# Abstract Algebra

**Ngo Dinh Hy, Nguyen Van Quang Huy, Le Phuc Lu**

Department of Knowledge Engineering - DACLab
VNUHCM - University of Science

{*ndhy, nvqhuy,lplu*}*@fit.hcmus.edu.vn*

August 13, 2023

# Contents

# Contents

**Definition (Binary Operations)**

A binary operation $\circ$ on a set $S$ is a function that maps the elements of the set $S \times S$ into the set $S$.

$$\circ : S \times S \to S$$

Let $a, b \in S$. Then, the value of the operation $\circ$ at $(a, b)$ can be written as $a \circ b$.

**Examples (Binary Operations):** The addition and multiplication on the set $\mathbb{Z}, \mathbb{R}, \mathbb{C}$, *etc.* are binary operations.

**Definition (Groups)**

Let $S$ be a set and $\circ$ be a binary operation on $S$. Then, a non-empty set $G \subseteq S$ together with the operation $\circ$, denoted by $(G, \circ)$, is called a group iff it satisfies the following properties:

- Closure: $\forall x, y \in G, x \circ y \in G$.
- Associativity: $\forall x, y, z \in G, x \circ (y \circ z) = (x \circ y) \circ z$.
- Identity element: $\exists e \in G, \forall x \in G, e \circ x = x \circ e = x$.
  Then, $e$ is called the identity element of $G$.
- Inverse element: Let $e$ be the identity element of $G$.

$$\forall x \in G, \exists x^{-1} \in G, x \circ x^{-1} = x^{-1} \circ x = e.$$

Then, $x^{-1}$ is called the inverse element of $x$.

**Examples (Groups)**

$\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are groups under the additive operation $+$. Moreover, they are abelian (commutative), i.e. $a + b = b + a, \forall a, b$.

**Remarks (Groups)**

Let $(G, \circ)$ be a group. Then,

- There are no two distinct identity elements $e$.
- For all $x \in G$, there are no two distinct inverse elements $x^{-1}$.

**Additive Group of Integers Modulo $n$**

Let $\overline{a}_n = \{\, a + kn \mid k \in \mathbb{Z} \,\}$. Therefore, $\overline{a}_n = \overline{b}_n \iff a = b \pmod{n}$.
Let $\mathbb{Z}_n = \{\, \overline{0}_n, \ldots, \overline{n-1}_n \,\}$ and $\oplus$ be a binary operation on $\mathbb{Z}_n$ such that

$$\begin{aligned} \oplus : \mathbb{Z}_n \times \mathbb{Z}_n &\to \mathbb{Z}_n \\ \left(\overline{a}_n, \overline{b}_n\right) &\mapsto \overline{a}_n \oplus \overline{b}_n = \overline{a+b}_n \end{aligned}$$

Then, $(\mathbb{Z}_n, \oplus)$ is the additive group of integers modulo $n$.

*Question:* Prove that the above statement is true?

**Multiplicative Group of Integers Modulo $n$**

Let $\mathbb{Z}_n^* = \{\, \overline{a}_n \mid gcd(a, n) = 1 \,\}$. Thus, $\overline{0}_n \notin \mathbb{Z}_n^*$ and $\mathbb{Z}_n^* \subset \mathbb{Z}_n$.
Let $\otimes$ be a binary operation on $\mathbb{Z}_n$ such that

$$\otimes : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$
$$\left(\overline{a}_n, \overline{b}_n\right) \mapsto \overline{a}_n \otimes \overline{b}_n = \overline{a \times b}_n$$

Then, $(\mathbb{Z}_n^*, \otimes)$ is the multiplicative group of integers modulo $n$.

*Question:*

1. Prove that the above statement is true?
2. Why is $(\mathbb{Z}_n, \otimes)$ not a group?

**Remarks (Additive and Multiplicative Groups of Integers Modulo $n$)**

- If $n$ is prime, then $gcd(a, n) = 1 \iff n \nmid a$. Thus, $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{ \overline{0}_n \}$, that means every element except $\overline{0}_n$ has its inverse one. That allows addition, subtraction, multiplication, and division to be well-defined on $\mathbb{Z}_n$. Therefore, with the finiteness property, $\mathbb{Z}_n$ is usually used in numerous computing-related applications, especially cryptography.
- In the case $n$ is composite, several cryptosystems are proposed based on multiplicative groups. A typical example is RSA, which uses the group $\mathbb{Z}_{pq}^*$ where $p$ and $q$ are prime numbers.

