LECTURE 1

Introduction

In this class, we will begin by studying the quadratic version of Class Field Theory (CFT), with an emphasis on explicit CFT. We will then develop a cohomological approach to CFT. Finally, we may discuss additional topics, such as explicit CFT (in greater depth), the Fontaine-Herr approach to Local Class Field Theory (LCFT), algebraic groups, or Tate duality.

Class Field Theory emerged in the nineteenth century from at least three lines of inquiry. The first was the question of solvability by radicals: which algebraic numbers in $\overline{\mathbb{Q}}$ could be expressed using nth roots, sums, etc.? Abel and Galois showed that an irreducible polynomial $f(x) \in K[x]$, for some number field K, has roots that can be expressed via radicals if and only if the Galois group of the splitting field of f is solvable, that is, the splitting field of f is an iterated extension of abelian extensions such as

$$\mathbb{Q} \overset{\mathbb{Z}/2\mathbb{Z}}{\subseteq} \mathbb{Q}(\zeta_3) \overset{\mathbb{Z}/3\mathbb{Z}}{\subseteq} \mathbb{Q}(\zeta_3, \sqrt[3]{2}),$$

where we have written the Galois group of each subextension above its respective inclusion. This criterion reduces the problem of identifying which algebraic numbers can be written in terms of radicals to understanding abelian (or even cyclic) extensions of number fields. Unfortunately, this problem hasn't been solved, though one can dream that cutting edge research is coming closer. However, abelian extensions of $\mathbb{Q}$ are known:

Theorem 1.1 (Kronecker–Weber). *Every abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_n)$ for some n, where ζ_n is a primitive nth root of unity.*

That is, if the splitting field of $f \in \mathbb{Q}[x]$ has an abelian Galois group, then all (equivalently, some) roots of f can be written as rational functions of ζ_n for some n. As a brief reminder, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ (i.e., the Euler totient function), and $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$, with an element $m \in (\mathbb{Z}/n\mathbb{Z})^\times$ acting as $\zeta_n \mapsto \zeta_n^m$. CFT is essentially equivalent to the Kronecker–Weber theorem for $\mathbb{Q}$, but gives additional (though inexplicit) control of the situation for general number fields.

The second question was that of finding identities for algebraic numbers. As we will see, Gauss explained that non-obvious identities in $\overline{\mathbb{Q}}$ have non-trivial arithmetic consequences. For instance, identites like

$$\sqrt{2} = \zeta_8 + \zeta_8^{-1} = \zeta_8 + \overline{\zeta_8} = \frac{1+i}{\sqrt{2}} + \frac{1-i}{\sqrt{2}},$$

$$\sqrt{-3} = \zeta_3 - \zeta_3^{-1} = \zeta_3 + \overline{\zeta_3} = \frac{-1+\sqrt{-3}}{2} + \frac{-1-\sqrt{-3}}{2},$$

are predicted by the Kronecker–Weber theorem (since these numbers have an associated abelian Galois group $\mathbb{Z}/2\mathbb{Z}$). These arithmetic consequences indicate that we should attempt to understand such identities more fully.

Finally, the third area was solvability of Diophantine equations. The following is an example of a typical theorem:

Theorem 1.2 (Hasse Principle). *Let K be a number field, and*

$$q(x_1,\dots,x_n)=\sum_i a_i x_i^2+\sum_{i\neq j} a_{ij}x_ix_j$$

for $a_i, a_{ij}\in K$. Then, for any $y\in K$, the equation

$$q(x_1,\dots,x_n)=y$$

has a solution if and only if it does in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes p.

Checking for solutions over $\mathbb{R}$ is easy, and over $\mathbb{Q}_p$ the problem reduces to elementary congruence properties; it turns out that this problem can be solved entirely algorithmically. We can recast such problems as asking if $y\in\mathbb{Q}$ is a norm in a quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, at least for the form $\mathrm{N}(x+y\sqrt{d})=x^2-dy^2$ (where $x,y\in\mathbb{Q}$), which is the hardest case of the above anyways. This question, and the broader idea of connecting local and global, will make a reappearance.

We now turn to the statements of the main theorems of CFT, which perhaps are not yet so inspiring. Let K a local field, so that either K is archimedean, in which case $K=\mathbb{R},\mathbb{C}$, or K is nonarchimedean, in which case $K/\mathbb{Q}_p$ or $K=\mathbb{F}_{p^n}((t))$ for some p and n. Let K^{sep} denote its separable closure. Observe that if K is any field with abelian extensions $K^{\mathrm{sep}}/K_1/K$ and $K^{\mathrm{sep}}/K_2/K$ (which are necessarily Galois), then the compositum $K_1\cdot K_2$ is also abelian, justifying the following definition:

Definition 1.3. The *maximal abelian extension* K^{ab}/K is the compositum of all abelian extensions $K^{\mathrm{sep}}/K'/K$, and $\mathrm{Gal}^{\mathrm{ab}}(K):=\mathrm{Gal}(K^{\mathrm{ab}}/K)$ is the abelianization of the *absolute Galois group* $\mathrm{Gal}(K):=\mathrm{Gal}(K^{\mathrm{sep}}/K)$.

