

Image

# Polynôme

**Author:** CatMono

**Date:** September, 2025

**Version:** 1.0

# Contents

<b>Preface</b>	<b>ii</b>
<b>Chapter 1 Preliminaries</b>	<b>1</b>
<b>Chapter 2 Univariate Polynomial Ring</b>	<b>2</b>
2.1 Univariate Polynomials . . . . .	2
2.2 Division . . . . .	2
2.3 Greatest Common Divisor and Relatively Prime . . . . .	2
2.4 Least Common Multiple . . . . .	3
2.5 Opposite Polynomials . . . . .	3
<b>Chapter 3 Factorization and Roots</b>	<b>4</b>
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
<b>Chapter 4 Integral Valued Polynomials</b>	<b>8</b>
4.1 Lagrange Interpolation Polynomial . . . . .	8
<b>Chapter 5 Multivariate Polynomial</b>	<b>9</b>
5.1 Symmetric Polynomial . . . . .	9
5.2 Symmetric Inequalities . . . . .	10

# Preface

Version notes are in the table below.

Version	Date	Description
0.1	September, 2025	Initial version
1.0	January, 2026	Basic content completed, including chapters on univariate polynomial rings, factorization and roots, integral valued polynomials and multivariate polynomial.

# 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  $g(x) | f(x)$ .

(In other words, the remainder  $r(x) = 0$ .)



### Property

**A Caution** In Euclidean division,  $g(x) \neq 0$  is required. However, in the case of  $g(x) | f(x)$ ,  $g(x)$  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.  $d(x) | f(x)$  and  $d(x) | g(x)$ ;
2. For any polynomial  $h(x) \in P[x]$ , if  $h(x) | f(x)$  and  $h(x) | g(x)$ , then  $h(x) | d(x)$ .

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

## 2.5 Opposite Polynomials

# Chapter 3 Factorization and Roots

## 3.1 Irreducible Polynomials

### Definition 3.1 (Irreducible Polynomial)

A polynomial  $p(x)$  of degree  $\geq 1$  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  $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$  with integer coefficients is called a **primitive polynomial** if the greatest common divisor of its coefficients is  $\pm 1$ , i.e.,  $(a_n, a_{n-1}, \dots, a_1, a_0) = \pm 1$ .



### 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  $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$  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  $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$  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  $i = 0, 1, \dots, n-1$ ;
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 (Viète's Formulas)**

Let  $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$  be a polynomial of degree  $n$  over field  $P$ , and let its  $n$  roots (counting multiplicities) be  $r_1, r_2, \dots, r_n$  in an extension field of  $P$ . Then the following relations hold:

$$\begin{aligned} r_1 + r_2 + \cdots + r_n &= -\frac{a_{n-1}}{a_n}, \\ r_1r_2 + r_1r_3 + \cdots + r_{n-1}r_n &= \frac{a_{n-2}}{a_n}, \\ &\vdots \\ r_1r_2 \cdots r_n &= (-1)^n \frac{a_0}{a_n}. \end{aligned}$$


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

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

that is,

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

## 3.4 Root of Unity

**Definition 3.3 (Root of Unity)**

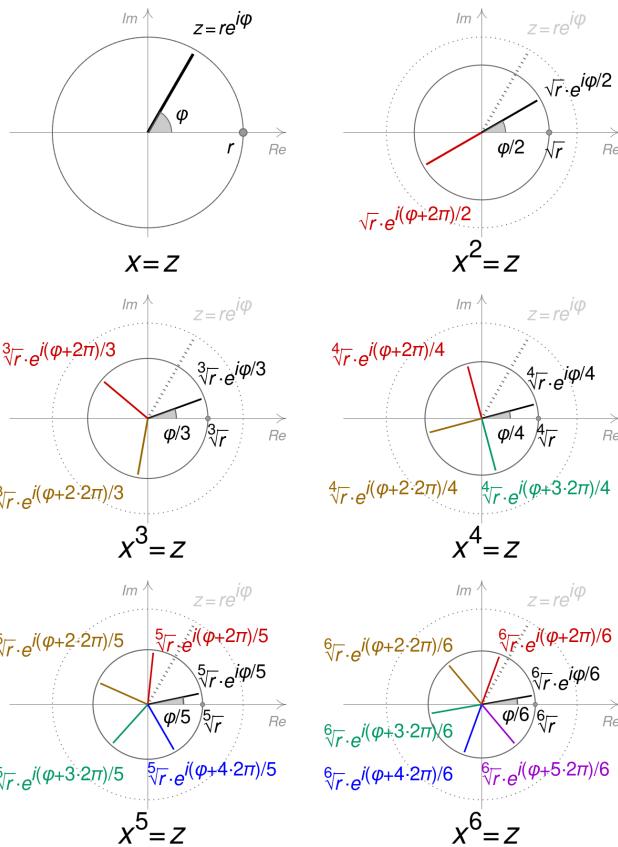
Let  $P$  be a number field and  $n \in \mathbb{N}^*$ . An element  $\omega \in P$  is called an  $n$ -th root of unity if it satisfies the equation  $x^n - 1 = 0$ , i.e.,  $\omega^n = 1$ .