**Definition (Subgroups)**

Let $(G, \circ)$ be a group. Then, a subset $H$ of $G$, i.e. $H \subset G$, is called a subgroup of $G$ iff $(H, \circ)$ is a group.

**Remarks (Subgroups):**

- If $e$ is the identity element of $G$, then $\{ e \}$ is a subgroup of $G$.
- If $e$ is the identity element of $G$ and $H$ is a subgroup of $G$, then $e \in H$.

**Examples (Subgroups):**

- $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.
- Let $G = \{ \overline{1}_5, \overline{2}_5, \overline{3}_5, \overline{4}_5 \}$ and $H = \{ \overline{1}_5, \overline{4}_5 \}$. Then, $(H, \otimes)$ is a subgroup of $(G, \otimes)$.

**Definition (Cyclic Groups)**

Let $(G, \circ)$ be a group and $g$ be an element of $G$ with the identity element $e$ and the inverse element $g^{-1}$. Then,

$$g^k = \begin{cases} \underbrace{g \circ \cdots \circ g}_{k \text{ times}}, & k \in \mathbb{Z}^+ \\ e, & k = 0 \\ \underbrace{g^{-1} \circ \cdots \circ g^{-1}}_{-k \text{ times}}, & k \in \mathbb{Z}^- \end{cases}$$

$(G, \circ)$ is a cyclic group with the generator $g$ iff

$$\forall a \in G, \exists k \in \mathbb{Z}, a = g^k$$

We use $\langle g \rangle$ to denote the cyclic group generated by $g$.

**Examples (Cyclic Groups)**

- $(\mathbb{Z}, +)$ is a cyclic group generated by 1.
- $G = \{\, \overline{1}_5, \overline{2}_5, \overline{3}_5, \overline{4}_5 \,\}$. Then, $(G, \otimes)$ is a cyclic group generated by $\overline{2}_5$.

**Remarks (Cyclic Groups)**

- For every element $a$ of the group $G$, the cyclic group $\langle a \rangle$ is a subgroup of $G$.
- All cyclic groups $(G, \circ)$ are commutative, i.e. $a \circ b = b \circ a, \forall a, b \in G$.
- All the additive groups $(\mathbb{Z}_n, \oplus)$ are cyclic.

**Primitive Roots of Unity Modulo $n$**

The multiplicative group $(\mathbb{Z}_n^*, \otimes)$ is cyclic iff $n = 2, 4, p^k, 2p^k$ where $p$ is an odd prime number and $k \in \mathbb{Z}$.
If the multiplicative group $(\mathbb{Z}_n^*, \otimes)$ is cyclic, then its generator is called a primitive root of unity modulo $n$.

**Remarks**

- Unlike additive groups, some but not all multiplicative ones are cyclic.
- In the case $n$ is prime, the multiplicative groups are applied in cryptosystems in the form of Diffie-Hellman problem. More generally, any cyclic groups can also be used in this problem instead of only multipicative ones, for example the group of points on an elliptic curve.

**Definition (Order of a group)**

Let $(G, \circ)$ be a group. If $(G, \circ)$ is finite, then the order of $(G, \circ)$ is the number of its elements. If $(G, \circ)$ is not finite, then the order of $(G, \circ)$ is infinite.
The order of $(G, \circ)$ is denoted by $ord(G)$ or $|G|$.

**Definition (Order of an element)**

Let $(G, \circ)$ be a group and $a$ be an element of $G$. Then, the order of the element $a$ is the order of the cyclic group $\langle a \rangle$ generated by $a$.
The order of $a$ is denoted by $ord(a)$ or $|a|$.

**Remarks (Order of groups and elements)**

- If the order of a group is finite, then the order of every subgroup is finite. Otherwise, if the order of a subgroup is infinite, the the order of the group is infinite.
- If the order of a group is infinite, then the order of a subgroup is not necessarily infinite.
- The order of an element $a$ is the order of the cyclic group $\langle a \rangle$. Moreover, $\langle a \rangle$ is an subgroup. Therefore, the above remarks also holds true for the order of elements.
- Let $G$ be a group with the identity element $e$, and $a$ be an element of $G$. If $|a| = k$, then
  - $a^k = e$.
  - $a^h \neq e, \forall h \in \{1, \ldots, k-1\}$.

