1 Symmetric Polynomials

Copyright © 2026, Gregory G. Smith
Last Updated: 2026–01–013

Symmetric polynomials are fundamental to Galois theory because they link univariate polynomials with permutations.

1.0 Polynomials in Several Variables

What is the polynomial ring in n variables? Fix $n \in \mathbb{N}$. A polynomial in the indeterminates $x_1, x_2, \dots, x_n$ with coefficients in a field K is a finite sum of terms, which are expressions of the form

$$c x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n} := c \prod_{i=1}^{n} x_i^{u_i} \quad \text{where } c \in K \text{ and } u_i \in \mathbb{N} \text{ for all } 1 \leqslant i \leqslant n.$$

For all $u := (u_1, u_2, \dots, u_n) \in \mathbb{N}^n$, the product $x^u := x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n}$ is a *monomial*. A term cx^u is *nonzero* if its coefficient c is nonzero. The *total degree* of a nonzero term cx^u is $\|u\|_1 = u_1 + u_2 + \cdots + u_n \in \mathbb{N}$.

Richard Dedekind introduced the German word "Körper" (meaning "body" or "corpus") for a set of real or complex numbers that is closed under the arithmetic operations; see L. Dirichlet, P. Gustav, and R. Dedekind, *Vorlesungen über Zahlentheorie*, (1879). The English term "field" first appears in E.H. Moore, *A doubly-infinite system of simple groups*, Bull. New York Math. Soc. **3** (1893) 73–78.

The constant $1 := x_1^0 x_2^0 \cdots x_n^0$ is a monomial.

The set of all polynomials in $x_1, x_2, \dots, x_n$ with coefficients in the field K is denoted by $K[x_1, x_2, \dots, x_n]$; it forms a commutative ring (and a K-algebra) under the standard addition and multiplication of polynomials. Given a nonzero $f \in K[x_1, x_2, \dots, x_n]$, the *total degree* $\deg(f)$ is the maximum of the total degrees of the nonzero terms in the polynomial f. Since K is a domain, one verifies that

$$\deg(fg) = \deg(f) + \deg(g)$$

for all nonzero $f, g \in K[x_1, x_2, \dots, x_n]$. As a consequence, the ring $K[x_1, x_2, \dots, x_n]$ is also a domain. Since $K[x_1, x_2, \dots, x_n]$ is a domain, its field of fractions is

$$\begin{aligned} K(x_1, x_2, \dots, x_n) &:= K[x_1, x_2, \dots, x_n]_{\langle 0 \rangle} \\ &= \left\{ \frac{f}{g} \;\middle|\; f, g \in K[x_1, x_2, \dots, x_n] \text{ such that } g \neq 0 \right\}. \end{aligned}$$

This larger K-algebra is the *field of rational functions* in n variables.

A K-algebra is both a ring and a K-vector space; the addition operations coincide and multiplication is K-linear. A K-algebra homomorphism is a K-linear ring homomorphism.

Among all commutative K-algebras, polynomial rings over K are characterized by the homomorphisms emanating from them.

1.0.0 Theorem (Universal property of polynomial rings)**.** *Let K be field and let R be commutative ring containing K. For all ring elements $\alpha_1, \alpha_2, \dots, \alpha_n \in R$, there exists a unique K-algebra homomorphism from $K[x_1, x_2, \dots, x_n]$ to R that sends x_j to α_j for all $1 \leqslant j \leqslant n$. Moreover, every K-algebra homorphism from $K[x_1, x_2, \dots, x_n]$ to R is determined by such a choice of ring elements $\alpha_1, \alpha_2, \dots, \alpha_n \in R$.*

Idea of proof. Given $\alpha_1, \alpha_2, \dots, \alpha_n \in R$, the *evaluation map*

$$\mathrm{ev}_\alpha : K[x_1, x_2, \dots, x_n] \to R$$

defined by $\mathrm{ev}_\alpha(f) = f(\alpha_1, \alpha_2, \dots, \alpha_n) \in R$ for all $f \in K[x_1, x_2, \dots, x_n]$ is K-algebra homomorphism, and every K-algebra homomorphism from $K[x_1, x_2, \dots, x_n]$ is uniquely determined by the images of the variables $x_1, x_2, \dots, x_n$. □

We next consider a special family of multivariate polynomials.

