NOTES ON CLASS FIELD THEORY, POSTECH SUMMER SCHOOL 2010

TERUYOSHI YOSHIDA

Contents

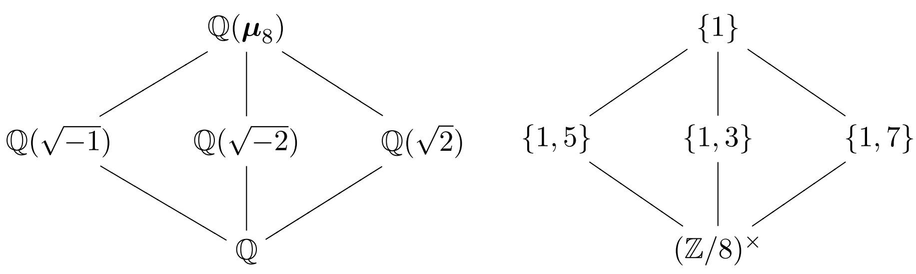
Preface

These are lecture notes I prepared for the Postech Summer School 2010: *Congruences of Modular Forms and Galois Representations* (July 2010). There must be typos and errors — I would very much appreciate if you could send the corrections to `teruyoshi@gmail.com`.

As a very brief introduction, let us observe, for an odd prime p:

(i) $\exists x, y \in \mathbb{Z},\ p = x^2 + y^2 \iff p \equiv 1 \pmod 4$,
(ii) $\exists x, y \in \mathbb{Z},\ p = x^2 + 2y^2 \iff p \equiv 1, 3 \pmod 8$,
(iii) $\exists x, y \in \mathbb{Z},\ p = x^2 - 2y^2 \iff p \equiv 1, 7 \pmod 8$.

Compare this with the Galois theory of corresponding quadratic fields, contained in $\mathbb{Q}(\boldsymbol{\mu}_8)$.



This beautiful correspondence is the first instance of class field theory over $\mathbb{Q}$.

Teruyoshi Yoshida
July 2010

Date: July 23, 2010; revised March 16, 2012.

Preliminaries: Galois theory, algebraic number theory

Algebras over rings. *Rings* are associative and commutative with a multiplicative identity 1. For a ring $\mathcal{O}$, its multiplicative group of units is denoted by $\mathcal{O}^\times$. An *$\mathcal{O}$-algebra* is a pair (A, φ) of ring A and a ring homomorphism $\varphi : \mathcal{O} \to A$ (the *structure morphism*), and a *morphism* of $\mathcal{O}$-algebras $f : (A, \varphi) \to (A', \varphi')$ is defined as a ring homomorphism $f : A \to A'$ such that $\varphi' = f \circ \varphi$. We often omit φ from the notation. Every ring is a $\mathbb{Z}$-algebra in a unique way. The category of $\mathcal{O}$-algebra has $\mathcal{O}$ as the initial object and the zero ring as the final object. The *tensor product* gives the direct sum, i.e. if A, A' are $\mathcal{O}$-algebras, we have canonical morphisms $i : A \to A \otimes_{\mathcal{O}} A'$ and $i' : A' \to A \otimes A'$ defined by $i(a) = a \otimes 1$ and $i(a') = 1 \otimes a'$, such that for every $\mathcal{O}$-algebra B,

$$\mathrm{Hom}_{\mathcal{O}}(A \otimes_{\mathcal{O}} A', B) \ni f \longmapsto (f \circ i,\ f \circ i') \in \mathrm{Hom}_{\mathcal{O}}(A, B) \times \mathrm{Hom}_{\mathcal{O}}(A', B)$$

is a bijection. An $\mathcal{O}$-algebra A is an *$\mathcal{O}$-subalgebra* of A' if it is a subring of A'. Every $\mathcal{O}$-algebra is an $\mathcal{O}$-module in a unique way, and $\mathrm{Hom}_{\mathcal{O}\text{-alg}}(A, A')$ injects into $\mathrm{Hom}_{\mathcal{O}\text{-mod}}(A, A')$. An $\mathcal{O}$-algebra A is *finite* if it is finitely generated as an $\mathcal{O}$-module. For an $\mathcal{O}$-algebra A, the union of all of its finite $\mathcal{O}$-subalgebras is called the *integral closure* of $\mathcal{O}$ in A. If A is an $\mathcal{O}$-algebra, then every A-algebra is an $\mathcal{O}$-algebra by the composition of structure morphisms.

Galois theory. Let F be a field. Its *charactersitic* $\mathrm{char}\, F \in \mathbb{N}$ is defined as a generator of the kernel of the structure morphism $\mathbb{Z} \to F$. For a field F, an F-algebra F' is called an *extension* F'/F if F' is a field. Morphisms of extensions of F are morphisms as F-algebras. Every morphism of extensions is injective. An extension F'/F is *finite* if F' is a finite F-algebra, and we write $[F' : F]$ for the dimension of F' as an F-vector space. Every endomorphism of a finite extension is an automorphism (by rank-nullity). A finite extension F'/F is *separable* if $|\mathrm{Hom}_F(F', E)| = [F' : F]$ for some extension E/F, and is *Galois* if we can take $E = F'$, in which case we call $\mathrm{Aut}_F(F') = \mathrm{Hom}_F(F', F')$ the *Galois group* of F'/F and denote by $\mathrm{Gal}(F'/F)$. If F'/F and F''/F' are finite extensions, then $[F'' : F] = [F'' : F'][F' : F]$. If moreover F''/F is Galois, then (i) F''/F' is Galois, and (ii) the left action of $\mathrm{Gal}(F''/F)$ on $\mathrm{Hom}_F(F', F'')$ is transitive, and the stabilizer of the structure morphism $F' \to F''$ is equal to $\mathrm{Gal}(F''/F')$. A Galois extension is called *abelian*, *cyclic* etc., if its Galois group is such. For a polynomial $P \in F[X]$, there is a finite extension F_P/F, unique up to isomorphism, such that, if E/F is an extension then P splits into linear factors in $E[X]$ if and only if $\mathrm{Hom}_F(F_P, E) \neq \emptyset$. This F_P is called the *splitting field* of P over F. If P and its derivative are coprime in $F[X]$, then F_P/F is Galois.

An extension (that is not necessarily finite) is called *separable* if it is a direct limit of finite separable extensions. A separable extension E/F is called *Galois* if it is a direct limit of finite Galois extensions E_λ/F, and its *Galois group* $\mathrm{Gal}(E/F) := \mathrm{Aut}_F(E)$ is equal to

$$\mathrm{Aut}_F(E) \subset \mathrm{Hom}_F(E, E) \xrightarrow{\cong} \varprojlim \mathrm{Hom}_F(E_\lambda, E) \xrightarrow{\cong} \varprojlim \mathrm{Gal}(E_\lambda/F) \subset \mathrm{Aut}_F(E),$$

because E_λ/F Galois implies $\mathrm{Hom}_F(E_\lambda, E) \cong \mathrm{Gal}(E_\lambda/F)$ under the canonical map $E_\lambda \to E$. A separable extension E/F is called a *separable closure* of F if every separable extension E'/E satisfies $E' \cong E$. Separable closure of F is unique up to isomorphism, and we usually fix one of them and denote by $\overline{F}$. Its Galois group $G_F := \mathrm{Gal}(\overline{F}/F)$ is called the *absolute Galois group* of F. Every separable extension of F is isomorphic to a *subextension* (i.e. an F-subalgebra) of $\overline{F}$. If E/F is Galois, then it is isomorphic to a unique (as a subset) subextension of $\overline{F}$. The *maximal abelian extension* F^{ab} is the union of all finite abelian subextensions of $\overline{F}/F$. Its Galois group $G_F^{\mathrm{ab}} := \mathrm{Gal}(F^{\mathrm{ab}}/F)$ is an abelian quotient of G_F. If F'/F is finite separable and $x \in F$, then $N_{F'/F}(x) := \prod_{\sigma \in \mathrm{Hom}_F(F', \overline{F})} \sigma(x)$ lies in F, and defines a homomorphism $N_{F'/F} : F'^\times \to F^\times$ (the *norm*).

Finite fields. If F is a field with $\operatorname{char} F = p > 0$, then F contains $\mathbb{F}_p := \mathbb{Z}/(p)$ as the image of $\mathbb{Z} \to F$, and $\mathrm{Fr}_p \in \mathrm{Hom}_{\mathbb{F}_p}(F, F)$ is defined by $\mathrm{Fr}_p(x) = x^p$. If F is a *finite field*, i.e. $q := |F| < \infty$, then it must have characteristic $p > 0$ and is finite over $\mathbb{F}_p$, thus if $f := [F : \mathbb{F}_p]$ then $q = p^f$. As $F^\times$ is cyclic of order $q - 1$, its elements are the q roots of $X^q - X$. Thus there is a unique subfield of $\overline{\mathbb{F}}_p$ with q elements, denoted by $\mathbb{F}_q$, and $\mathbb{F}_q \subset \mathbb{F}_{q'}$ if and only if $q' = q^n$ for some $n \in \mathbb{Z}_{>0}$. Every finite extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a Galois extension, with $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \langle \mathrm{Frob}_q \rangle$ where $\mathrm{Frob}_q := \mathrm{Fr}_p^{-f}$. We define isomorphisms $v_n : \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \xrightarrow{\cong} \mathbb{Z}/n\mathbb{Z}$ by $v_n(\mathrm{Frob}_q) = 1$, which satisfies $v_n|_{\mathbb{F}_{q^m}} = v_m$ for $m \mid n$.

Number fields. For an integral domain $\mathcal{O}$, there is an $\mathcal{O}$-algebra F, unique up to isomorphism, such that (i) F is a field, and (ii) if an $\mathcal{O}$-algebra F' is a field, then F'/F is an extension in a unique way, i.e. the structure morphism $\mathcal{O} \to F'$ uniquely factors through $\mathcal{O} \to F$. This F is called the *field of fractions* of $\mathcal{O}$ and is denoted by $\mathrm{Frac}(\mathcal{O})$. The field of *rational numbers* $\mathbb{Q}$ is defined as $\mathrm{Frac}(\mathbb{Z})$. A finite extension of $\mathbb{Q}$ is called a *number field*, often seen as a subfield of $\overline{\mathbb{Q}}$.

An integral domain $\mathcal{O}$ is called *integrally closed* if its integral closure in $\mathrm{Frac}(\mathcal{O})$ is $\mathcal{O}$ itself. Every UFD is integrally closed. An integrally closed noetherian domain is called a *Dedekind domain* if its non-zero prime ideals are all maximal. In a Dedekind domain, every ideal $I \neq 0, \mathcal{O}$ is written uniquely as a product of maximal ideals. If $\mathcal{O}$ is a ring and $\mathfrak{p}$ is its prime ideal, there is an $\mathcal{O}$-algebra $\mathcal{O}_\mathfrak{p}$, unique up to isomorphism, such that if (A, φ) is an $\mathcal{O}$-algebra and $\varphi(\mathcal{O} \setminus \mathfrak{p}) \subset A^\times$, then φ uniquely factors through $\mathcal{O} \to \mathcal{O}_\mathfrak{p}$. This $\mathcal{O}_\mathfrak{p}$ is called the *localization* of $\mathcal{O}$, and is a *local ring*, i.e. a ring with a unique maximal ideal. If $\mathcal{O}$ is an integral domain, then $\mathcal{O}_\mathfrak{p}$ is isomorphic to a unique subring of $\mathrm{Frac}(\mathcal{O})$, and canonically $\mathrm{Frac}(\mathcal{O}_\mathfrak{p}) \cong \mathrm{Frac}(\mathcal{O})$. If $\mathcal{O}$ is a Dedekind domain and $\mathfrak{p}$ is its maximal ideal, then $\mathcal{O}_\mathfrak{p}$ is a *discrete valuation ring*, or *DVR*, i.e. a local ring which is a PID but not a field. Every DVR is a Dedekind domain. If $\mathcal{O}$ is a DVR with the maximal ideal $\mathfrak{p}$ and $F = \mathrm{Frac}(\mathcal{O})$, then its (normalized) *valuation* is a unique surjective homomorphism $v : F^\times \to \mathbb{Z}$ of abelian groups such that (i) $\operatorname{Ker} v = \mathcal{O}^\times$, (ii) $v(x) \geq 0$ if and only if $x \in \mathcal{O}$. Then $v(x) > 0$ if and only if $x \in \mathfrak{p}$. An element $\varpi \in \mathfrak{p}$ with $v(\varpi) = 1$ is called a *uniformizer* of $\mathcal{O}$, and the set of all uniformizers of $\mathcal{O}$ is equal to $\{u\varpi \mid u \in \mathcal{O}^\times\}$. If $\mathcal{O}$ is a local ring with the maximal ideal $\mathfrak{p}$, then $\mathcal{O}/\mathfrak{p}$ is called its *residue field*, and its *completion* is defined as $\widehat{\mathcal{O}} := \varprojlim \mathcal{O}/\mathfrak{p}^m$, an inverse limit as $\mathcal{O}$-algebras. A local ring $\mathcal{O}$ is *complete* if $\mathcal{O} \cong \widehat{\mathcal{O}}$, and the completion of a local ring is a complete local ring with the maximal ideal $\widehat{\mathfrak{p}} := \mathfrak{p}\widehat{\mathcal{O}}$ and $\mathcal{O}/\mathfrak{p} \cong \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$. If $\mathcal{O}$ is a DVR, then $\widehat{\mathcal{O}}$ is a DVR, every uniformizer of $\mathcal{O}$ is a uniformizer of $\widehat{\mathcal{O}}$, and $\mathrm{Frac}(\widehat{\mathcal{O}}) \cong \mathrm{Frac}(\mathcal{O}) \otimes_\mathcal{O} \widehat{\mathcal{O}}$. The *ring of p-adic numbers* $\mathbb{Z}_p$ is defined as the completion of $\mathbb{Z}_{(p)}$, and $\mathbb{Q}_p := \mathrm{Frac}(\mathbb{Z}_p)$ is called the *p-adic field*.