**Examples (Order of groups and elements)**

- $|(\mathbb{Z}, +)| = \infty$.
- $|(\mathbb{Z}_n, \oplus)| = n$.
- $|(\mathbb{Z}_n^*, \otimes)| = \varphi(n)$ where $\varphi(n)$ is the number of integers $k$ coprime with $n$ in the range $0 < k < n$, i.e. $gcd(k, n) = 1$.
- Let $\overline{a} = \{ a + k \mid k \in \mathbb{Z} \}$, $\frac{\mathbb{R}}{\mathbb{Z}} = \{ \overline{a} \mid 0 \leq a < 1 \}$, and $\oplus$ be the following operation:

$$\oplus : \frac{\mathbb{R}}{\mathbb{Z}} \times \frac{\mathbb{R}}{\mathbb{Z}} \to \frac{\mathbb{R}}{\mathbb{Z}}$$
$$(\overline{x}, \overline{y}) \mapsto \overline{x} \oplus \overline{y} = \overline{x + y}$$

Then, $\left|\left(\frac{\mathbb{R}}{\mathbb{Z}}, \oplus\right)\right| = \infty$, while $\left|\overline{\frac{1}{n}}\right| = n$.

**Theorem (Lagrange's Theorem)**

Let $G$ be a finite group, and $H$ be a subgroup of $G$. Then, $|H| \mid |G|$.

**Remarks (Lagrange's Theorem)**

- Let $p$ be a prime number. Then, all groups which has $p$ elements are cyclic where all elements except the identity one are generators.
- Let $G$ be a group with the identity element $e$. If $|G| = k$, then $a^k = e, \forall a \in G$.
- This theorem can be used to prove two other well-known ones: Fermat's Little Theorem and Euler's Theorem.

**Fermat's Little Theorem**

If $p$ is a prime number, then for all integer $a$ coprime with $p$, i.e. $gcd(a, p) = 1$,

$$a^{p-1} = 1 \pmod{p}.$$

**Euler's Theorem**

Let $a$ and $n$ be integers such that $gcs(a, n) = 1$. Then,

$$a^{\varphi(n)} = 1 \pmod{n}$$

where $\varphi(n)$, Euler's Phi Function, is the number of integers $k$ coprime with $n$ in the range $0 < k < n$, i.e. $gcd(k, n) = 1$.

**Properties (Euler's Phi Function)**

- If $gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.
- Let $p$ be a prime number. Then, $\varphi(p^k) = p^k - p^{k-1}$.

**Formula (Euler's Phi Function)**

Let $n = p_1^{a_1} \dots p_k^{a_k}$ where $p_1, \dots, p_k$ are distinct prime numbers. Then, the formula of Euler's Phi Function is as follows:

$$\varphi(n) = \prod_{i=1}^{k} (p_i^{a_i} - p_i^{a_i - 1}) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

**Remark (Euler's Phi Function)**

The first property can be proved by constructing a bijective function from $\mathbb{Z}_{mn}^*$ to $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$, while the second one can be proved by ordinary counting methods.

**Remarks (Fermat's Little Theorem and Euler's Theorem)**

The theorems are applied in several cryptosystems:

- RSA cryptosystems are constructed based on multiplicative groups $\mathbb{Z}_{pq}^*$ where $p$ and $q$ are prime numbers. Therefore, the order of $\mathbb{Z}_{pq}^*$ is $\varphi(pq) = (p-1)(q-1)$, that is used to generate or recover keys. Thus, the security of RSA cryptosystems requires computing $\varphi(pq)$ is hard when only $n = pq$ is known. That's why Integer Factorization Assumption is necessary.
- Regarding Diffie-Hellman Key Exchange and ElGamal, cryptosystems use cyclic multiplicative groups $\mathbb{Z}_p^*$ with the prime number $p$. Thus, Fermat's Little Theorem plays an important role in these cryptosystems, as well as several operations like modular inverse.

## Fast Exponentiation Algorithm

Let $(G, \circ)$ be a group with the identity element $e$, $a$ be an element of $G$, and $n$ be a non-negative integer. Find the element $a^n \in G$.

1. $b \leftarrow e$.
2. Loop until $n = 0$.
   2.1. If $n$ is odd, i.e. $n = 1 \pmod 2$, then $b \leftarrow a \circ b$.
   2.2. $a \leftarrow a \circ a$; $n \leftarrow \left\lfloor \frac{n}{2} \right\rfloor$.
3. Return $b$.

