COURSE 2

Some important examples of rings

Let us remind that $(R, +, \cdot)$ is a **ring** if $(R, +)$ is an Abelian group, $\cdot$ is associative and the distributive laws hold (that is, $\cdot$ is distributive with respect to $+$). The ring $(R, +, \cdot)$ is a **unitary ring** if it has a multiplicative identity element.

Example 1. (**The residue-class rings**)

Let $n \in \mathbb{N},\ n \geq 2$. Let us remind **the Division Algorithm in** $\mathbb{Z}$: *For any integers a and b, with $b \neq 0$, there exists only one pair $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ such that*

$$a = b \cdot q + r \text{ and } 0 \leq r < |b|.$$

The Division Algorithm gives us a partition of $\mathbb{Z}$ in classes determined by the remainders one can find when dividing by n :

$$\{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\},$$

where $r + n\mathbb{Z} = \{r + nk \mid k \in \mathbb{Z}\}$ $(r \in \mathbb{Z})$. We use the following notations

$$\widehat{r} = r + n\mathbb{Z} \ (r \in \mathbb{Z}) \text{ şi } \mathbb{Z}_n = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\} = \{\widehat{0}, \widehat{1}, \ldots, \widehat{n-1}\}.$$

Let us notice that for $a, r \in \mathbb{Z}$,

$$\widehat{a} = \widehat{r} \Leftrightarrow a + n\mathbb{Z} = r + n\mathbb{Z} \Leftrightarrow a - r \in n\mathbb{Z} \Leftrightarrow n|a - r.$$

The operations

$$\widehat{a} + \widehat{b} = \widehat{a+b}, \quad \widehat{a}\,\widehat{b} = \widehat{ab}$$

are well defined, i.e. if one considers another representatives a' and b' for the classes $\widehat{a}$ and $\widehat{b}$, respectively, the operations provide us with the same results. Indeed, from $a' \in \widehat{a}$ şi $b' \in \widehat{b}$ it follows that

$$n|a' - a,\ n|b' - b \Rightarrow n|a' - a + b' - b \Rightarrow n|(a' + b') - (a + b) \Rightarrow \widehat{a' + b'} = \widehat{a + b}$$

and

$$a' = a + nk,\ b' = b + nl\ (k, l \in \mathbb{Z}) \Rightarrow a'b' = ab + n(al + bk + nkl) \in ab + n\mathbb{Z} \Rightarrow \widehat{a'b'} = \widehat{ab}.$$

One can easily check that the operations $+$ and $\cdot$ are associative and commutative, $+$ has $\widehat{0}$ as identity element, each class $\widehat{a}$ has an opposite in $(\mathbb{Z}_n, +)$, $-\widehat{a} = \widehat{-a} = \widehat{n-a}$, $\cdot$ has $\widehat{1}$ as identity element and $\cdot$ is distributive with respect to $+$. Thus, $(\mathbb{Z}_n, +, \cdot)$ is a unitary ring, called $(\mathbb{Z}_n, +, \cdot)$ is a commutative ring, called the **residue-class ring modulo** n.

Since $\widehat{2} \cdot \widehat{3} = \widehat{0}$, both $\widehat{2}$ and $\widehat{3}$ are zero divisors in the ring $(\mathbb{Z}_6, +, \cdot)$. Thus $(\mathbb{Z}_n, +, \cdot)$ is not a field in the general case. Actually, $\widehat{a} \in \mathbb{Z}_n$ is a unit if and only if $(a, n) = 1$. Thus $(\mathbb{Z}_n, +, \cdot)$ is a field if and only if n is a prime number.

Remark 2. If $(R, +, \cdot)$ is a ring, then $(R, +)$ is a group and $\cdot$ is associative, so that we may talk about multiples and positive powers of elements of R.

Definition 3. Let $(R,+,\cdot)$ be a ring, let $x \in R$ and let $n \in \mathbb{N}^*$. Then we define

$$n \cdot x = \underbrace{x + x + \cdots + x}_{n \text{ terms}}\,,\ 0 \cdot x = 0\,,\ (-n) \cdot x = -n \cdot x\,,$$

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

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 nonzero elements x by

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

Remark 4. 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 additive group $(R,+)$.

Theorem 5. 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.

$\square$

Definition 6. Let $(R,+,\cdot)$ be a ring and $A \subseteq R$. Then A is a **subring of** R if:
(1) A is closed under the operations of $(R,+,\cdot)$, that is,

$$\forall x, y \in A\,,\ x + y\,,\ x \cdot y \in A\,;$$

(2) $(A,+,\cdot)$ is a ring.

Remarks 7. (a) If $(R,+,\cdot)$ is a ring and $A \subseteq R$, then A is a subring of R if and only if A is a subgroup of $(R,+)$ and A is closed in $(R,\cdot)$.

This follows directly from subring definition knowing that the disributivity is preserved by the induced operations.
(b) A ring R may have subrings with or without (multiplicative) identity, as we will see in a forthcoming example.

Definition 8. Let $(K,+,\cdot)$ be a field and let $A \subseteq K$. Then A is called a **subfield of** K if:
(1) A is closed under the operations of $(K,+,\cdot)$, that is,

$$\forall x, y \in K\,,\ x + y\,,\ x \cdot y \in K\,;$$

(2) $(A,+,\cdot)$ is a field.

Remarks 9. (a) From (2) it follows that for a subfield A, we have $|A| \geq 2$.
(b) If $(K,+,\cdot)$ is a field and $A \subseteq K$, then A is a subfield if and only if A is a subgroup of $(K,+)$ and A^* is a subgroup of $(K^*,\cdot)$.
(c) f $(K,+,\cdot)$ is a field and $A \subseteq K$, then A is a subfield if and only if A is a subring of $(K,+,\cdot)$, $|A| \geq 2$ and for any $a \in A^*$, $a^{-1} \in A$.

