Math 361

February 8, 2023

Quiz

1. Let $A \subseteq B$ be domains. What does it mean to say the $\alpha \in B$ is *integral* over A?
2. Define the following terms:
   (i) Number field.
   (ii) Algebraic number.
   (iii) Algebraic integer.

Today

Today we will prove that the discriminant of a $\mathbb{Q}$-basis for a number field is a rational number. It's a rational integer if the basis consists of algebraic integers.

Today

Today we will prove that the discriminant of a $\mathbb{Q}$-basis for a number field is a rational number. It's a rational integer if the basis consists of algebraic integers.

To prove this theorem we need some tools:

Today

Today we will prove that the discriminant of a $\mathbb{Q}$-basis for a number field is a rational number. It's a rational integer if the basis consists of algebraic integers.

To prove this theorem we need some tools:

- the Vandermonde matrix

Today

Today we will prove that the discriminant of a $\mathbb{Q}$-basis for a number field is a rational number. It's a rational integer if the basis consists of algebraic integers.

To prove this theorem we need some tools:

- the Vandermonde matrix
- symmetric polynomials.

The discriminant

Number field: $K = \mathbb{Q}(\theta)$ with $[K : \mathbb{Q}] = n$. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial of θ.

The discriminant

Number field: $K = \mathbb{Q}(\theta)$ with $[K : \mathbb{Q}] = n$. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial of θ.

$K = \mathrm{Span}_{\mathbb{Q}}\{1, \theta, \ldots, \theta^{n-1}\}$.

The discriminant

Number field: $K = \mathbb{Q}(\theta)$ with $[K : \mathbb{Q}] = n$. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial of θ.

$K = \mathrm{Span}_{\mathbb{Q}}\{1, \theta, \ldots, \theta^{n-1}\}$.

Minimal polynomial for θ: $p = \prod_{i=1}^{n}(x - \theta_i)$ with θ_i distinct.

The discriminant

Number field: $K = \mathbb{Q}(\theta)$ with $[K : \mathbb{Q}] = n$. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial of θ.

$K = \mathrm{Span}_{\mathbb{Q}}\{1, \theta, \ldots, \theta^{n-1}\}$.

Minimal polynomial for θ: $p = \prod_{i=1}^{n}(x - \theta_i)$ with θ_i distinct.

Field embeddings $K \to \mathbb{C}$ given by $\sigma_i : \theta \mapsto \theta_i$.

The discriminant

Number field: $K = \mathbb{Q}(\theta)$ with $[K : \mathbb{Q}] = n$. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial of θ.

$K = \mathrm{Span}_{\mathbb{Q}}\{1, \theta, \ldots, \theta^{n-1}\}$.

Minimal polynomial for θ: $p = \prod_{i=1}^{n}(x - \theta_i)$ with θ_i distinct.

Field embeddings $K \to \mathbb{C}$ given by $\sigma_i : \theta \mapsto \theta_i$.

Definition. The *discriminant* for a basis $\alpha_1, \ldots, \alpha_n$ for K over $\mathbb{Q}$: is the square of the determinant of the $n \times n$ matrix with i, j-th entry $\sigma_i(\alpha_j)$:

The discriminant

Number field: $K = \mathbb{Q}(\theta)$ with $[K : \mathbb{Q}] = n$. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial of θ.

$K = \mathrm{Span}_{\mathbb{Q}}\{1, \theta, \ldots, \theta^{n-1}\}$.

Minimal polynomial for θ: $p = \prod_{i=1}^{n}(x - \theta_i)$ with θ_i distinct.

Field embeddings $K \to \mathbb{C}$ given by $\sigma_i : \theta \mapsto \theta_i$.

Definition. The *discriminant* for a basis $\alpha_1, \ldots, \alpha_n$ for K over $\mathbb{Q}$: is the square of the determinant of the $n \times n$ matrix with i, j-th entry $\sigma_i(\alpha_j)$:

$$\Delta[\alpha_1, \ldots, \alpha_n] := \left(\det(\sigma_i(\alpha_j))\right)^2 .$$

The discriminant

Number field: $K = \mathbb{Q}(\theta)$ with $[K : \mathbb{Q}] = n$. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial of θ.

$K = \mathrm{Span}_{\mathbb{Q}}\{1, \theta, \ldots, \theta^{n-1}\}$.

Minimal polynomial for θ: $p = \prod_{i=1}^{n}(x - \theta_i)$ with θ_i distinct.

Field embeddings $K \to \mathbb{C}$ given by $\sigma_i : \theta \mapsto \theta_i$.

Definition. The *discriminant* for a basis $\alpha_1, \ldots, \alpha_n$ for K over $\mathbb{Q}$: is the square of the determinant of the $n \times n$ matrix with i, j-th entry $\sigma_i(\alpha_j)$:

$$\Delta[\alpha_1, \ldots, \alpha_n] := \left(\det(\sigma_i(\alpha_j))\right)^2 .$$

Example. Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer $\neq 0, 1$.

The discriminant

Number field: $K = \mathbb{Q}(\theta)$ with $[K : \mathbb{Q}] = n$. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial of θ.

$K = \mathrm{Span}_{\mathbb{Q}}\{1, \theta, \ldots, \theta^{n-1}\}$.

