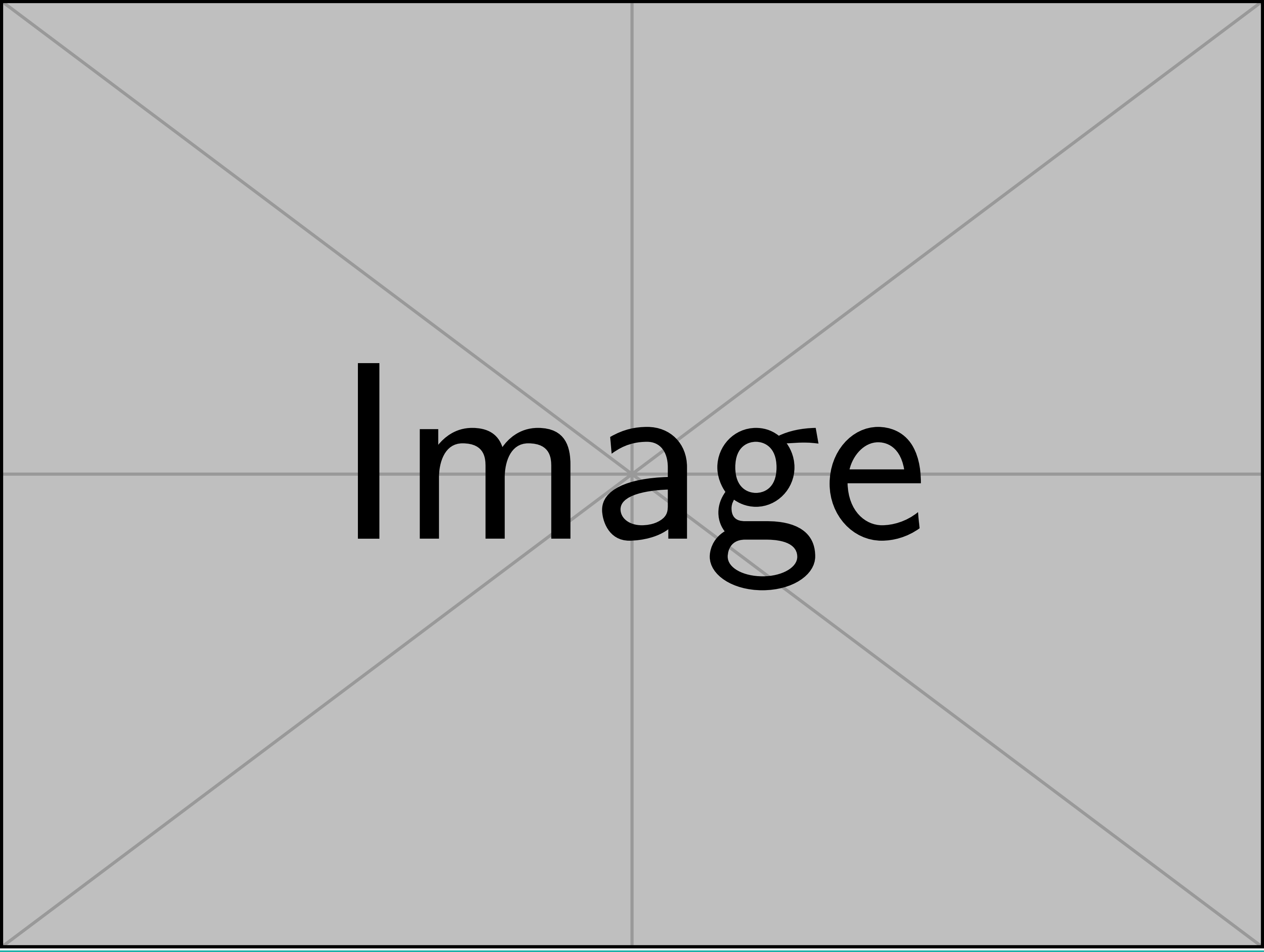


Polynôme

Author: CatMono

Date: September, 2025

Version: 0.1

Contents

Preface ii

Chapter 1 Preliminaries 1

Chapter 2 Univariate Polynomial Ring 2

2.1 Univariate Polynomials 2
2.2 Division 2
2.3 Greatest Common Divisor and Relatively Prime 2
2.4 Least Common Multiple 3

Chapter 3 Factorization and Roots 4

3.1 Irreducible Polynomials 4
3.2 Polynomials with Rational Coefficients 4
3.3 Relation between Roots and Coefficients 5
3.4 Root of Unity 6

Chapter 4 Integral Valued Polynomials 8

4.1 Lagrange Interpolation Polynomial 8

Chapter 5 Multivariate Polynomial 9

5.1 Symmetric Polynomial 9

Preface

This is the preface of the book…

Chapter 1 Preliminaries

Chapter 2 Univariate Polynomial Ring

2.1 Univariate Polynomials

2.2 Division

Theorem 2.1 (Euclidean Division (Division with Remainder))

Let $f(x), g(x) \in P[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in P[x]$ such that

$$f(x) = g(x) \cdot q(x) + r(x)$$

where $r(x) = 0$ or $\deg(r) < \deg(g)$.

