Course 8: 12.04.2021

Chapter 2 RINGS

2.1 Rings and fields

Let us begin with the definition of the main algebraic structures with two binary operations.

Definition 2.1.1 Let R be a set. Then a structure with two operations $(R,+,\cdot)$ is called a:

(1) *ring* if $(R,+)$ is an abelian group, $(R,\cdot)$ is a semigroup and the distributive laws hold, that is,

$$\forall x,y,z\in R,\quad x\cdot(y+z)=x\cdot y+x\cdot z \text{ and } (y+z)\cdot x=y\cdot x+z\cdot x.$$

(2) *unitary ring* if $(R,+,\cdot)$ is a ring and there exists an identity element 1 with respect to "$\cdot$".

(3) *division ring* (or *skew field*) if $(R,+,\cdot)$ is a ring, $|R|\geq 2$ and any $x\in R^*$ has an inverse $x^{-1}\in R^*$, where $R^*=R\setminus\{0\}$ and 0 is the identity element of the group $(R,+)$.

(4) *field* if it is a commutative division ring.

Definition 2.1.2 Let $(R,+,\cdot)$ be a ring.

An element $x\in R^*$ is called a *left (right) zero divisor* if $\exists y\in R^*$ such that $x\cdot y=0$ $(y\cdot x=0)$.

An element $x\in R^*$ is called a *zero divisor* if it is a left **or** right zero divisor.

We say that R is an *integral domain* if $R\neq\{0\}$, R is unitary, commutative and has no zero divisor. The last condition means that:

$$x,y\in R\,,\ x\cdot y=0\Longrightarrow x=0 \text{ or } y=0\,.$$

Remark 2.1.3 (1) The name of zero divisor is justified by the very classical concept of divisibility in a commutative monoid $(A,\cdot)$, namely: if $x\in A$, then

$$x|0\Longleftrightarrow \exists y\in A \text{ such that } x\cdot y=0\,.$$

(2) Notice that $x\in R^*$ is not a left (right) zero divisor if and only if

$$y\in R\,,\ x\cdot y=0\Longrightarrow y=0\quad (y\cdot x=0\Longrightarrow y=0)\,.$$

Let us now give the most important examples of rings and fields.

Example 2.1.4 (a) $(\mathbb{Z},+,\cdot)$ is an integral domain, but not a field.

(b) $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ and $(\mathbb{C},+,\cdot)$ are fields.

(c) Let $\{e\}$ be a single element set and let both "$+$" and "$\cdot$" be the only possible operation on $\{e\}$, defined by $e+e=e$ and $e\cdot e=e$. Then $(\{e\},+,\cdot)$ is a commutative ring, called the *trivial ring*, where $1=0=e$.

(d) Let $n\in\mathbb{N}$, $n\geq 2$. Then $(\mathbb{Z}_n,+,\cdot)$ is a commutative ring, called the *ring of residue classes modulo* n. The addition and the multiplication are defined by

$$\widehat{x}+\widehat{y}=\widehat{x+y}\,,$$

$$\widehat{x}\cdot\widehat{y}=\widehat{x\cdot y}\,,$$

for every $\widehat{x},\widehat{y}\in\mathbb{Z}_n$.

Since $\widehat{2}\cdot\widehat{3}=\widehat{0}$, both $\widehat{2}$ and $\widehat{3}$ are zero divisors in the ring $(\mathbb{Z}_6,+,\cdot)$.

Note that the ring $(\mathbb{Z}_n,+,\cdot)$ is a field if and only if n is a prime number (see seminar).

(e) Let $\mathbb{Z}[i]=\{x+iy\mid x,y\in\mathbb{Z}\}$. Then $(\mathbb{Z}[i],+,\cdot)$ is a ring, called the *ring of Gauss integers*, where the operations are the usual addition and multiplication of complex numbers.

(f) Let $(R,+,\cdot)$ be a commutative unitary ring. Then $(R[X],+,\cdot)$ is a commutative unitary ring, called the *polynomial ring over R in the indeterminate X*, where the operations are the usual addition and multiplication of polynomials. We will come back later to the study of polynomial rings.

(g) Let $n \in \mathbb{N}$, $n \geq 2$ and let $(R, +, \cdot)$ be a ring. Then $(M_n(R), +, \cdot)$ is a ring, called the *ring of* $n \times n$ *matrices with entries in* R, where the operations are the usual addition and multiplication of matrices.

Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Since $A \cdot B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, A and B are zero divisors in the ring $(M_2(\mathbb{C}), +, \cdot)$.

(h) Let M be a non-empty set and let $(R, +, \cdot)$ be a ring. Define on $R^M = \{f \mid f : M \to R\}$ two operations by: $\forall f, g \in R^M$, we have $f + g : M \to R$, $f \cdot g : M \to R$, where

$$(f+g)(x) = f(x) + g(x)\,, \quad \forall x \in M\,,$$

$$(f \cdot g)(x) = f(x) \cdot g(x)\,, \quad \forall x \in M\,.$$

Then $(R^M, +, \cdot)$ is a ring, called the *ring of functions with a set as domain and a ring as codomain.*

The zero element is the function $\theta : M \to R$ defined by $\theta(x) = 0$, $\forall x \in M$. The symmetric of any function $f : M \to R$ is the function $-f : M \to R$ defined by $(-f)(x) = -f(x)$, $\forall x \in M$.