Minimal polynomial for θ: $p = \prod_{i=1}^{n}(x - \theta_i)$ with θ_i distinct.

Field embeddings $K \to \mathbb{C}$ given by $\sigma_i : \theta \mapsto \theta_i$.

Definition. The *discriminant* for a basis $\alpha_1, \ldots, \alpha_n$ for K over $\mathbb{Q}$: is the square of the determinant of the $n \times n$ matrix with i, j-th entry $\sigma_i(\alpha_j)$:

$$\Delta[\alpha_1, \ldots, \alpha_n] := \left(\det(\sigma_i(\alpha_j))\right)^2 .$$

Example. Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer $\neq 0, 1$. Then

$$\Delta[1, \sqrt{d}] =$$

The discriminant

Number field: $K = \mathbb{Q}(\theta)$ with $[K : \mathbb{Q}] = n$. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial of θ.

$K = \mathrm{Span}_{\mathbb{Q}}\{1, \theta, \ldots, \theta^{n-1}\}$.

Minimal polynomial for θ: $p = \prod_{i=1}^{n}(x - \theta_i)$ with θ_i distinct.

Field embeddings $K \to \mathbb{C}$ given by $\sigma_i : \theta \mapsto \theta_i$.

Definition. The *discriminant* for a basis $\alpha_1, \ldots, \alpha_n$ for K over $\mathbb{Q}$: is the square of the determinant of the $n \times n$ matrix with i, j-th entry $\sigma_i(\alpha_j)$:

$$\Delta[\alpha_1, \ldots, \alpha_n] := \left(\det(\sigma_i(\alpha_j))\right)^2.$$

Example. Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer $\neq 0, 1$. Then

$$\Delta[1, \sqrt{d}] = \left(\det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}\right)^2 = (-2\sqrt{d})^2 = 4d.$$

The discriminant

Proposition. Let $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ be bases for the number field K over $\mathbb{Q}$.

The discriminant

Proposition. Let $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ be bases for the number field K over $\mathbb{Q}$. Let C be the change of basis matrix from the α_i to the β_i.

The discriminant

Proposition. Let $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ be bases for the number field K over $\mathbb{Q}$. Let C be the change of basis matrix from the α_i to the β_i. Then

$$\Delta[\beta_1, \ldots, \beta_n] = (\det C)^2 \Delta[\alpha_1, \ldots, \alpha_n].$$

The discriminant

Theorem. Let $K = \mathbb{Q}(\theta)$ be a number field, with embeddings σ_i and with $\theta_i = \sigma_i(\theta)$ for $i = 1, \ldots, n$.

The discriminant

Theorem. Let $K = \mathbb{Q}(\theta)$ be a number field, with embeddings σ_i and with $\theta_i = \sigma_i(\theta)$ for $i = 1, \ldots, n$. Let $\alpha_1, \ldots, \alpha_n$ be a basis for K over $\mathbb{Q}$.

The discriminant

Theorem. Let $K = \mathbb{Q}(\theta)$ be a number field, with embeddings σ_i and with $\theta_i = \sigma_i(\theta)$ for $i = 1, \ldots, n$. Let $\alpha_1, \ldots, \alpha_n$ be a basis for K over $\mathbb{Q}$.

Then the discriminant $\Delta[\alpha_1, \ldots, \alpha_n]$ is a nonzero rational number.

The discriminant

Theorem. Let $K = \mathbb{Q}(\theta)$ be a number field, with embeddings σ_i and with $\theta_i = \sigma_i(\theta)$ for $i = 1, \ldots, n$. Let $\alpha_1, \ldots, \alpha_n$ be a basis for K over $\mathbb{Q}$.

Then the discriminant $\Delta[\alpha_1, \ldots, \alpha_n]$ is a nonzero rational number. It is positive if all of the θ_i are real.

The discriminant

Theorem. Let $K = \mathbb{Q}(\theta)$ be a number field, with embeddings σ_i and with $\theta_i = \sigma_i(\theta)$ for $i = 1, \ldots, n$. Let $\alpha_1, \ldots, \alpha_n$ be a basis for K over $\mathbb{Q}$.

Then the discriminant $\Delta[\alpha_1, \ldots, \alpha_n]$ is a nonzero rational number.
It is positive if all of the θ_i are real.
It is a rational integer if the α_i are algebraic integers.

The discriminant

Theorem. Let $K = \mathbb{Q}(\theta)$ be a number field, with embeddings σ_i and with $\theta_i = \sigma_i(\theta)$ for $i = 1, \ldots, n$. Let $\alpha_1, \ldots, \alpha_n$ be a basis for K over $\mathbb{Q}$.

Then the discriminant $\Delta[\alpha_1, \ldots, \alpha_n]$ is a nonzero rational number.
It is positive if all of the θ_i are real.
It is a rational integer if the α_i are algebraic integers.

To prove this theorem we need some tools:

The discriminant

Theorem. Let $K = \mathbb{Q}(\theta)$ be a number field, with embeddings σ_i and with $\theta_i = \sigma_i(\theta)$ for $i = 1, \ldots, n$. Let $\alpha_1, \ldots, \alpha_n$ be a basis for K over $\mathbb{Q}$.

Then the discriminant $\Delta[\alpha_1, \ldots, \alpha_n]$ is a nonzero rational number.
It is positive if all of the θ_i are real.
It is a rational integer if the α_i are algebraic integers.

