

Part IV — Topics in Number Theory

Based on lectures by A. J. Scholl

Notes taken by Dexter Chua

Lent 2018

These notes are not endorsed by the lecturers, and I have modified them (often significantly) after lectures. They are nowhere near accurate representations of what was actually lectured, and in particular, all errors are almost surely mine.

The “Langlands programme” is a far-ranging series of conjectures describing the connections between automorphic forms on the one hand, and algebraic number theory and arithmetic algebraic geometry on the other. In these lectures we will give an introduction to some aspects of this programme.

Pre-requisites

The course will follow on naturally from the Michaelmas term courses *Algebraic Number Theory* and *Modular Forms and L-Functions*, and knowledge of them will be assumed. Some knowledge of algebraic geometry will be required in places.

Contents

0	Introduction	3
1	Class field theory	4
1.1	Preliminaries	4
1.2	Local class field theory	6
1.3	Global class field theory	11
1.4	Ideal-theoretic description of global class field theory	18
2	Hecke characters and abelian L-functions	20
2.1	Ideal-theoretic description of any Hecke character	21
3	Abelian L-functions	29
4	Non-abelian L-functions	32
	Index	38

0 Introduction

In this course, we shall first give an outline of class field theory. We then look at abelian L -functions (Hecke, Tate). We then talk about *non*-abelian L -functions, and in particular the Weil–Deligne group and local L - and ε -factors.

We then talk about local Langlands for GL_n a bit, and do a bit of global theory and automorphic forms at the end.

The aim is not to prove everything, because that will take 3 courses instead of one, but we are going to make precise definitions and statements of everything.

1 Class field theory

1.1 Preliminaries

Class field theory is the study of abelian extensions of local or global fields. Before we can do class field theory, we must first know *Galois* theory.

Notation. Let K be a field. We will write \bar{K} for a separable closure of K , and $\Gamma_K = \text{Gal}(\bar{K}/K)$. We have

$$\Gamma_k = \varprojlim_{L/K \text{ finite separable}} \text{Gal}(L/K),$$

which is a *profinite group*. The associated topology is the *Krull topology*.

Galois theory tells us

Theorem (Galois theory). There are bijections

$$\begin{aligned} \left\{ \begin{array}{c} \text{closed subgroups of} \\ \Gamma_K \end{array} \right\} &\longleftrightarrow \left\{ \begin{array}{c} \text{subfields} \\ K \subseteq L \subseteq \bar{K} \end{array} \right\} \\ \left\{ \begin{array}{c} \text{open subgroups of} \\ \Gamma_K \end{array} \right\} &\longleftrightarrow \left\{ \begin{array}{c} \text{finite subfields} \\ K \subseteq L \subseteq \bar{K} \end{array} \right\} \end{aligned}$$

Notation. We write K^{ab} for the maximal abelian subextension of \bar{K} , and

$$\text{Gal}(K^{\text{ab}}/K) = \Gamma_K^{\text{ab}} = \frac{\Gamma_K}{[\Gamma_K, \Gamma_K]}.$$

It is crucial to note that while \bar{K} is unique, it is only unique up to non-canonical isomorphism. Indeed, it has many automorphisms, given by elements of $\text{Gal}(\bar{K}/K)$. Thus, Γ_K is well-defined up to conjugation only. On the other hand, the abelianization Γ_K^{ab} is well-defined.

Definition (Non-Archimedean local field). A *non-Archimedean local field* is a finite extension of \mathbb{Q}_p or $\mathbb{F}_p((t))$.

We can also define Archimedean local fields, but they are slightly less interesting.

Definition (Archimedean local field). An Archimedean local field is a field that is \mathbb{R} or \mathbb{C} .

If F is a non-Archimedean local field, then it has a canonical normalized valuation

$$v = v_F : F^\times \rightarrow \mathbb{Z}.$$

Definition (Valuation ring). The *valuation ring* of a non-Archimedean local field F is

$$\mathcal{O} = \mathcal{O}_F = \{x \in F : v(x) \geq 0\}.$$

Any element $\pi = \pi_f \in \mathcal{O}_F$ with $v(\pi) = 1$ is called a *uniformizer*. This generates the maximal ideal

$$\mathfrak{m} = \mathfrak{m}_F = \{x \in \mathcal{O}_F : v(x) \geq 1\}.$$

Definition (Residue field). The *residue field* of a non-Archimedean field F is

$$k = k_F = \mathcal{O}_F/\mathfrak{m}_F.$$

This is a finite field of order $q = p^r$.

A particularly well-understood subfield of F^{ab} is the *maximal unramified extension* F^{ur} . We have

$$\text{Gal}(F^{\text{ur}}/F) = \text{Gal}(\bar{k}/k) = \hat{\mathbb{Z}} = \varprojlim_{n \geq 1} \mathbb{Z}/n\mathbb{Z}.$$

and this is completely determined by the behaviour of the residue field. The rest of Γ_F is called the *inertia group*.

Definition (Inertia group). The *inertia group* I_F is defined to be

$$I_F = \text{Gal}(\bar{F}/F^{\text{ur}}) \subseteq \Gamma_F.$$

We also define

Definition (Wild inertia group). The *wild inertia group* P_F is the maximal pro- p -subgroup of I_F .

Returning to the maximal unramified extension, note that saying $\text{Gal}(\bar{k}/k) \cong \hat{\mathbb{Z}}$ requires picking an isomorphism, and this is equivalent to picking an element of $\hat{\mathbb{Z}}$ to be the “1”. Naively, we might pick the following:

Definition (Arithmetic Frobenius). The *arithmetic Frobenius* $\varphi_q \in \text{Gal}(\bar{k}/k)$ (where $|k| = q$) is defined to be

$$\varphi_q(x) = x^q.$$

Identifying this with $1 \in \hat{\mathbb{Z}}$ leads to infinite confusion, and we shall not do so. Instead, we define

Definition (Geometric Frobenius). The *geometric Frobenius* is

$$\text{Frob}_q = \varphi_q^{-1} \in \text{Gal}(\bar{k}/k).$$

We shall identify $\text{Gal}(\bar{k}/k) \cong \hat{\mathbb{Z}}$ by setting the *geometric Frobenius* to be 1.

