On the construction of class fields

Carlo Sircana
joint work with Claus Fieker
and Tommy Hofmann

19/07/2018, Madison, WI
ANTS XIII

TRR 195
SYMBOLIC TOOLS

Why?

Constructive Class Field theory can be useful for:

- Tabulation of number fields with given Galois group.
- Construction of minimal fields with prescribed ramification behaviour.

As byproducts, we get useful tools such as the compact presentation for number field elements.

Correspondence Theorem

Abelian extensions → Congruence subgroups

If L/K is an abelian extension of conductor $\mathfrak{f}$, then there exists a congruence subgroup $A_{\mathfrak{f}} \subseteq \mathrm{Cl}_{\mathfrak{f}}$ of conductor $\mathfrak{f}$ such that the Artin map induces an isomorphism $\psi_{L/K} \colon \mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}} \to \mathrm{Gal}(L/K)$.

Congruence subgroups → Abelian extensions

If $A_{\mathfrak{f}}$ is a congruence subgroup of conductor $\mathfrak{f}$, then there exists an abelian extension L/K such that the Artin map induces an isomorphism $\psi_{L/K} \colon \mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}} \to \mathrm{Gal}(L/K)$.

Finding abelian extensions

Let K be a number field. We want to find abelian extensions L of K with a given Galois group $G = \mathrm{Gal}(L/K)$ and bounded norm of the discriminant.

- Find a list F of possible conductors.
- For every conductor $\mathfrak{f} \in F$, compute the ray class group $\mathrm{Cl}_{\mathfrak{f}}$ and find all subgroups $A_{\mathfrak{f}} \subseteq \mathrm{Cl}_{\mathfrak{f}}$ of conductor $\mathfrak{f}$ such that $\mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}} \simeq G$.
- Let L be the abelian extension corresponding to $(\mathfrak{f}, A_{\mathfrak{f}})$. If the norm of the discriminant of the corresponding extension is lower than the bound, compute a defining polynomial for L.

Ray Class Group

The ray class group mod $\mathfrak{m}$ is usually computed from:

$$1 \longrightarrow (\mathcal{O}_K/\mathfrak{m})^\times/\iota(\mathcal{O}_K^\times) \longrightarrow \mathrm{Cl}_\mathfrak{m} \longrightarrow \mathrm{Cl} \longrightarrow 0.$$

Ray Class Group

The ray class group mod $\mathfrak{m}$ is usually computed from:

$$1 \longrightarrow (\mathcal{O}_K/\mathfrak{m})^\times/\iota(\mathcal{O}_K^\times) \longrightarrow \mathrm{Cl}_\mathfrak{m} \longrightarrow \mathrm{Cl} \longrightarrow 0.$$

Observation

An abelian extension L of K of degree n corresponds to a subgroup $\mathrm{Cl}_\mathfrak{m}^n \subseteq A \subseteq \mathrm{Cl}_\mathfrak{m}$: we only need $\mathrm{Cl}_\mathfrak{m}/\mathrm{Cl}_\mathfrak{m}^n$.

If m is large enough, $B \mapsto B/B^m$ is exact on this sequence.

Advantages

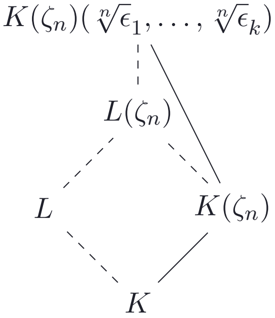
- The minimum number of generators of $\mathrm{Cl}/\mathrm{Cl}^m$ can be lower than the number of generators of Cl.
- We don't need to compute $\mathbf{F}_q^\times$ but the quotient $\mathbf{F}_q^\times/(\mathbf{F}_q^\times)^m$.

Ray Class Field

The computation of the defining polynomial of an abelian extension L/K using the Artin Map has three steps:

- Computation of a generator of the Kummer extension $L(\zeta_n)/K(\zeta_n)$.
- Reduction of the generator.
- Descent to K.

Kummer extension



Let $\epsilon_1, \ldots, \epsilon_k$ be the S-units (for a suitable set of primes S) modulo n-th powers. Then

$$L(\zeta_n) \subseteq K(\zeta_n)(\sqrt[n]{\epsilon_1}, \ldots, \sqrt[n]{\epsilon_k}).$$

We find the extension by computing the action of the automorphisms via the Artin map.

Idea

We take small primes and look at the action of the corresponding Frobenius on the S-units.

A similar strategy can be applied in the descent step.

Normal extensions

Additional hypotheses:

- K is a normal extension of a field K_0.
- We are searching for abelian extensions L/K such that L/K_0 is normal.

Tasks

- Computation of the subgroups of a ray class group corresponding to normal extensions of K_0.
- Computation of the automorphisms of L/K_0.