To prove this theorem we need some tools:

- Vandermonde matrix
- symmetric polynomials.

Vandermonde

Vandermonde matrix. Let $x_1, \ldots, x_n$ be indeterminates, and consider the $n \times n$ matrix

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \ldots & x_3^{n-1} \\ 1 & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{pmatrix}.$$

Vandermonde

Vandermonde matrix. Let $x_1, \ldots, x_n$ be indeterminates, and consider the $n \times n$ matrix

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \ldots & x_3^{n-1} \\ 1 & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{pmatrix}.$$

Then

$$\det V = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Vandermonde

Vandermonde matrix. Let $x_1, \ldots, x_n$ be indeterminates, and consider the $n \times n$ matrix

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \ldots & x_3^{n-1} \\ 1 & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{pmatrix}.$$

Then

$$\det V = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Sketch of proof.

Vandermonde

Vandermonde matrix. Let $x_1, \ldots, x_n$ be indeterminates, and consider the $n \times n$ matrix

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \ldots & x_3^{n-1} \\ 1 & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{pmatrix}.$$

Then

$$\det V = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Sketch of proof. $\det V \in \mathbb{Q}[x_1, \ldots, x_n]$,

Vandermonde

Vandermonde matrix. Let $x_1, \ldots, x_n$ be indeterminates, and consider the $n \times n$ matrix

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \ldots & x_3^{n-1} \\ 1 & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{pmatrix}.$$

Then

$$\det V = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Sketch of proof. $\det V \in \mathbb{Q}[x_1, \ldots, x_n]$, and if we set $x_i = x_j$, then $\det(V) = 0$ (why?).

Vandermonde

Vandermonde matrix. Let $x_1, \ldots, x_n$ be indeterminates, and consider the $n \times n$ matrix

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \ldots & x_3^{n-1} \\ 1 & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{pmatrix}.$$

Then

$$\det V = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Sketch of proof. $\det V \in \mathbb{Q}[x_1, \ldots, x_n]$, and if we set $x_i = x_j$, then $\det(V) = 0$ (why?). Algebra implies $x_j - x_i$ divides $\det V$ for all $1 \le i < j \le n$.

Vandermonde

Vandermonde matrix. Let $x_1, \ldots, x_n$ be indeterminates, and consider the $n \times n$ matrix

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \ldots & x_3^{n-1} \\ 1 & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{pmatrix}.$$

Then

$$\det V = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Sketch of proof. $\det V \in \mathbb{Q}[x_1, \ldots, x_n]$, and if we set $x_i = x_j$, then $\det(V) = 0$ (why?). Algebra implies $x_j - x_i$ divides $\det V$ for all $1 \le i < j \le n$. Compare degrees on both sides of the equation

Vandermonde

Vandermonde matrix. Let $x_1, \ldots, x_n$ be indeterminates, and consider the $n \times n$ matrix

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \ldots & x_3^{n-1} \\ 1 & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{pmatrix}.$$

Then

$$\det V = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Sketch of proof. $\det V \in \mathbb{Q}[x_1, \ldots, x_n]$, and if we set $x_i = x_j$, then $\det(V) = 0$ (why?). Algebra implies $x_j - x_i$ divides $\det V$ for all $1 \le i < j \le n$. Compare degrees on both sides of the equation to see $\det V = r \prod_{1 \le i < j \le n}(x_j - x_i)$ for some $r \in \mathbb{Q}$.

Vandermonde

Vandermonde matrix. Let $x_1, \ldots, x_n$ be indeterminates, and consider the $n \times n$ matrix

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \ldots & x_3^{n-1} \\ 1 & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{pmatrix}.$$

Then

$$\det V = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Sketch of proof. $\det V \in \mathbb{Q}[x_1, \ldots, x_n]$, and if we set $x_i = x_j$, then $\det(V) = 0$ (why?). Algebra implies $x_j - x_i$ divides $\det V$ for all $1 \le i < j \le n$. Compare degrees on both sides of the equation to see $\det V = r \prod_{1 \le i < j \le n}(x_j - x_i)$ for some $r \in \mathbb{Q}$. Compare coefficient of $x_2 x_3^2 \cdots x_n^{n-1}$ on both sides

Vandermonde

Vandermonde matrix. Let $x_1, \ldots, x_n$ be indeterminates, and consider the $n \times n$ matrix

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \ldots & x_3^{n-1} \\ 1 & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{pmatrix}.$$

Then

$$\det V = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Sketch of proof. $\det V \in \mathbb{Q}[x_1, \ldots, x_n]$, and if we set $x_i = x_j$, then $\det(V) = 0$ (why?). Algebra implies $x_j - x_i$ divides $\det V$ for all $1 \le i < j \le n$. Compare degrees on both sides of the equation to see $\det V = r \prod_{1 \le i < j \le n}(x_j - x_i)$ for some $r \in \mathbb{Q}$. Compare coefficient of $x_2 x_3^2 \cdots x_n^{n-1}$ on both sides to see $r = 1$. $\square$

Symmetric polynomials

Let $f \in R[x_1, \ldots, x_n]$ where R is a ring.

Symmetric polynomials

Let $f \in R[x_1, \ldots, x_n]$ where R is a ring. Let π be a permutation of $1, \ldots, n$.

