

Math 830 ABSTRACT ALGEBRA

PROGRESS CHECK – X

October 16 (Mon), 2006

Instructor: Yasuyuki Kachi

Line #: 17014.

• **Monomials and Polynomials.**

Let $\{x_1, \dots, x_n\}$ be a set, consisting of n elements. Let us consider a formal expression

$$x_1^{i_1} \cdot \dots \cdot x_n^{i_n},$$

where each i_ℓ is a non-negative integer. We omit $x_\ell^{i_\ell}$ when $i_\ell = 0$. For example, suppose $n = 5$, and we may write

$$x_2^2 x_3^7 x_5^6 = x_1^0 x_2^2 x_3^7 x_4^0 x_5^6.$$

When $i_1 = \dots = i_n = 0$, we may write

$$1 = x_1^0 \cdot \dots \cdot x_n^0.$$

When $i_\ell = 1$ for one i_ℓ and all the other $i_{\ell'}$ are 0, we may write it x_ℓ :

$$x_\ell = x_1^0 \cdot \dots \cdot x_{\ell-1}^0 x_\ell^1 x_{\ell+1}^0 \cdot \dots \cdot x_n^0.$$

We call $x_1^{i_1} \cdot \dots \cdot x_n^{i_n}$ a monomial in $\{x_1, \dots, x_n\}$.

• We call the original set $\{x_1, \dots, x_n\}$ the set of indeterminates.

• We define multiplication of two monomials in $\{x_1, \dots, x_n\}$ as

$$\left(x_1^{i_1} \cdot \dots \cdot x_n^{i_n}\right) \left(x_1^{j_1} \cdot \dots \cdot x_n^{j_n}\right) = x_1^{i_1+j_1} \cdot \dots \cdot x_n^{i_n+j_n}.$$

[I] (1) Verify

$$1 \cdot x_\ell = x_\ell. \quad x_\ell x_m = x_m x_\ell. \quad x_\ell x_\ell = x_\ell^2. \quad x_\ell x_\ell^i = x_\ell^{i+1}.$$

(2) More generally, verify that for monomials μ, ν, ρ , the following hold:

$$\text{(Commutativity)} \quad \mu \rho = \rho \mu,$$

$$\text{(Associativity)} \quad \mu(\nu \rho) = (\mu \nu) \rho,$$

$$\text{(Cancellability)} \quad \mu \nu = \mu \rho \quad \text{implies} \quad \nu = \rho.$$

(3) Verify that 1 serves as the multiplicative identity.

• **Formal sum of monomials.**

Let us consider a formal finite sum of monomials in $\{x_1, \dots, x_n\}$:

$$\sum_{(i_1, \dots, i_n)} x_1^{i_1} \cdots x_n^{i_n}.$$

Suppose $n = 3$.

$$\begin{aligned} x_1^4 + x_2^4 + 1, & \quad x_1^3 + x_2^2 x_3 + x_2^2 x_3 + x_2^3, \\ x_1 x_2 x_3 + x_1 x_2 x_3 + x_1 x_2 + x_1 x_3 + x_2 + x_3, \end{aligned}$$

are examples of formal finite sums of monomials in $\{x_1, x_2, x_3\}$. We agree that reordering monomials in the sum expression has no effect. For example,

$$x_1^2 x_2 + x_1 x_2^2 = x_1 x_2^2 + x_1^2 x_2.$$

In monomial sums, two or more monomials may appear in duplicate. We agree to “combine” more than one identical monomials appearing in the sum, as long as we indicate how many of the mutually identical monomials are combined in the sum. For example,

$$\begin{aligned} 2x_3^3 &= x_3^3 + x_3^3, \\ 4x_1 x_2 x_3 &= x_1 x_2 x_3 + x_1 x_2 x_3 + x_1 x_2 x_3 + x_1 x_2 x_3. \end{aligned}$$

This way, in general we may write a formal monomial sum in $\{x_1, \dots, x_n\}$ in the form

$$\xi = \sum_{(i_1, \dots, i_n)} \alpha_{(i_1, \dots, i_n)} x_1^{i_1} \cdots x_n^{i_n},$$

where $\alpha_{(i_1, \dots, i_n)}$ is a non-negative integer. $\alpha_{(i_1, \dots, i_n)}$ is called the coefficient of the monomial $x_1^{i_1} \cdots x_n^{i_n}$ in ξ .

