RINGS, IDEALS AND DIVISIBILITY

PAVEL RŮŽIČKA

ABSTRACT. We define rings, ring homomorphisms, ideals and factor rings. We prove that ideals correspond to kernels of ring homomorphism and we state the homomorphism and the first isomorphism theorem for rings. We will study the connection between divisibility in commutative rings and the order of their principal ideals. We define a characterize unique factorization domains applying the results proved for unique factorization monoids. Finally we prove that every principal ideal domain is a unique factorization domain.

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

(i) $(R,+)$ is an Abelian group, that is,
- $a+(b+c)=(a+b)+c$, for all $a,b,c\in R$;
- $a+b=b+a$, for all $a,b\in R$;
- there is an element 0 in R such that $a+0=0+a=a$, for all $a\in R$;
- for every $a\in R$, there is $-a\in R$ such that $a+(-a)=(-a)+a=0$.

(ii) $(R,\cdot)$ is a monoid, that is,
- $a\cdot(b\cdot c)=(a\cdot b)\cdot c$, for all $a,b,c\in R$;
- there is an element 1 in R such that $a\cdot 1=1\cdot a=a$, for all $a\in R$.

(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 $a,b,c\in R$.

(iv) we will also postulate *non-triviality* of the ring, that is, that $0\neq 1$.

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.

March 15, 2019.

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 2.1. *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 $\boldsymbol{Z}_p$.*

Example 2.2. *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 $\boldsymbol{M}_n(\boldsymbol{F})$.*

Definition 2.3. Let $\boldsymbol{R}$ and $\boldsymbol{S}$ be rings. A map $\varphi\colon \boldsymbol{R} \to \boldsymbol{S}$ is a *ring homomorphism* provided that

$$\varphi(a+b) = \varphi(a) + \varphi(b), \qquad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b), \quad \text{and} \quad \varphi(1) = 1,$$

for all $a, b \in R$. That is, the map φ is a ring homomorphism if and only if it is simultaneously a homomorphism of the additive abelian groups $(R, +) \to (S, +)$ and the multiplicative monoids $(R, \cdot, 1) \to (S, \cdot, 1)$.

A one-to-one ring homomorphism is called a *monomorphism* while a homomorphism $\varphi\colon \boldsymbol{R} \to \boldsymbol{S}$ is an *epimorphism* provided that it maps R onto S, i.e., every element of S has a pre-image in R. A ring homomorphism $\boldsymbol{R} \to \boldsymbol{S}$ is an *isomorphism* provided that it us both one-to-one and onto. Rings $\boldsymbol{R}$ and $\boldsymbol{S}$ are called *isomorphic* if there is an isomorphism $\boldsymbol{R} \to \boldsymbol{S}$. In this case we write $\boldsymbol{R} \simeq \boldsymbol{S}$. The following standard argument (applicable not exclusively on ring homomorphisms) characterizes isomorphisms as invertible homomorphism. Recall that 1_R (resp. 1_S) denote the identity map $R \to R$ (resp. $S \to S$).

Lemma 2.4. *Let $\boldsymbol{R}$, $\boldsymbol{S}$ be rings. A map $\varphi\colon R \to S$ is an isomorphism of the rings if and only if there is a ring homomorphism $\psi\colon \boldsymbol{S} \to \boldsymbol{R}$ satisfying $\psi \circ \varphi = 1_R$ and $\varphi \circ \psi = 1_S$.*

Proof. ($\Rightarrow$) Suppose that $\varphi\colon \boldsymbol{R} \to \boldsymbol{S}$ is an isomorphism. It follows that for every $c \in S$ there is a unique $a \in R$ such that $\varphi(a) = c$. Let us define $\psi(c) = a$. It follows readily from the definition that $\psi \circ \varphi = 1_R$ and $\varphi \circ \psi = 1_S$. We prove that ψ is a ring homomorphism. Since $\varphi(1) = 1$ we get readily from the definition that $\psi(1) = 1$. Let $c, d \in S$. Since the compositions $\varphi \circ \psi$ and $\psi \circ \varphi$ equal the identity maps and $\varphi\colon \boldsymbol{R} \to \boldsymbol{S}$ is a

ring homomorphism, we have that

$$\begin{aligned}\psi(c+d) &= \psi(\varphi\circ\psi(c)+\varphi\circ\psi(d)) = \psi(\varphi(\psi(c)+\psi(d)))\\ &= (\psi\circ\varphi)(\psi(c)+\psi(d)) = \psi(c)+\psi(d)\end{aligned}$$

and

$$\begin{aligned}\psi(c\cdot d) &= \psi(\varphi\circ\psi(c)\cdot\varphi\circ\psi(d)) = \psi(\varphi(\psi(c)\cdot\psi(d)))\\ &= (\psi\circ\varphi)(\psi(c)\cdot\psi(d)) = \psi(c)\cdot\psi(d).\end{aligned}$$