♡

Definition 2.1 (Exact Division)

If there exists $h(x) \in P[x]$ such that $f(x) = g(x) \cdot h(x)$, we say that $g(x)$ divides $f(x)$ and write $g(x) \mid f(x)$. (In other words, the remainder $r(x) = 0$.)

♣

Property

Caution *In Euclidean division, $g(x) \neq 0$ is required. However, in the case of $g(x) \mid f(x)$, $g(x)$ can equal 0. In this situation, $f(x) = g(x)h(x) = 0 \cdot g(x) = 0$, meaning that the* ***zero polynomial can only divide the zero polynomial****.*

2.3 Greatest Common Divisor and Relatively Prime

¶ `Greatest Common Divisor`

Definition 2.2 (Greatest Common Divisor (GCD))

Let $f(x), g(x) \in P[x]$. A polynomial $d(x) \in P[x]$ is called a greatest common divisor of $f(x)$ and $g(x)$ if:

1. $d(x) \mid f(x)$ and $d(x) \mid g(x)$;
2. For any polynomial $h(x) \in P[x]$, if $h(x) \mid f(x)$ and $h(x) \mid g(x)$, then $h(x) \mid d(x)$.

The greatest common divisor of $f(x)$ and $g(x)$, whose leading coefficient is 1 (also called **monic**), is denoted as $(f(x), g(x))$.

♣

Property

Theorem 2.2 (Euclidean Algorithm)

For all $f(x), g(x) \in P[x]$, there exists $d(x) \in P[x]$, where $d(x)$ is a greatest common divisor of $f(x)$ and $g(x)$, and $d(x)$ can be expressed as a linear combination of $f(x)$ and $g(x)$, i.e., there exist $u(x), v(x) \in P[x]$ such that

$$d(x) = u(x)f(x) + v(x)g(x).$$

The converse proposition does not hold in general.

♡

¶ `Relatively Prime`

Definition 2.3 (Relatively Prime)

Two polynomials $f(x)$ and $g(x)$ in $P[x]$ are called relatively prime if $(f(x), g(x)) = 1$, meaning they have no common divisor other than the zero-degree polynomial (nonzero constant).

2.4 Least Common Multiple

Chapter 3 Factorization and Roots

3.1 Irreducible Polynomials

Definition 3.1 (Irreducible Polynomial)

A polynomial $p(x)$ of degree ≥ 1 over a field P is called an irreducible polynomial over the field P if it cannot be expressed as the product of two polynomials of lower degree than $p(x)$ over the field P. ♣

Proposition 3.1

For all $f(x), g(x) \in P[x]$, $p(x)$ is an irreducible polynomial in $P[x]$, which is equivalent to the following two propositions:

1. Either $p(x) \mid f(x)$ or $(p(x), f(x)) = 1$;
2. If $p(x) \mid f(x)g(x)$, then either $p(x) \mid f(x)$ or $p(x) \mid g(x)$.

Similarly, monic polynomial $p(x)$, with degree greater than 0, is a power of an irreducible polynomial over the field P if and only if for all $f(x), g(x) \in P[x]$,

1. Either $p(x) \mid f^m(x)$ $(m \in \mathbb{N}^*)$ or $(p(x), f(x)) = 1$;
2. If $p(x) \mid f(x)g(x)$, then either $p(x) \mid f^m(x)$ $(m \in \mathbb{N}^*)$ or $p(x) \mid g(x)$. ♠

3.2 Polynomials with Rational Coefficients

Definition 3.2 (Primitive Polynomial)

A polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with integer coefficients is called a **primitive polynomial** if the greatest common divisor of its coefficients is ± 1, i.e., $(a_n, a_{n-1}, \ldots, a_1, a_0) = \pm 1$. ♣

Lemma 3.1 (Gauß's Lemma)

The product of two primitive polynomials is also a primitive polynomial. ♡

With the help of Gauß's lemma, we can establish the following important theorem:

