Infinite Galois Theory

June 8, 2020

Outline

- Infinite Galois extensions, failure and rescue of Galois correspondence
- Examples
- Some theorems making essential use of infinite Galois groups.

Classical Galois Theory (Review)

Let L/K be a finite extension of fields: $[L : K] = \dim_K(L) < \infty$.

All $\alpha \in L$ algebraic over K: $f(\alpha) = 0$ for nonzero $f(X) \in K[X]$,

A *K-automorphism* of L is a field isomorphism $L \xrightarrow{\sigma} L$ fixing K.

$\sigma(\alpha) = \alpha$ for $\alpha \in K$

Example. $\mathrm{Aut}(\mathbf{C}/\mathbf{R}) = \{z \mapsto z,\ z \mapsto \overline{z}\}$

Example. $\mathrm{Aut}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}) = \{\alpha \mapsto \alpha\}$.

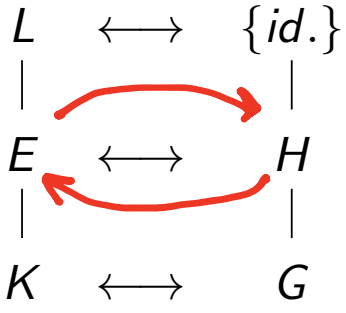
The group $\mathrm{Aut}(L/K)$ is finite with size $\leq [L : K]$.

Theorem. The following conditions are equivalent:
(1) $|\mathrm{Aut}(L/K)| = [L : K]$,
(2) L is splitting field over K of a separable polynomial in $K[X]$.
(3) The only elements of L fixed by $\mathrm{Aut}(L/K)$ are in K.
(4) L/K is separable and normal.

When this happens, call L/K a *Galois* extension and write $\mathrm{Aut}(L/K)$ as $\mathrm{Gal}(L/K)$. (Please don't use "Gal" in other cases.)

Classical Galois Correspondence (Review)

Let L/K be Galois, $G = \mathrm{Gal}(L/K)$.



L/K Galois means $L^G = K$

$\{\sigma \in G : \sigma(\alpha) = \alpha \ \forall \alpha \in E\}$

Galois correspondence

$$E \rightsquigarrow \mathrm{Gal}(L/E), \quad H \rightsquigarrow L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$$

(1) $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q}) \cong (\mathbf{Z}/m\mathbf{Z})^\times$ by $\sigma_a(\zeta_m) = \zeta_m^a$ for $(a, m) = 1$

$\overline{\zeta_m} = \zeta_m^{-1}$

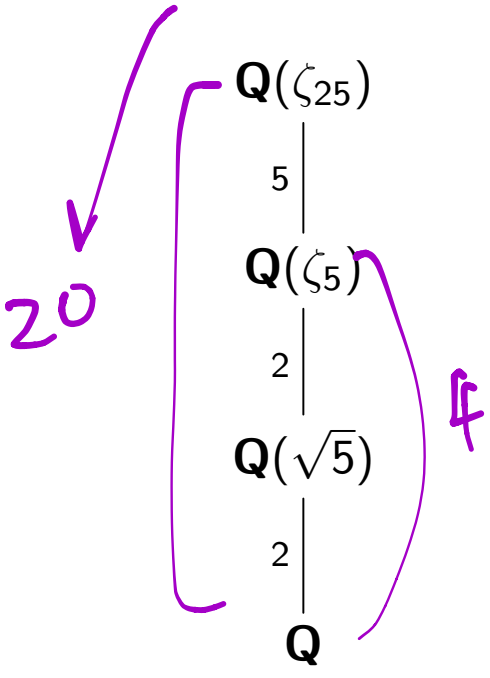
(2) For prime $p > 2$,

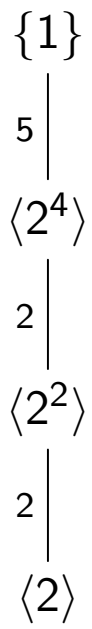
$$\mathrm{Gal}(\mathbf{Q}(\sqrt[p]{2}, \zeta_p)/\mathbf{Q}) \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbf{Z}/p\mathbf{Z})^\times, b \in \mathbf{Z}/p\mathbf{Z} \right\},$$

where $\sigma_{a,b}(\zeta_p) = \zeta_p^a$, $\sigma_{a,b}(\sqrt[p]{2}) = \zeta_p^b \sqrt[p]{2}$.