Each constituent

$$\alpha_{(i_1, \dots, i_n)} x_1^{i_1} \cdots x_n^{i_n}$$

in the sum is called a term of ξ . If a monomial $x_1^{i_1} \cdots x_n^{i_n}$ do not appear in the expression of ξ as above, we understand that the coefficient of the monomial $x_1^{i_1} \cdots x_n^{i_n}$ in ξ is 0.

• Now we may define addition of two formal monomial sums. Let ξ and η be monomial sums in $\{x_1, \dots, x_n\}$. Then the sum $\xi + \eta$ is simply the formal monomial sum obtained by simply adjoining the terms of ξ and η . For example, if

$$\xi = 7x_1^2 + 3x_2x_3 + 2x_3^2 + 6, \quad \eta = 2x_1^2 + 4x_2x_3 + 2,$$

then

$$\begin{aligned} \xi + \eta &= (7 + 2)x_1^2 + (3 + 4)x_2x_3 + 2x_3^2 + (6 + 2) \\ &= 9x_1^2 + 7x_2x_3 + 2x_3^2 + 8. \end{aligned}$$

• **Polynomials.**

We would like to define subtraction as well. For this reason, we will allow negative coefficients to a formal monomial sum. Thus, we consider

$$\xi = \sum_{(i_1, \dots, i_n)} \alpha_{(i_1, \dots, i_n)} x_1^{i_1} \cdots x_n^{i_n}, \quad \alpha_{(i_1, \dots, i_n)} \in \mathbb{Z}.$$

Definition. The above formal sum ξ with integer coefficients is called a polynomial. It is evident as to how we should define addition $\xi + \eta$ and subtraction $\xi - \eta$ for two polynomials ξ and η . Note $\xi - \xi = 0$. We have:

Lemma. The set of polynomials in $\{x_1, \dots, x_n\}$ forms an additive group.

[II] Let us define the set

$$M_+ = \left\{ (i_1, \dots, i_n) \mid i_\ell \in \mathbb{Z}; i_\ell \geq 0, \ell = 1, \dots, n \right\}.$$

Let ξ be a polynomial in $\{x_1, \dots, x_n\}$, thus

$$\xi = \sum_{(i_1, \dots, i_n)} \alpha_{(i_1, \dots, i_n)} x_1^{i_1} \cdots x_n^{i_n}, \quad \alpha_{(i_1, \dots, i_n)} \in \mathbb{Z}.$$

Show that this ξ gives rise to a mapping

$$\bar{\xi} : M_+ \longrightarrow \mathbb{Z}; \quad \bar{\xi}(i_1, \dots, i_n) = \alpha_{(i_1, \dots, i_n)}.$$

Show that this mapping satisfies the following:

$$\text{Supp } \xi = \left\{ (i_1, \dots, i_n) \in M_+ \mid \bar{\xi}(i_1, \dots, i_n) \neq 0 \right\}$$

is a finite subset of M_+ . $\text{Supp } \xi = \emptyset$ if and only if $\xi = 0$.

• **Multiplication of polynomials. The polynomial ring $\mathbb{Z}[x_1, \dots, x_n]$.**

Let ξ and η be two polynomials in $\{x_1, \dots, x_n\}$. We would like to define $\xi\eta$. When ξ and η are both monomials, this is already defined.

Otherwise, ξ and η are written as

$$\xi = \alpha_1 \xi_1 + \cdots + \alpha_r \xi_r, \quad \eta = \beta_1 \eta_1 + \cdots + \beta_s \eta_s,$$

where each ξ_i and η_j are monomials, and $\alpha_i, \beta_j \in \mathbb{Z}$ are coefficients. Then we define

$$\xi \eta = \sum_{i=1}^r \sum_{j=1}^s (\alpha_i \beta_j) \xi_i \eta_j.$$

Clearly we have $\xi \eta = \eta \xi$ (commutativity law). Moreover, we have the distributive law

$$\xi \cdot (\beta_1 \eta_1 + \cdots + \beta_s \eta_s) = \beta_1 \xi \eta_1 + \cdots + \beta_s \xi \eta_s.$$

Thus, the computation of $\xi \eta$ may go as follows: First regard η as a monomial sum, and apply distributive law. Then each term in the resulting distribution is of form

$$\xi (\beta_\ell \eta_\ell) = \beta_\ell \cdot (\xi \eta_\ell),$$

where η_ℓ is a monomial, and $\beta_\ell \in \mathbb{Z}$ is a coefficient. Regard ξ as a monomial sum and apply distributive law to $\xi \eta_\ell$. The resulting distribution is a sum of terms of form “an integer times a monomial”. Combine or cancel terms when necessary.

