Galois theory

Aurel Page

09/02/2022

Inria Bordeaux Sud-Ouest
CHARM Bootcamp

What is Galois theory about?

Original goal: characterise the solvability of equations by radicals.
Let $f \in \mathbb{Z}[X]$ be irreducible of degree n and $\alpha_1, \ldots, \alpha_n$ its roots.
Is there an expression for the α_i as iterated k-th roots?

Modern view: Can we construct a tower of fields

$$\mathbb{Q} \subset \mathbb{Q}(a_1^{1/k_1}) \subset \cdots \subset \mathbb{Q}(a_1^{1/k_1}, \ldots, a_m^{1/k_m}) = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$$

with $a_{i+1} \in \mathbb{Q}(a_1^{1/k_1}, \ldots, a_i^{1/k_i})$?
More generally, understand subfields and their inclusions.

Galois's solution: in terms of the symmetries of $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

More generally: study arithmetic properties of number fields in terms of their symmetries.

Plan

Fields

Setup

For simplicity, all the fields in this talk will have characteristic 0.
I will only present Galois theory of finite extensions.

Extensions and subfields

When we have an inclusion $F \subset K$ of fields, we say that

- K is an **extension** of F, or K/F is an extension (focus: F fixed and we think of K as varying over possible extensions).
- F is a **subfield** of K (focus: K fixed and we think of F as varying over possible subfields).
- K/F is **finite** if $\dim_F K < \infty$, of **degree** $[K : F] = \dim_F K$.

Examples:

- $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a finite extension.
- $\mathbb{Q}(\pi)/\mathbb{Q}$ is an infinite extension (π is transcendental).
- $\mathbb{Q}(\pi^2)$ is a subfield of $\mathbb{Q}(\pi)$.

Finite extensions

Let K/F be a finite extension, and let $a \in K$.
Let $m_a \colon x \mapsto ax \in \mathrm{End}_F(K)$.
Define

- the **trace** of a: $\mathrm{Tr}_{K/F}(a) = \mathrm{Tr}(m_a)$;
- the **norm** of a: $N_{K/F}(a) = \det(m_a)$;
- the **characteristic polynomial** of a: $\det(X\,\mathrm{Id}_K - m_a)$.

We have:

- $\mathrm{Tr}_{K/F} \colon K \to F$ is F-linear;
- $N_{K/F} \colon K \to F$ is multiplicative.

If $L/K/F$ are successive extensions, we have transitivity:

- $\mathrm{Tr}_{L/F} = \mathrm{Tr}_{K/F} \circ \mathrm{Tr}_{L/K}$;
- $N_{L/F} = N_{K/F} \circ N_{L/K}$;
- $[L : F] = [K : F][L : K]$.

Extensions of number fields: discriminants

Recall that a **number field** is a finite extension of $\mathbb{Q}$.
Let K/F be an extension of number fields, of discriminants Δ_F and Δ_K.
There is a notion of **relative discriminant** $\delta_{K/F}$, which is an ideal in $\mathbb{Z}_F$, such that

$$|\Delta_K| = |\Delta_F|^{[K:F]} N(\delta_{K/F}).$$

In particular we have $|\Delta_K| \geq |\Delta_F|^{[K:F]}$.
Define the **root discriminant** of K to be $\mathrm{rd}_K = |\Delta_K|^{1/[K:\mathbb{Q}]}$.
We have

$$\mathrm{rd}_F \leq \mathrm{rd}_K \,.$$

Extensions of number fields: ideals

Let K/F be an extension of number fields.

- If $\mathfrak{a}$ is a fractional ideal of F, its **extension** is $\mathfrak{a}\mathbb{Z}_K$. Induces an injective morphism $\mathrm{Ideals}_F \to \mathrm{Ideals}_K$.
- If $\mathfrak{A}$ is a fractional ideal of K, its **norm** is the ideal $N_{K/F}(\mathfrak{A})$ generated by the $N_{K/F}(a)$ for $a \in \mathfrak{A}$. Induces a morphism $\mathrm{Ideals}_K \to \mathrm{Ideals}_F$.
- We have $N_{K/F}(\mathfrak{a}\mathbb{Z}_K) = \mathfrak{a}^{[K:F]}$.
- On class groups, these induce an extension map $\mathrm{Cl}_F \to \mathrm{Cl}_K$ and a norm map $N_{K/F}\colon \mathrm{Cl}_K \to \mathrm{Cl}_F$.

Extension of number fields: prime ideals

Let K/F be an extension of number fields, and let $\mathfrak{p}$ be a prime ideal of F.

- We have $\mathfrak{p}\mathbb{Z}_K = \prod_i \mathfrak{P}_i^{e_i}$ for some prime ideals $\mathfrak{P}_i$ of Z_K. The integer e_i is the **ramification index** of $\mathfrak{P}_i$ over F.
- We have $\mathfrak{P}_i \cap F = \mathfrak{p}$.
- We have $N_{K/F}(\mathfrak{P}_i) = \mathfrak{p}^{f_i}$. The integer f_i is the **inertia degree** of $\mathfrak{P}_i$ over F.
- We have $\sum_i e_i f_i = [K : F]$.
- We say $\mathfrak{p}$ is **unramified** in K if all $e_i = 1$. Equivalently, $\mathfrak{p}$ does not divide $\delta_{K/F}$.

How do you construct extensions? I

Adjoining one element:

- By picking an element from a bigger field Ω: $K = F(\alpha)$ for some $\alpha \in \Omega$.
  Ex: from $\mathbb{Q} \subset \mathbb{C}$, construct $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\pi)$, ...
- Algebraically, by adjoining the root of a polynomial: $f \in F[X]$ being irreducible, $K = F[X]/(f(X)) = F(\alpha)$ where $\alpha = \overline{X}$ is an abstract root of f.
  Such an extension has degree $\deg f$.
  Ex: $\mathbb{Q}[X]/(X^2 - 2) = \mathbb{Q}(\sqrt{2})$.

Primitive element theorem

Theorem

Let K/F be a finite extension. Then there exists $\alpha \in K$ such that $K = F(\alpha)$.

Such an α is called a primitive element of K/F.

How do you construct extensions? II

Adjoining several elements:

- Pick several elements from Ω: $K = F(\alpha_1, \ldots, \alpha_m)$ for some $\alpha_i \in \Omega$.
  Ex: $\mathbb{Q}(\sqrt{2}, \pi)$.
- Algebraically, by specifying all relations:
  $K = F[X_1, \ldots, X_m]/(\text{relations}) = F(\alpha_1, \ldots, \alpha_m)$.
  Ex: $\mathbb{Q}[X_1, X_2]/(X_1^2 - 2, X_2^2 - 3) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
- Algebrically, by adjoining **all** roots of an irreducible $f \in F[X]$: $\widetilde{K} = F(\alpha_1, \ldots, \alpha_n)$ where $n = \deg f$.
  This is called the **splitting field** of f.