Let $\mathcal{O}$ be a Dedekind domain and $F = \mathrm{Frac}(\mathcal{O})$. For a finite separable extension F'/F, the integral closure $\mathcal{O}'$ of $\mathcal{O}$ in F' is a finite $\mathcal{O}$-algebra, is a Dedekind domain, and $F \otimes_\mathcal{O} \mathcal{O}' \cong F'$. In this case, if $\mathfrak{p}'$ is a maximal ideal of $\mathcal{O}'$, then $\mathfrak{p} = \mathfrak{p}' \cap \mathcal{O}$ is a maximal ideal of $\mathcal{O}$, and we say $\mathfrak{p}'$ *lies above* $\mathfrak{p}$ and write $\mathfrak{p}' \mid \mathfrak{p}$. The residue field of $\mathcal{O}'_{\mathfrak{p}'}$ is a finite extension of that of $\mathcal{O}_\mathfrak{p}$. For a maximal ideal $\mathfrak{p}$ of $\mathcal{O}$, there are only finitely many maximal ideals of $\mathcal{O}'$ lying above $\mathfrak{p}$, and we have $\mathcal{O}' \otimes_\mathcal{O} \widehat{\mathcal{O}}_\mathfrak{p} \cong \prod_{\mathfrak{p}' \mid \mathfrak{p}} \widehat{\mathcal{O}}'_{\mathfrak{p}'}$. In particular, if $\mathcal{O}$ is a complete DVR, then so is $\mathcal{O}'$. Writing $F_\mathfrak{p} := \mathrm{Frac}(\widehat{\mathcal{O}}_\mathfrak{p})$ and $F'_{\mathfrak{p}'} := \mathrm{Frac}(\widehat{\mathcal{O}}'_{\mathfrak{p}'})$ and tensoring F, we get $F' \otimes_F F_\mathfrak{p} \cong \prod_{\mathfrak{p}' \mid \mathfrak{p}} F'_{\mathfrak{p}'}$, and $F'_{\mathfrak{p}'}/F_\mathfrak{p}$ is a finite extension. We call $F_\mathfrak{p}$ the *completion* of F at $\mathfrak{p}$. If F is a number field, the *ring of integers* $\mathcal{O} = \mathcal{O}_F$ of F is defined as the integral closure of $\mathbb{Z}$ in F.

Lecture 1. CFT of $\mathbb{Q}$: classical (Mo. 19/7/10, 9:40–10:40)

We are interested in the *Galois representations* of a number field F, i.e. finite dimensional representations of G_F, and the *class field theory* is a theory of 1-dimensional Galois representations. In general, class field theory of a field F describes G_F^{ab} in terms of the base field F. When $F = \mathbb{Q}$, this has an explicit description by *cyclotomic fields*.

Galois groups. Let F'/F be an extension of fields. The union E/F of all finite subextensions of $\overline{F'}/F$ is isomorphic to $\overline{F}/F$, and every element of $\mathrm{Aut}_F(\overline{F'})$ stabilizes E. Thus we have

$$G_{F'} \ni \sigma \longmapsto \sigma|_E \in \mathrm{Gal}(E/F) \xrightarrow{\cong} G_F,$$

where the last isomorphism is given each time we fix an isomorphism $\overline{F} \cong E$, or an element in $\mathrm{Hom}_F(\overline{F}, \overline{F'})$. A different choice results in conjugation by an element of G_F. The same argument applies to F^{ab} and F'^{ab}, which gives a well-defined homomorphism $G_{F'}^{\mathrm{ab}} \to G_F^{\mathrm{ab}}$, that is compatible with any homomorphism $G_{F'} \to G_F$ obtained as above.

Cyclotomic extensions. Let F be a field, and let $N \in \mathbb{Z}_{>0}$ with $(\mathrm{char}\, F, N) = 1$. The *cyclotomic extension* $F(\boldsymbol{\mu}_N)$ is defined as a splitting field of $X^N - 1$ over F, and $\boldsymbol{\mu}_N$ is the set of roots of $X^N - 1$ in $F(\boldsymbol{\mu}_N)$. If $M \mid N$ then $F(\boldsymbol{\mu}_M) \subset F(\boldsymbol{\mu}_N)$, and their direct limit, or their union $F^{\mathrm{cyc}} := \bigcup_N F(\boldsymbol{\mu}_N)$ inside F^{ab}, is the *maximal cyclotomic extension* of F. The Galois group $G_F^{\mathrm{cyc}} := \mathrm{Gal}(F^{\mathrm{cyc}}/F)$ is a quotient of G_F. For example, every finite extension of finite fields is cyclotomic because $\mathbb{F}_{q^n} = \mathbb{F}_q(\boldsymbol{\mu}_{q^n-1})$, and thus $\overline{\mathbb{F}}_q = \mathbb{F}_q^{\mathrm{cyc}}$. Its absolute Galois group is given by the inverse limit of the isomorphisms v_n (see Preliminaries), namely:

$$v = \varprojlim v_n : \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \ni \mathrm{Frob}_q \xmapsto{\cong} 1 \in \widehat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n\mathbb{Z}.$$

Here $\widehat{\mathbb{Z}}$ is the additive group of the *profinite completion* $\widehat{\mathbb{Z}} := \varprojlim \mathbb{Z}/(N)$ of $\mathbb{Z}$, the inverse limit taken as rings, with respect to the natural surjections $\mathbb{Z}/(N) \to \mathbb{Z}/(M)$ for $M \mid N$. The *Chinese remainder theorem* says $\mathbb{Z}/(N) \cong \prod_{p|N} \mathbb{Z}/(p^m)$ when p^m is the exact power of p dividing N, and as the inverse limits commute with direct products, we have:

$$\widehat{\mathbb{Z}} \cong \textstyle\prod_p \mathbb{Z}_p, \quad \mathbb{Z}_p = \varprojlim \mathbb{Z}/p^m,$$

and also a variant $\widehat{\mathbb{Z}}^p := \varprojlim_{(p,N)=1} \mathbb{Z}/(N) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$.

In general, for each N prime to $\mathrm{char}\, F$, there is a canonical injection

$$\chi_N : \mathrm{Gal}(F(\boldsymbol{\mu}_N)/F) \ni \big(\zeta \mapsto \zeta^i,\ \forall \zeta \in \boldsymbol{\mu}_N\big) \longmapsto i \bmod N \in (\mathbb{Z}/(N))^\times,$$

by which we see $F(\boldsymbol{\mu}_N)/F$ is *abelian* and thus $F^{\mathrm{cyc}} \subset F^{\mathrm{ab}}$. The inverse limit of χ_N gives an injection:

$$\chi_F := \varprojlim \chi_N : G_F^{\mathrm{cyc}} \longrightarrow \begin{cases} \widehat{\mathbb{Z}}^\times = \varprojlim (\mathbb{Z}/(N))^\times & (\mathrm{char}\, F = 0), \\ \widehat{\mathbb{Z}}^{p,\times} = \varprojlim_{(p,N)=1} (\mathbb{Z}/(N))^\times & (\mathrm{char}\, F = p). \end{cases}$$

We see that when $F = \mathbb{F}_q$, then the image of $\chi_{\mathbb{F}_q}$ is $\{q^a \mid a \in \widehat{\mathbb{Z}}\}$, which is well-defined as $q^a \bmod N$ depends only on $a \bmod n$, where $N \mid q^n - 1$ or $q^n \equiv 1 \pmod N$. The group G_F^{cyc} is functorial under extensions F'/F, and we have $\chi_{F'} = \chi_F \circ (G_{F'}^{\mathrm{cyc}} \to G_F^{\mathrm{cyc}})$. We sometimes confuse χ_F with $\chi_F \circ (G_F^{\mathrm{ab}} \to G_F^{\mathrm{cyc}})$.

For any field F of characteristic 0, we have a surjection $G_F^{\mathrm{ab}} \to G_F^{\mathrm{cyc}}$, followed by an injection $\chi_F : G_F^{\mathrm{cyc}} \to \widehat{\mathbb{Z}}^\times$. The class field theory of $\mathbb{Q}$ tells us that they are both isomorphisms when $F = \mathbb{Q}$ (but χ_F is rarely an isomorphism for general F).

Decomposition law. Let $\mathcal{O}$ be a Dedekind domain and $F = \mathrm{Frac}(\mathcal{O})$. If F'/F is a finite *Galois* extension, then $G = \mathrm{Gal}(F'/F)$ acts on the integral closure $\mathcal{O}'$ of $\mathcal{O}$ in F'. If $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}$, then G acts transitively on the set $X_\mathfrak{p}$ of all maximal ideals of $\mathcal{O}'$ lying above $\mathfrak{p}$. Suppose that $k_\mathfrak{p}$ is *perfect*, i.e. its finite extension is always separable. If $\mathfrak{p}' \in X_\mathfrak{p}$ and $k_\mathfrak{p}, k_{\mathfrak{p}'}$ are the residue fields of $\mathfrak{p}, \mathfrak{p}'$ respectively, then $k_{\mathfrak{p}'}/k_\mathfrak{p}$ is finite Galois, and the stabilizer $D_{\mathfrak{p}'}$ of $\mathfrak{p}'$ surjects onto $\mathrm{Gal}(k_{\mathfrak{p}'}/k_\mathfrak{p})$ by $\sigma \mapsto (\sigma|_{\mathcal{O}'} \bmod \mathfrak{p}')$. We say $\mathfrak{p}$ is *unramified* in $\mathcal{O}'$ (or F') if $\mathfrak{p}\mathcal{O}'$ is the product of all elements of $X_\mathfrak{p}$ without multiplicities; in this case $D_{\mathfrak{p}'} \cong \mathrm{Gal}(k_{\mathfrak{p}'}/k_\mathfrak{p})$ for all $\mathfrak{p}' \in X_\mathfrak{p}$.

Now assume that $k_\mathfrak{p} \cong \mathbb{F}_q$. The element $\mathrm{Frob}_{\mathfrak{p}'} \in D_{\mathfrak{p}'}$ which maps to $\mathrm{Frob}_q \in \mathrm{Gal}(k_{\mathfrak{p}'}/k_\mathfrak{p})$ is called the *geometric Frobenius* of $\mathfrak{p}'$, and its order is equal to $|D_{\mathfrak{p}'}| = [k_{\mathfrak{p}'} : k_\mathfrak{p}]$. Changing $\mathfrak{p}'$ conjugates $D_{\mathfrak{p}'}$ and $\mathrm{Frob}_{\mathfrak{p}'}$, so the conjugacy class of $\mathrm{Frob}_{\mathfrak{p}'}$ in G is determined by $\mathfrak{p}$. This conjugacy class (which we denote by $\mathrm{Frob}_\mathfrak{p}$) determines $|X_\mathfrak{p}|$ by $|G| = |D_{\mathfrak{p}'}||X_\mathfrak{p}|$. This gives the *decomposition law* of primes as follows: if f is the order of $\mathrm{Frob}_\mathfrak{p}$ in G and $g = [F' : F]/f$, then $\mathfrak{p}\mathcal{O}' = \mathfrak{p}'_1 \cdots \mathfrak{p}'_g$.

If $F' = F(\boldsymbol{\mu}_N)$, then $\mathfrak{p}$ is unramified if $\mathrm{char}\, k_\mathfrak{p}$ is prime to N, because if $(\zeta \mapsto \zeta^i)$ is in $\mathrm{Ker}\,(D_{\mathfrak{p}'} \to \mathrm{Gal}(k_{\mathfrak{p}'}/k_\mathfrak{p}))$ then $\zeta^i - \zeta \in \mathfrak{p}'$, which implies $i \equiv 1 \bmod N$, because $\prod_{i=1}^{N-1}(1 - \zeta^i) = N \notin \mathfrak{p}'$. The geometric Frobenius must be $(\zeta \mapsto \zeta^q)^{-1}$, thus we see $\chi_N(\mathrm{Frob}_\mathfrak{p}) = (q \bmod N)^{-1}$, and the order of $\mathrm{Frob}_\mathfrak{p}$ in G is equal to the order of q in $(\mathbb{Z}/(N))^\times$ (the *reciprocity law*).

Let $\mathrm{char}\, F = 0$ and $\mathrm{char}\, k_\mathfrak{p} = p$. In order to describe the reciprocity law in the limit, define $F^{\mathrm{cyc},p} := \bigcup_{(p,N)=1} F(\boldsymbol{\mu}_N)$ inside F^{cyc}. As $\mathfrak{p}$ is unramified in all $F(\boldsymbol{\mu}_N)/F$ for $(p, N) = 1$, the element $\mathrm{Frob}_\mathfrak{p} \in G_F^{\mathrm{cyc},p} := \mathrm{Gal}(F^{\mathrm{cyc},p}/F)$ is well-defined, and we have the injection

$$\chi_F^p := \varprojlim \chi_N : G_F^{\mathrm{cyc},p} \to \widehat{\mathbb{Z}}^{p,\times},$$

and $\chi_F^p(\mathrm{Frob}_\mathfrak{p}) = q^{-1} \in \widehat{\mathbb{Z}}^{p,\times}$.

