Class Field Theory

CM Study Group. Lecture 3

Alberto Angurel Andrés

University of Nottingham

02/12/2022

Introduction

- Class field theory relates the abelian extensions of a local or a number field with the arithmetic of its field.

- It was developed between 1850 and 1930 by Kronecker, Webber, Hilbert, Artin...

- Its proofs comes from duality theorems in the cohomology theory of finite groups.

- It provides powerful results which are really useful in number theory.

- There are recent conjectures regarding to non-abelian extension $\rightarrow$ Langlands' program

Local Class Field Theory

- Let K be a local field
- Let $L|K$ be a finite, abelian extension

$\Rightarrow$ There is an isomorphism (Artin map)

$$(\ \ , L|K) : \frac{K^*}{N_{L|K}L^*} \to G(L|K)$$

Existence Theorem

There is a bijection between the finite, abelian extensions of K and the subgroups of finite index in K^*.

Example

$$G(K^{ab}|K) = \varprojlim_{L \subset K^{ab}} G(L|K) = \varprojlim_{L \subset K^{ab}} \frac{K^*}{N_{L|K}L^*} = \widehat{K^*}$$

Local Class Field Theory

- Let K be a local field
- Let $L|K$ be a finite, abelian extension

$\Rightarrow$ There is an isomorphism (Artin map)

$$(\ \ , L|K) : \frac{K^*}{N_{L|K} L^*} \rightarrow G(L|K)$$

Unramified Extensions

- $L|K$ unramified $\Rightarrow G(L|K) \cong G(l|k)$
- There is a Frobenius automorphism $\varphi \in G(L|K)$
- It is characterised by $\overline{\varphi(x)} = \overline{x}^q$, where $q = \#k$.
- $(a, L|K) = \varphi^{v(a)} \in G(L|K) \ \forall a \in K^*$
- $L|K$ unramified $\Leftrightarrow U_K \subset N_{L|K} L^*$

Ideles

$$I_K := \left\{ (a_{\mathfrak{p}}) \in \prod_{\mathfrak{p} \in M_K} K_{\mathfrak{p}}^* : a_{\mathfrak{p}} \in U_{\mathfrak{p}} \text{ for almost every } \mathfrak{p} \in M_K \right\}$$

We have an injection

$$K^* \hookrightarrow I_K : \; a \mapsto (a, a, \dots, a)$$

Definition

Idele Class Group: $C_K := \frac{I_K}{K^*}$

Proposition

The ideal class group is $\quad J_K := \dfrac{I_K}{I_K^{S_\infty} K^*}$

Global Artin Map

- Let K be a number field
- Let $L|K$ be a finite, abelian extension

$\Rightarrow$ There is an action of $G = G(L|K)$ on I_L that behaves well with principal ideals $\rightarrow$ There is a norm map in the class group. $\Rightarrow$

The following map (Artin map) is an isomorphism

$$(\ \ , L|K) : \frac{C_K}{N_{L|K} C_L} \rightarrow G(L|K), \ \overline{a} \mapsto \prod_{\mathfrak{p} \in M_K} (a_p, L_\beta | K_\mathfrak{p})$$

Existence Theorem

$\{\text{Abelian, finite extensions of } K\} \leftrightarrow \{\text{Open subgroups in } C_K\}$

Hilbert Class Field

Hilbert Class Field of a number field K

Abelian extension $H|K$ associated to the subgroup

$$I_K^{S_\infty} K^* = \left(\prod_{\mathfrak{p} \in M_K^\infty} K_\mathfrak{p}^* \times \prod_{\mathfrak{p} \in M_K^0} U_\mathfrak{p} \right) K^*$$

$$\boxed{G(H|K) \cong J_K}$$

Theorem

The Hilbert class field of K is the maximal abelian extension of K which is unramified at every (finite and infinite) prime $\mathfrak{p} \in M_K$.

Class Field Theory in terms of ideals

We fix an abelian extension $L|K$ of number fields and let S be the finite set of primes which ramifies in S.

Let $I \leq R_K$ be an integral ideal of K which is not divisible by any of the primes in S.