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

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

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:

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

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

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

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

Commonly used special cases:

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

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

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

When  $b = 1$ ,

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

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



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

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



Some common symmetric polynomials include:

### Elementary Symmetric Polynomials

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

That is,

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

Any symmetric polynomial can be expressed as a polynomial in elementary symmetric polynomials.

### Power Sum Symmetric Polynomials

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

### Complete Homogeneous Symmetric Polynomials

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

**Theorem 5.1 (Newton's Identities)**

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

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



We introduce some notations for convenience, where  $f$  can be any function of  $n$  variables, not necessarily be polynomials:

**Cyclic Sum** Perform a cyclic shift on all variables in an expression, then sum the resulting terms:

$$\sum_{\text{cyc}} f(x_1, x_2, \dots, x_n) = \sum_{i=1}^n f(x_i, x_{i+1}, \dots, x_{i+n-1}),$$

where the indices are taken modulo  $n$ .

For example,

$$\sum_{\text{cyc}} \frac{a}{b+c} = \frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geq \frac{3}{2},$$

which is called Nesbitt's inequality, to be proved later.

**Symmetric Sum** Sum over all distinct permutations of the variables in an expression:

$$\sum_{\text{sym}} f(x_1, x_2, \dots, x_n) = \sum_{\sigma \in S_n} f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}),$$

where  $S_n$  is the set of all permutations of  $n$  elements.

For example,

$$\sum_{\text{sym}} a^3 = a^3 + b^3 + c^3, \quad \sum_{\text{sym}} a^2b = a^2b + a^2c + b^2a + b^2c + c^2a + c^2b.$$

## 5.2 Symmetric Inequalities

*Definition 5.2 (Symmetric Inequality)*

An inequality  $f(x_1, x_2, \dots, x_n) \geq g(x_1, x_2, \dots, x_n)$  is called a **symmetric inequality** if the polynomial  $f(x_1, x_2, \dots, x_n)$  and  $g(x_1, x_2, \dots, x_n)$  are symmetric polynomials.



### Power Mean Inequality

*Theorem 5.2 (Power Mean Inequality)*

For positive real numbers  $a_1, a_2, \dots, a_n > 0$ , define the power mean of order  $p$  as:

$$M_p(a_1, a_2, \dots, a_n) = \begin{cases} \left(\frac{a_1^p + a_2^p + \dots + a_n^p}{n}\right)^{\frac{1}{p}}, & p \neq 0 \\ \lim_{p \rightarrow 0} M_p(a_1, a_2, \dots, a_n) = \sqrt[n]{a_1 a_2 \cdots a_n}, & p = 0. \end{cases}$$

Specially, when  $p \rightarrow 0$ , it is the **geometric mean** (G)

$$G = \sqrt[n]{a_1 a_2 \cdots a_n};$$

when  $p = 1$ , it is the **arithmetic mean** (A)

$$A = \frac{a_1 + a_2 + \cdots + a_n}{n};$$

when  $p = 2$ , it is the **quadratic mean** (Q)

$$Q = \sqrt{\frac{a_1^2 + a_2^2 + \cdots + a_n^2}{n}};$$

when  $p = -1$ , it is the **harmonic mean** (H)

$$H = \frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}}.$$

The following inequalities hold:

$$\cdots \leq M_{-2} \leq M_{-1} \leq M_0 \leq M_1 \leq M_2 \leq \cdots.$$

Thus, we have:

$$H \leq G \leq A \leq Q.$$



When  $n = 2$ , in the chain of power mean inequalities, we can insert the **logarithmic mean**: logarithmic

mean of  $a$  and  $b$  is defined as:

$$L(a, b) = \frac{a - b}{\ln a - \ln b} \quad (a \neq b, a, b > 0),$$

then we have:

$$G(a, b) \leq L(a, b) \leq A(a, b).$$

### Muirhead Inequality

This part mainly references [3].

#### Definition 5.3 (Convex Hull)

Let  $V$  be a linear space over the field  $\mathbb{R}$ , for a set  $X$ , the **convex hull** of  $X$  is defined as the intersection of all convex sets containing  $X$ :

$$S := \bigcap_{X \subseteq K \subseteq V} K, \quad \text{where } K \text{ is a convex set.}$$



For an  $n$ -dimensional vector  $\alpha = (a_1, a_2, \dots, a_n)$ , define  $\alpha_{[j]}$ ,  $1 \leq j \leq n$  is the  $j$ -th item of  $\alpha$  after sorting  $a_1, a_2, \dots, a_n$  in descending order, i.e.,

