $\boldsymbol{R}$. We will often write $a-b$ instead of $a+(-b)$.

A ring $\boldsymbol{R}$ is *commutative* provided that

$$a\cdot b = b\cdot a,$$

for all $a,b\in R$, i.e, the monoid $(R,\cdot)$ is commutative.

A commutative ring $\boldsymbol{F}=(F,+,\cdot)$ such that $(F\setminus\{0\},\cdot)$ is an (Abelian) group is called a *field*, i.e, a field is a commutative ring whose every non-zero element has a multiplicative inverse.

Example 10.1. *Let us recall some well known examples of fields.*

1. *The sets of all rational, real, or complex numbers respectively form fields that are usually denoted by* $\boldsymbol{Q}$, $\boldsymbol{R}$, *and* $\boldsymbol{C}$.
2. *For each prime number* p, *the set* $\mathbb{Z}_p=\{0,1,\dots,p-1\}$ *with the operations* $+_p$ *and* $\cdot_p$ *of addition and multiplication modulo* p, *respectively, is an example of a finite field. We will denote this field by* $\boldsymbol{Z}_p$.

The Lecture and the tutorial took place in Malá strana, room S11, on December 11, 2018.

Example 10.2. *Let us list a few examples of rings:*

1. *The ring* $\boldsymbol{Z} = (\mathbb{Z}, +, \cdot)$ *of all integers.*
2. *Let* $\boldsymbol{F}$ *be a field. All polynomials in a single variable* x *with coeficients from the field* $\boldsymbol{F}$ *form a ring which we denote by* $\boldsymbol{F}[x]$.
3. *Let* $\boldsymbol{F}$ *be a field and* n *a positive integer. All* $n \times n$ *matrices with entries from* $\boldsymbol{F}$ *form a ring. We will denote this ring by* $\boldsymbol{M}_n(\boldsymbol{F})$.

10.2. **Ideals and factor-rings.** An *ideal* of a ring $\boldsymbol{R} = (R, +, \cdot)$ is a subset $I \subseteq R$ such that

(i) $a, b \in I \implies a + b \in I$,
(ii) $b \in I \implies a \cdot b \cdot c \in I$,

for all $a, b, c \in R$.

Observe that $(I, +)$ is a subgroup of the Abelian group $(R, +)$, indeed, if $a \in I$, then $-a = (-1) \cdot a \in I$, due to (ii). We can form a factor-group $\boldsymbol{R/I}$, elements of the factor-group are cosets, $a + I$, of I.

Let $a, b \in R$. We have that

$$(a + I) \cdot (b + I) = a \cdot b + a \cdot I + I \cdot b + I \cdot I \subseteq a \cdot b + I.$$

And so $\boldsymbol{R/I}$ is a ring which will be called a *factor-ring* of $\boldsymbol{R}$ over the ideal I.

10.3. **Ring homomorphisms and their kernels.** Let $\boldsymbol{R}$ and $\boldsymbol{S}$ be rings. A map $\varphi\colon R \to S$ is a *(ring) homomorphism* provided that

(i) $\varphi(a + b) = \varphi(a) + \varphi(b)$, for all $a, b \in R$,
(ii) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, for all $a, b \in R$,
(iii) $\varphi(1) = 1$.

Note that a map $\varphi\colon R \to S$ is a ring homomorphism if and only if it is at the same a homomorphism $(R, +) \to (S, +)$ of Abelian groups and $(R, \cdot) \to (S, \cdot)$ of monoids.

Let $\varphi\colon \boldsymbol{R} \to \boldsymbol{S}$ be a ring homomorphism. The *kernel* of φ is the set

$$\ker \varphi := \{a \in R \mid \varphi(a) = 0\}.$$

Lemma 10.3. *Let* $\varphi\colon \boldsymbol{R} \to \boldsymbol{S}$ *be a ring homomorphism. Then* $\ker \varphi$ *is an ideal of* $\boldsymbol{R}$.

Proof. Let $a, b \in \ker \varphi$. Then

$$\varphi(a + b) = \varphi(a) + \varphi(b) = 0,$$

hence $a + b \in \ker \varphi$. If $b \in \ker \varphi$ and $a, c \in R$, then

$$\varphi(a \cdot b \cdot c) = \varphi(a) \cdot \varphi(b) \cdot \varphi(c) = \varphi(a) \cdot 0 \cdot \varphi(c) = 0,$$

hence $a \cdot b \cdot c \in \ker \varphi$. We conclude that $\ker \varphi$ is an ideal of $\boldsymbol{R}$. □

On the other hand, if I is an ideal of the ring $\boldsymbol{R}$, we define a map $\pi_{\boldsymbol{R/I}}\colon R \to R/I$ by $a \mapsto a + I$, for all $a \in R$. One readily sees that $\pi_{\boldsymbol{R/I}}\colon \boldsymbol{R} \to \boldsymbol{R/I}$ is a ring homomorphism and that $I = \ker \pi_{\boldsymbol{R/I}}$. Therefore, ideals correspond to kernels of rings homomorphisms.

