Math-123: The primitive element theorem, Galois group of cyclotomic extensions

Sebastien Vasey

Harvard University

April 15, 2020

Announcements

- The final exam will be a 48 hours "take home" and will be published on the last day of class (April 29).

Announcements

- The final exam will be a 48 hours “take home” and will be published on the last day of class (April 29).
- A sample exam, and more information, is on the course website.

Announcements

- The final exam will be a 48 hours “take home” and will be published on the last day of class (April 29).
- A sample exam, and more information, is on the course website.
- Assignment 11 will be the last assignment of the semester.

The primitive element theorem

Recall: an extension K/F is *simple* if $K = F(\theta)$ for some θ. We call θ a *primitive element* for K.

The primitive element theorem

Recall: an extension K/F is *simple* if $K = F(\theta)$ for some θ. We call θ a *primitive element* for K.

For example, $\mathbb{Q}(\sqrt{2})$ is simple and $\sqrt{2}$ is a primitive element.

The primitive element theorem

Recall: an extension K/F is *simple* if $K = F(\theta)$ for some θ. We call θ a *primitive element* for K.

For example, $\mathbb{Q}(\sqrt{2})$ is simple and $\sqrt{2}$ is a primitive element.

A less trivial example: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is in fact simple: $\theta = \sqrt{2} + \sqrt{3}$ is a primitive element (seen in assignments).

The primitive element theorem

Recall: an extension K/F is *simple* if $K = F(\theta)$ for some θ. We call θ a *primitive element* for K.

For example, $\mathbb{Q}(\sqrt{2})$ is simple and $\sqrt{2}$ is a primitive element.

A less trivial example: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is in fact simple: $\theta = \sqrt{2} + \sqrt{3}$ is a primitive element (seen in assignments).

Question: When is a finite extension K/F simple?

The primitive element theorem

Recall: an extension K/F is *simple* if $K = F(\theta)$ for some θ. We call θ a *primitive element* for K.

For example, $\mathbb{Q}(\sqrt{2})$ is simple and $\sqrt{2}$ is a primitive element.

A less trivial example: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is in fact simple: $\theta = \sqrt{2} + \sqrt{3}$ is a primitive element (seen in assignments).

Question: When is a finite extension K/F simple?

Theorem (Primitive element theorem)

If K/F is finite and separable, then K/F is simple.

The primitive element theorem

Recall: an extension K/F is *simple* if $K = F(\theta)$ for some θ. We call θ a *primitive element* for K.

For example, $\mathbb{Q}(\sqrt{2})$ is simple and $\sqrt{2}$ is a primitive element.

A less trivial example: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is in fact simple: $\theta = \sqrt{2} + \sqrt{3}$ is a primitive element (seen in assignments).

Question: When is a finite extension K/F simple?

Theorem (Primitive element theorem)

If K/F is finite and separable, then K/F is simple.

Recall that an extension K/F is *separable* if every element of K is the root of a separable polynomial in $F[x]$. In characteristic zero (more generally for perfect fields F), any finite extension is separable.

Lemma (Key lemma)

Let K/F be a finite extension. Then K/F is simple if and only if there exists only finitely-many subfields of K containing F.

Lemma (Key lemma)

Let K/F be a finite extension. Then K/F is simple if and only if there exists only finitely-many subfields of K containing F.

Proof of $\Rightarrow$: Assume $K = F(\theta)$. Let E be a subfield of K containing F.

Lemma (Key lemma)

Let K/F be a finite extension. Then K/F is simple if and only if there exists only finitely-many subfields of K containing F.

Proof of $\Rightarrow$: Assume $K = F(\theta)$. Let E be a subfield of K containing F.

Let $f(x) \in F[x]$ be the minimal poly of θ, let $g(x) \in E[x]$ be the minimal poly of θ over E.

Lemma (Key lemma)

Let K/F be a finite extension. Then K/F is simple if and only if there exists only finitely-many subfields of K containing F.

Proof of $\Rightarrow$: Assume $K = F(\theta)$. Let E be a subfield of K containing F.

Let $f(x) \in F[x]$ be the minimal poly of θ, let $g(x) \in E[x]$ be the minimal poly of θ over E.

We have that g divides f (in $E[x]$).

Lemma (Key lemma)

Let K/F be a finite extension. Then K/F is simple if and only if there exists only finitely-many subfields of K containing F.

Proof of $\Rightarrow$: Assume $K = F(\theta)$. Let E be a subfield of K containing F.

Let $f(x) \in F[x]$ be the minimal poly of θ, let $g(x) \in E[x]$ be the minimal poly of θ over E.

We have that g divides f (in $E[x]$).