The reason this is called the geometric Frobenius is that if we have a scheme over a finite field k , then there are two ways the Frobenius can act on it — either as a Galois action, or as a pullback along the morphism $(-)^q : k \rightarrow k$. The latter corresponds to the geometric Frobenius.

We now turn to understand the inertia groups. The point of introducing the wild inertia group is to single out the “ p -phenomena”, which we would like to avoid. To understand I_F better, let n be a natural number prime to p . As usual, we write

$$\mu_n(\bar{k}) = \{\zeta \in \bar{k} : \zeta^n = 1\}.$$

We also pick an n th root of π in \bar{F} , say π_n . By definition, this has $\pi_n^n = \pi$.

Definition (Tame mod n character). The *tame mod n character* is the map $t(n) : I_F = \text{Gal}(\bar{F}/F^{\text{ur}}) \rightarrow \mu_n(\bar{k})$ given by

$$\gamma \mapsto \gamma(\pi_n)/\pi_n \pmod{\pi}.$$

Note that since γ fixes $\pi = \pi_n^n$, we indeed have

$$\left(\frac{\gamma(\pi_n)}{\pi_n}\right)^n = \frac{\gamma(\pi_n^n)}{\pi_n^n} = 1.$$

Moreover, this doesn't depend on the choice of π_n . Any other choice differs by an n th root of unity, but the n th root of unity lies in F^{ur} since n is prime to p . So γ fixes it and so it cancels out in the fraction. For the same reason, if γ moves π_n at all, then this is visible down in \bar{k} , since γ would have multiplied π_n by an n th root of unity, and these n th roots are present in \bar{k} .

Now that everything is canonically well-defined, we can take the limit over all n to obtain a map

$$\hat{t} : I_F \rightarrow \lim_{(n,p)=1} \mu_n(\bar{k}) = \prod_{\ell \neq p} \lim_{m \geq 1} \mu_{\ell^m}(\bar{k}) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell(1)(\bar{k}).$$

This $\mathbb{Z}_\ell(1)(\bar{k})$ is the *Tate module* of \bar{k}^\times . This is isomorphic to \mathbb{Z}_ℓ , but not canonically.

Theorem. $\ker \hat{t} = P_F$.

Thus, it follows that *maximal tamely ramified extension* of F , i.e. the fixed field of P_F is

$$\bigcup_{(n,p)=1} F^{ur}(\sqrt[n]{\pi}).$$

Note that $t(n)$ extends to a map $\Gamma_F \rightarrow \mu_n$ given by the same formula, but this now depends on the choice of π_n , and further, it is not a homomorphism, because

$$t(n)(\gamma\delta) = \frac{\gamma\delta(\pi_n)}{\pi_n} = \frac{\gamma(\pi_n)}{\pi_n} \gamma\left(\frac{\delta(\pi_n)}{\pi_n}\right) = t(n)(\gamma) \cdot \gamma(t(n)(\delta)).$$

So this formula just says that $t(n)$ is a 1-cocycle. Of course, picking another π_n will modify $t(n)$ by a coboundary.

1.2 Local class field theory

Local class field theory is a (collection of) theorems that describe abelian extensions of a local field. The key takeaway is that finite abelian extensions of F correspond to open finite index subgroups of F^\times , but the theorem says a bit more than that:

Theorem (Local class field theory).

- (i) Let F be a local field. Then there is a continuous homomorphism, the *local Artin map*

$$\text{Art}_F : F^\times \rightarrow \Gamma_F^{\text{ab}}$$

with dense image characterized by the properties j

- (a) The following diagram commutes:

$$\begin{array}{ccc} F^\times & \xrightarrow{\text{Art}_F} & \Gamma_F^{\text{ab}} & \twoheadrightarrow & \Gamma_F/I_F \\ \downarrow v_F & & & & \downarrow \sim \\ \mathbb{Z} & \hookrightarrow & & & \hat{\mathbb{Z}} \end{array}$$

(b) If F'/F is finite, then the following diagram commutes:

$$\begin{array}{ccc} (F')^\times & \xrightarrow{\text{Art}_{F'}} & \Gamma_{F'}^{\text{ab}} = \text{Gal}(F'^{\text{ab}}/F') \\ \downarrow N_{F'/F} & & \downarrow \text{restriction} \\ F^\times & \xrightarrow{\text{Art}_F} & \Gamma_F^{\text{ab}} = \text{Gal}(F^{\text{ab}}/F) \end{array}$$

(ii) Moreover, the *existence theorem* says Art_F^{-1} induces a bijection

$$\left\{ \begin{array}{l} \text{open finite index} \\ \text{subgroups of } F^\times \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{open subgroups of } \Gamma_F^{\text{ab}} \end{array} \right\}$$

Of course, open subgroups of Γ_F^{ab} further corresponds to finite abelian extensions of F .

(iii) Further, Art_F induces an isomorphism

$$\mathcal{O}_F^\times \xrightarrow{\sim} \text{im}(I_F \rightarrow \Gamma_F^{\text{ab}})$$

and this maps $(1 + \pi\mathcal{O}_F)^\times$ to the image of P_F . Of course, the quotient $\mathcal{O}_F^\times / (1 + \pi\mathcal{O}_F)^\times \cong k^\times = \mu_\infty(k)$.

