Math 361

February 6, 2023

Today

- Tomorrow's quiz.
- Fundamental Theorem of Algebra.
- Field homomorphisms.
- The discriminant.

Tomorrow's quiz

See homepage.

Fundamental Theorem of Algebra

Theorem. (Fundamental theorem of algebra.) Let $h \in \mathbb{C}[x]$ be a nonconstant polynomial. Then there exists $\alpha \in \mathbb{C}$ such that $h(\alpha) = 0$.

Fundamental Theorem of Algebra

Theorem. (Fundamental theorem of algebra.) Let $h \in \mathbb{C}[x]$ be a nonconstant polynomial. Then there exists $\alpha \in \mathbb{C}$ such that $h(\alpha) = 0$.

Using polynomial division, we get the following (equivalent) formulation of the fundamental theorem of algebra:

Fundamental Theorem of Algebra

Theorem. (Fundamental theorem of algebra.) Let $h \in \mathbb{C}[x]$ be a nonconstant polynomial. Then there exists $\alpha \in \mathbb{C}$ such that $h(\alpha) = 0$.

Using polynomial division, we get the following (equivalent) formulation of the fundamental theorem of algebra:

Corollary. A polynomial $h \in \mathbb{C}[x]$ of degree n has n complex roots $\theta_1, \ldots, \theta_n$ counting multiplicities (i.e., the θ_i are not necessarily distinct), and

$$h = \beta \prod_{n=1}^{n} (x - \theta_i)$$

for some $\beta \in \mathbb{C}$.

Field homomorphisms

Let K be a number field.

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields,

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields, i.e., for all $a, b \in K$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b).$$

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields, i.e., for all $a, b \in K$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b).$$

1. The homomorphism σ is either injective or identically 0.

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields, i.e., for all $a, b \in K$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b).$$

1. The homomorphism σ is either injective or identically 0.
2. If σ is injective, then σ is the identity mapping when restricted to $\mathbb{Q} \in K$.

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields, i.e., for all $a, b \in K$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b).$$

1. The homomorphism σ is either injective or identically 0.
2. If σ is injective, then σ is the identity mapping when restricted to $\mathbb{Q} \in K$.
3. Suppose that $\alpha \in K$ and $h \in \mathbb{Q}[x]$ with $h(\alpha) = 0$. If $\sigma \neq 0$, then $h(\sigma(\alpha)) = 0$. Thus, σ permutes the roots of h in $\mathbb{C}$.

Field homomorphisms

Let K be a number field.

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields,

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields, i.e., for all $a, b \in K$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b).$$

1. $\ker \sigma$ is an ideal in K:

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields, i.e., for all $a, b \in K$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b).$$

1. $\ker \sigma$ is an ideal in K:

Proof.

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields, i.e., for all $a, b \in K$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b).$$

1. $\ker \sigma$ is an ideal in K:

Proof.

- $\sigma(0) = 0 \Rightarrow \ker \sigma \neq \emptyset$.

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields, i.e., for all $a, b \in K$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b).$$

1. $\ker\sigma$ is an ideal in K:

Proof.

- $\sigma(0) = 0 \Rightarrow \ker\sigma \neq \emptyset$.
- $a, b \in \ker\sigma,\ k \in K \Rightarrow$

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields, i.e., for all $a, b \in K$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b).$$

1. $\ker \sigma$ is an ideal in K:

Proof.

- $\sigma(0) = 0 \Rightarrow \ker \sigma \neq \emptyset$.
- $a, b \in \ker \sigma,\ k \in K \Rightarrow \sigma(a+b) = \sigma(a) + \sigma(b) = 0 + 0 = 0$, and

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields, i.e., for all $a, b \in K$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b).$$

1. $\ker\sigma$ is an ideal in K:

Proof.

- $\sigma(0) = 0 \Rightarrow \ker\sigma \neq \emptyset$.
- $a, b \in \ker\sigma,\ k \in K \Rightarrow \sigma(a+b) = \sigma(a) + \sigma(b) = 0 + 0 = 0$, and $\sigma(ka) = \sigma(k)\sigma(a) = \sigma(k) \cdot 0 = 0$.

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields, i.e., for all $a, b \in K$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b).$$

1. $\ker\sigma$ is an ideal in K:

Proof.

- $\sigma(0) = 0 \Rightarrow \ker\sigma \neq \emptyset$.
- $a, b \in \ker\sigma,\ k \in K \Rightarrow \sigma(a+b) = \sigma(a) + \sigma(b) = 0 + 0 = 0$, and $\sigma(ka) = \sigma(k)\sigma(a) = \sigma(k) \cdot 0 = 0$.

If $\ker\sigma \neq (0) = \{0\}$,

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields, i.e., for all $a, b \in K$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b).$$

1. $\ker\sigma$ is an ideal in K:

Proof.