Let $E' \subseteq E$ be the subfield generated by the coefficients of $g(x)$.

Lemma (Key lemma)

Let K/F be a finite extension. Then K/F is simple if and only if there exists only finitely-many subfields of K containing F.

Proof of $\Rightarrow$: Assume $K = F(\theta)$. Let E be a subfield of K containing F.

Let $f(x) \in F[x]$ be the minimal poly of θ, let $g(x) \in E[x]$ be the minimal poly of θ over E.

We have that g divides f (in $E[x]$).

Let $E' \subseteq E$ be the subfield generated by the coefficients of $g(x)$.

The minimal poly of θ over E' is still $g(x)$, so $[E' : F]$ is the degree of g, which is equal to $[E : F]$. Thus $E = E'$.

Lemma (Key lemma)

Let K/F be a finite extension. Then K/F is simple if and only if there exists only finitely-many subfields of K containing F.

Proof of $\Rightarrow$: Assume $K = F(\theta)$. Let E be a subfield of K containing F.

Let $f(x) \in F[x]$ be the minimal poly of θ, let $g(x) \in E[x]$ be the minimal poly of θ over E.

We have that g divides f (in $E[x]$).

Let $E' \subseteq E$ be the subfield generated by the coefficients of $g(x)$.

The minimal poly of θ over E' is still $g(x)$, so $[E' : F]$ is the degree of g, which is equal to $[E : F]$. Thus $E = E'$.

E was arbitrary, so we have seen any subfield of K is generated by the coefficients of a monic divisor of $f(x)$ (in $K[x]$). There are only finitely-many such divisors. Thus K has finitely-many subfields.

Lemma (Key lemma)

Let K/F be a finite extension. Then K/F is simple if and only if there exists only finitely-many subfields of K containing F.

Proof of $\Leftarrow$: Assume K has finitely-many subfields containing F.

If F is a finite field, we saw F is a simple extension last time, so assume F is infinite.

Lemma (Key lemma)

Let K/F be a finite extension. Then K/F is simple if and only if there exists only finitely-many subfields of K containing F.

Proof of $\Leftarrow$: Assume K has finitely-many subfields containing F.

If F is a finite field, we saw F is a simple extension last time, so assume F is infinite.

Let $\alpha, \beta \in K$. We will show $F(\alpha, \beta)/F$ is simple. Induction then gives the result.

Lemma (Key lemma)

Let K/F be a finite extension. Then K/F is simple if and only if there exists only finitely-many subfields of K containing F.

Proof of $\Leftarrow$: Assume K has finitely-many subfields containing F.

If F is a finite field, we saw F is a simple extension last time, so assume F is infinite.

Let $\alpha, \beta \in K$. We will show $F(\alpha, \beta)/F$ is simple. Induction then gives the result.

Consider the subfields $F(\alpha + c\beta)$, $c \in F$. They are subfields of $F(\alpha, \beta)$.

Lemma (Key lemma)

Let K/F be a finite extension. Then K/F is simple if and only if there exists only finitely-many subfields of K containing F.

Proof of $\Leftarrow$: Assume K has finitely-many subfields containing F.

If F is a finite field, we saw F is a simple extension last time, so assume F is infinite.

Let $\alpha, \beta \in K$. We will show $F(\alpha, \beta)/F$ is simple. Induction then gives the result.

Consider the subfields $F(\alpha + c\beta)$, $c \in F$. They are subfields of $F(\alpha, \beta)$.

There are infinitely-many choices for c, finitely-many subfields, so for some $c \neq c' \in F$, $F(\alpha + c\beta) = F(\alpha + c'\beta)$.

Lemma (Key lemma)

Let K/F be a finite extension. Then K/F is simple if and only if there exists only finitely-many subfields of K containing F.

Proof of $\Leftarrow$: Assume K has finitely-many subfields containing F.

If F is a finite field, we saw F is a simple extension last time, so assume F is infinite.

Let $\alpha, \beta \in K$. We will show $F(\alpha, \beta)/F$ is simple. Induction then gives the result.

Consider the subfields $F(\alpha + c\beta)$, $c \in F$. They are subfields of $F(\alpha, \beta)$.

There are infinitely-many choices for c, finitely-many subfields, so for some $c \neq c' \in F$, $F(\alpha + c\beta) = F(\alpha + c'\beta)$.

Thus $\alpha + c\beta - (\alpha + c'\beta) \in F(\alpha + c\beta)$, so $(c - c')\beta \in F(\alpha + c\beta)$, so $\beta \in F(\alpha + c\beta)$, so $\alpha \in F(\alpha + c\beta)$, as desired.

