Math 361

February 13, 2023

Tomorrow's quiz

See posting at our homepage.

Leftover

Proposition. Let C be an $n \times n$ integer matrix. The C is invertible and its inverse has integer coefficients if and only if $\det(C) = \pm 1$.

Leftover

Proposition. Let C be an $n \times n$ integer matrix. The C is invertible and its inverse has integer coefficients if and only if $\det(C) = \pm 1$.

Proof. ($\Rightarrow$) Suppose C is invertible and its inverse has integer coefficients.

Leftover

Proposition. Let C be an $n \times n$ integer matrix. The C is invertible and its inverse has integer coefficients if and only if $\det(C) = \pm 1$.

Proof. ($\Rightarrow$) Suppose C is invertible and its inverse has integer coefficients. Then

$$1 = CC^{-1} \quad \Rightarrow \quad 1 = \det(C)\det(C^{-1}).$$

Leftover

Proposition. Let C be an $n \times n$ integer matrix. The C is invertible and its inverse has integer coefficients if and only if $\det(C) = \pm 1$.

Proof. ($\Rightarrow$) Suppose C is invertible and its inverse has integer coefficients. Then

$$1 = CC^{-1} \quad \Rightarrow \quad 1 = \det(C)\det(C^{-1}).$$

But $\det(C)$ and $\det(C^{-1})$ are integers.

Leftover

Proposition. Let C be an $n \times n$ integer matrix. The C is invertible and its inverse has integer coefficients if and only if $\det(C) = \pm 1$.

Proof. ($\Rightarrow$) Suppose C is invertible and its inverse has integer coefficients. Then

$$1 = CC^{-1} \quad \Rightarrow \quad 1 = \det(C)\det(C^{-1}).$$

But $\det(C)$ and $\det(C^{-1})$ are integers. So $\det C = \pm 1$.

Leftover

Proposition. Let C be an $n \times n$ integer matrix. The C is invertible and its inverse has integer coefficients if and only if $\det(C) = \pm 1$.

Proof. ($\Rightarrow$) Suppose C is invertible and its inverse has integer coefficients. Then

$$1 = CC^{-1} \quad \Rightarrow \quad 1 = \det(C)\det(C^{-1}).$$

But $\det(C)$ and $\det(C^{-1})$ are integers. So $\det C = \pm 1$.

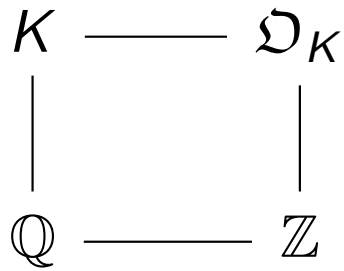
($\Leftarrow$) Suppose $\det(C) = \pm 1$. Then the adjugate formula for C^{-1} shows that C^{-1} has integer coefficients.

Today

1. Field polynomials
2. Norms and traces.

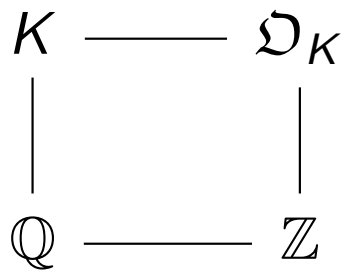
Field polynomials

Usual set-up:



Field polynomials

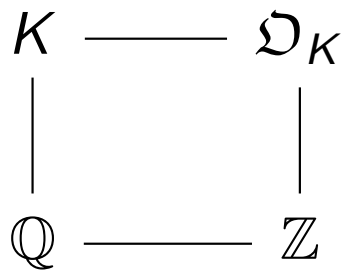
Usual set-up:



$K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$

Field polynomials

Usual set-up:

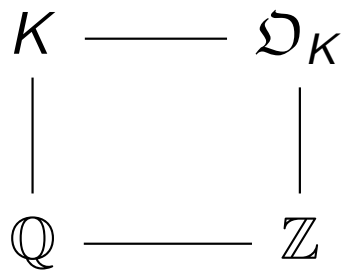


$K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$

min. poly. $p(x) = \prod_{i=1}^{n}(x - \theta_i)$

Field polynomials

Usual set-up:



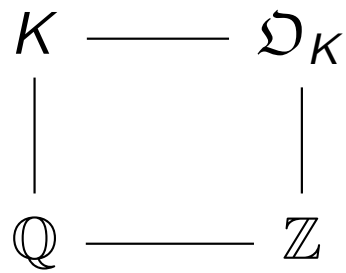
$K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$

min. poly. $p(x) = \prod_{i=1}^{n}(x - \theta_i)$

embeddings $\sigma_i : \theta \mapsto \theta_i$

Field polynomials

Usual set-up:



$K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$

min. poly. $p(x) = \prod_{i=1}^{n}(x - \theta_i)$

embeddings $\sigma_i : \theta \mapsto \theta_i$

The field polynomial for $\alpha \in K$ is

$$f_\alpha := \prod_{i=1}^{n}(x - \sigma_i(\alpha)).$$

Examples

Example. If $\alpha = \theta$, then f_α

Examples

Example. If $\alpha = \theta$, then f_α is the minimal polynomial for θ over $\mathbb{Q}$.

Examples

Example. If $\alpha = \theta$, then f_α is the minimal polynomial for θ over $\mathbb{Q}$.

Example. $K = \mathbb{Q}(\sqrt{2})$, $\alpha = 2 + 3\sqrt{2}$. Check that

$$f_\alpha = x^2 - 4x - 14,$$

Examples

Example. If $\alpha = \theta$, then f_α is the minimal polynomial for θ over $\mathbb{Q}$.

Example. $K = \mathbb{Q}(\sqrt{2})$, $\alpha = 2 + 3\sqrt{2}$. Check that

$$f_\alpha = x^2 - 4x - 14,$$

the minimal polynomial for α over $\mathbb{Q}$.

Examples

Example. If $\alpha = \theta$, then f_α is the minimal polynomial for θ over $\mathbb{Q}$.

Example. $K = \mathbb{Q}(\sqrt{2})$, $\alpha = 2 + 3\sqrt{2}$. Check that

$$f_\alpha = x^2 - 4x - 14,$$

the minimal polynomial for α over $\mathbb{Q}$.

For another example, let $\alpha = 5 \in \mathbb{Z}$.

Examples

Example. If $\alpha = \theta$, then f_α is the minimal polynomial for θ over $\mathbb{Q}$.

Example. $K = \mathbb{Q}(\sqrt{2})$, $\alpha = 2 + 3\sqrt{2}$. Check that

$$f_\alpha = x^2 - 4x - 14,$$

the minimal polynomial for α over $\mathbb{Q}$.