(iv) Finally, this is functorial, namely if we have an isomorphism $\alpha : F \xrightarrow{\sim} F'$ and extend it to $\bar{\alpha} : \bar{F} \xrightarrow{\sim} \bar{F}'$, then this induces isomorphisms between the Galois groups $\alpha_* : \Gamma_F \xrightarrow{\sim} \Gamma_{F'}$ (up to conjugacy), and $\alpha_*^{\text{ab}} \circ \text{Art}_F = \text{Art}_{F'} \circ \alpha_*^{\text{ab}}$. \square

On the level of finite Galois extensions E/F , we can rephrase the first part of the theorem as giving a map

$$\text{Art}_{E/F} : \frac{F^\times}{N_{E/F}(E^\times)} \rightarrow \text{Gal}(E/F)^{\text{ab}}$$

which is now an isomorphism (since a dense subgroup of a discrete group is the whole thing!).

We can write down these maps explicitly in certain special cases. We will not justify the following example:

Example. If $F = \mathbb{Q}_p$, then

$$F^{\text{ab}} = \mathbb{Q}_p(\mu_\infty) = \bigcup \mathbb{Q}_p(\mu_n) = \mathbb{Q}_p^{ur}(\mu_{p^\infty}).$$

Moreover, if we write $x \in \mathbb{Q}_p^\times$ as $p^n y$ with $y \in \mathbb{Z}_p^\times$, then

$$\text{Art}_{\mathbb{Q}}(x)|_{\mathbb{Q}_p^{ur}} = \text{Frob}_p^n, \quad \text{Art}_{\mathbb{Q}}(x)|_{\mathbb{Q}_p(\mu_{p^\infty})} = (\zeta_{p^n} \mapsto \zeta_{p^n}^{y \bmod p^n}).$$

If we had the arithmetic Frobenius instead, then we would have a $-y$ in the power there, which is less pleasant.

The cases of the Archimedean local fields are easy to write down and prove directly!

Example. If $F = \mathbb{C}$, then $\Gamma_F = \Gamma_F^{\text{ab}} = 1$ is trivial, and the Artin map is similarly trivial. There are no non-trivial open finite index subgroups of \mathbb{C}^\times , just as there are no non-trivial open subgroups of the trivial group.

Example. If $F = \mathbb{R}$, then $\bar{\mathbb{R}} = \mathbb{C}$ and $\Gamma_F = \Gamma_F^{\text{ab}} = \mathbb{Z}/2\mathbb{Z} = \{\pm 1\}$. The Artin map is given by the sign map. The unique open finite index subgroup of \mathbb{R}^\times is $\mathbb{R}_{>0}^\times$, and this corresponds to the finite Galois extension \mathbb{C}/\mathbb{R} .

As stated in the theorem, the Artin map has dense image, but is not surjective (in general). To fix this problem, it is convenient to introduce the *Weil group*.

Definition (Weil group). Let F be a non-Archimedean local field. Then the *Weil group* of F is the topological group W_F defined as follows:

- As a group, it is

$$W_F = \{\gamma \in \Gamma_F \mid \gamma|_{F^{\text{ur}}} = \text{Frob}_q^n \text{ for some } n \in \mathbb{Z}\}.$$

Recall that $\text{Gal}(F^{\text{ur}}/F) = \hat{\mathbb{Z}}$, and we are requiring $\gamma|_{F^{\text{ur}}}$ to be in \mathbb{Z} . In particular, $I_F \subseteq W_F$.

- The topology is defined by the property that I_F is an *open* subgroup with the profinite topology. Equivalently, W_F is a fiber product of topological groups

$$\begin{array}{ccc} W_F & \hookrightarrow & \Gamma_F \\ \downarrow & & \downarrow \\ \mathbb{Z} & \hookrightarrow & \hat{\mathbb{Z}} \end{array}$$

where \mathbb{Z} has the discrete topology.

Note that W_F is not profinite. It is totally disconnected but not compact.

This seems like a slightly artificial definition, but this is cooked up precisely so that

Proposition. Art_F induces an *isomorphism* of topological groups

$$\text{Art}_F^W : F^\times \rightarrow W_F^{\text{ab}}.$$

This maps \mathcal{O}_F^\times isomorphically onto the inertia subgroup of Γ_F^{ab} .

In the case of Archimedean local fields, we make the following definitions. They will seem rather ad hoc, but we will provide some justification later.

- The Weil group of \mathbb{C} is defined to be $W_{\mathbb{C}} = \mathbb{C}^\times$, and the Artin map $\text{Art}_{\mathbb{R}}^W$ is defined to be the identity.
- The Weil group of \mathbb{R} is defined the non-abelian group

$$W_{\mathbb{R}} = \langle \mathbb{C}^\times, \sigma \mid \sigma^2 = -1 \in \mathbb{C}^\times, \sigma z \sigma^{-1} = \bar{z} \text{ for all } z \in \mathbb{C}^\times \rangle.$$

This is a (non)-split extension of \mathbb{C}^\times by $\Gamma_{\mathbb{R}}$,

$$1 \rightarrow \mathbb{C}^\times \rightarrow W_{\mathbb{R}} \rightarrow \Gamma_{\mathbb{R}} \rightarrow 1,$$

where the last map sends $z \mapsto 0$ and $\sigma \mapsto 1$. This is in fact the unique non-split extension of $\Gamma_{\mathbb{R}}$ by \mathbb{C}^\times where $\Gamma_{\mathbb{R}}$ acts on \mathbb{C}^\times in a natural way.

The map $\text{Art}_{\mathbb{R}}^W$ is better described by its inverse, which maps

$$\begin{aligned} (\text{Art}_{\mathbb{R}}^W)^{-1} : W_{\mathbb{R}}^{\text{ab}} &\xrightarrow{\sim} \mathbb{R}^\times \\ z &\longmapsto z\bar{z} \\ \sigma &\longmapsto -1 \end{aligned}$$

To understand these definitions, we need the notion of the relative Weil group.

Definition (Relative Weil group). Let F be a non-Archimedean local field, and E/F Galois but not necessarily finite. We define

$$W_{E/F} = \{\gamma \in \text{Gal}(E^{\text{ab}}/F) : \gamma|_{F^{\text{ur}}} = \text{Frob}_q^n, n \in \mathbb{Z}\} = \frac{W_F}{[W_E, W_E]}.$$

with the quotient topology.