Splitting field examples

Let $f = x^4 - x^3 + 2x - 1$.
Let $K = \mathbb{Q}[X]/(f) = \mathbb{Q}(\alpha_1)$ of degree 4.
Over K, f factors as

$$f(X) = (X - \alpha_1) \cdot (X - \alpha_2) \cdot g(X)$$

where $\alpha_2 = -\alpha_1^3 - 1$ and $g = X^2 - (\alpha_1^3 - \alpha_1 + 2)X + \alpha_1^3 - \alpha_1 + 2$.

We can construct $\widetilde{K} = K[Y]/(g) = K(\alpha_3)$, and this field also contains the last root $\alpha_4 = 2 - 2\alpha_1 + \alpha_1^3 - \alpha_3$.

So $\widetilde{K} = K(\alpha_1)(\alpha_3) = K(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ is the splitting field of f.
It has degree $4 \cdot 2 = 8$ over $\mathbb{Q}$.

Splitting field examples

What is the "worst case" of this construction?

From $f \in F[X]$ of degree n, we construct

- $K_1 = F(\alpha_1)$, and over K_1 we have $f = (X - \alpha_1)f_1(X)$ where f_1 is irreducible of degree $n - 1$,
- $K_2 = K_1(\alpha_2)$, and $f = (X - \alpha_1)(X - \alpha_2)f_2(X)$ where $f_2 \in K_2[X]$ is irreducible of degree $n - 2$,
- $\ldots$
- $\widetilde{K} = K_n$ is the splitting field of f.

The degree of $\widetilde{K}/F$ is $n \cdot (n-1) \cdot (n-2) \cdots 1 = n!$.

Morphisms of fields

Let K, L be rings. A **morphism** is a map $\sigma\colon K \to L$ such that

- $\sigma(1) = 1$;
- σ is a morphism of additive groups;
- $\sigma(ab) = \sigma(a)\sigma(b)$ for all $a, b \in K$.

Fact: if K, L are fields, then σ is **injective.**
Proof: If $a \in \ker\sigma$ is such that $a \neq 0$,
then $1 = \sigma(1) = \sigma(a \cdot 1/a) = \sigma(a) \cdot \sigma(1/a) = 0$.

If in addition K/F and L/F are finite extensions and σ is F-linear, then σ is an **isomorphism** if and only if $[K : F] = [L : F]$.

How do you construct morphisms of fields?

Assume $K = F[X]/(f) = F(\alpha)$, and L/F is another extension, and we want to construct an F-linear morphism $\sigma\colon K \to L$.

- σ is completely determined by $\sigma(\alpha)$.
- We must have $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$.
- Let $\beta \in L$ be such that $f(\beta) = 0$. Then there exists a unique $\sigma\colon K \to L$ such that $\sigma(\alpha) = \beta$.

Proof: this is the only "field relation" satisfied by α. Formally, define $\sigma\colon F[X] \to L$ by $\sigma(X) = \beta$. Since for all $g \in F[X]$ we have $\sigma(fg) = f(\beta)g(\beta) = 0$, the map σ is trivial on the ideal (f) and therefore passes to the quotient.

How do you construct morphisms of fields?

Assume $K = F[X_1, \dots, X_m]/(\text{relations}) = F(\alpha_1, \dots, \alpha_m)$, and L/F is another extension, and we want to construct an F-linear morphism $\sigma\colon K \to L$.

- σ is completely determined by $\sigma(\alpha_1), \dots, \sigma(\alpha_m)$.
- We get a morphism iff the chosen images $\sigma(\alpha_1), \dots, \sigma(\alpha_m)$ satisfy all relations between the α_i.

Automorphisms

When K/F is a finite extension, a special role will be played by the group $\mathrm{Aut}_F(K)$ of **automorphisms** $K \to K$ that are F-linear.

If $K = F[X]/(f) = F(\alpha)$, these correspond exactly to roots of f over K. We don't have to check injectivity or surjectivity!

If $\widetilde{K} = F(\alpha_1, \ldots, \alpha_n)$ is the **splitting field** of f, then an automorphism σ must send each α_i to some α_j, and the images must all be distinct.
$\rightsquigarrow$ σ defines a **permutation** of $\alpha_1, \ldots, \alpha_n$.
$\mathrm{Aut}_F(K)$ is the set of permutations of the roots of f that preserves all relations between them.

Examples of automorphism groups

Let $K = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}[X]/(X^2 - 2)$.

Then $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$, so there is exactly one nontrivial automorphism $\sigma \colon \sqrt{2} \mapsto -\sqrt{2}$.

We have $\mathrm{Aut}_{\mathbb{Q}}(K) \cong C_2$.

Examples of automorphism groups

Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}[X, Y]/(X^2 - 2, Y^2 - 3)$.

There are four pairs of elements of K satisfying all the relations: $(\sqrt{2}, \sqrt{3})$, $(-\sqrt{2}, \sqrt{3})$, $(\sqrt{2}, -\sqrt{3})$ and $(-\sqrt{2}, -\sqrt{3})$, giving four automorphisms.

We have $\mathrm{Aut}_{\mathbb{Q}}(K) \cong C_2 \times C_2$.

Examples of automorphism groups

Let $f = x^4 - x^3 + 2x - 1$ and $K = \mathbb{Q}[X]/(f) = \mathbb{Q}(\alpha_1)$ as before.

As we saw, f had two roots α_1 and α_2 in K, giving two automorphisms: the identity, and one that swaps α_1 and α_2.

We have $\mathrm{Aut}_{\mathbb{Q}}(K) \cong C_2$.

Fixed fields

Let K/F be an extension and $H \subset \mathrm{Aut}_F(K)$ a subgroup. Define the **fixed field** of H to be

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

- By the morphism property, K^H is a subfield of K.
- By F-linearity, K^H contains F.

We now have a way of constructing subfields !

Galois theory

Galois extensions

Let K/F be a finite extension. We say that K/F is **Galois** (or **normal**) if the following equivalent properties hold:

1. $F = K^{\mathrm{Aut}_F(K)}$ (we always have $\subset$);
2. $|\mathrm{Aut}_F(K)| = [K : F]$ (we always have $\leq$);
3. every irreducible $g \in F[X]$ that has one root in K has all its roots in K;
4. K is the splitting field of some irreducible $f \in F[X]$.
5. K is the splitting field of some $f \in F[X]$.

When K/F is Galois, we define its **Galois group** to be

$$\mathrm{Gal}(K/F) = \mathrm{Aut}_F(K).$$

Warning

The "Galois group" of an irreducible polynomial $f \in F[X]$ is $\mathrm{Gal}(\widetilde{K}/F)$ where $\widetilde{K}$ is the splitting field of f. It is usually seen as a permutation group acting on the roots of f.

Example: multiquadratic fields

Let $K = \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_m})$ where $a_1, \dots, a_m \in \mathbb{Q}$ are multiplicatively independent up to squares.

Generalising what we saw earlier, $\mathrm{Aut}_{\mathbb{Q}}(K) \cong C_2^m$ is generated by the $\sigma_i \colon \sqrt{a_i} \mapsto -\sqrt{a_i}$ and leaving invariant the $\sqrt{a_j}$ for $j \neq i$.

We have $[K : \mathbb{Q}] = 2^m = |\mathrm{Aut}_{\mathbb{Q}}(K)|$ and $K/\mathbb{Q}$ is therefore a Galois extension!