Lemma (Key lemma)

Let K/F be a finite extension. Then K/F is simple if and only if there exists only finitely-many subfields of K containing F.

Theorem (Primitive element theorem)

If K/F is finite and separable, then K/F is simple.

Lemma (Key lemma)

Let K/F be a finite extension. Then K/F is simple if and only if there exists only finitely-many subfields of K containing F.

Theorem (Primitive element theorem)

If K/F is finite and separable, then K/F is simple.

Proof.

Let L/F be the Galois closure of K/F: the smallest Galois extension of F containing L (we saw last time it exists – we use separability here).

Lemma (Key lemma)

Let K/F be a finite extension. Then K/F is simple if and only if there exists only finitely-many subfields of K containing F.

Theorem (Primitive element theorem)

If K/F is finite and separable, then K/F is simple.

Proof.

Let L/F be the Galois closure of K/F: the smallest Galois extension of F containing L (we saw last time it exists – we use separability here).
Since L/F is finite, $\mathrm{Aut}(L/F)$ is finite, so by the Galois correspondence, L/F has finitely-many intermediate fields.

Lemma (Key lemma)

Let K/F be a finite extension. Then K/F is simple if and only if there exists only finitely-many subfields of K containing F.

Theorem (Primitive element theorem)

If K/F is finite and separable, then K/F is simple.

Proof.

Let L/F be the Galois closure of K/F: the smallest Galois extension of F containing L (we saw last time it exists – we use separability here).
Since L/F is finite, $\mathrm{Aut}(L/F)$ is finite, so by the Galois correspondence, L/F has finitely-many intermediate fields.
Thus also K/F has finitely-many intermediate fields. Apply the key lemma. □

Example: splitting field of $x^3 - 2$

Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$.

Example: splitting field of $x^3 - 2$

Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$.

By the primitive element theorem, K/F is simple. The proof shows a generator is of the form $\alpha_c = \sqrt[3]{2} + ce^{2\pi i/3}$, $c \in \mathbb{Q}$.

Example: splitting field of $x^3 - 2$

Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$.

By the primitive element theorem, K/F is simple. The proof shows a generator is of the form $\alpha_c = \sqrt[3]{2} + ce^{2\pi i/3}$, $c \in \mathbb{Q}$.

Which c works? We are in a Galois extension, so let's study what the Galois group does to α_c.

Example: splitting field of $x^3 - 2$

Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$.

By the primitive element theorem, K/F is simple. The proof shows a generator is of the form $\alpha_c = \sqrt[3]{2} + ce^{2\pi i/3}$, $c \in \mathbb{Q}$.

Which c works? We are in a Galois extension, so let's study what the Galois group does to α_c.

The Galois group has order 6. Say it is generated by σ (sending $\sqrt[3]{2}$ to $e^{2\pi i/3}\sqrt[3]{2}$, fixing $e^{2\pi i/3}$) and by τ (fixing $\sqrt[3]{2}$, sending $e^{2\pi i/3}$ to $e^{4\pi i/3}$).

Example: splitting field of $x^3 - 2$

Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$.

By the primitive element theorem, K/F is simple. The proof shows a generator is of the form $\alpha_c = \sqrt[3]{2} + ce^{2\pi i/3}$, $c \in \mathbb{Q}$.

Which c works? We are in a Galois extension, so let's study what the Galois group does to α_c.

The Galois group has order 6. Say it is generated by σ (sending $\sqrt[3]{2}$ to $e^{2\pi i/3}\sqrt[3]{2}$, fixing $e^{2\pi i/3}$) and by τ (fixing $\sqrt[3]{2}$, sending $e^{2\pi i/3}$ to $e^{4\pi i/3}$).

$\sigma(\alpha_c) = e^{2\pi i/3}\sqrt[3]{2} + ce^{2\pi i/3}$. This is different from α_c.

Example: splitting field of $x^3 - 2$

Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$.

By the primitive element theorem, K/F is simple. The proof shows a generator is of the form $\alpha_c = \sqrt[3]{2} + ce^{2\pi i/3}$, $c \in \mathbb{Q}$.

Which c works? We are in a Galois extension, so let's study what the Galois group does to α_c.

The Galois group has order 6. Say it is generated by σ (sending $\sqrt[3]{2}$ to $e^{2\pi i/3}\sqrt[3]{2}$, fixing $e^{2\pi i/3}$) and by τ (fixing $\sqrt[3]{2}$, sending $e^{2\pi i/3}$ to $e^{4\pi i/3}$).

$\sigma(\alpha_c) = e^{2\pi i/3}\sqrt[3]{2} + ce^{2\pi i/3}$. This is different from α_c.