Therefore $\psi\colon \boldsymbol{S}\to\boldsymbol{R}$ is a ring homomorphism. ($\Leftarrow$) Suppose that there is a ring homomorphism $\psi\colon \boldsymbol{S}\to\boldsymbol{R}$ satisfying $\psi\circ\varphi = 1_R$ and $\varphi\circ\psi = 1_S$. Similarly as above we prove that $\varphi\colon \boldsymbol{R}\to\boldsymbol{S}$ is a ring homomoprhism. Since $\varphi(\psi(c)) = c$ for every $c\in S$, the homomorphism φ maps R onto S. If $\varphi(a)=\varphi(b)$ for some $a,b\in R$, we get from $\psi\circ\varphi = 1_R$ that $a=\psi(\varphi(a)) = \psi(\varphi(b)) = b$, and so φ is one-to-one. Therefore φ is an isomorphism. □

The binary relation $\simeq$ of "being isomorphic" is clearly reflexive and transitive. It follows from Lemma 2.4 that $\simeq$ is also symmetric. Therefore it forms the equivalence on the class of all rings.

2.2. **Ideals, kernels of ring homomorphisms and factor-rings.**

Definition 2.5. Let $\boldsymbol{R}$ be a ring. A subset $I\subseteq R$ is an *ideal* of the ring $\boldsymbol{R}$ provided that

(i) if both $a,b\in I$, then $a+b\in I$,
(ii) if $a\in I$ or $b\in I$, then $a\cdot b\in I$,

for all $a,b\in R$.

Every ring has two *trivial ideals*: the zero ideal $\{0\}$ and the ring itself. Other ideals will be called non-trivial. Moreover, ideals of a ring $\boldsymbol{R}$ smaller than R will be called *proper* ideals. Observe that an ideal I of the ring $\boldsymbol{R}$ is proper if and only if $1\notin I$.

Definition 2.6. The *kernel* of a ring homomorphism $\varphi\colon \boldsymbol{R}\to\boldsymbol{S}$ is the set

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

Lemma 2.7. *The kernel of a ring homomorphism $\varphi\colon \boldsymbol{R}\to\boldsymbol{S}$ is a proper ideal of the ring $\boldsymbol{R}$.*

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

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

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

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

since $\varphi(a)=0$ or $\varphi(b)=0$. Therefore $a\cdot b\in\ker\varphi$. We conclude that $\ker\varphi$ is an ideal of $\boldsymbol{R}$. Since $\varphi(1)=1\neq 0$, the ideal $\ker\varphi$ is a proper ideal. □

Let I be an ideal of a ring $\boldsymbol{R}$. Observe that $(I,+)$ is a subgroup of the abelian group $(R,+)$. Indeed, if $a \in I$, then $-a = (-1)\cdot a \in I$. Let $a, b \in R$ and $a' \in a + I$, and $b' \in b + I$. There are $u, v \in I$ such that $a' = a + u$ and $b' = b + v$. We compute that

$$a' \cdot b' = (a+u)\cdot(b+v) = a\cdot b + \underbrace{a\cdot v + u\cdot(b+v)}_{\in I} \in a\cdot b + I. \tag{2.1}$$

For every $a \in R$, let $[\,a\,]_I$ denote the coset $a+I$ of I. It follows from (2.1) that if $a' \in [\,a\,]_I$ and $b' \in [\,b\,]_I$, then $a'\cdot b' \in [\,a\cdot b\,]_I$. Therefore we can define a multiplication of cosets of I by

$$[\,a\,]_I \cdot [\,b\,]_I = [\,a\cdot b\,]_I.$$

It is straightforward to verify the associativity of this multiplication, the distributivity of the addition and the multiplication of cosets, and that $[\,1\,]_I$ is a mutiplicative unit. Therefore we can talk of a *factor-ring* of $\boldsymbol{R}$ over the ideal I, whose elements are the cosets of I. We denote the factor-ring by $\boldsymbol{R/I}$.

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.

Similarly as in the case of groups, we can formulate the homomorphism and the first isomorphism theorems for rings. Their proofs are analogous.

Theorem 2.8 (The homomorphism theorem)**.** *Let $\varphi \colon \boldsymbol{R} \to \boldsymbol{S}$ be a homomorphism of rings. Let I be an ideal of the ring $\boldsymbol{R}$. There is a homomorphism $\psi \colon \boldsymbol{R/I} \to \boldsymbol{S}$ such that $\varphi = \psi \circ \pi_{\boldsymbol{R/I}}$ if and only if $I \subseteq \ker \varphi$. The homomorphism ψ is necessarily unique.*

Moreover ψ is a monomorphism if and only if $I = \ker \varphi$.