For another example, let $\alpha = 5 \in \mathbb{Z}$. Then

$$f_5 = (x - \sigma_1(5))(x - \sigma_2(5))$$

Examples

Example. If $\alpha = \theta$, then f_α is the minimal polynomial for θ over $\mathbb{Q}$.

Example. $K = \mathbb{Q}(\sqrt{2})$, $\alpha = 2 + 3\sqrt{2}$. Check that

$$f_\alpha = x^2 - 4x - 14,$$

the minimal polynomial for α over $\mathbb{Q}$.

For another example, let $\alpha = 5 \in \mathbb{Z}$. Then

$$f_5 = (x - \sigma_1(5))(x - \sigma_2(5)) = (x - 5)^2.$$

Examples

Example. If $\alpha = \theta$, then f_α is the minimal polynomial for θ over $\mathbb{Q}$.

Example. $K = \mathbb{Q}(\sqrt{2})$, $\alpha = 2 + 3\sqrt{2}$. Check that

$$f_\alpha = x^2 - 4x - 14,$$

the minimal polynomial for α over $\mathbb{Q}$.

For another example, let $\alpha = 5 \in \mathbb{Z}$. Then

$$f_5 = (x - \sigma_1(5))(x - \sigma_2(5)) = (x - 5)^2.$$

So f_5 is the square of the minimal polynomial $x - 5$ for 5 over $\mathbb{Q}$.

Field polynomials

Theorem. With notation as above, let p_α be the minimal polynomial for α over $\mathbb{Q}$.

Field polynomials

Theorem. With notation as above, let p_α be the minimal polynomial for α over $\mathbb{Q}$.

1. The field polynomial has rational coefficients: $f_\alpha \in \mathbb{Q}[x]$.

Field polynomials

Theorem. With notation as above, let p_α be the minimal polynomial for α over $\mathbb{Q}$.

1. The field polynomial has rational coefficients: $f_\alpha \in \mathbb{Q}[x]$.
2. There exists a positive integer k such that $f_\alpha = p_\alpha^k$.

Field polynomials

Theorem. With notation as above, let p_α be the minimal polynomial for α over $\mathbb{Q}$.

1. The field polynomial has rational coefficients: $f_\alpha \in \mathbb{Q}[x]$.
2. There exists a positive integer k such that $f_\alpha = p_\alpha^k$.
3. If α is an algebraic integer, then f_α has integer coefficients: $f_\alpha \in \mathbb{Z}[x]$.

Proof of theorem

Claim: The field polynomial has rational coefficients: $f_\alpha \in \mathbb{Q}[x]$.

Proof of theorem

Claim: The field polynomial has rational coefficients: $f_\alpha \in \mathbb{Q}[x]$.

Proof.

- There exists $r \in \mathbb{Q}[x]$ such that $\alpha = r(\theta)$.

Proof of theorem

Claim: The field polynomial has rational coefficients: $f_\alpha \in \mathbb{Q}[x]$.

Proof.

- There exists $r \in \mathbb{Q}[x]$ such that $\alpha = r(\theta)$.
- $\sigma_i(\alpha) = \sigma_i(r(\theta))$

Proof of theorem

Claim: The field polynomial has rational coefficients: $f_\alpha \in \mathbb{Q}[x]$.

Proof.

- There exists $r \in \mathbb{Q}[x]$ such that $\alpha = r(\theta)$.
- $\sigma_i(\alpha) = \sigma_i(r(\theta)) = r(\sigma_i(\theta))$

Proof of theorem

Claim: The field polynomial has rational coefficients: $f_\alpha \in \mathbb{Q}[x]$.

Proof.

- There exists $r \in \mathbb{Q}[x]$ such that $\alpha = r(\theta)$.
- $\sigma_i(\alpha) = \sigma_i(r(\theta)) = r(\sigma_i(\theta)) = r(\theta_i)$

Proof of theorem

Claim: The field polynomial has rational coefficients: $f_\alpha \in \mathbb{Q}[x]$.

Proof.

- There exists $r \in \mathbb{Q}[x]$ such that $\alpha = r(\theta)$.
- $\sigma_i(\alpha) = \sigma_i(r(\theta)) = r(\sigma_i(\theta)) = r(\theta_i)$
- $f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - r(\theta_i))$

Proof of theorem

Claim: The field polynomial has rational coefficients: $f_\alpha \in \mathbb{Q}[x]$.

Proof.

- There exists $r \in \mathbb{Q}[x]$ such that $\alpha = r(\theta)$.
- $\sigma_i(\alpha) = \sigma_i(r(\theta)) = r(\sigma_i(\theta)) = r(\theta_i)$
- $f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - r(\theta_i))$

  $= x^n - (\sigma_1(\alpha) + \cdots + \sigma_{p-2}(\alpha))x^{n-1} + \cdots + (-1)^n \sigma_1(\alpha) \cdots \sigma_{p-1}(\alpha)$

Proof of theorem

Claim: The field polynomial has rational coefficients: $f_\alpha \in \mathbb{Q}[x]$.

Proof.

- There exists $r \in \mathbb{Q}[x]$ such that $\alpha = r(\theta)$.
- $\sigma_i(\alpha) = \sigma_i(r(\theta)) = r(\sigma_i(\theta)) = r(\theta_i)$
- $f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - r(\theta_i))$

  $= x^n - (\sigma_1(\alpha) + \cdots + \sigma_{p-2}(\alpha))x^{n-1} + \cdots + (-1)^n \sigma_1(\alpha) \cdots \sigma_{p-1}(\alpha)$

- The coefficients are symmetric functions in the θ_i, hence, rational. $\square$

Proof of theorem.

Claim. There exists a positive integer k such that $f_\alpha = p_\alpha^k$.

Proof of theorem.

Claim. There exists a positive integer k such that $f_\alpha = p_\alpha^k$.

- $p_\alpha | f_\alpha$ in $\mathbb{Q}[x]$.

Proof of theorem.

Claim. There exists a positive integer k such that $f_\alpha = p_\alpha^k$.

- $p_\alpha | f_\alpha$ in $\mathbb{Q}[x]$.
- So we have write $f_\alpha = p_\alpha^k h$ for some $h \in \mathbb{Q}[x]$ relatively prime to p_α.

Proof of theorem.

Claim. There exists a positive integer k such that $f_\alpha = p_\alpha^k$.

- $p_\alpha | f_\alpha$ in $\mathbb{Q}[x]$.
- So we have write $f_\alpha = p_\alpha^k h$ for some $h \in \mathbb{Q}[x]$ relatively prime to p_α. Further, h is monic.

Proof of theorem.

Claim. There exists a positive integer k such that $f_\alpha = p_\alpha^k$.