Class field theory of $\mathbb{Q}$. Now let $F = \mathbb{Q}$. For $N \in \mathbb{Z}_{>0}$, we have $\chi_N(\mathrm{Frob}_{(p)}) = (p \bmod N)^{-1}$ for all p prime to N, thus χ_N is surjective, hence bijective. So are $\chi_\mathbb{Q}$ and $\chi_\mathbb{Q}^p$ for each p, by passing to the limit.

Theorem 1.1. (class field theory of $\mathbb{Q}$)

(i) (irreducibility of cyclotomic polynomials) *The injections χ_N are isomorphisms for all $N \in \mathbb{Z}_{>0}$. In particular, we have $\chi_\mathbb{Q} : G_\mathbb{Q}^{\mathrm{cyc}} \xrightarrow{\cong} \widehat{\mathbb{Z}}^\times$.*

(ii) (reciprocity law) *For each prime p, we have $\chi_\mathbb{Q}^p(\mathrm{Frob}_{(p)}) = p^{-1} \in \widehat{\mathbb{Z}}^{p,\times}$.*

(iii) (Kronecker-Weber theorem) $\mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}^{\mathrm{ab}}$, *i.e.* $G_\mathbb{Q}^{\mathrm{ab}} = G_\mathbb{Q}^{\mathrm{cyc}}$.

ℓ-adic variant. As $\widehat{\mathbb{Z}}^\times \cong \prod_\ell \mathbb{Z}_\ell^\times$, for each prime $\ell \neq \mathrm{char}\, F$, we can define a homomorphism $\chi_\ell := (\widehat{\mathbb{Z}}^\times \to \mathbb{Z}_\ell^\times) \circ \chi_F : G_F^{\mathrm{ab}} \to \mathbb{Z}_\ell^\times$, called the *$\ell$-adic cyclotomic character* of F. For any extension F'/F, the χ_ℓ of F' is the composite of χ_ℓ of F with $G_{F'}^{\mathrm{ab}} \to G_F^{\mathrm{ab}}$. It factors through $\mathrm{Gal}(F(\boldsymbol{\mu}_{\ell^\infty})/F) \to \mathbb{Z}_\ell^\times$, where $F(\boldsymbol{\mu}_{\ell^\infty}) := \bigcup_m F(\boldsymbol{\mu}_{\ell^m})$.

If $F = \mathrm{Frac}(\mathcal{O})$ for a Dedekind domain $\mathcal{O}$, a maximal ideal $\mathfrak{p}$ is unramified in $F(\boldsymbol{\mu}_{\ell^m})$ as long as $\mathrm{char}\, k_\mathfrak{p} \neq \ell$. If $k_\mathfrak{p}$ is finite, then we have $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(F(\boldsymbol{\mu}_{\ell^\infty})/F)$, and $\chi_\ell(\mathrm{Frob}_\mathfrak{p}) = q^{-1} \in \mathbb{Z}_\ell^\times$. In particular, when $F = \mathbb{Q}$ we have $\chi_\ell(\mathrm{Frob}_{(p)}) = p^{-1} \in \mathbb{Z}_\ell^\times$ for all $p \neq \ell$.

Lecture 2. CFT of $\mathbb{Q}$: via adeles (Mo. 19/7/10, 11:00–12:00)

Adeles and ideles. The *ring of finite adeles* is a $\mathbb{Q}$-algebra defined as $\mathbb{A}^\infty := \mathbb{Q} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$, and the *ring of adeles* is defined as $\mathbb{A} := \mathbb{R} \times \mathbb{A}^\infty$, a direct product of $\mathbb{Q}$-algebras. Its group of units $\mathbb{A}^\times = \mathbb{R}^\times \times (\mathbb{A}^\infty)^\times$ is called the *group of ideles*, and historically came before adeles — "adele" was a shorthand for *additive idele*). The structure morphism $\mathbb{Q} \to \mathbb{A}$ is injective, thus gives a subgroup $\mathbb{Q}^\times \subset \mathbb{A}^\times$. We also view the components $\mathbb{R}^\times, (\mathbb{A}^\infty)^\times$ as subgroups of $\mathbb{A}^\times$, and they respectively have subgroups $\mathbb{R}^\times_{>0}$ (the positive real numbers) and $\widehat{\mathbb{Z}}^\times$; the ring homomorphism $\widehat{\mathbb{Z}} \to \mathbb{A}^\infty$ is injective as $\widehat{\mathbb{Z}}$ is $\mathbb{Z}$-torsion free, thus $\widehat{\mathbb{Z}}^\times \subset (\mathbb{A}^\infty)^\times$.

Lemma 2.1. *The group $\mathbb{A}^\times$ is a direct product of its subgroups $\mathbb{Q}^\times$, $\mathbb{R}^\times_{>0}$, and $\widehat{\mathbb{Z}}^\times$.*

The proof is a straightforward exercise using the fact that $\mathbb{Z}$ is a UFD and that $\mathbb{Z}^\times = \{\pm 1\}$ (hence *inside* $(\mathbb{A}^\infty)^\times$, we have $\mathbb{Q}^\times \cap \widehat{\mathbb{Z}}^\times = \mathbb{Z}^\times = \{\pm 1\}$ and $\mathbb{Q}^\times_{>0} \cap \widehat{\mathbb{Z}}^\times = \{1\}$). This shows that $\widehat{\mathbb{Z}}^\times$ is a quotient of $\mathbb{A}^\times$. The composite

$$\mathrm{Art} : \mathbb{A}^\times \to \mathbb{Q}^\times \backslash \mathbb{A}^\times / \mathbb{R}^\times_{>0} \xrightarrow{\cong} \widehat{\mathbb{Z}}^\times \xrightarrow{\cong} G_{\mathbb{Q}}^{\mathrm{cyc}} = G_{\mathbb{Q}}^{\mathrm{ab}}$$

(the last map is $\chi_{\mathbb{Q}}^{-1}$) is called the *global Artin map of* $\mathbb{Q}$. The quotient group $\mathbb{Q}^\times \backslash \mathbb{A}^\times \cong \widehat{\mathbb{Z}}^\times \times \mathbb{R}^\times_{>0}$ is the *idele class group* of $\mathbb{Q}$, and its characters are called the *Hecke characters* of $\mathbb{Q}$ — these are the *automorphic representations of $GL_1(\mathbb{A})$* — and the ones which factor through $\widehat{\mathbb{Z}}^\times$, the *Dirichlet characters.* The projection to the other part $\mathbb{A}^\times \to \mathbb{Q}^\times \backslash \mathbb{A}^\times / \widehat{\mathbb{Z}}^\times \xrightarrow{\cong} \mathbb{R}^\times_{>0}$ is called the *absolute value* $|\cdot|$, a basic example of a (non-Dirichlet) Hecke character.

Restricted products. Recall $\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$ (Chinese remainder theorem). Tensoring $\mathbb{Q}$ does not commute with the (infinite) direct product, but as $\mathbb{Q} \otimes_{\mathbb{Z}} -$ is a functor, it gives a $\mathbb{Q}$-algebra homomorphism $\mathbb{A}^\infty \longrightarrow \prod_p \mathbb{Q}_p$ (note $\mathbb{Q}_p = \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_p$). This is seen to be an injection, and we identify $\mathbb{A}^\infty$ with its image, a subring of $\prod_p \mathbb{Q}_p$ (the *restricted product*). This homomorphism induces $(\mathbb{A}^\infty)^\times \to \prod_p \mathbb{Q}_p^\times$ as well. Thus:

$$\mathbb{A}^\infty = \Big\{ (x_p) \in \prod_p \mathbb{Q}_p \;\Big|\; x_p \in \mathbb{Z}_p \text{ for almost all } p \Big\}, \text{ and}$$

$$(\mathbb{A}^\infty)^\times = \Big\{ (x_p) \in \prod_p \mathbb{Q}_p^\times \;\Big|\; x_p \in \mathbb{Z}_p^\times \text{ for almost all } p \Big\},$$

where *almost all p* means "except for finitely many p". Therefore we obtain the injection $\mathbb{Q}_p^\times \ni x_p \mapsto (1, \ldots, 1, x_p, 1, \ldots) \in (\mathbb{A}^\infty)^\times \subset \mathbb{A}^\times$, similar to the injection $\mathbb{R}^\times \to \mathbb{A}^\times$. This is a section of the projection maps $\mathbb{A}^\times \to (\mathbb{A}^\infty)^\times \to \mathbb{Q}_p^\times$ coming from the natural ring homomorphisms.

Artin map and the reciprocity law. As we see that the images of these injections from $\mathbb{Q}_p^\times$'s and $\mathbb{R}^\times$ generates $\mathbb{A}^\times$, we can characterize Art by their restrictions to $\mathbb{Q}_p^\times$ and $\mathbb{R}^\times$. We know that $\mathrm{Art}|_{\mathbb{R}^\times} : \mathbb{R}^\times \to \mathbb{R}^\times / \mathbb{R}^\times_{>0} = \{\pm 1\} \xrightarrow{\cong} \{1, c\}$ where c, or $\mathrm{Frob}_{\mathbb{R}}$, is the *complex conjugate* on $\mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}^{\mathrm{ab}}$ defined by $\zeta \mapsto \zeta^{-1}$ for all $\zeta \in \boldsymbol{\mu}_N$. As for $\mathrm{Art}|_{\mathbb{Q}_p^\times}$, at least we know its image in the quotient $\mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc},p}/\mathbb{Q})$ of $G_{\mathbb{Q}}^{\mathrm{cyc}} = G_{\mathbb{Q}}^{\mathrm{ab}}$. Consider the following diagram.

$$\begin{array}{ccccccc}
\mathbb{Q}_p^\times & \longrightarrow & \mathbb{A}^\times & \longrightarrow & \widehat{\mathbb{Z}}^\times & \xleftarrow[\cong]{\chi_{\mathbb{Q}}} & G_{\mathbb{Q}}^{\mathrm{cyc}} \\
\downarrow & & & & \downarrow & & \downarrow \\
\mathbb{Q}_p^\times / \mathbb{Z}_p^\times & & \xrightarrow{(p \bmod \mathbb{Z}_p^\times) \longmapsto p^{-1}} & & \widehat{\mathbb{Z}}^{p,\times} & \xleftarrow[\cong]{\chi_{\mathbb{Q}}^p} & G_{\mathbb{Q}}^{\mathrm{cyc},p}
\end{array}$$

In the bottom-right corner, the reciprocity law singles out the element $p^{-1} \in \widehat{\mathbb{Z}}^{p,\times}$ which is mapped to $\mathrm{Frob}_{(p)}$. The inverse image of this element in $\widehat{\mathbb{Z}}^\times$ is $(1, p^{-1}, \ldots, p^{-1}, u, p^{-1}, \ldots)$, where 1 is at $\mathbb{R}$ and $u \in \mathbb{Z}_p^\times$ is at $\mathbb{Q}_p$, which in turn are the images of $up \in \mathbb{Q}_p^\times$ (because $(1, p, p, p, \ldots) \in \mathbb{Q}^\times\mathbb{R}^\times_{>0}$), i.e. the set of all uniformizers of $\mathbb{Z}_p$. Incidentally, this shows that $|\cdot|_p := |\cdot||_{\mathbb{Q}_p^\times}$ is given by $\mathbb{Q}_p^\times/\mathbb{Z}_p^\times \to \mathbb{R}^\times_{>0}$, where $|\varpi|_p = p^{-1}$ for every uniformizer ϖ of $\mathbb{Z}_p$. Thus we can reformulate the class field theory of $\mathbb{Q}$ as follows:

Theorem 2.2. (class field theory of $\mathbb{Q}$; adelic version) *There is a homomorphism* $\mathrm{Art} : \mathbb{Q}^\times\backslash\mathbb{A}^\times \to G_{\mathbb{Q}}^{\mathrm{cyc}} = G_{\mathbb{Q}}^{\mathrm{ab}}$*, which satisfies* (i) $\mathrm{Art}|_{\mathbb{R}^\times} : \mathbb{R}^\times \to \mathbb{R}^\times/\mathbb{R}^\times_{>0} \cong \{1, \mathrm{Frob}_{\mathbb{R}}\}$*, and* (ii) *for each prime p and every uniformizer ϖ of $\mathbb{Q}_p$, we have* $\mathrm{Art}|_{\mathbb{Q}_p^\times}(\varpi)|_{\mathbb{Q}^{\mathrm{cyc},p}} = \mathrm{Frob}_{(p)}$ (reciprocity law). *It induces an isomorphism* $\mathrm{Art} : \mathbb{Q}^\times\backslash\mathbb{A}^\times/\mathbb{R}^\times_{>0} \xrightarrow{\cong} G_{\mathbb{Q}}^{\mathrm{ab}}$*.*

These "local" properties characterize $\mathrm{Art}_{F/\mathbb{Q}} : \mathbb{A}^\times \ni x \mapsto \mathrm{Art}(x)|_F \in \mathrm{Gal}(F/\mathbb{Q})$ for every finite abelian $F/\mathbb{Q}$: as $F \subset \mathbb{Q}(\boldsymbol{\mu}_N)$ for some N, the map $\mathrm{Art}_{F/\mathbb{Q}}$ factors through $(\mathbb{Z}/(N))^\times$, and $F \subset \mathbb{Q}^{\mathrm{cyc},p}$ for all p not dividing N. But $(\mathbb{Z}/(N))^\times$ is generated by the images of $\mathbb{Q}_p^\times$ for these primes, where $\mathrm{Art}_{F/\mathbb{Q}}|_{\mathbb{Q}_p^\times}$ factors through $\mathbb{Q}_p^\times/\mathbb{Z}_p^\times$ and is determined. We will see that the *image* of $\mathrm{Art}|_{\mathbb{Q}_p^\times}$ has a *local* description, namely almost the image of $G_{\mathbb{Q}_p}^{\mathrm{ab}}$ in $G_{\mathbb{Q}}^{\mathrm{ab}}$ (note that the image of $\mathrm{Art}|_{\mathbb{R}^\times}$ was the image of $G_{\mathbb{R}} = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ in $G_{\mathbb{Q}}^{\mathrm{ab}}$); this suggests that the Artin map decomposes into "local" maps (the *local class field theory*).