1.0.1 Definition. The *elementary symmetric polynomials* in the ring $\mathbb{Z}[x_1, x_2, \dots, x_n]$ are

$$\begin{aligned}
e_1 = e_1(x_1, x_2, \dots, x_n) &:= \sum_{j=1}^{n} x_j = x_1 + x_2 + \cdots + x_n \\
e_2 = e_2(x_1, x_2, \dots, x_n) &:= \sum_{1 \leqslant j < k \leqslant n} x_j x_k = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\
&\vdots \\
e_r = e_r(x_1, x_2, \dots, x_n) &:= \sum_{1 \leqslant j_1 < j_2 < \cdots < j_r \leqslant n} x_{j_1} x_{j_2} \cdots x_{j_r} \\
&\vdots \\
e_n = e_n(x_1, x_2, \dots, x_n) &:= x_1 x_2 \cdots x_n \,.
\end{aligned}$$

For all $1 \leqslant r \leqslant n$, the terms in the polynomial e_r correspond bijectively to the r-element subset of the n-element set $[n] := \{1, 2, \dots, n\}$. In particular, e_r has $\binom{n}{r}$ terms.

1.0.2 Problem. When $n = 4$, list all terms in the four elementary symmetric polynomials.

Solution. By definition, we have

$$\begin{aligned}
e_1 &= x_1 + x_2 + x_3 + x_4 \\
e_2 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\
e_3 &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\
e_4 &= x_1x_2x_3x_4 \,.
\end{aligned}$$

□

1.0.3 Proposition. *In the ring* $(\mathbb{Z}[x_1, x_2, \dots, x_n])[x]$*, we have*

$$\begin{aligned}
&(x - x_1)(x - x_2) \cdots (x - x_n) \\
&= x^n - e_1 x^{n-1} + e_2 x^{n-2} - \cdots + (-1)^r e_r x^{x-r} + \cdots + (-1)^r e_r \,.
\end{aligned}$$

Proof. Expand the product $(x - x_1)(x - x_2) \cdots (x - x_n)$: For each of the n factors $x - x_j$, choose either x or $-x_j$, take the product of these n choices, and sum over all possible ways of making the n choices.

The terms involving x^{n-r} in $(x - x_1)(x - x_2) \cdots (x - x_n)$ are those products where x is choosen exactly $n - r$ times. Hence, there exists a subset $\{j_1, j_2, \dots, j_r\} \subseteq [n]$ such that $-x_{j_k}$ is chosen for the j_kth factors, for all $1 \leqslant k \leqslant r$, and x is chosen for the remaining $n - r$ factors. The product of these choices is

$$(-x_{j_1})(-x_{j_2}) \cdots (-x_{j_r}) x^{n-r} = (-1)^r x_{j_1} x_{j_2} \cdots x_{j_r} x^{n-r} \,.$$

Summing over all possible subsets, the coefficient of x^{n-r} is

$$(-1)^r \sum_{1 \leqslant j_1 < j_2 < \cdots < j_r \leqslant n} x_{j_1} x_{j_2} \cdots x_{j_r} = (-1)^r e_r \,.$$

□

1.0.4 Corollary. *Let* $f = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots a_{n-1} x + a_n$ *be a monic polynomial of degree* n *with coefficients in a field* K*. When* f *has roots* $\alpha_1, \alpha_2, \dots, \alpha_n$ *in a field* L *containing* K*, then the coefficients of* f *are expressed in terms of its roots as*

$$a_r = (-1)^r e_r(\alpha_1, \alpha_2, \dots, \alpha_r) \quad \textit{for all } 1 \leqslant r \leqslant n.$$

Proof. Since $\alpha_1, \alpha_2, \dots, \alpha_n$ are roots of the polynomial $f \in L[x]$, we have $f = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$. Hence, Proposition 1.0.3 implies that $a_r = (-1)^r e_r(\alpha_1, \alpha_2, \dots, \alpha_r)$ for all $1 \leqslant r \leqslant n$. □

Copyright © 2026 by Gregory G. Smith

1.1 Symmetric Polynomials

Which multivariate polynomials are invariant under the action of the symmetric group?