Invariant subgroups

"Trivial" statement

Let $\mathfrak{m}$ be a modulus which is invariant under the action of $\mathrm{Gal}(K/K_0)$. Subgroups of $\mathrm{Cl}_{\mathfrak{m}}$ that are invariant under the action of $\mathrm{Gal}(K/K_0)$ give rise to abelian extensions that are normal over K_0.
Viceversa, abelian extensions that are normal over K_0 have invariant conductor $\mathfrak{f}$ and the corresponding subgroup in $\mathrm{Cl}_{\mathfrak{f}}$ is invariant too.

Practical consequences

The conductors and the subgroups we need are invariant under the action of the automorphisms.

Given $G = \mathrm{Gal}(K/K_0)$ and n the exponent of $\mathrm{Cl}_{\mathfrak{m}}$, $\mathrm{Cl}_{\mathfrak{m}}$ has then a structure of $(\mathbf{Z}/n\mathbf{Z})[G]$-module.

Key lemma

The minimal submodules of $\mathrm{Cl}_{\mathfrak{m}}$ have exponent p, i.e. they are $\mathbf{F}_p[G]$-modules.

The Meataxe algorithm solves the problem of finding submodules in a $\mathbf{F}_p[G]$-module. Inductively, this allows to find all the $(\mathbf{Z}/n\mathbf{Z})[G]$-submodules of $\mathrm{Cl}_{\mathfrak{f}}$.

Duality

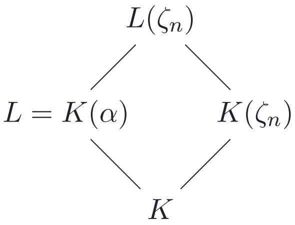
The Meataxe algorithm takes advantage of duality. The same applies to our case by considering the dual group instead of the dual vector space.

Automorphisms

Let L/K be an abelian extension for which we have computed a defining polynomial $L = K(\alpha)$.

Assumptions

L/K is cyclic and K and $\mathbf{Q}(\zeta_n)$ are linearly disjoint.



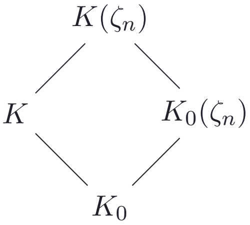
- res: $\mathrm{Gal}(L(\zeta_n)/K(\zeta_n)) \to \mathrm{Gal}(L/K)$ is an isomorphism.
- We computed $\beta \in K(\zeta_n)$ such that $L(\zeta_n) = K(\zeta_n, \sqrt[n]{\beta})$
- $\mathrm{Gal}(L(\zeta_n)/K(\zeta_n))$ is generated by $\sigma\colon \sqrt[n]{\beta} \mapsto \zeta_n \sqrt[n]{\beta}$

$\mathrm{Gal}(L/K)$ is generated by the restriction of σ to L.

Goal

Extend $\sigma \in \mathrm{Gal}(K/K_0)$ to an element of $\mathrm{Gal}(L/K_0)$.

First step: extend σ to $\tilde{\sigma} \in \mathrm{Gal}(K(\zeta_n)/K_0)$.

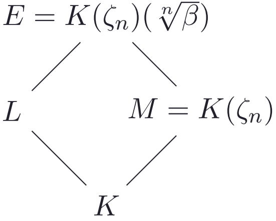


Since the extensions are linearly disjoint, you can choose any $\tau \in \mathrm{Gal}(K_0(\zeta_n)/K_0)$ and combine it with σ to get an element $\tilde{\sigma} \in \mathrm{Gal}(K(\zeta_n)/K_0)$.

Goal

Extend $\sigma \in \mathrm{Gal}(K/K_0)$ to an element of $\mathrm{Gal}(L/K_0)$.

Second step: extend $\tilde{\sigma}$ to $\hat{\sigma} \in \mathrm{Gal}(L(\zeta_n)/K_0)$.



Any extension $\hat{\sigma}$ must satisfy

$$\hat{\sigma}(\sqrt[n]{\beta}) = \mu \cdot \sqrt[n]{\beta}^{i}$$

with $\mu \in M$, $1 \leq i \leq n-1$. Applying $\mathrm{Frob}_{\mathfrak{p}}$ for sufficiently many primes $\mathfrak{p}$ in E/M, we can compute μ and i.

Applications

If G is a transitive permutation group of degree n and $0 \leq r \leq n$, we set $d_0(n, r, G)$ to be the smallest value of $|d_K|$, where $[K : \mathbf{Q}] = n$, K has r real embeddings, and if L is the Galois closure of K over $\mathbf{Q}$, then $\mathrm{Gal}(L/\mathbf{Q}) \cong G$ as a permutation group on the embeddings of K in L.

Results

- $d_0(15, 1, D_{15}) = 239^7$,
- $d_0(15, 3, D_5 \times C_3) = 7^{12} \cdot 17^6$,
- $d_0(15, 5, S_3 \times C_5) = 2^{10} \cdot 11^{13}$,
- $d_0(36, 36, C_9 \rtimes C_4) = 1129^{27}$,
- $d_0(36, 0, C_9 \rtimes C_4) = 3^{88} \cdot 29^{27}$.