Math 361

February 15, 2023

Quiz

Let K be a number field.

1. Let K be a number field. How would you describe all of the field embeddings $K \to \mathbb{C}$ using the primitive element theorem and minimal polynomials?
2. Let $(\alpha_1, \ldots, \alpha_n)$ be a $\mathbb{Q}$-basis for K. Define the discriminant, $\Delta[\alpha_1, \ldots, \alpha_n]$.

Announce math talk

Announce math talk!

Leftover

See the slides from last time.

Today

- Introduction to cyclotomic fields.

Today

- Introduction to cyclotomic fields.
- Theorem for degree and basis for ring of integers.

Today

- Introduction to cyclotomic fields.
- Theorem for degree and basis for ring of integers.
- Begin proof in special case (primes).

Today

- Introduction to cyclotomic fields.
- Theorem for degree and basis for ring of integers.
- Begin proof in special case (primes).
- Eisenstein's criterion.

Today

- Introduction to cyclotomic fields.
- Theorem for degree and basis for ring of integers.
- Begin proof in special case (primes).
- Eisenstein's criterion.
- Some useful norm and trace calculations.

Cyclotomic fields

Primitive m-th root of unity:

$$\zeta_m = e^{2\pi i/m} = \cos(2\pi/m) + i\sin(2\pi/m),$$

Cyclotomic fields

Primitive m-th root of unity:

$$\zeta_m = e^{2\pi i/m} = \cos(2\pi/m) + i\sin(2\pi/m),$$

The powers of ζ_m are the *m-th roots of unity*:

$$x^m - 1 = \prod_{k=1}^{m} (x - \zeta^k).$$

Cyclotomic fields

Primitive m-th root of unity:

$$\zeta_m = e^{2\pi i/m} = \cos(2\pi/m) + i\sin(2\pi/m),$$

The powers of ζ_m are the *m-th roots of unity*:

$$x^m - 1 = \prod_{k=1}^{m} (x - \zeta^k).$$

Since ζ_m satisfies a monic polynomial with integer coefficients, it is an algebraic integer.

Cyclotomic fields

Primitive m-th root of unity:

$$\zeta_m = e^{2\pi i/m} = \cos(2\pi/m) + i\sin(2\pi/m),$$

The powers of ζ_m are the *m-th roots of unity*:

$$x^m - 1 = \prod_{k=1}^{m} (x - \zeta^k).$$

Since ζ_m satisfies a monic polynomial with integer coefficients, it is an algebraic integer.

A *cyclotomic field* is a number field of the form $K = \mathbb{Q}(\zeta_m)$.

Examples

1. **Case $m = 2$.** We have $\zeta_2 = -1$ and $K = \mathbb{Q}$.

Examples

1. **Case** $m = 2$**.** We have $\zeta_2 = -1$ and $K = \mathbb{Q}$.
2. **Case** $m = 3$**.** We have

$$\zeta_3 = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{1}{2} + i\frac{\sqrt{3}}{2} = \frac{1 + i\sqrt{3}}{2}$$

$$x^3 - 1 = (x - 1)(x^2 + x + 1),$$

Examples

1. **Case** $m = 2$**.** We have $\zeta_2 = -1$ and $K = \mathbb{Q}$.
2. **Case** $m = 3$**.** We have

$$\zeta_3 = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{1}{2} + i\frac{\sqrt{3}}{2} = \frac{1 + i\sqrt{3}}{2}$$

$$x^3 - 1 = (x - 1)(x^2 + x + 1),$$

and the minimal polynomial for ζ_3 is $x^2 + x + 1$.

Examples

1. **Case** $m = 2$**.** We have $\zeta_2 = -1$ and $K = \mathbb{Q}$.
2. **Case** $m = 3$**.** We have

$$\zeta_3 = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{1}{2} + i\frac{\sqrt{3}}{2} = \frac{1 + i\sqrt{3}}{2}$$

$$x^3 - 1 = (x - 1)(x^2 + x + 1),$$

and the minimal polynomial for ζ_3 is $x^2 + x + 1$. So $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$.