$\tau(\alpha_c) = \sqrt[3]{2} + ce^{4\pi i/3}$. This is different from α_c if $c \neq 0$.

Example: splitting field of $x^3 - 2$

Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$.

By the primitive element theorem, K/F is simple. The proof shows a generator is of the form $\alpha_c = \sqrt[3]{2} + ce^{2\pi i/3}$, $c \in \mathbb{Q}$.

Which c works? We are in a Galois extension, so let's study what the Galois group does to α_c.

The Galois group has order 6. Say it is generated by σ (sending $\sqrt[3]{2}$ to $e^{2\pi i/3}\sqrt[3]{2}$, fixing $e^{2\pi i/3}$) and by τ (fixing $\sqrt[3]{2}$, sending $e^{2\pi i/3}$ to $e^{4\pi i/3}$).

$\sigma(\alpha_c) = e^{2\pi i/3}\sqrt[3]{2} + ce^{2\pi i/3}$. This is different from α_c.

$\tau(\alpha_c) = \sqrt[3]{2} + ce^{4\pi i/3}$. This is different from α_c if $c \neq 0$.

In general, if $c \neq 0$, α_c is not fixed by any non-identity automorphism.

Example: splitting field of $x^3 - 2$

Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$.

By the primitive element theorem, K/F is simple. The proof shows a generator is of the form $\alpha_c = \sqrt[3]{2} + ce^{2\pi i/3}$, $c \in \mathbb{Q}$.

Which c works? We are in a Galois extension, so let's study what the Galois group does to α_c.

The Galois group has order 6. Say it is generated by σ (sending $\sqrt[3]{2}$ to $e^{2\pi i/3}\sqrt[3]{2}$, fixing $e^{2\pi i/3}$) and by τ (fixing $\sqrt[3]{2}$, sending $e^{2\pi i/3}$ to $e^{4\pi i/3}$).

$\sigma(\alpha_c) = e^{2\pi i/3}\sqrt[3]{2} + ce^{2\pi i/3}$. This is different from α_c.

$\tau(\alpha_c) = \sqrt[3]{2} + ce^{4\pi i/3}$. This is different from α_c if $c \neq 0$.

In general, if $c \neq 0$, α_c is not fixed by any non-identity automorphism.

So if $c \neq 0$, the field $\mathbb{Q}(\alpha_c)$ corresponds to the group $\{1\}$, which has fixed field K, so α_c is a primitive element.

Cyclotomic extensions

Let $\zeta_n := e^{2\pi i/n}$. We have already determined that $\mathbb{Q}(\zeta_n)$ is an extension of degree $\phi(n)$. It is a Galois extension (splitting field of $x^n - 1$, which is separable). What is its Galois group?

Cyclotomic extensions

Let $\zeta_n := e^{2\pi i/n}$. We have already determined that $\mathbb{Q}(\zeta_n)$ is an extension of degree $\phi(n)$. It is a Galois extension (splitting field of $x^n - 1$, which is separable). What is its Galois group?

Theorem

The Galois group of $\mathbb{Q}(\zeta_n)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, the units of $\mathbb{Z}/n\mathbb{Z}$ under multiplication.

Cyclotomic extensions

Let $\zeta_n := e^{2\pi i/n}$. We have already determined that $\mathbb{Q}(\zeta_n)$ is an extension of degree $\phi(n)$. It is a Galois extension (splitting field of $x^n - 1$, which is separable). What is its Galois group?

Theorem

The Galois group of $\mathbb{Q}(\zeta_n)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, the units of $\mathbb{Z}/n\mathbb{Z}$ under multiplication.

Proof.

Any automorphism must send ζ_n to a primitive root of unity. There are $\phi(n)$-many automorphisms, so each possible such mapping gives an automorphism.

Cyclotomic extensions

Let $\zeta_n := e^{2\pi i/n}$. We have already determined that $\mathbb{Q}(\zeta_n)$ is an extension of degree $\phi(n)$. It is a Galois extension (splitting field of $x^n - 1$, which is separable). What is its Galois group?

Theorem

The Galois group of $\mathbb{Q}(\zeta_n)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, the units of $\mathbb{Z}/n\mathbb{Z}$ under multiplication.

Proof.

Any automorphism must send ζ_n to a primitive root of unity. There are $\phi(n)$-many automorphisms, so each possible such mapping gives an automorphism.

Let σ_a send ζ_n to ζ_n^a, a coprime to n.

Cyclotomic extensions

Let $\zeta_n := e^{2\pi i/n}$. We have already determined that $\mathbb{Q}(\zeta_n)$ is an extension of degree $\phi(n)$. It is a Galois extension (splitting field of $x^n - 1$, which is separable). What is its Galois group?

