MAU34101 Galois theory

2 - The Galois correspondence

Nicolas Mascot
mascotn@tcd.ie
Module web page

Michaelmas 2021–2022
Version: October 14, 2021

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

More about automorphisms

Bad ways to specify an automorphism

Let $K \subseteq L$ be a field extension. How to describe $\sigma \in \operatorname{Aut}_K(L)$?

Example

Take $K = \mathbb{Q} \subset L = \mathbb{Q}(\sqrt{2})$.
Because $L \simeq_{\mathbb{Q}} \mathbb{Q}[x]/(x^2 - 2) \simeq_{\mathbb{Q}} \mathbb{Q}(-\sqrt{2}) = L$, we have

$$\sigma : \begin{array}{ccc} L & \longrightarrow & L \\ a + b\sqrt{2} & \longmapsto & a - b\sqrt{2} \end{array}.$$

This σ takes $(1-\sqrt{2})^n \to 0$ to $(1+\sqrt{2})^n \to +\infty$, so it is not continuous at all!

Bad ways to specify an automorphism

Let $K \subseteq L$ be a field extension. How to describe $\sigma \in \mathrm{Aut}_K(L)$?

Remark

σ is a K-automorphism $\iff$ σ is K-linear: $\sigma(kx) = k\sigma(x)$ for $k \in K$, $x \in L$.

$\leadsto$ if $[L : K] < \infty$, we could fix a K-basis of L, and write down the matrix of σ.

Bad ways to specify an automorphism

Let $K \subseteq L$ be a field extension. How to describe $\sigma \in \mathrm{Aut}_K(L)$?

Remark

σ is a K-automorphism $\iff$ σ is K-linear: $\sigma(kx) = k\sigma(x)$ for $k \in K$, $x \in L$.

$\rightsquigarrow$ if $[L : K] < \infty$, we could fix a K-basis of L, and write down the matrix of σ.

But there is a much better way!

Good way to specify an automorphism

Lemma

Suppose $L = K(\alpha_1, \cdots, \alpha_r)$*. Any* $\sigma \in \mathrm{Aut}_K(L)$ *is completely determined by* $\sigma(\alpha_1), \cdots, \sigma(\alpha_r)$*.*

Proof.

Every $x \in L$ is of the form $x = \dfrac{\sum_{j_1,\cdots,j_r} a_{j_1,\cdots,j_r} \alpha_1^{j_1} \cdots \alpha_r^{j_r}}{\sum_{j_1,\cdots,j_r} b_{j_1,\cdots,j_r} \alpha_1^{j_1} \cdots \alpha_r^{j_r}}$

where $a_{i_1,\cdots,i_r}, \ b_{i_1,\cdots,i_r} \in K$

$$\rightsquigarrow \sigma(x) = \frac{\sum_{j_1,\cdots,j_r} \sigma(a_{j_1,\cdots,j_r}) \sigma(\alpha_1^{j_1} \cdots \alpha_r^{j_r})}{\sum_{j_1,\cdots,j_r} \sigma(b_{j_1,\cdots,j_r}) \sigma(\alpha_1^{j_1} \cdots \alpha_r^{j_r})} = \frac{\sum_{j_1,\cdots,j_r} a_{j_1,\cdots,j_r} \sigma(\alpha_1)^{j_1} \cdots \sigma(\alpha_r)^{j_r}}{\sum_{j_1,\cdots,j_r} b_{j_1,\cdots,j_r} \sigma(\alpha_1)^{j_1} \cdots \sigma(\alpha_r)^{j_r}}$$

determined by the values $\sigma(\alpha_1), \cdots, \sigma(\alpha_r)$. □

Good way to specify an automorphism

Lemma

Suppose $L = K(\alpha_1, \cdots, \alpha_r)$*. Any* $\sigma \in \mathrm{Aut}_K(L)$ *is completely determined by* $\sigma(\alpha_1), \cdots, \sigma(\alpha_r)$*.*

Example

$\sigma \in \mathrm{Aut}_{\mathbb{Q}}\left(\mathbb{Q}(\sqrt{2})\right)$ is determined by $\sigma(\sqrt{2})$.

$\sigma \in \mathrm{Aut}_{\mathbb{Q}}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3})\right)$ is determined by $\left(\sigma(\sqrt{2}), \sigma(\sqrt{3})\right)$.

Good way to specify an automorphism

Lemma

Suppose $L = K(\alpha_1, \cdots, \alpha_r)$*. Any* $\sigma \in \mathrm{Aut}_K(L)$ *is completely determined by* $\sigma(\alpha_1), \cdots, \sigma(\alpha_r)$*.*

Remark

K-automorphisms take roots of $F(x) \in K[x]$ to roots of $F(x) \in K[x]$
$\rightsquigarrow$ for each j, they take α_j to a conjugate of α_j.

Example

$\sigma \in \mathrm{Aut}_{\mathbb{Q}}\left(\mathbb{Q}(\sqrt{2})\right) \rightsquigarrow \sigma(\sqrt{2}) = \pm\sqrt{2}$.

$\sigma \in \mathrm{Aut}_{\mathbb{Q}}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3})\right) \rightsquigarrow \sigma(\sqrt{2}) = \pm\sqrt{2}$, $\sigma(\sqrt{3}) = \pm\sqrt{3}$.

$\sigma \in \mathrm{Aut}_{\mathbb{Q}}\left(\mathbb{Q}(\sqrt[3]{2})\right) \rightsquigarrow \sigma(\sqrt[3]{2})$ root of $x^3 - 2$.
But $\sigma(\sqrt[3]{2}) \in \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, so $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$, so $\sigma = \mathrm{Id}$.

Overview of the Galois correspondence

Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and $G = \mathrm{Aut}_K(L)$.
We admit that $G = \langle \sigma_2, \sigma_3 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where

$$\sigma_2(\sqrt{2}) = -\sqrt{2},\ \sigma_2(\sqrt{3}) = \sqrt{3},$$
$$\sigma_3(\sqrt{2}) = \sqrt{2},\ \sigma_3(\sqrt{3}) = -\sqrt{3}.$$

Reminder: if $H \subseteq \mathrm{Aut}_{\mathbb{Q}}(L)$, then

$$L^H = \{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in H\}$$

is a subfield of L containing $\mathbb{Q}$.

$H = \{\mathrm{Id}, \sigma_2\} \rightsquigarrow L^H = \mathbb{Q}(\sqrt{3})$.
$H = \{\mathrm{Id}, \sigma_3\} \rightsquigarrow L^H = \mathbb{Q}(\sqrt{2})$.
$H = G \rightsquigarrow L^H = \mathbb{Q}$.
$H = \{\mathrm{Id}\} \rightsquigarrow L^H = L$.

Overview of the Galois correspondence

Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and $G = \operatorname{Aut}_K(L)$.
We admit that $G = \langle \sigma_2, \sigma_3 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where

$$\sigma_2(\sqrt{2}) = -\sqrt{2},\ \sigma_2(\sqrt{3}) = \sqrt{3},$$
$$\sigma_3(\sqrt{2}) = \sqrt{2},\ \sigma_3(\sqrt{3}) = -\sqrt{3}.$$

$\rightsquigarrow$ Galois correspondence

$$\begin{array}{ccc} \text{subgroups } H \leqslant G & \longleftrightarrow & \text{intermediate extensions } K \subseteq E \subseteq L \\ H & \longmapsto & L^H \\ \operatorname{Aut}_E(L) & \longleftarrow\!\!\shortmid & E \end{array}$$

$$\begin{array}{ccc} & \{\mathrm{Id}\} & \\ \rotatebox{45}{$\subset$} & & \rotatebox{135}{$\subset$} \\ \{\mathrm{Id}, \sigma_3\} & & \{\mathrm{Id}, \sigma_2\} \\ \rotatebox{135}{$\subset$} & & \rotatebox{45}{$\subset$} \\ & G & \end{array} \quad \longleftrightarrow \quad \begin{array}{ccc} & \mathbb{Q}(\sqrt{2}, \sqrt{3}) & \\ \rotatebox{-45}{$\subset$} & & \rotatebox{-135}{$\subset$} \\ \mathbb{Q}(\sqrt{2}) & & \mathbb{Q}(\sqrt{3}) \\ \rotatebox{-135}{$\subset$} & & \rotatebox{-45}{$\subset$} \\ & \mathbb{Q} & \end{array}$$

Overview of the Galois correspondence

Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and $G = \operatorname{Aut}_K(L)$.
We <u>admit</u> that $G = \langle \sigma_2, \sigma_3 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where

$$\sigma_2(\sqrt{2}) = -\sqrt{2},\ \sigma_2(\sqrt{3}) = \sqrt{3},$$
$$\sigma_3(\sqrt{2}) = \sqrt{2},\ \sigma_3(\sqrt{3}) = -\sqrt{3}.$$

$\rightsquigarrow$ <u>Galois correspondence</u>

$$\begin{array}{ccc} \text{subgroups } H \leqslant G & \longleftrightarrow & \text{intermediate extensions } K \subseteq E \subseteq L \\ H & \longmapsto & L^H \\ \operatorname{Aut}_E(L) & \longleftarrow & E \end{array}$$

$$\begin{array}{ccc} & \{\mathrm{Id}\} & \\ \swarrow & \cap & \searrow \\ \{\mathrm{Id}, \sigma_3\} & \{\mathrm{Id}, \sigma_2\sigma_3\} & \{\mathrm{Id}, \sigma_2\} \\ \searrow & \cap & \swarrow \\ & G & \end{array} \quad \longleftrightarrow \quad \begin{array}{ccc} & \mathbb{Q}(\sqrt{2}, \sqrt{3}) & \\ \nearrow & \cup & \nwarrow \\ \mathbb{Q}(\sqrt{2}) & ? & \mathbb{Q}(\sqrt{3}) \\ \nwarrow & \cup & \nearrow \\ & \mathbb{Q} & \end{array}$$

Overview of the Galois correspondence

Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and $G = \operatorname{Aut}_K(L)$.
We admit that $G = \langle \sigma_2, \sigma_3 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where

$$\sigma_2(\sqrt{2}) = -\sqrt{2},\ \sigma_2(\sqrt{3}) = \sqrt{3},$$
$$\sigma_3(\sqrt{2}) = \sqrt{2},\ \sigma_3(\sqrt{3}) = -\sqrt{3}.$$

$\rightsquigarrow$ Galois correspondence

$$\begin{array}{ccc} \text{subgroups } H \leqslant G & \longleftrightarrow & \text{intermediate extensions } K \subseteq E \subseteq L \\ H & \longmapsto & L^H \\ \operatorname{Aut}_E(L) & \longleftarrow\!\shortmid & E \end{array}$$

$$\begin{array}{ccc} & \{\mathrm{Id}\} & \\ \supset & \cap & \subset \\ \{\mathrm{Id}, \sigma_3\} & \{\mathrm{Id}, \sigma_2\sigma_3\} & \{\mathrm{Id}, \sigma_2\} \\ \subset & \cap & \supset \\ & G & \end{array} \quad \longleftrightarrow \quad \begin{array}{ccc} & \mathbb{Q}(\sqrt{2}, \sqrt{3}) & \\ \subset & \cup & \supset \\ \mathbb{Q}(\sqrt{2}) & \mathbb{Q}(\sqrt{6}) & \mathbb{Q}(\sqrt{3}) \\ \supset & \cup & \subset \\ & \mathbb{Q} & \end{array}$$

But it can go very wrong!

Counter-example

Take $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$. Then $\mathrm{Aut}_K(L) = \{\mathrm{Id}\}$

$$\{\mathrm{Id}\} \qquad ??? \qquad \begin{array}{c} L \\ \cup \\ K \end{array}$$

$\rightsquigarrow$ We need the presence of automorphisms to make the Galois correspondence work.

Separable extensions

Separability

Definition (Separable element, separable extension)

Let $K \subseteq L$ be an algebraic extension, and let $\alpha \in L$.

1. *α is separable over K if its minimal polynomial over K is separable (disc $\neq 0$).*
2. *The extension $K \subseteq L$ is separable if all the elements of L are separable over K.*

Separability

Definition (Separable element, separable extension)

Let $K \subseteq L$ be an algebraic extension, and let $\alpha \in L$.

1. α *is separable over K if its minimal polynomial over K is separable (disc $\neq 0$).*
2. *The extension $K \subseteq L$ is separable if all the elements of L are separable over K.*

Bad things can happen in characteristic p!

Factorisation of $x^p - a$ in characteristic p

Lemma (Factorisation of $x^p - a$ in characteristic p)

Let char $K = p$, $a \in K$, *and* $F(x) = x^p - a \in K[x]$.

1. *If there exists* $b \in K$ *such that* $a = b^p$, *then the factorisation of* $F(x)$ *in* $K[x]$ *is* $F(x) = (x - b)^p$.
2. *Else,* $F(x)$ *is irreducible in* $K[x]$.

Proof.

If $a = b^p$, then $F(x) = x^p - b^p = (x - b)^p$.

Conversely, let $\beta \in \overline{K}$ be a root of $F(x)$, so $\beta^p = a$. Then $F(x) = (x - \beta)^p \in \overline{K}[x]$. Suppose $F(x)$ reducible over K, and let $G(x) \in K[x]$ be a nontrivial factor. Then

$$G(x) = (x - \beta)^d = x^d - d\beta x^{d-1} + \cdots$$

with $0 < d = \deg G < p$, so $d\beta \in K$.
But $0 \neq d \in K$, so $\beta \in K$. □

An example of inseparability

Counter-example

Let $K = \mathbb{F}_p(t)$ be the rational fraction field over $\mathbb{F}_p$.
Observe that $K^p = \text{Frob}(K) = \mathbb{F}_p(t^p)$, so $t \notin K^p$,
$\rightsquigarrow F(x) = x^p - t \in K[x]$ is irreducible.