Places. Let F be a number field with the ring of integers $\mathcal{O}$. A *finite place* v of F above p, denoted $v|p$, is defined as a (left) $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-orbit of $\mathrm{Hom}_{\mathbb{Q}}(F, \overline{\mathbb{Q}}_p)$, and the orbit of λ is denoted by $v(\lambda)$. The places of F above p are in canonical bijection with the maximal ideals $\mathfrak{p}$ of $\mathcal{O}$ lying over (p), because $F \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_{\mathfrak{p}|(p)} F_{\mathfrak{p}}$ (see Preliminaries) implies

$$\mathrm{Hom}_{\mathbb{Q}}(F, \overline{\mathbb{Q}}_p) \cong \mathrm{Hom}_{\mathbb{Q}_p}(F \otimes_{\mathbb{Q}} \mathbb{Q}_p,\ \overline{\mathbb{Q}}_p) \cong \textstyle\coprod_{\mathfrak{p}|(p)} \mathrm{Hom}_{\mathbb{Q}_p}(F_{\mathfrak{p}}, \overline{\mathbb{Q}}_p),$$

and $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts transitively on $\mathrm{Hom}_{\mathbb{Q}_p}(F_{\mathfrak{p}}, \overline{\mathbb{Q}}_p)$. We write $F_v := F_{\mathfrak{p}}$ (the *completion* of F at v, a finite extension of $\mathbb{Q}_p$). Recall that $F_v := \mathrm{Frac}(\mathcal{O}_v)$, where $\mathcal{O}_v := \widehat{\mathcal{O}}_{\mathfrak{p}}$, and the residue field $k_v := \mathcal{O}_v/\mathfrak{p}\mathcal{O}_v$ is a finite extension of $\mathbb{F}_p := \mathbb{Z}/(p)$.

An *infinite place* v of F, written $v|\infty$, is defined as a $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-orbit of $\mathrm{Hom}_{\mathbb{Q}}(F, \mathbb{C})$. We have $F \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{v|\infty} F_v$, where $F_v \cong \mathbb{R}$ or $\mathbb{C}$ and accordingly v is called *real* or *complex*. If F'/F is a finite extension, a place v' of F' *lies above* a place v of F (denoted $v'|v$) if $v = v(\lambda)$, $v' = v(\lambda')$ and $\lambda'|_F = \lambda$. We often denote by u a place of $\mathbb{Q}$, i.e. a prime p or ∞, where $\mathbb{Q}_\infty := \mathbb{R}$. Note that $|\cdot|_\infty := |\cdot||_{\mathbb{R}^\times} : \mathbb{R}^\times \to \mathbb{R}^\times_{>0}$ is the usual absolute value.

Local fields. By a *local field*, we mean a finite extension K of $\mathbb{Q}_p$ for some prime p (occasionally $\mathbb{R}$ and $\mathbb{C}$ as well). The *ring of integers* $\mathcal{O}$ of K is defined as the integral closure of $\mathbb{Z}_p$ in K. This is a complete DVR, and uniformizers of $\mathcal{O}$ are called the *uniformizers* of K. Let $\mathfrak{p}$ be its maximal ideal, and $k = \mathcal{O}/\mathfrak{p}$ be its residue field. Then $k/\mathbb{F}_p$ is finite, so $k \cong \mathbb{F}_q$. We have the (normalized) valuation $v : K^\times \to \mathbb{Z}$. Let K'/K be a finite extension, and denote the corresponding objects by $\mathcal{O}', \mathfrak{p}', k', q'$ and v'. Then the *ramification index* $e = e(K'/K) \in \mathbb{Z}_{>0}$ is defined by $\mathfrak{p}\mathcal{O}' = (\mathfrak{p}')^e$, or equivalently $v'|_{K^\times} = ev$. The *residual degree* is $f = f(K'/K) := [k' : k] \in \mathbb{Z}_{>0}$. Then we have $[K' : K] = ef$, and $v \circ N_{K'/K} = fv'$, where $N_{K'/K} : K'^\times \to K^\times$ is the norm. We say K'/K is *unramified* if $e = 1$, and *totally ramified* if $f = 1$. If K'/K is Galois, then the kernel of the surjection $D_{\mathfrak{p}'} = \mathrm{Gal}(K'/K) \to \mathrm{Gal}(k'/k)$ has order e, thus it is an isomorphism if K'/K is unramified, sending $\mathrm{Frob}_K := \mathrm{Frob}_{\mathfrak{p}}$ to Frob_q.

Lecture 3. Local CFT, local-global compatibility (Tu. 20/7/10, 9:40–10:40)

Unramified extensions and Weil groups. Let K be a local field, finite over $\mathbb{Q}_p$. If $N \in \mathbb{Z}_{>0}$ is prime to p, then $K(\boldsymbol{\mu}_N)$ is an unramified extension, and $\chi_N : \mathrm{Gal}(K(\boldsymbol{\mu}_N)/K) \to (\mathbb{Z}/(N))^\times$ sends Frob_q to $q^{-1} \bmod N$. Thus $[K(\boldsymbol{\mu}_N) : K] = f$ where f is the order of $q \bmod N$ in $(\mathbb{Z}/(N))^\times$, and $K(\boldsymbol{\mu}_N) = K(\boldsymbol{\mu}_{q^f-1})$. We write $K_f := K(\boldsymbol{\mu}_{q^f-1})$, with the ring of integers $\mathcal{O}_f$. If K'/K is an unramified of degree f, then its residue field is $k' \cong \mathbb{F}_{q^f}$. Hence $K'(\boldsymbol{\mu}_{q_f-1})/K'$ is of degree 1 and $K_f \subset K'$, but they are equal as both have degree f over K. Thus K_f/K is a unique unramified extension of degree f inside $\overline{K}$. The *maximal unramified extension* of K is defined as $K^{\mathrm{ur}} := K^{\mathrm{cyc},p} = \bigcup_{(p,N)=1} K(\boldsymbol{\mu}_N) = \bigcup_f K_f$. The integral closure of $\mathcal{O}$ in K^{ur} is $\mathcal{O}^{\mathrm{ur}} = \bigcup_f \mathcal{O}_f$, which is a DVR with the maximal ideal $\mathfrak{p}\mathcal{O}^{\mathrm{ur}}$ and the residue field $\mathcal{O}^{\mathrm{ur}}/\mathfrak{p} \cong \overline{k}$, and the limit of the above isomorphisms gives

$$\mathrm{Gal}(K^{\mathrm{ur}}/K) \ni \sigma \overset{\cong}{\longmapsto} (\sigma|_{\mathcal{O}^{\mathrm{ur}}} \bmod \mathfrak{p}) \in \mathrm{Gal}(\overline{k}/k).$$

We computed the injection χ_K^p in Lecture 1; we have the following commutative diagram.

$$\begin{array}{ccccc}
\chi_K^p : \mathrm{Gal}(K^{\mathrm{ur}}/K) & \xrightarrow[\cong]{v:\mathrm{Frob}_K \mapsto 1} & \widehat{\mathbb{Z}} & \xrightarrow{1 \mapsto q^{-1}} & \widehat{\mathbb{Z}}^{p,\times} \\
\Big\downarrow{\scriptstyle \sigma \mapsto (\sigma|_{\mathcal{O}^{\mathrm{ur}}} \bmod \mathfrak{p})} & & \Big\| & & \Big\| \\
\chi_k : \mathrm{Gal}(\overline{k}/k) & \xrightarrow[\cong]{v:\mathrm{Frob}_q \mapsto 1} & \widehat{\mathbb{Z}} & \xrightarrow{1 \mapsto q^{-1}} & \widehat{\mathbb{Z}}^{p,\times}
\end{array}$$

For a Galois subextension L/K of $\overline{K}/K$ containing K^{ur}, we define its *Weil group* by $W(L/K) := \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma|_{K^{\mathrm{ur}}} \in \mathrm{Frob}_K^{\mathbb{Z}}\}$. It has the *valuation* $v : W(L/K) \to \mathbb{Z}$ by $\sigma|_{K^{\mathrm{ur}}} = \mathrm{Frob}_K^{v(\sigma)}$. We write $W_K := W(\overline{K}/K)$ (the *Weil group* of K), and similarly $W_K^{\mathrm{ab}} := W(K^{\mathrm{ab}}/K)$ and $W_K^{\mathrm{cyc}} := W(K^{\mathrm{cyc}}/K)$. If K'/K is finite, then $W_{K'} \subset W_K$.

Image of $\mathbb{Q}_p^\times$ *under* Art. The *local Kronecker-Weber theorem* tells us that $\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p^{\mathrm{cyc}}$, i.e. $W_{\mathbb{Q}_p}^{\mathrm{ab}} = W_{\mathbb{Q}_p}^{\mathrm{cyc}}$. Recall that $\chi_{\mathbb{Q}_p} = \chi_{\mathbb{Q}} \circ (G_{\mathbb{Q}_p}^{\mathrm{ab}} \to G_{\mathbb{Q}}^{\mathrm{ab}})$. As the cyclotomic polynomials $(X^{p^m}-1)/(X^{p^{m-1}}-1)$ for all $m \in \mathbb{Z}_{>0}$ are irreducible over $\mathbb{Q}_p^{\mathrm{ur}}$ by the Eisenstein criterion, the homomorphism $\chi_{\mathbb{Q}_p}$ restricts to an isomorphism $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{cyc}}/\mathbb{Q}_p^{\mathrm{ur}}) \cong \mathbb{Z}_p^\times$. This results in the following commutative diagram.

$$\begin{array}{ccccccc}
\mathbb{Z}_p^\times & \xrightarrow{\quad\mathrm{id}\quad} & \mathbb{Z}_p^\times & \xleftarrow{\cong} & \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}^{\mathrm{cyc},p}) & \xleftarrow{\cong} & \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{cyc}}/\mathbb{Q}_p^{\mathrm{ur}}) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\mathbb{Q}_p^\times \longrightarrow \mathbb{A}^\times & \longrightarrow & \widehat{\mathbb{Z}}^\times & \xleftarrow[\cong]{\chi_{\mathbb{Q}}} & G_{\mathbb{Q}}^{\mathrm{cyc}} & \longleftarrow & G_{\mathbb{Q}_p}^{\mathrm{cyc}} \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\mathbb{Q}_p^\times/\mathbb{Z}_p^\times & \xrightarrow{(p \bmod \mathbb{Z}_p^\times) \longmapsto p^{-1}} & \widehat{\mathbb{Z}}^{p,\times} & \xleftarrow[\cong]{\chi_{\mathbb{Q}}^p} & G_{\mathbb{Q}}^{\mathrm{cyc},p} & \longleftarrow & \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p)
\end{array}$$

This diagram proves that $\mathrm{Art}(\mathbb{Q}_p^\times) = W_{\mathbb{Q}_p}^{\mathrm{cyc}}$, or more precisely, the injective image of $\mathbb{Q}_p^\times$ in $\mathbb{Q}^\times\backslash\mathbb{A}^\times/\mathbb{R}_{>0}^\times \cong \widehat{\mathbb{Z}}^\times$ is mapped isomorphically via $\mathrm{Art}_{\mathbb{Q}}$ to the (injective) image of $W_{\mathbb{Q}_p}^{\mathrm{cyc}}$ in $G_{\mathbb{Q}}^{\mathrm{cyc}}$. The composition of these isomorphisms gives an isomorphism $W_{\mathbb{Q}_p}^{\mathrm{ab}} = W_{\mathbb{Q}_p}^{\mathrm{cyc}} \cong \mathbb{Q}_p^\times$, which is essentially $\chi_{\mathbb{Q}_p}|_{W_{\mathbb{Q}_p}^{\mathrm{ab}}} : W_{\mathbb{Q}_p}^{\mathrm{ab}} \to \widehat{\mathbb{Z}}^\times$. This is the *local Artin map* which can be defined and characterized intrinsically, and moreover for general local fields, not just $\mathbb{Q}_p$.

Local class field theory. Now let K be any local field, finite over $\mathbb{Q}_p$.

Theorem 3.1. (local class field theory) *There is a unique homomorphism* $\mathrm{art}_K : W_K \to K^\times$*, such that* (i) $v \circ \mathrm{art}_K = v$*, and* (ii) $\mathrm{art}_K(W_{K'}) \subset N_{K'/K}(K'^\times)$ *for* K'/K *finite abelian. Moreover, it induces* $W_K^{\mathrm{ab}} \cong K^\times$*, thus* $\mathrm{Art}_K := \mathrm{art}_K^{-1} : K^\times \cong W_K^{\mathrm{ab}}$ (*the* local Artin map *of* K), and for *every* finite K'/K, we have $\mathrm{art}_K|_{W_{K'}} = N_{K'/K} \circ \mathrm{art}_{K'}$.