Theorem

The Galois group of $\mathbb{Q}(\zeta_n)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, the units of $\mathbb{Z}/n\mathbb{Z}$ under multiplication.

Proof.

Any automorphism must send ζ_n to a primitive root of unity. There are $\phi(n)$-many automorphisms, so each possible such mapping gives an automorphism.
Let σ_a send ζ_n to ζ_n^a, a coprime to n.
The map $a \mapsto \sigma_a$ is an isomorphism from $(\mathbb{Z}/n\mathbb{Z})^\times$ to $\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

□

Corollary

Let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, p_i distinct primes. Then the $\mathbb{Q}(\zeta_{p_i^{a_i}})$'s intersect only in $\mathbb{Q}$, and their composite is $\mathbb{Q}(\zeta_n)$.

Corollary

Let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, p_i distinct primes. Then the $\mathbb{Q}(\zeta_{p_i^{a_i}})$'s intersect only in $\mathbb{Q}$, and their composite is $\mathbb{Q}(\zeta_n)$. Thus:

$$\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathrm{Aut}(\mathbb{Q}(\zeta_{p_1^{a_1}})/\mathbb{Q}) \times ... \times \mathrm{Aut}(\mathbb{Q}(\zeta_{p_k^{a_k}})/\mathbb{Q})$$

Compare to the Chinese remainder theorem:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times$$

Corollary

Let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, p_i distinct primes. Then the $\mathbb{Q}(\zeta_{p_i^{a_i}})$'s intersect only in $\mathbb{Q}$, and their composite is $\mathbb{Q}(\zeta_n)$

Proof of Corollary: Note $\mathbb{Q}(\zeta_{p_i^{a_i}})$ is a subfield of $\mathbb{Q}(\zeta_n)$ ($p_i^{a_i}$ divides n).

Corollary

Let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, p_i distinct primes. Then the $\mathbb{Q}(\zeta_{p_i^{a_i}})$'s intersect only in $\mathbb{Q}$, and their composite is $\mathbb{Q}(\zeta_n)$

Proof of Corollary: Note $\mathbb{Q}(\zeta_{p_i^{a_i}})$ is a subfield of $\mathbb{Q}(\zeta_n)$ ($p_i^{a_i}$ divides n).

The composite of the $\mathbb{Q}(\zeta_{p_i^{a_i}})$'s contains the product $\zeta_{p_1^{a_1}} \zeta_{p_2^{a_2}} \dots \zeta_{p_k^{a_k}}$, which is a primitive nth root of unity (not a dth root of unity for any strict divisor d of n).

Corollary

Let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, p_i distinct primes. Then the $\mathbb{Q}(\zeta_{p_i^{a_i}})$'s intersect only in $\mathbb{Q}$, and their composite is $\mathbb{Q}(\zeta_n)$

Proof of Corollary: Note $\mathbb{Q}(\zeta_{p_i^{a_i}})$ is a subfield of $\mathbb{Q}(\zeta_n)$ ($p_i^{a_i}$ divides n).

The composite of the $\mathbb{Q}(\zeta_{p_i^{a_i}})$'s contains the product $\zeta_{p_1^{a_1}} \zeta_{p_2^{a_2}} \dots \zeta_{p_k^{a_k}}$, which is a primitive nth root of unity (not a dth root of unity for any strict divisor d of n).

Thus the composite is $\mathbb{Q}(\zeta_n)$.

Corollary

Let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, p_i distinct primes. Then the $\mathbb{Q}(\zeta_{p_i^{a_i}})$'s intersect only in $\mathbb{Q}$, and their composite is $\mathbb{Q}(\zeta_n)$

Proof of Corollary: Note $\mathbb{Q}(\zeta_{p_i^{a_i}})$ is a subfield of $\mathbb{Q}(\zeta_n)$ ($p_i^{a_i}$ divides n).

The composite of the $\mathbb{Q}(\zeta_{p_i^{a_i}})$'s contains the product $\zeta_{p_1^{a_1}} \zeta_{p_2^{a_2}} \dots \zeta_{p_k^{a_k}}$, which is a primitive nth root of unity (not a dth root of unity for any strict divisor d of n).

Thus the composite is $\mathbb{Q}(\zeta_n)$.

The degree of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $\phi(n)$, which is the product of $\phi(p_i^{a_i})$.