- $p_\alpha | f_\alpha$ in $\mathbb{Q}[x]$.
- So we have write $f_\alpha = p_\alpha^k h$ for some $h \in \mathbb{Q}[x]$ relatively prime to p_α. Further, h is monic.
- It suffices to show h is constant (i.e., $h = 1$ since monic).

Proof of theorem.

Claim. There exists a positive integer k such that $f_\alpha = p_\alpha^k$.

- $p_\alpha | f_\alpha$ in $\mathbb{Q}[x]$.
- So we have write $f_\alpha = p_\alpha^k h$ for some $h \in \mathbb{Q}[x]$ relatively prime to p_α. Further, h is monic.
- It suffices to show h is constant (i.e., $h = 1$ since monic). For sake of contradiction, suppose not.

Proof of theorem.

Claim. There exists a positive integer k such that $f_\alpha = p_\alpha^k$.

- $p_\alpha | f_\alpha$ in $\mathbb{Q}[x]$.
- So we have write $f_\alpha = p_\alpha^k h$ for some $h \in \mathbb{Q}[x]$ relatively prime to p_α. Further, h is monic.
- It suffices to show h is constant (i.e., $h = 1$ since monic). For sake of contradiction, suppose not. We will get the contradiction $p_\alpha | h$.

Proof of theorem.

Claim. There exists a positive integer k such that $f_\alpha = p_\alpha^k$.

- $p_\alpha | f_\alpha$ in $\mathbb{Q}[x]$.
- So we have write $f_\alpha = p_\alpha^k h$ for some $h \in \mathbb{Q}[x]$ relatively prime to p_α. Further, h is monic.
- It suffices to show h is constant (i.e., $h = 1$ since monic). For sake of contradiction, suppose not. We will get the contradiction $p_\alpha | h$. Factor in $\mathbb{C}[x]$:

$$f_\alpha = \prod_{i=1}^{n} (x - \sigma_i(\alpha)) = \prod_{i=1}^{n} (x - r(\theta_i)) = (p_\alpha(x))^k h(x),$$

Proof of theorem.

Claim. There exists a positive integer k such that $f_\alpha = p_\alpha^k$.

- $p_\alpha | f_\alpha$ in $\mathbb{Q}[x]$.
- So we have write $f_\alpha = p_\alpha^k h$ for some $h \in \mathbb{Q}[x]$ relatively prime to p_α. Further, h is monic.
- It suffices to show h is constant (i.e., $h = 1$ since monic). For sake of contradiction, suppose not. We will get the contradiction $p_\alpha | h$. Factor in $\mathbb{C}[x]$:

$$f_\alpha = \prod_{i=1}^{n} (x - \sigma_i(\alpha)) = \prod_{i=1}^{n} (x - r(\theta_i)) = (p_\alpha(x))^k h(x),$$

By unique factorization, it follows that there exists j such that $r(\theta_j)$ is a zero of h,

Proof of theorem.

Claim. There exists a positive integer k such that $f_\alpha = p_\alpha^k$.

- $p_\alpha | f_\alpha$ in $\mathbb{Q}[x]$.
- So we have write $f_\alpha = p_\alpha^k h$ for some $h \in \mathbb{Q}[x]$ relatively prime to p_α. Further, h is monic.
- It suffices to show h is constant (i.e., $h = 1$ since monic). For sake of contradiction, suppose not. We will get the contradiction $p_\alpha | h$. Factor in $\mathbb{C}[x]$:

$$f_\alpha = \prod_{i=1}^{n} (x - \sigma_i(\alpha)) = \prod_{i=1}^{n} (x - r(\theta_i)) = (p_\alpha(x))^k h(x),$$

By unique factorization, it follows that there exists j such that $r(\theta_j)$ is a zero of h, i.e., $h(r(\theta_j)) = 0$.

Proof of theorem.

Claim. There exists a positive integer k such that $f_\alpha = p_\alpha^k$.

- $p_\alpha | f_\alpha$ in $\mathbb{Q}[x]$.
- So we have write $f_\alpha = p_\alpha^k h$ for some $h \in \mathbb{Q}[x]$ relatively prime to p_α. Further, h is monic.
- It suffices to show h is constant (i.e., $h = 1$ since monic). For sake of contradiction, suppose not. We will get the contradiction $p_\alpha | h$. Factor in $\mathbb{C}[x]$:

$$f_\alpha = \prod_{i=1}^{n} (x - \sigma_i(\alpha)) = \prod_{i=1}^{n} (x - r(\theta_i)) = (p_\alpha(x))^k h(x),$$

By unique factorization, it follows that there exists j such that $r(\theta_j)$ is a zero of h, i.e., $h(r(\theta_j)) = 0$. Define $g(x) := h(r(x))$.

Proof of theorem.

Claim. There exists a positive integer k such that $f_\alpha = p_\alpha^k$.

- $p_\alpha | f_\alpha$ in $\mathbb{Q}[x]$.
- So we have write $f_\alpha = p_\alpha^k h$ for some $h \in \mathbb{Q}[x]$ relatively prime to p_α. Further, h is monic.
- It suffices to show h is constant (i.e., $h = 1$ since monic). For sake of contradiction, suppose not. We will get the contradiction $p_\alpha | h$. Factor in $\mathbb{C}[x]$:

$$f_\alpha = \prod_{i=1}^{n} (x - \sigma_i(\alpha)) = \prod_{i=1}^{n} (x - r(\theta_i)) = (p_\alpha(x))^k h(x),$$

By unique factorization, it follows that there exists j such that $r(\theta_j)$ is a zero of h, i.e., $h(r(\theta_j)) = 0$. Define $g(x) := h(r(x))$. Then $g(\theta_j) = 0$.

Proof of theorem

$$r(\theta) = \alpha$$

Proof of theorem

$$r(\theta) = \alpha$$

$$f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - r(\theta_i)) = (p_\alpha(x))^k h(x)$$

Proof of theorem

$r(\theta) = \alpha$

$f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - r(\theta_i)) = (p_\alpha(x))^k h(x)$

$g(x) := h(r(x))$,

Proof of theorem

$$r(\theta) = \alpha$$

$$f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - r(\theta_i)) = (p_\alpha(x))^k h(x)$$

$$g(x) := h(r(x)), \quad g(\theta_j) = h(r(\theta_j)) = 0$$

Proof of theorem

$r(\theta) = \alpha$

$f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - r(\theta_i)) = (p_\alpha(x))^k h(x)$

$g(x) := h(r(x)), \quad g(\theta_j) = h(r(\theta_j)) = 0$

- p is the minimal polynomial for all θ_i.

Proof of theorem

$r(\theta) = \alpha$

$f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - r(\theta_i)) = (p_\alpha(x))^k h(x)$

$g(x) := h(r(x)), \quad g(\theta_j) = h(r(\theta_j)) = 0$

- p is the minimal polynomial for all θ_i.
- In particular, p is the min. poly. for θ_j.