Example.

$$x_1 (2 + x_1 x_2 + x_3) = 2x_1 + x_1^2 x_2 + x_1 x_3.$$

$$(1 + x_1 x_2) (1 - x_1 x_2) = 1 - x_1^2 x_2^2.$$

$$\begin{aligned} (x_1 - x_2) (x_2 - x_3) (x_3 - x_1) \\ = x_1 x_2^2 - x_1^2 x_2 + x_2 x_3^2 - x_2^2 x_3 + x_3 x_1^2 - x_3^2 x_1. \end{aligned}$$

Notation. We denote the set of polynomials in $\{x_1, \dots, x_n\}$ endowed with the additive and the multiplicative structure, by

$$\mathbb{Z} [x_1, \dots, x_n].$$

Theorem. $R = \mathbb{Z} [x_1, \dots, x_n]$ forms a commutative ring. In other words, R satisfies the following five conditions (i–v):

(i) R is an additive group with respect to ‘+’, in particular, R admits the additive identity 0,

(ii) R is associative with respect to multiplication, namely,

$$\xi (\eta \zeta) = (\xi \eta) \zeta,$$

(iii) R is commutative with respect to multiplication, namely,

$$\xi \eta = \eta \xi,$$

(iv) R admits a multiplicative identity 1 , namely,

$$\xi \cdot 1 = \xi,$$

(v) R is distributive, namely,

$$\xi (\eta + \zeta) = \xi \eta + \xi \zeta.$$

• In view of the above Theorem, we call $\mathbb{Z} [x_1, \dots, x_n]$ the polynomial ring with n -variables (and with \mathbb{Z} -coefficients).

• The polynomial ring $R = \mathbb{Z} [x_1, \dots, x_n]$ contains the subset $\{x_1, \dots, x_n\}$, which we call the set of indeterminates of the polynomial ring R .

• When $n = 1, 2, 3$, we often denote the set of indeterminates $\{x\}$, $\{x, y\}$, $\{x, y, z\}$. We denote the corresponding polynomials rings

$$\mathbb{Z} [x], \quad \mathbb{Z} [x, y], \quad \mathbb{Z} [x, y, z].$$

[III] (1) In $\mathbb{Z} [x, y]$, verify

$$(x + y)(x - y) = x^2 - y^2, \quad (x + y)^2 = x^2 + 2xy + y^2.$$

(2) In $\mathbb{Z} [x, y, z]$, verify

$$(x + y + z)^2 = x^2 + y^2 + z^2 + 2xy + 2yz + 2zx.$$

(3) In $\mathbb{Z} [x, y, z]$, verify

$$\begin{aligned} (x - y)(x - z)(y - z) \\ = x^2y - xy^2 - x^2z + xz^2 + y^2z - yz^2. \end{aligned}$$

(4) In $\mathbb{Z}[x, y]$, verify

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k,$$

where

$$\binom{n}{k} = \frac{n!}{k! (n-k)!} \in \mathbb{Z} \quad \left(\underline{\text{the binomial coefficient}} \right).$$

[IV] Let

$$\Delta_n = \prod_{1 \leq i < j \leq n} (x_i - x_j) \in \mathbb{Z}[x_1, \dots, x_n].$$

For example,

$$\Delta_2 = x_1 - x_2,$$

$$\Delta_3 = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3),$$

$$\Delta_4 = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4).$$

Show that Δ_n consists of $(n!)$ terms. Show that, of those $n!$, $(n!)/2$ come with coefficient = 1, other $(n!)/2$ come with coefficient = -1. Show that the terms of Δ_n are $\pm x_1^{i_1} \cdots x_n^{i_n}$ such that $\{i_1, \dots, i_n\} = \{0, 1, 2, \dots, n-1\}$.

- An explicit formula for Δ_3 is found in [III] (3) in the previous page. An explicit formula for Δ_4 is found in Appendix A.

[V] Let $\xi \in \mathbb{Z}[x_1, \dots, x_n]$ be an arbitrary polynomial.

(1) Verify that ξ induces a mapping $\bar{\xi} : \mathbb{Z}^n \longrightarrow \mathbb{Z}$,

$$\bar{\xi}(m_1, \dots, m_n) = \sum_{i_1 \geq 0, \dots, i_n \geq 0} \alpha_{(i_1, \dots, i_n)} m_1^{i_1} \cdots m_n^{i_n}$$

(the polynomial substitution).