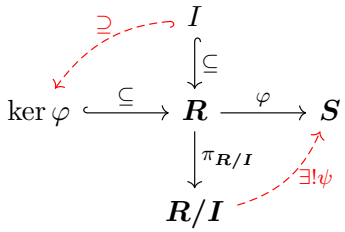

FIGURE 1. The homomorphism theorem

Corollary 2.9. *A ring homomorphism $\varphi \colon \boldsymbol{R} \to \boldsymbol{S}$ is a monomorphism if and only if $\ker \varphi = \{0\}$.*

Theorem 2.10 (The 1st isomorphism theorem)**.** *Let $\varphi \colon \boldsymbol{R} \to \boldsymbol{S}$ be a ring homomorphism. Then $\varphi(\boldsymbol{R})$ is a subring of $\boldsymbol{S}$ isomorphic to the factor ring $\boldsymbol{R/\ker \varphi}$.*

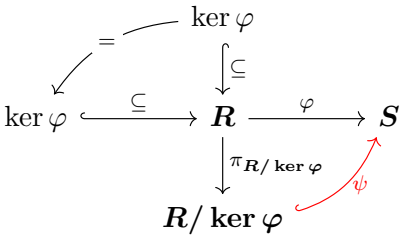

FIGURE 2. The 1st isomorphism theorem

2.3. **Divisibility and ideals.** Ideals of a ring $\boldsymbol{R}$ are ordered by inclusion. It is straightforward that ideals are closed under arbitrary intersections. It follows that the greatest ideal contained in ideals I, J is the intersection $I \cap J$. On the other hand, the least ideal containing I and J is the sum

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

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

Since the set of all ideals of the ring $\boldsymbol{R}$ is closed under arbitrary intersections, every subset $A \subseteq R$ possesses a least ideal containing A, the intersection of all ideals containing A. We will denote the ideal by (A) and call the *ideal generated* by the set A. Conversely, if I is an ideal of the ring $\boldsymbol{R}$ and $A \subseteq I$ is such that $I = (A)$, then the set A is called the *set of generators* of (the ideal) I. An ideal generated by a singleton set is called *principal*. We will use the notation (a) instead of, formally correct, $\{(a)\}$ to denote the ideal generated by a singleton set $\{a\}$.

Let $\boldsymbol{R}$ be a commutative ring. It is straightforward that, in this case,

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

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

$$(a) \subseteq (b) \iff b \mid a, \tag{2.2}$$

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

2.4. **Unique factorization domains.** A commutative ring $\boldsymbol{R}$ is an *integral domain* provided that

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

i.e., an integral domain is a commutative ring with no non-zero divisors of 0. Observe that a commutative ring $\boldsymbol{R}$ is an integral domain if and only if the set $R \setminus \{0\}$ is closed under multiplication.

Lemma 2.11. *A commutative ring $\boldsymbol{R}$ is an integral domain if and only if $(R \setminus \{0\}, \cdot, 1)$ is a cancellative monoid.*

Proof. ($\Rightarrow$) Suppose that $\boldsymbol{R}$ is an integral domain. Let a, b, c be non-zero elements of the ring $\boldsymbol{R}$ such that $a \cdot b = a \cdot c$. Then $a \cdot (b - c) = 0$. Since $a \neq 0$ and $\boldsymbol{R}$ is an integral domain, we conclude that $b - c = 0$. Therefore $b = c$, and so the monoid $(R \setminus \{0\}, \cdot, 1)$ is a cancellative. ($\Leftarrow$) Suppose that $(R \setminus \{0\}, \cdot, 1)$ is a monoid. It mean that the set $R \setminus \{0\}$ is closed under multiplication, an so the ring $\boldsymbol{R}$ has no non-zero divisors of 0. Therefore $\boldsymbol{R}$ is an integral domain. □

Al the notions that we have defined when having been studying the divisibility in commutative cancellative monoids can be transferred to integral domains. In particular, a nonzero element of an integral domain $\boldsymbol{R}$ is *prime*, resp. *irreducible*, provided that it is prime, resp. irreducible, in the monoid $(R \setminus \{0\}, \cdot, 1)$.

Definition 2.12. An integral domain $\boldsymbol{R}$ is a *unique factorization domain* (shortly *u.f.d.*) provided that $(R \setminus \{0\}, \cdot, 1)$ is a unique factorization monoid.