Consider stem field $L = \mathbb{F}_p(t^{1/p}) = \mathbb{F}_p(u)$, $u = t^{1/p}$.
Then $F(u) = 0$, so u algebraic / K with min poly $F(x)$.
But in $L[x]$, $F(x) = (x - u)^p \rightsquigarrow$ inseparable!

Besides, for all $\sigma \in \text{Aut}_K(L)$, $\sigma(u)$ root of $F(x) \in K[x]$
$\rightsquigarrow \sigma(u) = u \rightsquigarrow \text{Aut}_K(L) = \{\text{Id}\}$, bad for Galois!

Remark

Squarefree-ness of a polynomial depends on the ground field!
Separability does not, because it is detected by disc $\neq 0$.

Shape of inseparable irreducible polynomials

Lemma

Let $P(x) \in K[x]$ irreducible and inseparable. Then $P'(x) = 0$.

Proof.

$0 = \operatorname{disc} P \sim \operatorname{Res}(P, P')$, so P and P' have a common factor, which can only be P since P is irreducible.
But $\deg P' < \deg P$, so $P \mid P' \implies P' = 0$. □

Shape of inseparable irreducible polynomials

Lemma

Let $P(x) \in K[x]$ *irreducible and inseparable. Then* $P'(x) = 0$.

Proposition

Let char $K = p$, *and* $P(x) \in K[x]$ *irreducible in* $K[x]$. *TFAE:*

1. $P(x)$ *is inseparable,*
2. $P'(x) = 0$,
3. $P(x) = Q(x^p)$ *for some* $Q(x) \in K[x]$.

Proof.

$1 \Rightarrow 2$: By lemma.

Shape of inseparable irreducible polynomials

Proposition

Let char $K = p$, *and* $P(x) \in K[x]$ *irreducible in* $K[x]$. *TFAE:*

1. $P(x)$ *is inseparable,*
2. $P'(x) = 0$,
3. $P(x) = Q(x^p)$ *for some* $Q(x) \in K[x]$.

Proof.

$1 \Rightarrow 2$: By lemma.

$2 \Rightarrow 3$: Write $P(x) = \sum_j a_j x^j$. Then $0 = P'(x) = \sum_j j a_j x^{j-1}$, so $j a_j = 0$ for all j, so $a_j = 0$ unless $j = 0$ in K, that is unless $p \mid j$.

$3 \Rightarrow 1$: If $P(x) = Q(x^p)$, then $P'(x) = p x^{p-1} Q'(x^p) = 0$ as $p = 0$, so $\gcd(P, P') = P$. □

Perfect fields

Definition

A field is perfect if it has no inseparable extension.

Theorem

1. *If* char $K = 0$*, then* K *is perfect.*
2. *If* char $K = p$*, then* K *is perfect* $\iff K^p = K$.

Remark

If char $K = p$, then K perfect $\iff \text{Frob} \in \text{Aut}(K)$.
In particular, finite fields are perfect, even though they have char > 0.

Perfect fields

Theorem

1. *If* char $K = 0$, *then* K *is perfect.*
2. *If* char $K = p$, *then* K *is perfect* $\iff K^p = K$.

Proof.

Suppose K not perfect. Then we can find $K \subseteq L$ inseparable, meaning there is $\alpha \in L$ whose min poly $P(x) \in K[x]$ is inseparable, so has common factor with $P' \rightsquigarrow P' = 0$.

If char $K = 0$, then $\deg P' = \deg P - 1$, absurd.

If char $K = p$ and $K^p = K$, then $\text{Frob} \in \text{Aut}(K)$, so every $a \in K$ has a (unique) p-th root $a^{1/p} = \text{Frob}^{-1}(a) \in K$. We know $P(x) = Q(x^p)$, say $P(x) = \sum_j a_j x^{pj}$. But then $P(x) = \sum_j (a_j^{1/p})^p (x^j)^p = \left(\sum_j a_j^{1/p} x^j\right)^p$ not irreducible, absurd.

Perfect fields

Theorem

1. *If* char $K = 0$, *then* K *is perfect.*
2. *If* char $K = p$, *then* K *is perfect* $\iff K^p = K$.

Proof.

Conversely, if char $K = p$ and $K^p \subsetneq K$, let $a \in K \setminus K^p$; then $P(x) = x^p - a \in K[x]$ is irreducible, and inseparable since $P'(x) = 0$, so $L = K[x]/\big(P(x)\big) \simeq K(\sqrt[p]{a})$ is an inseparable extension of K. $\square$

Separability vs. embeddings

Preservation of separability

Proposition

Let $K \subseteq E \subseteq L$. If $K \subseteq L$ separable, then $K \subseteq E$ and $E \subseteq L$ separable.

Proof.

$K \subseteq E$: If $\alpha \in E$, then $\alpha \in L$, so α separable over K.

$E \subseteq L$: Let $\alpha \in L$ have min poly $P_K(x) \in K[x]$ over K and $P_E(x) \in E[x]$ over E. Then $P_E(x) \mid P_K(x)$ which is separable, so $P_E(x)$ cannot have multiple roots in any extension of E. □

Embeddings vs. roots

Let K be a field, and let L, M be extensions of K.
A field morphism $f : L \longrightarrow M$ is automatically injective, hence an embedding: $L \simeq \operatorname{Im} f \subseteq M$.

Suppose that $L = K[x]/\big(P(x)\big)$ with $P(x) \in K[x]$ irreducible, and let $\alpha = \overline{x} \in L$.

If f is a K-morphism, then $f(\alpha) \in M$ is a root of $P(x)$.

Conversely, if $\beta \in M$ is a root of $P(x)$, then

$$\begin{array}{ccc} K[x] & \xrightarrow{\mathrm{ev}_\beta} & M. \\ \downarrow & \nearrow & \\ L = K[x]/\big(P(x)\big) & & \end{array}$$

$\rightsquigarrow$ K-embeddings of L in M $\longleftrightarrow$ Roots of $P(x)$ in M.

Extensions of embeddings vs. roots

Let $L = K[x]/\big(P(x)\big)$ with $P(x) = \sum_j a_j x^j \in K[x]$ irreducible, and as previously $\alpha = \overline{x} \in L$.
Let also $\iota : K \hookrightarrow M$, and $P_\iota(x) = \sum_j \iota(a_j) x^j \in M[x]$.
We have $K \overset{\iota}{\simeq} \iota(K)$, so $P_\iota(x)$ is irreducible over $\iota(K)$.

$$\begin{array}{ccc} L & \overset{?}{\dashrightarrow} & M \\ \Big| & & \Big| \\ K & \underset{\iota}{\overset{\sim}{\longrightarrow}} & \iota(K) \end{array}$$

Suppose $\iota' : L \longrightarrow M$ extends ι. Then

$$0 = \iota'(P(\alpha)) = \sum_j \iota'(a_j)\iota'(\alpha)^j = P_\iota\big(\iota'(\alpha)\big).$$

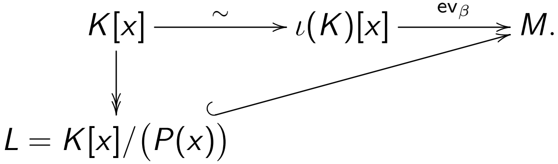
Extensions of embeddings vs. roots

Let $L = K[x]/\big(P(x)\big)$ with $P(x) = \sum_j a_j x^j \in K[x]$ irreducible, and as previously $\alpha = \overline{x} \in L$.
Let also $\iota : K \hookrightarrow M$, and $P_\iota(x) = \sum_j \iota(a_j) x^j \in M[x]$.
We have $K \overset{\iota}{\simeq} \iota(K)$, so $P_\iota(x)$ is irreducible over $\iota(K)$.

Suppose $\iota' : L \longrightarrow M$ extends ι. Then

$$0 = \iota'(P(\alpha)) = \sum_j \iota'(a_j)\iota'(\alpha)^j = P_\iota\big(\iota'(\alpha)\big).$$

Conversely, if $\beta \in M$ is a root of $P_\iota(x)$, then



$\rightsquigarrow$ Extensions of ι to $L \longleftrightarrow$ Roots of $P_\iota(x)$ in M.

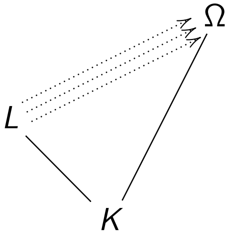
Separability by counting embeddings

Theorem

Let K be a field, let Ω be an algebraically closed extension of K (e.g. $\Omega = \overline{K}$), and let L be a finite extension of K. Then $\operatorname{Hom}_K(L, \Omega)$ is finite, and $N = \# \operatorname{Hom}_K(L, \Omega)$ is independent of Ω and satisfies

$$1 \leqslant N \leqslant [L : K],$$

with equality $N = [L : K] \iff K \subseteq L$ is separable.



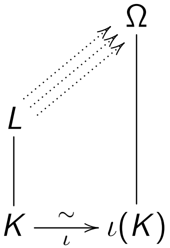
Separability by counting embeddings

Theorem

Let $\iota : K \hookrightarrow \Omega$ with Ω algebraically closed, and let L be a finite extension of K.
Then the set $\operatorname{Hom}_\iota(L, \Omega)$ of embeddings $L \hookrightarrow \Omega$ extending ι is finite, and $N = \# \operatorname{Hom}_\iota(L, \Omega)$ is independent of Ω and satisfies

$$1 \leqslant N \leqslant [L : K],$$

with equality $N = [L : K] \iff K \subseteq L$ is separable.



Separability by counting embeddings

Proof.

Write $L = K(\alpha_1, \cdots, \alpha_r)$. Induction on r to prove that $1 \leqslant N \leqslant [L : K]$ and $N = [L : K]$ if $K \subseteq L$ separable.

If $r = 0$, then $K = L$, so $\operatorname{Hom}_\iota(L, \Omega) = \{\iota\}$, OK.

Suppose true for $r - 1$.
Let $E = K(\alpha_1, \cdots, \alpha_{r-1})$, so $L = E(\alpha_r)$.
Then $N_E = \# \operatorname{Hom}_\iota(E, \Omega)$ satisfies $1 \leqslant N_E \leqslant [E : K]$, so let $\iota_E \in \operatorname{Hom}_\iota(E, \Omega)$. Besides $[L : E] = \frac{[L:K]}{[E:K]} < \infty$, so let $P(x) \in E[x]$ min poly of α_r. As $L \simeq_E E[x]/\big(P(x)\big)$, the number N_{ι_E} of $\iota' : L \hookrightarrow \Omega$ extending ι_E is

$$N_{\iota_E} = \# \text{ Roots of } P_{\iota_E}(x) \text{ in } \Omega \leqslant \deg P_{\iota_E} = \deg P = [L : E],$$

whence $N \leqslant N_E[L : E] \leqslant [E : K][L : E] = [L : K]$.

Separability by counting embeddings

Proof.

Suppose true for $r-1$.
Let $E = K(\alpha_1, \cdots, \alpha_{r-1})$, so $L = E(\alpha_r)$.
Then $N_E = \# \operatorname{Hom}_\iota(E, \Omega)$ satisfies $1 \leqslant N_E \leqslant [E:K]$, so let $\iota_E \in \operatorname{Hom}_\iota(E, \Omega)$. Besides $[L:E] = \frac{[L:K]}{[E:K]} < \infty$, so let $P(x) \in E[x]$ min poly of α_r. As $L \simeq_E E[x]/\big(P(x)\big)$, the number N_{ι_E} of $\iota' : L \hookrightarrow \Omega$ extending ι_E is

$$N_{\iota_E} = \# \text{ Roots of } P_{\iota_E}(x) \text{ in } \Omega \leqslant \deg P_{\iota_E} = \deg P = [L:E],$$

whence $N \leqslant N_E[L:E] \leqslant [E:K][L:E] = [L:K]$.

If furthermore $K \subseteq L$ is separable, then so are $K \subseteq E \subseteq L$, so $N_E = [E:K]$ by induction and $N_{\iota_E} = [L:E]$ for all $\iota_E \in \operatorname{Hom}_\iota(E, \Omega)$ as $\operatorname{disc} P_{\iota_E} = \iota_E(\operatorname{disc} P) \neq 0$.

Separability by counting embeddings

Proof.

If on the contrary $K \subseteq L$ is inseparable, write $L = K(\alpha_1, \cdots, \alpha_r)$ with α_1 inseparable over K.
Let $K_1 = K(\alpha_1)$, so that $K_1 \simeq_K K[x]/\big(Q(x)\big)$ where $Q(x) \in K[x]$ is the min poly of α_1 over K.
Then disc $Q_\iota = \iota(\text{disc } Q) = \iota(0) = 0$, so

$$\#\operatorname{Hom}_\iota\left(K_1, \Omega\right) = \#\text{Roots of } Q_\iota \text{ in } \Omega < \deg Q = [K_1 : K]$$

$\rightsquigarrow \#\operatorname{Hom}_\iota(L, \Omega) < [K_1 : K][L : K_1] = [L : K].$ □

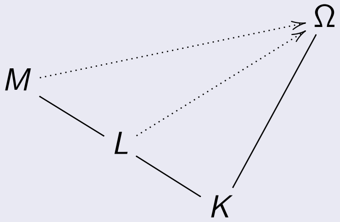
Separability by counting embeddings

Corollary

Let $K \subseteq L \subseteq M$ be finite extensions. Then $K \subseteq M$ is separable iff. $K \subseteq L$ and $L \subseteq M$ are separable.

Proof.

$$\# \operatorname{Hom}_K(M, \Omega) = \sum_{\iota \in \operatorname{Hom}_K(L,\Omega)} \# \operatorname{Hom}_\iota(M, \Omega). \qquad \square$$



Interlude : group actions

Reminder: Group actions

Definition

Let G be a group with identity $1_G \in G$, and let X be a set. A left action of G on X is a map

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g \cdot x \end{array}$$

such that $g \cdot h \cdot x = gh \cdot x$ and $1_G \cdot x = x$ for all $g, h \in G$ and $x \in X$.