The last property is the *local base change for* GL_1, which implies (ii). Define $W_K^{>0} := v^{-1}(\mathbb{Z}_{>0}) \subset W_K$, which generates W_K as a group. For a separable extension L/K, define the *norm group* $N(L/K)$ to be the intersection of $N_{K'/K}(K'^\times) \subset K^\times$ for all finite subextensions K'/K of L/K. Theorem 3.1 is implied by the following two theorems:

Theorem 3.2. (Lubin-Tate theory) *There is an abelian extension* K^{LT}/K *with* $K^{\mathrm{ur}} \subset K^{\mathrm{LT}}$ *and a homomorphism* $\mathrm{art}_K : W(K^{\mathrm{LT}}/K) \xrightarrow{\cong} K^\times$*, such that* (i) $v \circ \mathrm{art}_K = v$*, and* (ii) *for* $\sigma \in W_K^{>0}$*, let* K_σ *be its fixed field in* $\overline{K}$*. Then* $N(K_\sigma/K) = N(K_\sigma \cap K^{\mathrm{LT}}/K) = \mathrm{art}_K(\sigma)^{\mathbb{Z}}$.

Theorem 3.3. (local Kronecker-Weber theorem) $K^{\mathrm{LT}} = K^{\mathrm{ab}}$*, i.e.* $W_K^{\mathrm{ab}} = W(K^{\mathrm{LT}}/K)$.

Observe that the two conditions of Theorem 3.2 characterizes $\mathrm{art}_K : W(K^{\mathrm{LT}}/K) \to K^\times$. This art_K satisfies the local base change, because if K'/K is finite and $\sigma \in W_{K'}^{>0}$ (i.e. $K' \subset K_\sigma$), then $\mathrm{art}_K(\sigma)^{\mathbb{Z}} = N(K_\sigma/K) = N_{K'/K}(N(K_\sigma/K')) = N_{K'/K}(\mathrm{art}_{K'}(\sigma)^{\mathbb{Z}}) = N_{K'/K}(\mathrm{art}_{K'}(\sigma))^{\mathbb{Z}}$. (This implies $K^{\mathrm{LT}} \subset K'^{\mathrm{LT}}$.) Combining Theorem 3.3, we get an art_K satisfying (i),(ii) of Theorem 3.1. If another art'_K satisfies (i),(ii), then for $\sigma \in W_K^{>0}$, we have $\mathrm{art}'_K(\sigma) \in N(K_\sigma/K) = \mathrm{art}_K(\sigma)^{\mathbb{Z}}$ by (ii), and (i) implies $\mathrm{art}'_K = \mathrm{art}_K$. The following proposition is seen by checking that the cyclotomic theory is a special case of Lubin-Tate theory for $K = \mathbb{Q}_p$ with the uniformizer p, where $K^{\mathrm{LT}} = \mathbb{Q}_p^{\mathrm{cyc}}$ and $\mathrm{art}_K = \chi_{\mathbb{Q}_p}$.

Proposition 3.4. (local-global compatibility for the class field theory of $\mathbb{Q}$) *The restriction of* $\mathrm{Art} : \mathbb{A}^\times \to G_{\mathbb{Q}}^{\mathrm{ab}}$ *to* $\mathbb{Q}_p^\times$ *gives* $\mathrm{Art}_{\mathbb{Q}_p} : \mathbb{Q}_p^\times \xrightarrow{\cong} W_{\mathbb{Q}_p}^{\mathrm{ab}}$.

For $K = \mathbb{R}$ or $\mathbb{C}$, we define $W_K^{\mathrm{ab}} = W_K := G_K$, and $K^{\times 0} := \mathbb{R}_{>0}^\times$ or $\mathbb{C}^\times$ (the connected component of 1). Define the *local Artin map* as $\mathrm{Art}_K : K^\times/K^{\times 0} \cong W_K^{\mathrm{ab}} = G_K$.

Adeles over number fields. Now we consider adele rings over general number fields. Let F be a number field. We define the ring of finite adeles and adeles over F by $\mathbb{A}_F^\infty := F \otimes_{\mathbb{Q}} \mathbb{A}^\infty$ and $\mathbb{A}_F := F \otimes_{\mathbb{Q}} \mathbb{A} \cong F_\infty \times \mathbb{A}_F^\infty$, where $F_\infty := F \otimes_{\mathbb{Q}} \mathbb{R}$. They have descriptions as restricted products similar to $\mathbb{A}$, e.g. $\mathbb{A}_F$ is a restricted product of F_v with respect to $\mathcal{O}_v$, etc. We have injections $F^\times \to \mathbb{A}_F^\times$ and $F_v^\times \to \mathbb{A}_F^\times$ as before. For a finite place v, we denote the corresponding objects for F_v by $\mathcal{O}_v, \mathfrak{p}_v, k_v, q_v, \varpi_v, G_v, \mathrm{Frob}_v, W_v$. A finite extension F'/F is *unramified* at v if $F'_{v'}/F_v$ is unramified for all $v'|v$; it is unramified at almost all v. The product of norms $F'^\times_{v'} \to F_v^\times$ for $v'|v$ gives the *norm* $N_{F'/F} : \mathbb{A}_{F'}^\times \to \mathbb{A}_F^\times$. It restricts to $N_{F'/F}$ on $F'^\times$, thus the *absolute value* $|\cdot|_F := |N_{F/\mathbb{Q}}(\cdot)| : \mathbb{A}_F^\times \to \mathbb{R}_{>0}^\times$ factors through the *idele class group* $F^\times \backslash \mathbb{A}_F^\times$ of F. It satifies $|\cdot|_F|_{F_v^\times} = |\cdot|_v := |N_{F_v/\mathbb{Q}_u}(\cdot)|$ if $v|u$. When $K/\mathbb{Q}_u$ is finite we denote $|\cdot|_K = |N_{K/\mathbb{Q}_u}(\cdot)|$; if $K = F_v$ then $|\cdot|_K = |\cdot|_v$.

For a place v of F, we have a homomorphism $W_v^{\mathrm{ab}} \subset G_v^{\mathrm{ab}} \to G_F^{\mathrm{ab}}$. As $\mathrm{Hom}_F(\overline{F}, \overline{F}_v) = \varprojlim \mathrm{Hom}_F(F', \overline{F}_v)$ for finite F'/F, choosing a homomorphism $G_v \to G_F$ (up to a conjugation by G_v) amounts to choosing a compatible system of places $v' = \mathfrak{p}'$ of F' above v for all F'. When F'/F is Galois, the image of G_v is $\mathrm{Gal}(F'_{v'}/F_v)$, which is $D_{\mathfrak{p}'} \subset \mathrm{Gal}(F'/F)$. Thus the image of G_v in G_F is $\varprojlim D_{\mathfrak{p}'}$. Similarly the image of G_v^{ab} in G_F^{ab} is $\varprojlim D_{\mathfrak{p}'}$, but this does not depend on any choice.

Lecture 4. Global CFT, ℓ-adic characters (Tu. 20/7/10, 11:00–12:00)

Global Artin maps. We *define* the global Artin map of F as the product of local Artin maps as follows. For a place v of F, let $\mathrm{Art}_v : F_v^\times \to W_v^{\mathrm{ab}}$ be the local Artin map for F_v, and compose with $W_v^{\mathrm{ab}} \to G_F^{\mathrm{ab}}$. For each finite abelian F'/F, the product map $\mathrm{Art}_{F'/F} := \prod_v \mathrm{Art}_v : \mathbb{A}_F^\times \to \mathrm{Gal}(F'/F)$ is well defined (and surjective: Exercise 5), as the local components x_v of $x \in \mathbb{A}_F^\times$ are in $\mathcal{O}_v^\times$ for almost all v and thus their image is trivial, as F'/F is unramified at almost all v. Now define the *global Artin map* by $\mathrm{Art}_F := \varprojlim \mathrm{Art}_{F'/F} : \mathbb{A}_F^\times \to G_F^{\mathrm{ab}}$; it clearly satisfies $\mathrm{Art}_F|_{F_v^\times} = \mathrm{Art}_v$ for all v. The local base change implies the *global base change*, i.e. $\mathrm{Art}_{F'} = \mathrm{Art}_F \circ N_{F'/F}$ for finite F'/F. The global class field theory says Art_F is surjective, and describes its kernel. It was $\mathbb{Q}^\times \mathbb{R}_{>0}^\times$ when $F = \mathbb{Q}$; in general it is the *closure* of $F^\times \cdot \prod_{v|\infty} F_v^{\times 0}$ under a suitable topology.

Profinite structures. The *profinite* sets are the sets that are isomorphic to an inverse limit of finite sets. A *profinite structure* on a set (resp. group, ring) X is an isomorphism $X \cong \varprojlim X_\lambda$, where $\{X_\lambda\}_{\lambda \in \Lambda}$ is an inverse system of *finite* sets (resp. groups, rings). Two such structures are *equivalent* when there is an isomorphism between their cofinal subsystems. An equivalence class of profinite structure defines a topology on X, namely an inverse limit topology where each X_λ is considered as a discrete set (resp. group, ring). This is called a *profinite topology* on X. As inverse limit topology is the subspace topology when considered as a closed subspace of $\prod_\lambda X_\lambda$, it is compact Hausdorff, and is *totally disconnected*, i.e. every connected component is a singleton. Conversely, every compact, Hausdorff, and totally disconnected topology is seen to be a profinite topology, by considering all possible continuous maps into discrete finite sets. Its *open* subgroup are closed and of finite index, but not vice versa in general. We saw many examples of profinite groups, such as Galois groups G_F, G_F^{ab} etc., and $\widehat{\mathbb{Z}}, \widehat{\mathbb{Z}}^\times, \mathbb{Z}_p, \mathcal{O}_v, \mathcal{O}_v^\times$ etc. When F''/F is a Galois extension and F'/F is its subextension, then $\mathrm{Gal}(F''/F')$ is a *closed* subgroup of $\mathrm{Gal}(F''/F)$, and if it is normal, then F'/F is Galois and $\mathrm{Gal}(F'/F)$ is the quotient group. For example $F^{\mathrm{ab}} \subset \overline{F}$ corresponds to the *closure* of commutators $\overline{[G_F, G_F]}$, and the group G_F^{ab} is the *maximal abelian quotient* $G_F/\overline{[G_F, G_F]}$ of G_F. By a *character* of a topological group, we mean a *continuous* homomorphism into $\mathbb{C}^\times$ or $\overline{\mathbb{Q}}_\ell^\times$ for a prime ℓ (*ℓ-adic characters*). Therefore all characters of G_F factor through G_F^{ab}, i.e. considering the characters of G_F^{ab} is equivalent to considering the characters of G_F. Thus *class field theory* of F, which describes G_F^{ab}, is a theory of characters of G_F, i.e. 1-dimensional Galois representations.

Locally profinite / adelic groups. A group G with a specified profinite subgroup U can be topologized so that U is an open subgroup: its topology is determined by the topology of U and $G = \coprod_{g \in G/U} gU$. In general, a topological group G is called *locally profinite* if it has an open subgroup U such that the subspace topology on U is profinite. The examples of (G, U) are $(F_v, \mathcal{O}_v)$, $(F_v^\times, \mathcal{O}_v^\times)$, $(W_v, \mathrm{Ker}\, v)$, $(W_v^{\mathrm{ab}}, \mathrm{Ker}\, v)$, or $(\mathbb{A}^\infty, \widehat{\mathbb{Z}})$, $((\mathbb{A}^\infty)^\times, \widehat{\mathbb{Z}}^\times)$.

For an algebraic group G over $\mathbb{Q}$, we have an *adelic group* $G(\mathbb{A}) = G(\mathbb{R}) \times G(\mathbb{A}^\infty)$ (we get $\mathbb{A}^\times$ when $G = GL_1$), and if G is defined over $\mathbb{Z}$ as in the case $G = GL_n$, then $G(\mathbb{A}^\infty)$ is locally profinite with an open profinite subgroup $G(\widehat{\mathbb{Z}}) = \varprojlim G(\mathbb{Z}/(N))$, and the topology of $G(\mathbb{A})$ is the product topology with the ordinary topology of $G(\mathbb{R})$ as a Lie group. As locally profinite groups are totally disconnected, the connected component of 1 in $G(\mathbb{A})$ is equal to that in $G(\mathbb{R})$. When $G = \mathbb{G}_a$ (the additive group) or $G = GL_1$, we get locally profinite topology on $\mathbb{A}^\infty$ and $(\mathbb{A}^\infty)^\times$, but this topology on $(\mathbb{A}^\infty)^\times$ is *not* the subspace topology of $\mathbb{A}^\infty$. In $\mathbb{A}^\times = \mathbb{R}^\times \times (\mathbb{A}^\infty)^\times$, the subgroup $\mathbb{R}_{>0}^\times \times \widehat{\mathbb{Z}}^\times$ is open, and $\mathbb{Q}^\times$ is *discrete*.