The $W_{\bar{F}/F} = W_F$, while $W_{F/F} = W_F^{\text{ab}} = F^\times$ by local class field theory.

Now if E/F is a finite extension, then we have an exact sequence of Galois groups

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \text{Gal}(E^{\text{ab}}/E) & \longrightarrow & \text{Gal}(E^{\text{ab}}/F) & \longrightarrow & \text{Gal}(E/F) & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \parallel & & \\ 1 & \longrightarrow & W_E^{\text{ab}} & \longrightarrow & W_{E/F} & \longrightarrow & \text{Gal}(E/F) & \longrightarrow & 1. \end{array}$$

By the Artin map, $W_E^{\text{ab}} = E^\times$. So the relative Weil group is an extension of $\text{Gal}(E/F)$ by E^\times . In the case of non-Archimedean fields, we have

$$\lim_E E^\times = \{1\},$$

where the field extensions are joined by the norm map. So \bar{F}^\times is invisible in $W_F = \lim W_{E/F}$. The weirdness above comes from the fact that the separable closures of \mathbb{R} and \mathbb{C} are finite extensions.

We are, of course, not going to prove local class field theory in this course. However, we can say something about the proofs. There are a few ways of proving it:

- The cohomological method (see Artin–Tate, Cassels–Fröhlich), which only treats the first part, namely the existence of Art_K . We start off with a finite Galois extension E/F , and we want to construct an isomorphism

$$\text{Art}_{E/F} : F^\times / N_{E/F}(E^\times) \rightarrow \text{Gal}(E/F)^{\text{ab}}.$$

Writing $G = \text{Gal}(E/F)$, this uses the cohomological interpretation

$$F^\times / N_{E/F}(E^\times) = \hat{H}^0(G, E^\times),$$

where \hat{H} is the Tate cohomology of finite groups. On the other hand, we have

$$G^{\text{ab}} = H_1(G, \mathbb{Z}) = \hat{H}^{-2}(G, \mathbb{Z}).$$

The main step is to compute

$$H^2(G, E^\times) = \hat{H}^2(G, E^\times) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z} = H^2(\Gamma_F, \bar{F}^\times).$$

where $n = [E : F]$. The final group $H^2(\Gamma_F, \bar{F}^\times)$ is the *Brauer group* $\text{Br}(F)$, and the subgroup is just the kernel of $\text{Br}(F) \rightarrow \text{Br}(E)$.

Once we have done this, we then define $\text{Art}_{E/F}$ to be the cup product with the generator of $\hat{H}^2(G, E^\times)$, and this maps $\hat{H}^{-2}(G, \mathbb{Z}) \rightarrow \hat{H}^0(G, E^\times)$. The fact that this map is an isomorphism is rather formal.

The advantage of this method is that it generalizes to duality theorems about $H^*(G, M)$ for arbitrary M , but this map is not at all explicit, and is very much tied to abelian extensions.

- Formal group methods: We know that the maximal abelian extension of \mathbb{Q}_p is obtained in two steps — we can write

$$\mathbb{Q}_p^{\text{ab}} = \mathbb{Q}_p^{\text{ur}}(\mu_{p^\infty}) = \mathbb{Q}_p^{\text{ur}}(\text{torsion points in } \hat{\mathbb{G}}_m),$$

where $\hat{\mathbb{G}}_m$ is the formal multiplication group, which we can think of as $(1 + \mathfrak{m}_{\mathbb{Q}_p})^\times$. This generalizes to any F/\mathbb{Q}_p — we have

$$F^{\text{ab}} = F^{\text{ur}}(\text{torsion points in } \hat{\mathbb{G}}_\pi),$$

where $\hat{\mathbb{G}}_\pi$ is the “Lubin–Tate formal group”. This is described in Iwasawa’s book, and also in a paper of Yoshida’s. The original paper by Lubin and Tate is also very readable.

The advantage of this is that it is very explicit, and when done correctly, gives both the existence of the Artin map and the existence theorem. This also has a natural generalization to non-abelian extensions. However, it does not give duality theorems.

- Neukrich’s method: Suppose E/F is abelian and finite. If $g \in \text{Gal}(E/F)$, we want to construct $\text{Art}_{E/F}^{-1}(g) \in F^\times/N_{E/F}(E^\times)$. The point is that there is only one possibility, because $\langle g \rangle$ is a cyclic subgroup of $\text{Gal}(E/F)$, and corresponds to some cyclic extension $\text{Gal}(E/F')$. We have the following lemma:

Lemma. There is a finite K/F' such that $K \cap E = F'$, so $\text{Gal}(KE/K) \cong \text{Gal}(E/F') = \langle g \rangle$. Moreover, KE/K is unramified.

Let $g'|_E = g$, and suppose $g' = \text{Frob}_{KE/K}^a$. If local class field theory is true, then we have to have

$$\text{Art}_{KE/K}^{-1}(g') = \pi_K^a \pmod{N_{KE/K}(KE^\times)}.$$

Then by our compatibility conditions, this implies

$$\text{Art}_{E/F}^{-1}(g) = N_{K/F}(\pi_K^a) \pmod{N_{E/F}(E^\times)}.$$

The problem is then to show that this does not depend on the choices, and then show that it is a homomorphism. These are in fact extremely complicated. Note that everything so far is just Galois theory. Solving these two problems is then where all the number theory goes in.

- When class field theory was first done, we first did *global* class field theory, and deduced the local case from that. No one does that anymore nowadays, since we now have purely local proofs. However, when we try to generalize to the Langlands programme, what we have so far all start with global theorems and then proceed to deduce local results.

1.3 Global class field theory

We now proceed to discuss global class field theory.

Definition (Global field). A *global field* is a number field or $k(C)$ for a smooth projective absolutely irreducible curve C/\mathbb{F}_q , i.e. a finite extension of $\mathbb{F}_q(t)$.