1.1.0 Definition. A polynomial $f \in \mathbb{Z}[x_1, x_2, \dots, x_n]$ is *symmetric* if

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

for all permutations σ in the symmetric group $\mathfrak{S}_n$. The symmetric polynomials form the *ring of invariants* $\mathbb{Z}[x_1, x_2, \dots, x_n]^{\mathfrak{S}_n}$ defined to be the subring $\{f \in \mathbb{Z}[x_1, x_2, \dots, x_n] \mid \sigma(f) = f \text{ for all } \sigma \in \mathfrak{S}_n\}$.

The sum and product of symmetric polynomials are also symmetric, and the unit 1 is symmetric.

1.1.1 Remark. For all $u \in \mathbb{N}^n$, the *monomial symmetric polynomial* $m_u \in \mathbb{Z}[x_1, x_2, \dots, x_n]$ is the sum of all monomials x^v where v ranges over all distinct permutations of $u = (u_1, u_2, \dots, u_n)$. For example, when $n = 3$, we have

$$m_{(3,2,1)} = x_1^3x_2^2x_3 + x_1^3x_2x_3^2 + x_1^2x_2^3x_3 + x_1^2x_2x_3^3 + x_1x_2^3x_3^2 + x_1x_2^2x_3^3,$$
$$m_{(2,1,1)} = x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2.$$

In the definition of the monomial symmetric polynomials, one may assume that $u_1 \geqslant u_2 \geqslant \cdots \geqslant u_n$.

1.1.2 Remark. For all $d \in \mathbb{N}$, the *complete homogeneous symmetric polynomial* $h_d \in \mathbb{Z}[x_1, x_2, \dots, x_n]$ is the sum of all monomials of total degree d. For example, when $n = 3$, we have

$$h_1 = x_1 + x_2 + x_3 + x_4 = e_1$$
$$h_2 = x_1^2 + x_1x_2 + x_1x_3 + x_2^2 + x_2x_3 + x_3^2$$
$$h_3 = x_1^3 + x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_2x_3 + x_1x_3^2 + x_2^3 + x_2^2x_3 + x_2x_3^2 + x_3^3.$$

1.1.3 The Fundamental Theorem of Symmetric Polynomials. *Every symmetric polynomial in the ring $\mathbb{Z}[x_1, x_2, \dots, x_n]$ can be expressed uniquely as a polynomial in the elementary symmetric polynomials with coefficients in $\mathbb{Z}$: $\mathbb{Z}[x_1, x_2, \dots, x_n]^{\mathfrak{S}_n} = \mathbb{Z}[e_1, e_2, \dots, e_n]$.*

Proof by Gauss (1816). To begin, we introduce another structure on the polynomial ring $\mathbb{Z}[x_1, x_2, \dots, x_n]$. The *graded lexicographic order* $>_{\text{glex}}$ on the monomials in $\mathbb{Z}[x_1, x_2, \dots, x_n]$ is defined by $x^u >_{\text{glex}} x^v$ when $\|u\|_1 > \|v\|_1$, or $\|u\|_1 = \|v\|_1$ and the first nonzero entry in the difference $u - v = (u_1 - v_1, u_2 - v_2, \dots, u_n - v_n)$ is positive. This total order has an important feature: given a monomial x^u, there are only finitely many monomials x^v such that $x^v < x^u$. Indeed, the inequality $\|u\|_1 = u_1 + u_2 + \cdots + u_n \geqslant v_1 + v_2 + \cdots + v_n = \|v\|_1$ implies that there are at most $1 + \|u\|_1$ possibilities for each v_j. The *leading term* of a polynomial in $\mathbb{Z}[x_1, x_2, \dots, x_n]$ is the term whose monomial is greatest with respect to $<_{\text{glex}}$.

The graded lexicographic order gives $x_1^2 >_{\text{glex}} x_1x_2 >_{\text{glex}} x_1x_3 >_{\text{glex}} x_2^2$.

For all $1 \leqslant r \leqslant n$, the leading term of the elementary symmetric polynomial e_r is $x_1x_2 \cdots x_r$.