Theorem 3.1

If a polynomial $f(x)$ with integer coefficients is reducible over the field of rational numbers $\mathbb{Q}$, then it is also reducible over the ring of integers $\mathbb{Z}$. ♡

A corollary can be derived from this theorem:

Corollary 3.1

Let $f(x), g(x) \in \mathbb{Z}[x]$ be two polynomials, and $g(x)$ is primitive. If $f(x) = g(x)h(x)$, where $h(x) \in \mathbb{Q}[x]$, then $h(x) \in \mathbb{Z}[x]$. ♡

¶ `Searching and Judging of Rational Roots`

Now we can use the following theorem to search for rational roots of polynomials with integer coefficients:

Theorem 3.2 (Rational Root Theorem)

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. If $\frac{r}{s}$ (in lowest terms) is a rational root of $f(x)$, then $r \mid a_0$ and $s \mid a_n$.
Obviously, if $f(x)$ is monic, then any rational root must be an integer divisor of a_0.

Next, we can use the following theorem to judge whether a polynomial with integer coefficients is irreducible over the field of rational numbers:

Theorem 3.3 (Eisenstein's Criterion)

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. If there exists a prime number p such that:

1. $p \nmid a_n$;
2. $p \mid a_i$ for all $i = 0, 1, \ldots, n-1$;
3. $p^2 \nmid a_0$;

then $f(x)$ is irreducible over the field of rational numbers $\mathbb{Q}$.

3.3 Relation between Roots and Coefficients

Theorem 3.4 (Vièta's Formulas)

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial of degree n over field P, and let its n roots (counting multiplicities) be $r_1, r_2, \ldots, r_n$ in an extension field of P. Then the following relations hold:

$$\begin{aligned}
&r_1 + r_2 + \cdots + r_n = -\frac{a_{n-1}}{a_n},\\
&r_1 r_2 + r_1 r_3 + \cdots + r_{n-1} r_n = \frac{a_{n-2}}{a_n},\\
&\vdots\\
&r_1 r_2 \cdots r_n = (-1)^n \frac{a_0}{a_n}.
\end{aligned}$$

Using symmetric polynomial notation (5.1), Vièta's formulas can be expressed as:

$$\begin{aligned}
\sigma_1(r_1, r_2, \ldots, r_n) &= -\frac{a_{n-1}}{a_n},\\
\sigma_2(r_1, r_2, \ldots, r_n) &= \frac{a_{n-2}}{a_n},\\
&\vdots\\
\sigma_n(r_1, r_2, \ldots, r_n) &= (-1)^n \frac{a_0}{a_n},
\end{aligned}$$

that is,

$$\sigma_i(r_1, r_2, \ldots, r_n) = (-1)^i \frac{a_{n-i}}{a_n}, \quad i = 1, 2, \ldots, n.$$

3.4 Root of Unity

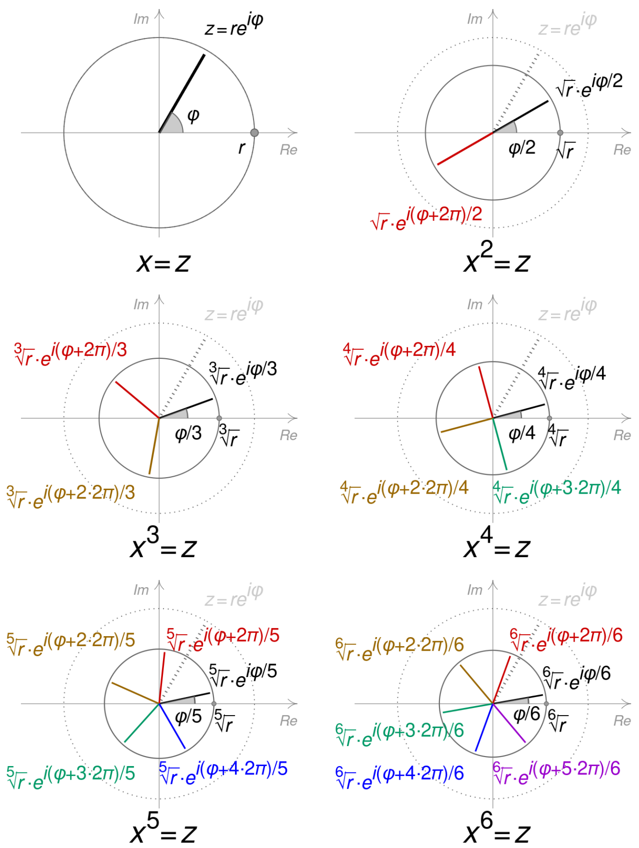
Definition 3.3 (Root of Unity)