Examples

1. **Case** $m = 2$**.** We have $\zeta_2 = -1$ and $K = \mathbb{Q}$.
2. **Case** $m = 3$**.** We have

$$\zeta_3 = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{1}{2} + i\frac{\sqrt{3}}{2} = \frac{1 + i\sqrt{3}}{2}$$

$$x^3 - 1 = (x - 1)(x^2 + x + 1),$$

and the minimal polynomial for ζ_3 is $x^2 + x + 1$. So $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$.

3. **Case** $m = 4$**.** We have

$$\zeta_4 = \cos(2\pi/4) + i\sin(2\pi/4) = i$$

$$x^4 - 1$$

Examples

1. **Case** $m = 2$**.** We have $\zeta_2 = -1$ and $K = \mathbb{Q}$.
2. **Case** $m = 3$**.** We have

$$\zeta_3 = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{1}{2} + i\frac{\sqrt{3}}{2} = \frac{1 + i\sqrt{3}}{2}$$

$$x^3 - 1 = (x - 1)(x^2 + x + 1),$$

and the minimal polynomial for ζ_3 is $x^2 + x + 1$. So $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$.

3. **Case** $m = 4$**.** We have

$$\zeta_4 = \cos(2\pi/4) + i\sin(2\pi/4) = i$$

$$x^4 - 1 = (x^2 - 1)(x^2 + 1)$$

Examples

1. **Case** $m = 2$**.** We have $\zeta_2 = -1$ and $K = \mathbb{Q}$.
2. **Case** $m = 3$**.** We have

$$\zeta_3 = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{1}{2} + i\frac{\sqrt{3}}{2} = \frac{1 + i\sqrt{3}}{2}$$

$$x^3 - 1 = (x-1)(x^2 + x + 1),$$

and the minimal polynomial for ζ_3 is $x^2 + x + 1$. So $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$.

3. **Case** $m = 4$**.** We have

$$\zeta_4 = \cos(2\pi/4) + i\sin(2\pi/4) = i$$

$$x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x-1)(x+1)(x^2 + 1)$$

Examples

1. **Case** $m = 2$**.** We have $\zeta_2 = -1$ and $K = \mathbb{Q}$.
2. **Case** $m = 3$**.** We have

$$\zeta_3 = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{1}{2} + i\frac{\sqrt{3}}{2} = \frac{1 + i\sqrt{3}}{2}$$

$$x^3 - 1 = (x-1)(x^2 + x + 1),$$

and the minimal polynomial for ζ_3 is $x^2 + x + 1$. So $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$.

3. **Case** $m = 4$**.** We have

$$\zeta_4 = \cos(2\pi/4) + i\sin(2\pi/4) = i$$

$$x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x-1)(x+1)(x^2 + 1)$$

and the minimal polynomial for ζ_4 is $x^2 + 1$.

Examples

1. **Case** $m = 2$**.** We have $\zeta_2 = -1$ and $K = \mathbb{Q}$.
2. **Case** $m = 3$**.** We have

$$\zeta_3 = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{1}{2} + i\frac{\sqrt{3}}{2} = \frac{1 + i\sqrt{3}}{2}$$

$$x^3 - 1 = (x-1)(x^2 + x + 1),$$

and the minimal polynomial for ζ_3 is $x^2 + x + 1$. So $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$.

3. **Case** $m = 4$**.** We have

$$\zeta_4 = \cos(2\pi/4) + i\sin(2\pi/4) = i$$

$$x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x-1)(x+1)(x^2 + 1)$$

and the minimal polynomial for ζ_4 is $x^2 + 1$. So $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$, also.

Theorem

Theorem We have

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$$

where ϕ is the Euler totient function:

Theorem

Theorem We have

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$$

where ϕ is the Euler totient function:

$$\phi(m) = |\{a : 1 \leq a < m \text{ and } \gcd(a, m) = 1\}| = m \prod_{\substack{p|m \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

Theorem

Theorem We have

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$$

where ϕ is the Euler totient function:

$$\phi(m) = |\{a : 1 \leq a < m \text{ and } \gcd(a, m) = 1\}| = m \prod_{\substack{p|m \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

Further, $\mathfrak{O}_{\mathbb{Q}(\zeta_m)}$ has integral basis $1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{\phi(m)-1}$,

Theorem

Theorem We have

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$$

where ϕ is the Euler totient function:

$$\phi(m) = |\{a : 1 \leq a < m \text{ and } \gcd(a, m) = 1\}| = m \prod_{\substack{p|m \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

Further, $\mathfrak{O}_{\mathbb{Q}(\zeta_m)}$ has integral basis $1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{\phi(m)-1}$, i.e., $\mathfrak{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$.