Proof of theorem

$r(\theta) = \alpha$

$f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - r(\theta_i)) = (p_\alpha(x))^k h(x)$

$g(x) := h(r(x)), \quad g(\theta_j) = h(r(\theta_j)) = 0$

- p is the minimal polynomial for all θ_i.
- In particular, p is the min. poly. for θ_j. Therefore, $g(\theta_j) = 0 \Rightarrow p|g$ in $\mathbb{Q}[x]$.

Proof of theorem

$r(\theta) = \alpha$

$f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - r(\theta_i)) = (p_\alpha(x))^k h(x)$

$g(x) := h(r(x)), \quad g(\theta_j) = h(r(\theta_j)) = 0$

- p is the minimal polynomial for all θ_i.
- In particular, p is the min. poly. for θ_j. Therefore, $g(\theta_j) = 0 \Rightarrow p|g$ in $\mathbb{Q}[x]$.
- Since $p|g$, all θ_i are zeros of g.

Proof of theorem

$r(\theta) = \alpha$

$f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - r(\theta_i)) = (p_\alpha(x))^k h(x)$

$g(x) := h(r(x)), \quad g(\theta_j) = h(r(\theta_j)) = 0$

- p is the minimal polynomial for all θ_i.
- In particular, p is the min. poly. for θ_j. Therefore, $g(\theta_j) = 0 \Rightarrow p|g$ in $\mathbb{Q}[x]$.
- Since $p|g$, all θ_i are zeros of g. In particular, letting $i = 1$, we have $g(\theta) = 0$.

Proof of theorem

$r(\theta) = \alpha$

$f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - r(\theta_i)) = (p_\alpha(x))^k h(x)$

$g(x) := h(r(x)), \quad g(\theta_j) = h(r(\theta_j)) = 0$

- p is the minimal polynomial for all θ_i.
- In particular, p is the min. poly. for θ_j. Therefore, $g(\theta_j) = 0 \Rightarrow p|g$ in $\mathbb{Q}[x]$.
- Since $p|g$, all θ_i are zeros of g. In particular, letting $i = 1$, we have $g(\theta) = 0$.
- Hence, $h(\alpha) = h(r(\theta)) =$

Proof of theorem

$r(\theta) = \alpha$

$f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - r(\theta_i)) = (p_\alpha(x))^k h(x)$

$g(x) := h(r(x)), \quad g(\theta_j) = h(r(\theta_j)) = 0$

- p is the minimal polynomial for all θ_i.
- In particular, p is the min. poly. for θ_j. Therefore, $g(\theta_j) = 0 \Rightarrow p|g$ in $\mathbb{Q}[x]$.
- Since $p|g$, all θ_i are zeros of g. In particular, letting $i = 1$, we have $g(\theta) = 0$.
- Hence, $h(\alpha) = h(r(\theta)) = g(\theta)$

Proof of theorem

$r(\theta) = \alpha$

$f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - r(\theta_i)) = (p_\alpha(x))^k h(x)$

$g(x) := h(r(x)), \quad g(\theta_j) = h(r(\theta_j)) = 0$

- p is the minimal polynomial for all θ_i.
- In particular, p is the min. poly. for θ_j. Therefore, $g(\theta_j) = 0 \Rightarrow p|g$ in $\mathbb{Q}[x]$.
- Since $p|g$, all θ_i are zeros of g. In particular, letting $i = 1$, we have $g(\theta) = 0$.
- Hence, $h(\alpha) = h(r(\theta)) = g(\theta) = 0$.

Proof of theorem

$r(\theta) = \alpha$

$f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - r(\theta_i)) = (p_\alpha(x))^k h(x)$

$g(x) := h(r(x)), \quad g(\theta_j) = h(r(\theta_j)) = 0$

- p is the minimal polynomial for all θ_i.
- In particular, p is the min. poly. for θ_j. Therefore, $g(\theta_j) = 0 \Rightarrow p|g$ in $\mathbb{Q}[x]$.
- Since $p|g$, all θ_i are zeros of g. In particular, letting $i = 1$, we have $g(\theta) = 0$.
- Hence, $h(\alpha) = h(r(\theta)) = g(\theta) = 0$.
- So $p_\alpha|h$.

Proof of theorem

$r(\theta) = \alpha$

$f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - r(\theta_i)) = (p_\alpha(x))^k h(x)$

$g(x) := h(r(x)), \quad g(\theta_j) = h(r(\theta_j)) = 0$

- p is the minimal polynomial for all θ_i.
- In particular, p is the min. poly. for θ_j. Therefore, $g(\theta_j) = 0 \Rightarrow p|g$ in $\mathbb{Q}[x]$.
- Since $p|g$, all θ_i are zeros of g. In particular, letting $i = 1$, we have $g(\theta) = 0$.
- Hence, $h(\alpha) = h(r(\theta)) = g(\theta) = 0$.
- So $p_\alpha|h$. Contradiction. $\square$

Proof of theorem

Claim: If α is an algebraic integer, the f_α has integer coefficients: $f_\alpha \in \mathbb{Z}[x]$.

Proof of theorem

Claim: If α is an algebraic integer, the f_α has integer coefficients: $f_\alpha \in \mathbb{Z}[x]$.

Proof. The minimal polynomial for α over $\mathbb{Q}$ is p_α.

Proof of theorem

Claim: If α is an algebraic integer, the f_α has integer coefficients: $f_\alpha \in \mathbb{Z}[x]$.

Proof. The minimal polynomial for α over $\mathbb{Q}$ is p_α.
So if α is an algebraic integer, then $p_\alpha \in \mathbb{Z}[x]$.

Proof of theorem

Claim: If α is an algebraic integer, the f_α has integer coefficients: $f_\alpha \in \mathbb{Z}[x]$.

Proof. The minimal polynomial for α over $\mathbb{Q}$ is p_α.
So if α is an algebraic integer, then $p_\alpha \in \mathbb{Z}[x]$.