10.4. **Divisibility in commutative monoids.** Let $\boldsymbol{M} = (M, \cdot, 1)$ be a commutative monoid and $a, b \in M$. We say that a *divides* b (and we write $a \mid b$) if there is $c \in M$ such that $b = a \cdot c$. It is straightforward that the binary relation $\mid$ defined on the set M is reflexive and transitive, that is, it is a quasi-order on M.

The quasi-order of divisibility induces an equivalence relation $\sim$ on M given by $a \sim b$ provided that $a \mid b$ and $b \mid a$, for all $a, b \in M$. When $a \sim b$, we say that the elements a and b are *associated*. We denote by $[a]_\sim$ the block of the equivalence relation $\sim$ containing $a \in M$.

Lemma 10.4. *Assume that the monoid $\boldsymbol{M}$ is cancellative. Let $a, b \in M$. Then $a \sim b$ if and only if there is an invertible element $u \in M$ such that $b = a \cdot u$.*

Proof. ($\Rightarrow$) Suppose that $a \sim b$. Then $a \mid b$ and $b \mid a$, that is, there are $u, v \in M$ satisfying $b = a \cdot u$ and $a = b \cdot v$. It follows that $b = a \cdot u \cdot v$ and from the cancellativity we get that $1 = u \cdot v$. Since $\boldsymbol{M}$ is commutative, we conclude that u is invertible. ($\Leftarrow$) Suppose that there is an invertible element $u \in M$ such that $b = a \cdot u$. Let v be an inverse of u. Then $1 = u \cdot v$, and so $a = a \cdot 1 = a \cdot u \cdot v = b \cdot v$. Therefore $a \mid b$ and $b \mid a$, hence $a \sim b$. □

An element $p \in M$ is *prime* provided that p is not invertible and $p \mid a \cdot b$ implies that $p \mid a$ or $p \mid b$, for all $a, b \in M$.

An element $q \in M$ is *irreducible* provided that q is not invertible and $q \sim a \cdot b$ implies that either $q \sim a$ or $q \sim b$, for all $a, b \in M$.

By induction we prove that

Lemma 10.5. *An element $p \in M$ is prime if and only if*

$$p \mid a_1 \cdots a_n \implies p \mid a_i \text{ for some } i \in \{1, 2, \dots, n\},$$

for all $n \in \mathbb{N}$ and all $a_1, \dots, a_n \in M$.

An element $q \in M$ is irreducible if and only if

$$q \sim a_1 \cdots a_n \implies q \sim a_i \text{ for some } i \in \{1, 2, \dots, n\},$$

for all $n \in \mathbb{N}$ and all $a_1, \dots, a_n \in M$.

Lemma 10.6. *Every prime element of $\boldsymbol{M}$ is irreducible.*

Proof. Let $p \in M$ be a prime element and $p \sim a \cdot b$ for some $a, b \in M$. Then either $p \mid a$ or $p \mid b$. Since both $a \mid p$ and $b \mid p$, we conclude that either $p \sim a$ or $p \sim b$. It follows that p is irreducible. □

In general not every irreducible element is prime. We will have a closer look at this phenomenon later.

A common divisor of elements $a_1, \dots, a_n \in M$ is $b \in M$ such that $b \mid a_i$ for all $i \in \{1, 2, \dots, n\}$. A *greatest common divisor* of elements $a_1, \dots, a_n$ is

- a common divisor of $a_1, \dots, a_n$,
- if c is a common divisor of $a_1, \dots, a_n$, then $c \mid d$.

The greatest common divisor of $a_1, \dots, a_n$ may not be unique. However, it is easy to see that all the greatest common divisors are associated. On the other hand, if d is a greatest common divisor of the elements $a_1, \dots, a_n$ and $c \sim d$ then c is a greatest common divisor of $a_1, \dots, a_n$ as well. Therefore, all greatest common divisors of $a_1, \dots, a_n$ form a block of the equivalence $\sim$. We will denote the block by $(a_1, \dots, a_n)$.

Lemma 10.7. *Let $\boldsymbol{M}$ be a commutative monoid, $a, b, c \in M$. Then*

$$(a, (b, c)) = ((a, b), c). \tag{10.1}$$

Proof. Pick $d \in (a, (b, c))$ and $e \in ((a, b), c)$. We prove that $d \sim e$. Pick $f \in (b, c)$ and $g \in (a, b)$. Then $d \mid a$ and $d \mid f$. Since $d \mid f$, we have that $d \mid b$ and $d \mid c$. From $d \mid a$ and $d \mid b$ we infer that $d \mid g$ and, since $d \mid c$, we conclude that $d \mid e$. Similarly we prove that $e \mid d$. □