Theorem

Theorem We have

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$$

where ϕ is the Euler totient function:

$$\phi(m) = |\{a : 1 \leq a < m \text{ and } \gcd(a, m) = 1\}| = m \prod_{\substack{p|m \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

Further, $\mathfrak{O}_{\mathbb{Q}(\zeta_m)}$ has integral basis $1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{\phi(m)-1}$, i.e., $\mathfrak{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$.

Example If $m = 4$, then $\phi(4) = 2 = 4\left(1 - \frac{1}{2}\right)$.

Theorem

Theorem We have

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$$

where ϕ is the Euler totient function:

$$\phi(m) = |\{a : 1 \leq a < m \text{ and } \gcd(a, m) = 1\}| = m \prod_{\substack{p \mid m \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

Further, $\mathfrak{O}_{\mathbb{Q}(\zeta_m)}$ has integral basis $1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{\phi(m)-1}$, i.e., $\mathfrak{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$.

Example If $m = 4$, then $\phi(4) = 2 = 4\left(1 - \frac{1}{2}\right)$. The ring of integers in $\mathbb{Q}(i)$ is $\mathbb{Z}[i] = \mathrm{Span}_{\mathbb{Z}}\{1, i\}$.

Goal

Let p be an odd prime, and let $\zeta = \zeta_p$.

Goal

Let p be an odd prime, and let $\zeta = \zeta_p$. We have $\phi(p) =$

Goal

Let p be an odd prime, and let $\zeta = \zeta_p$. We have $\phi(p) = p - 1$.

Goal

Let p be an odd prime, and let $\zeta = \zeta_p$. We have $\phi(p) = p - 1$. Our goal is to prove the theorem for this case:

Goal

Let p be an odd prime, and let $\zeta = \zeta_p$. We have $\phi(p) = p - 1$. Our goal is to prove the theorem for this case:

Theorem. Let $K = \mathbb{Q}(\zeta)$. Then

- $[K : \mathbb{Q}] = p - 1$,

Goal

Let p be an odd prime, and let $\zeta = \zeta_p$. We have $\phi(p) = p - 1$. Our goal is to prove the theorem for this case:

Theorem. Let $K = \mathbb{Q}(\zeta)$. Then

- $[K : \mathbb{Q}] = p - 1$, and
- $\mathfrak{O}_K = \mathbb{Q}[\zeta] = \mathrm{Span}_{\mathbb{Z}}\{1, \zeta, \ldots, \zeta^{p-1}\}$.

Goal

Let p be an odd prime, and let $\zeta = \zeta_p$. We have $\phi(p) = p - 1$. Our goal is to prove the theorem for this case:

Theorem. Let $K = \mathbb{Q}(\zeta)$. Then

- $[K : \mathbb{Q}] = p - 1$, and
- $\mathfrak{O}_K = \mathbb{Q}[\zeta] = \mathrm{Span}_{\mathbb{Z}}\{1, \zeta, \ldots, \zeta^{p-1}\}$.

We will prove the first part today and the second on Friday.

Eisenstein's criterion

Theorem. Let

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Eisenstein's criterion

Theorem. Let

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Suppose there is a prime $q \in \mathbb{Z}$ such that

(i) $q | a_i$ for $i = 0, 1, \ldots, n-1$;

Eisenstein's criterion

Theorem. Let

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Suppose there is a prime $q \in \mathbb{Z}$ such that

(i) $q | a_i$ for $i = 0, 1, \ldots, n-1$; (ii) $q \nmid a_n$; and

Eisenstein's criterion

Theorem. Let

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Suppose there is a prime $q \in \mathbb{Z}$ such that

(i) $q | a_i$ for $i = 0, 1, \ldots, n-1$; (ii) $q \nmid a_n$; and (iii) $q^2 \nmid a_0$.