- $\sigma(0) = 0 \Rightarrow \ker\sigma \neq \emptyset$.
- $a, b \in \ker\sigma,\ k \in K \Rightarrow \sigma(a+b) = \sigma(a) + \sigma(b) = 0 + 0 = 0$, and $\sigma(ka) = \sigma(k)\sigma(a) = \sigma(k)\cdot 0 = 0$.

If $\ker\sigma \neq (0) = \{0\}$, then take $0 \neq \alpha \in \ker\sigma$.

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields, i.e., for all $a, b \in K$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b).$$

1. $\ker\sigma$ is an ideal in K:

Proof.

- $\sigma(0) = 0 \Rightarrow \ker\sigma \neq \emptyset$.
- $a, b \in \ker\sigma,\ k \in K \Rightarrow \sigma(a+b) = \sigma(a) + \sigma(b) = 0 + 0 = 0$, and $\sigma(ka) = \sigma(k)\sigma(a) = \sigma(k) \cdot 0 = 0$.

If $\ker\sigma \neq (0) = \{0\}$, then take $0 \neq \alpha \in \ker\sigma$. Since K is a field, $\frac{1}{\alpha} \in K$,

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields, i.e., for all $a, b \in K$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b).$$

1. $\ker\sigma$ is an ideal in K:

Proof.

- $\sigma(0) = 0 \Rightarrow \ker\sigma \neq \emptyset$.
- $a, b \in \ker\sigma,\ k \in K \Rightarrow \sigma(a+b) = \sigma(a) + \sigma(b) = 0 + 0 = 0$, and $\sigma(ka) = \sigma(k)\sigma(a) = \sigma(k)\cdot 0 = 0$.

If $\ker\sigma \neq (0) = \{0\}$, then take $0 \neq \alpha \in \ker\sigma$. Since K is a field, $\frac{1}{\alpha} \in K$, and since $\ker\sigma$ is an ideal, $\frac{1}{\alpha}\cdot\alpha = 1 \in \ker\sigma$.

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields, i.e., for all $a, b \in K$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b).$$

1. $\ker\sigma$ is an ideal in K:

Proof.

- $\sigma(0) = 0 \Rightarrow \ker\sigma \neq \emptyset$.
- $a, b \in \ker\sigma,\ k \in K \Rightarrow \sigma(a+b) = \sigma(a) + \sigma(b) = 0 + 0 = 0$, and $\sigma(ka) = \sigma(k)\sigma(a) = \sigma(k)\cdot 0 = 0$.

If $\ker\sigma \neq (0) = \{0\}$, then take $0 \neq \alpha \in \ker\sigma$. Since K is a field, $\frac{1}{\alpha} \in K$, and since $\ker\sigma$ is an ideal, $\frac{1}{\alpha}\cdot\alpha = 1 \in \ker\sigma$. So $\ker\sigma = (1) = K$,

Field homomorphisms

Let K be a number field. Let $\sigma\colon K \to \mathbb{C}$ be a homomorphism of fields, i.e., for all $a, b \in K$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b).$$

1. $\ker\sigma$ is an ideal in K:

Proof.

- $\sigma(0) = 0 \Rightarrow \ker\sigma \neq \emptyset$.
- $a, b \in \ker\sigma,\ k \in K \Rightarrow \sigma(a+b) = \sigma(a) + \sigma(b) = 0 + 0 = 0$, and $\sigma(ka) = \sigma(k)\sigma(a) = \sigma(k)\cdot 0 = 0$.

If $\ker\sigma \neq (0) = \{0\}$, then take $0 \neq \alpha \in \ker\sigma$. Since K is a field, $\frac{1}{\alpha} \in K$, and since $\ker\sigma$ is an ideal, $\frac{1}{\alpha}\cdot\alpha = 1 \in \ker\sigma$. So $\ker\sigma = (1) = K$, i.e., $\sigma = 0$.

Field homomorphisms

2. If σ is injective, then σ is the identity mapping when restricted to $\mathbb{Q} \in K$.

Field homomorphisms

2. If σ is injective, then σ is the identity mapping when restricted to $\mathbb{Q} \in K$.

Proof. Suppose σ is injective. Then the standard argument shows that $\sigma(1) = 1$:

$$\sigma(1) = \sigma(1 \cdot 1) = \sigma(1)\sigma(1).$$

Field homomorphisms

2. If σ is injective, then σ is the identity mapping when restricted to $\mathbb{Q} \in K$.

Proof. Suppose σ is injective. Then the standard argument shows that $\sigma(1) = 1$:

$$\sigma(1) = \sigma(1 \cdot 1) = \sigma(1)\sigma(1).$$

Since σ is injective, $\sigma(1) \neq 0$. Multiplying the above equation through by $1/\sigma(1)$, gives $\sigma(1) = 1$.