(2) Prove

$$\overline{\xi_1}(m_1, \dots, m_n) + \overline{\xi_2}(m_1, \dots, m_n) = \overline{\xi_1 + \xi_2}(m_1, \dots, m_n),$$

$$\overline{\xi_1}(m_1, \dots, m_n) \overline{\xi_2}(m_1, \dots, m_n) = \overline{\xi_1 \xi_2}(m_1, \dots, m_n).$$

(3) Let $\xi = \Delta_n$ be as in [IV]. Prove that $\overline{\Delta_n}(m_1, \dots, m_n) \neq 0$ if and only if m_1, \dots, m_n are all distinct.

Example. When $n = 1$, the ring $\mathbb{Z}[x_1, \dots, x_n]$ is simply written as $\mathbb{Z}[x]$. An element of $\mathbb{Z}[x]$ is of form

$$\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots + \alpha_n x^n,$$

$\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{Z}$.

• **Degrees of monomials.**

Let $x_1^{i_1} \dots x_n^{i_n}$ be a monomial in $\{x_1, \dots, x_n\}$. We call the number

$$i_1 + \dots + i_n = d$$

the degree of the monomial $x_1^{i_1} \dots x_n^{i_n}$. We write it $\deg(x_1^{i_1} \dots x_n^{i_n})$.

Example. $\deg(x_1^2 x_3) = 3$. $\deg(x_1 x_2 x_3 x_4) = 4$. $\deg(x_1 x_2^2 x_3^3) = 6$.

• **Counting monomials. Polynomials with Rational Coefficients.**

We may count the number of monomials of degree d in $\mathbb{Z}[x_1, \dots, x_n]$, for each $d \geq 0$.

Lemma. Let $d \in \mathbb{Z}$, $d \geq 0$. Then there are

$$P_d(n) = \binom{d+n-1}{d} = \frac{n(n+1) \dots (d+n-1)}{d!}$$

monomials of degree d in $\{x_1, \dots, x_n\}$.

• See Appendix B for a proof.

Example.
$$P_2(n) = \frac{n(n+1)}{2} = \frac{1}{2}n^2 + \frac{1}{2}n.$$

$$P_3(n) = \frac{n(n+1)(n+2)}{3!} = \frac{1}{6}n^3 + \frac{1}{2}n^2 + \frac{1}{3}n.$$

- Observe that each P_d defines a mapping $P_d: \mathbb{Z}_+ \rightarrow \mathbb{Z}_+$ taking n into $P_d(n)$.
- It makes sense to think of P_d as the “polynomial substitution” of

$$\xi_d = \frac{x(x+1)\cdots(x+d-1)}{d!},$$

even though ξ_d does not have coefficients in \mathbb{Z} but only in \mathbb{Q} . This motivates us to introduce polynomials with \mathbb{Q} -coefficients.

• **Polynomials with Rational Coefficients.**

Definition. Let $\mathbb{Q}[x_1, \dots, x_n]$ be the set of formal sums of monomials in $\{x_1, \dots, x_n\}$, having coefficients in \mathbb{Q} :

$$\begin{aligned} \mathbb{Q}[x_1, \dots, x_n] &= \left\{ \xi = \sum_{i_1 \geq 0, \dots, i_n \geq 0} \alpha_{(i_1, \dots, i_n)} x_1^{i_1} \cdots x_n^{i_n} \mid \begin{array}{l} \alpha_{(i_1, \dots, i_n)} \in \mathbb{Q}, \\ \alpha_{(i_1, \dots, i_n)} = 0 \text{ except for} \\ \text{finitely many } (i_1, \dots, i_n) \end{array} \right\}. \end{aligned}$$

This set $\mathbb{Q}[x_1, \dots, x_n]$ admits an addition and a multiplication, and it forms a commutative ring. We call $\mathbb{Q}[x_1, \dots, x_n]$ the polynomial ring with \mathbb{Q} -coefficients.

- When $n = 1$, $\mathbb{Q}[x_1, \dots, x_n]$ is written as $\mathbb{Q}[x]$.