Global class field theory. Let F be a number field with the ring of integers $\mathcal{O}$. The group $\mathbb{A}_F^\times$ is the adelic group for $G = \mathrm{Res}_{F/\mathbb{Q}}(GL_1)$, which is an algebraic group defined as $G(R) := GL_1(F \otimes_\mathbb{Q} R)$ for every $\mathbb{Q}$-algebra R (the *Weil restriction* of GL_1). In particular $G(\mathbb{A}^\infty) = (\mathbb{A}_F^\infty)^\times$ is locally profinite with $\widehat{\mathcal{O}}^\times$ as an open profinite subgroup (here $\widehat{\mathcal{O}} := \mathcal{O} \otimes_\mathbb{Z} \widehat{\mathbb{Z}} \cong \prod_{v:\mathrm{fin}} \mathcal{O}_v$). With this topology, the map Art_F is a unique continuous homomorphism satisfying $\mathrm{Art}_F|_{F_v^\times} = \mathrm{Art}_v$ for all v. The connected component of 1 in $\mathbb{A}_F^\times$ is $F_\infty^{\times 0} := \prod_{v|\infty} F_v^{\times 0}$. Again $F^\times$ is a discrete subgroup of $\mathbb{A}_F^\times$. But in general $\mathbb{A}_F^\times$ is *not* a direct product of $F^\times$ (discrete) and $F_\infty^{\times 0} \times \widehat{\mathcal{O}}^\times$ (open), in two ways: there is the *narrow class group* $\mathrm{Cl}_F^+ := F^\times \backslash \mathbb{A}_F^\times / (F_\infty^{\times 0} \times \widehat{\mathcal{O}}^\times)$ (finite), and the group of *totally positive units* $\mathcal{O}_{>0}^\times := F^\times \cap (F_\infty^{\times 0} \times \widehat{\mathcal{O}}^\times)$ (finitely generated $\mathbb{Z}$-module of rank $|\{v|\infty\}| - 1$). We have $\mathrm{Cl}_\mathbb{Q}^+ = \mathcal{O}_{>0}^\times = 1$ only when $F = \mathbb{Q}$. (We get the *ideal class group* Cl_F and the group of *units* $\mathcal{O}^\times$ if we replace $F_\infty^{\times 0}$ by $F_\infty^\times$ in each definition.) When $\mathcal{O}_{>0}^\times$ is not finite (i.e. when $|\{v|\infty\}| > 1$) it is not closed in $\widehat{\mathcal{O}}^\times$, hence $\mathcal{O}_{>0}^\times F_\infty^{\times 0}$ is not closed in $F_\infty^{\times 0} \times \widehat{\mathcal{O}}^\times$, thus $F^\times F_\infty^{\times 0}$ is not closed in $\mathbb{A}_F^\times$. But its closure gives the kernel of Art_F:

Theorem 4.1. (global class field theory) *The global Artin map* Art_F *induces an isomorphism* $\mathbb{A}_F^\times / \overline{F^\times F_\infty^{\times 0}} \cong G_F^{\mathrm{ab}}$, *where* $F_\infty^{\times 0} := \prod_{v|\infty} F_v^{\times 0}$, *and* $\overline{F^\times F_\infty^{\times 0}}$ *is the closure in* $\mathbb{A}_F^\times$.

In other words, the kernel of $\mathrm{Art}_F : F^\times \backslash \mathbb{A}_F^\times \to G_F^{\mathrm{ab}}$ is the connected component of 1.

Hecke/Galois characters. We call the characters $\Pi : F^\times \backslash \mathbb{A}_F^\times \to \mathbb{C}^\times$ the *Hecke characters* of F. Its *local component* at v is defined as $\Pi_v := \Pi|_{F_v^\times}$. It has *weight* (0) if $\Pi|_{F_\infty^{\times 0}} = 1$, which ensures that it vanishes on $\overline{F^\times F_\infty^{\times 0}}$. Thus we have a bijection between the Hecke characters Π of weight (0) and the characters $R : G_F^{\mathrm{ab}} \to \mathbb{C}^\times$, given by $\Pi = R \circ \mathrm{Art}_F$. We extend this correspondence so that it includes $|\cdot|_F \leftrightarrow \chi_\ell$. A Hecke character is *algebraic of weight* (a_τ), if there is $a_\tau \in \mathbb{Z}$ for each $\tau \in \mathrm{Hom}_\mathbb{Q}(F, \mathbb{C}) = \coprod_{v|\infty} \mathrm{Hom}_\mathbb{R}(F_v, \mathbb{C})$, such that for all $v|\infty$,

$$\Pi_v(x_v) = \prod_{v(\tau)=v} \tau(x_v)^{-a_\tau} \qquad (\forall x_v \in F_v^{\times 0}).$$

The absolute value $|\cdot|_F$ is algebraic of weight (-1).

Let ℓ be a prime. For a character $R : G_F^{\mathrm{ab}} \to \overline{\mathbb{Q}}_\ell^\times$, its *local component* R_v is defined as $R \circ (W_v^{\mathrm{ab}} \to G_F^{\mathrm{ab}})$. It is *algebraic of weight* (b_λ), if there is $b_\lambda \in \mathbb{Z}$ for each $\lambda \in \mathrm{Hom}_\mathbb{Q}(F, \overline{\mathbb{Q}}_\ell) = \coprod_{v|\ell} \mathrm{Hom}_{\mathbb{Q}_\ell}(F_v, \overline{\mathbb{Q}}_\ell)$ and an open subgroup $U_v \subset \mathcal{O}_v^\times$ for each $v|\ell$, such that

$$R_v \circ \mathrm{Art}_v(x_v) = \prod_{v(\lambda)=v} \lambda(x_v)^{-b_\lambda} \qquad (\forall x_v \in U_v).$$

For example χ_ℓ is algebraic of weight (-1), as $\chi_{\ell,v} \circ \mathrm{Art}_v|_{\mathcal{O}_v^\times} = N_{F_v/\mathbb{Q}_\ell}|_{\mathcal{O}_v^\times}$. For a field isomorphism $\iota : \overline{\mathbb{Q}}_\ell \cong \mathbb{C}$ and a Π algebraic of weight (a_τ), define $\Pi_\iota : F^\times \backslash \mathbb{A}_F^\times \to \overline{\mathbb{Q}}_\ell^\times$ by

$$\Pi_\iota : \mathbb{A}^\times \ni x \longmapsto \iota^{-1}\Big(\Pi(x) \cdot \prod_{\tau \in \mathrm{Hom}_\mathbb{Q}(F,\mathbb{C})} \tau(x_{v(\tau)})^{a_\tau}\Big) \cdot \prod_{\lambda \in \mathrm{Hom}_\mathbb{Q}(F, \overline{\mathbb{Q}}_\ell)} \lambda(x_{v(\lambda)})^{-a_{\iota\circ\lambda}} \in \overline{\mathbb{Q}}_\ell^\times.$$

Thus, defining $\Pi \leftrightarrow R$ by $\Pi_\iota = R \circ \mathrm{Art}_F$, we obtain the CFT for ℓ-adic characters:

Theorem 4.2. (global Langlands correspondence for GL_1) *Let F be a number field, and fix $a_\tau \in \mathbb{Z}$ for each $\tau \in \mathrm{Hom}_\mathbb{Q}(F, \mathbb{C})$. For each prime ℓ and an isomorphism $\iota : \overline{\mathbb{Q}}_\ell \cong \mathbb{C}$, there is a following bijection, satisfying $\Pi_v = \iota \circ R_v \circ \mathrm{Art}_v$ for all v not above ℓ, ∞.*

$$\left\{ \begin{array}{c} \Pi : F^\times \backslash \mathbb{A}_F^\times \to \mathbb{C}^\times, \\ \textit{algebraic of weight } (a_\tau) \end{array} \right\} \stackrel{1:1}{\longleftrightarrow} \left\{ \begin{array}{c} R : G_F^{\mathrm{ab}} \to \overline{\mathbb{Q}}_\ell^\times, \\ \textit{algebraic of weight } (b_\lambda = a_{\iota\circ\lambda}) \end{array} \right\}$$

Appendix A. More on GLC for GL_1: algebraic Hecke characters

Finiteness and algebraicity. Every character of a locally profinite group G into $\mathbb{C}^\times$ factors through a discrete group G/U, where U is an open subgroup of G. Thus any Galois character $G_F^{\mathrm{ab}} \to \mathbb{C}^\times$ has finite image, and every character of $\widehat{\mathbb{Z}}^\times$ factors through $(\mathbb{Z}/(N))^\times$ for some $N \in \mathbb{Z}_{>0}$ (composed with the projection $\mathbb{A}^\times \to \widehat{\mathbb{Z}}^\times$, we call them *Dirichlet characters*). As $\mathbb{Q}^\times\backslash\mathbb{A}^\times \cong \mathbb{R}^\times_{>0} \times \widehat{\mathbb{Z}}^\times$, every Hecke character $\Pi : \mathbb{Q}^\times\backslash\mathbb{A}^\times \to \mathbb{C}^\times$ of $\mathbb{Q}$ is a product of $|\cdot|^w$ for $w \in \mathbb{C}$ and a Dirichlet character. It is algebraic if and only if $w \in \mathbb{Z}$.

Consider $\Pi : F^\times\backslash\mathbb{A}_F^\times \to \mathbb{C}^\times$ for general F; it is determined by its *finite part* $\Pi^\infty := \Pi|_{(\mathbb{A}_F^\infty)^\times}$. The kernel U of $\Pi^\infty|_{\widehat{\mathcal{O}}^\times}$ is called the *level*, which is open and thus contains $\mathrm{Ker}\,(\widehat{\mathcal{O}}^\times \to (\mathcal{O}/I)^\times)$ for some ideal I of $\mathcal{O}$. The largest such I is called the *conductor* of Π. It is a product $\prod_{v:\mathrm{fin}} \mathfrak{p}_v^{m_v}$, where $m_v \in \mathbb{N}$ is the smallest such that $1 + \mathfrak{p}_v^{m_v} \subset \mathrm{Ker}\,\Pi_v$ (or $\Pi_v|_{\mathcal{O}_v^\times}$ factors through $(\mathcal{O}_v/\mathfrak{p}_v^{m_v})^\times$), the *conductor* of Π_v. We see that Π_v is *unramified*, i.e. trivial on $\mathcal{O}_v^\times$ (or $m_v = 0$), for almost all v. An unramified Π_v is a character of $F_v^\times/\mathcal{O}_v^\times \cong \mathbb{Z}$, thus determined by the *Hecke eigenvalue* $\Pi_v(\varpi) \in \mathbb{C}^\times$, where ϖ is any uniformizer of F_v. If we fix the weight $\Pi|_{F_\infty^{\times 0}}$ and the level U, then $F_\infty^{\times 0} \times U$ has finite index in $F_\infty^\times \times \widehat{\mathcal{O}}^\times$. Thus setting $\mathcal{O}_U^{\times 0} := F^\times \cap (F_\infty^{\times 0} \times U)$, the subgroup $\mathcal{O}_U^{\times 0}\backslash(F_\infty^{\times 0} \times U)$ has finite index in $F^\times\backslash\mathbb{A}_F^\times$, because $\mathrm{Cl}_F = F^\times\backslash\mathbb{A}_F^\times/(F_\infty^\times \times \widehat{\mathcal{O}}^\times)$ is finite *(finiteness of class numbers)*. Thus there are only finitely many choices for Π, and such Π exists if and only if $\Pi_\infty|_{\mathcal{O}_U^{\times 0}} = 1$ (as $\mathbb{C}^\times$ is divisible, hence an injective additive group). If $\Pi|_{F_\infty^{\times 0}} = 1$ then $\mathrm{Im}\,\Pi$ is finite. If Π is algebraic, then $\mathrm{Im}\,\Pi^\infty$ is contained in a number field: in fact, if $F^\times_{>0} := F^\times \cap F_\infty^{\times 0}$ then $F^\times_{>0}U$ has finite index in $(\mathbb{A}_F^\infty)^\times$ (weak approximation), and on $F^\times_{>0}$ the character Π^∞ is equal to $\Pi_\infty^{-1} = \prod_\tau \tau^{a_\tau}$. In particular, the Hecke eigenvalues are *algebraic numbers.*

Theorem A.1. *Let $\Pi : F^\times\backslash\mathbb{A}_F^\times \to \mathbb{C}^\times$ be an algebraic Hecke character of weight (a_τ).*

- (i) *Its local component Π_v is unramified for almost all v (true for all Hecke characters).*
- (ii) (finiteness) *There is only a finite number of algebraic Hecke characters of a fixed weight (a_τ) and conductor I.*
- (iii) (algebraicity) *Every weight (0) character has finite image. In general, there is a number field E and $\tau_E \in \mathrm{Hom}_{\mathbb{Q}}(E, \mathbb{C})$, such that for every finite v there is a character $\pi_v : F_v^\times \to E^\times$ with $\Pi_v = \tau_E \circ \pi_v$. In particular, $\mathrm{Im}\,\Pi^\infty \subset \tau_E(E)^\times$.*

