COURSE 1

Groups, rings and fields

Definition 1. By a **binary operation** on a set A we understand a map

$$\varphi : A \times A \to A\,.$$

Since all the operations considered in this section are binary operations, we briefly call them **operations**. Usually, we denote operations by symbols like $*$, $\cdot$, $+$, and the image of an arbitrary pair $(x, y) \in A \times A$ is denoted by $x * y$, $x \cdot y$ (multiplicative notation), $x + y$ (additive notation), respectively.

Examples 2. a) The usual addition and multiplication are operations on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, but not on the set of irrational numbers.
b) The usual subtraction is an operation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$, but not on $\mathbb{N}$.
c) The usual division is an operation on $\mathbb{Q}^*, \mathbb{R}^*$, $\mathbb{C}^*$, but not on $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{N}^*$ or $\mathbb{Z}^*$.

Definitions 3. Let $*$ be an operation on A. We say that:
i) $*$ is **associative** if

$$(a_1 * a_2) * a_3 = a_1 * (a_2 * a_3),\ \forall a_1, a_2, a_3 \in A;$$

ii) $*$ is **commutative** if

$$a_1 * a_2 = a_2 * a_1,\ \forall a_1, a_2 \in A.$$

iii) $e \in A$ is an **identity element** for $*$ if

$$a * e = e * a = a,\ \forall a \in A.$$

When using the multiplicative or additive notation, an identity element e is usually denoted by 1 or 0, respectively.

Definition 4. Let A be set and let $\cdot$ be an operation with an identity element 1. An element $a \in A$ **has an inverse** if there exists an element $a' \in A$ such that

$$a \cdot a' = a' \cdot a = e.$$

We say that a' is an **inverse** for a.

When using the multiplicative notation, the inverse of a is denoted by a^{-1}. When using the or additive notation the inverse of a is denoted by $-a$, and it is called **the opposite of** a.

Definitions 5. A pair $(A, *)$ is called **monoid** if $*$ is associative and it has an **identity element**. A monoid with a commutative operation is called **commutative monoid**.

Definition 6. A pair $(A, \cdot)$ is called **group** if it is a monoid in which every element has an inverse. If the operation is commutative as well, the structure is called **commutative** or **Abelian group**.

Examples 7. a) $(\mathbb{N}, +)$ and $(\mathbb{Z}, \cdot)$ are commutative monoids, but they are not groups.
b) $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ are commutative monoids, but they are not groups since 0 has no inverse.
c) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ are Abelian groups.

Remark 8. The group definition can be rewritten: $(A, \cdot)$ is a **group** if and only if it follows the following conditions:

(i) $(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3),\ \forall a_1, a_2, a_3 \in A$ ($\cdot$ is associative);
(ii) $\exists 1 \in A,\ \forall a \in A:\ a \cdot 1 = 1 \cdot a = a$ (there exists an identity element for $\cdot$);
(iii) $\forall a \in A,\ \exists a^{-1} \in A:\ a \cdot a^{-1} = a^{-1} \cdot a = 1$ (all the elements of A have inverses).

Definitions 9. Let φ be an operation on the set A and $B \subseteq A$. We say that B **is closed under** φ if

$$b_1, b_2 \in B \Rightarrow \varphi(b_1, b_2) \in B.$$

If B is closed under φ, one can define an operation on B as follows:

$$\varphi' : B \times B \to B,\ \varphi'(b_1, b_2) = \varphi(b_1, b_2).$$

We call φ' the **operation induced** by φ on B or, briefly, the **induced operation**. Most of the time, we denote it also by φ.

Remarks 10. a) Let φ be an operation on the set A, $B \subseteq A$ closed under φ and let φ' be the induced operation on B. If φ is associative or commutative, then φ' is associative or commutative, respectively.
b) Let φ_1 and φ_2 be operations on A, let $B \subseteq A$ be closed under φ_1 and φ_2, and let φ_1' and φ_2' be the operations induced by φ_1 and φ_2 on B, respectively. If φ_1 is distributive with respect to φ_2, i.e.

$$\varphi_1(a_1, \varphi_2(a_2, a_3)) = \varphi_2(\varphi_1(a_1, a_2), \varphi_1(a_1, a_3)), \forall a_1, a_2, a_3 \in A,$$

then φ_1' is distributive with respect to φ_2'.
c) The existence of an identity element is not always preserved by induced operations. For instance, $\mathbb{N}^*$ is closed in $(\mathbb{N}, +)$, but $(\mathbb{N}^*, +)$ has no identity element.

Definition 11. Let $(G, \cdot)$ be a group. A subset $H \subseteq G$ is called a **subgroup of** G if:
i) H is closed under the operation of $(G, \cdot)$, that is,

$$\forall x, y \in H\,, \quad x \cdot y \in H\,;$$

ii) H is a group with respect to the induced operation.

