

COURSE 3

Some important examples of rings

We 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.

The polynomial ring over a field

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

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

If $f : \mathbb{N} \rightarrow K$ 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:

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

$$f \cdot g = (c_0, c_1, c_2, \dots) \quad (2)$$

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 1. $K^{\mathbb{N}}$ 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

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

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

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

Theorem 2. i) $K^{(\mathbb{N})}$ is a subring of $K^{\mathbb{N}}$ which contains the multiplicative identity element.
ii) The mapping $\varphi : K \rightarrow K^{(\mathbb{N})}$, $\varphi(a) = (a, 0, 0, \dots)$ 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 $(a, 0, 0, \dots)$. This 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:

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

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

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

This way we have

Theorem 3. Any $f \in K^{(\mathbb{N})}$ which is not zero can be uniquely written as

$$f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \quad (4)$$

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

We can rewrite

$$K^{(\mathbb{N})} = \{f = a_0 + a_1X + \dots + a_nX^n \mid a_0, a_1, \dots, a_n \in K, n \in \mathbb{N}\} \stackrel{\text{not}}{=} K[X].$$

The elements of $K[X]$ are called **polynomials over K** , and if $f = a_0 + a_1X + \dots + a_nX^n$ then $a_0, \dots, a_n \in K$ are **the coefficients of f** , a_0, a_1X, \dots, a_nX^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

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

Therefore:

- i) $\deg(f + g) \leq \max\{\deg f, \deg g\}, \forall f, g \in K[X]$;
- 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 $f \in K[X]$ 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

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

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

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

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

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

The gcd and lcm are defined as for integers, the product of a gcd and lcm of 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

$$f(c) = a_0 + a_1c + a_2c^2 + \cdots + a_nc^n \in K$$

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

Theorem 4. (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 $a_0, \dots, a_n, b_0, \dots, b_m \in K$, $b_m \neq 0$ and

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

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

For $f \neq 0$ we prove by induction that 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 $a_n X^n$ is the maximum degree monomial of the polynomial $a_n b_m^{-1} X^{n-m} g$, for $h = f - a_n b_m^{-1} X^{n-m} g$, we have $\deg h < n$ and, according to our assumption, there exist $q', r \in R[X]$ such that

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

Thus, we have $f = h + a_n b_m^{-1} X^{n-m} g = (a_n b_m^{-1} X^{n-m} + q')g + r = gq + r$ where $q = a_n b_m^{-1} X^{n-m} + q'$. 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 $r_1 = r$. \square

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

Corollary 5. 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 6. Let K be a field. The element $c \in K$ is a root of f if and only if $(X - c) \mid f$.

Corollary 7. 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 polynomial with 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 .

The ring of square matrices over a field

Let K be a set and $m, n \in \mathbb{N}^*$. A mapping

$$A : \{1, \dots, m\} \times \{1, \dots, n\} \rightarrow K$$

is called $m \times n$ **matrix** over K . When $m = n$, we call A a **square matrix of size n** . For each $i = 1, \dots, m$ and $j = 1, \dots, n$ we denote $A(i, j)$ by $a_{ij} (\in K)$ and we represent A as a rectangular array with m rows and n columns in which the image of each pair (i, j) is written in the i 'th row and the j 'th column

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

We also denote this array by

$$A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$$

or, simpler, $A = (a_{ij})$. We denote the set of all $m \times n$ matrices over K by $M_{m,n}(K)$ and, when $m = n$, by $M_n(K)$.

Let $(K, +, \cdot)$ be a field. Then $+$ from K determines an operation $+$ on $M_{m,n}(K)$ defined as follows: if $A = (a_{ij})$ and $B = (b_{ij})$ are two $m \times n$ matrices, then

$$A + B = (a_{ij} + b_{ij}).$$

One can easily check that this operation is associative, commutative, it has an identity element which is the matrix $O_{m,n}$ consisting only of 0 (called **the $m \times n$ zero matrix**) and each matrix $A = (a_{ij})$ from $M_{m,n}(K)$ has an opposite (the matrix $-A = (-a_{ij})$). Therefore,

Theorem 8. $(M_{m,n}(K), +)$ is an Abelian group.