Field homomorphisms

2. If σ is injective, then σ is the identity mapping when restricted to $\mathbb{Q} \in K$.

Proof. Suppose σ is injective. Then the standard argument shows that $\sigma(1) = 1$:

$$\sigma(1) = \sigma(1 \cdot 1) = \sigma(1)\sigma(1).$$

Since σ is injective, $\sigma(1) \neq 0$. Multiplying the above equation through by $1/\sigma(1)$, gives $\sigma(1) = 1$.
Then, for each $n \in \mathbb{N}$,

$$\sigma(n) = \sigma(\underbrace{1 + \cdots + 1}_{n \text{ times}}) = \underbrace{\sigma(1) + \cdots + \sigma(1)}_{n \text{ times}} = \underbrace{1 + \cdots + 1}_{n \text{ times}} = n.$$

Field homomorphisms

2. If σ is injective, then σ is the identity mapping when restricted to $\mathbb{Q} \in K$.

Proof. Suppose σ is injective. Then the standard argument shows that $\sigma(1) = 1$:

$$\sigma(1) = \sigma(1 \cdot 1) = \sigma(1)\sigma(1).$$

Since σ is injective, $\sigma(1) \neq 0$. Multiplying the above equation through by $1/\sigma(1)$, gives $\sigma(1) = 1$.
Then, for each $n \in \mathbb{N}$,

$$\sigma(n) = \sigma(\underbrace{1 + \cdots + 1}_{n \text{ times}}) = \underbrace{\sigma(1) + \cdots + \sigma(1)}_{n \text{ times}} = \underbrace{1 + \cdots + 1}_{n \text{ times}} = n.$$

It follows that σ fixes $\mathbb{Q}$:

Field homomorphisms

2. If σ is injective, then σ is the identity mapping when restricted to $\mathbb{Q} \in K$.

Proof. Suppose σ is injective. Then the standard argument shows that $\sigma(1) = 1$:

$$\sigma(1) = \sigma(1 \cdot 1) = \sigma(1)\sigma(1).$$

Since σ is injective, $\sigma(1) \neq 0$. Multiplying the above equation through by $1/\sigma(1)$, gives $\sigma(1) = 1$.
Then, for each $n \in \mathbb{N}$,

$$\sigma(n) = \sigma(\underbrace{1 + \cdots + 1}_{n \text{ times}}) = \underbrace{\sigma(1) + \cdots + \sigma(1)}_{n \text{ times}} = \underbrace{1 + \cdots + 1}_{n \text{ times}} = n.$$

It follows that σ fixes $\mathbb{Q}$: (i) For $n \in \mathbb{Z}_{>0}$, apply σ to the identity $(1/n)n = 1$ to get $\sigma(1/n) = 1/n$.

Field homomorphisms

2. If σ is injective, then σ is the identity mapping when restricted to $\mathbb{Q} \in K$.

Proof. Suppose σ is injective. Then the standard argument shows that $\sigma(1) = 1$:

$$\sigma(1) = \sigma(1 \cdot 1) = \sigma(1)\sigma(1).$$

Since σ is injective, $\sigma(1) \neq 0$. Multiplying the above equation through by $1/\sigma(1)$, gives $\sigma(1) = 1$.
Then, for each $n \in \mathbb{N}$,

$$\sigma(n) = \sigma(\underbrace{1 + \cdots + 1}_{n \text{ times}}) = \underbrace{\sigma(1) + \cdots + \sigma(1)}_{n \text{ times}} = \underbrace{1 + \cdots + 1}_{n \text{ times}} = n.$$

It follows that σ fixes $\mathbb{Q}$: (i) For $n \in \mathbb{Z}_{>0}$, apply σ to the identity $(1/n)n = 1$ to get $\sigma(1/n) = 1/n$. (ii) Next show $\sigma(m/n) = m/n$ for all $m, n \in \mathbb{N}$ with $n \neq 0$.

Field homomorphisms

2. If σ is injective, then σ is the identity mapping when restricted to $\mathbb{Q} \in K$.

Proof. Suppose σ is injective. Then the standard argument shows that $\sigma(1) = 1$:

$$\sigma(1) = \sigma(1 \cdot 1) = \sigma(1)\sigma(1).$$

Since σ is injective, $\sigma(1) \neq 0$. Multiplying the above equation through by $1/\sigma(1)$, gives $\sigma(1) = 1$.
Then, for each $n \in \mathbb{N}$,

$$\sigma(n) = \sigma(\underbrace{1 + \cdots + 1}_{n \text{ times}}) = \underbrace{\sigma(1) + \cdots + \sigma(1)}_{n \text{ times}} = \underbrace{1 + \cdots + 1}_{n \text{ times}} = n.$$

It follows that σ fixes $\mathbb{Q}$: (i) For $n \in \mathbb{Z}_{>0}$, apply σ to the identity $(1/n)n = 1$ to get $\sigma(1/n) = 1/n$. (ii) Next show $\sigma(m/n) = m/n$ for all $m, n \in \mathbb{N}$ with $n \neq 0$. (iii) Finally, show that for any $\alpha \in K$, we have $\sigma(-\alpha) = -\sigma(\alpha)$.