Let $f \in \mathbb{Z}[x_1, x_2, \dots, x_n]$ be a nonzero symmetric polynomial with leading term is cx^u. We claim that $u_1 \geqslant u_2 \geqslant \cdots \geqslant u_n$. Otherwise there exists $1 \leqslant j < n$ such that $u_j < u_{j+1}$. Being symmetric, f is unchanged when x_j and x_{j+1} are swapped, so

$$cx^v := cx_1^{u_1}x_2^{u_2} \cdots x_j^{u_{j+1}}x_{j+1}^{u_j} \cdots x_n^{u_n}$$

is also a term in f. Since $\|u\|_1 = \|v\|_1$ and

$$v - u = (0, 0, \dots, u_{j+1} - u_j, u_j - u_{j+1}, 0, \dots, 0),$$

Copyright © 2026 by Gregory G. Smith

it follows that $x^v > x^u$, which contradicts the assumption that cx^u is the leading term.

Consider $g := e_1^{u_1-u_2} e_2^{u_2-u_3} \cdots e_{n-1}^{u_{n-1}-u_n} e_n^{u_n}$. Since the leading term of a product is a product of the leading terms, the leading term of the symmetric polynomial g is

$$\begin{aligned}(x_1)^{u_1-u_2}(x_1x_2)^{u_2-u_3}\cdots(x_1x_2\cdots x_{n-1})^{u_{n-1}-u_n}(x_1x_2\cdots x_n)^{u_n}\\ = x_1^{u_1-u_2+u_2-u_3+\cdots+u_n} x_2^{u_2-u_3+\cdots+u_n}\cdots x_{n-1}^{u_{n-1}-u_n+u_n} x_{n-1}^{u_n} = x^u\,.\end{aligned}$$

It follows that f and cg have the same leading term. Hence, $f - cg$ has a strictly smaller leading term. Moreover, the difference $f - cg$ is symmetric because f and g are.

Repeat the process starting with $f - cg$ instead of f. After finitely many repetitions, this process will terminate because there are only finitely many monomials less than the leading term of f. Thus, this algorithm expresses a symmetric polynomials as a polynomial in the elementary symmetric polynomials $e_1, e_2, \ldots, e_n$.

It remains to see that this expression is unique. Suppose that there is $0 \neq h \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ such that $h(e_1, e_2, \ldots, e_n) = 0$. If cx^w is a term in h, then $cx_1^{w_1+w_2+\cdots+w_n} x_2^{w_2+w_3+\cdots+w_n} \cdots x_n^{w_n}$ is the leading term in the product $ce_1^{w_1} e_2^{w_2} \ldots e_n^{w_n}$. Since the linear map

$$(w_1, w_2, \ldots, w_n) \mapsto (w_1 + w_2 + \cdots + w_n, w_2 + w_3 + \cdots + w_n, \ldots, w_n)$$

is injective, all other terms in the expansion of $h(e_1, e_2, \ldots, e_n)$ have different leading terms. Hence, the leading term is not cancelled by any other monomial, so $h(e_1, e_2, \ldots, e_n) \neq 0$. This contradiction established uniqueness. □

Since there a no nontrivial polynomial relations among the $e_1, e_2, \ldots, e_r$, this collection of polynomials is *algebraically independent.*

1.1.4 Problem. Express the symmetric polynomial $h_2 \in \mathbb{Z}[x_1, x_2, x_3]$ as polynomial in the elementary symmetric polynomials.

Solution. Since the leading term of h_2 is x_1^2, we first consider

$$\begin{aligned}h_2 - (e_1)^2 &= x_1^2 + x_1x_2 + x_1x_3 + x_2^2 + x_2x_3 + x_3^2 - (x_1 + x_2 + x_3)^2\\ &= -x_1x_2 - x_1x_3 - x_2x_2\,.\end{aligned}$$

We deduce that $h_2 = e_1^2 - e_2$. □

1.1.5 Corollary. *Let $f \in K[x]$ be a monic polynomial of degree n and having roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ in a field L containing K. For all symmetric polynomials $g \in K[x_1, x_2, \ldots, x_n]$, we have $g(\alpha_1, \alpha_2, \ldots, \alpha_n) \in K$.*