Thus adopting the definition from the previous chapter, an integral domain $\boldsymbol{R}$ is a u.f.d. if and only if every nonzero non-invertible element of $a \in R$ has a factorization $a = q_1 \cdots q_n$ into a product of irreducible elements and the elements $\boldsymbol{q}_1, \dots, \boldsymbol{q}_n$ are uniquely determined up to permutation. It follows from (2.2) that $b \sim c$ if and only if $(b) = (c)$ for all $b, c \in R$. Therefore the elements $\boldsymbol{q}_1, \dots, \boldsymbol{q}_n$ are uniquely determined up to permutation if and only if the ideals $(q_1), \dots, (q_n)$ are unique up to permutation.

Apllying (2.2) we reformulate Theorem 1.27:

Theorem 2.13. *An integral domain $\boldsymbol{R}$ is a unique factorization domain if and only if every irreducible element of $\boldsymbol{R}$ is prime and there is no infinite strictly increasing chain $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$ of principal ideals.*

Moreover, Corollary 1.28 implies that

Proposition 2.14. *An integral domain $\boldsymbol{R}$ is a unique factorization domain if and only if every every nonzero non-unit element of $\boldsymbol{R}$ is a product of primes.*

2.5. **Principal ideal domains.** A *principal ideal domain* (shortly *p.i.d.*) is an integral domain whose every ideal is principal.

Lemma 2.15. *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 $(a) + (b)$ is principal, hence generated by a single element $d \in R$. Since $(d) = (a) + (b) \supseteq (a)$, it follows from (2.2) that $d \mid a$. Similarly we get that $d \mid b$, and so d is a common divisor of a and b. On the other hand, if c is a common divisor of a, b then, again by (2.2), $(a) \subseteq (c)$ and $(b) \subseteq (c)$, hence $(a) + (b) \subseteq (c)$.

It follows that $(d) \subseteq (c)$, and so $c \mid d$. Therefore $\boldsymbol{d}$ is the greatest common divisor of a and b. □

Observe that, in the situation of the proof of Lemma 2.15, all generators of the ideal $(a) + (b)$ form a block of $\sim$, corresponding to (a, b). Applying Theorem 1.21 we conclude that

Corollary 2.16. *Every irreducible element of a principal ideal domain is prime.*

Let $\boldsymbol{R}$ be a ring and suppose that there is an infinite strictly increasing chain $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$ of principal ideals of $\boldsymbol{R}$. Put $I = \bigcup_{i=1}^{\infty}(a_i)$. If $a, b \in I$, then there are i, j such that $a \in (a_i)$ and $b \in (a_j)$. Then both a and $b$belong to $(a_{\max\{i,j\}}$, hence $a + b \in a_{\max\{i,j\}}$. Similarly, if $a \in I$ then $a \in (a_i)$ for some i. Let r be an arbitrary element of R. It follows from the definition of an ideal that both $r \cdot a$ and $a \cdot r$ belong to (a_i), hence *a fortiori* to I. Therefore I is an ideal. We claim that the ideal I is not principal. Otherwise there would be c such that $I = (c)$. But, since $I = \bigcup_{i=1}^{\infty}(a_i)$, there is i with $c \in (a_i)$. Consequently,

$$I = (c) \subseteq (a_i) \subsetneq (a_{i+1}) \subseteq I,$$

which is impossible. Therefore a principal ideal domain contains no infinite strictly increasing chain of principal ideals. Applying Corollary 2.16 and Theorem 2.13 we conclude that

Theorem 2.17. *Every principal ideal domain is a unique factorization domain.*

Lemma 2.18. *Let $\boldsymbol{R}$ be a principal ideal domain. Let $a, b \in R$ and $\boldsymbol{d} = (a, b)$. Then there are $r, s \in R$ such that*

$$d = r \cdot a + s \cdot b. \tag{2.3}$$

Proof. Since $\boldsymbol{d}$ is a greatest common divisor of a and b, we have that $(d) = (a) + (b)$. It folows that

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

□

Lemma 2.18 states that in principal ideal domains, greatest common divisors are expressed as linear combinations of the elements. Equality (2.3) is called *Bézout identity*.

Exercises

Exercise 2.1. *Prove that*

(i) $a \cdot 0 = 0 \cdot a = 0$,
(ii) $(-a) \cdot b = a \cdot (-b) = -a \cdot b$,

for every pair of elements a, b of a ring.

Exercise 2.2. *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 2.3. *Prove that the ring*

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

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

Exercise 2.4. *Prove that the ring*

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

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

Exercise 2.5. *List all ideals of the rings $\mathbb{Z}$ of all integers.*

Exercise 2.6. *List all ideals of the rings $\mathbb{Z}_{p^n}$ where p is a prime and n is a positive integer.*