Let P be a number field and $n \in \mathbb{N}^*$. An element $\omega \in P$ is called an n-th root of unity if it satisfies the equation $x^n - 1 = 0$, i.e., $\omega^n = 1$. ♣

Unless otherwise specified, the roots of unity may be taken to be complex numbers, and in this case, the n-th roots of unity are

$$\omega_k = \exp\frac{2k\pi i}{n} = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right), \quad k = 0, 1, \ldots, n-1.$$

Obviously, the modulus of each n-th root of unity is 1, i.e., $|\omega_k| = 1$, and they are evenly distributed on the unit circle in the complex plane, with an angle of $\frac{2\pi}{n}$ between adjacent roots.



Property

1. *The n-th roots of unity form a cyclic group under multiplication, with $\omega = \exp\frac{2\pi i}{n}$ as a generator.*

Proposition 3.2 (Formulas for Sums and Differences of Powers)

For $n \in \mathbb{N}^+$ and n being odd:

$$a^n + b^n = (a+b)\left(a^{n-1}b^0 - a^{n-2}b^1 + a^{n-3}b^2 - \cdots - a^1b^{n-2} + a^0b^{n-1}\right).$$

When n is even, there is no general formula for the n-th power sum.

For $n \in \mathbb{N}^+$:

$$a^n - b^n = (a-b)\left(a^{n-1}b^0 + a^{n-2}b^1 + a^{n-3}b^2 + \cdots + a^0b^{n-1}\right).$$

Commonly used special cases:

$$a^2 - b^2 = (a+b)(a-b).$$

$$a^3 + b^3 = (a+b)(a^2 - ab + b^2), \quad a^3 - b^3 = (a-b)(a^2 + ab + b^2).$$

$$\begin{aligned} a^4 - b^4 = (a^2 + b^2)(a^2 - b^2) &= (a^2 + b^2)(a+b)(a-b), \\ &= (a-b)(a^3 + a^2 b + ab^2 + b^3). \end{aligned}$$

When $b = 1$,

$$x^n + 1 = (x+1)\big(x^{n-1} - x^{n-2} + x^{n-3} - \cdots + x - 1\big), \quad n \in \mathbb{N}^+, \, n \text{ is odd}.$$

$$x^n - 1 = (x-1)\big(x^{n-1} + x^{n-2} + x^{n-3} + \cdots + x + 1\big), \quad n \in \mathbb{N}^+.$$

Chapter 4 Integral Valued Polynomials

4.1 Lagrange Interpolation Polynomial

Chapter 5 Multivariate Polynomial

5.1 Symmetric Polynomial

Definition 5.1 (Symmetric Polynomial)

A polynomial $f(x_1, x_2, \ldots, x_n)$ in n variables is called a **symmetric polynomial** if it remains unchanged under any permutation of its variables. In other words, for any permutation σ of the set $\{1, 2, \ldots, n\}$, the following holds:

$$f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = f(x_1, x_2, \ldots, x_n).$$

♣

Some common symmetric polynomials include:

Elementary Symmetric Polynomials:

$$\sigma_k(x_1, x_2, \ldots, x_n) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k}, \quad k = 1, 2, \ldots, n.$$

That is,

$$\begin{aligned}
\sigma_0 &= 1, \\
\sigma_1 &= x_1 + x_2 + \cdots + x_n, \\
\sigma_2 &= \sum_{1 \le i < j \le n} x_i x_j, \\
&\vdots \\
\sigma_n &= x_1 x_2 \cdots x_n, \\
\sigma_k &= 0, \quad k > n.
\end{aligned}$$

Power Sum Symmetric Polynomials:

$$p_k(x_1, x_2, \ldots, x_n) = x_1^k + x_2^k + \cdots + x_n^k, \quad k = 1, 2, \ldots.$$

Complete Homogeneous Symmetric Polynomials:

$$h_k(x_1, x_2, \ldots, x_n) = \sum_{i_1 + i_2 + \cdots + i_n = k} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}, \quad k = 1, 2, \ldots.$$

Theorem 5.1 (Newton's Identities)

For $k \ge 1$, the following relations hold between the elementary symmetric polynomials σ_k and the power sum symmetric polynomials p_k:

$$k\sigma_k = \sum_{i=1}^{k} (-1)^{i-1} \sigma_{k-i} p_i.$$

♡

Bibliography

[1] 南秀全, 黄振国. *多项式理论*. 哈尔滨工业大学出版社, 2016.

[2] 王萼芳, 石生明. 高等代数 *(5th edition)* , 高等教育出版社, 2019.