Corollary

Let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, p_i distinct primes. Then the $\mathbb{Q}(\zeta_{p_i^{a_i}})$'s intersect only in $\mathbb{Q}$, and their composite is $\mathbb{Q}(\zeta_n)$

Proof of Corollary: Note $\mathbb{Q}(\zeta_{p_i^{a_i}})$ is a subfield of $\mathbb{Q}(\zeta_n)$ ($p_i^{a_i}$ divides n).

The composite of the $\mathbb{Q}(\zeta_{p_i^{a_i}})$'s contains the product $\zeta_{p_1^{a_1}} \zeta_{p_2^{a_2}} \dots \zeta_{p_k^{a_k}}$, which is a primitive nth root of unity (not a dth root of unity for any strict divisor d of n).

Thus the composite is $\mathbb{Q}(\zeta_n)$.

The degree of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $\phi(n)$, which is the product of $\phi(p_i^{a_i})$.

By counting automorphisms (and using induction), we get that the intersection must be $\mathbb{Q}$.

Example: $\mathbb{Q}(\zeta_5)$

$\phi(5) = 4$, so the extension has degree 4.

Example: $\mathbb{Q}(\zeta_5)$

$\phi(5) = 4$, so the extension has degree 4.

The Galois group is $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$.

Example: $\mathbb{Q}(\zeta_5)$

$\phi(5) = 4$, so the extension has degree 4.

The Galois group is $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$.

So here we have an extension of degree 4 with a cyclic Galois group. A generator would be the automorphism σ sending ζ_5 to ζ_5^2.

Example: $\mathbb{Q}(\zeta_5)$

$\phi(5) = 4$, so the extension has degree 4.

The Galois group is $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$.

So here we have an extension of degree 4 with a cyclic Galois group. A generator would be the automorphism σ sending ζ_5 to ζ_5^2.

The only nontrivial subgroup is $\{1, \sigma^2\}$.

Example: $\mathbb{Q}(\zeta_5)$

$\phi(5) = 4$, so the extension has degree 4.

The Galois group is $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$.

So here we have an extension of degree 4 with a cyclic Galois group. A generator would be the automorphism σ sending ζ_5 to ζ_5^2.

The only nontrivial subgroup is $\{1, \sigma^2\}$. What is the fixed field?

Example: $\mathbb{Q}(\zeta_5)$

$\phi(5) = 4$, so the extension has degree 4.

The Galois group is $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$.

So here we have an extension of degree 4 with a cyclic Galois group. A generator would be the automorphism σ sending ζ_5 to ζ_5^2.

The only nontrivial subgroup is $\{1, \sigma^2\}$. What is the fixed field?

Note σ^2 sends ζ_5 to $\zeta_5^4 = \zeta_5^{-1}$. So $\alpha = \zeta_5 + \zeta_5^{-1}$ is a member of the fixed field.

Example: $\mathbb{Q}(\zeta_5)$

$\phi(5) = 4$, so the extension has degree 4.

The Galois group is $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$.

So here we have an extension of degree 4 with a cyclic Galois group. A generator would be the automorphism σ sending ζ_5 to ζ_5^2.

The only nontrivial subgroup is $\{1, \sigma^2\}$. What is the fixed field?

Note σ^2 sends ζ_5 to $\zeta_5^4 = \zeta_5^{-1}$. So $\alpha = \zeta_5 + \zeta_5^{-1}$ is a member of the fixed field.

Note $\alpha = 2\cos(2\pi/5)$. By the fundamental theorem, it must generate the fixed field: a quadratic extension.

Example: $\mathbb{Q}(\zeta_5)$

$\phi(5) = 4$, so the extension has degree 4.

The Galois group is $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$.

So here we have an extension of degree 4 with a cyclic Galois group. A generator would be the automorphism σ sending ζ_5 to ζ_5^2.

The only nontrivial subgroup is $\{1, \sigma^2\}$. What is the fixed field?

Note σ^2 sends ζ_5 to $\zeta_5^4 = \zeta_5^{-1}$. So $\alpha = \zeta_5 + \zeta_5^{-1}$ is a member of the fixed field.

Note $\alpha = 2\cos(2\pi/5)$. By the fundamental theorem, it must generate the fixed field: a quadratic extension.

Using that $x^4 + x^3 + x^2 + x + 1$ is the minimal polynomial of ζ_5, one can deduce that $\alpha^2 + \alpha - 1 = 0$, and solving we get that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$.

Example: $\mathbb{Q}(\zeta_5)$

$\phi(5) = 4$, so the extension has degree 4.

The Galois group is $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$.

So here we have an extension of degree 4 with a cyclic Galois group. A generator would be the automorphism σ sending ζ_5 to ζ_5^2.

The only nontrivial subgroup is $\{1, \sigma^2\}$. What is the fixed field?