Eisenstein's criterion

Theorem. Let

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Suppose there is a prime $q \in \mathbb{Z}$ such that

(i) $q | a_i$ for $i = 0, 1, \ldots, n-1$; (ii) $q \nmid a_n$; and (iii) $q^2 \nmid a_0$.

Then up to a constant factor, f is irreducible in $\mathbb{Z}[x]$

Eisenstein's criterion

Theorem. Let

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Suppose there is a prime $q \in \mathbb{Z}$ such that

(i) $q | a_i$ for $i = 0, 1, \ldots, n-1$; (ii) $q \nmid a_n$; and (iii) $q^2 \nmid a_0$.

Then up to a constant factor, f is irreducible in $\mathbb{Z}[x]$ and, hence, f is irreducible in $\mathbb{Q}[x]$.

Minimal polynomial for ζ

Proposition. The minimal polynomial for ζ is $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Minimal polynomial for ζ

Proposition. The minimal polynomial for ζ is $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Proof. Since

$$x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1},$$

all of the p-th roots of unity except 1 are zeros of f.

Minimal polynomial for ζ

Proposition. The minimal polynomial for ζ is $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Proof. Since

$$x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1},$$

all of the p-th roots of unity except 1 are zeros of f.

It remains to show that f is irreducible over $\mathbb{Q}$.

Minimal polynomial for ζ

Proposition. The minimal polynomial for ζ is $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Proof. Since

$$x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1},$$

all of the p-th roots of unity except 1 are zeros of f.

It remains to show that f is irreducible over $\mathbb{Q}$.

It suffices to show $f(x + 1)$ is irreducible

Minimal polynomial for ζ

Proposition. The minimal polynomial for ζ is $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Proof. Since

$$x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1},$$

all of the p-th roots of unity except 1 are zeros of f.

It remains to show that f is irreducible over $\mathbb{Q}$.

It suffices to show $f(x+1)$ is irreducible ($f(x) = g(x)h(x)$ if and only if $f(x+1) = g(x+1)h(x+1)$).

Minimal polynomial for ζ

Proposition. The minimal polynomial for ζ is $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Proof. Since

$$x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1},$$

all of the p-th roots of unity except 1 are zeros of f.

It remains to show that f is irreducible over $\mathbb{Q}$.

It suffices to show $f(x+1)$ is irreducible ($f(x) = g(x)h(x)$ if and only if $f(x+1) = g(x+1)h(x+1)$).

Idea: apply Eisenstein's criterion to $f(x+1)$.

Minimal polynomial for ζ

Proposition. The minimal polynomial for ζ is $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Minimal polynomial for ζ

Proposition. The minimal polynomial for ζ is $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Proof continued.
We have

Minimal polynomial for ζ

Proposition. The minimal polynomial for ζ is $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Proof continued.
We have

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1}$$

Minimal polynomial for ζ

Proposition. The minimal polynomial for ζ is $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Proof continued.
We have

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1}$$

$$= \frac{x^p + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{1}x + 1 - 1}{x}$$

Minimal polynomial for ζ

Proposition. The minimal polynomial for ζ is $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Proof continued.
We have

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1}$$

$$= \frac{x^p + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{1}x + 1 - 1}{x}$$

$$= x^{p-1} + \binom{p}{p-1}x^{p-2} + \binom{p}{p-2}x^{p-3} + \cdots + \binom{p}{1}.$$

Minimal polynomial for ζ

Proposition. The minimal polynomial for ζ is $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Proof continued.
We have

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1}$$

$$= \frac{x^p + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{1}x + 1 - 1}{x}$$

$$= x^{p-1} + \binom{p}{p-1}x^{p-2} + \binom{p}{p-2}x^{p-3} + \cdots + \binom{p}{1}.$$

Eisenstein's criterion now applies. Note that $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is divisible by p for $1 \leq k \leq p-1$.

First part of theorem

Corollary. We have $[K : \mathbb{Q}] = p - 1$ and $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is a $\mathbb{Q}$-basis for K.