Example. $\frac{1}{2}x_1^2 + \frac{1}{2}x_2 + 1 \in \mathbb{Q}[x_1, x_2].$

$$\frac{1}{6}x_1^3 + \frac{1}{2}x_2^2 + \frac{1}{3}x_3x_4 \in \mathbb{Q}[x_1, x_2, x_3, x_4].$$

• In some sense, the algebraic structure of the polynomial ring $\mathbb{Q}[x_1, \dots, x_n]$ is simpler than that of the polynomial ring $\mathbb{Z}[x_1, \dots, x_n]$. It takes a little bit of a ring theory (which we have not covered yet) to explain what this precisely means, but this is attributed to the fact that \mathbb{Q} is a field, whereas \mathbb{Z} is not. (See “the field axioms” in Pg. Ch. I). We may stretch our imagination and want to define the polynomial ring $F[x_1, \dots, x_n]$ over an arbitrary field F . This indeed makes perfect sense. For example, we may define $\mathbb{R}[x_1, \dots, x_n]$, $\mathbb{C}[x_1, \dots, x_n]$, *etc.* Although this way of generalizing the concept of polynomial rings is very important, especially in the context of the theory of roots of polynomial equations, we will not discuss this at this stage. Let us stick with $\mathbb{Q}[x_1, \dots, x_n]$ for a while.

• **Symmetric group S_n acting on $\mathbb{Q}[x_1, \dots, x_n]$.**

Let $G = S_n$ be the n -th symmetric group, as before. Let

$$R = \mathbb{Q}[x_1, \dots, x_n]$$

be the polynomial ring with \mathbb{Q} -coefficients. Since each $\sigma \in G$ induces a bijection

$$\sigma : \{x_1, \dots, x_n\} \longrightarrow \{x_1, \dots, x_n\},$$

accordingly for each monomial $\xi = x_1^{i_1} \dots x_n^{i_n}$ in R , we may define

$$\xi^\sigma = x_{\sigma(1)}^{i_1} \dots x_{\sigma(n)}^{i_n}.$$

Evidently this is again a monomial, and therefore it belongs to R . Next, for an arbitrary polynomial $\xi \in R$, we may write

$$\xi = \alpha_1 \xi_1 + \dots + \alpha_s \xi_s,$$

where every ξ_ℓ is a monomial, and $\alpha_\ell \in \mathbb{Q}$. Then we define

$$\xi^\sigma = \alpha_1 \xi_1^\sigma + \dots + \alpha_s \xi_s^\sigma.$$

Note that $\xi_\ell^\sigma = \xi_\ell$ whenever $\xi_\ell = 1$ ($= x_1^0 \cdots x_n^0$).

Example. Let $n = 4$, and $\sigma \in G = S_4$ be defined as

$$\sigma(1) = 2, \quad \sigma(2) = 1, \quad \sigma(3) = 4, \quad \sigma(4) = 3.$$

Let

$$\begin{aligned} \xi &= x_1 x_2^3 x_3^2 - 2x_1 x_2^2 x_3^3 - 3x_2^3 x_3^2 x_4 + 4x_2^2 x_3^3 x_4 \\ &\quad + 5x_1 x_3^3 x_4^2 - 6x_2 x_3^3 x_4^2 - 7x_2^2 x_3 x_4^3 + 8x_2 x_3^2 x_4^3. \end{aligned}$$

Then

$$\begin{aligned} \xi^\sigma &= x_1^3 x_2 x_4^2 - 2x_1^2 x_2 x_4^3 - 3x_1^3 x_3 x_4^2 + 4x_1^2 x_3 x_4^3 \\ &\quad + 5x_2 x_3^2 x_4^3 - 6x_1 x_3^2 x_4^3 - 7x_1^2 x_3^3 x_4 + 8x_1 x_3^3 x_4^2. \end{aligned}$$

[VI] Let $G = S_n$ and $R = \mathbb{Q}[x_1, \dots, x_n]$ be as before.

(1) Let $\xi, \xi_1, \xi_2 \in R$ and $\sigma, \tau \in G$ be arbitrary. Let $\underline{e} \in G$ denote the identity element of G . Show

$$(i) \quad (\xi_1 + \xi_2)^\sigma = \xi_1^\sigma + \xi_2^\sigma. \quad (ii) \quad (\xi_1 \xi_2)^\sigma = (\xi_1^\sigma) (\xi_2^\sigma).$$

$$(iii) \quad \left((\xi)^\sigma \right)^\tau = \xi^{\tau\sigma}. \quad (iv) \quad \xi^e = \xi.$$

(2) Let $\sigma, \tau \in G$ and $\xi \in R$ be such that $\xi^\sigma = \xi = \xi^\tau$. Show

$$\xi^{\tau\sigma} = \xi = \xi^{(\sigma^{-1})}.$$

Hence $\text{Stab}(\xi) = \left\{ \sigma \in G \mid \xi^\sigma = \xi \right\}$ forms a subgroup of G .