A 5-Power Cyclotomic Example (Review)

$[\mathbf{Q}(\zeta_{25}) : \mathbf{Q}] = \varphi(25) = 4 \cdot 5, \quad \mathrm{Gal}(\mathbf{Q}(\zeta_{25})/\mathbf{Q}) \cong (\mathbf{Z}/25\mathbf{Z})^\times = \langle 2 \rangle.$





$\sigma_a(\zeta_{25}) = \zeta_{25}^a$ for $a \in (\mathbb{Z}/25)^*$.

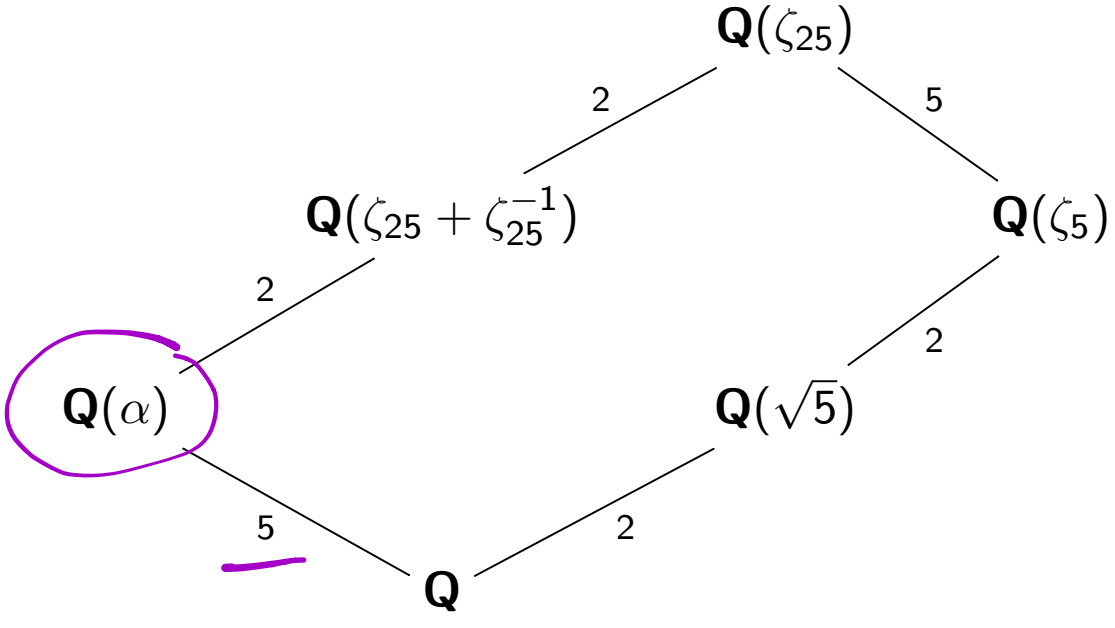
Can find extension $\mathbf{Q}(\alpha)/\mathbf{Q}$ of degree 5 as fixed field of a subgroup of order 4.

$7^2 \equiv -1 \pmod{25}$

Since 2 mod 25 has order 20, $2^5 = 32 = 7$ mod 25 has order 4.
This suggests trying $\alpha = \zeta_{25} + \zeta_{25}^7 + \zeta_{25}^{7^2} + \zeta_{25}^{7^3} \ldots$

A 5-Power Cyclotomic Example (Review)

For $\alpha = \zeta_{25} + \zeta_{25}^{7} + \zeta_{25}^{7^2} + \zeta_{25}^{7^3}$, Galois theory predicts α has degree 5 over $\mathbf{Q}$. PARI-GP says minimal polynomial of α over $\mathbf{Q}$ is $X^5 - 10X^3 + 5X^2 + 10X + 1$.



Now allow $[L : K] = \infty$, keeping L/K algebraic: each $\alpha \in L$ is the root of a nonzero polynomial in $K[X]$.

Examples. Taking $K = \mathbf{Q}$, here are some L:

$$\mathbf{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \dots),$$

$$\mathbf{Q}(\zeta_{p^\infty}) = \bigcup_{n \geq 1} \mathbf{Q}(\zeta_{p^n}) \quad (p \text{ prime})$$

$$\bigcup_{n \geq 1} \mathbf{Q}(\sqrt[n]{2}) \subset \mathbf{R}$$

$$\overline{\mathbf{Q}} = \text{ all algebraic numbers (in } \mathbf{C})$$

Built-in finiteness: each finite set of elements of L is in a finite subextension of K.

First description of Galois extn. for finite degree makes no sense for infinite deg., but other descriptions make sense and agree.

Defining Infinite Galois Group, First Example

The following conditions on an algebraic extension L/K (perhaps of infinite degree) are equivalent and they define what it means for L/K to be Galois.