First part of theorem

Corollary. We have $[K : \mathbb{Q}] = p - 1$ and $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is a $\mathbb{Q}$-basis for K.

The second part of the theorem is to show that $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is also a $\mathbb{Z}$-basis for $\mathfrak{O}_K$.

First part of theorem

Corollary. We have $[K : \mathbb{Q}] = p - 1$ and $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is a $\mathbb{Q}$-basis for K.

The second part of the theorem is to show that $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is also a $\mathbb{Z}$-basis for $\mathfrak{O}_K$.

We will do that next time. For now, we will calculate some needed norms and traces.

Some norms and traces

The minimal polynomial for ζ factors as $f(x) = \prod_{i=1}^{p-1}(x - \zeta^i)$.

Some norms and traces

The minimal polynomial for ζ factors as $f(x) = \prod_{i=1}^{p-1}(x - \zeta^i)$.

So the embeddings of K are given by $\sigma_i(\zeta) = \zeta^i$ for $i = 1, \ldots, p-1$.

Some norms and traces

The minimal polynomial for ζ factors as $f(x) = \prod_{i=1}^{p-1}(x - \zeta^i)$.

So the embeddings of K are given by $\sigma_i(\zeta) = \zeta^i$ for $i = 1, \ldots, p-1$.

The field polynomial for ζ is its minimal polynomial:

$$f(x) = f_\zeta(x) = \prod_{i=1}^{p-1}(x - \sigma_i(\zeta)) =$$

Some norms and traces

The minimal polynomial for ζ factors as $f(x) = \prod_{i=1}^{p-1}(x - \zeta^i)$.

So the embeddings of K are given by $\sigma_i(\zeta) = \zeta^i$ for $i = 1, \ldots, p-1$.

The field polynomial for ζ is its minimal polynomial:

$$f(x) = f_\zeta(x) = \prod_{i=1}^{p-1}(x - \sigma_i(\zeta)) =$$

$$= x^{p-1} - (\underbrace{\sigma_1(\zeta) + \cdots + \sigma_{p-1}(\zeta)}_{T(\zeta)})x^{p-2} + \cdots + (-1)^{p-1}\underbrace{\sigma_1(\zeta)\cdots\sigma_{p-1}(\zeta)}_{N(\zeta)}$$

Some norms and traces

The minimal polynomial for ζ factors as $f(x) = \prod_{i=1}^{p-1}(x - \zeta^i)$.

So the embeddings of K are given by $\sigma_i(\zeta) = \zeta^i$ for $i = 1, \ldots, p-1$.

The field polynomial for ζ is its minimal polynomial:

$$f(x) = f_\zeta(x) = \prod_{i=1}^{p-1}(x - \sigma_i(\zeta)) =$$

$$= x^{p-1} - (\underbrace{\sigma_1(\zeta) + \cdots + \sigma_{p-1}(\zeta)}_{T(\zeta)})x^{p-2} + \cdots + (-1)^{p-1}\underbrace{\sigma_1(\zeta)\cdots\sigma_{p-1}(\zeta)}_{N(\zeta)}$$

But $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Some norms and traces

The minimal polynomial for ζ factors as $f(x) = \prod_{i=1}^{p-1}(x - \zeta^i)$.

So the embeddings of K are given by $\sigma_i(\zeta) = \zeta^i$ for $i = 1, \ldots, p-1$.

The field polynomial for ζ is its minimal polynomial:

$$f(x) = f_\zeta(x) = \prod_{i=1}^{p-1}(x - \sigma_i(\zeta)) =$$

$$= x^{p-1} - (\underbrace{\sigma_1(\zeta) + \cdots + \sigma_{p-1}(\zeta)}_{T(\zeta)})x^{p-2} + \cdots + (-1)^{p-1}\underbrace{\sigma_1(\zeta)\cdots\sigma_{p-1}(\zeta)}_{N(\zeta)}$$

But $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. So $T(\zeta) = -1$,

Some norms and traces

The minimal polynomial for ζ factors as $f(x) = \prod_{i=1}^{p-1}(x - \zeta^i)$.

So the embeddings of K are given by $\sigma_i(\zeta) = \zeta^i$ for $i = 1, \ldots, p-1$.