In other words, it is a group morphism from G to the group of bijections from X to itself.

Notation: $G \circlearrowright X$.

Reminder: Group actions

Definition

Let G be a group with identity $1_G \in G$, and let X be a set.
A right action of G on X is a map

$$\begin{array}{ccc} X \times G & \longrightarrow & X \\ (x, g) & \longmapsto & x \cdot g \end{array}$$

such that $x \cdot g \cdot h = x \cdot gh$ and $x \cdot 1_G = x$ for all $g, h \in G$ and $x \in X$.

In other words, it is a group "anti-morphism",
i.e. $\phi(gh) = \phi(h)\phi(g)$, from G to the group of bijections from X to itself.

Notation: $X \circlearrowleft G$.

Reminder: Group actions

Definition

Let G be a group with identity $1_G \in G$, and let X be a set. A left action of G on X is a map

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g,x) & \longmapsto & g \cdot x \end{array}$$

such that $g \cdot h \cdot x = gh \cdot x$ and $1_G \cdot x = x$ for all $g, h \in G$ and $x \in X$.

In other words, it is a group morphism from G to the group of bijections from X to itself.

Example

A Rubik's cube is not a group, but rather a set of configurations acted on by a group of rotations of the faces.

Transitivity and freedom

Definition

Let $x \in X$. The orbit of x is $G \cdot x = \{g \cdot x \mid g \in G\} \subseteq X$. The stabiliser G_x of x is $\{g \in G \mid g \cdot x = x\} \leqslant G$.

The action is transitive if for all $x, y \in X$, there exists $g \in G$ such that $g \cdot x = y$, i.e. if there is only one orbit.

The action is free if for all $x \in X$ and $g \in G$,

$$g \cdot x = x \Longrightarrow g = 1_G.$$

Example

The action of the group of motions on the set of configurations of a Rubik's cube is free. It is transitive iff. we only include the configurations of the cube that are reachable without taking the cube apart.

Normal extensions

Normal extensions

Let K be a field, L a finite extension of K, and Ω an algebraically closed extension of K.

$\mathrm{Aut}_K(L)$ acts on $\mathrm{Hom}_K(L, \Omega)$ on the right by

$$\iota \cdot \sigma = \iota \circ \sigma \qquad \big(\iota \in \mathrm{Hom}_K(L, \Omega),\ \sigma \in \mathrm{Aut}_K(L)\big).$$

This action is free: $\iota \circ \sigma = \iota \implies \sigma = \mathrm{Id}$ since ι is injective.

$$\rightsquigarrow \# \mathrm{Aut}_K(L) \leqslant \# \mathrm{Hom}_K(L, \Omega).$$

Definition (Normal extension)

The extension $K \subseteq L$ is normal if

$$\# \mathrm{Aut}_K(L) = \# \mathrm{Hom}_K(L, \Omega).$$

Normal extensions

Definition (Normal extension)

The extension $K \subseteq L$ is normal if

$$\# \operatorname{Aut}_K(L) = \# \operatorname{Hom}_K(L, \Omega).$$

Counter-example

Take $K = \mathbb{Q} \subset L = \mathbb{Q}(\sqrt[3]{2}) \simeq_{\mathbb{Q}} \mathbb{Q}[x]/(x^3 - 2)$.

Since char $= 0$, this extension is separable, so

$$\# \operatorname{Hom}_K(L, \mathbb{C}) = [L : K] = 3.$$

However, $\# \operatorname{Aut}_K(L) = \#\{\operatorname{Id}\} = 1 < 3$, so this extension is not normal.

Characterisation of normal extensions

Theorem

Let $K \subseteq L$ be a finite extension. TFAE:

1. *The extension $K \subseteq L$ is normal,*
2. *The action of $\mathrm{Aut}_K(L)$ on $\mathrm{Hom}_K(L, \Omega)$ is transitive,*
3. *The elements of $\mathrm{Hom}_K(L, \Omega)$ all have the same image,*
4. *Whenever an irreducible $P(x) \in K[x]$ has a root in L, it splits into linear factors over L,*
5. *L is a splitting field over K of some $F(x) \in K[x]$.*

Characterisation of normal extensions

Counter-example

Take $K = \mathbb{Q} \subset L = \mathbb{Q}[x]/(x^3 - 2) \simeq_K \mathbb{Q}(\sqrt[3]{2})$.

1. The extension $K \subseteq L$ is not normal.
2. $\operatorname{Aut}_K(L) = \{\mathrm{Id}\}$ cannot act transitively on $\operatorname{Hom}_K(L, \mathbb{C})$.
3. The 3 elements of $\operatorname{Hom}_K(L, \mathbb{C})$ have images $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, $\mathbb{Q}(\zeta_3 \sqrt[3]{2}) \not\subset \mathbb{R}$, $\mathbb{Q}(\zeta_3^2 \sqrt[3]{2}) \not\subset \mathbb{R}$, where $\zeta_3 = e^{2\pi i/3}$.
4. $P(x) = x^3 - 2 \in K[x]$ is irreducible over K and has a root in L, but only factors as $1 + 2$ over L.
5. L is not the splitting field of $x^3 - 2$ over K.

Characterisation of normal extensions

Theorem

1. *The extension $K \subseteq L$ is normal,*
2. *The action of $\mathrm{Aut}_K(L)$ on $\mathrm{Hom}_K(L, \Omega)$ is transitive,*
3. *The elements of $\mathrm{Hom}_K(L, \Omega)$ all have the same image,*

Proof.

$1 \Leftrightarrow 2$: Clear.

$2 \Rightarrow 3$: Let $\iota_1, \iota_2 \in \mathrm{Hom}_K(L, \Omega)$. Then $\iota_2 = \iota_1 \circ \sigma$ for some $\sigma \in \mathrm{Aut}_K(L)$, so $\iota_1 = \iota_2 \circ \sigma^{-1}$, so $\operatorname{Im} \iota_1 = \operatorname{Im} \iota_2$.

$3 \Rightarrow 2$: Let $\iota_1, \iota_2 \in \mathrm{Hom}_K(L, \Omega)$. Then

$$L \xrightarrow[\iota_2]{\sim} \mathrm{Im}(\iota_2) = \mathrm{Im}(\iota_1) \xleftarrow[\iota_1]{\sim} L$$

so $\sigma = \iota_1^{-1} \circ \iota_2 \in \mathrm{Aut}_K(L)$ satisfies $\iota_2 = \iota_1 \circ \sigma$.

Characterisation of normal extensions

Theorem

3 *The elements of* $\operatorname{Hom}_K(L,\Omega)$ *all have the same image,*

4 *Whenever an irreducible* $P(x) \in K[x]$ *has a root in* L*, it splits into linear factors over* L*,*

Proof.

$3 \Rightarrow 4$: Let $\iota \in \operatorname{Hom}_K(L,\Omega)$, $I = \operatorname{Im} \iota \subseteq \Omega$. Let $P(x) \in K[x]$ irreducible have a root in $L \rightsquigarrow$ root $\beta \in I$. WTP that if $\gamma \in \Omega$ is another root of $P(x)$, then $\gamma \in I$.
Write $L = K(\alpha_1, \cdots, \alpha_r)$, let $0 \neq F(x) \in K[x]$ such that $F(\alpha_j) = 0$ for all j, and let $S \subseteq \Omega$ be the splitting field of $P(x)F(x)$. Then $F\big(\iota(\alpha_j)\big) = 0$ for all j, so $I = K\big(\iota(\alpha_1), \cdots, \iota(\alpha_r)\big) \subseteq S$.
S is a splitting field and $\beta, \gamma \in S$ are K-conjugate $\rightsquigarrow \gamma = \Phi(\beta)$ for some $\Phi \in \operatorname{Aut}_K(S)$. But then $\gamma \in \Phi(I) = \operatorname{Im} \Phi \circ \iota = I$ since $\Phi \circ \iota \in \operatorname{Hom}_K(L,\Omega)$.

Characterisation of normal extensions

Theorem

3 *The elements of* $\text{Hom}_K(L, \Omega)$ *all have the same image,*

4 *Whenever an irreducible* $P(x) \in K[x]$ *has a root in* L*, it splits into linear factors over* L*,*

5 L *is a splitting field over* K *of some* $F(x) \in K[x]$*.*

Proof.

$4 \Rightarrow 5$: Write again $L = K(\alpha_1, \cdots, \alpha_r)$. Let $P_j(x) \in K[x]$ min poly of α_j, let $F(x) = \prod_j P_j(x) \in K[x]$, and let $S \subseteq \overline{L}$ be the splitting of $F(x)$ over K. Then $L \subseteq S$; but since the $P_j(x)$ have all their roots in L, $S \subseteq L$.

$5 \Rightarrow 3$: If L is the splitting field of $F(x) \in K[x]$, then for any $\iota \in \text{Hom}_K(L, \Omega)$, $\iota(L) \subseteq \Omega$ is the splitting field of $F(x)$ contained in Ω. □

Normal closure

Corollary

Let $K \subseteq L$ finite. There exists a minimal finite $L \subseteq N$ such that $K \subseteq N$ normal. This N is unique up to K-isomorphism.

Proof.

Again write $L = K(\alpha_1, \cdots, \alpha_r)$ and let $P_j(x) \in K[x]$ min poly of α_j. Then N is a splitting field of $\prod_j P_j(x)$. □

Definition (Normal closure)

This N is the normal closure of $K \subseteq L$.

Example

The normal closure of $K = \mathbb{Q} \subseteq L = \mathbb{Q}(\sqrt[3]{2})$ is $N = \mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}) = L(\zeta_3)$, where $\zeta_3 = e^{2\pi i/3}$.

Galois extensions

Galois extensions

Let K be a field, and $\Omega \supseteq K$ algebraically closed. We have proved that if $K \subseteq L$ finite, then

$$\# \operatorname{Aut}_K(L) \underset{\text{Normal?}}{\leqslant} \# \operatorname{Hom}_K(L, \Omega) \underset{\text{Separable?}}{\leqslant} [L : K].$$

Definition (Galois extension)

A finite extension $K \subseteq L$ is Galois if

$$\# \operatorname{Aut}_K(L) = [L : K].$$

Characterisation of Galois extensions

Theorem

Let $K \subseteq L$ be a finite extension. TFAE:

1. $K \subseteq L$ *is Galois,*
2. $K \subseteq L$ *is normal and separable,*
3. $L =$ *splitting field over* K *of some* <u>*separable*</u> $F(x) \in K[x]$,
4. *For all* $\alpha \in L$, *we have* $\alpha \in K \iff \sigma(\alpha) = \alpha \ \forall \sigma \in \operatorname{Aut}_K(L)$; *in other words,* $K \subseteq L^{\operatorname{Aut}_K(L)}$ *is actually an equality,*
5. *The min poly over* K *of any* $\alpha \in L$ *is* $\displaystyle\prod_{\beta \in \operatorname{Aut}_K(L)\cdot\alpha} (x - \beta)$, *where* $\operatorname{Aut}_K(L) \cdot \alpha = \{\sigma(\alpha) \mid \sigma \in \operatorname{Aut}_K(L)\}$ *without multiplicities.*

Characterisation of Galois extensions

Counter-example

Take $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2}) \rightsquigarrow \mathrm{Aut}_K(L) = \{\mathrm{Id}\}$.

1 $\# \mathrm{Aut}_K(L) = 1 < 3 = [L : K]$.

2 $K \subseteq L$ is not normal.

3 $K \subseteq L$ is not the splitting field of $x^3 - 2$ over K,

4 $\sqrt[3]{2} \in L$ is fixed by all the elements of $\mathrm{Aut}_K(L) = \{\mathrm{Id}\}$, yet does not lie in K,

5 The min poly over K of $\sqrt[3]{2} \in L$ is not

$$\prod_{\beta \in \mathrm{Aut}_K(L) \cdot \sqrt[3]{2}} (x - \beta) = x - \sqrt[3]{2}.$$

Characterisation of Galois extensions

Counter-example

Take $K = \mathbb{F}_p(t)$, $L = \mathbb{F}_p(t^{1/p}) \rightsquigarrow \mathrm{Aut}_K(L) = \{\mathrm{Id}\}$.

1 $\# \mathrm{Aut}_K(L) = 1 < p = [L : K]$.

2 $K \subseteq L$ is not separable.

3 $K \subseteq L$ is the splitting field of $x^p - t = (x - t^{1/p})^p$ over K but this polynomial is not separable,

4 $t^{1/p} \in L$ is fixed by all the elements of $\mathrm{Aut}_K(L) = \{\mathrm{Id}\}$, yet does not lie in K,

5 The min poly over K of $t^{1/p} \in L$ is not

$$\prod_{\beta \in \mathrm{Aut}_K(L) \cdot t^{1/p}} (x - \beta) = x - t^{1/p}.$$

Characterisation of Galois extensions

Theorem

1 $K \subseteq L$ *is Galois,*

2 $K \subseteq L$ *is normal and separable,*

3 $L =$ *splitting field over* K *of some* <u>*separable*</u> $F(x) \in K[x]$,

Proof.

$1 \Leftrightarrow 2$: Clear.

$2 \Rightarrow 3$: $K \subseteq L$ normal $\rightsquigarrow$ splitting field of some $F(x) \in K[x]$. For each root $\alpha \in L$ of $F(x)$, let $P_\alpha(x)$ be its min poly. Then $P_\alpha(x)$ separable, so $K[x] \ni G(x) = \prod_{\text{distinct}} P_\alpha(x)$ too, and $K \subseteq L$ is its splitting field.

$3 \Rightarrow 2$: Splitting fields are normal. A splitting field of a separable polynomial is obtained as a succession of separable extensions, so is separable.