Theorem. The following conditions are equivalent:
(1) $L = \bigcup_i L_i$, with each L_i/K a finite Galois extension,
(2) L/K is splitting field of set of separable polynomials in $K[X]$,
(3) The only elements of L fixed by $\mathrm{Aut}(L/K)$ are in K.
(4) L/K is separable and normal.

Examples on previous slide are Galois over $\mathbf{Q}$ except $\bigcup_n \mathbf{Q}(\sqrt[n]{2})$.

Let L/K be Galois, maybe $[L : K] = \infty$. Define, *exactly* as before,

$$\mathrm{Gal}(L/K) = \{\text{field automorphisms of } L \text{ fixing all of } K\}.$$

effect of σ on $\sqrt{1}$, $\sqrt{2}$, $\sqrt{3}$, ⋮

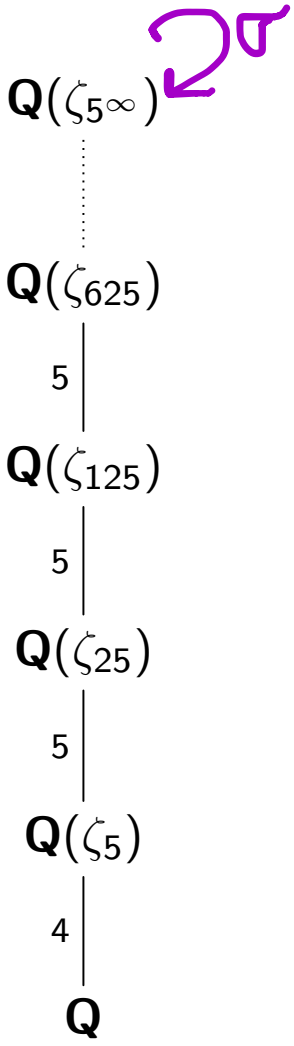
Example.

$$\mathrm{Gal}(\mathbf{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \dots)/\mathbf{Q}) = \{\pm 1\} \times \prod_p \{\pm 1\}.$$

Why is $\bigcup_{n\geq 1} \mathbb{Q}(\sqrt[n]{2})$ not Galois over $\mathbb{Q}$?

It's inside $\mathbb{R}$ and $\sqrt[n]{2}$ is in the field but nonreal n^{th} roots of 2 are not for $n \geq 3$.

Second Example: Full 5-Power Cyclotomic Extension



$\sigma(\zeta_{625}) = \zeta_{625}^{c}$, $c \equiv b \bmod 125$

$\sigma(\zeta_{125}) = \zeta_{125}^{b}$, $b \equiv a \bmod 25$, $a \equiv 2 \pmod 5$

$\sigma(\zeta_{25}) = \begin{cases} \zeta_{25}, \zeta_{25}^{5} \\ \zeta_{25}^{7}, \zeta_{25}^{17} \\ \zeta_{25}^{22} \end{cases}$ / $\zeta_{25}^{5} = \zeta_5$

$= \zeta_{25}^{a}$

$\Rightarrow \sigma(\zeta_{25}^{5}) = \zeta_5^{2}$

$\sigma(\zeta_{25})^5 = \zeta_5^2$

$\sigma(\zeta_5) = \zeta_5^2$

Choose this

So if $\sigma(\zeta_{25}) = \zeta_{25}^{a}$ then $(\zeta_{25}^{a})^5 = \zeta_5^2 \Rightarrow a \equiv 2 \bmod 5$

$\zeta_{5^n} = e^{2\pi i/5^n}$

Second Example: Full 5-Power Cyclotomic Extension

The elements of $\mathrm{Gal}(\mathbf{Q}(\zeta_{5^\infty})/\mathbf{Q})$ can be thought of as sequences $(a_n \bmod 5^n)_{n\geq 1}$ with $a_n \not\equiv 0 \bmod 5$ for all n fitting the *consistency condition*

$$a_n \equiv a_{n-1} \bmod 5^{n-1},$$

which makes the first condition the same as $a_1 \not\equiv 0 \bmod 5$: these are the invertible 5-adic integers (5-adic units).

Example. A particular invertible 5-adic integer could be written as

$$2 \bmod 5 \longleftarrow 2 + 5 \bmod 5^2 \longleftarrow 2 + 5 + 3 \cdot 5^2 \bmod 5^3 \longleftarrow \cdots$$

or more simply as a "power series in 5": $2 + 5 + 3 \cdot 5^2 + \cdots$.