Field homomorphisms

3. Suppose that $\alpha \in K$ and $h \in \mathbb{Q}[x]$ with $h(\alpha) = 0$. If $\sigma \neq 0$, then $h(\sigma(\alpha)) = 0$. Thus, σ permutes the roots of h in $\mathbb{C}$.

Field homomorphisms

3. Suppose that $\alpha \in K$ and $h \in \mathbb{Q}[x]$ with $h(\alpha) = 0$. If $\sigma \neq 0$, then $h(\sigma(\alpha)) = 0$. Thus, σ permutes the roots of h in $\mathbb{C}$.

Proof. So suppose $\sigma \neq 0$, in which case σ

Field homomorphisms

3. Suppose that $\alpha \in K$ and $h \in \mathbb{Q}[x]$ with $h(\alpha) = 0$. If $\sigma \neq 0$, then $h(\sigma(\alpha)) = 0$. Thus, σ permutes the roots of h in $\mathbb{C}$.

Proof. So suppose $\sigma \neq 0$, in which case σ is injective.

Field homomorphisms

3. Suppose that $\alpha \in K$ and $h \in \mathbb{Q}[x]$ with $h(\alpha) = 0$. If $\sigma \neq 0$, then $h(\sigma(\alpha)) = 0$. Thus, σ permutes the roots of h in $\mathbb{C}$.

Proof. So suppose $\sigma \neq 0$, in which case σ is injective.

Say $h = \sum_{i=1}^{n} a_i x^i$ and that $h(\alpha) = 0$.

Field homomorphisms

3. Suppose that $\alpha \in K$ and $h \in \mathbb{Q}[x]$ with $h(\alpha) = 0$. If $\sigma \neq 0$, then $h(\sigma(\alpha)) = 0$. Thus, σ permutes the roots of h in $\mathbb{C}$.

Proof. So suppose $\sigma \neq 0$, in which case σ is injective.

Say $h = \sum_{i=1}^{n} a_i x^i$ and that $h(\alpha) = 0$. Then, using the fact that σ preserves sums and products, σ is the identity on $\mathbb{Q}$, and the $a_i \in \mathbb{Q}$,

Field homomorphisms

3. Suppose that $\alpha \in K$ and $h \in \mathbb{Q}[x]$ with $h(\alpha) = 0$. If $\sigma \neq 0$, then $h(\sigma(\alpha)) = 0$. Thus, σ permutes the roots of h in $\mathbb{C}$.

Proof. So suppose $\sigma \neq 0$, in which case σ is injective.

Say $h = \sum_{i=1}^{n} a_i x^i$ and that $h(\alpha) = 0$. Then, using the fact that σ preserves sums and products, σ is the identity on $\mathbb{Q}$, and the $a_i \in \mathbb{Q}$,

$$0 = \sigma(0) = \sigma(\textstyle\sum_{i=1}^{n} a_i \alpha^i)$$

Field homomorphisms

3. Suppose that $\alpha \in K$ and $h \in \mathbb{Q}[x]$ with $h(\alpha) = 0$. If $\sigma \neq 0$, then $h(\sigma(\alpha)) = 0$. Thus, σ permutes the roots of h in $\mathbb{C}$.

Proof. So suppose $\sigma \neq 0$, in which case σ is injective.

Say $h = \sum_{i=1}^{n} a_i x^i$ and that $h(\alpha) = 0$. Then, using the fact that σ preserves sums and products, σ is the identity on $\mathbb{Q}$, and the $a_i \in \mathbb{Q}$,

$$\begin{aligned} 0 = \sigma(0) &= \sigma\left(\textstyle\sum_{i=1}^{n} a_i \alpha^i\right) \\ &= \sum_{i=1}^{n} \sigma(a_i)(\sigma(\alpha))^i \end{aligned}$$

Field homomorphisms

3. Suppose that $\alpha \in K$ and $h \in \mathbb{Q}[x]$ with $h(\alpha) = 0$. If $\sigma \neq 0$, then $h(\sigma(\alpha)) = 0$. Thus, σ permutes the roots of h in $\mathbb{C}$.

Proof. So suppose $\sigma \neq 0$, in which case σ is injective.

Say $h = \sum_{i=1}^{n} a_i x^i$ and that $h(\alpha) = 0$. Then, using the fact that σ preserves sums and products, σ is the identity on $\mathbb{Q}$, and the $a_i \in \mathbb{Q}$,

$$\begin{aligned} 0 = \sigma(0) &= \sigma\left(\textstyle\sum_{i=1}^{n} a_i \alpha^i\right) \\ &= \sum_{i=1}^{n} \sigma(a_i)(\sigma(\alpha))^i \\ &= \sum_{i=1}^{n} a_i(\sigma(\alpha))^i = h(\sigma(\alpha)). \end{aligned}$$

□

Field embeddings

What are all of the *embeddings* (injective field homomorphisms) of a number field K into $\mathbb{C}$?