The field polynomial for ζ is its minimal polynomial:

$$f(x) = f_\zeta(x) = \prod_{i=1}^{p-1}(x - \sigma_i(\zeta)) =$$

$$= x^{p-1} - (\underbrace{\sigma_1(\zeta) + \cdots + \sigma_{p-1}(\zeta)}_{T(\zeta)})x^{p-2} + \cdots + (-1)^{p-1}\underbrace{\sigma_1(\zeta)\cdots\sigma_{p-1}(\zeta)}_{N(\zeta)}$$

But $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. So $T(\zeta) = -1$, and $N(\zeta) = 1$ since p is odd.

Some norms and traces

We have just seen that $N(\zeta) = 1$ and $T(\zeta) = -1$.

Some norms and traces

We have just seen that $N(\zeta) = 1$ and $T(\zeta) = -1$.

By multiplicativity, $N(\zeta^i) = 1$ for all i.

Some norms and traces

We have just seen that $N(\zeta) = 1$ and $T(\zeta) = -1$.

By multiplicativity, $N(\zeta^i) = 1$ for all i.

What about traces?

Some norms and traces

We have just seen that $N(\zeta) = 1$ and $T(\zeta) = -1$.

By multiplicativity, $N(\zeta^i) = 1$ for all i.

What about traces? First note if $1 \leq i < k \leq p-1$,

Some norms and traces

We have just seen that $N(\zeta) = 1$ and $T(\zeta) = -1$.

By multiplicativity, $N(\zeta^i) = 1$ for all i.

What about traces? First note if $1 \leq i < k \leq p-1$,

$$\sigma_i(\zeta^j) = \sigma_k(\zeta^j) \Longleftrightarrow \zeta^{ij} = \zeta^{kj}$$

Some norms and traces

We have just seen that $N(\zeta) = 1$ and $T(\zeta) = -1$.

By multiplicativity, $N(\zeta^i) = 1$ for all i.

What about traces? First note if $1 \leq i < k \leq p-1$,

$$\sigma_i(\zeta^j) = \sigma_k(\zeta^j) \iff \zeta^{ij} = \zeta^{kj} \iff \zeta^{(i-k)j} = 1$$

Some norms and traces

We have just seen that $N(\zeta) = 1$ and $T(\zeta) = -1$.

By multiplicativity, $N(\zeta^i) = 1$ for all i.

What about traces? First note if $1 \leq i < k \leq p-1$,

$$\begin{aligned} \sigma_i(\zeta^j) = \sigma_k(\zeta^j) &\iff \zeta^{ij} = \zeta^{kj} \iff \zeta^{(i-k)j} = 1 \\ &\iff (i-k)j = 0 \bmod p \end{aligned}$$

Some norms and traces

We have just seen that $N(\zeta) = 1$ and $T(\zeta) = -1$.

By multiplicativity, $N(\zeta^i) = 1$ for all i.

What about traces? First note if $1 \leq i < k \leq p-1$,

$$\sigma_i(\zeta^j) = \sigma_k(\zeta^j) \iff \zeta^{ij} = \zeta^{kj} \iff \zeta^{(i-k)j} = 1$$
$$\iff (i-k)j = 0 \bmod p \iff j = 0 \bmod p.$$

Some norms and traces

We have just seen that $N(\zeta) = 1$ and $T(\zeta) = -1$.

By multiplicativity, $N(\zeta^i) = 1$ for all i.

What about traces? First note if $1 \leq i < k \leq p-1$,

$$\sigma_i(\zeta^j) = \sigma_k(\zeta^j) \iff \zeta^{ij} = \zeta^{kj} \iff \zeta^{(i-k)j} = 1$$
$$\iff (i-k)j = 0 \bmod p \iff j = 0 \bmod p.$$

Therefore, for $j \neq 0 \bmod p$,

$$\{\sigma_1(\zeta^j), \ldots, \sigma_{p-1}(\zeta^j)\} = \{\zeta, \zeta^2, \ldots, \zeta^{p-1}\},$$

Some norms and traces

We have just seen that $N(\zeta) = 1$ and $T(\zeta) = -1$.