We also recall the following definition:

Definition 1.4. For a group G, the inverse limit

$$\widehat{G}:=\varprojlim_{\substack{H\lhd G\\ [G:H]<\infty}} G/H$$

over quotients by finite-index normal subgroups is the *profinite completion* of G.

We can now state the main theorem of Local Class Field Theory:

Theorem 1.5 (Main Theorem of LCFT). *For any finite extension $K/\mathbb{Q}_p$, there is a canonical isomorphism*

$$\mathrm{Gal}^{\mathrm{ab}}(K)\simeq\widehat{K^\times}$$

of profinite groups.

Example 1.6. The first-order structure of $K^\times$ is given by the short exact sequence

$$1\to\mathcal{O}_K^\times\to K^\times\xrightarrow{v}\mathbb{Z}\to 0, \tag{1.1}$$

where v is the valuation homomorphism taken with respect to the maximal ideal $\mathfrak{p}_K \subseteq \mathcal{O}_K$ (i.e., it sends a uniformizer of $\mathcal{O}_K$ to 1); the ring of integers $\mathcal{O}_K^\times$ is profinite and open in $K^\times$. The second-order structure of $K^\times$ is given by the inverse limit

$$\mathcal{O}_K^\times = \varprojlim_n \mathcal{O}_K^\times/(1+\mathfrak{p}_K^n),$$

so that (1.1) becomes

$$1 \to \mathcal{O}_K^\times \to \widehat{K^\times} \xrightarrow{\hat{v}} \widehat{\mathbb{Z}} \to 0$$

after taking profinite completions.

Now, for any finite Galois extension L/K, there is an action of $\mathrm{Gal}(L/K)$ on L that preserves $\mathcal{O}_L$ and $\mathfrak{p}_L$. Thus, it descends to an action on $k_L := \mathcal{O}_L/\mathfrak{p}_L$ fixing $k_K := \mathcal{O}_K/\mathfrak{p}_L$; these are finite fields, say $k_L = \mathbb{F}_{q^n}$ and $k_K = \mathbb{F}_q$ for some prime-power q. We therefore have a map

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k_K) = \mathbb{Z}/n\mathbb{Z},$$

which is an isomorphism if L/K is unramified; the group $\mathrm{Gal}(k_L/k_K)$ is generated by the Frobenius automorphism $x \mapsto x^q$. Taking inverse limits over all such L/K then yields a homomorphism

$$\mathrm{Gal}(K) \to \mathrm{Gal}(k) = \widehat{\mathbb{Z}}$$

given by the Frobenius elements, which factors through $\mathrm{Gal}^{\mathrm{ab}}(K)$ by the universal property of abelianization. Under LCFT, this map coincides with the map $\hat{v}$ above.

Now, recall that the *ring of adèles* of a number field F is defined as the direct limit

$$\mathbb{A}_F := \varinjlim_S \left(\prod_{v\in S} F_v \times \prod_{v\notin S} \mathcal{O}_{F_v} \right)$$

over finite sets S of places F. It comes with a diagonal embedding

$$F \hookrightarrow \mathbb{A}_F,$$

by which F is discretely embedded (think $\mathbb{Z} \hookrightarrow \mathbb{R}$). Morally, $\mathbb{A}_F$ amalgamates all local information about F, while this embedding encodes its global aspects. Inside $\mathbb{A}_F$ lies the group $\mathbb{A}_F^\times$ of units, topologized via the direct limit

$$\mathbb{A}_F^\times = \varinjlim_S \left(\prod_{v\in S} F_v^\times \times \prod_{v\notin S} \mathcal{O}_{F_v}^\times \right),$$

with S as before (and all terms open in $\mathbb{A}_F^\times$), rather than the finer subspace topology. We are now ready to state the main theorem of Global Class Field Theory (GCFT):

THEOREM 1.7 (Main Theorem of GCFT). *For any finite extension $F/\mathbb{Q}$, there is a canonical isomorphism*

$$\mathrm{Gal}^{\mathrm{ab}}(F) \simeq \widehat{\mathbb{A}_F^\times/F^\times}$$

of profinite groups.