Characterisation of Galois extensions

Theorem

1. *$K \subseteq L$ is Galois,*
4. *For all $\alpha \in L$, we have $\alpha \in K \iff \sigma(\alpha) = \alpha \ \forall \sigma \in \operatorname{Aut}_K(L)$,*
5. *The min poly over K of any $\alpha \in L$ is $\displaystyle\prod_{\beta \in \operatorname{Aut}_K(L)\cdot\alpha} (x - \beta)$.*

Proof.

$1 \Rightarrow 4$: Let $K \subseteq E = L^{\operatorname{Aut}_K(L)} \subseteq L$, so $\operatorname{Aut}_K(L) = \operatorname{Aut}_E(L)$.
Then $[L:K] = \# \operatorname{Aut}_K(L) = \# \operatorname{Aut}_E(L) \leqslant [L:E]$
$\rightsquigarrow [E:K] = \frac{[L:K]}{[L:E]} \leqslant 1$.

$4 \Rightarrow 5$: $F_\alpha(x) = \displaystyle\prod_{\beta \in \operatorname{Aut}_K(L)\cdot\alpha} (x - \beta) \in L[x]$ has α as a root, and coefficients in $L^{\operatorname{Aut}_K(L)} = K$. Conversely, every β must be a root of the min poly of α over K.

Characterisation of Galois extensions

Theorem

2 $K \subseteq L$ *is normal and separable,*

5 *The min poly over* K *of any* $\alpha \in L$ *is* $\displaystyle\prod_{\beta \in \mathrm{Aut}_K(L)\cdot\alpha} (x - \beta)$.

Proof.

$5 \Rightarrow 2$: Let $\alpha \in L$; its min poly is $F_\alpha(x) = \displaystyle\prod_{\beta \in \mathrm{Aut}_K(L)\cdot\alpha} (x - \beta)$, which has distinct roots $\rightsquigarrow K \subseteq L$ separable. Now suppose $P(x) \in K[x]$ irreducible has a root $\alpha \in L$; then $P(x)$ is the min poly of $\alpha \rightsquigarrow P(x) = F_\alpha(x)$ has all its roots in L.

Characterisation of Galois extensions

Theorem

1 *$K \subseteq L$ is Galois,*

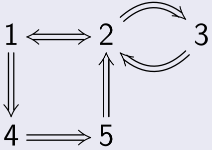
2 *$K \subseteq L$ is normal and separable,*

3 *$L =$ splitting field over K of some <u>separable</u> $F(x) \in K[x]$,*

4 *For all $\alpha \in L$, we have $\alpha \in K \iff \sigma(\alpha) = \alpha \ \forall \sigma \in \mathrm{Aut}_K(L)$,*

5 *The min poly over K of any $\alpha \in L$ is* $\displaystyle\prod_{\beta \in \mathrm{Aut}_K(L) \cdot \alpha} (x - \beta)$.

Proof.



□

Characterisation of Galois extensions

Theorem

1. $K \subseteq L$ is Galois,
2. $K \subseteq L$ is normal and separable,
3. $L =$ splitting field over K of some separable $F(x) \in K[x]$,
4. For all $\alpha \in L$, we have $\alpha \in K \iff \sigma(\alpha) = \alpha \ \forall \sigma \in \mathrm{Aut}_K(L)$,
5. The min poly over K of any $\alpha \in L$ is $\displaystyle\prod_{\beta \in \mathrm{Aut}_K(L) \cdot \alpha} (x - \beta)$.

Remark

The main obstruction to Galois-ness is often normal-ness rather than separability (e.g. in char 0).

If $K \subseteq L$ is separable but not normal, its the normal closure N is still separable over K, so $K \subseteq N$ is Galois over K. It is therefore sometimes called the Galois closure of $K \subseteq L$.

Galois groups

The Galois group of a Galois extension

From now on, we write L/K rather than $K \subseteq L$.

Definition (Galois group)

The Galois group of a Galois extension L/K is

$$\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L).$$

Example

$$\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{Id}, z \mapsto \bar{z}\} \simeq \mathbb{Z}/2\mathbb{Z}.$$

Determination of the Galois group

Let L/K be a Galois extension.

- $\# \operatorname{Gal}(L/K) = [L : K]$.
- For all $\alpha \in L$, the minimal polynomial $P(x)$ of α over K has all its roots in L; and whenever $\beta, \gamma \in L$ are roots of $P(x)$, there exists $\sigma \in \operatorname{Gal}(L/K)$ such that $\sigma(\beta) = \gamma$.
- The elements of $\operatorname{Gal}(L/K)$ are automorphisms $\rightsquigarrow$ they preserve algebraic relations over K, e.g. if $\sigma \in \operatorname{Gal}(L/K)$ and if $\alpha \in L$ satisfies $F(\alpha) = 0$ where $F(x) \in K[x]$, then $F\big(\sigma(\alpha)\big) = 0$ as well.

Example 1: $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2})$.

- Since both $\pm\sqrt{2} \in L$, L is the splitting field of separable $x^2 - 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$ $\rightsquigarrow$ L is Galois over $\mathbb{Q}$.
- Let $G = \operatorname{Gal}(L/\mathbb{Q})$. We have $\#G = [L : \mathbb{Q}] = 2$.
  $\operatorname{Id} \in G \rightsquigarrow$ need one other $\sigma \in \operatorname{Gal}(L/\mathbb{Q})$,
  $G = \{\operatorname{Id}, \sigma\} \simeq \mathbb{Z}/2\mathbb{Z}$.
- Any $\tau \in G$ is completely determined by $\tau(\sqrt{2})$,
  and $\tau(\sqrt{2}) = \pm\sqrt{2} \rightsquigarrow 2$ possibilities.
  $\#G = 2$, so both must occur $\rightsquigarrow \sigma(\sqrt{2}) = -\sqrt{2}$,
  so σ is $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ $(a, b \in \mathbb{Q})$.

Example 1: $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2})$.

- Since both $\pm\sqrt{2} \in L$, L is the splitting field of separable $x^2 - 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$ $\rightsquigarrow$ L is Galois over $\mathbb{Q}$.
- Let $G = \operatorname{Gal}(L/\mathbb{Q})$. We have $\#G = [L : \mathbb{Q}] = 2$.
  $\operatorname{Id} \in G \rightsquigarrow$ need one other $\sigma \in \operatorname{Gal}(L/\mathbb{Q})$,
  $G = \{\operatorname{Id}, \sigma\} \simeq \mathbb{Z}/2\mathbb{Z}$.
- Alternatively, there must exist $\tau \in G$ taking $\sqrt{2}$ to its conjugate $-\sqrt{2}$.

Example 2: $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

- Since both $\pm\sqrt{2}$ and both $\pm\sqrt{3} \in L$, L is the splitting field of separable $(x^2-2)(x^2-3) \in \mathbb{Q}[x]$ over $\mathbb{Q}$ $\rightsquigarrow$ L is Galois over $\mathbb{Q}$. Let $G = \operatorname{Gal}(L/\mathbb{Q})$.
- $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset L$, so $[L:\mathbb{Q}] = [L:\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$ where $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ and $[L:\mathbb{Q}(\sqrt{2})] \leqslant 2$.
  If $[L:\mathbb{Q}(\sqrt{2})] < 2$, then $\mathbb{Q}(\sqrt{2}) = L \ni \sqrt{3}$,
  so $\sqrt{3} = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$.
  Then $3 = (a+b\sqrt{2})^2 = (a^2+2b^2) + 2ab\sqrt{2}$,
  so $a^2 + 2b^2 = 3$ and $2ab = 0$, absurd.
  So $[L:\mathbb{Q}(\sqrt{2})] = 2$, so $\#G = [L:\mathbb{Q}] = 4$.
- Any $\tau \in G$ is completely determined by $\tau(\sqrt{2}) = \pm\sqrt{2}$ and $\tau(\sqrt{3}) = \pm\sqrt{3}$ $\rightsquigarrow$ $2 \times 2 = 4$ possibilites.
  $\#G = 4$ $\rightsquigarrow$ all 4 possibilities occur.
  So $G \simeq \{+,-\} \times \{+,-\} \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Example 2: $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

- $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset L$, so $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ where $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[L : \mathbb{Q}(\sqrt{2})] \leqslant 2$.
  If $[L : \mathbb{Q}(\sqrt{2})] < 2$, then $\mathbb{Q}(\sqrt{2}) = L \ni \sqrt{3}$,
  so $\sqrt{3} = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$.
  Then $3 = (a + b\sqrt{2})^2 = (a^2 + 2b^2) + 2ab\sqrt{2}$,
  so $a^2 + 2b^2 = 3$ and $2ab = 0$, absurd.
  So $[L : \mathbb{Q}(\sqrt{2})] = 2$, so $\#G = [L : \mathbb{Q}] = 4$.
- Alternatively, there must exist $\tau_2 \in G$ taking $\sqrt{2}$ to $-\sqrt{2}$, and τ_3 taking $\sqrt{3}$ to $-\sqrt{3}$. But can we do both simultaneously? E.g. can we move $\sqrt{2}$ but fix $\sqrt{3}$?
  $L =$ splitting field of $x^2 - 3$ over $\mathbb{Q}(\sqrt{2}) \rightsquigarrow$ any element of $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ extends to an element of $\text{Gal}(L/\mathbb{Q})$.
  Besides, $L/\mathbb{Q}(\sqrt{2})$ Galois, and $\text{Gal}\left(L/\mathbb{Q}(\sqrt{2})\right) \simeq \mathbb{Z}/2\mathbb{Z}$, so we can move $\sqrt{3}$ as we want without touching $\sqrt{2}$.

Example 3: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[3]{2})$. Let $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \zeta_3\sqrt[3]{2}$, $\alpha_3 = \zeta_3^2\sqrt[3]{2}$ be the complex roots of $F(x) = x^3 - 2 \in \mathbb{Q}[x]$, where $\zeta_3 = e^{2\pi i/3}$.

- $L/\mathbb{Q}$ is not Galois! So we consider its Galois closure $N = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$. Let $G = \mathrm{Gal}(N/\mathbb{Q})$; we have $\#G = [N : \mathbb{Q}] = [N : L][L : \mathbb{Q}] \geqslant 2 \times 3 = 6$.
- Any $\sigma \in G$ must take a root of $F(x) \in \mathbb{Q}[x]$ to a root of $F(x)$, and is completely characterised by how it permutes $\alpha_1, \alpha_2, \alpha_3 \rightsquigarrow$ we can view G as a subgroup of S_3 permuting $\alpha_1, \alpha_2, \alpha_3$.
- Since $\#G \geq 6$, necessarily $G = S_3$.

Remark

If $L =$ splitting field over K of $F(x) \in K[x]$ separable of degree d, then $\mathrm{Gal}(L/K)$ can, and should, be thought of as a subgroup of S_d permuting the d roots of $F(x)$ in L.

Example 3: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[3]{2})$. Let $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \zeta_3\sqrt[3]{2}$, $\alpha_3 = \zeta_3^2\sqrt[3]{2}$ be the complex roots of $F(x) = x^3 - 2 \in \mathbb{Q}[x]$, where $\zeta_3 = e^{2\pi i/3}$.

- $L/\mathbb{Q}$ is not Galois! So we consider its Galois closure $N = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$. Let $G = \mathrm{Gal}(N/\mathbb{Q})$; we have $\#G = [N : \mathbb{Q}] = [N : L][L : \mathbb{Q}] \geqslant 2 \times 3 = 6$.
- Any $\sigma \in G$ must take a root of $F(x) \in \mathbb{Q}[x]$ to a root of $F(x)$, and is completely characterised by how it permutes $\alpha_1, \alpha_2, \alpha_3 \rightsquigarrow$ we can view G as a subgroup of S_3 permuting $\alpha_1, \alpha_2, \alpha_3$.
- Since $\#G \geq 6$, necessarily $G = S_3$.

Remark

The Galois group does **NOT** preserve real-ness!

In other words, $\mathbb{R}$ is **NOT** normal over $\mathbb{Q}$!

Example 4: $\mathbb{Q}(\sqrt{5+\sqrt{21}})/\mathbb{Q}$

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt{5+\sqrt{21}}$.

- We have $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{21}) \subseteq L$, with $[\mathbb{Q}(\sqrt{21}) : \mathbb{Q}] = 2$ and $[L : \mathbb{Q}(\sqrt{21})] \leqslant 2$. If $[L : \mathbb{Q}(\sqrt{21})] = 1$, then $\alpha = a + b\sqrt{21}$ for some $a, b \in \mathbb{Q}$, so $5 + \sqrt{21} = (a + b\sqrt{21})^2 = (a^2 + 21b^2) + 2ab\sqrt{21}$, so $a^2 + 21b^2 = 5$ and $2ab = 1 \rightsquigarrow a^4 - 5a^2 + 21/4 = 0$, whence $a^2 = \frac{5 \pm 2}{2}$, absurd. So $[L : \mathbb{Q}] = 4$.
- α is a root of $P(x) = (x^2 - 5)^2 - 21 \in \mathbb{Q}[x]$, so this is its min poly over $\mathbb{Q}$
  $\rightsquigarrow$ the conjugates of α are α, $-\alpha$, $\beta = \sqrt{5 - \sqrt{21}}$, $-\beta$.
- $\alpha\beta = \sqrt{(5+\sqrt{21})(5-\sqrt{21})} = \sqrt{4} = 2 \in \mathbb{Q}$, so $\beta \in L$, so $L/\mathbb{Q}$ is Galois.
  Let $G = \mathrm{Gal}(L/\mathbb{Q})$; it is a subgroup of order $[L : \mathbb{Q}] = 4$ of S_4 permuting $\pm\alpha$, $\pm\beta$.