Example: cyclotomic fields

Let $K = \mathbb{Q}(\zeta_m) = \mathbb{Q}[X]/(\Phi_m)$ be the m-th cyclotomic field, of degree $\phi(m)$.

The roots of Φ_m are exactly the primitive m-th roots of unity. The $\zeta_m^a \in K$ for $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ are $\phi(m)$ distinct such roots of unity, so K is the splitting field of Φ_m, so $K/\mathbb{Q}$ is Galois.

For $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, let σ_a be the automorphism of K that sends ζ_m to ζ_m^a.
The map $a \mapsto \sigma_a$ defines an isomorphism

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(K/\mathbb{Q}).$$

Galois closure

Fact: if K/F is a finite extension, then there exists a smallest $\widetilde{K}/K$ such that $\widetilde{K}/F$ is Galois.

Proof: write $K = F[X]/(f)$ for some irreducible f, and let $\widetilde{K}$ be the splitting field of f.

$\widetilde{K}/F$ is called the **Galois closure** (or **normal closure**) of K/F.

Example of Galois closure

Let $f = x^4 - x^3 + 2x - 1$ and $K = \mathbb{Q}[X]/(f) = \mathbb{Q}(\alpha_1)$ as before.

Recall $\alpha_2 \in K$ and $\widetilde{K} = K(\alpha_3)$ is the splitting field of K, so $\widetilde{K}/\mathbb{Q}$ is the Galois closure of $K/\mathbb{Q}$.

We know that $|\operatorname{Gal}(\widetilde{K}/\mathbb{Q})| = [\widetilde{K} : \mathbb{Q}] = 8$, so let's determine it.

Let $\sigma \in \operatorname{Gal}(\widetilde{K}/\mathbb{Q})$. Since $\widetilde{K} = \mathbb{Q}(\alpha_1, \alpha_3)$, σ is completely determined by its value on α_1 and α_3. At most 4 possible images for α_1. Choosing $\sigma(\alpha_1)$ forces $\sigma(\alpha_2) \rightsquigarrow$ at most 2 possible images for α_3. Total $4 \cdot 2 = 8$ possible pairs of images, but must have 8 automorphisms, so each possibility is an actual automorphism!

We have $\operatorname{Gal}(\widetilde{K}/\mathbb{Q}) \cong D_4$.

Example : a Kummer field

Let p be a prime and $a \in \mathbb{Q}^\times$ that is not a p-th power, and let $K = \mathbb{Q}(a^{1/p}) = \mathbb{Q}[X]/(X^p - a)$ of degree p.

Let $\widetilde{K}/\mathbb{Q}$ be the Galois closure of $K/\mathbb{Q}$. Then $\widetilde{K}$ contains two distinct p-th roots of a, so it contains a primitive p-th root of unity ζ_p. The elements $a^{1/p}, a^{1/p}\zeta_p, \dots, a^{1/p}\zeta_p^{p-1}$ are p distinct roots of $X^p - a$, so $\widetilde{K} = \mathbb{Q}(a^{1/p}, \zeta_p)$.

Let's determine $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$.

Example : a Kummer field

Since $\widetilde{K}$ contains K and $\mathbb{Q}(\zeta_p)$, we have $[\widetilde{K} : \mathbb{Q}] \geq p(p-1)$.

Let $\sigma \in \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$. We have $\sigma(\zeta_p) = \zeta_p^u$ for some $u \in \mathbb{F}_p^\times$ and $\sigma(a^{1/p}) = a^{1/p}\zeta_p^t$ for some $t \in \mathbb{F}_p$, so $|\mathrm{Gal}(\widetilde{K}/\mathbb{Q})| \leq p(p-1)$. So there must be equality, and all these possibilities define an automorphism $\sigma_{u,t}$!

We compute

- $\sigma_{v,s}\sigma_{u,t}(\zeta_p) = \sigma_{v,s}(\zeta_p^u) = \zeta_p^{vu}$, and
- $\sigma_{v,s}\sigma_{u,t}(a^{1/p}) = \sigma_{v,s}(a^{1/p}\zeta_p^t) = a^{1/p}\zeta_p^{vt+s}$.

So $\sigma_{v,s}\sigma_{u,t} = \sigma_{vu,vt+s}$, and $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ is isomorphic to the group of matrices $\begin{pmatrix} u & t \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$.

Example : S_n

Consider our "worst case" example f with $K_1 = F(\alpha_1)$ of degree n and $\widetilde{K} = F(\alpha_1, \ldots, \alpha_n)$ of degree $n!$.
The splitting field $\widetilde{K}$ is the Galois closure of K_1 over F.

Every automorphism of $\widetilde{K}/F$ defines a permutation of the n roots, giving an injection $\mathrm{Gal}(\widetilde{K}/F) \hookrightarrow S_n$. So we have $|\mathrm{Gal}(\widetilde{K}/F)| \leq n!$, and there must be equality!

We get $\mathrm{Gal}(\widetilde{K}/F) \cong S_n$.

Fundamental theorem of Galois theory

Theorem

Let K/F be a Galois extension of Galois group $G = \mathrm{Gal}(K/F)$. There is an inclusion-reversing bijection between

- *intermediate fields $F \subset L \subset K$, and*
- *subgroups H of G,*

given by

- $L \mapsto \mathrm{Aut}_L(K)$*, and*
- $H \mapsto K^H$*.*

Note: for every intermediate field $F \subset L \subset K$, the extension K/L is Galois, we have $\mathrm{Gal}(K/K^H) = H$ and $[K^H : F] = [G : H]$.

Fundamental theorem of Galois theory

$G = \mathrm{Gal}(K/F)$.

$$\begin{tikzcd}
1 \arrow[d, no head] & & K \arrow[d, no head] \arrow[d, bend left, no head, "H"] \\
H = \mathrm{Gal}(K/L) \arrow[d, no head] \arrow[rr, leftrightarrow] & & L = K^H \arrow[d, no head] \arrow[d, bend left, no head, "{[G:H]}"] \\
G & & F
\end{tikzcd}$$

Examples: Galois correspondence

Let $K = \mathbb{Q}(\zeta_9)$, Galois over $\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/9\mathbb{Z})^\times$.

The group $(\mathbb{Z}/9\mathbb{Z})^\times \cong C_6$ has two proper subgroups: $\langle -1 \rangle$ of order 2 and $\langle 4 \rangle$ of order 3.

The fixed field $K^{\langle -1 \rangle}$ is $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, and the fixed field $K^{\langle 4 \rangle}$ is $\mathbb{Q}(\zeta_9^3) = \mathbb{Q}(\zeta_3)$.

Examples: Galois correspondence

$$\begin{tikzcd}[column sep=small]
& 1 \arrow[dl, dash] \arrow[dr, dash] & \\
\langle -1 \rangle \arrow[dr, dash] & & \langle 4 \rangle \arrow[dl, dash] \\
& (\mathbb{Z}/9\mathbb{Z})^\times &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
& \mathbb{Q}(\zeta_9) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\zeta_9 + \zeta_9^{-1}) \arrow[dr, dash] & & \mathbb{Q}(\zeta_3) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

Examples: Galois correspondence

Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ with $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) = \langle \sigma_1, \sigma_2 \rangle \cong C_2 \times C_2$.