Symmetric polynomials

Let $f \in R[x_1, \ldots, x_n]$ where R is a ring. Let π be a permutation of $1, \ldots, n$. Define $f^\pi \in R[x_1, \ldots, x_n]$ by

$$f^\pi(x_1, \ldots, x_n) = f\big(x_{\pi(1)}, \ldots, x_{\pi(n)}\big).$$

Symmetric polynomials

Let $f \in R[x_1, \ldots, x_n]$ where R is a ring. Let π be a permutation of $1, \ldots, n$. Define $f^\pi \in R[x_1, \ldots, x_n]$ by

$$f^\pi(x_1, \ldots, x_n) = f\big(x_{\pi(1)}, \ldots, x_{\pi(n)}\big).$$

Example. Let $f = 3x_1^2 - 5x_2x_3 + x_1x_4^3$,

Symmetric polynomials

Let $f \in R[x_1, \ldots, x_n]$ where R is a ring. Let π be a permutation of $1, \ldots, n$. Define $f^\pi \in R[x_1, \ldots, x_n]$ by

$$f^\pi(x_1, \ldots, x_n) = f\big(x_{\pi(1)}, \ldots, x_{\pi(n)}\big).$$

Example. Let $f = 3x_1^2 - 5x_2x_3 + x_1x_4^3$, and let π be the permutation $\pi(1) = 3$, $\pi(2) = 1$, $\pi(3) = 4$, and $\pi(4) = 2$,

Symmetric polynomials

Let $f \in R[x_1, \ldots, x_n]$ where R is a ring. Let π be a permutation of $1, \ldots, n$. Define $f^\pi \in R[x_1, \ldots, x_n]$ by

$$f^\pi(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)}).$$

Example. Let $f = 3x_1^2 - 5x_2x_3 + x_1x_4^3$, and let π be the permutation $\pi(1) = 3$, $\pi(2) = 1$, $\pi(3) = 4$, and $\pi(4) = 2$, Then $f^\pi = 3x_3^2 - 5x_1x_4 + x_3x_2^3$.

Symmetric polynomials

Let $f \in R[x_1, \ldots, x_n]$ where R is a ring. Let π be a permutation of $1, \ldots, n$. Define $f^\pi \in R[x_1, \ldots, x_n]$ by

$$f^\pi(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)}).$$

Example. Let $f = 3x_1^2 - 5x_2x_3 + x_1x_4^3$, and let π be the permutation $\pi(1) = 3$, $\pi(2) = 1$, $\pi(3) = 4$, and $\pi(4) = 2$, Then $f^\pi = 3x_3^2 - 5x_1x_4 + x_3x_2^3$.

Definition. f is *symmetric* if $f = f^\pi$ for all permutations π.

Symmetric polynomials

Let $f \in R[x_1, \ldots, x_n]$ where R is a ring. Let π be a permutation of $1, \ldots, n$. Define $f^\pi \in R[x_1, \ldots, x_n]$ by

$$f^\pi(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)}).$$

Example. Let $f = 3x_1^2 - 5x_2x_3 + x_1x_4^3$, and let π be the permutation $\pi(1) = 3$, $\pi(2) = 1$, $\pi(3) = 4$, and $\pi(4) = 2$, Then $f^\pi = 3x_3^2 - 5x_1x_4 + x_3x_2^3$.

Definition. f is *symmetric* if $f = f^\pi$ for all permutations π.

Example. f in the above examples is not symmetric.

Symmetric polynomials

Let $f \in R[x_1, \ldots, x_n]$ where R is a ring. Let π be a permutation of $1, \ldots, n$. Define $f^\pi \in R[x_1, \ldots, x_n]$ by

$$f^\pi(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)}).$$

Example. Let $f = 3x_1^2 - 5x_2x_3 + x_1x_4^3$, and let π be the permutation $\pi(1) = 3$, $\pi(2) = 1$, $\pi(3) = 4$, and $\pi(4) = 2$, Then $f^\pi = 3x_3^2 - 5x_1x_4 + x_3x_2^3$.

Definition. f is *symmetric* if $f = f^\pi$ for all permutations π.

Example. f in the above examples is not symmetric.

What are some examples of symmetric functions?

Examples

For $1 \leq r \leq n$, the *elementary symmetric polynomials* in $x_1, \ldots, x_n$ are $s_r(x_1, \ldots, x_n)$ formed by summing all products of exactly r of the indeterminates $x_1, \ldots, x_n$:

Examples

For $1 \leq r \leq n$, the *elementary symmetric polynomials* in $x_1, \ldots, x_n$ are $s_r(x_1, \ldots, x_n)$ formed by summing all products of exactly r of the indeterminates $x_1, \ldots, x_n$:

$$s_1 = x_1 + x_2 + \cdots + x_n$$

Examples

For $1 \leq r \leq n$, the *elementary symmetric polynomials* in $x_1, \ldots, x_n$ are $s_r(x_1, \ldots, x_n)$ formed by summing all products of exactly r of the indeterminates $x_1, \ldots, x_n$:

$$s_1 = x_1 + x_2 + \cdots + x_n$$
$$s_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n$$