Example 4: $\mathbb{Q}(\sqrt{5+\sqrt{21}})/\mathbb{Q}$

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt{5+\sqrt{21}}$.
The conjugates of α are α, $-\alpha$, $\beta = \sqrt{5-\sqrt{21}} = 2/\alpha$, $-\beta$.
Any $\tau \in G$ is determined by $\tau(\alpha)$, which is one of 4 the conjugates of α
$\rightsquigarrow$ as $\#G = 4$, all possibilities must occur.

- If $\tau(\alpha) = \alpha$, then $\tau = \mathrm{Id}$ fixes $\alpha, -\alpha, \beta, -\beta$.
- If $\tau(\alpha) = -\alpha$, then $\tau(-\alpha) = -\tau(\alpha) = \alpha$,
  $\tau(\beta) = \tau(2/\alpha) = \tau(2)/\tau(\alpha) = 2/-\alpha = -\beta$,
  $\tau(-\beta) = -\tau(\beta) = \beta$.
- If $\tau(\alpha) = \beta$, then $\tau(-\alpha) = -\tau(\alpha) = -\beta$,
  $\tau(\beta) = \tau(2/\alpha) = 2/\beta = \alpha$, $\tau(-\beta) = -\tau(\beta) = -\alpha$.
- If $\tau(\alpha) = -\beta$, then $\tau(-\alpha) = -\tau(\alpha) = \beta$,
  $\tau(\beta) = \tau(2/\alpha) = 2/-\beta = -\alpha$, $\tau(-\beta) = -\tau(\beta) = \alpha$.

Conclusion: $G = V_4 \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Example 4: $\mathbb{Q}(\sqrt{5+\sqrt{21}})/\mathbb{Q}$

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt{5+\sqrt{21}}$.

Remark

The Galois group of a splitting field is the group of permutations of the roots that preserve the relations between these roots:
In this example, $-\alpha = -(\alpha)$ and $\alpha\beta = 2$.

The Galois correspondence: Statement and proof

Main slide of the module!

Theorem (Galois correspondence, FUNDAMENTAL)

Let L/K be a finite Galois extension, $G = \mathrm{Gal}(L/K)$,
$\mathcal{E} = \{\text{interm. exts. } K \subseteq E \subseteq L\}$, and $\mathcal{H} = \{\text{subgroups of } G\}$.

1. *For all $E \in \mathcal{E}$, the extension L/E is Galois.*
2. *The maps $\begin{array}{ccc} \mathcal{H} & \to & \mathcal{E} \\ H & \mapsto & L^H \end{array}$ and $\begin{array}{ccc} \mathcal{E} & \to & \mathcal{H} \\ E & \mapsto & \mathrm{Gal}(L/E) \end{array}$ are inclusion-reversing bijections, and inverses of each other.*
3. *If $E \in \mathcal{E}$ and $H \in \mathcal{H}$ correspond to each other, then*
$$[L : E] = \#H \qquad \text{and} \qquad [E : K] = [G : H].$$
4. *Let $\sigma \in G$. If $E \in \mathcal{E}$ corresponds to $H \in \mathcal{H}$, then $\sigma(E)$ corresponds to $\sigma H \sigma^{-1} = \{\sigma h \sigma^{-1} \mid h \in H\}$.*
5. *If $E \in \mathcal{E}$ and $H \in \mathcal{H}$ correspond to each other, then*
$$E/K \text{ is Galois} \iff H \text{ is a } \underline{\text{normal}} \text{ subgroup of } G.$$
In this case, $\mathrm{Gal}(E/K) \simeq G/H$ via $\sigma \mapsto \sigma_{|E}$.

Proof of part 1

Theorem (Galois correspondence)

Let L/K be a finite Galois extension, $G = \mathrm{Gal}(L/K)$, $\mathcal{E} = \{$interm. exts. $K \subseteq E \subseteq L\}$, and $\mathcal{H} = \{$subgroups of $G\}$.

1. *For all $E \in \mathcal{E}$, the extension L/E is Galois.*

L/K is Galois, so L is the splitting field over K of some separable $F(x) \in K[x]$, say $L = K(\alpha_1, \alpha_2, \cdots)$ where the α_j are the roots of $F(x)$.

Then for all $E \in \mathcal{E}$, we also have $L = E(\alpha_1, \alpha_2, \cdots)$, so L is the splitting field over E of $F(x) \in E[x]$. □

Linear lemma

Lemma

Let K field, and $H \leqslant \mathrm{Aut}(K)$. Let $a_{i,j} \in K$ such that the equations $\sum_j a_{1,j} x_j = \sum_j a_{2,j} x_j = \cdots = 0$ has a nonzero solution $x_1, x_2, \cdots \in K$, and such that the equations are invariant by H. Then they have a nonzero solution in K^H.

Proof.

Let $x_1, x_2, \cdots$ nonzero solution with as many $x_j = 0$ as possible, and let j_0 such that $x_{j_0} \neq 0$. WLOG, $x_{j_0} = 1$.
Let $\sigma \in H$. Then $\sigma(x_1), \sigma(x_2), \cdots$ is also a solution, and so is $y_1 = \sigma(x_1) - x_1, y_2 = \sigma(x_2) - x_2, \cdots$.
If $x_j = 0$, then $y_j = \sigma(0) - 0 = 0$; and $y_{j_0} = \sigma(1) - 1 = 0$.
Thus $y_j = 0$ for all j, so x_j fixed by all $\sigma \in H$. □

Proof of part 2

Theorem (Galois correspondence)

2 *The maps* $\Phi : \begin{array}{ccc} \mathcal{H} & \to & \mathcal{E} \\ H & \mapsto & L^H \end{array}$ *and* $\Psi : \begin{array}{ccc} \mathcal{E} & \to & \mathcal{H} \\ E & \mapsto & \operatorname{Gal}(L/E) \end{array}$ *are inclusion-reversing bijections, and inverses of each other.*

That Φ and Ψ are inclusion-reversing is clear.

Let $E \in \mathcal{E}$; then L/E Galois, so
$E = L^{\operatorname{Gal}(L/E)} = L^{\Psi(E)} = \Phi(\Psi(E))$.

Proof of part 2

Theorem (Galois correspondence)

2 *The maps* $\Phi : \begin{array}{ccc} \mathcal{H} & \to & \mathcal{E} \\ H & \mapsto & L^H \end{array}$ *and* $\Psi : \begin{array}{ccc} \mathcal{E} & \to & \mathcal{H} \\ E & \mapsto & \operatorname{Gal}(L/E) \end{array}$ *are inclusion-reversing bijections, and inverses of each other.*

Let $H \in \mathcal{H}$, and $H' = \Psi(\Phi(H)) = \operatorname{Gal}(L/L^H)$. Clearly $H \leqslant H'$.
Let $n = \#H$, let $\alpha_1, \cdots, \alpha_{n+1} \in L$, and consider the n equations $\displaystyle\sum_{j=1}^{n+1} \sigma(\alpha_j)x_j = 0$, $\sigma \in H$. That's $\#H = n$ equations in $n+1$ unknowns, so nonzero solution $x_1, \cdots, x_{n+1} \in L$.
Equations are invariant by H; by lemma, may assume $x_1, \cdots, x_{n+1} \in L^H$. Take $\sigma = \operatorname{Id}$: $\sum_{j=1}^{n+1} x_j\alpha_j = 0$
$\rightsquigarrow [L : L^H] < n+1$. But L/L^H Galois
$\rightsquigarrow \#H' = \#\operatorname{Gal}(L/L^H) = [L : L^H] \leqslant n = \#H$
$\rightsquigarrow H = H'$. □

Proof of part 3

Theorem (Galois correspondence)

Let L/K be a finite Galois extension, $G = \mathrm{Gal}(L/K)$,
$\mathcal{E} = \{$interm. exts. $K \subseteq E \subseteq L\}$, and $\mathcal{H} = \{$subgroups of $G\}$.

3 *If $E \in \mathcal{E}$ and $H \in \mathcal{H}$ correspond to each other, then*

$$[L:E] = \#H \qquad \text{and} \qquad [E:K] = [G:H].$$

L/E is Galois, so $[L:E] = \#\,\mathrm{Gal}(L/E) = \#H$.

Therefore $[G:H] = \frac{\#G}{\#H} = \frac{\#\,\mathrm{Gal}(L/K)}{\#\,\mathrm{Gal}(L/E)} = \frac{[L:K]}{[L:E]} = [E:K]$. $\square$

Proof of part 4

Theorem (Galois correspondence)

Let L/K be a finite Galois extension, $G = \mathrm{Gal}(L/K)$, $\mathcal{E} = \{\text{interm. exts. } K \subseteq E \subseteq L\}$, and $\mathcal{H} = \{\text{subgroups of } G\}$.

4 *Let $\sigma \in G$. If $E \in \mathcal{E}$ corresponds to $H \in \mathcal{H}$, then $\sigma(E)$ corresponds to $\sigma H \sigma^{-1} = \{\sigma h \sigma^{-1} \mid h \in H\}$.*

Since $H = \mathrm{Gal}(L/E)$,

$$\begin{aligned} \tau \in \mathrm{Gal}(L/\sigma(E)) &\iff \forall e \in E,\ \tau(\sigma(e)) = \sigma(e) \\ &\iff \forall e \in E,\ \sigma^{-1}\tau\sigma(e) = e \\ &\iff \sigma^{-1}\tau\sigma \in H \\ &\iff \tau \in \sigma H \sigma^{-1}. \quad \square \end{aligned}$$

A new understanding of normal

Lemma

Let L/K Galois, and let $E \in \mathcal{E}$. Then

$$E/K \text{ Galois} \iff \sigma(E) = E \text{ for all } \sigma \in \mathrm{Gal}(L/K).$$

Proof.

E/K separable since L/K is, so E/K Galois iff. normal.

$\Rightarrow$: If E/K normal, then $E =$ splitting field over K of some $F(x) \in K[x]$, so $E = K(\alpha_1, \alpha_2, \cdots)$ where α_j roots of $F(x)$ in L. This description is invariant by $\mathrm{Gal}(L/K)$.

$\Leftarrow$: Let $P(x) \in K[x]$ irreducible over K have a root $\alpha \in E$. L/K normal, $\alpha \in L$, so $P(x)$ has all its roots in L; and if $\beta \in L$ is such a root, then $\beta = \sigma(\alpha)$ for some $\sigma \in \mathrm{Gal}(L/K)$. But then $\beta \in \sigma(E) = E$, so $P(x)$ has all its roots in E, so E/K normal. □

Proof of part 5

Theorem (Galois correspondence)

5 *If $E \in \mathcal{E}$ and $H \in \mathcal{H}$ correspond to each other, then*

$$E/K \text{ is Galois} \iff H \text{ is a } \underline{\text{normal}} \text{ subgroup of } G.$$

In this case, $\mathrm{Gal}(E/K) \simeq G/H$ *via* $\sigma \mapsto \sigma_{|E}$.

By lemma, E/K Galois $\iff \forall \sigma \in G, \sigma(E) = E$

$$\iff \forall \sigma \in G, \sigma H \sigma^{-1} = H$$

$$\iff H \text{ normal in } G.$$

Suppose this is the case. Then $\begin{array}{ccc} \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(E/K) \\ \sigma & \longmapsto & \sigma_{|E} \end{array}$

well-defined since each σ stabilises E, and group morphism, whose kernel is $H \rightsquigarrow$ induces injection $G/H \longrightarrow \mathrm{Gal}(E/K)$. As $\#(G/H) = [G : H] = [E : K] = \# \mathrm{Gal}(E/K)$, actually bijection. □

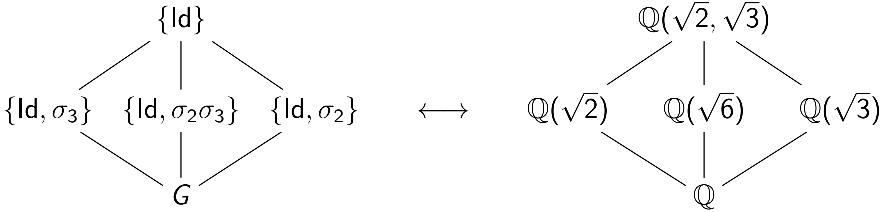
The Galois correspondence: Practice by examples

Example 1: $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$

$L = \mathbb{Q}(\sqrt{2},\sqrt{3})$ is Galois over $\mathbb{Q}$ with Galois group $G = \operatorname{Gal}(L/\mathbb{Q}) = \{\mathrm{Id}, \sigma_2, \sigma_3, \sigma_2\sigma_3\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where

$$\sigma_2(\sqrt{2}) = -\sqrt{2},\ \sigma_2(\sqrt{3}) = \sqrt{3},$$
$$\sigma_3(\sqrt{2}) = \sqrt{2},\ \sigma_3(\sqrt{3}) = -\sqrt{3}.$$

Galois correspondence:



Let $H = \{\mathrm{Id}, \sigma_2\}$; the corresponding E is $L^H = \mathbb{Q}(\sqrt{3})$.
Since G is Abelian, H is normal in G, so $E/\mathbb{Q}$ is Galois, and $\operatorname{Gal}(E/\mathbb{Q}) = G/H = \{\{\mathrm{Id}, \sigma_2\}, \{\sigma_3, \sigma_2\sigma_3\}\} \simeq \mathbb{Z}/2\mathbb{Z}$.

Example 2: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$. $[L : \mathbb{Q}] = 3$, so $\mathrm{Gal}(L/\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$ which has no non-trivial subgroups, so there are no non-trivial intermediate subfields.

Example 2: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$. $[L : \mathbb{Q}] = 3$, so $\mathrm{Gal}(L/\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$ which has no non-trivial subgroups, so there are no non-trivial intermediate subfields.