Note σ^2 sends ζ_5 to $\zeta_5^4 = \zeta_5^{-1}$. So $\alpha = \zeta_5 + \zeta_5^{-1}$ is a member of the fixed field.

Note $\alpha = 2\cos(2\pi/5)$. By the fundamental theorem, it must generate the fixed field: a quadratic extension.

Using that $x^4 + x^3 + x^2 + x + 1$ is the minimal polynomial of ζ_5, one can deduce that $\alpha^2 + \alpha - 1 = 0$, and solving we get that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$.

[Another way: fun exercise: $\cos(\pi/5) = \frac{\sqrt{5}+1}{4}$*.]*.

Example: $\mathbb{Q}(\zeta_5)$

$\phi(5) = 4$, so the extension has degree 4.

The Galois group is $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$.

So here we have an extension of degree 4 with a cyclic Galois group. A generator would be the automorphism σ sending ζ_5 to ζ_5^2.

The only nontrivial subgroup is $\{1, \sigma^2\}$. What is the fixed field?

Note σ^2 sends ζ_5 to $\zeta_5^4 = \zeta_5^{-1}$. So $\alpha = \zeta_5 + \zeta_5^{-1}$ is a member of the fixed field.

Note $\alpha = 2\cos(2\pi/5)$. By the fundamental theorem, it must generate the fixed field: a quadratic extension.

Using that $x^4 + x^3 + x^2 + x + 1$ is the minimal polynomial of ζ_5, one can deduce that $\alpha^2 + \alpha - 1 = 0$, and solving we get that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$.

[Another way: fun exercise: $\cos(\pi/5) = \frac{\sqrt{5}+1}{4}$*.]*.

For more fun, see DF on computing the subfields of $\mathbb{Q}(\zeta_{13})$.

Definition

A field extension K/F is called an *abelian extension* if K/F is Galois and the Galois group is abelian.

Definition

A field extension K/F is called an *abelian extension* if K/F is Galois and the Galois group is abelian.

They are the "nicest" Galois extensions: all the intermediate extensions of abelian extensions are Galois and abelian.

Definition

A field extension K/F is called an *abelian extension* if K/F is Galois and the Galois group is abelian.

They are the "nicest" Galois extensions: all the intermediate extensions of abelian extensions are Galois and abelian.

We saw $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is always an abelian extension.

Definition

A field extension K/F is called an *abelian extension* if K/F is Galois and the Galois group is abelian.

They are the "nicest" Galois extensions: all the intermediate extensions of abelian extensions are Galois and abelian.

We saw $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is always an abelian extension.

Theorem

Any finite abelian group is the Galois group of an extension of $\mathbb{Q}$ (in fact of a subfield of a cyclotomic extension).

Theorem

Any finite abelian group is the Galois group of an extension of $\mathbb{Q}$ (in fact of a subfield of a cyclotomic extension).

Theorem

Any finite abelian group is the Galois group of an extension of $\mathbb{Q}$ (in fact of a subfield of a cyclotomic extension).

Proof: Let G be an abelian group. We know $G \cong Z_{n_1} \times Z_{n_2} \times \ldots \times Z_{n_k}$ for natural numbers $n_1, \ldots, n_k$.

Theorem

Any finite abelian group is the Galois group of an extension of $\mathbb{Q}$ (in fact of a subfield of a cyclotomic extension).

Proof: Let G be an abelian group. We know $G \cong Z_{n_1} \times Z_{n_2} \times \ldots \times Z_{n_k}$ for natural numbers $n_1, \ldots, n_k$.

If we had $n_i = p_i - 1$, for $p_1, \ldots, p_k$ distinct primes, we would be done: take $\mathbb{Q}(\zeta_{p_1 \ldots p_k})$.

Theorem

Any finite abelian group is the Galois group of an extension of $\mathbb{Q}$ (in fact of a subfield of a cyclotomic extension).

Proof: Let G be an abelian group. We know $G \cong Z_{n_1} \times Z_{n_2} \times \ldots \times Z_{n_k}$ for natural numbers $n_1, \ldots, n_k$.

If we had $n_i = p_i - 1$, for $p_1, \ldots, p_k$ distinct primes, we would be done: take $\mathbb{Q}(\zeta_{p_1 \ldots p_k})$.

We use as a black box that for any natural number $n \geq 2$, there are infinitely-many primes p with $p \equiv 1 \bmod n$. (a proof is outlined in DF). *[Example for $n = 5$: $p = 11, 31, 41, 51, 61, 71, 101, \ldots$]*

Theorem

Any finite abelian group is the Galois group of an extension of $\mathbb{Q}$ (in fact of a subfield of a cyclotomic extension).