If R is unitary, then R^M is unitary and its identity element is the function $\varepsilon : M \to R$ defined by $\varepsilon(x) = 1$, $\forall x \in M$. If R is commutative, then so is R^M.

But even if R has no zero divisor, then R^M might have. Actually, this happens for any set M with $|M| \geq 2$. For instance, take $M = R = \mathbb{R}$ and consider the functions $f, g : \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \neq 0 \end{cases}$$

$$g(x) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x \neq 0 \end{cases}.$$

Then $f \neq \theta$ and $g \neq \theta$, but $f \cdot g = \theta$. Hence the ring $(\mathbb{R}^{\mathbb{R}}, +, \cdot)$ has zero divisors, even if the initial ring (in fact field) $(\mathbb{R}, +, \cdot)$ does not.

(i) Let $(G, +)$ be an abelian group. Define on the set $End(G, +)$ of its endomorphisms two operations by: $\forall f, g \in End(G, +)$,

$$(f+g)(x) = f(x) + g(x)\,, \quad \forall x \in G\,,$$

$$(f \circ g)(x) = f(g(x))\,, \quad \forall x \in G\,,$$

that is, the addition defined in the previous example and the composition of functions. Then $(End(G, +), +, \circ)$ is a unitary ring, called the *endomorphism ring of the abelian group* $(G, +)$.

The zero element is the trivial endomorphism $f \in End(G, +)$, defined by $f(x) = 0$, $\forall x \in G$. The symmetric of any $f \in End(G, +)$ is $-f \in End(G, +)$ defined by $(-f)(x) = -f(x)$, $\forall x \in G$. The identity element is the identity endomorphism $1_G \in End(G, +)$.

(j) On the set $\mathbb{H} = \{a_1 + a_2 i + a_3 j + a_4 k \mid a_1, a_2, a_3, a_4 \in \mathbb{R}\}$ one defines the following operations of addition and multiplication. For every $q = a_1 + a_2 i + a_3 j + a_4 k$, $q' = b_1 + b_2 i + b_3 j + b_4 k \in \mathbb{H}$,

$$\begin{aligned} q + q' &= (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k, \\ q \cdot q' &= (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3)i \\ &\quad + (a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2)j + (a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1)k. \end{aligned}$$

Then $(\mathbb{H}, +, \cdot)$ is a division ring, called the *quaternion division ring.* Note that the quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is a subgroup of the group $(\mathbb{H}^*, \cdot)$, and the product in $\mathbb{H}$ is determined by the product of the elements of the group $(Q, \cdot)$.

If $q = a_1 + a_2 i + a_3 j + a_4 k \in \mathbb{H}$, then

$$\bar{q} = a_1 - a_2 i - a_3 j - a_4 k \in \mathbb{H}$$

is called the *conjugate of* q. One can easily see that $\overline{q + q'} = \bar{q} + \overline{q'}$, $\overline{q \cdot q'} = \bar{q} \cdot \overline{q'}$, $\bar{\bar{q}} = q$ and $\overline{aq} = a\bar{q}$ for every $q, q' \in \mathbb{H}$ and every $a \in \mathbb{R}$.

For every $q \in \mathbb{H}$, the positive real number

$$N(q) = q \cdot \bar{q} = \bar{q} \cdot q = a_1^2 + a_2^2 + a_3^2 + a_4^2$$

is called the *norm* of q. Note that $N(q \cdot q') = N(q) \cdot N(q')$ for every $q, q' \in \mathbb{H}$. For every $q \in \mathbb{H}^*$, $q^{-1} = \frac{1}{N(q)}\bar{q}$.

Remark 2.1.5 If $(R, +, \cdot)$ is a ring, then $(R, +)$ is a group and $(R, \cdot)$ is a semigroup, so that we may talk about multiples and positive powers of elements of R.

Definition 2.1.6 Let $(R, +, \cdot)$ be a ring, let $x \in R$ and let $n \in \mathbb{N}^*$. Then we define

$$n \cdot x = \underbrace{x + x + \cdots + x}_{n \text{ times}},$$

$$0 \cdot x = 0,$$

$$(-n) \cdot x = -n \cdot x,$$

$$x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ times}}.$$

If R is a unitary ring, then we may also consider $x^0 = 1$.

If R is a division ring, then we may also define negative powers of x, namely

$$x^{-n} = (x^{-1})^n.$$

Remark 2.1.7 Notice that in the definition $0 \cdot x = 0$, the first 0 is the integer zero and the second 0 is the zero element of the ring R, i.e., the identity element of the group $(R, +)$.

