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*

remainder (or residue) they are $0, 1, \dots, n-1$.

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

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

multiple of n

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

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

the residue-class set modulo n

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

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

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

$+, \cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$

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.

during the seminar

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.

coprime = relatively prime

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

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

ℕ ∈R ℤ the opposite in (R,+)

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

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) $x \cdot 0 = 0 \cdot x = 0$; ← homework: complete the proof
(iii) $x \cdot (-y) = (-x) \cdot y = -x \cdot y$.

Proof. (i) $x \cdot \big| (y-z)+z = y+(z-z)=y \Longrightarrow x\cdot[(y-z)+z] = xy \iff$

$\iff x\cdot(y-z) + xz = xy \,\big|\, -xz \Longrightarrow x\cdot(y-z) = xy - xz.$

(ii) $\forall y \in R,\ y - y = 0 \Longrightarrow x\cdot 0 = x\cdot(y-y) \overset{(i)}{=} xy - xy = 0$

(iii) $x\cdot(-y) + x\cdot y = x\cdot(-y+y) = x\cdot 0 \overset{(ii)}{=} 0 \Longrightarrow x\cdot(-y) = -xy.$

□

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,

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

ind. op.

(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,

ind. op.

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

(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) If $(K, +, \cdot)$ 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 $a \in A^*$, $a^{-1} \in A$. $\setminus\{0\}$

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

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

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

isom. = bij. hom.
endom. = hom. from a ring into itself

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

autom = bij. endom.

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

the additive id. elem.

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

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. $(1_R(x) = x)$.

(c) Let $(R, +, \cdot)$ be a ring and let $A \leq R$. Define $i : A \to R$ by $i(x) = x$, $\forall x \in A$. Then i is a homomorphism, called the **inclusion homomorphism**.

A subring in $(R,+,\cdot)$

(d) Let us take $f : \mathbb{C} \to \mathbb{C}$, $f(z) = \overline{z}$ (where $\overline{z}$ is the complex conjugate of z). Since

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

$f \circ f = 1_{\mathbb{C}}$.

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 $f(1) = 1'$. (the high-school version of homomorphism.)

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. $f(x)\cdot f(x^{-1}) = f(x\cdot x^{-1}) = f(1) = 1'$

$f(x^{-1})\cdot f(x) = f(x^{-1}\cdot x) = f(1) = 1'$ $\implies f(x^{-1}) = [f(x)]^{-1}$.

□

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

Indeed, let $(K,+,\cdot), (K',+,\cdot)$ be fields, $f : K \to K'$ be a homom. $f(1) \overset{?}{=} 1'$

f non-zero $\implies \exists\, x_0 \in K : f(x_0) \neq 0'$ $(x_0 \neq 0 \implies \exists\, x_0^{-1} \in K)$

$[f(x_0)]^{-1}\cdot$ / $f(x_0)\cdot 1' = f(x_0) = f(x_0 \cdot 1) = f(x_0)\cdot f(1) \implies 1' = f(1)$

The polynomial ring over a field

the set of natural numbers.

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

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

R: $f = g \iff a_i = b_i,\ \forall i \in \mathbb{N}$.

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

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

elem. of K.

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

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

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

$(0, 0, \ldots, 0, \ldots)$ the zero elem.

$-f = (-a_0, -a_1, \ldots, -a_n, \ldots)$

$(1, 0, \ldots, 0, \ldots)$ the multipl. id. elem.

□

COURSE 3

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

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

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

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

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

Proof. □

The ring $(K^{(\mathbb{N})}, +, \cdot)$ is called **polynomial ring** over K. How can we make this ring look like the one we know from high school?

The injective morphism φ allows us to identify $a \in K$ with $(a, 0, 0, \dots)$. Thi way K can be seen as a subring of $K^{(\mathbb{N})}$. The polynomial

$$X = (0, 1, 0, 0, \dots)$$

is called **indeterminate** or **variable**. From (2) one deduces that:

$$\begin{aligned}
&X^2 = (0, 0, 1, 0, 0, \dots) \\
&X^3 = (0, 0, 0, 1, 0, 0, \dots) \\
&\vdots \\
&X^m = (\underbrace{0, 0, \dots, 0}_{m\ ori}, 1, 0, 0, \dots) \\
&\vdots
\end{aligned}$$

Since we identified $a \in K$ with $(a, 0, 0, \dots)$, from (2) it follows:

$$aX^m = (\underbrace{0, 0, \dots, 0}_{m\ ori}, a, 0, 0, \dots) \tag{3}$$

This way we have

Theorem 19. Any $f \in K^{(\mathbb{N})}$ which is not zero can be uniquely written as

$$f = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \tag{4}$$

where $a_i \in K$, $i \in \{0, 1, \dots, n\}$ and $a_n \neq 0$.

We can rewrite

$$K^{(\mathbb{N})} = \{f = a_0 + a_1 X + \cdots + a_n X^n \mid a_0, a_1, \dots, a_n \in K,\ n \in \mathbb{N}\} \overset{not}{=} K[X].$$

The elements of $K[X]$ are called **polynomials over** K, and if $f = a_0 + a_1 X + \cdots + a_n X^n$ then $a_0, \dots, a_n \in K$ are **the coefficients of** f, $a_0, a_1 X \dots, a_n X^n$ are called **monomials**, and a_0 is **the constant term of** f. Now, we can rewrite the operations from $(K[X], +, \cdot)$ as we did in high school (during the seminar).