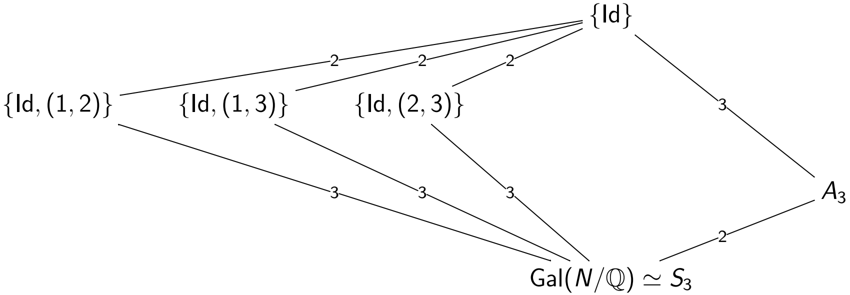
WRONG! $L/\mathbb{Q}$ is not Galois, so the correspondence may not apply. But it applies to the extension $N/\mathbb{Q}$,
where $N = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is the Galois closure of L over $\mathbb{Q}$.

Example 2: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

$\mathrm{Gal}(N/\mathbb{Q}) \simeq S_3$ permuting conjugates

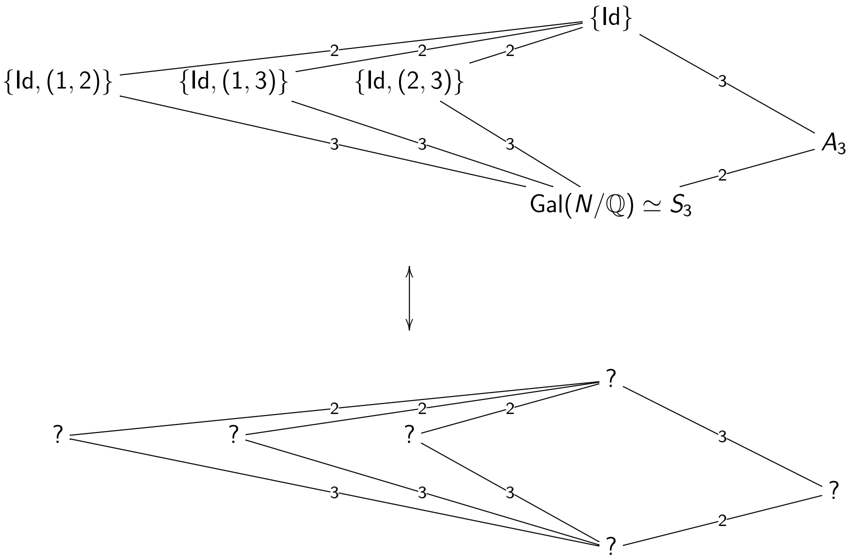
$$\alpha_1 = \sqrt[3]{2}, \quad \alpha_2 = \zeta_3\sqrt[3]{2}, \quad \alpha_3 = \zeta_3^2\sqrt[3]{2},$$

$\rightsquigarrow$ subgroup diagram:



where $A_3 = \{\mathrm{Id}, (1,2,3), (1,3,2)\} \simeq \mathbb{Z}/3\mathbb{Z}$ is the alternate subgroup of S_3.

Example 2: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

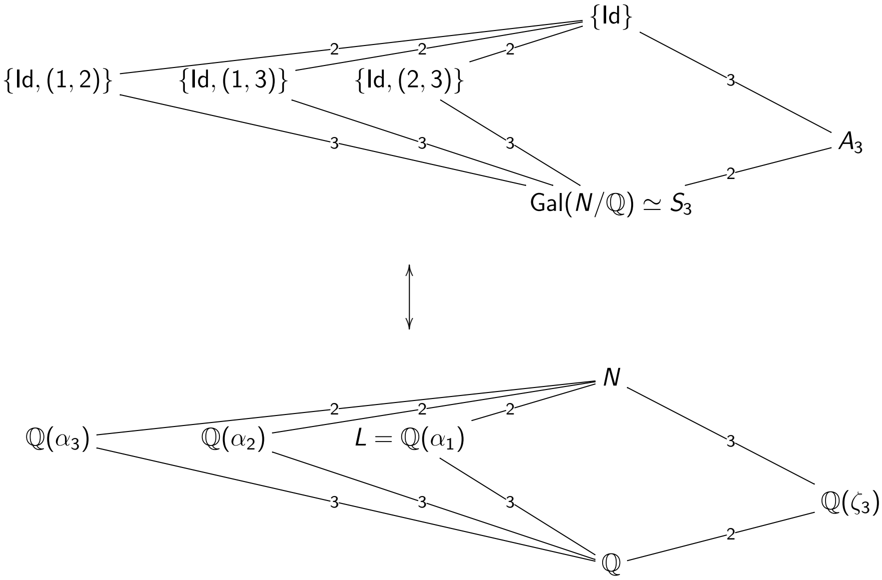


Example 2: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

$H = \{\mathrm{Id}, (2,3)\}$ has order 2 and index 3, so $E = N^H$ has $[E : \mathbb{Q}] = 3$ and $[N : E] = 2$.
α_1 is fixed by H, so $\alpha_1 \in E$, so $\mathbb{Q}(\alpha_1) \subseteq E$. By tower law applied to $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1) \subseteq E$, actually $E = \mathbb{Q}(\alpha_1) = L$.

Let us now determine $F = N^{A_3}$.
We have $[F : \mathbb{Q}] = 2$ and $[N : F] = 3$.
Observe that $\zeta_3 = \frac{\alpha_2}{\alpha_1} = \frac{\alpha_3}{\alpha_2} = \frac{\alpha_1}{\alpha_3}$ is fixed by H, so $\mathbb{Q}(\zeta_3) \subseteq F$.
Also note that α_3 root of irreducible $x^2 + x + 1 = \frac{x^3-1}{x-1} \in \mathbb{Q}[x]$
$\rightsquigarrow [\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$, so $F = \mathbb{Q}(\zeta_3)$ by tower law.

Example 2: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$



Example 2: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

For each intermediate E, N/E is Galois (actually splitting field of $x^3 - 2$ over E).
Only A_3 is normal in S_3, so only $\mathbb{Q}(\zeta_3)$ is Galois over $K = \mathbb{Q}$.

In fact, the other subgroups

$$\{\mathrm{Id}, (1,2)\}, \quad \{\mathrm{Id}, (1,3)\}, \quad \{\mathrm{Id}, (2,3)\}$$

are group-conjugate to each other in S_3, so that the corresponding intermediate extensions

$$\mathbb{Q}(\alpha_3), \quad \mathbb{Q}(\alpha_2), \quad \mathbb{Q}(\alpha_1)$$

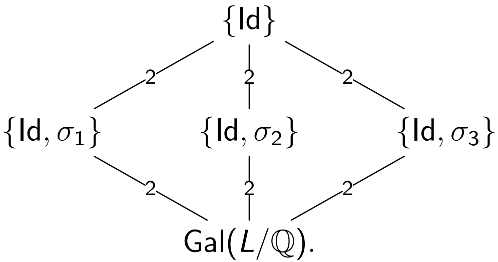
are Galois-conjugate to each other.

Example 3: $\mathbb{Q}(\sqrt{5+\sqrt{21}})/\mathbb{Q}$

Let $L = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt{5+\sqrt{21}}$. We know that $\mathrm{Gal}(L/\mathbb{Q}) \simeq V_4$ acting on conjugates α, $-\alpha$, $\beta = 2/\alpha$, $-\beta$.

Let $\sigma_1 : \alpha \mapsto -\alpha$, $\sigma_2 : \alpha \mapsto \beta$, $\sigma_3 : \alpha \mapsto -\beta$.

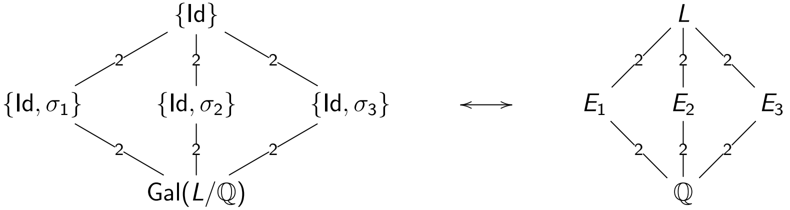
As $V_4 \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, subgroup diagram



Example 3: $\mathbb{Q}(\sqrt{5+\sqrt{21}})/\mathbb{Q}$

For $i = 1, 2, 3$, write $H_i = \{\mathrm{Id}, \sigma_i\}$ and $E_i = L^{H_i}$.

We have $[E_i : \mathbb{Q}] = [G : H_i] = 2$, $[L : E_i] = \#H_i = 2$.

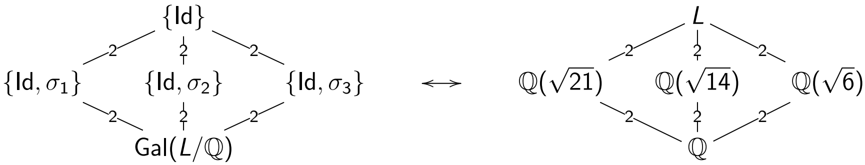


Example 3: $\mathbb{Q}(\sqrt{5+\sqrt{21}})/\mathbb{Q}$

$\sigma_1 : \alpha \mapsto -\alpha$ fixes $\alpha^2 = 5 + \sqrt{21}$, so $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{21}) \subseteq E_1$, so $E_1 = \mathbb{Q}(\sqrt{21})$ by degree.

$\sigma_2 : \alpha \leftrightarrow \beta$ fixes $\alpha\beta = 2$, so $\mathbb{Q}(\alpha\beta) = \mathbb{Q} \subseteq E_2$, useless; but σ_2 also fixes $\alpha + \beta$, and $(\alpha+\beta)^2 = \alpha^2 + \beta^2 + 2\alpha\beta = 14$, so $\sqrt{14} \in E_2$, so $E_2 = \mathbb{Q}(\sqrt{14})$ by degree.

$\sigma_3 : \alpha \leftrightarrow -\beta$ fixes $\alpha - \beta$; as $(\alpha-\beta)^2 = 6$, $E_3 = \mathbb{Q}(\sqrt{6})$.



$\mathrm{Gal}(L/\mathbb{Q})$ Abelian $\rightsquigarrow$ all subgroups normal $\rightsquigarrow$ all E Galois / $\mathbb{Q}$.

We see $L = \mathbb{Q}(\sqrt{21}, \sqrt{14}, \sqrt{6})$. Yet $[L : \mathbb{Q}] = 4$ not 8; in fact, any two generators suffice, e.g. $\sqrt{6} = \frac{\sqrt{21}\sqrt{14}}{7} \in \mathbb{Q}(\sqrt{14}, \sqrt{21})$.

Example 4: $\mathbb{Q}(\sqrt{5+\sqrt{15}})/\mathbb{Q}$

Let $L = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt{5+\sqrt{15}}$.
We have $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{15}) \subseteq L$, and $\alpha \notin \mathbb{Q}(\sqrt{15}) \rightsquigarrow [L:\mathbb{Q}] = 4$
$\rightsquigarrow$ α has min poly $(x^2-5)^2 - 15 \in \mathbb{Q}[x]$ over $\mathbb{Q}$
$\rightsquigarrow$ α has conjugates $\pm\alpha, \pm\beta$ over $\mathbb{Q}$, where $\beta = \sqrt{5-\sqrt{15}}$.

This time, $\alpha\beta = \sqrt{10} \notin \mathbb{Q}$, so not clear whether $\beta \in L$.

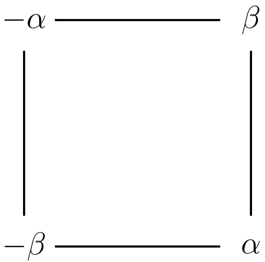
Suppose $\beta \in L$. Then $L/\mathbb{Q}$ Galois, $\text{Gal}(L/\mathbb{Q})$ of order 4, and $E = \mathbb{Q}(\sqrt{15})$ corresponds to a subgroup $H = \{\text{Id}, \sigma\}$.
As $\alpha^2 = 5 + \sqrt{15} \in E$, $\sigma(\alpha^2) = \alpha^2$, so $\sigma(\alpha) = \pm\alpha$.
$\alpha \notin E$ lest $L = E$, so $\sigma(\alpha) = -\alpha$.
Besides, σ permutes $\pm\alpha$, $\pm\beta$ injectively, so $\sigma(\beta) = \pm\beta$.
If $\sigma(\beta) = \beta$, then $\beta \in E$, whereas $[\mathbb{Q}(\beta):\mathbb{Q}] = 4$, absurd.
If $\sigma(\beta) = -\beta$, then $\sqrt{10} = \alpha\beta \in E = \mathbb{Q}(\sqrt{15})$, absurd.
So $\beta \notin L$.

Example 4: $\mathbb{Q}(\sqrt{5+\sqrt{15}})/\mathbb{Q}$

Since $\beta \notin L$, L not Galois over $\mathbb{Q}$; its Galois closure over $\mathbb{Q}$ is $N = \mathbb{Q}(\pm\alpha, \pm\beta) = L(\beta) \supsetneq L$.

As $\beta^2 = 5 - \sqrt{15} \in L$, $[N : L] \leqslant 2$, so $[N : L] = 2$;
thus $\# \operatorname{Gal}(N/\mathbb{Q}) = [N : \mathbb{Q}] = 8$, subgroup of $S_4 \circlearrowright \pm\alpha, \pm\beta$.

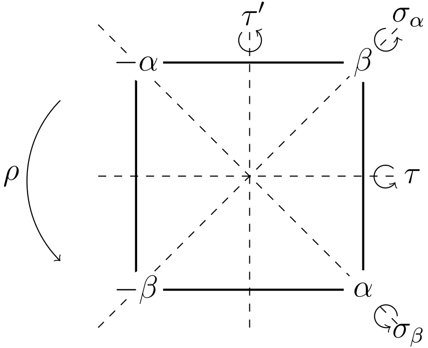
$\operatorname{Gal}(N/\mathbb{Q})$ preserves negatives, so preserves square



so contained in symmetry group D_8 of the square.
But $\# D_8 = 8$, so $\operatorname{Gal}(N/\mathbb{Q}) = D_8$.