All 5-adic units – and 5-adic integers – act on all ζ_{5^n} as exponents:

$$\zeta_{25}^{2+5+3\cdot 5^2+\cdots} = \zeta_{25}^2 \zeta_{25}^5 \cdot 1 \cdot 1 \cdots = \zeta_{25}^7.$$

In $\mathbf{Z}_2$, for $a = c_0 + 2c_1 + 2^2 c_2 + \cdots$, find $(-1)^a$ and i^a:

$$(-1)^q = (-1)^{c_0}(-1)^{2c_1}(-1)^{4c_2}\cdots = (-1)^{c_0}$$

$$q^a = q^{c_0}\, q^{2c_1}\, q^{4c_2}\, q^{8c_3}\cdots = q^{c_0+2c_1}$$

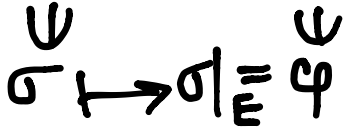
"Constructing" Elements of Infinite Galois Groups

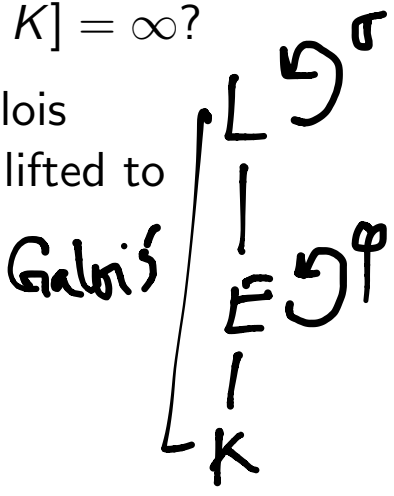
How do you write down elements of $\mathrm{Gal}(L/K)$ if $[L:K] = \infty$?

Theorem. If L/K is Galois and E/K is a (finite) Galois subextension, then all elements of $\mathrm{Gal}(E/K)$ can be lifted to $\mathrm{Gal}(L/K)$: the restriction homomorphism

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$$

is onto.





Proof. Zorn's lemma (axiom of choice). See appendix to notes.

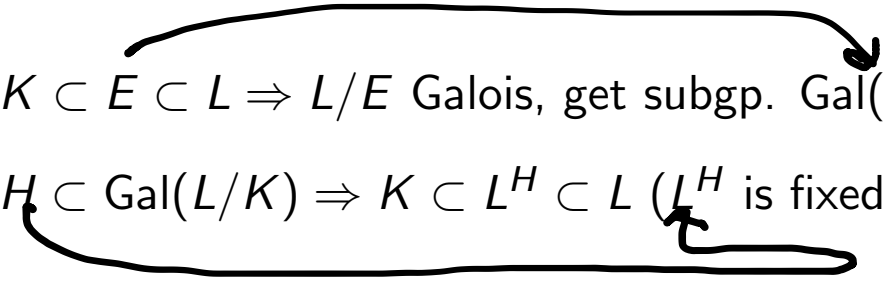
Example. The conjugation $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ in $\mathrm{Gal}(\mathbf{Q}(\sqrt{2})/\mathbf{Q})$ can be lifted to $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ in *many* ways.

Example. The automorphism in $\mathrm{Gal}(\mathbf{Q}(\zeta_{25})/\mathbf{Q})$ where $\zeta_{25} \mapsto \zeta_{25}^7$ can be lifted to $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ in *many* ways.

Note: In a finite Galois group, all automorphisms have finite order, but in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ there are *no* nonidentity elements of finite order except complex conjugation (on $\overline{\mathbf{Q}}$) and its conjugates of it.

Infinite-Degree Galois Correspondence

For an infinite-degree Galois extension L/K, both directions in the Galois correspondence ($E \rightsquigarrow \mathrm{Gal}(L/E)$, $H \rightsquigarrow L^H$) make sense.



- $K \subset E \subset L \Rightarrow L/E$ Galois, get subgp. $\mathrm{Gal}(L/E) \subset \mathrm{Gal}(L/K)$.
- $H \subset \mathrm{Gal}(L/K) \Rightarrow K \subset L^H \subset L$ (L^H is fixed field of H in L).

Field to subgroup to field: $E \rightsquigarrow \mathrm{Gal}(L/E) \rightsquigarrow L^{\mathrm{Gal}(L/E)} \stackrel{!}{=} E$. The containment $E \subset L^{\mathrm{Gal}(L/E)}$ is easy, the other way needs work: the lifting property from Zorn's lemma *and* finite Galois theory: see course notes, Theorem 4.7(3).