Field embeddings

What are all of the *embeddings* (injective field homomorphisms) of a number field K into $\mathbb{C}$?

Write $K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$ for some algebraic number θ.

Field embeddings

What are all of the *embeddings* (injective field homomorphisms) of a number field K into $\mathbb{C}$?

Write $K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$ for some algebraic number θ. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial for θ.

Field embeddings

What are all of the *embeddings* (injective field homomorphisms) of a number field K into $\mathbb{C}$?

Write $K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$ for some algebraic number θ. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial for θ.

Facts from algebra.

Field embeddings

What are all of the *embeddings* (injective field homomorphisms) of a number field K into $\mathbb{C}$?

Write $K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$ for some algebraic number θ. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial for θ.

Facts from algebra.

- The number of embeddings is $n := \deg(p) = [K : \mathbb{Q}]$.

Field embeddings

What are all of the *embeddings* (injective field homomorphisms) of a number field K into $\mathbb{C}$?

Write $K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$ for some algebraic number θ. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial for θ.

Facts from algebra.

- The number of embeddings is $n := \deg(p) = [K : \mathbb{Q}]$.
- If $\sigma_1, \ldots, \sigma_n$ are the embeddings, define $\theta_i := \sigma_i(\theta)$.

Field embeddings

What are all of the *embeddings* (injective field homomorphisms) of a number field K into $\mathbb{C}$?

Write $K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$ for some algebraic number θ. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial for θ.

Facts from algebra.

- The number of embeddings is $n := \deg(p) = [K : \mathbb{Q}]$.
- If $\sigma_1, \ldots, \sigma_n$ are the embeddings, define $\theta_i := \sigma_i(\theta)$. Then $p = \prod_{i=1}^{n}(x - \theta_i)$.

Field embeddings

What are all of the *embeddings* (injective field homomorphisms) of a number field K into $\mathbb{C}$?

Write $K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$ for some algebraic number θ. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial for θ.

Facts from algebra.

- The number of embeddings is $n := \deg(p) = [K : \mathbb{Q}]$.
- If $\sigma_1, \ldots, \sigma_n$ are the embeddings, define $\theta_i := \sigma_i(\theta)$. Then $p = \prod_{i=1}^{n}(x - \theta_i)$.
- $\theta \mapsto \theta_i$ determines σ_i.

Field embeddings

What are all of the *embeddings* (injective field homomorphisms) of a number field K into $\mathbb{C}$?

Write $K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$ for some algebraic number θ. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial for θ.

Facts from algebra.

- The number of embeddings is $n := \deg(p) = [K : \mathbb{Q}]$.
- If $\sigma_1, \ldots, \sigma_n$ are the embeddings, define $\theta_i := \sigma_i(\theta)$. Then $p = \prod_{i=1}^{n}(x - \theta_i)$.
- $\theta \mapsto \theta_i$ determines σ_i.

To see last fact, recall that $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis for K.

Field embeddings

What are all of the *embeddings* (injective field homomorphisms) of a number field K into $\mathbb{C}$?

Write $K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$ for some algebraic number θ. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial for θ.

Facts from algebra.

- The number of embeddings is $n := \deg(p) = [K : \mathbb{Q}]$.
- If $\sigma_1, \ldots, \sigma_n$ are the embeddings, define $\theta_i := \sigma_i(\theta)$. Then $p = \prod_{i=1}^{n}(x - \theta_i)$.
- $\theta \mapsto \theta_i$ determines σ_i.

To see last fact, recall that $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis for K. So for each fixed i, we have $\sigma_i \colon \sum_{j=1}^{n} \alpha_j \theta^j \mapsto$

Field embeddings

What are all of the *embeddings* (injective field homomorphisms) of a number field K into $\mathbb{C}$?

Write $K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$ for some algebraic number θ. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial for θ.

Facts from algebra.

- The number of embeddings is $n := \deg(p) = [K : \mathbb{Q}]$.
- If $\sigma_1, \ldots, \sigma_n$ are the embeddings, define $\theta_i := \sigma_i(\theta)$. Then $p = \prod_{i=1}^{n}(x - \theta_i)$.
- $\theta \mapsto \theta_i$ determines σ_i.

To see last fact, recall that $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis for K. So for each fixed i, we have $\sigma_i \colon \sum_{j=1}^{n} \alpha_j \theta^j \mapsto \sum_{j=1}^{n} \alpha_j \theta_i^j$.

Field embedding examples

What are the embeddings $\mathbb{Q}(\sqrt{5}) \to \mathbb{C}$?