These two main theorems are compatible in the following manner. If v is a place of a global field F with algebraic closure $\overline{F}$, then we have maps

$$\begin{tikzcd} F \arrow[r, hook] \arrow[d, hook] & F_v \arrow[d, hook] \\ \overline{F} \arrow[r, hook] & \overline{F}_v, \end{tikzcd}$$

which induce (injective) maps

$$\mathrm{Gal}(F_v) \to \mathrm{Gal}(F),$$
$$\mathrm{Gal}^{\mathrm{ab}}(F_v) \to \mathrm{Gal}^{\mathrm{ab}}(F).$$

The diagram

$$\begin{tikzcd} F_v^\times \arrow[r, "x \mapsto (1,\ldots,1,x,1,\ldots)"] \arrow[d, "\mathrm{LCFT}"] & \mathbb{A}_F^\times/F^\times \arrow[d, "\mathrm{GCFT}"] \\ \mathrm{Gal}^{\mathrm{ab}}(F_v) \arrow[r] & \mathrm{Gal}^{\mathrm{ab}}(F), \end{tikzcd}$$

whose vertical arrows are obtained by composing the the natural map from each group to its profinite completion with the respective identifications of the main theorems of Local and Global CFT, then commutes.

We will begin by spending several weeks setting up CFT for quadratic extensions of local fields and $\mathbb{Q}$, since this nicely captures what is exciting about the subject, and is more hands-on than the cohomological approach we will develop afterwards. To start, let K be any field of characteristic $\mathrm{char}(K) \neq 2$. Let $\mathrm{Gal}_2(K)$ be the maximal quotient of $\mathrm{Gal}(K)$ in which $g^2 = 1$ for all $g \in \mathrm{Gal}(K)$. It is necessarily abelian, so there is a surjection

$$\mathrm{Gal}^{\mathrm{ab}}(K) \twoheadrightarrow \mathrm{Gal}_2(K),$$

and it carries the structure of an $\mathbb{F}_2$-vector space.

Claim 1.8. *There is a canonical isomorphism*

$$\mathrm{Gal}_2(K) \simeq (K^\times/(K^\times)^2)^\vee := \mathrm{Hom}(K^\times/(K^\times)^2, \mathbb{Z}/2\mathbb{Z})$$

of $\mathbb{F}_2$-vector spaces.

Proof. We first construct such a map as follows: given $\sigma \in \mathrm{Gal}_2(K)$, define $\chi_\sigma \in (K^\times/(K^\times)^2)^\vee$ by

$$\chi_\sigma \colon K^\times/(K^\times)^2 \to \mathbb{Z}/2\mathbb{Z},$$
$$d \mapsto \begin{cases} 0 & \text{if } \sigma(\sqrt{d}) = \sqrt{d}, \\ 1 & \text{if } \sigma(\sqrt{d}) = -\sqrt{d}. \end{cases}$$

It is easy to see that this is, in fact, a homomorphism: given $\sigma_1, \sigma_2 \in \mathrm{Gal}_2(K)$ and $d \in K^\times/(K^\times)^2$, we have

$$(\sigma_1\sigma_2)(\sqrt{d}) = (-1)^{\chi_{\sigma_1}(d)}(-1)^{\chi_{\sigma_1}(d)}\sqrt{d},$$

which implies that

$$\chi_{\sigma_1\sigma_2} = \chi_{\sigma_1} + \chi_{\sigma_2}.$$

Now, since both the source and target are profinite 2-torsion abelian groups, it suffices to show that this map is an isomorphism after taking continuous duals. As usual, we have

$$\mathrm{Hom}_{\mathrm{cts}}((K^\times/(K^\times)^2)^\vee, \mathbb{Z}/2\mathbb{Z}) = K^\times/(K^\times)^2,$$

and giving a continuous map $\mathrm{Gal}_2(K) \to \mathbb{Z}/2\mathbb{Z}$ is the same as giving a quadratic extension $K^{\mathrm{sep}}/F/K$, which has the form $K(\sqrt{d})$ with $d \in K^\times$ defined up to multiplication by a square. □

Example 1.9. In the case $K = \mathbb{Q}$, this result gives an isomorphism

$$\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \xrightarrow{\simeq} \bigoplus_p \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z},$$

where the direct sum ranges over all primes p. However, it's not at all clear how to compare this group to the profinite completion

$$\left[\mathbb{Q}^\times \backslash \mathbb{A}_\mathbb{Q}^\times/(\mathbb{A}_\mathbb{Q}^\times)^2\right]^\wedge,$$

as the main theorem of GCFT would have us do.

Now, if K is a local field, then LCFT predicts that $K^\times/(K^\times)^2$ is canonically self-dual; the pairing

$$(\cdot,\cdot)\colon K^\times/(K^\times)^2 \times K^\times/(K^\times)^2 \to \{1,-1\}$$

realizing this duality is called the *Hilbert symbol.* Our goal in the next few lectures will be to construct it and show that this is indeed the case.

MIT OpenCourseWare
https://ocw.mit.edu

18.786 Number Theory II: Class Field Theory
Spring 2016

For information about citing these materials or our Terms of Use, visit: https://ocw.mit.edu/terms.