The scalar multiplication of a matrix $A = (a_{ij}) \in M_{m,n}(K)$ and a scalar $\alpha \in K$ is defined by

$$\alpha A = (\alpha a_{ij}).$$

One can easily check that:

- i) $\alpha(A + B) = \alpha A + \alpha B$, $\forall \alpha \in K$, $\forall A, B \in M_{m,n}(K)$;
- ii) $(\alpha + \beta)A = \alpha A + \beta A$, $\forall \alpha, \beta \in K$, $\forall A \in M_{m,n}(K)$;
- iii) $(\alpha\beta)A = \alpha(\beta A)$, $\forall \alpha, \beta \in K$, $\forall A \in M_{m,n}(K)$;
- iv) $1 \cdot A = A$, $\forall A \in M_{m,n}(K)$.

The matrix multiplication is defined as follows: if $A = (a_{ij}) \in M_{m,n}(K)$ and $B = (b_{ij}) \in M_{n,p}(K)$, then

$$AB = (c_{ij}) \in M_{m,p}, \text{ cu } c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}, \quad (i, j) \in \{1, \dots, m\} \times \{1, \dots, p\}.$$

For $n \in \mathbb{N}^*$ we consider the $n \times n$ square matrix

$$I_n = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

If $m, n, p, q \in \mathbb{N}^*$, then:

- 1) $(AB)C = A(BC)$, for any matrices $A \in M_{m,n}(K)$, $B \in M_{n,p}(K)$, $C \in M_{p,q}(K)$;
- 2) $I_m A = A = A I_n$, $\forall A \in M_{m,n}(K)$;
- 3) $A(B + C) = AB + AC$ for any matrices $A \in M_{m,n}(K)$, $B, C \in M_{n,p}(K)$;
- 3') $(B + C)D = BD + CD$, for any matrices $B, C \in M_{n,p}(K)$, $D \in M_{p,q}(K)$;
- 4) $\alpha(AB) = (\alpha A)B = A(\alpha B)$, $\forall \alpha \in K$, $\forall A \in M_{m,n}(K)$, $\forall B \in M_{n,p}(K)$.

If we work with $n \times n$ square matrices the matrix multiplication becomes a binary (internal) operation \cdot on $M_n(K)$, and the equalities 1)–3') show that \cdot is associative, I_n is a multiplicative identity element (called **the identity matrix** of size n) and \cdot is distributive with respect to $+$. Hence,

Theorem 9. $(M_n(K), +, \cdot)$ is a unitary ring called **the ring of the square matrices of size n over K** .

Remarks 10. a) If $n \geq 2$ then $M_n(K)$ is not commutative and it has zero divisors. If $a, b \in K^*$, the non-zero matrices

$$\begin{pmatrix} a & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \dots & b \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

can be used to prove this.

b) Using the properties of the addition, multiplication and scalar multiplication, one can easily prove that

$$f : K \rightarrow M_n(K), f(a) = \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & a \end{pmatrix} = aI_n$$

is a unitary injective ring homomorphism.

The transpose of an $m \times n$ matrix $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = (a_{ij})$ is the $n \times m$

matrix

$${}^t A = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{12} & a_{22} & \dots & a_{m2} \\ \vdots & \vdots & \dots & \vdots \\ a_{1n} & a_{2n} & \dots & a_{mn} \end{pmatrix} = (a_{ji}).$$

The way the transpose acts with respect to the matrix addition, matrix multiplication and scalar multiplication is given bellow:

$$\begin{aligned} {}^t(A + B) &= {}^t A + {}^t B, \forall A, B \in M_{m,n}(K); \\ {}^t(AB) &= {}^t B \cdot {}^t A, \forall A \in M_{m,n}(K), \forall B \in M_{n,p}(K); \\ {}^t(\alpha A) &= \alpha \cdot {}^t A, \forall A \in M_{m,n}(K). \end{aligned}$$

Let K be a field. The set of the units of $M_n(K)$ is

$$GL_n(K) = \{A \in M_n(K) \mid \exists B \in M_n(K) : AB = BA = I_n\}.$$

The set $GL_n(K)$ is closed in $(M_n(K), \cdot)$ and $(GL_n(K), \cdot)$ is a group called **the general linear group of degree n over K** . We know from high school that if K is one of the number fields (\mathbb{Q} , \mathbb{R} sau \mathbb{C}) then $A \in M_n(K)$ is invertible if and only if $\det A \neq 0$. Thus,

$$GL_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) \mid \det A \neq 0\},$$

and analogously we can rewrite $GL_n(\mathbb{R})$ and $GL_n(\mathbb{Q})$. We will see next that this recipe works for any matrix ring $M_n(K)$ with K field. This is why our next course topic will be **the determinant of a square matrix over a field K** .