## Remarks

- Fermat's Little Theorem and Euler's Theorem require exponential operations. Thus, Fast Exponentiation Algorithm is important to compute them efficiently.
- If $a^n = e$, then $a^{-1} = a^{n-1}$. Thus, Fast Exponentiation Algorithm is also used to compute the inverse element.

# Contents

**Definition (Monoids)**

Let $S$ be a set and $\cdot$ be a binary operation on $S$. Then, a non-empty set $R \subseteq S$ together with the operation $\cdot$, denoted by $(R, \cdot)$, is called a monoid iff it satisfies the following properties:

- Closure: $\forall x, y \in R, x \cdot y \in R$.
- Associativity: $\forall x, y, z \in R, x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
- Identity element: $\exists 1 \in R, \forall x \in R, 1 \cdot x = x \cdot 1 = x$.
  Then, 1 is called the identity element of $R$.

**Remark (Monoids)**

In other words, monoids are groups without inverse elements.

**Definition (Rings)**

Let $S$ be a set and $+$, $\cdot$ be two binary operations on $S$. Then, a non-empty set $R \subseteq S$ together with the operations $+$ and $\cdot$, denoted by $(R, +, \cdot)$, is called a ring iff it satisfies the following properties:

- $(R, +)$ is a group where the additive identity element is denoted by 0, the additive inverse element of $x \in R$ is denoted by $-x$.
- $(R, \cdot)$ is a monoid where the multiplicative identity element is denoted by 1.
- Multiplicative Distribution over Addition: $\forall a, b, c \in R$,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
$$(b + c) \cdot a = (b \cdot a) + (c \cdot a)$$

**Examples (Rings)**

$\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are rings under the additive operation $+$ and the multiplicative operation $\times$.

**Remarks I (Rings)**

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

- There are no two distinct additive identity elements 0.
- For all $x \in R$, there are no two distinct additive inverse elements $-x$.
- There are no two distinct multiplicative identity elements 1.
- $x \cdot 0 = 0 \cdot x = 0, \forall x \in R$.
- If $-1$ is the additive inverse element of 1, then $\forall x \in R$, $x \cdot (-1) = (-1) \cdot x = -x$ is the additive inverse element of $x$.
- The group $(R, +)$ is abelian (commutative), i.e. $a + b = b + a, \forall a, b \in R$.

**Remarks II (Rings)**

- The commutative property of $(R, +)$ is provable. Therefore, for convenience, $(R, +)$ is stated as an abelian group in some definitions of rings.
- If $0 = 1$, then $R = \{ 0 \}$ which is called the zero ring. Thus, only the case $0 \neq 1$ is considered.
- The concept of multiplicative operations can be considered as an extension from groups to rings. The extension is necessary, especially for the ring of real numbers. Multiplications of real numbers is too complicated to be represented as additions, therefore multiplications should be independent of additions, that forms rings.
- Rings play an important role in the definition of several later algebraic structures, such as fields or polynomial rings, used in Elliptic-curve Cryptography.

**Definition (Commutative Rings)**

Let $(R, +, \cdot)$ be a ring. Then, $(R, +, \cdot)$ is commutative iff the multiplicative operation $\cdot$ is commutative, i.e. $a \cdot b = b \cdot a, \forall a, b \in R$.

**Definition (Sequences)**

A sequence in a set $S$ is a function $\sigma : \mathbb{N} \to S$, that means $\sigma = (s_0, s_1, \ldots, s_i, \ldots)$ where $s_0, s_1, \ldots, s_i, \ldots \in S$.

**Definition (Polynomials)**

Let $(R, +, \cdot)$ be a commutative ring with the additive identity element 0. A sequence $\sigma = (s_0, s_1, \ldots, s_i, \ldots)$ in $R$ is called a polynomial iff there is an integer $n \geq 0$ such that $s_i = 0, \forall i > n$, that means

$$\sigma = (s_0, s_1, \ldots, s_n, 0, 0, \ldots)$$

**Remarks (Polynomials)**

- $\sigma = (0, 0, \ldots)$ is called the zero polynomial, and denoted by $\sigma = 0$.
- If a polynomial $\sigma \neq 0$, there is an integer $n \geq 0$ such that $s_n \neq 0$ and $s_i = 0, \forall i > n$. Then, the degree of $\sigma$, denoted by $\deg(\sigma)$, is $n$.
- The zero polynomial 0 has no degree.
- Two polynomials $\sigma = (s_0, s_1, \ldots)$ and $\tau = (t_0, t_1, \ldots)$ are equal iff $s_i = t_i, \forall i \in \mathbb{N}$.
- The set of all polynomials in a commutative ring $R$ is denoted by $R[X]$.