The group $C_2 \times C_2$ has exactly three proper subgroups, all of order 2: $\langle \sigma_1 \rangle$, $\langle \sigma_2 \rangle$ and $\langle \sigma_1 \sigma_2 \rangle$.

The corresponding subfields are $K^{\langle \sigma_1 \rangle} = \mathbb{Q}(\sqrt{3})$, $K^{\langle \sigma_2 \rangle} = \mathbb{Q}(\sqrt{2})$ and $K^{\langle \sigma_1 \sigma_2 \rangle} = \mathbb{Q}(\sqrt{6})$.

Examples: Galois correspondence

$$
\begin{tikzcd}
 & 1 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle \sigma_1 \rangle \arrow[dr, dash] & \langle \sigma_1\sigma_2 \rangle \arrow[d, dash] & \langle \sigma_2 \rangle \arrow[dl, dash] \\
 & \langle \sigma_1, \sigma_2 \rangle &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{3}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash] & \mathbb{Q}(\sqrt{2}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

Examples: Galois correspondence

Let $K = \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_m})$ as before, with $\mathrm{Gal}(K/\mathbb{Q}) \cong C_2^m \cong \mathbb{F}_2^m$.

The subgroups of $\mathbb{F}_2^m$ of index 2^k are exactly the $\mathbb{F}_2$-subspaces of dimension $m-k$ and there are approximately $2^{\binom{m}{k}}$ such subspaces. They correspond to subfields of K of degree 2^k, which are also multiquadratic.

Examples: Galois correspondence

Let $K = \mathbb{Q}(a^{1/p}) = \mathbb{Q}[X]/(X^p - a)$ and $\widetilde{K} = \mathbb{Q}(a^{1/p}, \zeta_p)$ as before, with $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \cong \begin{pmatrix} \mathbb{F}_p^\times & \mathbb{F}_p \\ 0 & 1 \end{pmatrix}$.

Let $H \subset \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ be a nontrivial subgroup.

- If H does not contain $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, then $H = \langle \begin{pmatrix} u & t \\ 0 & 1 \end{pmatrix} \rangle$ for some $u \in \mathbb{F}_p^\times$ and some $t \in \mathbb{F}_p$ with $u \neq 1$;
- otherwise $H = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix} \rangle$ for some $u \in \mathbb{F}_p^\times$.

Examples: Galois correspondence

Recall $\begin{pmatrix} u & t \\ 0 & 1 \end{pmatrix}$ acts by $\zeta_p \mapsto \zeta_p^u$ and $a^{1/p} \mapsto a^{1/p}\zeta_p^t$.

Let $u \in \mathbb{F}_p^\times$ have order d.

- The fixed field of $\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$ is $\mathbb{Q}(\zeta_p)$.
- The fixed field of $\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix} \rangle$ is the subfield $L \subset \mathbb{Q}(\zeta_p)$ with $[\mathbb{Q}(\zeta_p) : L] = d$.
- If $d \neq 1$, the fixed field of $\langle \begin{pmatrix} u & t \\ 0 & 1 \end{pmatrix} \rangle$ is $L(a^{1/p}\zeta_p^{t/(1-u)})$.

Examples: Galois correspondence

d = order of u in $\mathbb{F}_p^\times$.

$$
\begin{tikzcd}
1 \arrow[d, dash] \\
\langle \sigma_{u,t} \rangle \arrow[d, dash] \\
\langle \sigma_{1,1}, \sigma_{u,0} \rangle \arrow[d, dash] \\
\mathrm{Gal}(\widetilde{K}/\mathbb{Q})
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
\widetilde{K} \arrow[d, dash, "d"] \\
L(a^{1/p}\zeta_p^{t/(1-u)}) \arrow[d, dash, "p"] \\
L \arrow[d, dash, "\frac{p-1}{d}"] \\
\mathbb{Q}
\end{tikzcd}
$$

Examples: subgroup corresponding to a non-Galois field

Let $f = x^4 - x^3 + 2x - 1$ and $K = \mathbb{Q}[X]/(f) = \mathbb{Q}(\alpha_1)$ as before, with Galois closure $\widetilde{K} = K(\alpha_1, \alpha_3)$ and $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \cong D_4$.

Let's determine the subgroup $H = \mathrm{Gal}(\widetilde{K}/K)$ corresponding to K. It is the subgroup of automorphisms $\sigma \in \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ fixing α_1. Such an automorphism must also fix α_2, so there are only two possiblities: the identity and one automorphism that swaps $\alpha_3 \leftrightarrow \alpha_4$.

Geometrically, if we see D_4 as the symmetry group of the square, H is the group generated by one reflection: the one fixing the two vertices corresponding to α_1 and α_2.

Examples: subgroup corresponding to a non-Galois field

Let f, $K/\mathbb{Q}$ of degree n and $\widetilde{K}/\mathbb{Q}$ of degree $n!$
and $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \cong S_n$ be our "worst case" example.

Let's determine the subgroup $H = \mathrm{Gal}(\widetilde{K}/K)$ corresponding to K. It is the subgroup of automorphisms fixing α_1. This corresponds to the stabiliser of 1 in S_n, which is isomorphic to S_{n-1}.

Galois theory II

Aurel Page

02/03/2022

Inria Bordeaux Sud-Ouest
CHARM Bootcamp

Reminder : goal

Goal of Galois theory: study arithmetic properties of number fields (in particular subfields) in terms of their symmetries.

Reminder : morphisms of fields

- A field extension K/F can be represented $K = F(\alpha) = F[X]/(f(X))$ where $f \in F[X]$ is irreducible.
- A morphism of fields is always injective.
  If dimensions match it is always an isomorphism.
- (F-linear morphism $K \to L$) $\longleftrightarrow$ (root $\beta \in L$ of f).

Reminder : Galois extensions

Let K/F be a finite extension. We say that K/F is **Galois** (or **normal**) if the following equivalent properties hold:

1. $F = K^{\mathrm{Aut}_F(K)}$ (we always have $\subset$);
2. $|\mathrm{Aut}_F(K)| = [K : F]$ (we always have $\leq$);
3. every irreducible $g \in F[X]$ that has one root in K has all its roots in K;
4. K is the splitting field of some irreducible $f \in F[X]$.
5. K is the splitting field of some $f \in F[X]$.

When K/F is Galois, we define its **Galois group** to be

$$\mathrm{Gal}(K/F) = \mathrm{Aut}_F(K).$$

Reminder : example

Let $K = \mathbb{Q}(\zeta_m) = \mathbb{Q}[X]/(\Phi_m)$ be the m-th **cyclotomic field**, of degree $\phi(m)$.

K is the splitting field of Φ_m, so $K/\mathbb{Q}$ is Galois.

For $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, let σ_a be the automorphism of K that sends ζ_m to ζ_m^a.
The map $a \mapsto \sigma_a$ defines an isomorphism

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(K/\mathbb{Q}).$$

Reminder : Galois closure

The **Galois closure** of K/F is the smallest $\widetilde{K}/K$ such that $\widetilde{K}/F$ is Galois.