A lot of what we can do can be simultaneously done for both types of global fields, but we are mostly only interested in the case of number fields, and our discussions will mostly focus on those.

Definition (Place). Let K be a global field. Then a *place* is a valuation on K . If K is a number field, we say a valuation v is a *finite place* if it is the valuation at a prime $\mathfrak{p} \triangleleft \mathcal{O}_K$. A valuation v is an *infinite place* if comes from a complex or real embedding of K . We write Σ_K for the set of places of K , and Σ_K^∞ and $\Sigma_{K,\infty}$ for the sets of finite and infinite places respectively. We also write $v \nmid \infty$ if v is a finite place, and $v \mid \infty$ otherwise.

If K is a function field, then all places are finite, and these correspond to closed points of the curve.

If $v \in \Sigma_K$ is a place, then there is a completion $K \hookrightarrow K_v$. If v is infinite, then K_v is \mathbb{R} or \mathbb{C} , i.e. an Archimedean local field. Otherwise, K_v is a non-Archimedean local field.

Example. If $\mathbb{Q} = K$, then there is one infinite prime, which we write as ∞ , given by the embedding $\mathbb{Q} \hookrightarrow \mathbb{R}$. If $v = p$, then we get the embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ into the p -adic completion.

Notation. If v is a finite place, we write $\mathcal{O}_v \subseteq K_v$ for the valuation ring of the completion.

Any local field has a canonically normalized valuation, but there is no canonical absolute value. It is useful to fix the absolute value of our local fields. For doing class field theory, the right way to put an absolute value on K_v (and hence K) is by

$$|x|_v = q_v^{-v(x)},$$

where

$$q_v = \left| \frac{\mathcal{O}_v}{\pi_v \mathcal{O}_v} \right|$$

is the cardinality of the residue field at v . For example, if $K = \mathbb{Q}$ and $v = p$, then $q_v = p$, and $|p|_v = \frac{1}{p}$.

In the Archimedean case, if K_v is real, then we set $|x|$ to be the usual absolute value; if K_v is complex, then we take $|x|_v = x\bar{x} = |x|^2$.

The reason for choosing these normalizations is that we have the following product formula:

Proposition (Product formula). If $x \in K^\times$, then

$$\prod_{v \in \Sigma_K} |x|_v = 1.$$

The proof is not difficult. First observe that it is true for \mathbb{Q} , and then show that this formula is “stable under finite extensions”, which extends the result to all finite extensions of \mathbb{Q} .

Global class field theory is best stated in terms of adèles and ideles. We make the following definition:

Definition (Adele). The *adèles* is defined to be the restricted product

$$\mathbb{A}_K = \prod'_v K_v = \left\{ (x_v)_{v \in K_v} : x_v \in \mathcal{O}_v \text{ for all but finitely many } v \in \Sigma_K^\infty \right\}.$$

We can write this as $K_\infty \times \hat{K}$ or $\mathbb{A}_{K,\infty} \times \mathbb{A}_K^\infty$, where

$$K_\infty = \mathbb{A}_{K,\infty} = K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

consists of the product over the infinite places, and

$$\hat{K} = \mathbb{A}_K^\infty = \prod'_{v \nmid \infty} K_v = \bigcup_{S \subseteq \Sigma_K^\infty \text{ finite}} \prod_{v \in S} K_v \times \prod_{v \in \Sigma_K^\infty \setminus S} \mathcal{O}_v.$$

This contains $\hat{\mathcal{O}}_K = \prod_{v \nmid \infty} \mathcal{O}_K$. In the case of a number field, $\hat{\mathcal{O}}_K$ is the profinite completion of \mathcal{O}_K . More precisely, if K is a number field then

$$\hat{\mathcal{O}}_K = \lim_{\mathfrak{a}} \mathcal{O}_K / \mathfrak{a} = \lim \mathcal{O}_K / N\mathcal{O}_K = \mathcal{O}_K \otimes_{\mathbb{Z}} \hat{\mathbb{Z}},$$

where the last equality follows from the fact that \mathcal{O}_K is a finite \mathbb{Z} -module.

Definition (Idele). The *ideles* is the restricted product

$$J_K = \mathbb{A}_K^\times = \prod'_v K_v^\times = \left\{ (x_v)_v \in \prod K_v^\times : x_v \in \mathcal{O}_v^\times \text{ for almost all } v \right\}.$$

These objects come with natural topologies. On \mathbb{A}_K , we take $K_\infty \times \hat{\mathcal{O}}_K$ to be an open subgroup with the product topology. Once we have done this, there is a unique structure of a topological ring for which this holds. On J_K , we take $K_\infty^\times \times \hat{\mathcal{O}}_K^\times$ to be open with the product topology. Note that this is not the subspace topology under the inclusion $J_K \hookrightarrow \mathbb{A}_K$. Instead, it is induced by the inclusion

$$\begin{aligned} J_K &\hookrightarrow \mathbb{A}_K \times \mathbb{A}_K \\ x &\mapsto (x, x^{-1}). \end{aligned}$$

It is a basic fact that $K^\times \subseteq J_K$ is a *discrete* subgroup.

Definition (Idele class group). The *idele class group* is then

$$C_K = J_K / K^\times.$$

The idele class group plays an important role in global class field theory. Note that J_K comes with a natural absolute value

$$\begin{aligned} |\cdot|_A : J_K &\rightarrow \mathbb{R}_{>0}^\times \\ (x_v) &\mapsto \prod_{v \in \Sigma_K} |x_v|_v. \end{aligned}$$

The product formula implies that $|K^\times|_A = \{1\}$. So this in fact a map $C_K \rightarrow \mathbb{R}_{>0}^\times$. Moreover, we have

Theorem. The map $|\cdot|_{\mathbb{A}} : C_K \rightarrow \mathbb{R}_{>0}^{\times}$ has compact kernel.