Subgroup to field to subgroup: $H \rightsquigarrow L^H \rightsquigarrow \mathrm{Gal}(L/L^H) \stackrel{?}{=} H$. The containment $H \subset \mathrm{Gal}(L/L^H)$ is easy, and the other way is true in finite Galois theory, but for infinite Galois theory it is *very false*: can have $H \neq H'$ in $\mathrm{Gal}(L/K)$ but $\mathrm{Gal}(L/L^H) = \mathrm{Gal}(L/L^{H'})$.

Example of Failure of Galois Correspondence

Let $L = \mathbf{Q}(\zeta_{2^\infty}) = \bigcup_{n \geq 1} \mathbf{Q}(\zeta_{2^n})$, with $L_n = \mathbf{Q}(\zeta_{2^n})$. Then

$$\mathrm{Gal}(L_n/\mathbf{Q}) \cong (\mathbf{Z}/2^n\mathbf{Z})^\times \text{ by } \sigma_a(\zeta_{2^n}) = \zeta_{2^n}^a.$$

$$\begin{array}{ccc} \mathbf{Q}(\zeta_{2^\infty}) & = & L \\ \vdots & & \\ \mathbf{Q}(\zeta_8) & & \\ | & & \\ \mathbf{Q}(\zeta_4) & = & \mathbf{Q}(i) \\ | & & \\ \mathbf{Q}(\zeta_2) & = & \mathbf{Q} \end{array}$$

Let $H = \langle \sigma_5 \rangle$ and $H' = \langle \sigma_{13} \rangle$. For $n \geq 1$,

$$\sigma_5(\zeta_{2^n}) = \zeta_{2^n}^5, \quad \sigma_{13}(\zeta_{2^n}) = \zeta_{2^n}^{13}.$$

Both H and H' are cyclic subgroups of $\mathrm{Gal}(L/\mathbf{Q})$. We have $H \neq H'$: if not then $\zeta_{2^n}^5 = \zeta_{2^n}^{13^{\pm 1}}$ for all n, so $5 \equiv 13^{\pm 1} \bmod 2^n$ for all n, so $5 = 13^{\pm 1}$: nonsense! (Or get contradiction using $n = 7$.)
However, it turns out that $L^H = L^{H'}$!

Example of Failure of Galois Correspondence (Contd.)

Let $L_n = \mathbf{Q}(\zeta_{2^n})$, so $\mathrm{Gal}(L_n/\mathbf{Q}) \cong (\mathbf{Z}/2^n\mathbf{Z})^\times$ by $\sigma_a(\zeta_{2^n}) = \zeta_{2^n}^a$.

$$\begin{array}{ccc} \mathbf{Q}(\zeta_{2^n}) & = & L_n \\ \vdots & & \\ \mathbf{Q}(\zeta_4) & = & \mathbf{Q}(i) \\ | & & \\ \mathbf{Q}(\zeta_2) & = & \mathbf{Q} \end{array}$$

Since $5 \equiv 1 \bmod 4$, $\sigma_5(i) = i$, so $\mathbf{Q}(i) \subset L^H$. Since $13 \equiv 1 \bmod 4$, also get $\mathbf{Q}(i) \subset L^{H'}$.

Fact: $\boxed{\text{for } n \geq 2, \langle 5 \bmod 2^n \rangle = \langle 13 \bmod 2^n \rangle \text{ in } (\mathbf{Z}/2^n\mathbf{Z})^\times}$.

By the *finite* Galois correspondence, $L_n^H = \mathbf{Q}(i)$ and $L_n^{H'} = \mathbf{Q}(i)$ for all $n \geq 2$, so $L^H = \mathbf{Q}(i) = L^{H'}$ while also $H \neq H'$.

What Happened?

Infinite Galois groups have *too many subgroups* for the Galois correspondence to be true with no constraints.

Dedekind (1901) discovered weird behavior in p-power cyclotomic fields and said Galois groups should be "continuous manifolds".

Krull (1928) defined a topology on $\mathrm{Gal}(L/K)$ with the following properties:

- multiplication and inversion on $\mathrm{Gal}(L/K)$ are continuous,
- the topology is compact, Hausdroff, and totally disconnected,
- for finite L/K the topology is discrete,
- if $K \subset E \subset L$ then $\mathrm{Gal}(L/E)$ is *closed* in $\mathrm{Gal}(L/K)$.
- for subgroups $H \subset \mathrm{Gal}(L/K)$, $L^H = L^{\overline{H}}$ and $\mathrm{Gal}(L/L^H) = \overline{H}$.

So $\mathrm{Gal}(L/L^H) = H$, as in finite Galois theory, if and only if H is closed. The Galois correspondence is a bijection between all the intermediate fields and closed subgroups.