[VII] Let G and R be as above. Let $H \subseteq G$ be an arbitrary subgroup. Let

$$R^H = \left\{ \xi \in R \mid \xi^\sigma = \xi \text{ for an arbitrary } \sigma \in H \right\}.$$

(1) Show

$$1, \quad \xi_1 + \xi_2, \quad \xi_1 \xi_2 \in R^H \quad \left(\xi_1, \xi_2 \in R^H \right),$$

$$\alpha \xi \in R^H \quad \left(\alpha \in \mathbb{Q}, \quad \xi \in R^H \right).$$

$(R^H$ is called the ring of invariants of H inside R).

(2) For $\xi \in R$, let $\text{Stab}(\xi)$ be the subgroup of G as defined in [VI]. Show

$$\text{Stab}(\xi) \supseteq H \quad (\xi \in R^H).$$

In particular,

$$\text{Stab}(\xi) = G \quad (\xi \in R^G).$$

When $H \neq G$, can we always claim $\text{Stab}(\xi) = H$ for $\xi \in R^H$?

(3) Show that

$$p_1 = \sum_{\ell=1}^n x_\ell = x_1 + \cdots + x_n, \quad p_n = \prod_{\ell=1}^n x_\ell = x_1 \cdots x_n,$$

and

$$p_2 = \sum_{1 \leq i < j \leq n} x_i x_j = x_1 x_2 + x_1 x_3 + \cdots \cdots + x_1 x_n$$

$$+ x_2 x_3 + \cdots \cdots + x_2 x_n$$

$$+ \cdots \cdots \cdots$$

$$+ x_{n-1} x_n$$

all belong to R^G . More generally, let $d \in \mathbb{Z}$, $1 \leq d \leq n$ be arbitrary. Show

$$p_d = \sum_{1 \leq i_1 < \cdots < i_d \leq n} \left(\prod_{\ell=1}^d x_{i_\ell} \right) \in R^G$$

(the d -th fundamental symmetric polynomial).

[VIII] Let G , R and R^G be as above. Let $\Delta = \Delta_n$ be as in [IV]:

$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j) \in R.$$

(1) Show

$$\Delta \notin R^G,$$

by observing that $(\Delta)^\sigma = -\Delta$, for a transposition $\sigma \in G$. This motivates us to define

$$(R^G)^* = \left\{ \xi_1 + \xi_2 \in R \mid \begin{array}{l} \xi_1 \in R^G, \xi_2 \in R, \\ \xi_2^\sigma = \xi_2 \text{ or } \xi_2^\sigma = -\xi_2 \text{ for an arbitrary } \sigma \in G \end{array} \right\}.$$

Show

$$R^G \subseteq (R^G)^*, \quad \text{and} \quad \Delta \in (R^G)^*.$$

(2) Let

$$H = \text{Stab}(\Delta) = \left\{ \sigma \in G \mid (\Delta)^\sigma = \Delta \right\},$$

as in [VI] (2). H forms a subgroup of G . Show that H is generated by the subset

$$\left\{ \sigma_1 \sigma_2 \in G \mid \sigma_1, \sigma_2 \text{ are transpositions} \right\}$$

of G .

(3) Let H be as in (2). Consider the ring of invariants

$$R^H = \left\{ \xi \in R \mid \xi^\sigma = \xi \text{ for an arbitrary } \sigma \in H \right\},$$

as in [VII]. Show

$$R^H = (R^G)^*.$$

- We often denote R^{alt} for $R^H = (R^G)^*$. We often denote also R^{symm} for R^G .

We have

$$R \supseteq R^{alt} \supseteq R^{symm}.$$

[IX] Let $R = \mathbb{Q}[x_1, \dots, x_n]$. Let $R^{alt} \subseteq R$ be as defined above. Assume $n \geq 3$. Show

$$R^{alt} \neq R.$$

How about the same for $n = 2$?