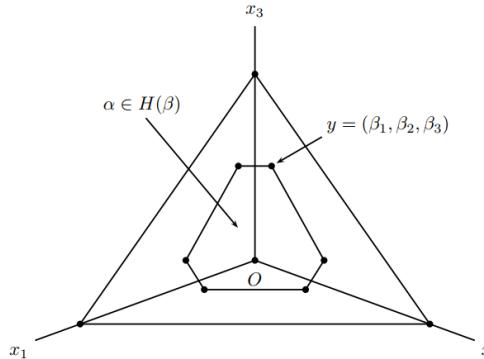
$$a_{[1]} \geq a_{[2]} \geq \cdots \geq a_{[n]}.$$

Then we can obtain

$$\alpha_{\downarrow} = (a_{[1]}, a_{[2]}, \dots, a_{[n]}).$$

Define  $S_n$  be the set of all permutations of the set  $\{1, 2, \dots, n\}$ , then we define the convex hull of  $\alpha$  as:

$$H(\alpha) = \{b_{\tau(1)}, b_{\tau(2)}, \dots, b_{\tau(n)} | \tau \in S_n\}.$$



**Figure 5.1:** Relation graph of convex hull in  $\mathbb{R}^3$ .

#### Theorem 5.3 (Muirhead Inequality)

For  $\alpha = (a_1, a_2, \dots, a_n), \beta = (b_1, b_2, \dots, b_n) \in \mathbb{R}^n$ , and  $\alpha \in H(\beta)^a$ , then for positive numbers  $x_1, x_2, \dots, x_n > 0$ , the following inequality holds:

$$\sum_{\sigma \in S_n} x_{\sigma(1)}^{a_1} x_{\sigma(2)}^{a_2} \cdots x_{\sigma(n)}^{a_n} \leq \sum_{\sigma \in S_n} x_{\sigma(1)}^{b_1} x_{\sigma(2)}^{b_2} \cdots x_{\sigma(n)}^{b_n},$$

where  $\sum_{\sigma \in S_n}$  denotes summation over all permutations  $\sigma$  in  $S_n$ .

The equality holds if and only if  $x_1 = x_2 = \cdots = x_n$  or  $\alpha_{\downarrow} = \beta_{\downarrow}$ .

<sup>a</sup>It is often called **Muirhead's condition** that  $\alpha \in H(\beta)$ .



Since Muirhead's condition is difficult to verify directly, we derive the following conditions.

#### Definition 5.4 (Majorization)

For  $\alpha = (a_1, a_2, \dots, a_n), \beta = (b_1, b_2, \dots, b_n) \in \mathbb{R}^n$ , if the following conditions hold:

1.  $a_{[1]} + a_{[2]} + \dots + a_{[n]} = b_{[1]} + b_{[2]} + \dots + b_{[n]}$ ;
2. For all  $k = 1, 2, \dots, n-1$ ,

$$a_{[1]} + a_{[2]} + \dots + a_{[k]} \leq b_{[1]} + b_{[2]} + \dots + b_{[k]};$$

then we say that  $\beta$  majorizes  $\alpha$ , denoted as  $\alpha \prec \beta$ .



#### Definition 5.5 (Doubly Stochastic Matrix)

An  $n \times n$  matrix  $P = (p_{ij})$  is called a **doubly stochastic matrix** if the sum of each row and the sum of each column both equal 1.



Now we can give two equivalent conditions:

#### Theorem 5.4

In the same conditions as Muirhead's inequality, the following two statements are equivalent to  $\alpha \prec \beta$ :

1. There exists a doubly stochastic matrix  $D$  such that  $\alpha = D\beta$ .
2.  $\alpha \in H(\beta)$ .



With Muirhead's inequality, we can prove many symmetric inequalities easily.

#### Proposition 5.1 (Schur Inequality)

For non-negative real numbers  $a, b, c \geq 0$  and a real number  $r \geq 0$ , the following inequality holds:

$$a^r(a-b)(a-c) + b^r(b-c)(b-a) + c^r(c-a)(c-b) \geq 0.$$

When  $r = 1$ , the following well-known special case can be derived:

$$a^3 + b^3 + c^3 + 3abc \geq ab(a+b) + bc(b+c) + ca(c+a).$$



#### Proposition 5.2 (Nesbitt's Inequality)

For positive real numbers  $a, b, c > 0$ , the following inequality holds:

$$\sum_{\text{cyc}} \frac{a}{b+c} = \frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geq \frac{3}{2}.$$



**Proof** By finding a common denominator and cross-multiplying, we have:

$$2 \sum_{\text{cyc}} a(a+b)(a+c) \geq 3(a+b)(b+c)(c+a),$$

which is equivalent to

$$\sum_{\text{sym}} a^3 \geq \sum_{\text{sym}} a^2 b.$$

Note that  $(3, 0, 0) \succ (2, 1, 0)$ , thus by Muirhead's inequality, the above inequality holds. ■

## 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.
- [3] 陈柏宇, 张福春. *Muirhead 不等式*, 数学传播-38 卷 2 期, pp.41-58, 2019.