Clearly, the first computational properties of a ring $(R, +, \cdot)$ are the properties of the group $(R, +)$ and of the semigroup $(R, \cdot)$. Some relationship properties between the two operations are given in the following result.

Theorem 2.1.8 *Let $(R, +, \cdot)$ be a ring and let $x, y, z \in R$. Then:*
(i) $x \cdot (y - z) = x \cdot y - x \cdot z$;
$(y - z) \cdot x = y \cdot x - z \cdot x$;
(ii) $x \cdot 0 = 0 \cdot x = 0$;
(iii) $x \cdot (-y) = (-x) \cdot y = -x \cdot y$.

Proof. (i) We have

$$x \cdot (y - z) = x \cdot y - x \cdot z \Longleftrightarrow x \cdot (y - z) + x \cdot z = x \cdot y \Longleftrightarrow x \cdot (y - z + z) = x \cdot y,$$

the last equality being obviously true. Similarly, $(y - z) \cdot x = y \cdot x - z \cdot x$.

(ii) We have

$$x \cdot 0 = x \cdot (y - y) = x \cdot y - x \cdot y = 0.$$

Similarly, $0 \cdot x = 0$.

(iii) We have

$$x \cdot (-y) = -x \cdot y \Longleftrightarrow x \cdot (-y) + x \cdot y = 0 \Longleftrightarrow x \cdot (-y + y) = 0 \Longleftrightarrow x \cdot 0 = 0,$$

the last equality being true by (ii). □

Remark 2.1.9 Note that all zeros appearing in Theorem 2.1.8 (ii) are the zero element of the ring R.

Theorem 2.1.10 *Let $(R, +, \cdot)$ be a ring and let $a \in R^*$. Then the following statements are equivalent:*
(i) a is not a left (right) zero divisor;
(ii) the left (right) cancellation law holds for a, that is,

$$a \cdot x = a \cdot y \Longrightarrow x = y \quad (x \cdot a = y \cdot a \Longrightarrow x = y),$$

where $x, y \in R$.

Proof. $(i) \Longrightarrow (ii)$ Let $x, y \in R$ be such that $a \cdot x = a \cdot y$. Then $a \cdot (x - y) = 0$ and since a is not a left zero divisor, we must have $x - y = 0$, i.e., $x = y$.

$(ii) \Longrightarrow (i)$ Let $b \in R$ be such that $a \cdot b = 0$. Then we have $a \cdot b = a \cdot 0$, whence it follows by the left cancellation law that $b = 0$. Hence a is not a left zero divisor.

Theorem 2.1.11 *Let $(R, +, \cdot)$ be a unitary ring and let $a \in R^*$. Consider the following statements:*
(1) a is invertible;
(2) a is not a zero divisor.
Then $(1) \Longrightarrow (2)$ and if R is finite, then $(1) \Longleftrightarrow (2)$.

Proof. $(1) \Longrightarrow (2)$ Let $b \in R$ be such that $a \cdot b = 0$. By multiplying by a^{-1} on the left hand side, we get $b = 0$. Hence a is not a left zero divisor. Similarly, a is not a right zero divisor.

$(2) \Longrightarrow (1)$ Now we know that R is finite. Consider the function $t_a : R \to R$ defined by $t_a(x) = a \cdot x$, $\forall x \in R$. Then t_a is injective, since

$$t_a(x) = t_a(y) \Longrightarrow a \cdot x = a \cdot y \Longrightarrow a(x - y) = 0 \Longrightarrow x - y = 0 \Longrightarrow x = y\,.$$

But since R is finite, the injective function $t_a : R \to R$ must be surjective as well. Then $\exists b \in R$ such that $a \cdot b = 1$. Similarly, by considering the function $t'_a : R \to R$ defined by $t'_a(x) = x \cdot a$, $\forall x \in R$, there exists $c \in R$ such that $c \cdot a = 1$. But then we have

$$cab = (ca)b = 1 \cdot b = b$$

and, on the other hand,

$$cab = c(ab) = c \cdot 1 = c,$$

hence $b = c$. Therefore, a is invertible. $\square$

Corollary 2.1.12 *(i) Every field has no zero divisor. Moreover, every field is an integral domain.*
(ii) Every finite integral domain is a field.

Example 2.1.13 Let p be a prime. The ring $(\mathbb{Z}_p, +, \cdot)$ of residue classes modulo p is non-zero, unitary and commutative. If $\hat{x}, \hat{y} \in \mathbb{Z}_p$ are such that $\hat{x} \cdot \hat{y} = \hat{0}$, then $\widehat{xy} = \hat{0}$, and thus $p|xy$. Hence $p|x$ or $p|y$, which implies that $\hat{x} = \hat{0}$ or $\hat{y} = \hat{0}$. This shows that $(\mathbb{Z}_p, +, \cdot)$ has no zero divisor. Therefore, $(\mathbb{Z}_p, +, \cdot)$ is an integral domain, and consequently, it is a field by the above corollary.