**Definition (Polynomial Additions and Multiplications)**

Let $\sigma = (s_0, s_1, \ldots, s_i, \ldots)$ and $\tau = (t_0, t_1, \ldots, t_i, \ldots)$ be two polynomials in a commutative ring. $(R, +, \cdot)$. Then, the additive operation $\oplus$ and the multiplicative operation $\odot$ over $R[X]$ are defined as follows:

$$\begin{aligned}
\oplus : R[X] \times R[X] &\to R[X] \\
(\sigma, \tau) &\mapsto \sigma \oplus \tau = (s_0 + t_0, s_1 + t_1, \ldots, s_i + t_i, \ldots) \\
\odot : R[X] \times R[X] &\to R[X] \\
(\sigma, \tau) &\mapsto \sigma \odot \tau = (a_0, a_1, \ldots, a_i, \ldots)
\end{aligned}$$

where $a_k = \sum_{i+j=k} s_i t_j = \sum_{i=0}^{k} s_i t_{k-i}$.

**Theorem (Polynomial Rings)**

Let $(R, +, \cdot)$ be a commutative ring. Then, $(R[X], \oplus, \odot)$ forms a ring called the ring of polynomials over $R$.

## Remarks (Polynomial Rings)

- Polynomial rings are commutative.
- The additive identity element is the zero polynomial 0.
- The multiplicative identity element is the polynomial $1 = (1, 0, 0, \ldots)$.
- The additive inverse element of $\sigma = (s_0, s_1, \ldots, s_n, 0, 0, \ldots)$ is $-\sigma = (-s_0, -s_1, \ldots, -s_n, 0, 0, \ldots)$.
- Let $\sigma = (s_0, s_1, \ldots, s_n, 0, 0, \ldots)$ be a polynomial and $f_\sigma$ be a function satisfying

$$f_\sigma : R \to R$$
$$a \mapsto s_0 + s_1 \cdot a + s_2 \cdot a^2 + \cdots + s_n \cdot a^n$$

$$\text{Then, } \begin{cases} f_{\sigma \oplus \tau}(a) = f_\sigma(a) + f_\tau(a) \\ f_{\sigma \odot \tau}(a) = f_\sigma(a) \cdot f_\tau(a) \end{cases} , \forall \sigma, \tau \in R[X], a \in R.$$

# Contents

# Fields

**Definition (Fields)**

Let $(F, +, \cdot)$ be a commutative ring with the additive identity element 0. Then, $(F, +, \cdot)$ is called a field iff $(F \setminus \{0\}, \cdot)$ is a group.

**Examples (Fields)**

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields under the additive operation $+$ and the multiplicative operation $\cdot$.
- $\mathbb{Z}_p$ with the prime number $p$ are fields under the additive operation $\oplus$ and the multiplicative operation $\odot$ of integers modulo $p$.

**Remarks I (Fields)**

- $1 \in F \setminus \{0\}$ and $0 \notin F \setminus \{0\}$, so $1 \neq 0$. Therefore, the zero ring is not a field.
- The multiplicative inverse element of a nonzero element $x$ is denoted by $x^{-1}$.
- Let $a, b \in F$. If $a \cdot b = 0$, then $a = 0$ or $b = 0$.

**Remarks II (Fields)**

- Several infinite fields are $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. However, finite fields have important applications, especially for computer science and cryptography, because computers can fully and accurately express these fields, that can only be achieved for infinite fields by approximation methods.
- Several properties of a finite field $(F, +, \cdot)$:
  - $\exists! p \in \mathbb{Z}^+, \forall a \in F \setminus \{0\}, |a|_+ = p$. Moreover, $p$ is a prime number.
  - $\langle 1 \rangle_+$ is a subfield of $F$. Moreover, $\left|\langle 1 \rangle_+\right| = |a|_+ = p$ is a prime number.
  - The prime number $p$ mentioned above is called the characteristic of $F$.