Corollary 10.8. *Let $\boldsymbol{M}$ be a commutative monoid. If a greatest common divisor exists for each pair of elements of $\boldsymbol{M}$, then a greatest common divisor exists for every non-empty finite subset $\{a_1, \dots, a_n\}$ of $\boldsymbol{M}$ and it can be computed inductively as*

$$(a_1, a_2, \dots, a_n) = (a_1, (a_2, \dots, a_n)).$$

Lemma 10.9. *Let $\boldsymbol{M}$ be a commutative cancellative monoid. Let $a, b, c \in M$ be such that both (a, b) and $(a \cdot c, b \cdot c)$ exist. Then*

$$(a \cdot c, b \cdot c) = (a, b) \cdot c.$$

Proof. Pick $d \in (a, b)$ and $e \in (a \cdot c, b \cdot c)$. From $d \cdot c \mid a \cdot c$ and $d \cdot c \mid b \cdot c$ we infer that $d \cdot c \mid e$, in particular, there is $x \in M$ such that

$$e = d \cdot c \cdot x.$$

Since $e \mid a \cdot c$ and $e \mid b \cdot c$, there are $y, z \in M$ such that

$$a \cdot c = e \cdot y = d \cdot c \cdot x \cdot y,$$
$$b \cdot c = e \cdot z = d \cdot c \cdot x \cdot z.$$

Since the monoid $\boldsymbol{M}$ is cancellatice, we infer that

$$a = d \cdot x \cdot y \quad \text{and} \quad b = d \cdot x \cdot z.$$

Therefore $d \cdot x$ is a common divisor of a, b, and so $d \cdot x \mid d$. It follows that $d \cdot x \sim d$, hence $e = d \cdot x \cdot c \sim d \cdot c$. We conclude that $d \cdot c$ is a greatest common divisor of $a \cdot c$ and $b \cdot c$. □

We say that $a, b \in M$ are *relatively prime* if the only common divisors of a and b are the invertible elements of $\boldsymbol{M}$. Clearly, elements $a, b \in M$ are relatively prime if and only if $(a, b) = [\,1\,]_\sim$.

Lemma 10.10. *Let $\boldsymbol{M}$ be a commutative cancellative monoid such that the greatest common divisor exists for each pair of elements of M. Let $a, b, c \in M$. If $(a, b) = [\,1\,]_\sim$ and $(a, c) = [\,1\,]_\sim$, then $(a, b \cdot c) = [\,1\,]_\sim$.*

Proof. Applying Lemma 10.9, we get from $(a,b) = [\,1\,]_\sim$, that $(a\cdot c, b\cdot c) = [\,1\,]_\sim \cdot c = [\,c\,]_\sim$. Similarly, we infer from $(1,c) = [\,1\,]_\sim$, that $(a, a\cdot c) = [\,a\,]_\sim$. Applying Lemma 10.7 we conclude that

$$(a, b\cdot c) = ((a, a\cdot c), b\cdot c) = (a, (a\cdot c, b\cdot c)) = (a,c) = [\,1\,]_\sim.$$

□

Observe that from Lemma 10.10 it follows that

Corollary 10.11. *Let $\boldsymbol{M}$ be a commutative cancellative monoid such that the greatest common divisor exists for each pair of elements of M, $a \in M$. Then the set of all elements of $\boldsymbol{M}$ that are relatively prime to the element a forms a submonoid of $\boldsymbol{M}$.*

Theorem 10.12. *Let $\boldsymbol{M}$ be a commutative cancellative monoid. If every pair of elements of $\boldsymbol{M}$ has a greatest common divisor, then every irreducible element of $\boldsymbol{M}$ is prime.*

Proof. Suppose that the assumptions of the theorem hold true and let q be an irreducible element of $\boldsymbol{M}$. Let $a, b \in M$. Since q is irreducible either $q \mid a$, in which case $(q,a) = [\,a\,]_\sim$ or $(q,a) = [\,1\,]_\sim$. It follows that if $q \nmid a$ and $q \nmid b$, then $(q,a) = (q,b) = [\,1\,]_\sim$. From Lemma 10.10 we infer that $(q, a\cdot b) = [\,1\,]_\sim$, hence $q \nmid a\cdot b$. Therefore q is a prime element of $\boldsymbol{M}$. □

Exercises

Exercise 10.1. *Let $\boldsymbol{R} = (R, +, \cdot)$ be a ring. Prove that*

(i) $a\cdot 0 = 0\cdot a = 0$, *for all* $a \in R$.
(ii) $(-a)\cdot b = a\cdot(-b) = -a\cdot b$, *for all* $a, b \in R$.

Exercise 10.2. *Let $\boldsymbol{R}$ be a commutative ring such that for every element $1 \neq a \in R$ there is $b \in R$ such that $a + b - a\cdot b = 0$. Prove that $\boldsymbol{R}$ is a field.*

Exercise 10.3. *Prove that the ring*

$$\boldsymbol{C} := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$$

with operations of matrix addition and multiplication is isomorphic to the field of all complex numbers.

Exercise 10.4. *Prove that the ring*

$$\boldsymbol{T} := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Z}_3 \right\}$$

with operations of matrix addition and multiplication is a field. What is the size of $\boldsymbol{T}$?

Exercise 10.5. *Prove that*

$$(\boldsymbol{R}[x])[y] \simeq (\boldsymbol{R}[y])[x]$$

for every ring $\boldsymbol{R}$.