Examples 10. (a) Every non-trivial ring $(R,+,\cdot)$ has two subrings, namely $\{0\}$ and R, called the **trivial subrings**.
(b) $\mathbb{Z}$ is a subring of $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ and $(\mathbb{C},+,\cdot)$, $\mathbb{Q}$ is a subfield of $(\mathbb{R},+,\cdot)$ and $(\mathbb{C},+,\cdot)$, $\mathbb{R}$ is a subfield of $(\mathbb{C},+,\cdot)$.
(c) If K is a field, then $\{0\}$ is a subring of K which is not a subfield.

Definition 11. Let $(R,+,\cdot)$ and $(R',+,\cdot)$ be rings and $f : R \to R'$. Then f is called a **(ring) homomorphism** if

$$f(x+y) = f(x) + f(y)\,,\ \forall x,y \in R$$

$$f(x \cdot y) = f(x) \cdot f(y)\,,\ \forall x,y \in R.$$

The notions of **(ring) isomorphism**, **endomorphism** and **automorphism** are defined as usual.

We denote by $R \simeq R'$ the fact that two rings R and R' are isomorphic.

Remark 12. If $f : R \to R'$ is a ring homomorphism, then the first condition from its definition tells us that f is a group homomorphism between $(R,+)$ and $(R',+)$. Thus,

$$f(0) = 0' \text{ and } f(-x) = -f(x),\ \forall x \in R.$$

But in general, even if R and R' have multiplicative identities, denoted by 1 and $1'$ respectively, in general it does not follow that a ring homomorphism $f : R \to R'$ has the property that $f(1) = 1'$.

Examples 13. (a) Let $(R,+,\cdot)$ and $(R',+,\cdot)$ be rings and let $f : R \to R'$ be defined by

$$f(x) = 0',\ \forall x \in R.$$

Then f is a homomorphism, called the **trivial homomorphism**. Notice that if R and $R' \neq \{0'\}$ have identities, we do not have $f(1) = 1'$.
(b) Let $(R,+,\cdot)$ be a ring. Then the identity map $1_R : R \to R$ is an automorphism of R.
(c) Let us take $f : \mathbb{C} \to \mathbb{C}$, $f(z) = \overline{z}$ (where $\overline{z}$ is the complex conjugate of z). Since

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2},\ \overline{z_1 z_2} = \overline{z_1}\ \overline{z_2} \text{ and } \overline{\overline{z}} = z,$$

f is an automorphism of $(\mathbb{C},+,\cdot)$ and $f^{-1} = f$.

Definition 14. Let $(R,+,\cdot)$ and $(R',+,\cdot)$ be unitary rings with the multiplicative identity elements 1 and $1'$ respectively and let $f : R \to R'$ be a ring homomorphism. Then f is called a **unitary homomorphism** if $f(1) = 1'$.

Theorem 15. Let $(R,+,\cdot)$ and $(R',+,\cdot)$ be rings with identity elements 1 and $1'$ respectively and let $f : R \to R'$ be a unitary ring homomorphism. If $x \in R$ has an inverse element $x^{-1} \in R$, then $f(x)$ has an inverse and $f(x^{-1}) = [f(x)]^{-1}$.

Proof.

□

Remark 16. Any non-zero homomorphism between two fields is a unitary homomorphism.

Indeed, ...

The polynomial ring over a field - preparations

Let $(K, +, \cdot)$ be a field and let us denote by $K^{\mathbb{N}}$ the set

$$K^{\mathbb{N}} = \{f \mid f : \mathbb{N} \to K\}.$$

If $f : \mathbb{N} \to K$ then, denoting $f(n) = a_n$, we can write

$$f = (a_0, a_1, a_2, \dots).$$

For $f = (a_0, a_1, a_2, \dots),\ g = (b_0, b_1, b_2, \dots) \in K^{\mathbb{N}}$ one defines:

$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots) \tag{1}$$

$$f \cdot g = (c_0, c_1, c_2, \dots) \tag{2}$$

where

$$\begin{aligned}
&c_0 = a_0 b_0, \\
&c_1 = a_0 b_1 + a_1 b_0, \\
&\vdots \\
&c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 = \sum_{i+j=n} a_i b_j, \\
&\vdots
\end{aligned}$$

Theorem 17. $K^{\mathbb{N}}$ forms a commutative unitary ring with respect to the operations defined by (1) and (2) called **the ring of formal power series over** K.

Proof. HOMEWORK

□

Let $f = (a_0, a_1, a_2, \dots) \in K^{\mathbb{N}}$. The **support of** f is the subset of $\mathbb{N}$ defined by

$$supp\, f = \{k \in \mathbb{N} \mid a_k \neq 0\}.$$

Let us denote by $K^{(\mathbb{N})}$ the subset consisting of all the sequences from $K^{\mathbb{N}}$ with a finite support. We have

$$f \in K^{(\mathbb{N})} \Leftrightarrow \exists\, n \in \mathbb{N} \text{ such that } a_i = 0 \text{ for } i \geq n \Leftrightarrow f = (a_0, a_1, a_2, \dots, a_{n-1}, 0, 0, \dots).$$

We will begin our next course with:

Theorem 18. i) $K^{(\mathbb{N})}$ is a subring of $K^{\mathbb{N}}$ which contains the multiplicative identity element.
ii) The mapping $\varphi : K \to K^{(\mathbb{N})},\ \varphi(a) = (a, 0, 0, \dots)$ is an injective unitary ring morphism.