If $f \in K[X]$, $f \neq 0$ and f is given by (4), then n is called **the degree of** f, and if $f = 0$ we say that the degree of f is $-\infty$. We will denote the degree of f by $\deg f$. Thus we have

$$\deg f = 0 \Leftrightarrow f \in K^*.$$

By definition

$$-\infty + m = m + (-\infty) = -\infty,\ -\infty + (-\infty) = -\infty,\ -\infty < m,\ \forall\, m \in \mathbb{N}.$$

Therefore:
i) $\deg(f+g) \leq \max\{\deg f, grad\, g\}, \forall f, g \in K[X]$;
ii) $\deg(fg) = \deg f + \deg g, \forall f, g \in K[X]$;
iii) $K[X]$ is an integral domain (during the seminar);
iv) a polynomial $f \in K[X]$ este is a unit in $K[X]$ if and only if $f \in K^*$ (during the seminar).

Here are some useful notions and results concerning polynomials:
If $f, g \in K[X]$ then

$$f \mid g \Leftrightarrow \exists\, h \in R,\ g = fh.$$

The divisibility $\mid$ is reflexive and transitive. The polynomial 0 satisfies the following relations

$$f \mid 0,\ \forall f \in K[X] \text{ and } \nexists f \in K[X] \setminus \{0\}:\ 0 \mid f.$$

Two polynomials $f, g \in K[X]$ are **associates** (we write $f \sim g$) if

$$\exists\, a \in K^*:\ f = ag.$$

The relation $\sim$ is reflexive, transitive and symmetric.

A polynomial $f \in K[X]^*$ is **irreducible** if $\deg f \geq 1$ and

$$f = gh\ (g, h \in K[X]) \Rightarrow g \in K^* \text{ or } h \in K^*.$$

The gcd and lcm are defined as for integers, the product of a gcm and lcma af two polynomials f, g and the product fg are associates and the polynomials divisibility acts with respect to sum and product in the way we are familiar with from the integers case.

If $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X]$ and $c \in K$, then

$$f(c) = a_0 + a_1c + a_2cX^2 + \cdots + a_nc^n \in K$$

is called **the evaluation of** f **at** c. The element $c \in K$ is **a root of** f if $f(c) = 0$.

Theorem 20. (The Division Algorithm in $K[X]$) For any polynomials $f, g \in K[X]$, $g \neq 0$, there exist $q, r \in K[X]$ uniquely determined such that

$$f = gq + r \text{ and } \deg r < \deg g. \tag{5}$$

Proof. (optional) Let $a_0, \ldots, a_n, b_0, \ldots, b_m \in K$, $b_m \neq 0$ and

$$f = a_0 + a_1X + \cdots + a_nX^n \text{ şi } g = b_0 + b_1X + \cdots + b_mX^m.$$

The existence of q and r: If $f = 0$ then $q = r = 0$ satisfy (5).

For $f \neq 0$ we prove by induction that that the property holds for any $n = \deg f$. If $n < m$ (since $m \geq 0$, there exist polynomials f which satisfy this condition), then (5) holds for $q = 0$ and $r = f$.

Let us assume the statement proved for any polynomials with the degree $n \geq m$. Since a_nX^n is the maximum degree monomial of the polynomial $a_nb_m^{-1}X^{n-m}g$, for $h = f - a_nb_m^{-1}X^{n-m}g$, we have $\deg h < n$ and, according to ourassumption, there exist $q', r \in R[X]$ such that

$$h = gq' + r \text{ and } \deg r < \deg g.$$

Thus, we have $f = h+a_nb_m^{-1}X^{n-m}g = (a_nb_m^{-1}X^{n-m}+q')g+r = gq+r$ where $q = a_nb_m^{-1}X^{n-m}+q'$. Now, the existence of q and r from (5) is proved.

The uniqueness of q and r: If we also have

$$f = gq_1 + r_1 \text{ and } \deg r_1 < \deg g,$$

then $gq + r = gq_1 + r_1$. It follows that $r - r_1 = g(q_1 - q)$ and $\deg(r - r_1) < \deg g$. Since $g \neq 0$ we have $q_1 - q = 0$ and, consequently, $r - r_1 = 0$, thus $q_1 = q$ and $r_1 = r$. □

We call the polynomials q and r from (5) **the quotient** and **the remainder** of f when dividing by g, respectively.

Corollary 21. Let K be a field and $c \in K$. The remainder of a polynomial $f \in K[X]$ when dividing by $X - c$ is $f(c)$.

Indeed, from (5) one deduces that $r \in K$, and since $f = (X - c)q + r$, one finds that $r = f(c)$. For $r = 0$ we obtain:

Corollary 22. Let K be a field. The element $c \in K$ is a root of f if and only if $(X - c) \mid f$.

Corollary 23. If K is a field and $f \in K[X]$ has the degree $k \in \mathbb{N}$, then the number of the roots of f from K is at most k.

Indeed, the statement is true for zero-degree polynomials, since they have no roots. We consider $k > 0$ and we assume the property valid for any polynomialwith the degree smaller than k. If $c_1 \in K$ is a root of f then $f = (X - c_1)q$ and $\deg q = k - 1$. According to our assumption, q has at most $k - 1$ roots in K. Since K is a field, $K[X]$ is an integral domain and from $f = (X - c_1)q$ it follows that $c \in K$ is a root of f if and only if $c = c_1$ or c is a root of q. Thus f has at most k roots in K.