The result now follows since $f_\alpha = p_\alpha^k$. $\square$

Norm and Trace

Definition. Let $\alpha \in K$. The *norm* of α is

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

Norm and Trace

Definition. Let $\alpha \in K$. The *norm* of α is

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

and the *trace* of α is

$$T(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Norm and Trace

Definition. Let $\alpha \in K$. The *norm* of α is

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

and the *trace* of α is

$$T(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Example. For $\alpha = 2 + 3\sqrt{2} \in K = \mathbb{Q}(\sqrt{2})$,

Norm and Trace

Definition. Let $\alpha \in K$. The *norm* of α is

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

and the *trace* of α is

$$T(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Example. For $\alpha = 2 + 3\sqrt{2} \in K = \mathbb{Q}(\sqrt{2})$,

$$N(\alpha) = \sigma_1(2 + 3\sqrt{2})\sigma_2(2 + 3\sqrt{2})$$

Norm and Trace

Definition. Let $\alpha \in K$. The *norm* of α is

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

and the *trace* of α is

$$T(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Example. For $\alpha = 2 + 3\sqrt{2} \in K = \mathbb{Q}(\sqrt{2})$,

$$N(\alpha) = \sigma_1(2 + 3\sqrt{2})\sigma_2(2 + 3\sqrt{2}) = (2 + 3\sqrt{2})(2 - 3\sqrt{2})$$

Norm and Trace

Definition. Let $\alpha \in K$. The *norm* of α is

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

and the *trace* of α is

$$T(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Example. For $\alpha = 2 + 3\sqrt{2} \in K = \mathbb{Q}(\sqrt{2})$,

$$N(\alpha) = \sigma_1(2 + 3\sqrt{2})\sigma_2(2 + 3\sqrt{2}) = (2 + 3\sqrt{2})(2 - 3\sqrt{2}) = -14$$

Norm and Trace

Definition. Let $\alpha \in K$. The *norm* of α is

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

and the *trace* of α is

$$T(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Example. For $\alpha = 2 + 3\sqrt{2} \in K = \mathbb{Q}(\sqrt{2})$,

$$N(\alpha) = \sigma_1(2 + 3\sqrt{2})\sigma_2(2 + 3\sqrt{2}) = (2 + 3\sqrt{2})(2 - 3\sqrt{2}) = -14$$

and

$$T(\alpha) = \sigma_1(2 + 3\sqrt{2}) + \sigma_2(2 + 3\sqrt{2})$$

Norm and Trace

Definition. Let $\alpha \in K$. The *norm* of α is

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

and the *trace* of α is

$$T(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Example. For $\alpha = 2 + 3\sqrt{2} \in K = \mathbb{Q}(\sqrt{2})$,

$$N(\alpha) = \sigma_1(2 + 3\sqrt{2})\sigma_2(2 + 3\sqrt{2}) = (2 + 3\sqrt{2})(2 - 3\sqrt{2}) = -14$$

and

$$T(\alpha) = \sigma_1(2 + 3\sqrt{2}) + \sigma_2(2 + 3\sqrt{2}) = (2 + 3\sqrt{2}) + (2 - 3\sqrt{2})$$

Norm and Trace

Definition. Let $\alpha \in K$. The *norm* of α is

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

and the *trace* of α is

$$T(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Example. For $\alpha = 2 + 3\sqrt{2} \in K = \mathbb{Q}(\sqrt{2})$,

$$N(\alpha) = \sigma_1(2 + 3\sqrt{2})\sigma_2(2 + 3\sqrt{2}) = (2 + 3\sqrt{2})(2 - 3\sqrt{2}) = -14$$

and

$$T(\alpha) = \sigma_1(2+3\sqrt{2}) + \sigma_2(2+3\sqrt{2}) = (2+3\sqrt{2}) + (2-3\sqrt{2}) = 4.$$

Properties of the norm and trace

1. $N(\alpha\beta) = N(\alpha)N(\beta)$ and $T(\alpha + \beta) = T(\alpha) + T(\beta)$.

Properties of the norm and trace

1. $N(\alpha\beta) = N(\alpha)N(\beta)$ and $T(\alpha+\beta) = T(\alpha)+T(\beta)$.

2. The norm and trace appear as coefficients of the corresponding field polynomial: $f_\alpha = \prod_{i=1}^{n}(x-\sigma_i(x))$

Properties of the norm and trace

1. $N(\alpha\beta) = N(\alpha)N(\beta)$ and $T(\alpha+\beta) = T(\alpha) + T(\beta)$.

2. The norm and trace appear as coefficients of the corresponding field polynomial: $f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(x))$

$$= x^n - (\underbrace{\sigma_1(\alpha) + \cdots + \sigma_n(\alpha)}_{T(\alpha)})x^{n-1} + \cdots + (-1)^n \underbrace{\sigma_1(\alpha)\cdots\sigma_n(\alpha)}_{N(\alpha)}.$$

Properties of the norm and trace

1. $N(\alpha\beta) = N(\alpha)N(\beta)$ and $T(\alpha+\beta) = T(\alpha) + T(\beta)$.

2. The norm and trace appear as coefficients of the corresponding field polynomial: $f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(x))$

$$= x^n - (\underbrace{\sigma_1(\alpha) + \cdots + \sigma_n(\alpha)}_{T(\alpha)})x^{n-1} + \cdots + (-1)^n \underbrace{\sigma_1(\alpha)\cdots\sigma_n(\alpha)}_{N(\alpha)}.$$

3. $N(\alpha), T(\alpha) \in \mathbb{Q}$. If $\alpha \in \mathfrak{O}_K$, then $N(\alpha), T(\alpha) \in \mathbb{Z}$

Properties of the norm and trace

1. $N(\alpha\beta) = N(\alpha)N(\beta)$ and $T(\alpha+\beta) = T(\alpha) + T(\beta)$.

2. The norm and trace appear as coefficients of the corresponding field polynomial: $f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(x))$

$$= x^n - (\underbrace{\sigma_1(\alpha) + \cdots + \sigma_n(\alpha)}_{T(\alpha)})x^{n-1} + \cdots + (-1)^n \underbrace{\sigma_1(\alpha)\cdots\sigma_n(\alpha)}_{N(\alpha)}.$$

3. $N(\alpha), T(\alpha) \in \mathbb{Q}$. If $\alpha \in \mathfrak{O}_K$, then $N(\alpha), T(\alpha) \in \mathbb{Z}$ (since $f_\alpha \in \mathbb{Z}[x]$ in this case).

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

5. Suppose that $\alpha \in \mathfrak{O}_K$. If $N(\alpha) = q \in \mathbb{Z}$ where q is a rational prime, then α is irreducible.

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

5. Suppose that $\alpha \in \mathfrak{O}_K$. If $N(\alpha) = q \in \mathbb{Z}$ where q is a rational prime, then α is irreducible.

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] =$$

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

5. Suppose that $\alpha \in \mathfrak{O}_K$. If $N(\alpha) = q \in \mathbb{Z}$ where q is a rational prime, then α is irreducible.

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta))$$

where p' is the derivative of p.

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

5. Suppose that $\alpha \in \mathfrak{O}_K$. If $N(\alpha) = q \in \mathbb{Z}$ where q is a rational prime, then α is irreducible.

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta))$$

where p' is the derivative of p.

7. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K.

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

5. Suppose that $\alpha \in \mathfrak{O}_K$. If $N(\alpha) = q \in \mathbb{Z}$ where q is a rational prime, then α is irreducible.

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta))$$

where p' is the derivative of p.

7. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K. Let S be the $n \times n$ matrix with ij-th entry $T(\alpha_i \alpha_j)$.

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

5. Suppose that $\alpha \in \mathfrak{O}_K$. If $N(\alpha) = q \in \mathbb{Z}$ where q is a rational prime, then α is irreducible.

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta))$$

where p' is the derivative of p.

7. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K. Let S be the $n \times n$ matrix with ij-th entry $T(\alpha_i \alpha_j)$. Then

$$\Delta[\alpha_1, \ldots, \alpha_n] =$$

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

5. Suppose that $\alpha \in \mathfrak{O}_K$. If $N(\alpha) = q \in \mathbb{Z}$ where q is a rational prime, then α is irreducible.

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta))$$

where p' is the derivative of p.

7. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K. Let S be the $n \times n$ matrix with ij-th entry $T(\alpha_i \alpha_j)$. Then

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det S = \det((T(\alpha_i \alpha_j))).$$

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

Proof. ($\Rightarrow$) Suppose there exist $\beta \in \mathfrak{O}_K$ such that $\alpha\beta = 1$.

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

Proof. ($\Rightarrow$) Suppose there exist $\beta \in \mathfrak{O}_K$ such that $\alpha\beta = 1$. Then

$$1 = N(1)$$

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

Proof. ($\Rightarrow$) Suppose there exist $\beta \in \mathfrak{O}_K$ such that $\alpha\beta = 1$. Then

$$1 = N(1) = N(\alpha\beta)$$

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

Proof. ($\Rightarrow$) Suppose there exist $\beta \in \mathfrak{O}_K$ such that $\alpha\beta = 1$. Then

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

Proof. ($\Rightarrow$) Suppose there exist $\beta \in \mathfrak{O}_K$ such that $\alpha\beta = 1$. Then

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

But $N(\alpha), N(\beta) \in \mathbb{Z}$.

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

Proof. ($\Rightarrow$) Suppose there exist $\beta \in \mathfrak{O}_K$ such that $\alpha\beta = 1$. Then

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

But $N(\alpha), N(\beta) \in \mathbb{Z}$. So $N(\alpha) = \pm 1$.

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

Proof. ($\Rightarrow$) Suppose there exist $\beta \in \mathfrak{O}_K$ such that $\alpha\beta = 1$. Then

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

But $N(\alpha), N(\beta) \in \mathbb{Z}$. So $N(\alpha) = \pm 1$.

($\Leftarrow$) Suppose that $N(\alpha) = \pm 1$:

$$\pm 1 = \prod_{i=1}^{n} \sigma_i(\alpha) = \alpha \underbrace{\sigma_2(\alpha) \cdots \sigma_n(\alpha)}_{\beta}.$$

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

Proof. ($\Rightarrow$) Suppose there exist $\beta \in \mathfrak{O}_K$ such that $\alpha\beta = 1$. Then

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

But $N(\alpha), N(\beta) \in \mathbb{Z}$. So $N(\alpha) = \pm 1$.

($\Leftarrow$) Suppose that $N(\alpha) = \pm 1$:

$$\pm 1 = \prod_{i=1}^{n} \sigma_i(\alpha) = \alpha \underbrace{\sigma_2(\alpha) \cdots \sigma_n(\alpha)}_{\beta}.$$

We claim $\beta \in \mathfrak{O}_K$.

1. $\beta \in K$ since

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

Proof. ($\Rightarrow$) Suppose there exist $\beta \in \mathfrak{O}_K$ such that $\alpha\beta = 1$. Then

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

But $N(\alpha), N(\beta) \in \mathbb{Z}$. So $N(\alpha) = \pm 1$.

($\Leftarrow$) Suppose that $N(\alpha) = \pm 1$:

$$\pm 1 = \prod_{i=1}^{n} \sigma_i(\alpha) = \alpha \underbrace{\sigma_2(\alpha) \cdots \sigma_n(\alpha)}_{\beta}.$$

We claim $\beta \in \mathfrak{O}_K$.

1. $\beta \in K$ since $\beta = \pm\frac{1}{\alpha} \in K$.

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

Proof. ($\Rightarrow$) Suppose there exist $\beta \in \mathfrak{O}_K$ such that $\alpha\beta = 1$. Then

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

But $N(\alpha), N(\beta) \in \mathbb{Z}$. So $N(\alpha) = \pm 1$.

($\Leftarrow$) Suppose that $N(\alpha) = \pm 1$:

$$\pm 1 = \prod_{i=1}^{n} \sigma_i(\alpha) = \alpha \underbrace{\sigma_2(\alpha) \cdots \sigma_n(\alpha)}_{\beta}.$$

We claim $\beta \in \mathfrak{O}_K$.

1. $\beta \in K$ since $\beta = \pm\frac{1}{\alpha} \in K$.
2. β is an algebraic number:

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

Proof. ($\Rightarrow$) Suppose there exist $\beta \in \mathfrak{O}_K$ such that $\alpha\beta = 1$. Then

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

But $N(\alpha), N(\beta) \in \mathbb{Z}$. So $N(\alpha) = \pm 1$.

($\Leftarrow$) Suppose that $N(\alpha) = \pm 1$:

$$\pm 1 = \prod_{i=1}^{n} \sigma_i(\alpha) = \alpha \underbrace{\sigma_2(\alpha) \cdots \sigma_n(\alpha)}_{\beta}.$$

We claim $\beta \in \mathfrak{O}_K$.

1. $\beta \in K$ since $\beta = \pm\frac{1}{\alpha} \in K$.
2. β is an algebraic number: Each $\sigma_i(\alpha)$ satisfies the minimal polynomial for α, and

Properties of norm and trace

4. Suppose that $\alpha \in \mathfrak{O}_K$. Then α is a unit if and only if $N(\alpha) = \pm 1$.

Proof. ($\Rightarrow$) Suppose there exist $\beta \in \mathfrak{O}_K$ such that $\alpha\beta = 1$. Then

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

But $N(\alpha), N(\beta) \in \mathbb{Z}$. So $N(\alpha) = \pm 1$.

($\Leftarrow$) Suppose that $N(\alpha) = \pm 1$:

$$\pm 1 = \prod_{i=1}^{n} \sigma_i(\alpha) = \alpha \underbrace{\sigma_2(\alpha) \cdots \sigma_n(\alpha)}_{\beta}.$$

We claim $\beta \in \mathfrak{O}_K$.