By multiplicativity, $N(\zeta^i) = 1$ for all i.

What about traces? First note if $1 \leq i < k \leq p-1$,

$$\sigma_i(\zeta^j) = \sigma_k(\zeta^j) \iff \zeta^{ij} = \zeta^{kj} \iff \zeta^{(i-k)j} = 1$$
$$\iff (i-k)j = 0 \bmod p \iff j = 0 \bmod p.$$

Therefore, for $j \neq 0 \bmod p$,

$$\{\sigma_1(\zeta^j), \ldots, \sigma_{p-1}(\zeta^j)\} = \{\zeta, \zeta^2, \ldots, \zeta^{p-1}\},$$

from which it follows that

$$T(\zeta^j) = \sum_{i=1}^{p-1} \sigma_i(\zeta^j) = \zeta + \zeta^2 + \cdots + \zeta^{p-1} = -1.$$

Some norms and traces

If $j = 0 \bmod p$, then $\zeta^j = 1$,

Some norms and traces

If $j = 0 \bmod p$, then $\zeta^j = 1$, and

$$T(1) = \sum_{i=1}^{p-1} \sigma_i(1) = \sum_{i=1}^{p-1} 1 = p - 1.$$

Some norms and traces

If $j = 0 \bmod p$, then $\zeta^j = 1$, and

$$T(1) = \sum_{i=1}^{p-1} \sigma_i(1) = \sum_{i=1}^{p-1} 1 = p - 1.$$

One last norm:

Some norms and traces

If $j = 0 \bmod p$, then $\zeta^j = 1$, and

$$T(1) = \sum_{i=1}^{p-1} \sigma_i(1) = \sum_{i=1}^{p-1} 1 = p - 1.$$

One last norm:

$$N(1-\zeta) = \prod_{i=1}^{p-1} \sigma_i(1-\zeta)$$

Some norms and traces

If $j = 0 \bmod p$, then $\zeta^j = 1$, and

$$T(1) = \sum_{i=1}^{p-1} \sigma_i(1) = \sum_{i=1}^{p-1} 1 = p - 1.$$

One last norm:

$$N(1-\zeta) = \prod_{i=1}^{p-1} \sigma_i(1-\zeta) = \prod_{i=1}^{p-1} (1-\zeta^i) = f(1)$$

Some norms and traces

If $j = 0 \bmod p$, then $\zeta^j = 1$, and

$$T(1) = \sum_{i=1}^{p-1} \sigma_i(1) = \sum_{i=1}^{p-1} 1 = p - 1.$$

One last norm:

$$N(1-\zeta) = \prod_{i=1}^{p-1} \sigma_i(1-\zeta) = \prod_{i=1}^{p-1} (1-\zeta^i) = f(1) = \underbrace{1 + \cdots + 1}_{p \text{ times}} = p.$$

Some norms and traces

Summary:

Let $\zeta = e^{2\pi i/p}$. Then

$$N(\zeta^j) = 1 \qquad \text{for all } i \in \mathbb{Z}$$
$$N(1-\zeta) = p$$

and

$$T(\zeta^j) = \begin{cases} -1 & \text{if } j \neq 0 \bmod p \\ p-1 & \text{if } j = 0 \bmod p. \end{cases}$$

A useful lemma

Given $\alpha \in K = \mathfrak{O}_K$, write

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$$

for some unique $a_i \in \mathbb{Q}$. (Why is this possible?)

A useful lemma

Given $\alpha \in K = \mathfrak{O}_K$, write

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$$

for some unique $a_i \in \mathbb{Q}$. (Why is this possible?)

Lemma. For $0 \leq k \leq p-2$,

$$T(\alpha\zeta^{-k} - \alpha\zeta) = pa_k \in \mathbb{Z}.$$

A useful lemma

Given $\alpha \in K = \mathfrak{O}_K$, write

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$$

for some unique $a_i \in \mathbb{Q}$. (Why is this possible?)

Lemma. For $0 \leq k \leq p-2$,

$$T(\alpha\zeta^{-k} - \alpha\zeta) = pa_k \in \mathbb{Z}.$$

Proof. First step: why is $T(\alpha\zeta^{-k} - \alpha\zeta) \in \mathbb{Z}$?