Proof: Let G be an abelian group. We know $G \cong Z_{n_1} \times Z_{n_2} \times \ldots \times Z_{n_k}$ for natural numbers $n_1, \ldots, n_k$.

If we had $n_i = p_i - 1$, for $p_1, \ldots, p_k$ distinct primes, we would be done: take $\mathbb{Q}(\zeta_{p_1 \ldots p_k})$.

We use as a black box that for any natural number $n \geq 2$, there are infinitely-many primes p with $p \equiv 1 \bmod n$. (a proof is outlined in DF). *[Example for* $n = 5$*:* $p = 11, 31, 41, 51, 61, 71, 101, \ldots$*]*

Find distinct primes $p_1, \ldots, p_k$ so that $p_i \equiv 1 \bmod n_i$. Let $n = p_1 p_2 \ldots p_k$.

Theorem

Any finite abelian group is the Galois group of an extension of $\mathbb{Q}$ (in fact of a subfield of a cyclotomic extension).

Proof: Let G be an abelian group. We know $G \cong Z_{n_1} \times Z_{n_2} \times \ldots \times Z_{n_k}$ for natural numbers $n_1, \ldots, n_k$.

If we had $n_i = p_i - 1$, for $p_1, \ldots, p_k$ distinct primes, we would be done: take $\mathbb{Q}(\zeta_{p_1 \ldots p_k})$.

We use as a black box that for any natural number $n \geq 2$, there are infinitely-many primes p with $p \equiv 1 \bmod n$. (a proof is outlined in DF). *[Example for $n = 5$: $p = 11, 31, 41, 51, 61, 71, 101, \ldots$]*

Find distinct primes $p_1, \ldots, p_k$ so that $p_i \equiv 1 \bmod n_i$. Let $n = p_1 p_2 \ldots p_k$.

The Galois group of $\mathbb{Q}(\zeta_n)$ is $(\mathbb{Z}/p_1 p_2 \ldots p_k \mathbb{Z})^\times \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_k\mathbb{Z})^\times \cong Z_{p_1 - 1} \times \ldots Z_{p_k - 1}$.

Theorem

Any finite abelian group is the Galois group of an extension of $\mathbb{Q}$ (in fact of a subfield of a cyclotomic extension).

Proof: Let G be an abelian group. We know $G \cong Z_{n_1} \times Z_{n_2} \times \ldots \times Z_{n_k}$ for natural numbers $n_1, \ldots, n_k$.

If we had $n_i = p_i - 1$, for $p_1, \ldots, p_k$ distinct primes, we would be done: take $\mathbb{Q}(\zeta_{p_1 \ldots p_k})$.

We use as a black box that for any natural number $n \geq 2$, there are infinitely-many primes p with $p \equiv 1 \bmod n$. (a proof is outlined in DF). *[Example for $n = 5$: $p = 11, 31, 41, 51, 61, 71, 101, \ldots$]*

Find distinct primes $p_1, \ldots, p_k$ so that $p_i \equiv 1 \bmod n_i$. Let $n = p_1 p_2 \ldots p_k$.

The Galois group of $\mathbb{Q}(\zeta_n)$ is $(\mathbb{Z}/p_1 p_2 \ldots p_k \mathbb{Z})^\times \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_k\mathbb{Z})^\times \cong Z_{p_1 - 1} \times \ldots Z_{p_k - 1}$.

n_i divides $p_i - 1$, so find H_i a subgroup of $Z_{p_i - 1}$ of index n_i. The fixed field of $H_1 \times \ldots H_k$ is the desired extension.

The following is not known...

Question (The inverse Galois problem)

If G is an arbitrary finite group, is G the Galois group of an extension of $\mathbb{Q}$?

Summary

- Any finite separable extension is simple (primitive element theorem). Sometimes we can compute the generator using Galois theory.

Summary

- Any finite separable extension is simple (primitive element theorem). Sometimes we can compute the generator using Galois theory.
- The Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $(\mathbb{Z}/n\mathbb{Z})^\times$.

Summary

- Any finite separable extension is simple (primitive element theorem). Sometimes we can compute the generator using Galois theory.
- The Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $(\mathbb{Z}/n\mathbb{Z})^\times$.
- Any finite abelian group occurs as the Galois group of a subfield of a cyclotomic extension.

Summary

- Any finite separable extension is simple (primitive element theorem). Sometimes we can compute the generator using Galois theory.
- The Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $(\mathbb{Z}/n\mathbb{Z})^\times$.
- Any finite abelian group occurs as the Galois group of a subfield of a cyclotomic extension.

Next time: for which n can we construct the n-gon with just straightedge and compass?