Examples

For $1 \leq r \leq n$, the *elementary symmetric polynomials* in $x_1, \ldots, x_n$ are $s_r(x_1, \ldots, x_n)$ formed by summing all products of exactly r of the indeterminates $x_1, \ldots, x_n$:

$$
\begin{aligned}
s_1 &= x_1 + x_2 + \cdots + x_n \\
s_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\
&\vdots \\
s_n &= x_1x_2 \ldots x_n.
\end{aligned}
$$

Examples

For $1 \leq r \leq n$, the *elementary symmetric polynomials* in $x_1, \ldots, x_n$ are $s_r(x_1, \ldots, x_n)$ formed by summing all products of exactly r of the indeterminates $x_1, \ldots, x_n$:

$$
\begin{aligned}
s_1 &= x_1 + x_2 + \cdots + x_n \\
s_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\
&\vdots \\
s_n &= x_1x_2 \ldots x_n.
\end{aligned}
$$

Is $2s_1^2 - 5s_2^2s_5^4$ symmetric?

Examples

For $1 \leq r \leq n$, the *elementary symmetric polynomials* in $x_1, \ldots, x_n$ are $s_r(x_1, \ldots, x_n)$ formed by summing all products of exactly r of the indeterminates $x_1, \ldots, x_n$:

$$
\begin{aligned}
s_1 &= x_1 + x_2 + \cdots + x_n \\
s_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\
&\vdots \\
s_n &= x_1x_2 \ldots x_n.
\end{aligned}
$$

Is $2s_1^2 - 5s_2^2s_5^4$ symmetric?

Answer: Yes. In general, if $h \in R[x_1, \ldots, x_n]$, then $h(s_1, \ldots, s_n)$ is symmetric.

Symmetric functions

Theorem. (I. Newton) Let R be a ring, and let $f \in R[x_1, \ldots, x_n]$.

Symmetric functions

Theorem. (I. Newton) Let R be a ring, and let $f \in R[x_1, \ldots, x_n]$. Then f is symmetric if and only if there exists $h \in R[x_1, \ldots, x_n]$ such that

$$f = h(s_1, \ldots, s_n)$$

where the s_i are the elementary symmetric polynomials.

Symmetric functions

Theorem. (I. Newton) Let R be a ring, and let $f \in R[x_1, \ldots, x_n]$. Then f is symmetric if and only if there exists $h \in R[x_1, \ldots, x_n]$ such that

$$f = h(s_1, \ldots, s_n)$$

where the s_i are the elementary symmetric polynomials.

Proof. See our textbook, Theorem 1.12.

Connection between symmetric functions and our subject

Suppose $f \in \mathbb{Q}[x]$ is monic of degree 4.

Connection between symmetric functions and our subject

Suppose $f \in \mathbb{Q}[x]$ is monic of degree 4. Then by the FTA, there exist $\theta_1, \ldots, \theta_4$ such that

$$f = (x - \theta_1)(x - \theta_2)(x - \theta_3)(x - \theta_4).$$

Connection between symmetric functions and our subject

Suppose $f \in \mathbb{Q}[x]$ is monic of degree 4. Then by the FTA, there exist $\theta_1, \ldots, \theta_4$ such that

$$f = (x - \theta_1)(x - \theta_2)(x - \theta_3)(x - \theta_4).$$

Expand:

$$\begin{aligned} f = x^4 - (\theta_1 + \cdots + \theta_4)x^3 + (\theta_1\theta_2 + \cdots + \theta_3\theta_4)x^2 \\ - (\theta_1\theta_2\theta_3 + \cdots + \theta_2\theta_3\theta_4)x + (\theta_1\theta_2\theta_3\theta_4) \end{aligned}$$

Connection between symmetric functions and our subject

Suppose $f \in \mathbb{Q}[x]$ is monic of degree 4. Then by the FTA, there exist $\theta_1, \ldots, \theta_4$ such that

$$f = (x - \theta_1)(x - \theta_2)(x - \theta_3)(x - \theta_4).$$

Expand:

$$\begin{aligned} f &= x^4 - (\theta_1 + \cdots + \theta_4)x^3 + (\theta_1\theta_2 + \cdots + \theta_3\theta_4)x^2 \\ &\quad - (\theta_1\theta_2\theta_3 + \cdots + \theta_2\theta_3\theta_4)x + (\theta_1\theta_2\theta_3\theta_4) \\ &= x^4 - s_1(\theta_1, \theta_2, \theta_3, \theta_4)x^3 + s_2(\theta_1, \theta_2, \theta_3, \theta_4)x^2 \\ &\quad - s_3(\theta_1, \theta_2, \theta_3, \theta_4)x + s_4(\theta_1, \theta_2, \theta_3, \theta_4). \end{aligned}$$

Connection between symmetric functions and our subject

Suppose $f \in \mathbb{Q}[x]$ is monic of degree 4. Then by the FTA, there exist $\theta_1, \ldots, \theta_4$ such that

$$f = (x - \theta_1)(x - \theta_2)(x - \theta_3)(x - \theta_4).$$

Expand:

$$\begin{aligned} f &= x^4 - (\theta_1 + \cdots + \theta_4)x^3 + (\theta_1\theta_2 + \cdots + \theta_3\theta_4)x^2 \\ &\quad - (\theta_1\theta_2\theta_3 + \cdots + \theta_2\theta_3\theta_4)x + (\theta_1\theta_2\theta_3\theta_4) \\ &= x^4 - s_1(\theta_1, \theta_2, \theta_3, \theta_4)x^3 + s_2(\theta_1, \theta_2, \theta_3, \theta_4)x^2 \\ &\quad - s_3(\theta_1, \theta_2, \theta_3, \theta_4)x + s_4(\theta_1, \theta_2, \theta_3, \theta_4). \end{aligned}$$