**Definition (Vector Spaces)**

A vector space over a field $(F, +, \cdot)$ is a non-empty set $V$ together with two binary operations $\oplus : V \times V \to V$ and $\odot : F \times V \to V$ such that:

- $\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V, \mathbf{u} \oplus (\mathbf{v} \oplus \mathbf{w}) = (\mathbf{u} \oplus \mathbf{v}) \oplus \mathbf{w}$.
- $\forall \mathbf{u}, \mathbf{v} \in V, \mathbf{u} \oplus \mathbf{v} = \mathbf{v} \oplus \mathbf{u}$.
- $\exists \mathbf{0} \in V, \forall \mathbf{u} \in V, \mathbf{u} \oplus \mathbf{0} = \mathbf{0} \oplus \mathbf{u} = \mathbf{u}$.
- $\forall \mathbf{u} \in V, \exists -\mathbf{u} \in V, \mathbf{u} \oplus (-\mathbf{u}) = (-\mathbf{u}) \oplus \mathbf{u} = \mathbf{0}$.
- $\forall \mathbf{u} \in V, \forall a, b \in F, a \odot (b \odot \mathbf{u}) = (a \cdot b) \odot \mathbf{u}$.
- $\forall \mathbf{u} \in V, 1 \odot \mathbf{u} = \mathbf{u}$ where 1 is the multiplicative identity element of $F$.
- $\forall \mathbf{u}, \mathbf{v} \in V, \forall a \in F, a \odot (\mathbf{u} \oplus \mathbf{v}) = (a \odot \mathbf{u}) \oplus (a \odot \mathbf{v})$.
- $\forall \mathbf{u} \in V, \forall a, b \in F, (a + b) \odot \mathbf{u} = (a \odot \mathbf{u}) \oplus (b \odot \mathbf{u})$.

## Remarks (Fields and Vector Spaces)

- A field is a vector space over any subfield.
- For a finite field $F$, $F$ is a finite-dimensional vector space over $\langle 1 \rangle_+$. Therefore, the number of elements in $F$ has the form of $p^n$ with a prime number $p$ and a positive integer $n$.

## Examples (Fields and Vector Spaces)

- The field of complex numbers $\mathbb{C}$ is a two-dimensional vector space over the field of real numbers $\mathbb{R}$ which is a subfield of $\mathbb{C}$.
- The field $F = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$ is a two-dimensional vector space over the field of rational numbers $\mathbb{Q}$ which is a subfield of $F$. The multiplicative inverse element of $a + b\sqrt{2}$ is

$$\frac{1}{a^2 - 2b^2}(a - b\sqrt{2}).$$

## The ring of polynomials over a field $F$

- Let $f$ and $g$ be two polynomials in $F[X]$ with the degree of $\deg(f)$ and $\deg(g)$ respectively. Then, $\deg(fg) = \deg(f) + \deg(g)$.
- Let $f$ and $g$ be two polynomials in $F[X]$. Then,

$$fg = 0 \iff f = 0 \vee g = 0.$$

- Let $f$ be a polynomial in $F[X]$ with the degree of $\deg(f) > 0$. Then, there is no polynomial $g$ in $F[X]$ such that $fg = 1$.
- Let $f$ be a polynomial in $F[X]$ with the degree of $\deg(f) > 0$. Then, $\forall g \in F[X], \exists! q, r \in F[X], g = fq + r$ where $r = 0$ or $\deg(r) < \deg(f)$.
- Let $f$ be a nonzero polynomial in $F[X]$. A polynomial $g \in F[X]$ satisfying $f \mid g$ iff $\exists k \in F[X], g = kf$. Therefore, two polynomials $a, b \in F[X]$ satisfying $a = b \pmod{f}$ iff $\exists k \in F[X], a - b = kf$.

**The ring of polynomials over a field $F$**

- Let $f$ be a non-constant polynomial in $F[X]$, i.e. $\deg(f) > 0$. Then, $f$ is called irreducible iff there are no non-constant polynomials $p$ and $q$ in $F[X]$, i.e. $\deg(p), \deg(q) > 0$, such that $f = pq$.
- For all non-constant polynomial $f \in F[X]$, i.e. $\deg(f) > 0$, there exists an irreducible polynomial $p \in F[X]$ such that $p \mid f$.
- Let $f$ be a polynomial in $F[X]$ with the degree of $\deg(f) = n$, i.e. $f = (s_0, \ldots, s_n, 0, \ldots)$ where $s_n \neq 0$. Then, $f$ is called monic iff $s_n = 1$.