By the unique factorisation in Dedekind domains, $I = \mathfrak{p}_1^{\alpha_1} \cdots p_r^{\alpha_r}$

We define

$$(I, L|K) := \prod_{i=1}^{r} \left(\pi_{\mathfrak{p}_i}^{\alpha_i}, L_\beta | K_\mathfrak{p}\right)$$

Conductor

Proposition

Let $L|K$ be a finite, abelian extension. The **conductor** $c_{l|K}$ is the maximal ideal $\mathfrak{c}$ satisfying the property

$$((\alpha), L|K) = 1 \ \forall \alpha \in K^* \text{ such that } \alpha \equiv 1 \ (mod \mathfrak{c})$$

Remark

It is clear that the maximal ideal exist since, assuming that $\mathfrak{c}_1$ and $\mathfrak{c}_2$ satisfy the property in the above definition, then $\mathfrak{c}_1 + \mathfrak{c}_2$ does so.

Explicit Computation of the Conductor

Theorem

Given a finite, abelian extension of number fields $L|K$, we have that

$$c_{L|K} = \prod_{\mathfrak{p} \in M_K^0} \mathfrak{p}^{n_\mathfrak{p}}$$

where $n_\mathfrak{p}$ is the minimal natural number n such that

$$U_\mathfrak{p}^n = 1 + (\pi^n) \subset N_{L_\beta | K_\mathfrak{p}}$$

(Notice that $n_\mathfrak{p} = 0$ if and only if $L|K$ is unramified at $\mathfrak{p}$.

Example

The conductor of the Hilbert Class Field extension is (1).

Ray Class Field

Definition

Given an integral ideal $\mathfrak{c}$ of K, the ray class field $K_{\mathfrak{c}}$ is a finite, abelian extension of K whose conductor is $\mathfrak{c}$ with the property that for any finite abelian extension $L|K$

$$\mathfrak{c}_{l|K}|\mathfrak{c} \Rightarrow L \subset K_{\mathfrak{c}}$$

Remark

If $\mathfrak{c} = \mathfrak{p}_1^{\alpha_1} \cdots p_r^{\alpha_r}$, the ray class $K_{\mathfrak{c}}$ is the field extension associated to the norm group

$$N = \left(\prod_{\mathfrak{p} \neq \mathfrak{p}_i} K_{\mathfrak{p}}^* \times \prod_{i=1}^{r} U_{\mathfrak{p}_i}^{\alpha_i} \right) K^*$$

Example

The Hilbert class field it the ray class field of $\mathfrak{c} = 1$.

Theorem

Let $L|K$ be a finite abelian extension of number fields and let $\mathfrak{c}$ be an integral ideal of K.

- The Artin map
$$(\cdot, L|K): \ I(\mathfrak{c}_{l|K}) \to Gal(L|K)$$
is a surjective homomorphism.
- The kernel of the Artin map is $(N_{L|K} I_L)P(\mathfrak{c}_{L|K})$.
- There exists a unique ray class field $K_{\mathfrak{c}}$ of K associated to $\mathfrak{c}$. The conductor of $K_{\mathfrak{c}}|K$ divides $\mathfrak{c}$.
- That ray class field $K_{\mathfrak{c}}$ is characterised by the property that it is an abelian extension of K and satisfies that the primes of K that split completely in $K_{\mathfrak{c}}$ are exactly those in $P(\mathfrak{c})$.

Dirichlet's prime number and Kronecker-Webber theorems

Theorem (Dirichlet)

Let K be a number field and $\mathfrak{c}$ an integral ideal of K. Then every ideal class in $I(\mathfrak{c})/P(\mathfrak{c})$ contains infinitely many degree 1 primes.

Theorem (Kronecker-Webber)

Every finite, abelian extension $L|\mathbb{Q}$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta)|\mathbb{Q}$, where ζ is a root of unity.

Corollary

$\mathbb{Q}^{ab}$ is generated by the roots of unity.

Cyclotomic Class Field Theory

Consider the Artin Map

$$I_{\mathbb{Q}} \to G(\mathbb{Q}^{ab}|\mathbb{Q}) : \ s \mapsto [s, \mathbb{Q}]$$