In particular, the $s_i(\theta_1, \ldots, \theta_4) \in \mathbb{Q}$ (why?),

Connection between symmetric functions and our subject

Suppose $f \in \mathbb{Q}[x]$ is monic of degree 4. Then by the FTA, there exist $\theta_1, \ldots, \theta_4$ such that

$$f = (x - \theta_1)(x - \theta_2)(x - \theta_3)(x - \theta_4).$$

Expand:

$$\begin{aligned} f &= x^4 - (\theta_1 + \cdots + \theta_4)x^3 + (\theta_1\theta_2 + \cdots + \theta_3\theta_4)x^2 \\ &\quad - (\theta_1\theta_2\theta_3 + \cdots + \theta_2\theta_3\theta_4)x + (\theta_1\theta_2\theta_3\theta_4) \\ &= x^4 - s_1(\theta_1, \theta_2, \theta_3, \theta_4)x^3 + s_2(\theta_1, \theta_2, \theta_3, \theta_4)x^2 \\ &\quad - s_3(\theta_1, \theta_2, \theta_3, \theta_4)x + s_4(\theta_1, \theta_2, \theta_3, \theta_4). \end{aligned}$$

In particular, the $s_i(\theta_1, \ldots, \theta_4) \in \mathbb{Q}$ (why?), and if $f \in \mathbb{Z}[x]$, they are in $\mathbb{Z}$.

Example

Let $\omega = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$.

Example

Let $\omega = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$. Then

$x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$

Example

Let $\omega = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$. Then

$$x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$$

$$= x^3 - (1+\omega+\omega^2)x^2 + (1\cdot\omega + 1\cdot\omega^2 + \omega\cdot\omega^2)x - (1\cdot\omega\cdot\omega^2)$$

Example

Let $\omega = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$. Then

$$\begin{aligned} x^3 - 1 &= (x-1)(x-\omega)(x-\omega^2) \\ &= x^3 - (1+\omega+\omega^2)x^2 + (1\cdot\omega + 1\cdot\omega^2 + \omega\cdot\omega^2)x - (1\cdot\omega\cdot\omega^2) \\ &= x^3 - s_1(1,\omega,\omega^2)x^2 + s_2(1,\omega,\omega^2)x - s_3(1,\omega,\omega^2). \end{aligned}$$

Example

Let $\omega = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$. Then

$$\begin{aligned} x^3 - 1 &= (x-1)(x-\omega)(x-\omega^2) \\ &= x^3 - (1+\omega+\omega^2)x^2 + (1\cdot\omega + 1\cdot\omega^2 + \omega\cdot\omega^2)x - (1\cdot\omega\cdot\omega^2) \\ &= x^3 - s_1(1,\omega,\omega^2)x^2 + s_2(1,\omega,\omega^2)x - s_3(1,\omega,\omega^2). \end{aligned}$$

Comparing coefficients, we see that

Example

Let $\omega = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$. Then

$$\begin{aligned} x^3 - 1 &= (x-1)(x-\omega)(x-\omega^2) \\ &= x^3 - (1+\omega+\omega^2)x^2 + (1\cdot\omega + 1\cdot\omega^2 + \omega\cdot\omega^2)x - (1\cdot\omega\cdot\omega^2) \\ &= x^3 - s_1(1,\omega,\omega^2)x^2 + s_2(1,\omega,\omega^2)x - s_3(1,\omega,\omega^2). \end{aligned}$$

Comparing coefficients, we see that

$$s_1(1,\omega,\omega^2) = 1+\omega+\omega^2 = 0$$

Example

Let $\omega = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$. Then

$$\begin{aligned} x^3 - 1 &= (x-1)(x-\omega)(x-\omega^2) \\ &= x^3 - (1+\omega+\omega^2)x^2 + (1\cdot\omega + 1\cdot\omega^2 + \omega\cdot\omega^2)x - (1\cdot\omega\cdot\omega^2) \\ &= x^3 - s_1(1,\omega,\omega^2)x^2 + s_2(1,\omega,\omega^2)x - s_3(1,\omega,\omega^2). \end{aligned}$$

Comparing coefficients, we see that

$$s_1(1,\omega,\omega^2) = 1+\omega+\omega^2 = 0$$

$$s_2(1,\omega,\omega^2) = 1\cdot\omega + 1\cdot\omega^2 + \omega\cdot\omega^2 = \omega+\omega^2+1 = 0$$

Example

Let $\omega = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$. Then

$$\begin{aligned} x^3 - 1 &= (x-1)(x-\omega)(x-\omega^2) \\ &= x^3 - (1+\omega+\omega^2)x^2 + (1\cdot\omega + 1\cdot\omega^2 + \omega\cdot\omega^2)x - (1\cdot\omega\cdot\omega^2) \\ &= x^3 - s_1(1,\omega,\omega^2)x^2 + s_2(1,\omega,\omega^2)x - s_3(1,\omega,\omega^2). \end{aligned}$$