This seemingly innocent theorem is actually quite powerful. For example, we will later construct a continuous surjection $C_K \rightarrow \text{Cl}(K)$ to the ideal class group of K . In particular, this implies $\text{Cl}(K)$ is finite! In fact, the theorem is equivalent to the finiteness of the class group and Dirichlet's unit theorem.

Example. In the case $K = \mathbb{Q}$, we have, by definition,

$$J_{\mathbb{Q}} = \mathbb{R}^{\times} \times \prod'_p \mathbb{Q}_p^{\times}.$$

Suppose we have an idele $x = (x_v)$. It is easy to see that there exists a unique rational number $y \in \mathbb{Q}^{\times}$ such that $\text{sgn}(y) = \text{sgn}(x_{\infty})$ and $v_p(y) = v_p(x_p)$. So we have

$$J_{\mathbb{Q}} = \mathbb{Q}^{\times} \times \left(\mathbb{R}_{>0}^{\times} \times \prod_p \mathbb{Z}_p^{\times} \right).$$

Here we think of \mathbb{Q}^{\times} as being embedded diagonally into $J_{\mathbb{Q}}$, and as we have previously mentioned, \mathbb{Q}^{\times} is discrete. From this description, we can read out a description of the idele class group

$$C_{\mathbb{Q}} = \mathbb{R}_{>0}^{\times} \times \hat{\mathbb{Z}}^{\times},$$

and $\hat{\mathbb{Z}}^{\times}$ is the kernel $|\cdot|_{\mathbb{A}}$.

From the decomposition above, we see that $C_{\mathbb{Q}}$ has a maximal connected subgroup $\mathbb{R}_{>0}^{\times}$. In fact, this is the intersection of all open subgroups containing 1. For a general K , we write C_K^0 for the maximal connected subgroup, and then

$$\pi_0(C_K) = C_K / C_K^0,$$

In the case of $K = \mathbb{Q}$, we can naturally identify

$$\pi_0(C_{\mathbb{Q}}) = \hat{\mathbb{Z}}^{\times} = \lim_n (\mathbb{Z}/n\mathbb{Z})^{\times} = \lim_n \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \text{Gal}(\mathbb{Q}(\zeta_{\infty})/\mathbb{Q}).$$

The field $\mathbb{Q}(\zeta_{\infty})$ is not just any other field. The Kronecker–Weber theorem says this is in fact the maximal abelian extension of \mathbb{Q} . Global class field theory is a generalization of this isomorphism to all fields.

Just like in local class field theory, global class field theory involves a certain Artin map. In the local case, we just pulled them out of a hat. To construct the global Artin map, we simply have to put these maps together to form a global Artin map.

Let L/K be a finite Galois extension, v a place of K , and $w | v$ a place of L extending v . For finite places, this means the corresponding primes divide; for infinite places, this means the embedding w is an extension of v . We then have the *decomposition group*

$$\text{Gal}(L_w/K_v) \subseteq \text{Gal}(L/K).$$

If L/K is abelian, since any two places lying above v are conjugate, this depends only on v . In this case, we can now define the *global Artin map*

$$\begin{aligned} \text{Art}_{L/K} : J_K &\longrightarrow \text{Gal}(L/K) \\ (x_v)_v &\longmapsto \prod_v \text{Art}_{L_w/K_v}(x_v), \end{aligned}$$

where we pick one w for each v . To see this is well-defined, note that if $x_v \in \mathcal{O}_v^\times$ and L/K is unramified at $v \nmid \infty$, then $\text{Art}_{K_w/K_v}(x_v) = 1$. So the product is in fact finite.

By the compatibility of the Artin maps, we can pass on to the limit over all extensions L/K , and get a continuous map

$$\text{Art}_K : J_K \rightarrow \Gamma_K^{\text{ab}}.$$

Theorem (Artin reciprocity law). $\text{Art}_K(K^\times) = \{1\}$, so induces a map $C_K \rightarrow \Gamma_K^{\text{ab}}$. Moreover,

- (i) If $\text{char}(K) = p > 0$, then Art_K is injective, and induces an isomorphism $\text{Art}_K : C_K \xrightarrow{\sim} W_K^{\text{ab}}$, where W_K is defined as follows: since K is a finite extension of $\mathbb{F}_q(T)$, and wlog assume $\bar{\mathbb{F}}_q \cap K = \mathbb{F}_q \equiv k$. Then W_K is defined as the pullback

$$\begin{array}{ccc} W_K & \hookrightarrow & \Gamma_K = \text{Gal}(\bar{K}/K) \\ \downarrow & & \downarrow \text{restr.} \\ \mathbb{Z} & \hookrightarrow & \hat{\mathbb{Z}} \cong \text{Gal}(\bar{k}/k) \end{array}$$

- (ii) If $\text{char}(K) = 0$, we have an isomorphism

$$\text{Art}_K : \pi_0(C_K) = \frac{C_K}{C_K^0} \xrightarrow{\sim} \Gamma_K^{\text{ab}}.$$

Moreover, if L/K is finite, then we have a commutative diagram

$$\begin{array}{ccc} C_L & \xrightarrow{\text{Art}_L} & \Gamma_L^{\text{ab}} \\ \downarrow N_{L/K} & & \downarrow \text{restr.} \\ C_K & \xrightarrow{\text{Art}_K} & \Gamma_K^{\text{ab}} \end{array}$$

If this is in fact Galois, then this induces an isomorphism

$$\text{Art}_{L/K} : \frac{J_K}{K^\times N_{L/K}(J_L)} \xrightarrow{\sim} \text{Gal}(L/K)^{\text{ab}}.$$

Finally, this is functorial, namely if $\sigma : K \xrightarrow{\sim} K'$ is an isomorphism, then we have a commutative square

$$\begin{array}{ccc} C_K & \xrightarrow{\text{Art}_K} & \Gamma_K^{\text{ab}} \\ \downarrow \sigma & & \downarrow \\ C_{K'} & \xrightarrow{\text{Art}_{K'}} & \Gamma_{K'}^{\text{ab}} \end{array}$$

Observe that naturality and functoriality are immediate consequences of the corresponding results for local class field theory.