Notice the Galois automorphisms act on $\mu := (\mathbb{C}^*)_{tors}$

$$\mu \cong \mathbb{Q}/\mathbb{Z}$$

Idelic Multiplication on $\mathbb{Q}/\mathbb{Z}$

- Let $x \in I_{\mathbb{Q}}$. Our goal is to define a multiplication by x

$$\mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/x\mathbb{Z}$$

- Notice that $\mathbb{Q}/\mathbb{Z} \cong \bigoplus_p \mathbb{Q}_p/\mathbb{Z}_p$.Why?
  - Each torsion, abelian group is the direct sum of its p-primary components.
  - $(\mathbb{Q}/\mathbb{Z})_p = \mathbb{Z}[p^{-1}]/\mathbb{Z} \cong \mathbb{Q}_p/\mathbb{Z}_p$
- We define

$$x\mathbb{Z} := \prod_p p^{v_p(x_p)} = N_x\mathbb{Z}$$

- $\mathbb{Q}/x\mathbb{Z} := \mathbb{Q}/N_x\mathbb{Z} \cong \bigoplus \mathbb{Q}_p/N_x\mathbb{Z}_p \cong \bigoplus \mathbb{Q}_p/x_p\mathbb{Z}_p$
- We have the following commutative diagram

$$\begin{array}{ccc} \mathbb{Q}/\mathbb{Z} & \xrightarrow{\;x\;} & \mathbb{Q}/x\mathbb{Z} \\ \downarrow \wr & & \downarrow \wr \\ \bigoplus_p \mathbb{Q}_p/\mathbb{Z}_p & \xrightarrow{\oplus \cdot x_p} & \bigoplus \mathbb{Q}_p/x_p\mathbb{Z}_p \end{array}$$

Cyclotomic class field Theory

Theorem

Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ and let $s \in \mathbb{A}_{\mathbb{Q}}$ be an idele such that $[s, \mathbb{Q}] = \sigma|_{\mathbb{Q}^{ab}}$.

Let N_S be the unique rational number such that $v_p(s_p) = v_p(N_s)$ and $\mathrm{sgn}(s_\infty) = \mathrm{sgn}(N_S)$and define the maps

$$f: \mathbb{C}/\mathbb{Z} \to \mu; \quad t \mapsto e^{2\pi i t} \qquad f_s: \mathbb{C}/s^{-1}\mathbb{Z} \to \mu \quad t \mapsto e^{2\pi i N_s t}$$

Then the following diagram is commutative

$$\begin{array}{ccc} \mathbb{Q}/\mathbb{Z} & \xrightarrow{s^{-1}} & \mathbb{Q}/s^{-1}\mathbb{Z} \\ \downarrow f & & \downarrow f_s \\ \mathbb{C}^* & \xrightarrow{\sigma} & \mathbb{C}^* \end{array}$$

Cyclotomic class field theory

Proof.

- We need to proof that

$$(e^{2\pi it})^{[s,\mathbb{Q}]} = e^{2\pi iN_s(s^{-1}t)}$$

- Let $t = \frac{a}{n}$ and let $\zeta = f(t) = e^{\frac{2\pi iat}{n}}$
- Case 1: $s_p \equiv 1 \mod n\mathbb{Z}_p$ and $s_\infty > 0$
  - $[s,\mathbb{Q}]_{\mathbb{Q}(\zeta)} = (s,\mathbb{Q}(\zeta)|\mathbb{Q}) = (N_s\mathbb{Z},\mathbb{Q}(\zeta)|\mathbb{Q}) \Rightarrow$
  - $f(t)^{[s,\mathbb{Q}]} = \zeta^{[s,\mathbb{Q}]} = \zeta^{N_s} = f(t)^{N_s}$
  - $t = \frac{a}{n} = \sum \frac{a_p}{p^{e_p}} \in \bigoplus_p \mathbb{Q}_p/\mathbb{Z}_p$
  - $s^{-1}t := \sum \frac{s_p^{-1}a_p}{p^{e_p}} \equiv \sum \frac{a_p}{p^{e_p}} = t$
  - $f_s(s^{-1}t) = f_s(t) = e^{2\pi iN_s t} = f(t)^{N_s} = f(t)^{[s,\mathbb{Q}]}$

□

Cyclotomic class field theory

Proof.

- General Case:
  - Chinese remainder theorem $\Rightarrow \exists r \in \mathbb{Q}^*$ such that rs satisfies the hypothesis of case 1.
  - We have that $N_{rs} = rN_s$and $(rs)^{-1}t = r^{-1}(s^{-1}t)$
  - $f(t)^{[s,\mathbb{Q}]} = f(t)^{[rs,\mathbb{Q}]} = f_{rs}((rs)^{-1}t) = e^{2\pi i t N_{rs}(rs)^{-1}t} = e^{2\pi i t N_s s^{-1}t} = f_s(s^{-1}t)$

$\square$

Thank you for your attention!