If $K = F[X]/(f(X))$ then the Galois closure $\widetilde{K}$ is the splitting field of f.

Reminder : example

Consider our "worst case" example f with $K_1 = F(\alpha_1)$ of degree n and $\widetilde{K} = F(\alpha_1, \ldots, \alpha_n)$ of degree $n!$.
The splitting field $\widetilde{K}$ is the Galois closure of K_1 over F.

Every automorphism of $\widetilde{K}/F$ defines a permutation of the n roots, inducing an isomorphism

$$\mathrm{Gal}(\widetilde{K}/F) \cong S_n.$$

Reminder : fundamental theorem of Galois theory

Theorem

Let K/F be a Galois extension of Galois group $G = \mathrm{Gal}(K/F)$. There is an inclusion-reversing bijection between

- *intermediate fields $F \subset L \subset K$, and*
- *subgroups H of G,*

given by

- $L \mapsto \mathrm{Aut}_L(K)$*, and*
- $H \mapsto K^H$.

Note: for every intermediate field $F \subset L \subset K$, the extension K/L is Galois, we have $\mathrm{Gal}(K/K^H) = H$ and $[K^H : F] = [G : H]$.

Reminder: fundamental theorem of Galois theory

$G = \mathrm{Gal}(K/F)$.

$$
\begin{tikzcd}
1 \arrow[d, dash] & & K \arrow[d, dash] \arrow[d, bend left, phantom, "H"] \\
H = \mathrm{Gal}(K/L) \arrow[d, dash] \arrow[r, leftrightarrow] & & L = K^H \arrow[d, dash] \arrow[d, bend left, phantom, "{[G:H]}"] \\
G & & F
\end{tikzcd}
$$

Reminder: example

Let $K = \mathbb{Q}(2^{1/3}) = \mathbb{Q}[X]/(X^3 - 2)$ and $\widetilde{K} = \mathbb{Q}(2^{1/3}, \zeta_3)$, with

$$\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \cong \begin{pmatrix} \mathbb{F}_3^\times & \mathbb{F}_3 \\ 0 & 1 \end{pmatrix} \cong S_3,$$

where $\sigma_{u,t} = \begin{pmatrix} u & t \\ 0 & 1 \end{pmatrix}$ acts by $\zeta_3 \mapsto \zeta_3^u$ and $2^{1/3} \mapsto 2^{1/3}\zeta_3^t$.

Reminder: example

$$\sigma_{u,t} \colon \zeta_3 \mapsto \zeta_3^u, \; 2^{1/3} \mapsto 2^{1/3}\zeta_3^t.$$

$$\begin{tikzcd}[column sep=small]
 & 1 \arrow[dl, dash] \arrow[dr, dash] & \\
\langle \sigma_{1,1} \rangle \arrow[dr, dash] & & \langle \sigma_{-1,-t} \rangle \arrow[dl, dash] \\
 & \mathrm{Gal}(\widetilde{K}/\mathbb{Q}) &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(2^{1/3}, \zeta_3) \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\zeta_3) \arrow[dr, dash, "2"'] & & \mathbb{Q}(2^{1/3}\zeta_3^t) \arrow[dl, dash, "3"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Plan

1. Fields
2. Galois theory
3. Properties of Galois extensions
4. Cyclotomic fields
5. Class field theory

Subfields of a non-Galois extension

Galois theory also determines the intermediate fields of a non-Galois extension.

Let K/F be a finite extension and $\widetilde{K}/F$ be its Galois closure with $G = \mathrm{Gal}(\widetilde{K}/F)$. Let $H_0 = \mathrm{Gal}(\widetilde{K}/K)$ be the subgroup corresponding to K.

By the inclusion-reversing property, the intermediate fields $F \subset L \subset K$ correspond to subgroups H of G that contain H_0.

Subfields of a non-Galois extension

$$G = \mathrm{Gal}(\widetilde{K}/F).$$

$$\begin{tikzcd}
1 \arrow[d, dash] & & \widetilde{K} \arrow[d, dash] \arrow[d, dash, bend left, "H_0"] \arrow[dd, dash, bend left=60, "H"] \\
H_0 = \mathrm{Gal}(\widetilde{K}/K) \arrow[d, dash] & & K \arrow[d, dash] \\
H = \mathrm{Gal}(\widetilde{K}/L) \arrow[d, dash] \arrow[r, leftrightarrow] & & L = \widetilde{K}^H \arrow[d, dash] \arrow[d, dash, bend left, "{[G{:}H]}"] \\
G & & F
\end{tikzcd}$$

Example: subfields of a non-Galois extension

Let f, $K/\mathbb{Q}$ of degree n and $\widetilde{K}/\mathbb{Q}$ of degree $n!$
and $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \cong S_n$ be our "worst case" example.

We can check that there are no subgroups $H \subset S_n$ strictly between $H_0 = S_{n-1}$ and S_n. Therefore, there are no proper intermediate fields $F \subset L \subset K$.

When is an intermediate field Galois?

Let K/F be a Galois extension with Galois group $G = \mathrm{Gal}(K/F)$, and let $L = K^H$ correspond to a subgroup $H = \mathrm{Gal}(K/L)$. When is L/F Galois?

Write $L = F[X]/(f) = F(\alpha)$.
Let $\sigma \in G$. Then $\sigma(L) = F(\sigma(\alpha))$ is another sufield of K, corresponding to the subgroup $\sigma H \sigma^{-1}$.

- If $\sigma(L) \neq L$ then $\sigma(\alpha) \notin L$: L/F is not Galois.
- If $\sigma(L) = L$ for all $\sigma \in G$, then all roots of f are in L so L/F is Galois.

Therefore, L/F is Galois iff $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$, iff H is a **normal subgroup** of G. In this case, we have $\mathrm{Gal}(L/F) = G/H$.

When is an intermediate field Galois?

$G = \mathrm{Gal}(K/F)$ and H a subgroup of G.

$$\begin{array}{ccc}
1 & & K \\
| & & |\ \Big)\ H{=}\mathrm{Gal}(K/L) \\
H & \longleftrightarrow & L = K^H \\
| & & |\ \Big)\ [G{:}H] \\
G & & F
\end{array}$$

When is an intermediate field Galois?

$G = \mathrm{Gal}(K/F)$ and H a **normal** subgroup of G.

$$\begin{tikzcd} 1 \arrow[d, dash] & & K \arrow[d, dash, "H=\mathrm{Gal}(K/L)"] \\ H \arrow[d, dash] & \longleftrightarrow & L = K^H \arrow[d, dash, "G/H=\mathrm{Gal}(L/F)"] \\ G & & F \end{tikzcd}$$

When is an intermediate field Galois?

As a special case, if $\mathrm{Gal}(K/F)$ is an abelian group, then all the intermediate extensions L/F are Galois !