1. $\beta \in K$ since $\beta = \pm\frac{1}{\alpha} \in K$.
2. β is an algebraic number: Each $\sigma_i(\alpha)$ satisfies the minimal polynomial for α, and the algebraic numbers form a ring. $\square$

Properties of norm and trace

5. Suppose that $\alpha \in \mathfrak{O}_K$. If $N(\alpha) = q \in \mathbb{Z}$ where q is a rational prime, then α is irreducible.

Properties of norm and trace

5. Suppose that $\alpha \in \mathfrak{O}_K$. If $N(\alpha) = q \in \mathbb{Z}$ where q is a rational prime, then α is irreducible.

Proof. Suppose that $\alpha = \beta\gamma$ for some $\beta, \gamma \in \mathfrak{O}_K$.

Properties of norm and trace

5. Suppose that $\alpha \in \mathfrak{O}_K$. If $N(\alpha) = q \in \mathbb{Z}$ where q is a rational prime, then α is irreducible.

Proof. Suppose that $\alpha = \beta\gamma$ for some $\beta, \gamma \in \mathfrak{O}_K$. Then

$$q = N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma).$$

Properties of norm and trace

5. Suppose that $\alpha \in \mathfrak{O}_K$. If $N(\alpha) = q \in \mathbb{Z}$ where q is a rational prime, then α is irreducible.

Proof. Suppose that $\alpha = \beta\gamma$ for some $\beta, \gamma \in \mathfrak{O}_K$. Then

$$q = N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma).$$

Since $N(\beta), N(\gamma) \in \mathbb{Z}$ and q is prime, one of $N(\beta)$ or $N(\gamma)$ is ± 1.

Properties of norm and trace

5. Suppose that $\alpha \in \mathfrak{O}_K$. If $N(\alpha) = q \in \mathbb{Z}$ where q is a rational prime, then α is irreducible.

Proof. Suppose that $\alpha = \beta\gamma$ for some $\beta, \gamma \in \mathfrak{O}_K$. Then

$$q = N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma).$$

Since $N(\beta), N(\gamma) \in \mathbb{Z}$ and q is prime, one of $N(\beta)$ or $N(\gamma)$ is ± 1. Without loss of generality, say $N(\beta) = \pm 1$.

Properties of norm and trace

5. Suppose that $\alpha \in \mathfrak{O}_K$. If $N(\alpha) = q \in \mathbb{Z}$ where q is a rational prime, then α is irreducible.

Proof. Suppose that $\alpha = \beta\gamma$ for some $\beta, \gamma \in \mathfrak{O}_K$. Then

$$q = N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma).$$

Since $N(\beta), N(\gamma) \in \mathbb{Z}$ and q is prime, one of $N(\beta)$ or $N(\gamma)$ is ± 1. Without loss of generality, say $N(\beta) = \pm 1$. It follows that β is a unit.

Properties of norm and trace

5. Suppose that $\alpha \in \mathfrak{O}_K$. If $N(\alpha) = q \in \mathbb{Z}$ where q is a rational prime, then α is irreducible.

Proof. Suppose that $\alpha = \beta\gamma$ for some $\beta, \gamma \in \mathfrak{O}_K$. Then

$$q = N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma).$$

Since $N(\beta), N(\gamma) \in \mathbb{Z}$ and q is prime, one of $N(\beta)$ or $N(\gamma)$ is ± 1. Without loss of generality, say $N(\beta) = \pm 1$. It follows that β is a unit. Thus, α is irreducible. $\square$

Properties of norm and trace

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta)).$$

Properties of norm and trace

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta)).$$

Proof. $\Delta[1, \theta, \ldots, \theta^{n-1}] = \prod_{1 \le i < j \le n} (\theta_j - \theta_i)^2$, where $\theta_i = \sigma_i(\theta)$.

Properties of norm and trace

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta)).$$

Proof. $\Delta[1, \theta, \ldots, \theta^{n-1}] = \prod_{1 \le i < j \le n} (\theta_j - \theta_i)^2$, where $\theta_i = \sigma_i(\theta)$.

For each $j = 1, \ldots, n$,

$$p(x) = \prod_{i=1}^{n} (x - \theta_i) \Rightarrow$$

Properties of norm and trace

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta)).$$

Proof. $\Delta[1, \theta, \ldots, \theta^{n-1}] = \prod_{1 \le i < j \le n} (\theta_j - \theta_i)^2$, where $\theta_i = \sigma_i(\theta)$.

For each $j = 1, \ldots, n$,

$$p(x) = \prod_{i=1}^{n} (x - \theta_i) \Rightarrow p'(x) = \sum_{k=1}^{n} \prod_{i : i \neq k} (x - \theta_i)$$

Properties of norm and trace

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta)).$$

Proof. $\Delta[1, \theta, \ldots, \theta^{n-1}] = \prod_{1 \le i < j \le n} (\theta_j - \theta_i)^2$, where $\theta_i = \sigma_i(\theta)$.

For each $j = 1, \ldots, n$,

$$p(x) = \prod_{i=1}^{n} (x - \theta_i) \Rightarrow p'(x) = \sum_{k=1}^{n} \prod_{i : i \neq k} (x - \theta_i)$$

$$\Rightarrow p'(\theta_j) = \prod_{i : i \neq j} (\theta_j - \theta_i).$$

Properties of norm and trace

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta)).$$

Proof. $\Delta[1, \theta, \ldots, \theta^{n-1}] = \prod_{1 \le i < j \le n} (\theta_j - \theta_i)^2$, where $\theta_i = \sigma_i(\theta)$.

For each $j = 1, \ldots, n$,

$$p(x) = \prod_{i=1}^{n} (x - \theta_i) \Rightarrow p'(x) = \sum_{k=1}^{n} \prod_{i : i \neq k} (x - \theta_i)$$

$$\Rightarrow p'(\theta_j) = \prod_{i : i \neq j} (\theta_j - \theta_i).$$

So

$$N(p'(\theta)) = \prod_{j=1}^{n} \sigma_j(p'(\theta))$$

Properties of norm and trace

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta)).$$

Proof. $\Delta[1, \theta, \ldots, \theta^{n-1}] = \prod_{1 \le i < j \le n} (\theta_j - \theta_i)^2$, where $\theta_i = \sigma_i(\theta)$.

For each $j = 1, \ldots, n$,

$$p(x) = \prod_{i=1}^{n} (x - \theta_i) \Rightarrow p'(x) = \sum_{k=1}^{n} \prod_{i : i \neq k} (x - \theta_i)$$

$$\Rightarrow p'(\theta_j) = \prod_{i : i \neq j} (\theta_j - \theta_i).$$

So

$$N(p'(\theta)) = \prod_{j=1}^{n} \sigma_j(p'(\theta)) = \prod_{j=1}^{n} p'(\theta_j)$$

Properties of norm and trace

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta)).$$

Proof. $\Delta[1, \theta, \ldots, \theta^{n-1}] = \prod_{1 \le i < j \le n} (\theta_j - \theta_i)^2$, where $\theta_i = \sigma_i(\theta)$.

