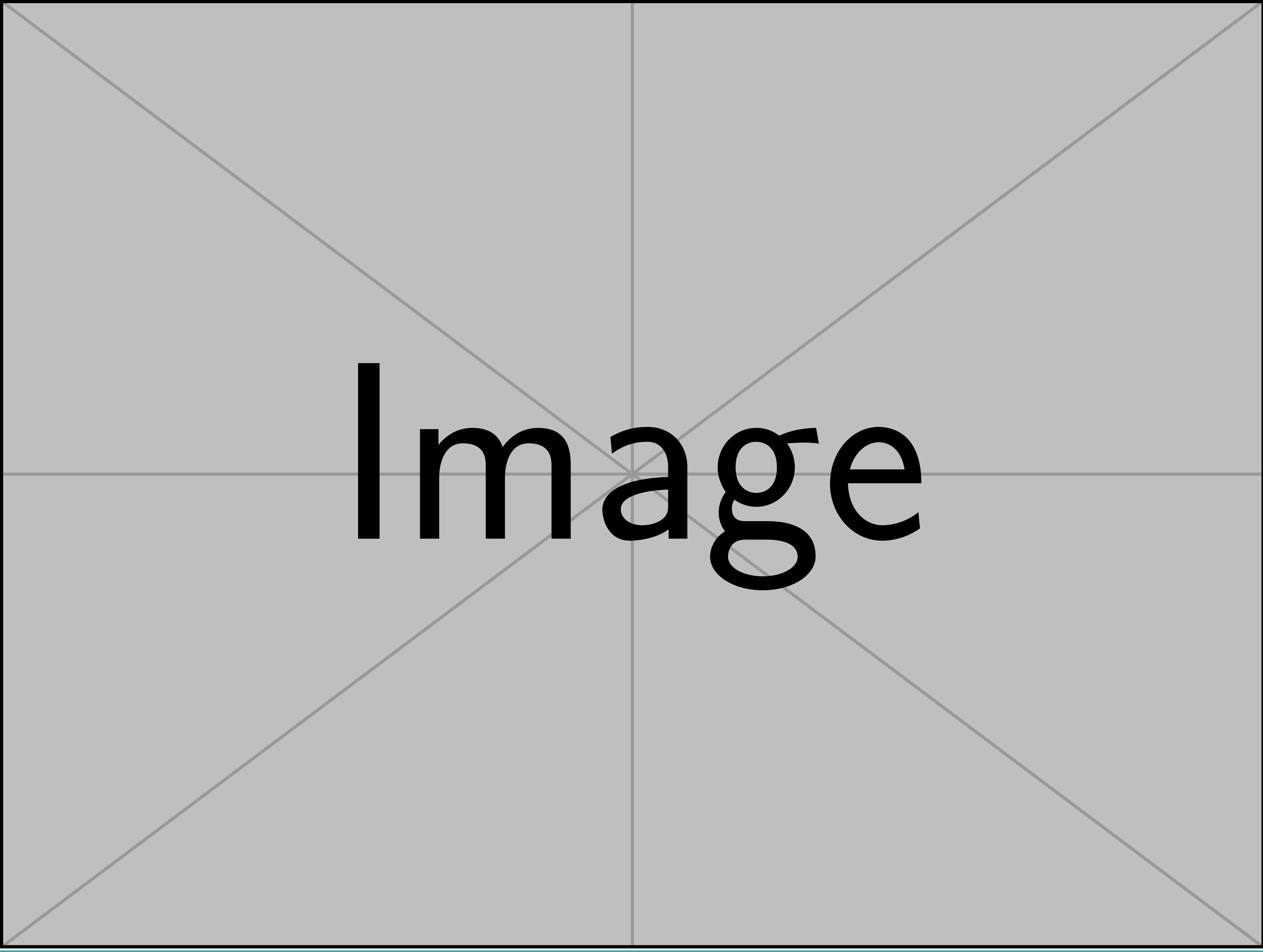


Polynôme

Author: CatMono

Date: September, 2025

Version: 0.1

Contents

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, $p(x)$, with a leading coefficient of 1 and 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.

3.3 Root of Unity

Definition 3.3 (Root of Unity)

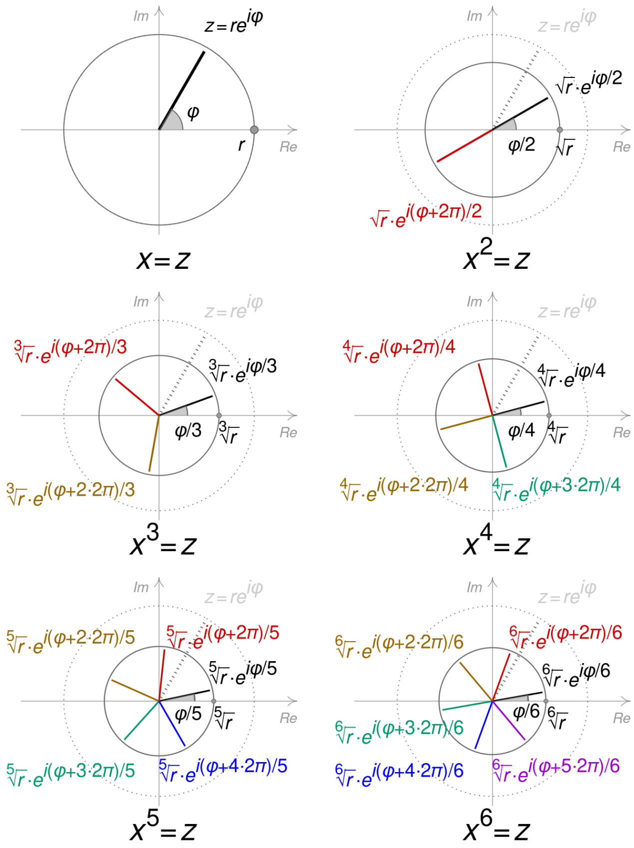
Let P be a number field and $n \in \mathbb{N}^*$. An element $\omega \in P$ is called an n-th root of unity if it satisfies the equation $x^n - 1 = 0$, i.e., $\omega^n = 1$.

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:

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

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

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

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

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 Polynomials and Rational Polynomials

Bibliography

[1] 作者, Title1, Journal1, Year1. *This is an example of a reference.*

[2] Author2, Title2, Journal2, Year2. *This is another example of a reference.*