Example of non-Galois intermediate fields

$$K = \mathbb{Q}(2^{1/3}) = F[X]/(X^3 - 2) \text{ and } \widetilde{K} = \mathbb{Q}(2^{1/3}, \zeta_3).$$

$$\begin{tikzcd}
1 \arrow[d, dash] \\
\langle \sigma_{-1,-t} \rangle \arrow[d, dash] \arrow[d, phantom, shift left=6ex, "\text{not normal}"] \\
\mathrm{Gal}(\widetilde{K}/\mathbb{Q})
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
\widetilde{K} \arrow[d, dash, "\mathbb{F}_3^\times"] \\
\mathbb{Q}(2^{1/3}\zeta_3^t) \arrow[d, dash, "3"] \arrow[d, bend left, dash, "\text{not Galois}"] \\
\mathbb{Q}
\end{tikzcd}$$

Automorphisms of a subfield

Let K/F be an extension with Galois closure $\widetilde{K}$, and $G = \mathrm{Gal}(\widetilde{K}/K)$, and let $H = \mathrm{Gal}(\widetilde{K}/K)$ be the corresponding subgroup of G.
Question: determine $\mathrm{Aut}_F(K)$.

Let $\sigma \in \mathrm{Aut}_F(K)$. Then σ extends to an element $\sigma \in G$. Since $\sigma(K) = K$ we have $\sigma H \sigma^{-1} = H$, i.e. $\sigma \in \mathcal{N}_G(H)$.

Elements of $\mathcal{N}_G(H)$ induce the same automorphism iff they differ by an element of H:

$$\mathrm{Aut}_F(K) \cong \mathcal{N}_G(H)/H.$$

Automorphisms of a subfield : example

Let $K = \mathbb{Q}(2^{1/4}) \subset \widetilde{K} = \mathbb{Q}(2^{1/4}, \zeta_4)$, with

$$G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \cong \begin{pmatrix} (\mathbb{Z}/4\mathbb{Z})^\times & \mathbb{Z}/4\mathbb{Z} \\ 0 & 1 \end{pmatrix}$$

where

$$\begin{pmatrix} u & t \\ 0 & 1 \end{pmatrix} : \zeta_4 \mapsto \zeta_4^u,\ 2^{1/4} \mapsto 2^{1/4}\zeta_4^t.$$

We have

$$H = \begin{pmatrix} (\mathbb{Z}/4\mathbb{Z})^\times & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \mathcal{N}_G(H) = \begin{pmatrix} (\mathbb{Z}/4\mathbb{Z})^\times & 2(\mathbb{Z}/4\mathbb{Z}) \\ 0 & 1 \end{pmatrix},$$

so $\mathrm{Aut}_{\mathbb{Q}}(K) \cong C_2$ is generated by $2^{1/4} \mapsto 2^{1/4}\zeta_4^2 = -2^{1/4}$.

Properties of Galois extensions

Normal basis theorem

Theorem

Let K/F be a Galois extension. Then there exists $\lambda \in K$ such that the elements $\sigma(\lambda)$ for $\sigma \in \mathrm{Gal}(K/F)$ form an F-basis of K.

Example: $K = \mathbb{Q}(\sqrt{2})$.

- $\lambda = \sqrt{2}$ does not work: $\{\sqrt{2}, -\sqrt{2}\}$ is not a basis of K.
- $\lambda = 1 + \sqrt{2}$ works: $\{1 + \sqrt{2}, 1 - \sqrt{2}\}$ is a basis of K.

The group ring

Let G be a finite group. The **group ring** $\mathbb{Z}[G]$ of G is the set of formal linear combinations

$$x = \sum_{\sigma \in G} x_\sigma \sigma, \ \ x_\sigma \in \mathbb{Z}$$

with coefficientwise addition and multiplication given by the group law of G.

Construct the **group algebra** $\mathbb{Q}[G]$ with $\mathbb{Z}$ replaced by $\mathbb{Q}$.

Group ring example

Let $G = \langle \sigma \rangle$ with σ of order 3.

Let $x = 1 + \sigma \in \mathbb{Z}[G]$.

We have $x^3 = (1+\sigma)^3 = 1 + 3\sigma + 3\sigma^2 + \sigma^3 = 2 + 3\sigma + 3\sigma^2$.

Action of the group ring

Let K be a field and $G \subset \mathrm{Aut}(K)$ be a finite subgroup of automorphisms.

Let $x = \sum_{\sigma \in G} x_\sigma \sigma \in \mathbb{Q}[G]$ and $\lambda \in K$. We define the **additive action** of $\mathbb{Q}[G]$ on K by

$$x \cdot \lambda = \sum_{\sigma \in G} x_\sigma \sigma(\lambda).$$

Assume $x \in \mathbb{Z}[G]$ and $\lambda \in K^\times$. We define the **multiplicative action** of $\mathbb{Z}[G]$ on $K^\times$ by

$$\lambda^x = \prod_{\sigma \in G} \sigma(\lambda)^{x_\sigma}.$$

Example: actions of the group ring

Let $K = \mathbb{Q}(\sqrt{2})$ and $G = \langle\sigma\rangle$ with $\sigma(\sqrt{2}) = -\sqrt{2}$.

Let $x = 1 - 2\sigma \in \mathbb{Z}[G]$ and $\lambda = 1 + \sqrt{2} \in K^\times$.

We have

$$x \cdot \lambda = (1 - 2\sigma) \cdot (1 + \sqrt{2}) = (1 + \sqrt{2}) - 2(1 - \sqrt{2}) = -1 + 3\sqrt{2},$$

and

$$\lambda^x = (1 + \sqrt{2})^{1-2\sigma} = \frac{1 + \sqrt{2}}{(1 - \sqrt{2})^2} = (1 + \sqrt{2})^3 = 7 + 5\sqrt{2}.$$

Number field case: actions on ideals

Let K be a number field and $G \subset \mathrm{Aut}(K)$ be a finite subgroup of automorphisms.

Let $\mathfrak{a}$ be an ideal of K and $\sigma \in G$. Then $\mathfrak{a}^\sigma = \sigma(\mathfrak{a})$ is an ideal of K.

We extend this action multiplicatively to an action of $\mathbb{Z}[G]$ on the set of fractional ideals.

On principal ideals, this action is compatible with the multiplicative action on elements, so this induces an action of $\mathbb{Z}[G]$ on Cl_K.

Norm and trace in the Galois setting

Let K/F be a Galois extension with Galois group G.
Let $L = K^H$ correspond to a subgroup $H \subset G$.

We define the **norm element** $N_H \in \mathbb{Z}[G]$ to be

$$N_H = \sum_{\sigma \in H} \sigma.$$

For all $\lambda \in K$ and fractional ideals $\mathfrak{a}$ we have

- $\mathrm{Tr}_{K/L}(\lambda) = N_H \cdot \lambda$,
- $N_{K/L}(\lambda) = \lambda^{N_H}$, and
- $N_{K/L}(\mathfrak{a}) = \mathfrak{a}^{N_H} \cap L$.

Cutting things using the group ring action

Let M be something on which $\mathbb{Q}[G]$ acts (a "$\mathbb{Q}[G]$-module").
Let $e \in \mathbb{Q}[G]$.

Then the image $e \cdot M = \{e \cdot m : m \in M\}$ and the kernel $\{m \in M \mid e \cdot m = 0\}$ are subgroups of M, possibly proper.