Global structures. We consider the kernel of $|\cdot|_F : F^\times\backslash\mathbb{A}_F^\times \to \mathbb{R}^\times_{>0}$. Recall $\mathcal{O}^\times = F^\times \cap (F_\infty^\times \times \widehat{\mathcal{O}}^\times)$. As the open subgroup $\mathcal{O}^\times\backslash(F_\infty^\times \times \widehat{\mathcal{O}}^\times)$ of $F^\times\backslash\mathbb{A}_F^\times$ has finite index, the group $\mathrm{Ker}' := \mathrm{Ker}\,|\cdot|_F \cap \big(\mathcal{O}^\times\backslash(F_\infty^\times \times \widehat{\mathcal{O}}^\times)\big)$ has finite index in $\mathrm{Ker}\,|\cdot|_F$. Let $U_\infty := \prod_{v|\infty} \mathrm{Ker}\,|\cdot|_v$ (the maximal compact subgroup of $F_\infty^\times$). Then $\boldsymbol{\mu}_F := \mathcal{O}^\times \cap U_\infty$ is the finite group of all roots of unity in F. Writing $\overline{\mathcal{O}^\times} := \mathcal{O}^\times/\boldsymbol{\mu}_F$, we have a commutative diagram:

$$
\begin{array}{ccccc}
\mathcal{O}^\times\backslash(U_\infty \times \widehat{\mathcal{O}}^\times) & \longrightarrow & \mathrm{Ker}' & \longrightarrow & \overline{\mathcal{O}^\times} \setminus \mathrm{Ker}\,\big((\mathbb{R}^\times_{>0})^r \to \mathbb{R}^\times_{>0}\big) \\
\| & & \downarrow & & \downarrow \\
\mathcal{O}^\times\backslash(U_\infty \times \widehat{\mathcal{O}}^\times) & \longrightarrow & \mathcal{O}^\times\backslash(F_\infty^\times \times \widehat{\mathcal{O}}^\times) & \xrightarrow{(|\cdot|_v)_{v|\infty}} & \overline{\mathcal{O}^\times} \setminus (\mathbb{R}^\times_{>0})^r \\
 & & {\scriptstyle |\cdot|_F}\downarrow & & \downarrow{\scriptstyle \text{product}} \\
 & & \mathbb{R}^\times_{>0} & = & \mathbb{R}^\times_{>0}
\end{array}
$$

where $r := |\{v|\infty\}|$ and all rows and columns are short exact sequences. Then *Dirichlet's unit theorem* says that $\overline{\mathcal{O}^\times}$ sits in $\mathrm{Ker}\,\big((\mathbb{R}^\times_{>0})^r \to \mathbb{R}^\times_{>0}\big) \cong \mathbb{R}^{r-1}$ as a $\mathbb{Z}$-lattice, thus making the quotient compact ($\cong (\mathbb{R}/\mathbb{Z})^{r-1}$). Thus $\operatorname{Ker}|\cdot|_F$ is compact. It is the maximal compact subgroup as $\mathbb{R}^\times_{>0}$ has no compact subgroup, hence all characters $F^\times\backslash\mathbb{A}_F^\times \to \mathbb{R}^\times_{>0}$ factor through $|\cdot|_F$. As every continuous character $\mathbb{R}^\times_{>0} \to \mathbb{R}^\times_{>0}$ is of the form $(\cdot)^w$ for $w \in \mathbb{R}$:

Lemma A.2. *The kernel of $|\cdot|_F : F^\times\backslash\mathbb{A}_F^\times \to \mathbb{R}^\times_{>0}$ is the maximal compact subgroup of $F^\times\backslash\mathbb{A}_F^\times$. Every character $F^\times\backslash\mathbb{A}_F^\times \to \mathbb{R}^\times_{>0}$ has the form $|\cdot|_F^w$ for $w \in \mathbb{R}$.*

Purity. Now we apply Lemma A.2 to $|\Pi|_\mathbb{C}$, and let $|\Pi|_\mathbb{C} = |\cdot|_F^{-w}$. For $v|\infty$, we have $|\cdot|_v^{-w} = |\Pi_v|_\mathbb{C} = |\prod_{v(\tau)=v}\tau^{-a_\tau}|_\mathbb{C} = \prod_{v(\tau)=v}\tau^{-(a_\tau+a_{c\circ\tau})} = |\cdot|_v^{-(a_\tau+a_{c\circ\tau})}$, thus $w = a_\tau + a_{c\circ\tau}$ for all τ (*Hodge symmetry*, or purity at ∞). In particular w is twice the average of all a_τ. Similarly if v is finite and ϖ is a uniformizer of F_v, then we have $q_v^w = |\varpi|_v^{-w} = |\Pi_v(\varpi)|_\mathbb{C}$, i.e. the integer w "aligns" the complex absolute values of the Hecke eigenvalues at all finite places. But $\Pi_v(\varpi) \in E$ are algebraic numbers, hence we can also consider its conjugates.

If Π is algebraic of weight (a_τ), then $\sigma \circ \Pi^\infty$ for $\sigma \in \operatorname{Aut}(\mathbb{C})$ is a finite part of another algebraic Hecke character $\sigma\Pi$ of weight ($a'_\tau := a_{\sigma^{-1}\circ\tau}$), and satisfies Theorem A.1(iii) for $\sigma \circ \tau_E \in \operatorname{Hom}_\mathbb{Q}(E,\mathbb{C})$. As $\operatorname{Aut}(\mathbb{C})$ acts transitively on $\operatorname{Hom}_\mathbb{Q}(E,\mathbb{C})$, there is a $\sigma\Pi$ for each $\tau_E \in \operatorname{Hom}_\mathbb{Q}(E,\mathbb{C})$, and these are the finitely many Galois *conjugates* of Π. Changing $\iota : \overline{\mathbb{Q}}_\ell \cong \mathbb{C}$ in Theorem 4.2 will only shuffle around the Galois conjugates.

Now all conjugates $\sigma\Pi$ have the same value of $w = a_\tau + a_{c\circ\tau}$, hence the Hecke eigenvalues $\Pi_v(\varpi)$ are a very special kind of algebraic numbers called Weil q_v^w-numbers: for a prime power q, an element of a number field $x \in E$ is called a *Weil q-number* if $|\tau_E(x)|_\mathbb{C} = q$ for all $\tau_E \in \operatorname{Hom}_\mathbb{Q}(E,\mathbb{C})$. This is the *Ramanujan conjecture* for GL_1.

Hodge symmetry puts a strong constraint on the weights (a_τ). Note that the weight of a product of two characters is the sum of their weights, hence the quotient of two characters of the same weight has weight (0). If F is *totally real*, i.e. if all infinite places of F are real, then all a_τ are equal, thus Π is always a product of an integer power of $|\cdot|$ and a weight (0) character, just as when $F = \mathbb{Q}$. New algebraic Π of non-zero weight appear when we take *totally imaginary* (i.e. all infinite places are complex) quadratic extensions of totally real fields (*imaginary CM fields*). By *CM fields* we mean either totally real or imaginary CM fields. For general F, its maximal totally real subfield F_0^+ is the maximal subfield on which $\tau = c\tau$ (we omit $\circ$ for a while) for all $\tau \in \operatorname{Hom}_\mathbb{Q}(F,\mathbb{C})$. In other words $\sigma\tau = c\sigma\tau$ for all $\sigma \in \operatorname{Aut}(\mathbb{C})$, or $\tau = (\sigma^{-1}c\sigma)\tau$. Relaxing this condition, the maximal CM subfield F_0 is where $c\tau = (\sigma^{-1}c\sigma)\tau$ for all $\sigma \in \operatorname{Aut}(\mathbb{C})$. Then $\tau^{-1}c\tau \in \operatorname{Aut}_\mathbb{Q}(F_0)$ is independent of τ as $\tau^{-1}c\tau = (\sigma\tau)^{-1}c(\sigma\tau)$, and we denote it again by c (the *complex conjugate* on F_0); its fixed field is F_0^+. Now if $\tau|_{F_0} = \tau'|_{F_0}$ then there exists $\sigma \in \operatorname{Aut}(\mathbb{C})$ such that $c\tau = (\sigma^{-1}c\sigma)\tau'$. As the Hodge symmetry for $\sigma\Pi$ says $a_{\sigma^{-1}\tau} + a_{\sigma^{-1}c\tau} = w$ for all τ, or $a_{\tau'} + a_{(\sigma^{-1}c\sigma)\tau'} = w$, thus $w - a_\tau = a_{c\tau} = a_{(\sigma^{-1}c\sigma)\tau'} = w - a_{\tau'}$, i.e. a_τ depends only on $\tau|_{F^0}$.

When $F = F_0$, for any (a_τ) satifying $w = a_\tau + a_{c\circ\tau}$, the $\Pi|_{F_\infty^{\times 0}} = \prod_\tau \tau^{-a_\tau}$ restricts to $|\cdot|_{F_0^+}^{-w}$ on the elements of $(F_0^+)^\times_\infty$. As $\mathcal{O}^\times \cap F_0^+$ is the unit group of F_0^+ and has finite index in $\mathcal{O}^\times$ (as both have the same rank), by Chevalley's lemma ([Ch], Théorème 1), we can choose a level U such that $\mathcal{O}_U^{\times 0} \subset \mathcal{O}^\times \cap F_0^+$, which ensures $\Pi_\infty|_{\mathcal{O}_U^{\times 0}} = 1$. Then there exists Π of weight (a_τ) and level U. Thus we conclude:

Theorem A.3. *Let $\Pi : F^\times\backslash\mathbb{A}_F^\times \to \mathbb{C}^\times$ be an algebraic Hecke character of weight (a_τ).*

(i) (Hodge symmetry) *The number $w := a_\tau + a_{c\circ\tau} \in \mathbb{Z}$ is independent of τ. If F_0 is the maximal CM subfield of F, then a_τ depends only on $\tau_0 := \tau|_{F_0}$.*

(ii) (Ramanujan conjecture) *Let v be finite. If ϖ is a uniformizer of F_v, then $\pi_v(\varpi)$ is a Weil q_v^w-number, where π_v is as in Theorem A.1(iii).*

(iii) (classification) *If F is totally real, then there is a Hecke character Π' of weight* (0) *such that $\Pi = \Pi' \cdot |\cdot|_F^{-w/2}$. In general, if F_0 is the maximal CM subfield of F, then there is an algebraic Hecke character Π_0 of F_0 and a Hecke character Π' of weight* (0) *such that $\Pi = \Pi' \cdot (\Pi_0 \circ N_{F/F_0})$.*

Appendix B. More on GLC for GL_1: algebraic Galois characters

Now we combine Theorems A.1 and A.3 with Theorem 4.2. Let us make two remarks. First, the global base change implies that if F'/F is a finite extension and $\Pi \leftrightarrow R$ over F, then $\Pi \circ N_{F'/F} \leftrightarrow R|_{F'} := R \circ (G_{F'}^{\mathrm{ab}} \to G_F^{\mathrm{ab}})$ over F'. Second, when Π is unramified at v, the local-global compatibility $\Pi_v = \iota \circ R_v \circ \mathrm{Art}_v$ reduces to $\Pi_v(\varpi_v) = \iota R_v(\mathrm{Frob}_v)$ (the *reciprocity law*).

We define the *conductor* of $R_v : W_v^{\mathrm{ab}} \to \overline{\mathbb{Q}}_\ell^\times$ as the conductor of Π_v for corresponding Π under some ι. Recall that $\Pi_v = \iota \circ R_v \circ \mathrm{Art}_v$ when v is not above ℓ, and when $v|\ell$, we have $\Pi_v = \iota\big(R_v \cdot \prod_{v(\lambda)=v}(\lambda \circ \mathrm{Art}_v^{-1})^{b_\lambda}\big) \circ \mathrm{Art}_v$ from the definition of Π_ι, and their conductors are independent of ι. We define the *conductor* of R as the product taken in the same way as for the Hecke characters, so it is equal to the conductor of Π. We define $r_v : W_v^{\mathrm{ab}} \to E^\times$ by $\pi_v = r_v \circ \mathrm{Art}_v$, where $\Pi_v = \tau_E \circ \pi_v$. Setting $\lambda_E := \iota^{-1} \circ \tau_E$, we have $\lambda_E \circ r_v = R_v$ when v is not above ℓ, and when $v|\ell$,

$$\lambda_E \circ r_v = \lambda_E \circ \pi_v \circ \mathrm{Art}_v^{-1} = \iota^{-1} \circ \Pi_v \circ \mathrm{Art}_v^{-1} = R_v \cdot \prod_{v(\lambda)=v} (\lambda \circ \mathrm{Art}_v^{-1})^{b_\lambda}.$$

Theorem B.1. *Let $R : G_F^{\mathrm{ab}} \to \overline{\mathbb{Q}}_\ell^\times$ be an algebraic Galois character of weight (b_λ).*

(i) *Its local component R_v is unramified for almost all v (true for all Galois characters).*
(ii) (finiteness) *There is only a finite number of algebraic Galois characters of a fixed weight (b_λ) and conductor I.*
(iii) (algebraicity) *If $(b_\lambda) = (0)$, then R has finite image. In general, there is a number field E and $\lambda_E \in \mathrm{Hom}_{\mathbb{Q}}(E, \overline{\mathbb{Q}}_\ell)$, such that there is a character $r_v : W_v^{\mathrm{ab}} \to E^\times$, with $R_v = \lambda_E \circ r_v$ when v not above ℓ, and $R_v = (\lambda_E \circ r_v) \cdot \prod_{v(\lambda)=v}(\lambda \circ \mathrm{Art}_v^{-1})^{b_\lambda}$ when $v|\ell$. In particular, $\mathrm{Im}\, R \subset E_w^\times$ where $w = v(\lambda_E)$.*
(iv) (Hodge symmetry) *If F_0 is the maximal CM subfield of F, then b_λ depends only on $\lambda_0 := \lambda|_{F_0}$. The number $w := b_{\lambda_0} + b_{\lambda_0 \circ c} \in \mathbb{Z}$ is independent of λ_0.*
(v) (purity) *Let v be finite, not above ℓ. If $\phi \in W_v^{\mathrm{ab}}$ and $v(\phi) = 1$, then $r_v(\phi)$ is a Weil q_v^w-number. (We say R is* pure *of* Frobenius weight *w.)*
(vi) (classification) *If F is totally real, then there is a finite image character R' such that $R = R' \cdot \chi_\ell^{-w/2}$. If F_0 is the maximal CM subfield of F, then there is an algebraic Galois character R_0 of F_0 and a finite image character R' such that $R = R' \cdot R_0|_F$.*