Proof. The evaluation map from $K[x_1, x_2, \ldots, x_n]$ to L determined by the roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ is a K-algebra homomorphism. The Fundamental Theorem of Symmetric Polynomials establishes that the symmetric polynomial g is the elementary symmetric polynomials with coefficients in K. Hence, evaluation at $\alpha_1, \alpha_2, \ldots, \alpha_n$ is a polynomial in the $e_r(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for all $1 \leqslant r \leqslant n$. Corollary 1.0.4 shows that, up to sign, each $e_r(\alpha_1, \alpha_2, \ldots, \alpha_n) \in K$ is a coefficient of f. Since $f \in K[x]$, we conclude that $e_r(\alpha_1, \alpha_2, \ldots, \alpha_n) \in K$. □

Copyright © 2026 by Gregory G. Smith

1.2 The Discriminant

How can we define the discriminant for all univariate polynomials?

The word "discriminant" was coined in J.J. Sylvester, *On a remarkable discovery in the theory of canonical forms and of hyperdeterminants*, Philos. Mag. (2), **12** (1851), 391–410.

1.2.0 Definition. The *discriminant* is the polynomial

$$\Delta := \prod_{1 \leqslant j < k \leqslant n} (x_j - x_k)^2 \in \mathbb{Z}[x_1, x_2, \dots, x_n] .$$

1.2.1 Remark. There are $\binom{n}{2}$ factors in the defining product of Δ. Since $(x_j - x_k)^2 = -(x_j - x_k)(x_k - x_j)$, we see that

$$\Delta := (-1)^{n(n-1)/2} \prod_{j \neq k} (x_j - x_k) \in \mathbb{Z}[x_1, x_2, \dots, x_n] .$$

In particular, the discriminant is invariant under any transposition. We conclude that Δ is a symmetric polynomial.

1.2.2 Problem. Express the discriminant $\Delta \in \mathbb{Z}[x_1, x_2, x_3]$ as a polynomial in the elementary symmetric polynomials.

Solution. We have

$$\begin{aligned} \Delta &= (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_2)^2 \\ &= x_1^4 x_2^2 - 2x_1^3 x_2^3 + \cdots - 2x_1^4 x_2 x_3 + 2x_1^3 x_2^2 x_3 + \cdots - 6x_1^2 x_2^2 x_3^2 + \cdots + x_2^2 x_3^4 \\ &= e_1^2 e_2^2 - 4e_2^3 - 4e_1^3 e_3 + 18 e_1 e_2 e_3 - 27 e_3^2 . \end{aligned}$$

□

From the definition of the discriminant, we see that

$$\begin{aligned} \sqrt{\Delta} &:= \prod_{1 \leqslant j < k \leqslant n} (x_j - x_k) \in \mathbb{Z}[x_1, x_2, \dots, x_n] \\ &= \det \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-2} & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-2} & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-2} & x_n^{n-1} \end{bmatrix} . \end{aligned}$$

This is the *Vandermonde* matrix.

1.2.3 Remark. For all $d \in \mathbb{N}$, the *power sum symmetric polynomials* $p_d \in K[x_1, x_2, \dots, x_n]$ is the sum of all dth powers of the variables: $p_d = \sum_{j=1}^{n} x_j^d$. For example, when $n = 3$, we have

$$\begin{aligned} p_1 &= x_1 + x_2 + x_3 = e_1 , \\ p_2 &= x_1^2 + x_2^2 + x_3^2 = e_1^2 - 2e_2 , \\ p_3 &= x_1^3 + x_2^3 + x_3^3 = e_1^3 - 3e_1 e_2 + 3e_3 . \end{aligned}$$

It follows that

$$\begin{aligned} \Delta &= \left(\det \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-2} & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-2} & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-2} & x_n^{n-1} \end{bmatrix} \right)^2 \\ &= \det \left(\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ x_1 & x_2 & x_3 & \cdots & x_{n-2} & x_n \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \cdots & x_{n-1}^{n-1} & x_n^{n-1} \end{bmatrix} \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-2} & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-2} & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-2} & x_n^{n-1} \end{bmatrix} \right) \\ &= \det \begin{bmatrix} p_0 & p_1 & p_2 & \cdots & p_{n-1} & p_{n-1} \\ p_1 & p_3 & p_4 & \cdots & p_{n-1} & p_n \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ p_{n-1} & p_n & p_{n+1} & \cdots & p_{2n-3} & p_{2n-2} \end{bmatrix} . \end{aligned}$$

