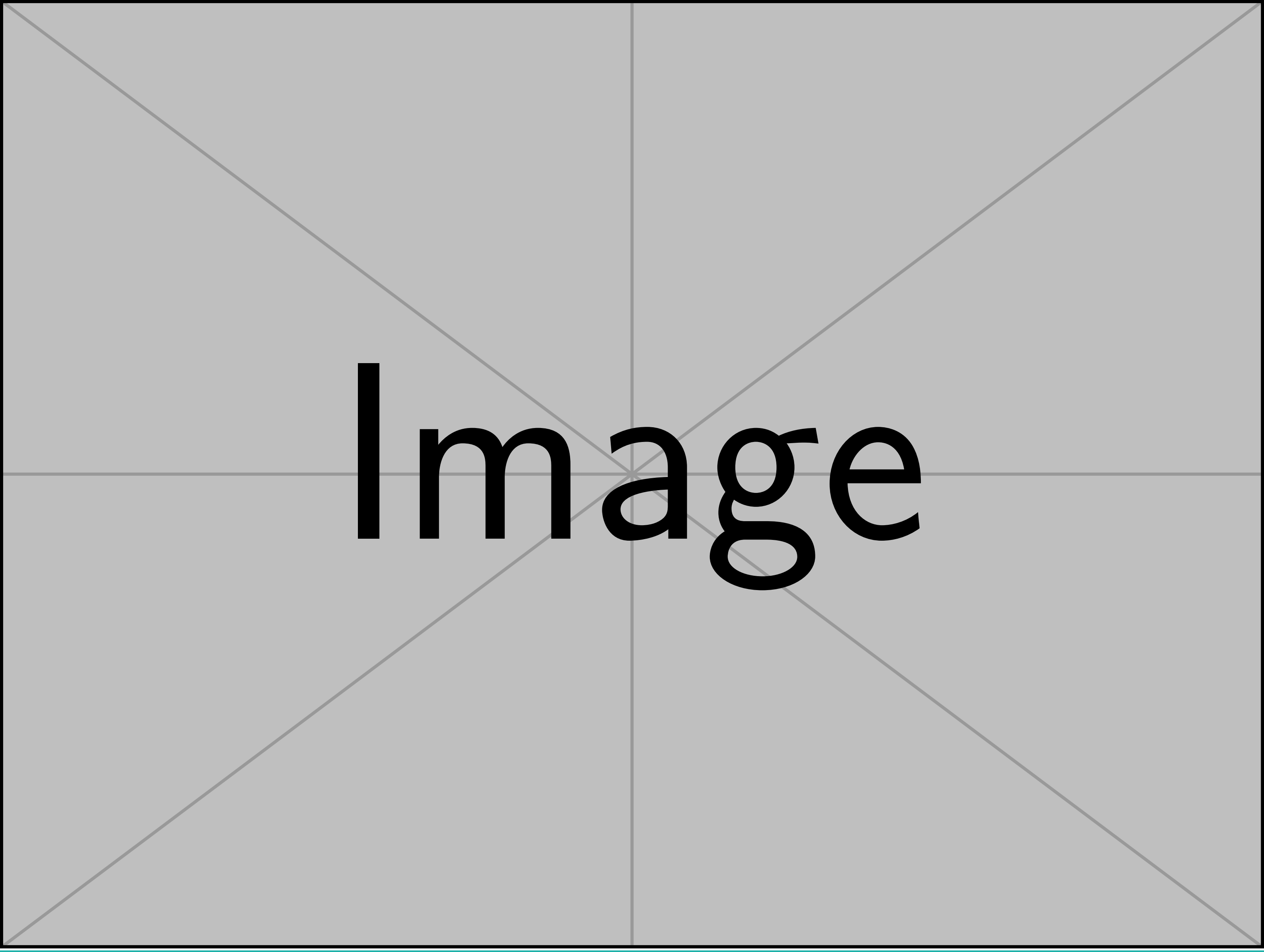

Polynôme

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, 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. ♡

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.*