Examples 12. a) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are subgroups of $(\mathbb{C}, +)$, $\mathbb{Z}$, $\mathbb{Q}$ are subgroups of $(\mathbb{R}, +)$ and $\mathbb{Z}$ is a subgroup of $(\mathbb{Q}, +)$.
b) $\mathbb{Q}^*$, $\mathbb{R}^*$ are subgroups of $(\mathbb{C}^*, \cdot)$ and $\mathbb{Q}^*$ is a subgroup of $(\mathbb{R}^*, \cdot)$.
c) $\mathbb{N}$ is closed in $(\mathbb{Z}, +)$, but it is not a subgroup.
d) Every non-trivial group $(G, \cdot)$ has two subgroups, namely $\{1\}$ and G. Any other subgroup of $(G, \cdot)$ is called **proper subgroup**.

Definition 13. Let $(G, *)$, $(G', \perp)$ be two groups. A map $f : G \to G'$ is called **homomorphism** (or **morphism**) if

$$f(x_1 * x_2) = f(x_1) \perp f(x_2),\ \forall\ x_1, x_2 \in G.$$

A bijective homomorphism is called **isomorphism**. A homomorphism of $(G, *)$ into itself is called **endomorphism** of $(G, *)$. An isomorphism al lui $(G, *)$into itself is called **automorphism** of $(G, *)$. If there exists an isomorphism $f : G \to G$, we say that the groups $(G, *)$ and $(G', \perp)$ are isomorphic and we denote this by $G \simeq G'$ or $(G, *) \simeq (G', \perp)$.

Let us come back to the multiplicative notation.

Theorem 14. Let $(G,\cdot)$ and $(G',\cdot)$ be groups, and let 1 and $1'$, respectively, be the identity element of $(G,\cdot)$ and $(G',\cdot)$, respectively. If $f : G \to G'$ is a group homomorphism, then:
(i) $f(1) = 1'$;
(ii) $[f(x)]^{-1} = f(x^{-1})$, $\forall x \in G$.

Proof.

$\square$

Definition 15. Let R be a set. A structure $(R,+,\cdot)$ with two operations is called:
(1) **ring** if $(R,+)$ is an Abelian group, $\cdot$ is associative and the distributive laws hold (that is, $\cdot$ is distributive with respect to $+$).
(2) **unitary ring** if $(R,+,\cdot)$ is a ring and there exists a multiplicative identity element.

Definition 16. Let $(R,+,\cdot)$ be e unital ring. An element $x \in R$ which has an inverse $x^{-1} \in R$ is called **unit**. The ring $(R,+,\cdot)$ is called **division ring** if it is a unitary ring, $|R| \geq 2$ and any $x \in R^*$ is a unit. A commutative division ring is called **field**.

Definition 17. Let $(R,+,\cdot)$ be a ring. An element $x \in R^*$ is called **zero divisor** if there exists $y \in R^*$ such that

$$x \cdot y = 0 \text{ or } y \cdot x = 0.$$

We say that R is an **integral domain** if $R \neq \{0\}$, R is unitary, commutative and has no zero divisors.

Remarks 18. (1) Notice that $x \in R^*$ is not a zero divisor iff

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

(2) A ring R has no zero divisors if and only if

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

(3) $(R,+,\cdot)$ is a division ring if and only if it satisfies the following conditions:
i) $(R,+)$ is an Abelian group;
ii) R^* is closed in $(R,\cdot)$ and $(R^*,\cdot)$ is a group;
iii) $\cdot$ is distributive with respect to $+$.
(4) The fields have no zero divisors. Moreover, every field is an integral domain.

Examples 19. (a) $(\mathbb{Z},+,\cdot)$ is an integral domain, but it is not a field. Its units are -1 and 1.
(b) $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ are fields.
(c) Let $\{0\}$ be a single element set and let both $+$ and $\cdot$ be the only operation on $\{0\}$, defined by $0+0=0$ and $0\cdot 0=0$. Then $(\{0\},+,\cdot)$ is a commutative unitary ring, called the **trivial ring** (or **zero ring**). The multiplicative identity element is, of course, 0, hence we can write $1=0$. As matter of fact, this equality characterize the trivial ring.

Remark 20. 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 21. 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 22. 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 23. 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.

□

Definition 24. 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 25. (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 and Remark 10 b).

(b) A ring R may have subrings with or without (multiplicative) identity, as we will see in a forthcoming example.

Definition 26. 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 27. (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 28. (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 29. 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 30. 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 31. (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 32. 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 33. 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.

$\square$

Remark 34. Any non-zero homomorphism between two fields is a unitary homomorphism.

Indeed, ...

The polynomial ring over a field

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

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

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

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

Theorem 35. $K^{\mathbb{N}}$ 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

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

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

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

Theorem 36. 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.

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

$$f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \tag{4}$$

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

We can rewrite

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

The elements of $K[X]$ are called **polynomials over** K, and if $f = a_0 + a_1X + \cdots + a_nX^n$ 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

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

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

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

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

Theorem 38. (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 $r_1 = r$. $\square$

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

Corollary 39. 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 40. Let K be a field. The element $c \in K$ is a root of f if and only if $(X - c) \mid f$.

Corollary 41. 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.