Field embedding examples

What are the embeddings $\mathbb{Q}(\sqrt{5}) \to \mathbb{C}$?

Minimal polynomial:

Field embedding examples

What are the embeddings $\mathbb{Q}(\sqrt{5}) \to \mathbb{C}$?

Minimal polynomial: $p = (x - \sqrt{5})(x + \sqrt{5})$.

Field embedding examples

What are the embeddings $\mathbb{Q}(\sqrt{5}) \to \mathbb{C}$?

Minimal polynomial: $p = (x - \sqrt{5})(x + \sqrt{5})$.

Embeddings:

Field embedding examples

What are the embeddings $\mathbb{Q}(\sqrt{5}) \to \mathbb{C}$?

Minimal polynomial: $p = (x - \sqrt{5})(x + \sqrt{5})$.

Embeddings: $\sigma_1 : \sqrt{5} \mapsto \sqrt{5}$

Field embedding examples

What are the embeddings $\mathbb{Q}(\sqrt{5}) \to \mathbb{C}$?

Minimal polynomial: $p = (x - \sqrt{5})(x + \sqrt{5})$.

Embeddings: $\sigma_1 : \sqrt{5} \mapsto \sqrt{5}$ and $\sigma_2 : \sqrt{5} \mapsto -\sqrt{5}$.

Field embedding examples

What are the embeddings $\mathbb{Q}(\sqrt{5}) \to \mathbb{C}$?

Minimal polynomial: $p = (x - \sqrt{5})(x + \sqrt{5})$.

Embeddings: $\sigma_1 : \sqrt{5} \mapsto \sqrt{5}$ and $\sigma_2 : \sqrt{5} \mapsto -\sqrt{5}$.

$$\sigma_1(r + s\sqrt{5})$$

Field embedding examples

What are the embeddings $\mathbb{Q}(\sqrt{5}) \to \mathbb{C}$?

Minimal polynomial: $p = (x - \sqrt{5})(x + \sqrt{5})$.

Embeddings: $\sigma_1 : \sqrt{5} \mapsto \sqrt{5}$ and $\sigma_2 : \sqrt{5} \mapsto -\sqrt{5}$.

$$\sigma_1(r + s\sqrt{5}) = r + s\sqrt{5}.$$

Field embedding examples

What are the embeddings $\mathbb{Q}(\sqrt{5}) \to \mathbb{C}$?

Minimal polynomial: $p = (x - \sqrt{5})(x + \sqrt{5})$.

Embeddings: $\sigma_1 : \sqrt{5} \mapsto \sqrt{5}$ and $\sigma_2 : \sqrt{5} \mapsto -\sqrt{5}$.

$$\sigma_1(r + s\sqrt{5}) = r + s\sqrt{5}.$$

$$\sigma_2(r + s\sqrt{5})$$

Field embedding examples

What are the embeddings $\mathbb{Q}(\sqrt{5}) \to \mathbb{C}$?

Minimal polynomial: $p = (x - \sqrt{5})(x + \sqrt{5})$.

Embeddings: $\sigma_1 : \sqrt{5} \mapsto \sqrt{5}$ and $\sigma_2 : \sqrt{5} \mapsto -\sqrt{5}$.

$$\sigma_1(r + s\sqrt{5}) = r + s\sqrt{5}.$$

$$\sigma_2(r + s\sqrt{5}) = r - s\sqrt{5}.$$

Field embedding examples

What are the embeddings $\mathbb{Q}(\sqrt{5}) \to \mathbb{C}$?

Minimal polynomial: $p = (x - \sqrt{5})(x + \sqrt{5})$.

Embeddings: $\sigma_1 : \sqrt{5} \mapsto \sqrt{5}$ and $\sigma_2 : \sqrt{5} \mapsto -\sqrt{5}$.

$$\sigma_1(r + s\sqrt{5}) = r + s\sqrt{5}.$$

$$\sigma_2(r + s\sqrt{5}) = r - s\sqrt{5}.$$

Note that in this case the image of the embedding is $\mathbb{Q}(\sqrt{5})$.

Field embedding examples

What are the embeddings $\mathbb{Q}(\sqrt{5}) \to \mathbb{C}$?

Minimal polynomial: $p = (x - \sqrt{5})(x + \sqrt{5})$.

Embeddings: $\sigma_1 : \sqrt{5} \mapsto \sqrt{5}$ and $\sigma_2 : \sqrt{5} \mapsto -\sqrt{5}$.

$$\sigma_1(r + s\sqrt{5}) = r + s\sqrt{5}.$$

$$\sigma_2(r + s\sqrt{5}) = r - s\sqrt{5}.$$

Note that in this case the image of the embedding is $\mathbb{Q}(\sqrt{5})$. So they are *automorphisms* of K.

Field embedding examples

What are the embeddings $\mathbb{Q}(\sqrt{5}) \to \mathbb{C}$?