Now pick another prime ℓ' and $\lambda'_E \in \mathrm{Hom}_{\mathbb{Q}}(E, \overline{\mathbb{Q}}_{\ell'})$, and apply Theorem 4.2 to Π again for an $\iota' : \overline{\mathbb{Q}}_{\ell'} \cong \mathbb{C}$ such that $\iota \circ \lambda_E = \iota' \circ \lambda'_E$. Setting $\rho := \iota^{-1} \circ \iota' : \overline{\mathbb{Q}}_{\ell'} \cong \overline{\mathbb{Q}}_\ell$, we obtain:

Theorem B.2. (compatible system) *Let $R : G_F^{\mathrm{ab}} \to \overline{\mathbb{Q}}_\ell^\times$ be an algebraic Galois character of weight (b_λ). For each prime ℓ' and $\lambda'_E \in \mathrm{Hom}_{\mathbb{Q}}(E, \overline{\mathbb{Q}}_{\ell'})$, there is an algebraic Galois character $R' : G_F^{\mathrm{ab}} \to \overline{\mathbb{Q}}_{\ell'}^\times$ of weight $(b'_{\lambda'} = b_{\rho \circ \lambda'})$, where $\rho : \overline{\mathbb{Q}}_{\ell'} \cong \overline{\mathbb{Q}}_\ell$ is such that $\lambda_E = \rho \circ \lambda'_E$, such that $R'_v = \lambda'_E \circ r_v$ for all v not above ℓ', and $R'_v = (\lambda'_E \circ r_v) \cdot \prod_{v(\lambda')=v}(\lambda' \circ \mathrm{Art}_v^{-1})^{-b'_{\lambda'}}$ for $v|\ell'$.*

For $F = \mathbb{Q}$, we had the basic example of compatible system of ℓ-adic cyclotomic characters $R = \chi_\ell$ for all ℓ, corresponding to $\Pi = |\cdot|$.

Exercises

1. Quadratic reciprocity (Lecture 1). We deduce the *quadratic reciprocity law*, which desribes the decomposition of primes in a quadratic field, from the reciprocity law for the cylotomic extensions of $\mathbb{Q}$.

(i) (Decomposition of primes in a quadratic field) Let p be an odd prime. The *Legendre symbol* is a unique non-trivial character $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \to \{\pm 1\}$ of the cyclic group $\mathbb{F}_p^\times$ (its kernel Q_p is the group of *quadratic residues* mod p). Let $d \in \mathbb{Z}$ be square free. Then a prime p not dividing $2d$ decomposes in $\mathbb{Q}(\sqrt{d})$ as:

$$(p) = \mathfrak{p}_1\mathfrak{p}_2 \iff \left(\frac{d}{p}\right) = 1, \qquad (p) = \mathfrak{p} \iff \left(\frac{d}{p}\right) = -1.$$

(ii) (Decomposition of primes in a subextensions of cyclotomic fields) If F'/F is a subextension of an abelian extension F''/F of number fields and $\mathfrak{p}$ is a prime of $\mathcal{O}_F$, then $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(F'/F)$ is the restriction of $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(F''/F)$ to F'. If $F/\mathbb{Q}$ is a subextension of $\mathbb{Q}(\boldsymbol{\mu}_N)/\mathbb{Q}$, corresponding to $H \subset (\mathbb{Z}/(N))^\times \cong \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_N)/\mathbb{Q})$, then (p) *splits completely* in F (i.e. $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ for $n = [F : \mathbb{Q}]$) if and only if $p \bmod N \in H$.

(iii) Show that $\mathbb{Q}(\sqrt{2})$ corresponds to the subgroup $\{\overline{1}, \overline{7}\}$ of $\mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_8)/\mathbb{Q}) \cong (\mathbb{Z}/(8))^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$. Comparing (i) and (ii) for $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{2})$, deduce the *first/second complementary law*, namely if p is an odd prime, then:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & (p \equiv 1 \pmod 4) \\ -1 & (p \equiv 3 \pmod 4), \end{cases} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & (p \equiv 1, 7 \pmod 8), \\ -1 & (p \equiv 3, 5 \pmod 8). \end{cases}$$

(iv) Let ℓ be an odd prime, and $F_\ell/\mathbb{Q}$ be the quadratic subextension of $\mathbb{Q}(\boldsymbol{\mu}_\ell)/\mathbb{Q}$ corresponding to the unique subgroup H_ℓ of index 2 of the cyclic group $\mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_\ell)/\mathbb{Q}) \cong (\mathbb{Z}/(\ell))^\times = \mathbb{F}_\ell^\times$. This F_ℓ is $\mathbb{Q}(\sqrt{\ell})$ when $\ell \equiv 1 \pmod 4$, and $\mathbb{Q}(\sqrt{-\ell})$ when $\ell \equiv 3 \pmod 4$.

(v) Deduce the *quadratic reciprocity law*, namely for odd primes p, ℓ:

$$\left(\frac{p}{\ell}\right)\left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}}, \quad \text{i.e.,} \quad \begin{cases} \left(\frac{p}{\ell}\right) = \left(\frac{\ell}{p}\right) & (p \text{ or } \ell \equiv 1 \pmod 4), \\ \left(\frac{p}{\ell}\right) = -\left(\frac{\ell}{p}\right) & (p \equiv \ell \equiv 3 \pmod 4). \end{cases}$$

2. Ramified primes in cyclotomic extension (Lecture 2/3). (i) Let $K''/K'/K$ be successive finite extensions of local fields. Show that $e(K''/K) = e(K''/K')e(K'/K)$ and $f(K''/K) = f(K''/K')f(K'/K)$. If K'/K is unramified and K''/K is totally ramified, then $K' \cap K'' = K$.

(ii) A finite extension F'/F of number fields is *totally ramified* at a finite place v of F if there is only one place v' of F' above v and $F'_{v'}/F_v$ is totally ramified. If F'/F is unramified at v and F''/F is totally ramified at v, then $F' \cap F'' = F$.

(iii) For a number field F, the cyclotomic extension $F(\boldsymbol{\mu}_p)/F$ is totally ramified at all places above p.

(iv) Let $N \in \mathbb{Z}_{>0}$. By looking at a prime dividing $\Phi_N(x)$ for $x \in \mathbb{Z}$ (where Φ_N is the cyclotomic polynomial whose roots are primitive N-th roots of unity), show that there are infinitely many primes p such that $p \equiv 1 \pmod N$.

3. Finite extensions of local fields (Lecture 3). Let K'/K be a finite extension of local fields (finite extensions of $\mathbb{Q}_p$).

(i) If K'/K is Galois, then $W_K/W_{K'} \cong \mathrm{Gal}(K'/K)$.

(ii) If K'/K is abelian, then $W_K^{\mathrm{ab}} \,/\, \mathrm{Im}\,(W_{K'}^{\mathrm{ab}} \to W_K^{\mathrm{ab}}) \cong \mathrm{Gal}(K'/K)$.

(iii) For any K'/K, the Art_K induces $K^\times/N_{K'/K}(K'^\times) \xrightarrow{\cong} \mathrm{Gal}(K' \cap K^{\mathrm{ab}}/K)$.

(iv) Assume $p \neq 2$. How many quadratic extensions of K are there (inside a given $\overline{K}$)? Can you write them explicitly as $K(\sqrt{a})$ for $a \in K^\times$?

4. Artin maps for cyclotomic extensions (Lecture 3/4). Recall the notation $F^{\mathrm{cyc}} := \bigcup_N F(\boldsymbol{\mu}_N)$ and $G_F^{\mathrm{cyc}} := \mathrm{Gal}(F^{\mathrm{cyc}}/F)$ from Lecture 1.

(i) Let K be a local field (a finite extension of $\mathbb{Q}_p$), and let W_K^{cyc} be the Weil group of K^{cyc} (see Lecture 3). Then Art_K induces

$$K^\times/\mathrm{Ker}\, N_{K/\mathbb{Q}_p} \xrightarrow{\cong} N_{K/\mathbb{Q}_p}(K^\times) \xrightarrow{\cong} W_K^{\mathrm{cyc}}.$$

(ii) Let F be a number field, and let $N_{F/\mathbb{Q}} : \mathbb{A}_F^\times \to \mathbb{A}^\times$ be the norm map. For each $N \in \mathbb{Z}_{>0}$, the map $\mathrm{Art}_{F(\boldsymbol{\mu}_N)/F}$ gives:

$$F^\times\backslash\mathbb{A}_F^\times/(F_\infty^{\times 0} \times N_{F/\mathbb{Q}}^{-1}(U_N)) \xrightarrow{\cong} \mathbb{Q}^\times\backslash N_{F/\mathbb{Q}}(\mathbb{A}_F^\times)/(\mathbb{R}_{>0}^\times \times U_N) \xrightarrow{\cong} \mathrm{Gal}(F(\boldsymbol{\mu}_N)/F),$$

where $U_N := 1 + N\widehat{\mathbb{Z}} = \mathrm{Ker}\left(\widehat{\mathbb{Z}}^\times \to (\mathbb{Z}/(N))^\times\right) \subset \widehat{\mathbb{Z}}^\times$. Passing to the limit, we see that Art_F induces

$$\mathbb{A}_F^\times/\overline{N_{F/\mathbb{Q}}^{-1}(\mathbb{Q}^\times)F_\infty^{\times 0}} \xrightarrow{\cong} \mathbb{Q}^\times\backslash N_{F/\mathbb{Q}}(\mathbb{A}_F^\times)/\mathbb{R}_{>0}^\times \xrightarrow{\cong} G_F^{\mathrm{cyc}}.$$

5. Surjectivity of global Artin maps for finite extensions (Lecture 4). We show that $\mathrm{Art}_{F'/F} : \mathbb{A}_F^\times \to \mathrm{Gal}(F'/F)$ is surjective for every finite abelian extension F'/F of number fields. This is true when F'/F is *cyclotomic* by Exercise 4. For general F'/F, take $N \in \mathbb{Z}_{>0}$ which kills $\mathrm{Gal}(F'/F)$, and choose a prime p such that (i) $p \equiv 1 \pmod{N}$ and (ii) $F'/\mathbb{Q}$ is unramified at p, by Exercise 2 (iv).

(i) Using Exercise 2 (ii), show that $F(\boldsymbol{\mu}_p) \cap F' = F$ and $\mathbb{Q}(\boldsymbol{\mu}_p) \cap F = \mathbb{Q}$. Deduce that $\mathrm{Gal}(F'(\boldsymbol{\mu}_p)/F) \cong \mathrm{Gal}(F'/F) \times \mathrm{Gal}(F(\boldsymbol{\mu}_p)/F) \cong \mathrm{Gal}(F'/F) \times \mathbb{F}_p^\times$.

(ii) For $\sigma \in \mathrm{Gal}(F'/F)$, let $E \subset F'(\boldsymbol{\mu}_p)$ be the fixed field of (σ, τ) where τ is the generator of $\mathbb{F}_p^\times$. Show that $E(\boldsymbol{\mu}_p) = F'(\boldsymbol{\mu}_p)$, and thus $\mathrm{Art}_{F'(\boldsymbol{\mu}_p)/E}$ is surjective. By global base change, conclude that $\sigma \in \mathrm{Im}\,(\mathrm{Art}_{F'/F})$.

(A similar argument reduces the proof of *Chebotarev density theorem* to the cyclotomic case, which is shown by the non-vanishing at $s = 1$ of the Dirichlet L series (the class number formula), thus without CFT. I learned this from Jack Thorne.)

6. Hilbert class fields (Lecture 4). A finite extension F'/F of number fields is called *everywhere unramified* if it is unramified at all finite places of F. The union H/F of all finite everywhere unramified *abelian* extensions (inside F^{ab}) is called the *Hilbert class field* of F. Deduce from the global class field theory that Art_F induces:

$$\mathrm{Cl}_F = F^\times\backslash\mathbb{A}_F^\times/(F_\infty^\times \times \widehat{\mathcal{O}}^\times) \xrightarrow{\cong} \mathrm{Gal}(H/F).$$

References

[AT] Artin, E., Tate, J., *Class Field Theory*, Benjamin, 1967.

[Ch] Chevalley, C., *Deux Théorèmes d'Arithmétique*, J. Math. Soc. Japan **3**-1 (1951), 36–44.

[Se] Serre, J.-P., *Abelian ℓ-adic representations and elliptic curves*, Benjamin, 1968.

[We] Weil, A., *On a Certain Type of Characters of the Idèle-Class Group of an Algebraic Number-Field*, in: *Proceedings of the International Symposium on Algebraic Number Theory* (Tokyo-Nikko 1955), The Science Council of Japan, 1956, 1–7.

[Y] Yoshida, T., *Local class field theory via Lubin-Tate theory*, Ann. Fac. Sci. Toulouse Math., Ser. 6. **17**-2 (2008), 411–438.

Index