A useful lemma

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \in \mathfrak{O}_K, \quad a_i \in \mathbb{Q}$$

Lemma. For $0 \leq k \leq p-2$,

$$T(\alpha\zeta^{-k} - \alpha\zeta) = pa_k \in \mathbb{Z}.$$

A useful lemma

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \in \mathfrak{O}_K, \quad a_i \in \mathbb{Q}$$

Lemma. For $0 \leq k \leq p-2$,

$$T(\alpha\zeta^{-k} - \alpha\zeta) = pa_k \in \mathbb{Z}.$$

Proof continued. We then calculate $T(\alpha\zeta^{-k} - \alpha\zeta)$

A useful lemma

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \in \mathfrak{O}_K, \quad a_i \in \mathbb{Q}$$

Lemma. For $0 \leq k \leq p-2$,

$$T(\alpha\zeta^{-k} - \alpha\zeta) = pa_k \in \mathbb{Z}.$$

Proof continued. We then calculate $T(\alpha\zeta^{-k} - \alpha\zeta)$

$$= T(\alpha\zeta^{-k}) - T(\alpha\zeta)$$

□

A useful lemma

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \in \mathfrak{O}_K, \quad a_i \in \mathbb{Q}$$

Lemma. For $0 \leq k \leq p-2$,

$$T(\alpha\zeta^{-k} - \alpha\zeta) = pa_k \in \mathbb{Z}.$$

Proof continued. We then calculate $T(\alpha\zeta^{-k} - \alpha\zeta)$

$$\begin{aligned}
&= T(\alpha\zeta^{-k}) - T(\alpha\zeta) \\
&= T(a_0\zeta^{-k} + a_1\zeta^{-k+1} + \cdots + a_k + \cdots + a_{p-2}\zeta^{-k+p-2}) \\
&\quad - T(a_0\zeta + a_1\zeta^2 + \cdots + a_{p-2}\zeta^{p-1})
\end{aligned}$$

□

A useful lemma

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \in \mathfrak{O}_K, \quad a_i \in \mathbb{Q}$$

Lemma. For $0 \leq k \leq p-2$,

$$T(\alpha\zeta^{-k} - \alpha\zeta) = pa_k \in \mathbb{Z}.$$

Proof continued. We then calculate $T(\alpha\zeta^{-k} - \alpha\zeta)$

$$\begin{aligned}
&= T(\alpha\zeta^{-k}) - T(\alpha\zeta) \\
&= T(a_0\zeta^{-k} + a_1\zeta^{-k+1} + \cdots + a_k + \cdots + a_{p-2}\zeta^{-k+p-2}) \\
&\quad - T(a_0\zeta + a_1\zeta^2 + \cdots + a_{p-2}\zeta^{p-1}) \\
&= -a_0 - a_1 - \cdots - a_{k-1} + (p-1)a_k - a_{k+1} - \cdots - a_{p-2} \\
&\quad - (-a_0 - a_1 - \cdots - a_{p-2})
\end{aligned}$$

□

A useful lemma

$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \in \mathfrak{O}_K, \quad a_i \in \mathbb{Q}$

Lemma. For $0 \leq k \leq p-2$,

$$T(\alpha\zeta^{-k} - \alpha\zeta) = pa_k \in \mathbb{Z}.$$

Proof continued. We then calculate $T(\alpha\zeta^{-k} - \alpha\zeta)$

$$\begin{aligned}
&= T(\alpha\zeta^{-k}) - T(\alpha\zeta) \\
&= T(a_0\zeta^{-k} + a_1\zeta^{-k+1} + \cdots + a_k + \cdots + a_{p-2}\zeta^{-k+p-2}) \\
&\quad - T(a_0\zeta + a_1\zeta^2 + \cdots + a_{p-2}\zeta^{p-1}) \\
&= -a_0 - a_1 - \cdots - a_{k-1} + (p-1)a_k - a_{k+1} - \cdots - a_{p-2} \\
&\quad - (-a_0 - a_1 - \cdots - a_{p-2}) \\
&= pa_k.
\end{aligned}$$

□