As a consequence of the isomorphism, we have a correspondence

$$\left\{ \begin{array}{c} \text{finite abelian extensions} \\ L/K \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{finite index open subgroups} \\ \text{of } J_K \text{ containing } K^\times \end{array} \right\}$$

$$L \mapsto \ker(\text{Art}_{L/K} : J_K \rightarrow \text{Gal}(L/K))$$

Note that there exists finite index subgroups that are not open!

Recall that in local class field theory, if we decompose $K_v = \langle \pi \rangle \times \mathcal{O}_v^\times$, then the local Artin map sends \mathcal{O}_v^\times to (the image of) the inertia group. Thus an extension L_w/K_v is unramified iff the local Artin map kills \mathcal{O}_v^\times . Globally, this tells us

Proposition. If L/K is an abelian extension of global fields, which corresponds to the open subgroup $U \subseteq J_K$ under the Artin map, then L/K is unramified at a finite $v \nmid \infty$ iff $\mathcal{O}_v^\times \subseteq U$.

We can extend this to the infinite places if we make the appropriate definitions. Since \mathbb{C} cannot be further extended, there is nothing to say for complex places.

Definition (Ramification). If $v \mid \infty$ is a real place of K , and L/K is a finite abelian extension, then we say v is ramified if for some (hence all) places w of L above v , w is complex.

The terminology is not completely standard. In this case, Neukrich would say v is inert instead.

With this definition, L/K is unramified at a real place v iff $K_v^\times = \mathbb{R}^\times \subseteq U$. Note that since U is open, it automatically contains $\mathbb{R}_{>0}^\times$.

We can similarly read off splitting information.

Proposition. If v is finite and unramified, then v splits completely iff $K_v^\times \subseteq U$.

Proof. v splits completely iff $L_w = K_v$ for all $w \mid v$, iff $\text{Art}_{L_w/K_v}(K_v^\times) = \{1\}$. \square

Example. We will use global class field theory to compute all S_3 extensions L/\mathbb{Q} which are unramified outside 5 and 7.

If we didn't have global class field theory, then to solve this problem we have to find all cubics whose discriminant are divisible by 5 and 7 only, and there is a cubic diophantine problem to solve.

While S_3 is not an abelian group, it is solvable. So we can break our potential extension as a chain

$$\begin{array}{c} L \\ | \\ 3 \\ K \\ | \\ 2 = \langle \sigma \rangle \\ \mathbb{Q} \end{array}$$

Since L/\mathbb{Q} is unramified outside 5 and 7, we know that K must be one of $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(\sqrt{-35})$. We then consider each case in turn, and then see what are the possibilities for L . We shall only do the case $K = \mathbb{Q}(\sqrt{-7})$ here. If we perform similar computations for the other cases, we find that the other choices of K do not work.

So fix $K = \mathbb{Q}(\sqrt{-7})$. We want L/K to be cyclic of degree 3, and σ must act non-trivially on L (otherwise we get an abelian extension).

Thus, by global class field theory, we want to find a subgroup $U \leq J_K$ of index 3 such that $\mathcal{O}_v^\times \subseteq U$ for all $v \nmid 35$. We also need $\sigma(U) = U$, or else the composite extension would not even be Galois, and σ has to act as -1 on $J_K/U \cong \mathbb{Z}/3\mathbb{Z}$ to get a non-abelian extension.

We know $K = \mathbb{Q}(\sqrt{-7})$ has class number 1, and the units are ± 1 . So we know

$$\frac{C_K}{C_K^0} = \frac{\hat{\mathcal{O}}_K^\times}{\{\pm 1\}}.$$

By assumption, we know U contains $\prod_{v \nmid 35} \mathcal{O}_v^\times$. So we have to look at the places that divide 35. In $\mathcal{O}_{\mathbb{Q}(\sqrt{-7})}$, the prime 5 is inert and 7 is ramified.

Since 5 is inert, we know K_5/\mathbb{Q}_5 is an unramified quadratic extension. So we can write

$$\mathcal{O}_{(5)}^\times = \mathbb{F}_{25}^\times \times (1 + 5\mathcal{O}_{(5)})^\times.$$

The second factor is a pro-5 group, and so it must be contained in U for the quotient to have order 3. On \mathbb{F}_{25}^\times , σ acts as the Frobenius $\sigma(x) = x^5$. Since \mathbb{F}_{25}^\times is cyclic of order 24, there is a unique index 3 subgroup, cyclic of order 6. This gives an index 3 subgroup $U_5 \subseteq \mathcal{O}_{(5)}^\times$. Moreover, on here, σ acts by $x \mapsto x^5 = x^{-1}$. Thus, we can take

$$U = \prod_{v \neq (5)} \mathcal{O}_v^\times \times U_5,$$

and this gives an S_3 extension of \mathbb{Q} that is unramified outside 5 and 7. It is an exercise to explicitly identify this extension.

We turn to the prime 7 = $-\sqrt{-7}^2$. Since this is ramified, we have

$$\mathcal{O}_{(\sqrt{-7})}^\times = \mathbb{F}_7^\times \times (1 + (\sqrt{-7})\mathcal{O}_{\sqrt{-7}})^\times,$$

and again the second factor is a pro-7 group. Moreover σ acts trivially on \mathbb{F}_7^\times . So U must contain $\mathcal{O}_{(\sqrt{-7})}^\times$. So what we found above is the unique such extension.