Minimal polynomial: $p = (x - \sqrt{5})(x + \sqrt{5})$.

Embeddings: $\sigma_1 : \sqrt{5} \mapsto \sqrt{5}$ and $\sigma_2 : \sqrt{5} \mapsto -\sqrt{5}$.

$$\sigma_1(r + s\sqrt{5}) = r + s\sqrt{5}.$$

$$\sigma_2(r + s\sqrt{5}) = r - s\sqrt{5}.$$

Note that in this case the image of the embedding is $\mathbb{Q}(\sqrt{5})$. So they are *automorphisms* of K. The next example shows that embeddings do not need to be automorphisms.

Field embedding examples

Let $K = \mathbb{Q}(\sqrt[3]{5})$.

Field embedding examples

Let $K = \mathbb{Q}(\sqrt[3]{5})$. Then the minimal polynomial is

$$p = x^3 - 5 =$$

Field embedding examples

Let $K = \mathbb{Q}(\sqrt[3]{5})$. Then the minimal polynomial is

$$p = x^3 - 5 = (x - \sqrt[3]{5})(x - \omega\sqrt[3]{5})(x - \omega^2\sqrt[3]{5}),$$

Field embedding examples

Let $K = \mathbb{Q}(\sqrt[3]{5})$. Then the minimal polynomial is

$$p = x^3 - 5 = (x - \sqrt[3]{5})(x - \omega\sqrt[3]{5})(x - \omega^2\sqrt[3]{5}),$$

where $\omega = e^{2\pi i/3} = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{-1+i\sqrt{3}}{2}$.

Field embedding examples

Let $K = \mathbb{Q}(\sqrt[3]{5})$. Then the minimal polynomial is

$$p = x^3 - 5 = (x - \sqrt[3]{5})(x - \omega\sqrt[3]{5})(x - \omega^2\sqrt[3]{5}),$$

where $\omega = e^{2\pi i/3} = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{-1+i\sqrt{3}}{2}$. The three embeddings of $\mathbb{Q}(\sqrt[3]{5})$ are given by

Field embedding examples

Let $K = \mathbb{Q}(\sqrt[3]{5})$. Then the minimal polynomial is

$$p = x^3 - 5 = (x - \sqrt[3]{5})(x - \omega\sqrt[3]{5})(x - \omega^2\sqrt[3]{5}),$$

where $\omega = e^{2\pi i/3} = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{-1+i\sqrt{3}}{2}$. The three embeddings of $\mathbb{Q}(\sqrt[3]{5})$ are given by

$$\sigma_1(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := \mathrm{id}(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2)$$

Field embedding examples

Let $K = \mathbb{Q}(\sqrt[3]{5})$. Then the minimal polynomial is

$$p = x^3 - 5 = (x - \sqrt[3]{5})(x - \omega\sqrt[3]{5})(x - \omega^2\sqrt[3]{5}),$$

where $\omega = e^{2\pi i/3} = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{-1+i\sqrt{3}}{2}$. The three embeddings of $\mathbb{Q}(\sqrt[3]{5})$ are given by

$$\sigma_1(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := \mathrm{id}(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) = 1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2$$

Field embedding examples

Let $K = \mathbb{Q}(\sqrt[3]{5})$. Then the minimal polynomial is

$$p = x^3 - 5 = (x - \sqrt[3]{5})(x - \omega\sqrt[3]{5})(x - \omega^2\sqrt[3]{5}),$$

where $\omega = e^{2\pi i/3} = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{-1+i\sqrt{3}}{2}$. The three embeddings of $\mathbb{Q}(\sqrt[3]{5})$ are given by

$$\sigma_1(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := \mathrm{id}(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) = 1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2$$

$$\sigma_2(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := 1 + a\omega\sqrt[3]{5} + b(\omega\sqrt[3]{5})^2$$

Field embedding examples

Let $K = \mathbb{Q}(\sqrt[3]{5})$. Then the minimal polynomial is

$$p = x^3 - 5 = (x - \sqrt[3]{5})(x - \omega\sqrt[3]{5})(x - \omega^2\sqrt[3]{5}),$$

where $\omega = e^{2\pi i/3} = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{-1+i\sqrt{3}}{2}$. The three embeddings of $\mathbb{Q}(\sqrt[3]{5})$ are given by

$$\sigma_1(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := \mathrm{id}(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) = 1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2$$

$$\sigma_2(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := 1 + a\omega\sqrt[3]{5} + b(\omega\sqrt[3]{5})^2 = 1 + a\omega\sqrt[3]{5} + b\omega^2(\sqrt[3]{5})^2$$