We cannot get anything nontrivial this way by only using the action of group elements, since they all act invertibly!

The best situation is when e is an **idempotent**, i.e. $e^2 = e$.
Then we have

- $e \cdot M = \ker(1 - e)$;
- $(1 - e) \cdot M = \ker(e)$;
- $M = e \cdot M \oplus (1 - e) \cdot M$.

Cutting things: example

Let K/F be a Galois extension with Galois group G.
Let $\sigma \in G$ be an element of order 2 and $L = K^{\langle\sigma\rangle}$.
Let $e = \frac{1}{2}N_{\langle\sigma\rangle}$. We have

$$e^2 = \frac{1}{2^2}(1+\sigma)^2 = \frac{1}{4}(1+2\sigma+\sigma^2) = \frac{1}{4}(2+2\sigma) = e,$$

so e is an idempotent.
Considering $\mathbb{Q}[G]$ acting on K, we have

- $e \cdot K = \frac{1}{2}\mathrm{Tr}_{K/L}(K) = L = \{\lambda \in K \mid \sigma(\lambda) = \lambda\}$, and
- $\ker(e) = \{\lambda \in K \mid \mathrm{Tr}_{K/L}(\lambda) = 0\} = \{\lambda \in K \mid \sigma(\lambda) = -\lambda\}$,

and K is the direct sum of these two subspaces.

Cutting things: example

What about the group ring action on $M = K^\times$?

The element e does not act because of the denominator, so we will instead use the action of $2e = 1 + \sigma$ and $2(1 - e) = 1 - \sigma$.

We have

- $(1 + \sigma)M = N_{K/L}(K^\times) \subset L^\times = \ker(1 - \sigma)$,
- $(1 - \sigma)M = \{\lambda/\sigma(\lambda) \colon \lambda \in K\}$,
- $\ker(1 + \sigma) = \{\lambda \in K^\times \mid N_{K/L}(\lambda) = 1\}$,
- $(1 - \sigma)M \subset \ker(1 + \sigma)$, but in fact they are equal!

For every $\lambda \in K$ we have $\lambda^2 = \lambda/\sigma(\lambda) \cdot N_{K/L}(\lambda)$.

Number field case: real and complex embeddings

Let K/F be a Galois extension of number fields with Galois group G.

Let $\tau \colon F \hookrightarrow \mathbb{C}$ be a complex embedding of F, and $\mathcal{T} \colon K \hookrightarrow \mathbb{C}$ a complex embedding of K that extends τ. Then all other $\mathcal{T}'$ extending τ are of the form $\mathcal{T}' = \mathcal{T} \circ \sigma$ for some $\sigma \in G$. In particular, they are all real or all complex.

In addition, if τ is real, there exists a **complex conjugation** $c_{\mathcal{T}} \in G$ such that for all $\lambda \in K$ we have

$$\overline{\mathcal{T}(\lambda)} = \mathcal{T}(c_{\mathcal{T}}(\lambda)),$$

and $c_{\mathcal{T}}$ has order 2 if τ is real and $\mathcal{T}$ complex, and $c_{\mathcal{T}} = 1$ otherwise. As $\mathcal{T}'$ varies, the $c_{\mathcal{T}'}$ form a conjugacy class c_τ.

Example: cyclotomic fields

Let $K = \mathbb{Q}(\zeta_m)$, Galois over $\mathbb{Q}$ with group $G \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

Let $\tau\colon \mathbb{Q} \hookrightarrow \mathbb{C}$ be the inclusion, and let $\mathcal{T}(\zeta_m) = \exp(2i\pi/m)$.

Since G is abelian, c_τ is a well-defined element of G.

We have

$$\overline{\mathcal{T}(\zeta_m)} = \exp(-2i\pi/m) = \mathcal{T}(\zeta_m^{-1}).$$

Therefore $c_\tau = -1$ as an element of $(\mathbb{Z}/m\mathbb{Z})^\times$.

Number field case: prime ideals

Let K/F be a Galois extension of number fields with Galois group G.

Let $\mathfrak{p}$ be a prime ideal of F and $\mathfrak{P}$ a prime ideal of K dividing $\mathfrak{p}\mathbb{Z}_K$. Then all other such $\mathfrak{P}'$ are of the form $\mathfrak{P}' = \mathfrak{P}^\sigma$ for some $\sigma \in G$. In particular, they all have the same residue degree $f_\mathfrak{p}$ and inertia index $e_\mathfrak{p}$, and the number of such prime ideals is a divisor $g_\mathfrak{p}$ of $|G|$, such that

$$[K : F] = e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p}.$$

In addition, if $\mathfrak{p}$ is unramified ($e_\mathfrak{p} = 1$), there exist a **Frobenius element** $\mathrm{Frob}_\mathfrak{P} \in G$ of order $f_\mathfrak{p}$ such that for all $\lambda \in \mathbb{Z}_K$ we have

$$\mathrm{Frob}_\mathfrak{P}(\lambda) = \lambda^{N(\mathfrak{p})} \bmod \mathfrak{P}.$$

As $\mathfrak{P}'$ varies, the $\mathrm{Frob}_{\mathfrak{P}'}$ form a conjugacy class $\mathrm{Frob}_\mathfrak{p}$.

Example: cyclotomic fields

Let $K = \mathbb{Q}(\zeta_m)$, Galois over $\mathbb{Q}$ with group $G \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

Let p be a prime number not dividing m, so that p is unramified in K, and let $\mathfrak{P}$ be a prime dividing $p\mathbb{Z}_K$.

Since G is abelian, Frob_p is a well-defined element of G.

We have (tautologically!)

$$\zeta_m^p = \zeta_m^p \bmod \mathfrak{P}.$$

Therefore $\mathrm{Frob}_p = p$ as an element of $(\mathbb{Z}/m\mathbb{Z})^\times$.

Chebotarev's theorem

Theorem

Let K/F be a Galois extension of number fields of Galois group G. For every $\sigma \in G$, there exists infinitely many prime $\mathfrak{P}$ such that

$$\mathrm{Frob}_{\mathfrak{P}} = \sigma.$$

Because of the cyclotomic example, this implies Dirichlet's theorem that for $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ there are infinitely many primes p such that $p = a \bmod m$!

Cyclotomic fields

Basic properties

Let $K = \mathbb{Q}(\zeta_m)$ (for this whole section).
We have

- $\mathbb{Z}_K = \mathbb{Z}[\zeta_m]$;
- $\Delta_K = (-1)^{\phi(m)/2} \frac{m^{\phi(m)}}{\prod_{p|m} p^{\phi(m)/(p-1)}}$, and in particular
- $\log|\Delta_K| \sim \phi(m) \log m$;
- $G = \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ and we write $\sigma_a \colon \zeta_m \mapsto \zeta_m^a$;
- the complex conjugation $c \in G$ is σ_{-1}.

Decomposition of primes

Let p be a prime and $m = p^k m'$ with m' not divisible by m.
Let f be the order of p in $(\mathbb{Z}/m'\mathbb{Z})^\times$.
Then p decomposes in K as follows:

$$p\mathbb{Z}_K = (\mathfrak{p}_1 \dots \mathfrak{p}_g)^e$$

where $g = \phi(m')/f$, the ramification index is $e = \phi(p^k)$, and the inertia degree of all $\mathfrak{p}_i$ is f.