Comparing coefficients, we see that

$$s_1(1,\omega,\omega^2) = 1+\omega+\omega^2 = 0$$

$$s_2(1,\omega,\omega^2) = 1\cdot\omega + 1\cdot\omega^2 + \omega\cdot\omega^2 = \omega+\omega^2+1 = 0$$

$$s_3(1,\omega,\omega^2) = 1\cdot\omega\cdot\omega^2 = 1.$$

Example

Let $\omega = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$. Then

$$\begin{aligned} x^3 - 1 &= (x-1)(x-\omega)(x-\omega^2) \\ &= x^3 - (1+\omega+\omega^2)x^2 + (1\cdot\omega + 1\cdot\omega^2 + \omega\cdot\omega^2)x - (1\cdot\omega\cdot\omega^2) \\ &= x^3 - s_1(1,\omega,\omega^2)x^2 + s_2(1,\omega,\omega^2)x - s_3(1,\omega,\omega^2). \end{aligned}$$

Comparing coefficients, we see that

$$s_1(1,\omega,\omega^2) = 1+\omega+\omega^2 = 0$$

$$s_2(1,\omega,\omega^2) = 1\cdot\omega + 1\cdot\omega^2 + \omega\cdot\omega^2 = \omega+\omega^2+1 = 0$$

$$s_3(1,\omega,\omega^2) = 1\cdot\omega\cdot\omega^2 = 1.$$

Since $x^3 - 1$ has integer coefficients, the elementary functions of its roots are all integers, too.

Main theorem

Theorem. Let $K = \mathbb{Q}(\theta)$ be a number field, with embeddings σ_i and with $\theta_i = \sigma_i(\theta)$ for $i = 1, \ldots, n$. Let $\alpha_1, \ldots, \alpha_n$ be a basis for K over $\mathbb{Q}$.

Main theorem

Theorem. Let $K = \mathbb{Q}(\theta)$ be a number field, with embeddings σ_i and with $\theta_i = \sigma_i(\theta)$ for $i = 1, \ldots, n$. Let $\alpha_1, \ldots, \alpha_n$ be a basis for K over $\mathbb{Q}$.

Then the discriminant $\Delta[\alpha_1, \ldots, \alpha_n]$ is a nonzero rational number.

Main theorem

Theorem. Let $K = \mathbb{Q}(\theta)$ be a number field, with embeddings σ_i and with $\theta_i = \sigma_i(\theta)$ for $i = 1, \ldots, n$. Let $\alpha_1, \ldots, \alpha_n$ be a basis for K over $\mathbb{Q}$.

Then the discriminant $\Delta[\alpha_1, \ldots, \alpha_n]$ is a nonzero rational number.

It is positive if all of the θ_i are real.

Main theorem

Theorem. Let $K = \mathbb{Q}(\theta)$ be a number field, with embeddings σ_i and with $\theta_i = \sigma_i(\theta)$ for $i = 1, \ldots, n$. Let $\alpha_1, \ldots, \alpha_n$ be a basis for K over $\mathbb{Q}$.

Then the discriminant $\Delta[\alpha_1, \ldots, \alpha_n]$ is a nonzero rational number.

It is positive if all of the θ_i are real.

It is a rational integer if the α_i are algebraic integers.

Proof of main theorem

We know $1, \theta, \ldots, \theta^{n-1}$ is a $\mathbb{Q}$-basis for K.

Proof of main theorem

We know $1, \theta, \ldots, \theta^{n-1}$ is a $\mathbb{Q}$-basis for K. We have $\sigma_i(\theta^j) = \sigma_i(\theta)^j = \theta_i^j$.

Proof of main theorem

We know $1, \theta, \ldots, \theta^{n-1}$ is a $\mathbb{Q}$-basis for K. We have $\sigma_i(\theta^j) = \sigma_i(\theta)^j = \theta_i^j$. Therefore, by Vandermonde:

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = \det \begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \ldots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \ldots & \theta_2^{n-1} \\ 1 & \theta_3 & \theta_3^2 & \ldots & \theta_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \theta_n^2 & \ldots & \theta_n^{n-1} \end{pmatrix}^2 = \prod_{1 \leq i < j \leq n} (\theta_j - \theta_i)^2.$$

Proof of main theorem

We know $1, \theta, \ldots, \theta^{n-1}$ is a $\mathbb{Q}$-basis for K. We have $\sigma_i(\theta^j) = \sigma_i(\theta)^j = \theta_i^j$. Therefore, by Vandermonde:

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = \det \begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \ldots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \ldots & \theta_2^{n-1} \\ 1 & \theta_3 & \theta_3^2 & \ldots & \theta_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \theta_n^2 & \ldots & \theta_n^{n-1} \end{pmatrix}^2 = \prod_{1 \leq i < j \leq n} (\theta_j - \theta_i)^2.$$

Letting C be the change of basis matrix from $1, \theta, \ldots, \theta^{n-1}$ to $\alpha_1, \ldots, \alpha_n$,

Proof of main theorem

We know $1, \theta, \ldots, \theta^{n-1}$ is a $\mathbb{Q}$-basis for K. We have $\sigma_i(\theta^j) = \sigma_i(\theta)^j = \theta_i^j$. Therefore, by Vandermonde:

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = \det \begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \ldots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \ldots & \theta_2^{n-1} \\ 1 & \theta_3 & \theta_3^2 & \ldots & \theta_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \theta_n^2 & \ldots & \theta_n^{n-1} \end{pmatrix}^2 = \prod_{1 \leq i < j \leq n} (\theta_j - \theta_i)^2.$$

Letting C be the change of basis matrix from $1, \theta, \ldots, \theta^{n-1}$ to $\alpha_1, \ldots, \alpha_n$, we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \Delta[1, \theta, \ldots, \theta^{n-1}] = (\det C)^2 \prod_{1 \leq i < j \leq n} (\theta_j - \theta_i)^2.$$

Proof of main theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

Proof of main theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

Key idea: note that $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric polynomial in the θ_i.

Proof of main theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

Key idea: note that $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric polynomial in the θ_i. Let $p = \prod_{i=1}^{n}(x - \theta_i)$ be the minimal polynomial for θ over $\mathbb{Q}$.

Proof of main theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

Key idea: note that $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric polynomial in the θ_i. Let $p = \prod_{i=1}^{n}(x - \theta_i)$ be the minimal polynomial for θ over $\mathbb{Q}$. The symmetric polynomials in the θ_i are, up to sign, the coefficients of p,

Proof of main theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

Key idea: note that $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric polynomial in the θ_i. Let $p = \prod_{i=1}^{n}(x - \theta_i)$ be the minimal polynomial for θ over $\mathbb{Q}$. The symmetric polynomials in the θ_i are, up to sign, the coefficients of p, which are rational.

Proof of main theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

Key idea: note that $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric polynomial in the θ_i. Let $p = \prod_{i=1}^{n}(x - \theta_i)$ be the minimal polynomial for θ over $\mathbb{Q}$. The symmetric polynomials in the θ_i are, up to sign, the coefficients of p, which are rational. The entries in C are rational.

Proof of main theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

Key idea: note that $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric polynomial in the θ_i. Let $p = \prod_{i=1}^{n}(x - \theta_i)$ be the minimal polynomial for θ over $\mathbb{Q}$. The symmetric polynomials in the θ_i are, up to sign, the coefficients of p, which are rational. The entries in C are rational. Hence, the discriminant is rational.

Proof of main theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

Key idea: note that $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric polynomial in the θ_i. Let $p = \prod_{i=1}^{n}(x - \theta_i)$ be the minimal polynomial for θ over $\mathbb{Q}$. The symmetric polynomials in the θ_i are, up to sign, the coefficients of p, which are rational. The entries in C are rational. Hence, the discriminant is rational.

Its positive if the θ_i are real (why?).

Proof of main theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

Key idea: note that $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric polynomial in the θ_i. Let $p = \prod_{i=1}^{n}(x - \theta_i)$ be the minimal polynomial for θ over $\mathbb{Q}$. The symmetric polynomials in the θ_i are, up to sign, the coefficients of p, which are rational. The entries in C are rational. Hence, the discriminant is rational.

Its positive if the θ_i are real (why?).

Finally, what can we say if each α_i is an algebraic integer? (See next page)

Proof of main theorem

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(\sigma_i(\alpha_j))^2 = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Proof of main theorem

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(\sigma_i(\alpha_j))^2 = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Suppose that each α_i is an algebraic integer.

Proof of main theorem

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(\sigma_i(\alpha_j))^2 = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Suppose that each α_i is an algebraic integer. Then the $\sigma_i(\alpha_j)$ are algebraic integers. (Why? Start with the definition of an algebraic integer.)

Proof of main theorem

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(\sigma_i(\alpha_j))^2 = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Suppose that each α_i is an algebraic integer. Then the $\sigma_i(\alpha_j)$ are algebraic integers. (Why? Start with the definition of an algebraic integer.)

We have seen that the algebraic integers in K form a ring.

Proof of main theorem

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(\sigma_i(\alpha_j))^2 = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Suppose that each α_i is an algebraic integer. Then the $\sigma_i(\alpha_j)$ are algebraic integers. (Why? Start with the definition of an algebraic integer.)

We have seen that the algebraic integers in K form a ring. Hence, the discriminant $\det(\sigma_i(\alpha_j))^2$ is an algebraic integer.

Proof of main theorem

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(\sigma_i(\alpha_j))^2 = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Suppose that each α_i is an algebraic integer. Then the $\sigma_i(\alpha_j)$ are algebraic integers. (Why? Start with the definition of an algebraic integer.)

We have seen that the algebraic integers in K form a ring. Hence, the discriminant $\det(\sigma_i(\alpha_j))^2$ is an algebraic integer. However, we have just seen that it is a rational number.

Proof of main theorem

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(\sigma_i(\alpha_j))^2 = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Suppose that each α_i is an algebraic integer. Then the $\sigma_i(\alpha_j)$ are algebraic integers. (Why? Start with the definition of an algebraic integer.)

We have seen that the algebraic integers in K form a ring. Hence, the discriminant $\det(\sigma_i(\alpha_j))^2$ is an algebraic integer. However, we have just seen that it is a rational number. We also know that if a rational number is integral over $\mathbb{Q}$, then it must be an ordinary integer. $\square$