Copyright © 2026 by Gregory G. Smith

1.2.4 Proposition. *For all $\sigma \in \mathfrak{S}_n$, we have $\sigma(\sqrt{\Delta}) = \operatorname{sgn}(\sigma)\sqrt{\Delta}$.*

Proof. Suppose that $\sigma := (i \;\; j)$. Observe that

$$\begin{aligned}\sigma(\sqrt{\Delta}) &= \sigma((x_i - x_j)) \prod_{k\neq i,j} (x_i - x_k)(x_j - x_k) \prod_{\substack{\ell,m\neq i,j \\ \ell<m}} (x_\ell - x_m) \\ &= (x_j - x_i) \prod_{k\neq i,j} (x_i - x_k)(x_j - x_k) \prod_{\substack{\ell,m\neq i,j \\ \ell<m}} (x_\ell - x_m) \\ &= -\sigma(\sqrt{\Delta}) .\end{aligned}$$

Every permutation is a product $\sigma = \tau_1\tau_2\cdots\tau_\ell$ of transpositions, so we obtain $\sigma(\sqrt{\Delta}) = (\tau_1\tau_2\cdots\tau_\ell)(\sqrt{\Delta}) = (-1)^\ell\sqrt{\Delta} = \operatorname{sgn}(\sigma)\sqrt{\Delta}$. □

The discriminant of a monic polynomial is obtain from this more general discriminant polynomial.

1.2.5 Definition. The *discriminant* of a monic polynomial

$$f = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_jx^{n-j} + \cdots + a_n \in K[x]$$

of positive degree n is defined to be

$$\Delta(f) := \Delta(-a_1, a_2, \ldots, (-1)^j a_j, \ldots, (-1)^n a_n) \in K ,$$

where Δ is regarded as a polynomial in $K[e_1, e_2, \ldots, e_n]$.

The evaluation map $e_r \mapsto (-1)^j a_r$ sends the Δ to $\Delta(f)$.

1.2.6 Problem. When $f = x^2 + bx + c$, verify that $\Delta(f) = b^2 - 4c$.

Solution. When α_1, α_2 denote the roots of f, we have

$$\begin{aligned}\Delta(f) = (\alpha_1 - \alpha_2)^2 &= \alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2 \\ &= \big(e_1(\alpha_1, \alpha_2)\big)^2 - 4e_2(\alpha_1, \alpha_2) = b^2 - 4c .\end{aligned}$$ □

1.2.7 Proposition. *For any monic polynomial $f \in K[x]$ having degree n and roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ in a field L containing K, we have*

$$\Delta(f) = \prod_{1\leqslant j<k\leqslant n} (\alpha_j - \alpha_k)^2 .$$

Proof. Observe that

$$\operatorname{ev}_\alpha(\Delta) = \operatorname{ev}_\alpha\left(\prod_{1\leqslant j<k\leqslant n} (x_j - x_k)^2\right) = \prod_{1\leqslant j<k\leqslant n} (\alpha_j - \alpha_k)^2 .$$

Since Δ is symmetric, the image $\operatorname{ev}_\alpha(\Delta)$ can be expressed uniquely as a polynomial in $\operatorname{ev}_\alpha(e_1), \operatorname{ev}_\alpha(e_2), \ldots, \operatorname{ev}_\alpha(e_n)$. Corollary 1.0.4 shows that $a_r = (-1)^r e_r(\alpha_1, \alpha_2, \ldots, \alpha_n) = (-1)^r \operatorname{ev}_\alpha(e_r)$ for all $1 \leqslant r \leqslant n$, so we conclude that $\operatorname{ev}_\alpha(\Delta) = \Delta(f)$. □

1.2.8 Corollary. *Let $f \in K[x]$ be monic polynomial having degree n and roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ in a field L containing K. The discriminant $\Delta(f)$ equals zero if and only if at least two roots coincide.*

Proof. Proposition 1.2.7 establishes that $\Delta(f) = \prod_{1\leqslant j<k\leqslant n}(\alpha_j - \alpha_k)^2$. Since L is a domain, this product equals zero if and only if at least one of the factor equals zero. □

Copyright © 2026 by Gregory G. Smith