If p does not divide m, then $\mathrm{Frob}_p = \sigma_p$.

Real subfield

Let $K^+ = K^{\langle c \rangle}$ be the maximal real subfield of K.
We have

- $K^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ and $\mathbb{Z}_{K^+} = \mathbb{Z}[\zeta_m + \zeta_m^{-1}]$.
- The index $Q = [\mathbb{Z}_K^\times : \langle -1, \zeta_m \rangle \mathbb{Z}_{K^+}^\times]$ is finite, and in fact $Q = 1$ if m is a prime power and $Q = 2$ otherwise.
- The map $\mathrm{Cl}_{K^+} \to \mathrm{Cl}_K$ is injective.
- We write $h_m = |\,\mathrm{Cl}_K\,|$, $h_m^+ = |\,\mathrm{Cl}_{K^+}\,|$ and $h_m^- = h_m / h_m^+$.
- There is an explicit formula for h_m^-.
- $\log h_m^- \sim \frac{1}{4}\phi(m) \log m$.
- h_m^+ should be much smaller but is hard to control.

Cyclotomic units

Let

$$V_m = \langle -1, \zeta_m, 1 - \zeta_m^a \text{ for } 1 < a \leq m-1 \rangle.$$

Define the group of **cyclotomic units** to be $C_m = V_m \cap \mathbb{Z}_K^\times$, and $C_m^+ = C_m \cap K^+$.

- If m is not a prime power then $1 - \zeta_m^a \in \mathbb{Z}_K^\times$ whenever $(a, m) = 1$.
- If $m = p^k$ then $C_m = \langle -1, \zeta_m, \frac{1-\zeta_m^a}{1-\zeta_m} \text{ for } (a, p) = 1 \rangle$.

Let ω be the number of distinct prime factors of m. We have

$$[\mathbb{Z}_{K^+}^\times : C_m^+] = 2^b h_m^+, \text{ where } b = \lfloor 2^{\omega - 2} + 1 - \omega \rfloor.$$

Stickleberger's theorem

Let the **Stickleberger element** be

$$\theta = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \left(\frac{a}{m} - \left\lfloor \frac{a}{m} \right\rfloor \right) \sigma_a \in \mathbb{Q}[G].$$

Theorem

Let $x \in \mathbb{Z}[G]$ be such that $y = \theta x \in \mathbb{Z}[G]$. For every fractional ideal $\mathfrak{a}$ of K, $\mathfrak{a}^y$ is principal.

Stickleberger's theorem

Theorem

Let $x \in \mathbb{Z}[G]$ be such that $y = \theta x \in \mathbb{Z}[G]$. For every fractional ideal $\mathfrak{a}$ of K, $\mathfrak{a}^y$ is principal.

- Says nothing about Cl_{K^+}.
- "Optimised" version of the fact that $\mathfrak{a}^{h_m}$ is always principal, or even $\mathfrak{a}^{(1-c)h_m^-}$.
- The corresponding relations in the class group are explicit.

Class field theory

Goal

Let F be a number field.

Ultimate goal: classify all Galois extensions K/F and their Galois group.

Reasonable goal (class field theory): classify all Galois extensions K/F with **abelian** Galois group.

Kronecker–Weber theorem

Case $F = \mathbb{Q}$.

Theorem

Let $K/\mathbb{Q}$ be a Galois extension with abelian Galois group. Then there exists m such that

$$K \subset \mathbb{Q}(\zeta_m).$$

By Galois theory, there exists a subgroup $H \subset (\mathbb{Z}/m\mathbb{Z})^\times$ such that

$$K = \mathbb{Q}(\zeta_m)^H \text{ and } \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times/H.$$

Ray class groups

We need a generalisation of $(\mathbb{Z}/m\mathbb{Z})^\times$ to other number fields F.

Let $\mathfrak{m}$ be an ideal of $\mathbb{Z}_F$. Let $\alpha \in F^\times$. We say that

$$\alpha =^* 1 \bmod \mathfrak{m}$$

if $\sigma(\alpha) > 0$ for every $\sigma\colon F \to \mathbb{R}$ and $v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}(\mathfrak{m})$ for all $\mathfrak{p}$ dividing $\mathfrak{m}$.

The **ray class group** of modulus $\mathfrak{m}$ is

$$\mathrm{Cl}_F(\mathfrak{m}) = \frac{(\text{fractional ideals coprime to } \mathfrak{m})}{(\text{ideals } \alpha\mathbb{Z}_F \text{ with } \alpha =^* 1 \bmod \mathfrak{m})}.$$

This is a finite group.

Example: $\mathrm{Cl}_\mathbb{Q}(m) = (\mathbb{Z}/m\mathbb{Z})^\times$.

Ray class fields

Theorem

*Let F be a number field and $\mathfrak{m}$ an ideal. There exists a Galois extension $F(\mathfrak{m})$ of F, called the **ray class field** of modulus $\mathfrak{m}$ such that the extension $F(\mathfrak{m})/F$ is ramified exactly at the primes dividing $\mathfrak{m}$, and such that the map*

$$\mathrm{Cl}_F(\mathfrak{m}) \to \mathrm{Gal}(F(\mathfrak{m})/F)$$

defined by $\mathfrak{p} \mapsto \mathrm{Frob}_{\mathfrak{p}}$ is well-defined and is an isomorphism.

Example: $\mathbb{Q}(m) = \mathbb{Q}(\zeta_m)$.

Hilbert class field

Theorem

*Let F be a number field. There exists a Galois extension $\mathrm{Hilb}(F)$ of F, called the **Hilbert class field** of F such that the extension $\mathrm{Hilb}(F)/F$ is unramified everywhere, and such that the map*

$$\mathrm{Cl}_F \to \mathrm{Gal}(\mathrm{Hilb}(F)/F)$$

defined by $\mathfrak{p} \mapsto \mathrm{Frob}_{\mathfrak{p}}$ is well-defined and is an isomorphism.

Example: $\mathrm{Hilb}(\mathbb{Q}) = \mathbb{Q}$.

Exhaustivity

Theorem

Let K/F be a Galois extension with abelian Galois group. Then there exists $\mathfrak{m}$ such that

$$K \subset F(\mathfrak{m}).$$

By Galois theory, there exists a subgroup $H \subset \mathrm{Cl}_F(\mathfrak{m})$ such that

$$K = F(\mathfrak{m})^H \text{ and } \mathrm{Gal}(K/F) \cong \mathrm{Cl}_F(\mathfrak{m})/H.$$

Hilbert towers

Theorem

There exists a number field F such that the tower

$$F = F_0 \subset F_1 = \mathrm{Hilb}(F) \subset F_2 = \mathrm{Hilb}(\mathrm{Hilb}(F)) \subset \dots$$

never stabilises. The extensions F_i/F are all unramified, and

$$|\Delta_{F_i}| = 2^{O([F_i:\mathbb{Q}])}.$$

Thank you!

Questions ?