**Bézout's lemma and GCD for polynomials over a field $F$**

Let $a$ and $b$ be two nonzero polynomials in $F[X]$ and
$S = \{ ax + by \mid x, y \in F[X] \}$.
Let $d$ be a monic polynomial in $S$ such that $\deg(d) \leq \deg(f), \forall f \in S$.
Then, we have the following results:

- $(d \mid a)$ and $(d \mid b)$.
- $\forall f \in F[X], (f \mid a) \wedge (f \mid b) \implies f \mid d$.
- $d$ is unique.

Therefore, $d$ is called $gcd(a, b)$.

**The ring of polynomials over a field $F$**

- The Euclidean algorithm and the extended version can be applied for polynomials over a field $F$.
- Let $p \in F[X]$ be an irreducible polynomial and $a \in F[X]$ be a nonzero polynomial. Then, $gcd(a, p) = 1$ or $gcd(a, p) = kp, k \in F$. Moreover, if $\deg(a) < \deg(p)$, then $gcd(a, p) = 1$.

## Fields and Quotient Rings

- Let $F$ be a field, $F[X]$ be a ring of polynomials over $F$, and $p$ is a nonzero polynomial in $F[X]$.
  Let $\pi(a) = \{ x \in F[X] \mid x = a \pmod{p} \}$.
  Then, $F[X]/p = \{ \pi(x) \mid x \in F[X] \}$ can form a ring which is called a quotient ring of $F[X]$ modulo $p$.
- If $p$ is irreducible, then the quotient ring quotient ring $F[X]/p$ becomes a field.
- If $F$ is a finite field of size $q$ and $p$ is an irreducible polynomial of degree $n$, then $F[X]/p$ is a finite field of size $q^n$.

**Remarks (Finite Fields)**

- Every finite subgroup of the multiplicative group of a field is cyclic. Therefore, every subgroup of the multiplicative group of a finite field is cyclic.
- For all prime number $p$ and all positive integer $n$, there always exists a field having $p^n$ elements.
- For all prime number $p$ and all positive integer $n$, there always exists an irreducible polynomial of degree $n$ over $\mathbb{Z}_p$.
- Let $R$ be a nonzero finite ring.
  - If $\forall a, b \in R, ab = 0 \iff (a = 0) \vee (b = 0)$, then $\forall x \in R \setminus \{0\}, \exists x^{-1} \in R, xx^{-1} = x^{-1}x = 1$.
  - If $\forall x \in R \setminus \{0\}, \exists x^{-1} \in R, xx^{-1} = x^{-1}x = 1$, then $\forall a, b \in R, ab = ba$. Therefore, $R$ is a finite field.

**Example (Finite Fields)** Multiplication table of $\mathbb{F}_9 = \mathbb{Z}_3/(X^2+1)$

| | $1$ | $2$ | $X$ | $X+1$ | $X+2$ | $2X$ | $2X+1$ | $2X+2$ |
|---|---|---|---|---|---|---|---|---|
| $1$ | $1$ | $2$ | $X$ | $X+1$ | $X+2$ | $2X$ | $2X+1$ | $2X+2$ |
| $2$ | $2$ | $1$ | $2X$ | $2X+2$ | $2X+1$ | $X$ | $X+2$ | $X+1$ |
| $X$ | $X$ | $2X$ | $2$ | $X+2$ | $2X+2$ | $1$ | $X+1$ | $2X+1$ |
| $X+1$ | $X+1$ | $2X+2$ | $X+2$ | $2X$ | $1$ | $2X+1$ | $2$ | $X$ |
| $X+2$ | $X+2$ | $2X+1$ | $2X+2$ | $1$ | $X$ | $X+1$ | $2X$ | $2$ |
| $2X$ | $2X$ | $X$ | $1$ | $2X+1$ | $X+1$ | $2$ | $2X+2$ | $X+2$ |
| $2X+1$ | $2X+1$ | $X+2$ | $X+1$ | $2$ | $2X$ | $2X+2$ | $X$ | $1$ |
| $2X+2$ | $2X+2$ | $X+1$ | $2X+1$ | $X$ | $2$ | $X+2$ | $1$ | $2X$ |