For each $j = 1, \ldots, n$,

$$p(x) = \prod_{i=1}^{n} (x - \theta_i) \Rightarrow p'(x) = \sum_{k=1}^{n} \prod_{i : i \neq k} (x - \theta_i)$$

$$\Rightarrow p'(\theta_j) = \prod_{i : i \neq j} (\theta_j - \theta_i).$$

So

$$N(p'(\theta)) = \prod_{j=1}^{n} \sigma_j(p'(\theta)) = \prod_{j=1}^{n} p'(\theta_j) = \prod_{\substack{i,j \\ i \neq j}}^{n} (\theta_j - \theta_i).$$

Properties of norm and trace

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta)).$$

Properties of norm and trace

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta)).$$

Proof continued.

$$N(p'(\theta)) = \prod_{j=1}^{n} \sigma_j(p'(\theta)) = \prod_{j=1}^{n} p'(\theta_j) = \prod_{\substack{i,j=1 \\ i \neq j}}^{n} (\theta_j - \theta_i).$$

Properties of norm and trace

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta)).$$

Proof continued.

$$N(p'(\theta)) = \prod_{j=1}^{n} \sigma_j(p'(\theta)) = \prod_{j=1}^{n} p'(\theta_j) = \prod_{\substack{i,j=1 \\ i \neq j}}^{n} (\theta_j - \theta_i).$$

On the right-hand side, each $\theta_j - \theta_i$ appears twice: once when $j < i$, and once when $j > i$.

Properties of norm and trace

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta)).$$

Proof continued.

$$N(p'(\theta)) = \prod_{j=1}^{n} \sigma_j(p'(\theta)) = \prod_{j=1}^{n} p'(\theta_j) = \prod_{\substack{i,j=1 \\ i \neq j}}^{n} (\theta_j - \theta_i).$$

On the right-hand side, each $\theta_j - \theta_i$ appears twice: once when $j < i$, and once when $j > i$. Grouping these two occurrences together gives

$$N(p'(\theta)) = \prod_{1 \leq i < j \leq n} \left(-(\theta_j - \theta_i)^2 \right)$$

Properties of norm and trace

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta)).$$

Proof continued.

$$N(p'(\theta)) = \prod_{j=1}^{n} \sigma_j(p'(\theta)) = \prod_{j=1}^{n} p'(\theta_j) = \prod_{\substack{i,j=1 \\ i \neq j}}^{n} (\theta_j - \theta_i).$$

On the right-hand side, each $\theta_j - \theta_i$ appears twice: once when $j < i$, and once when $j > i$. Grouping these two occurrences together gives

$$N(p'(\theta)) = \prod_{1 \leq i < j \leq n}^{n} \left(-(\theta_j - \theta_i)^2\right) = (-1)^{\binom{n}{2}} \prod_{1 \leq i < j \leq n} (\theta_j - \theta_i)^2,$$

Properties of norm and trace

6. Let p be the minimal polynomial for θ. Then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta)).$$

Proof continued.

$$N(p'(\theta)) = \prod_{j=1}^{n} \sigma_j(p'(\theta)) = \prod_{j=1}^{n} p'(\theta_j) = \prod_{\substack{i,j=1 \\ i \neq j}}^{n} (\theta_j - \theta_i).$$

On the right-hand side, each $\theta_j - \theta_i$ appears twice: once when $j < i$, and once when $j > i$. Grouping these two occurrences together gives

$$N(p'(\theta)) = \prod_{1 \leq i < j \leq n}^{n} \left(-(\theta_j - \theta_i)^2\right) = (-1)^{\binom{n}{2}} \prod_{1 \leq i < j \leq n} (\theta_j - \theta_i)^2,$$

where $\binom{n}{2} = n(n-1)/2$ is the number of pairs i, j with $i < j$. $\square$

Properties of norm and trace

7. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K.

Properties of norm and trace

7. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K. Let $S = (T(\alpha_i \alpha_j))$.

Properties of norm and trace

7. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K. Let $S = (T(\alpha_i\alpha_j))$. Then $\Delta[\alpha_1, \ldots, \alpha_n] = \det S = \det((T(\alpha_i\alpha_j)))$.

Properties of norm and trace

7. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K. Let $S = (T(\alpha_i\alpha_j))$. Then $\Delta[\alpha_1, \ldots, \alpha_n] = \det S = \det((T(\alpha_i\alpha_j)))$.

Proof.

Properties of norm and trace

7. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K. Let $S = (T(\alpha_i\alpha_j))$. Then $\Delta[\alpha_1, \ldots, \alpha_n] = \det S = \det((T(\alpha_i\alpha_j)))$.

Proof.

$$S_{ij} = T(\alpha_i\alpha_j)$$

Properties of norm and trace

7. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K. Let $S = (T(\alpha_i\alpha_j))$. Then $\Delta[\alpha_1, \ldots, \alpha_n] = \det S = \det((T(\alpha_i\alpha_j)))$.

Proof.

$$S_{ij} = T(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j)$$

Properties of norm and trace

7. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K. Let $S = (T(\alpha_i\alpha_j))$. Then $\Delta[\alpha_1, \ldots, \alpha_n] = \det S = \det((T(\alpha_i\alpha_j)))$.

Proof.

$$S_{ij} = T(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j).$$

To compute the discriminant, let $A = (\sigma_i(\alpha_j))$.

Properties of norm and trace

7. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K. Let $S = (T(\alpha_i\alpha_j))$. Then $\Delta[\alpha_1, \ldots, \alpha_n] = \det S = \det((T(\alpha_i\alpha_j)))$.

Proof.

$$S_{ij} = T(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j).$$

To compute the discriminant, let $A = (\sigma_i(\alpha_j))$. Then

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det A)^2 = \det(A)\det(A) = \det(A^t)\det(A) = \det(A^tA).$$

Properties of norm and trace

7. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K. Let $S = (T(\alpha_i\alpha_j))$. Then $\Delta[\alpha_1, \ldots, \alpha_n] = \det S = \det((T(\alpha_i\alpha_j)))$.

Proof.

$$S_{ij} = T(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j).$$

To compute the discriminant, let $A = (\sigma_i(\alpha_j))$. Then

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det A)^2 = \det(A)\det(A) = \det(A^t)\det(A) = \det(A^tA).$$

Check that $A^tA = S$. □