Field embedding examples

Let $K = \mathbb{Q}(\sqrt[3]{5})$. Then the minimal polynomial is

$$p = x^3 - 5 = (x - \sqrt[3]{5})(x - \omega\sqrt[3]{5})(x - \omega^2\sqrt[3]{5}),$$

where $\omega = e^{2\pi i/3} = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{-1+i\sqrt{3}}{2}$. The three embeddings of $\mathbb{Q}(\sqrt[3]{5})$ are given by

$$\sigma_1(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := \mathrm{id}(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) = 1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2$$

$$\sigma_2(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := 1 + a\omega\sqrt[3]{5} + b(\omega\sqrt[3]{5})^2 = 1 + a\omega\sqrt[3]{5} + b\omega^2(\sqrt[3]{5})^2$$

$$\sigma_3(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := 1 + a\omega^2\sqrt[3]{5} + b(\omega^2\sqrt[3]{5})^2$$

Field embedding examples

Let $K = \mathbb{Q}(\sqrt[3]{5})$. Then the minimal polynomial is

$$p = x^3 - 5 = (x - \sqrt[3]{5})(x - \omega\sqrt[3]{5})(x - \omega^2\sqrt[3]{5}),$$

where $\omega = e^{2\pi i/3} = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{-1+i\sqrt{3}}{2}$. The three embeddings of $\mathbb{Q}(\sqrt[3]{5})$ are given by

$$\sigma_1(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := \mathrm{id}(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) = 1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2$$

$$\sigma_2(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := 1 + a\omega\sqrt[3]{5} + b(\omega\sqrt[3]{5})^2 = 1 + a\omega\sqrt[3]{5} + b\omega^2(\sqrt[3]{5})^2$$

$$\sigma_3(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := 1 + a\omega^2\sqrt[3]{5} + b(\omega^2\sqrt[3]{5})^2 = 1 + a\omega^2\sqrt[3]{5} + b\omega(\sqrt[3]{5})^2.$$

Field embedding examples

Let $K = \mathbb{Q}(\sqrt[3]{5})$. Then the minimal polynomial is

$$p = x^3 - 5 = (x - \sqrt[3]{5})(x - \omega\sqrt[3]{5})(x - \omega^2\sqrt[3]{5}),$$

where $\omega = e^{2\pi i/3} = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{-1+i\sqrt{3}}{2}$. The three embeddings of $\mathbb{Q}(\sqrt[3]{5})$ are given by

$$\sigma_1(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := \mathrm{id}(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) = 1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2$$

$$\sigma_2(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := 1 + a\omega\sqrt[3]{5} + b(\omega\sqrt[3]{5})^2 = 1 + a\omega\sqrt[3]{5} + b\omega^2(\sqrt[3]{5})^2$$

$$\sigma_3(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := 1 + a\omega^2\sqrt[3]{5} + b(\omega^2\sqrt[3]{5})^2$$

Unlike the previous example, note that neither $\mathrm{im}(\sigma_2)$ nor $\mathrm{im}(\sigma_3)$ are contained in $\mathbb{Q}(\sqrt[3]{5})$.

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.

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.

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

Embeddings $\sigma_i : \theta \mapsto \theta_i$.

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.

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

Embeddings $\sigma_i : \theta \mapsto \theta_i$.

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.

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

Embeddings $\sigma_i : \theta \mapsto \theta_i$.

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 $\sigma_i(\alpha_j)$:

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

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.

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

Embeddings $\sigma_i : \theta \mapsto \theta_i$.

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 $\sigma_i(\alpha_j)$:

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

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.

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

Embeddings $\sigma_i : \theta \mapsto \theta_i$.

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 $\sigma_i(\alpha_j)$:

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

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.

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

Embeddings $\sigma_i : \theta \mapsto \theta_i$.

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 $\sigma_i(\alpha_j)$:

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

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

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

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

Proof. $A = (\sigma_i(\alpha_j))$ and $B = (\sigma_i(\beta_j))$.

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

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

Proof. $A = (\sigma_i(\alpha_j))$ and $B = (\sigma_i(\beta_j))$. Then $B = AC$.

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

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

Proof. $A = (\sigma_i(\alpha_j))$ and $B = (\sigma_i(\beta_j))$. Then $B = AC$. So

$$\det(B)^2 =$$

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

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

Proof. $A = (\sigma_i(\alpha_j))$ and $B = (\sigma_i(\beta_j))$. Then $B = AC$. So

$$\det(B)^2 = (\det(AC))^2 =$$

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

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

Proof. $A = (\sigma_i(\alpha_j))$ and $B = (\sigma_i(\beta_j))$. Then $B = AC$. So

$$\det(B)^2 = (\det(AC))^2 = (\det(A)\det(C))^2 = \text{etc.} \qquad \square$$

The discriminant

Next time, we will prove the following:

The discriminant

Next time, we will prove the following:

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

Next time, we will prove the following:

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

Next time, we will prove the following:

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

Next time, we will prove the following:

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

Next time, we will prove the following:

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.