Example 4: $\mathbb{Q}(\sqrt{5+\sqrt{15}})/\mathbb{Q}$

Name the elements of $\mathrm{Gal}(N/\mathbb{Q})$:

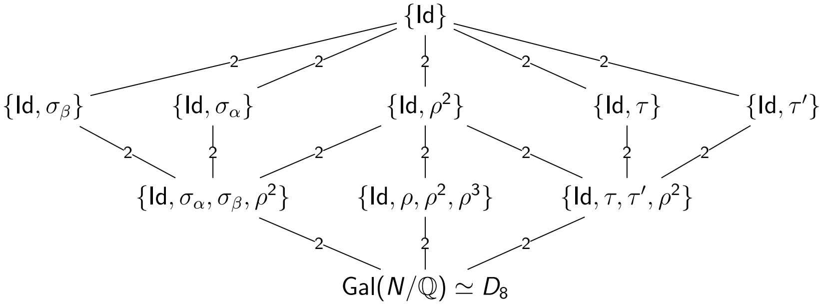


meaning $\sigma_\alpha : \alpha \mapsto -\alpha,\ -\alpha \mapsto \alpha,\ \beta \mapsto \beta,\ -\beta \mapsto -\beta$
and $\rho : \alpha \mapsto \beta \mapsto -\alpha \mapsto -\beta \mapsto \alpha$, etc.
The central symmetry is $\sigma_\alpha\sigma_\beta = \sigma_\beta\sigma_\alpha = \tau\tau' = \tau'\tau = \rho^2$.

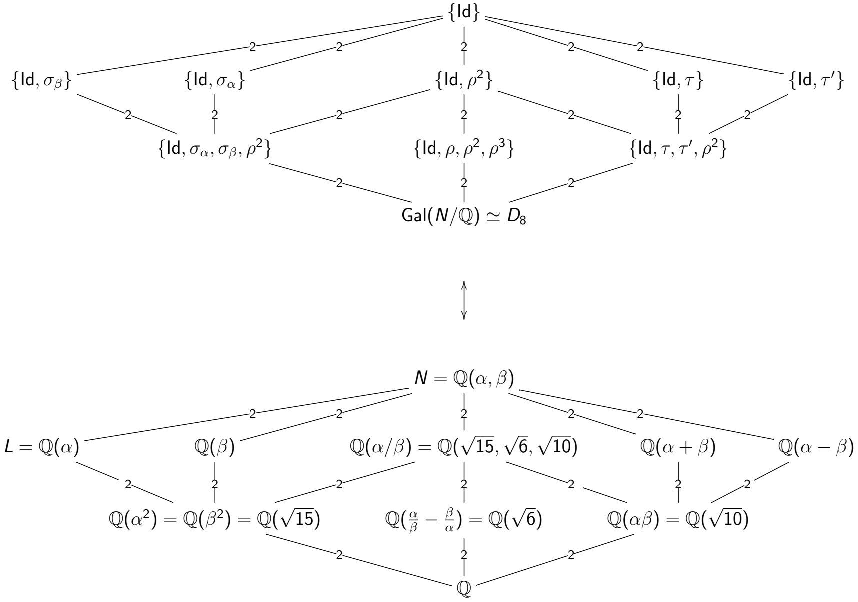
Example 4: $\mathbb{Q}(\sqrt{5+\sqrt{15}})/\mathbb{Q}$

By Lagrange, possible subgroup orders 2 and 4.
$\#H = 2 \rightsquigarrow H = \{\mathrm{Id}, \gamma\} \simeq \mathbb{Z}/2\mathbb{Z}$, γ of order 2.
$\#H = 4 \rightsquigarrow$ either $H = \{\mathrm{Id}, \gamma, \gamma^2, \gamma^3\} \simeq \mathbb{Z}/4\mathbb{Z}$, γ of order 4, or $H = \{\mathrm{Id}, \gamma, \gamma', \gamma\gamma'\} \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, γ and γ' of order 2 and commute.

$\rightsquigarrow$ Subgroup diagram:



Example 4: $\mathbb{Q}(\sqrt{5+\sqrt{15}})/\mathbb{Q}$



Example 4: $\mathbb{Q}(\sqrt{5+\sqrt{15}})/\mathbb{Q}$

The group-conjugates of σ_α are σ_α and σ_β, so the subgroups $\{\text{Id}, \sigma_\alpha\}$ and $\{\text{Id}, \sigma_\beta\}$ are not normal, and are conjugate to each other (by ρ). Correspondingly, $\mathbb{Q}(\beta)$ and $\mathbb{Q}(\alpha)$ are not Galois over $\mathbb{Q}$, and are switched by ρ.

Similarly, $\{\text{Id}, \tau\}$ and $\{\text{Id}, \tau'\}$ are conjugate (by ρ again); correspondingly, $\mathbb{Q}(\alpha+\beta)$ and $\mathbb{Q}(\alpha-\beta)$ are not Galois over $\mathbb{Q}$, and are switched by ρ.

All the other subgroups are normal; correspondingly, all the other subfields are Galois over $\mathbb{Q}$.

Application to cyclotomy

Complex N-th roots of unity

Fix $N \in \mathbb{N}$. Let $\zeta_N = e^{2\pi i/N} \in \mathbb{C}$.

Definition (Root of 1)

A (complex) N-th root of unity is a $z \in \mathbb{C}$ such that $z^N = 1$.

These are the ζ_N^k, $k = 0, 1, \cdots, N-1$. They form a subgroup μ_N of $\mathbb{C}^\times$, isomorphic to $\mathbb{Z}/N\mathbb{Z}$ by $\mathbb{Z}/N\mathbb{Z} \ni k \longleftrightarrow \zeta_N^k \in \mu_N$. They have $|z| = 1$, so $z^{-1} = \overline{z}$.

Definition (Primitive root of 1)

$z \in \mu_N$ is primitive if $z^M \neq 1$ for all $\mathbb{N} \ni M < N$.

Example (N=4)

The 4th roots of unity are $1 = \zeta_4^0$, $i = \zeta_4$, $-1 = \zeta_4^2$, $-i = \zeta_4^3$. Only i and $-i$ are primitive.

Complex N-th roots of unity

These are the ζ_N^k, $k = 0, 1, \cdots, N-1$. They form a subgroup μ_N of $\mathbb{C}^\times$, isomorphic to $\mathbb{Z}/N\mathbb{Z}$ by $\mathbb{Z}/N\mathbb{Z} \ni k \longleftrightarrow \zeta_N^k \in \mu_N$. They have $|z| = 1$, so $z^{-1} = \bar{z}$.

Definition (Primitive root of 1)

$z \in \mu_N$ is primitive if $z^M \neq 1$ for all $\mathbb{N} \ni M < N$.

Example (N=4)

The 4th roots of unity are $1 = \zeta_4^0$, $i = \zeta_4$, $-1 = \zeta_4^2$, $-i = \zeta_4^3$. Only i and $-i$ are primitive.

Proposition

ζ_N^k *is a primitive N-th root of 1* $\iff \gcd(k, N) = 1$

$\iff k \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Unofficial notation: $\mu_N^\times$.

Cyclotomic polynomials

Let $z \in \mu_N$. Then z root of $x^N - 1 \in \mathbb{Q}[x]$, so algebraic / $\mathbb{Q}$.
But $x^N - 1$ is usually not the min poly!

Definition (Cyclotomic polynomial)

The N-th cyclotomic polynomial is

$$\Phi_N(x) = \prod_{z \in \mu_N^\times} (x - z) = \prod_{k \in (\mathbb{Z}/N\mathbb{Z})^\times} (x - \zeta_N^k).$$

Theorem

$\Phi_N(x) \in \mathbb{Z}[x]$, *and is irreducible over* $\mathbb{Q}$.

Proposition

$$x^N - 1 = \prod_{d | N} \Phi_d(x).$$

Cyclotomic polynomials

Theorem

$\Phi_N(x) \in \mathbb{Z}[x]$, *and is irreducible over* $\mathbb{Q}$.

Proposition

$$x^N - 1 = \prod_{d|N} \Phi_d(x).$$

Example

For $p \in \mathbb{N}$ prime, $x^p - 1 = \Phi_1(x)\Phi_p(x) = (x-1)\Phi_p(x)$
$\rightsquigarrow \Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + \cdots + x + 1.$

Example

$$\Phi_9(x) = \frac{x^9 - 1}{\Phi_1(x)\Phi_3(x)} = \frac{x^9 - 1}{(x-1)(x^2+x+1)} = x^6 + x^3 + 1.$$

Cyclotomic extensions

Definition

The N-th cyclotomic extension is $\mathbb{Q}(\zeta_N) = \mathbb{Q}(\mu_N)$.

$$[\mathbb{Q}(\zeta_N) : \mathbb{Q}] = \deg \Phi_N(x) = \#\mu_N^\times = \#(\mathbb{Z}/N\mathbb{Z})^\times = \phi(N).$$

$\mathbb{Q}(\zeta_N) \supset \mu_N$ is splitting field / $\mathbb{Q}$ of $x^N - 1$, and of $\Phi_N(x)$
$\rightsquigarrow \mathbb{Q}(\zeta_N)/\mathbb{Q}$ is Galois.

Theorem

$\operatorname{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ *is canonically isomorphic to* $(\mathbb{Z}/N\mathbb{Z})^\times$.

Cyclotomic extensions

Theorem

Gal$(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ *is canonically isomorphic to* $(\mathbb{Z}/N\mathbb{Z})^\times$.

Proof.

Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. Determined by $\sigma(\zeta_N)$, which is a root of $\Phi_N(x) \rightsquigarrow$ at most $\phi(n)$ choices $\rightsquigarrow$ all must occur.
For each $k \in (\mathbb{Z}/N\mathbb{Z})^\times$, let $\sigma_k : \zeta_N \mapsto \zeta_N^k$.
Then for any $z \in \mu_N$, say $z = \zeta_N^j$, we have
$\sigma_k(z) = \sigma_k(\zeta_N^j) = \sigma_k(\zeta_N)^j = (\zeta_N^k)^j = \zeta_N^{kj} = (\zeta_N^j)^k = z^k$.
Therefore $\sigma_j \sigma_k = (z \mapsto z^k \mapsto (z^k)^j = z^{jk}) = \sigma_{jk}$. □

Example

Complex conjugation is $\sigma_{-1} : z \mapsto z^{-1} = \bar{z}$.

Aside: Abelian extensions (NON-EXAMINABLE)

Definition (Abelian extension)

An Abelian extension is a Galois extension whose Galois group is Abelian.

So cyclotomic fields are Abelian extensions of $\mathbb{Q}$.

Suppose $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(\zeta_N)$.
Then E corresponds to $H \leqslant G = \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$.
Since G is Abelian, H is automatically normal; so $E/\mathbb{Q}$ is Galois and $\mathrm{Gal}(E/\mathbb{Q}) \simeq G/H$ is still Abelian. Conversely,

Theorem (Kronecker-Weber)

If K is an Abelian extension of $\mathbb{Q}$, then there exists $N \in \mathbb{N}$ such that $K \subseteq \mathbb{Q}(\zeta_N)$.

Example

For all $n \in \mathbb{Z}$, $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\zeta_{4n})$.

Example: $N = 9$

Let $L = \mathbb{Q}(\zeta_9)$, $G = \mathrm{Gal}(L/\mathbb{Q})$.
The min poly of ζ_9 is $\Phi_9(x) = x^6 + x^3 + 1$.
$[L : \mathbb{Q}] = 6 = \phi(9)$, $G \simeq (\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, -4, -2, -1\}$.
We observe that $(\mathbb{Z}/9\mathbb{Z})^\times$ is cyclic, generated by 2.

$$\begin{array}{ccccc} \mathbb{Z}/6\mathbb{Z} & \overset{\sim}{\longleftrightarrow} & (\mathbb{Z}/9\mathbb{Z})^\times & \overset{\sim}{\longleftrightarrow} & G \\ m & \longleftrightarrow & 2^m & \longleftrightarrow & \sigma_{2^m} \end{array}$$

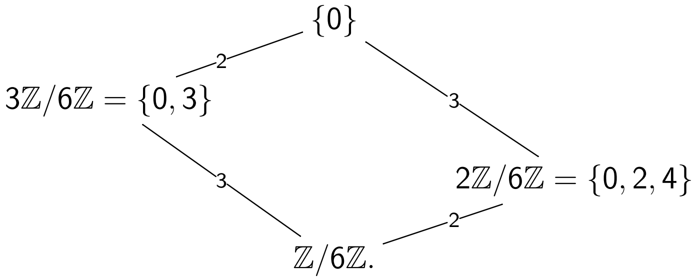
Example: $N = 9$

Let $L = \mathbb{Q}(\zeta_9)$, $G = \mathrm{Gal}(L/\mathbb{Q})$.
The min poly of ζ_9 is $\Phi_9(x) = x^6 + x^3 + 1$.
$[L : \mathbb{Q}] = 6 = \phi(9)$, $G \simeq (\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, -4, -2, -1\}$.
We observe that $(\mathbb{Z}/9\mathbb{Z})^\times$ is cyclic, generated by 2.

$$\mathbb{Z}/6\mathbb{Z} \overset{\sim}{\longleftrightarrow} (\mathbb{Z}/9\mathbb{Z})^\times \overset{\sim}{\longleftrightarrow} G$$

$$m \longleftrightarrow 2^m \longleftrightarrow \sigma_{2^m}$$

Subgroup diagram:



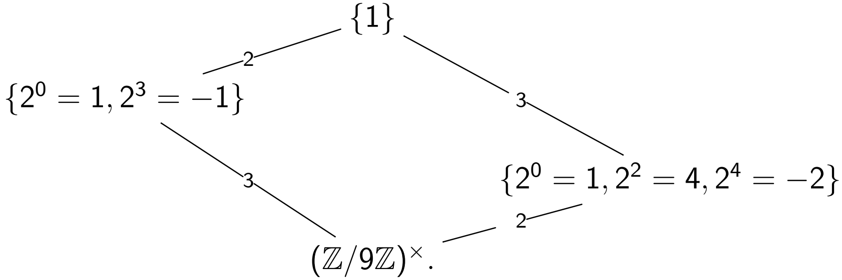
Example: $N = 9$

Let $L = \mathbb{Q}(\zeta_9)$, $G = \mathrm{Gal}(L/\mathbb{Q})$.
The min poly of ζ_9 is $\Phi_9(x) = x^6 + x^3 + 1$.
$[L : \mathbb{Q}] = 6 = \phi(9)$, $G \simeq (\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, -4, -2, -1\}$.
We observe that $(\mathbb{Z}/9\mathbb{Z})^\times$ is cyclic, generated by 2.

$$\mathbb{Z}/6\mathbb{Z} \overset{\sim}{\longleftrightarrow} (\mathbb{Z}/9\mathbb{Z})^\times \overset{\sim}{\longleftrightarrow} G$$

$$m \longleftrightarrow 2^m \longleftrightarrow \sigma_{2^m}$$

Subgroup diagram:

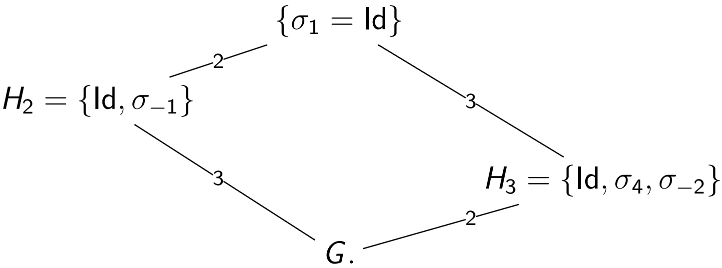


Example: $N = 9$

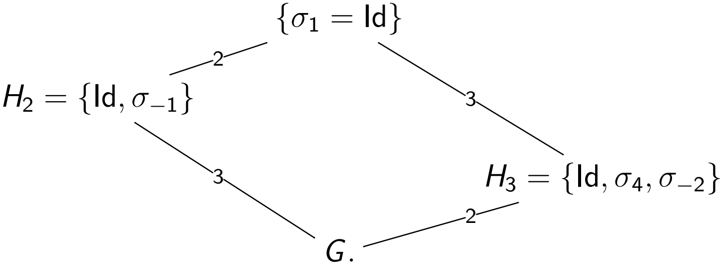
Let $L = \mathbb{Q}(\zeta_9)$, $G = \mathrm{Gal}(L/\mathbb{Q})$.
The min poly of ζ_9 is $\Phi_9(x) = x^6 + x^3 + 1$.
$[L : \mathbb{Q}] = 6 = \phi(9)$, $G \simeq (\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, -4, -2, -1\}$.
We observe that $(\mathbb{Z}/9\mathbb{Z})^\times$ is cyclic, generated by 2.

$$\begin{array}{ccccc} \mathbb{Z}/6\mathbb{Z} & \overset{\sim}{\longleftrightarrow} & (\mathbb{Z}/9\mathbb{Z})^\times & \overset{\sim}{\longleftrightarrow} & G \\ m & \longleftrightarrow & 2^m & \longleftrightarrow & \sigma_{2^m} \end{array}$$

Subgroup diagram:



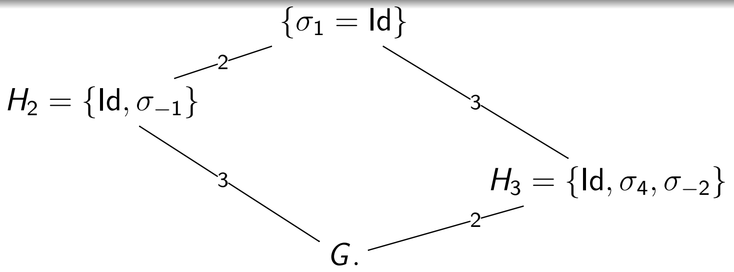
Example: $N = 9$



$L^{H_3} \ni \zeta_9 + \zeta_9^4 + \zeta_9^{-2} = \frac{\zeta_9^3 + \zeta_9^6 + 1}{\zeta_9^2} = 0$, useless.
But also $L^{H_3} \ni \zeta_9 \zeta_9^4 \zeta_9^{-2} = \zeta_9^3 = \zeta_3$, so $\mathbb{Q}(\zeta_3) \subseteq L^{H_3}$.

$[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = \phi(3) = 2 = [G : H_3] = [L^{H_3} : \mathbb{Q}]$,
so $L^{H_3} = \mathbb{Q}(\zeta_3)$.

Example: $N = 9$



$L^{H_2} = L \cap \mathbb{R}$ since σ_{-1} is complex conjugation.

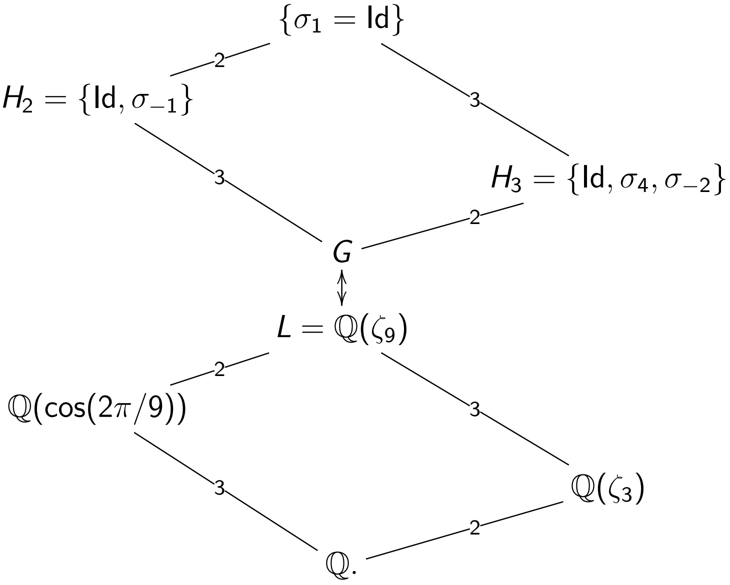
$L^{H_2} \ni \zeta_9 \zeta_9^{-1} = 1$ and $\alpha = \zeta_9 + \zeta_9^{-1} = 2\cos(2\pi/9)$,
whose conjugates are $\alpha = \sigma_{\pm 1}(\alpha)$,

$$\beta = \sigma_{\pm 2}(\alpha) = \zeta_9^2 + \zeta_9^{-2} = 2\cos(4\pi/9),$$
$$\text{and } \gamma = \sigma_{\pm 4}(\alpha) = \zeta_9^4 + \zeta_9^{-4} = 2\cos(8\pi/9).$$

α, β, γ distinct, so $\alpha \notin L^G = \mathbb{Q}$, so $\mathbb{Q} \subsetneq \mathbb{Q}(\alpha) \subseteq L^{H_2}$.

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg_{\mathbb{Q}} \alpha = \#\text{conjs} = 3 = [G : H_2] = [L^{H_2} : \mathbb{Q}]$
$\rightsquigarrow L^{H_2} = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = \mathbb{Q}(\gamma)$.

Example: $N = 9$


$\{\sigma_1 = \mathrm{Id}\}$
$H_2 = \{\mathrm{Id}, \sigma_{-1}\}$
$H_3 = \{\mathrm{Id}, \sigma_4, \sigma_{-2}\}$
G
$L = \mathbb{Q}(\zeta_9)$
$\mathbb{Q}(\cos(2\pi/9))$
$\mathbb{Q}(\zeta_3)$
$\mathbb{Q}.$
2
3
3
2
2
3
3
2

Example: $N = 9$

The min poly of α over $\mathbb{Q}$ is

$$P(x) = \prod_{c \in G \cdot \alpha} (x - c) = (x - \alpha)(x - \beta)(x - \gamma).$$

Its coefficients are combinations of powers of ζ_9 which lie in $\mathbb{Q}$
$\rightsquigarrow$ fixed by G
$\rightsquigarrow$ symmetric in roots of $\Phi_9(x) = x^6 + x^3 + 1$
$\rightsquigarrow$ computable by Vieta.

One finds $P(x) = x^3 - 3x + 1$.

Other applications (NON-EXAMINABLE)

Constructible numbers

Theorem (Wantzel)

$\alpha \in \mathbb{R}$ *is constructible* $\iff$ *there exist fields*

$$\mathbb{Q} = E_0 \subset \cdots \subset E_r = \mathbb{Q}(\alpha)$$

such that $[E_{j+1} : E_j] = 2$ *for all* j*.*

Corollary

α *constructible* $\Rightarrow$ α *alg.* $/\,\mathbb{Q}$ *and* $[\mathbb{Q}(\alpha) : \mathbb{Q}] =$ *power of 2.*

Counter-example

Let $\alpha \in \mathbb{R}$ root of $f(x) = x^4 - 8x^2 + 4x + 2 \in \mathbb{Q}[x]$.
$f(x)$ irr $/\,\mathbb{Q}$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$; yet α not constructible!
Indeed, let $N = \mathbb{Q}(\alpha_1, \cdots, \alpha_4)$ where α_j roots of $f(x)$. Then $G = \mathrm{Gal}(N/\mathbb{Q}) \leqslant S_4$, and $\mathbb{Q}(\alpha) \subset N$ corresponds to $G_\alpha \leqslant G$.
It turns out that $G = S_4$, so $G_\alpha = \{\mathrm{Id}\} \times S_3 \leqslant S_4$. Since there is no $G_\alpha < H < G$, there is no $\mathbb{Q} \subsetneq E \subsetneq \mathbb{Q}(\alpha)$.

Constructible numbers vs. 2-groups

Definition

Let $p \in \mathbb{N}$ be prime. A p-group is a finite group G such that $\#G$ is a power of p.

Proposition

If G is a p-group, then there exist

$$\{1_G\} = H_0 < \cdots < H_r = G$$

such that $[H_{j+1} : H_j] = p$ for all j.

Theorem

Let $\alpha \in \mathbb{R}$ alg./$\mathbb{Q}$, and N = Galois closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$. Then

$$\alpha \textit{ is constructible} \iff \mathrm{Gal}(N/\mathbb{Q}) \textit{ is a 2-group.}$$

Finiteness of subextensions

Proposition

If L/K is a finite <u>*separable*</u> *extension,*
then the number of $K \subseteq E \subseteq L$ is finite.

Proof.

Let $N =$ normal closure of L/K. Then N/K is finite Galois, so $G = \text{Gal}(N/K)$ is finite, so there are finitely many $H \leqslant G$, whence finitely many $K \subseteq E \subseteq N$. □

A vector space lemma

Lemma

Let K be a field, and V a vector space over K.
If $V = \bigcup_{j=1}^{r} W_j$ with $W_j \subsetneq V$ subspaces, then K is finite.

Proof.

WLOG there exists $v \in V \setminus \bigcup_{j=1}^{r-1} W_j$, in particular $v \in W_r$.
Let also $a \in V \setminus W_r$, and $L = \{a + \lambda v \mid \lambda \in K\}$.

If $p = a + \lambda v \in L \cap W_r$, then $a = p - \lambda v \in W_r$, absurd.
So $L \cap W_r = \emptyset$.

If $p = a + \lambda v$, $q = a + \mu v \in L \cap W_j$ for $j < r$, then
$(\mu - \lambda)v = q - p \in W_j$, so $p = q \rightsquigarrow \#(L \cap W_j) \leqslant 1$.

As $L = L \cap V = \bigcup_{j=1}^{r}(L \cap W_j)$, $\#K = \#L \leqslant r - 1$. □

The primitive element theorem

Theorem (Primitive element theorem)

Let L/K be a finite separable extension. There exists a *primitive element* $\gamma \in L$*, i.e. such that* $L = K(\gamma)$.

Proof.

If K finite, OK. Suppose K infinite.
$L = \bigcup_{\alpha \in L} K(\alpha)$. This is actually a finite union, since there are finitely many $K \subseteq E \subseteq L$. Apply lemma. □

Example

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(x\sqrt{2} + y\sqrt{3}) \text{ for all } 0 \neq x, y \in \mathbb{Q}.$$

An inseparable counterexample

Counter-example

Let $L = k(s,t)$ where char $k = p$, and $K = k(s^p, t^p)$.
$[L : K] = p^2$, because $K \subset k(s, t^p) = K(s) \subset L$.

For all $\alpha = f(s,t) \in L$, $a = \alpha^p = \operatorname{Frob} \alpha \in k^p(s^p, t^p) \subseteq K$, so α root of $x^p - a \in K[x]$, so $[K(\alpha) : K] \leqslant p$, so $L \supsetneq K(\alpha)$.

For $\lambda \in k$, let $E_\lambda = K(s + \lambda t)$. If $E_\lambda = E_\mu$ for $\lambda \neq \mu$, then $s + \mu t \in K(s + \lambda t)$, so $t = \frac{(s+\mu t)-(s+\lambda t)}{\mu - \lambda} \in K(s+\lambda t)$ and $s = (s + \lambda t) - \lambda t \in K(s + \lambda t)$, so $L = K(s,t) = K(s + \lambda t)$, absurd.
$\rightsquigarrow$ If $\#k = \infty$, e.g. $k = \mathbb{F}_p(u)$, that's ∞ many $K \subset E_\lambda \subset L$.