Definition. We call the subgroup $H = \text{Stab}(\Delta)$ of $G = S_n$, defined in [VIII] (2), the (n -th) alternating group, and denote it by A_n . Note that the order of A_n is $(n!)/2$:

$$o(A_n) = \frac{n!}{2}.$$

- $o(A_3) = 3$, $o(A_4) = 12$, $o(A_5) = 60$, $o(A_6) = 360$, \dots .
- The group A_n for $n \geq 5$ is an example of a “so-called” simple group.
- **Appendix A — Calculation of Δ_4 .**

In $\mathbb{Q}[x_1, x_2, x_3, x_4]$, we have

$$\begin{aligned} \Delta_4 &= (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4) \\ &= x_1^3 x_2^2 x_3 - x_1^2 x_2^3 x_3 - x_1^3 x_2 x_3^2 + x_1^2 x_2 x_3^3 + x_1 x_2^3 x_3^2 - x_1 x_2^2 x_3^3 \\ &\quad - x_1^3 x_2^2 x_4 + x_1^2 x_2^3 x_4 + x_1^3 x_2^2 x_4 - x_1^2 x_3^3 x_4 - x_2^3 x_3^2 x_4 + x_2^2 x_3^3 x_4 \\ &\quad + x_1^3 x_2 x_4^2 - x_1^3 x_3 x_4^2 - x_1 x_2^3 x_4^2 + x_2^3 x_3 x_4^2 + x_1 x_3^3 x_4^2 - x_2 x_3^3 x_4^2 \\ &\quad - x_1^2 x_2 x_4^3 + x_1 x_2^2 x_4^3 + x_1^2 x_3 x_4^3 - x_1 x_3^2 x_4^3 - x_2^2 x_3 x_4^3 + x_2 x_3^2 x_4^3. \end{aligned}$$

Proof. $\Delta_4 = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$

$$\begin{aligned}
&= \left[x_1^2 x_2 - x_1 x_2^2 - x_1^2 x_3 + x_1 x_2^2 + x_2^2 x_3 - x_2 x_3^2 \right] \\
&\quad \left[x_1 x_2 x_3 - (x_1 x_2 + x_1 x_3 + x_2 x_3) x_4 + (x_1 + x_2 + x_3) x_4^2 - x_4^3 \right] \\
&= \left[x_1^3 x_2^2 x_3 - x_1^2 x_2^3 x_3 - x_1^3 x_2 x_3^2 + x_1^2 x_2 x_3^3 + x_1 x_2^3 x_3^2 - x_1 x_2^2 x_3^3 \right] \\
&\quad + \left[-x_1^3 x_2^2 + x_1^2 x_2^3 + x_1^3 x_2 x_3 - x_1^2 x_2 x_3^2 - x_1 x_2^3 x_3 + x_1 x_2^2 x_3^2 \right] x_4 \\
&\quad + \left[-x_1^3 x_2 x_3 + x_1^2 x_2^2 x_3 + x_1^3 x_3^2 - x_1^2 x_3^3 - x_1 x_2^2 x_3^2 + x_1 x_2 x_3^3 \right] x_4 \\
&\quad + \left[-x_1^2 x_2^2 x_3 + x_1 x_2^3 x_3 + x_1^2 x_2 x_3^2 - x_1 x_2 x_3^3 - x_2^3 x_3^2 + x_2^2 x_3^3 \right] x_4 \\
&\quad + \left[x_1^3 x_2 - x_1^2 x_2^2 - x_1^3 x_3 + x_1^2 x_3^2 + x_1 x_2^2 x_3 - x_1 x_2 x_3^2 \right] x_4^2 \\
&\quad + \left[x_1^2 x_2^2 - x_1 x_2^3 - x_1^2 x_2 x_3 + x_1 x_2 x_3^2 + x_2^3 x_3 - x_2^2 x_3^2 \right] x_4^2 \\
&\quad + \left[x_1^2 x_2 x_3 - x_1 x_2^2 x_3 - x_1^2 x_3^2 + x_1 x_3^3 + x_2^2 x_3^2 - x_2 x_3^3 \right] x_4^2 \\
&\quad + \left[-x_1^2 x_2 + x_1 x_2^2 + x_1^2 x_3 - x_1 x_3^2 - x_2^2 x_3 + x_2 x_3^2 \right] x_4^3 \\
&= x_1^3 x_2^2 x_3 - x_1^2 x_2^3 x_3 - x_1^3 x_2 x_3^2 + x_1^2 x_2 x_3^3 + x_1 x_2^3 x_3^2 - x_1 x_2^2 x_3^3 \\
&\quad - x_1^3 x_2^2 x_4 + x_1^2 x_2^3 x_4 + x_1^3 x_2 x_3 x_4 - x_1^2 x_2 x_3^2 x_4 - x_1 x_2^3 x_3 x_4 + x_1 x_2^2 x_3^2 x_4 \\
&\quad - x_1^3 x_2 x_3 x_4 + x_1^2 x_2^2 x_3 x_4 + x_1^3 x_2^2 x_4 - x_1^2 x_3^3 x_4 - x_1 x_2^2 x_3^2 x_4 + x_1 x_2 x_3^3 x_4 \\
&\quad - x_1^2 x_2^2 x_3 x_4 + x_1 x_2^3 x_3 x_4 + x_1^2 x_2 x_3^2 x_4 - x_1 x_2 x_3^3 x_4 - x_2^3 x_3^2 x_4 + x_2^2 x_3^3 x_4 \\
&\quad + x_1^3 x_2 x_4^2 - x_1^2 x_2^2 x_4^2 - x_1^3 x_3 x_4^2 + x_1^2 x_3^2 x_4^2 + x_1 x_2^2 x_3 x_4^2 - x_1 x_2 x_3^2 x_4^2 \\
&\quad + x_1^2 x_2^2 x_4^2 - x_1 x_2^3 x_4^2 - x_1^2 x_2 x_3 x_4^2 + x_1 x_2 x_3^2 x_4^2 + x_2^3 x_3 x_4^2 - x_2^2 x_3^2 x_4^2 \\
&\quad + x_1^2 x_2 x_3 x_4^2 - x_1 x_2^2 x_3 x_4^2 - x_1^2 x_3^2 x_4^2 + x_1 x_3^3 x_4^2 + x_2^2 x_3^2 x_4^2 - x_2 x_3^3 x_4^2 \\
&\quad - x_1^2 x_2 x_4^3 + x_1 x_2^2 x_4^3 + x_1^2 x_3 x_4^3 - x_1 x_3^2 x_4^3 - x_2^2 x_3 x_4^3 + x_2 x_3^2 x_4^3 \\
&= x_1^3 x_2^2 x_3 - x_1^2 x_2^3 x_3 - x_1^3 x_2 x_3^2 + x_1^2 x_2 x_3^3 + x_1 x_2^3 x_3^2 - x_1 x_2^2 x_3^3 \\
&\quad - x_1^3 x_2^2 x_4 + x_1^2 x_2^3 x_4 + x_1^3 x_2 x_3 x_4 - x_1^2 x_3^3 x_4 - x_2^3 x_3^2 x_4 + x_2^2 x_3^3 x_4 \\
&\quad + x_1^3 x_2 x_4^2 - x_1^3 x_3 x_4^2 - x_1 x_2^2 x_4^2 + x_2^3 x_3 x_4^2 + x_1 x_3^3 x_4^2 - x_2 x_3^3 x_4^2 \\
&\quad - x_1^2 x_2 x_4^3 + x_1 x_2^2 x_4^3 + x_1^2 x_3 x_4^3 - x_1 x_3^2 x_4^3 - x_2^2 x_3 x_4^3 + x_2 x_3^2 x_4^3 . \quad \square
\end{aligned}$$

• **Appendix B.**

We prove what is postponed in the main text. We prove the following Lemma:

Lemma. Let $d \in \mathbb{Z}$, $d \geq 0$. Then there are

$$P_d(n) = \binom{d+n-1}{d} = \frac{n(n+1) \cdots (d+n-1)}{d!}$$

monomials of degree d in $\{x_1, \dots, x_n\}$.

Proof. The number of monomials in $\{x_1, \dots, x_n\}$ of degree d is the same as the number of $(i_1, \dots, i_n) \in \mathbb{Z}^n$ such that

$$i_1 \geq 0, \quad \dots, \quad i_n \geq 0, \quad i_1 + \dots + i_n = d.$$

This number is the same as the number of $(j_1, \dots, j_n) \in \mathbb{Z}^n$ such that

$$j_1 \geq 1, \quad \dots, \quad j_n \geq 1, \quad j_1 + \dots + j_n = d + n.$$

This number is the same as the number of ways to split consecutive $(d+n)$ letters

$$\lambda_1 \lambda_2 \cdots \lambda_{d+n}$$

into exactly n parts, preserving the order:

$$[\lambda_1 \cdots \lambda_{i_1}] \mid [\lambda_{i_1+1} \cdots \lambda_{i_2}] \mid [\cdots \cdots] \mid [\lambda_{i_{n-1}+1} \cdots \lambda_{d+n}]$$

so that each part contains at least one letter. Such number is equal to

$$\binom{d+n-1}{n-1} = \binom{d+n-1}{d}. \quad \square$$