We previously explicitly described $C_{\mathbb{Q}}$ as $\mathbb{R}_{>0}^\times \times \hat{\mathbb{Z}}$. It would be nice to have a similar description of C_K for an arbitrary K . The connected component will come from the infinite places $K_\infty^\times \prod_{v|\infty} K_v^\times$. The connected component is given by

$$K_\infty^{\times,0} = (\mathbb{R}_{>0}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2},$$

where there are r_1 real places and r_2 complex ones. Thus, we find that

Proposition.

$$C_K/C_K^0 = \frac{\{\pm 1\}^{r_1} \times \hat{K}^\times}{K^\times}.$$

There is a natural map from the ideles to a more familiar group, called the content homomorphism.

Definition (Content homomorphism). The *content homomorphism* is the map

$$c : J_K \rightarrow \text{fractional ideals of } K$$

$$(x_v)_v \mapsto \prod_{v \nmid \infty} \mathfrak{p}_v^{v(x_v)},$$

where \mathfrak{p}_v is the prime ideal corresponding to v . We ignore the infinite places completely.

Observe that $c(K^\times)$ is the set of all principal ideals by definition. Moreover, the kernel of the content map is $K_\infty^\times \times \hat{\mathcal{O}}_K^\times$, by definition. So we have a short exact sequence

$$1 \rightarrow \frac{\{\pm 1\}^{r_1} \times \hat{\mathcal{O}}_K^\times}{\mathcal{O}_K^\times} \rightarrow C_K/C_K^0 \rightarrow \text{Cl}(K) \rightarrow 1.$$

If $K = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{-D})$, then $\overline{\mathcal{O}_K^\times} = \mathcal{O}_K^\times$ is finite, and in particular is closed. But in general, it will not be closed, and taking the closure is indeed needed.

Returning to the case $K = \mathbb{Q}$, our favorite abelian extensions are those of the form $L = \mathbb{Q}(\zeta_N)$ with $N > 1$. This comes with an Artin map

$$\hat{\mathbb{Z}}^\times \cong C_\mathbb{Q}/C_\mathbb{Q}^0 \rightarrow \text{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times.$$

By local class field theory for \mathbb{Q}_p , we see that with our normalizations, this is just the quotient map, whose kernel is

$$(1 + N\hat{\mathbb{Z}})^\times = \prod_{p \nmid N} \mathbb{Z}_p^\times \times \prod_{p \mid N} (1 + N\mathbb{Z}_p)^\times \subseteq \prod_{p \mid N} \mathbb{Z}_p^\times = \hat{\mathbb{Z}}^\times.$$

Note that if we used the arithmetic Frobenius, then we would get the *inverse* of the quotient map.

These subgroups of $\hat{\mathbb{Z}}^\times$ are rather special ones. First of all $(1 + N\hat{\mathbb{Z}})^\times$ form a neighbourhood of the identity in $\hat{\mathbb{Z}}^\times$. Thus, any open subgroup contains a subgroup of this form. Equivalently, every abelian extension of \mathbb{Q} is contained in $\mathbb{Q}(\zeta_N)$ for some N . This is the *Kronecker–Weber theorem*.

For a general number field K , we want to write down an explicit basis for open subgroups of 1 in $\pi_0(C_k)$.

Definition (Modulus). A *modulus* is a finite formal sum

$$\mathfrak{m} = \sum_{v \in \Sigma_k} m_v \cdot (v)$$

of places of K , where $m_v \geq 0$ are integers.

Given a modulus \mathfrak{m} , we define the subgroup

$$U_{\mathfrak{m}} = \prod_{v \mid \infty, m_v > 0} K_v^{\times, 0} \times \prod_{v \mid \infty, m_v = 0} K_v^\times \times \prod_{v \nmid \infty, m_v > 0} (1 + \mathfrak{p}_v^{m_v} \mathcal{O}_v)^\times \times \prod_{v \nmid \infty, m_v = 0} \mathcal{O}_v^\times \subseteq J_K.$$

Then essentially by definition of the topology of J_K , any open subgroup of J_K containing $K_\infty^{\times, 0}$ contains some $U_{\mathfrak{m}}$.

In our previous example, our moduli are all of the form

Definition ($\mathfrak{a}(\infty)$). If $\mathfrak{a} \triangleleft \mathcal{O}_K$ is an ideal, we write $\mathfrak{a}(\infty)$ for the modulus with $m_v = v(\mathfrak{a})$ for all $v \nmid \infty$, and $m_v = 1$ for all $v \mid \infty$.

If $k = \mathbb{Q}$ and $\mathfrak{m} = (N)(\infty)$, then we simply get $U_{\mathfrak{m}} = \mathbb{R}_{>0}^\times \times (1 + N\hat{\mathbb{Z}})^\times$, and so

$$\frac{J_\mathbb{Q}}{\mathbb{Q}^\times U_{\mathfrak{m}}} = (\mathbb{Z}/n\mathbb{Z})^\times,$$

corresponding to the abelian extension $\mathbb{Q}(\zeta_N)$.

In general, we define

Definition (Ray class field). If L/K is abelian with $\text{Gal}(L/K) \cong J_K/K^\times U_{\mathfrak{m}}$ under the Artin map, we call L the *ray class field* of K modulo \mathfrak{m} .

Definition (Conductor). If L corresponds to $U \subseteq J_K$, then $U \supseteq K^\times U_{\mathfrak{m}}$ for some \mathfrak{m} . The minimal such \mathfrak{m} is the *conductor* of L/K .

1.4 Ideal-theoretic description of global class field theory

Originally, class field theory was discovered using ideals, and the ideal-theoretic formulation is at times more convenient.

Let \mathfrak{m} be a modulus, and let S be the set of finite v such that $m_v > 0$. Let I_S be the group of fractional ideals prime to S . Consider

$$P(\mathfrak{m}) = \{(x) \in I(S) : x \equiv 1 \pmod{\mathfrak{m}}\}.$$

To be precise, we require that for all $v \in S$, we have $v(x-1) \geq m_v$, and for all infinite v real with $m_v > 0$, then $\tau(x) > 0$ for $\tau : K \rightarrow \mathbb{R}$ the corresponding to v . In other words, $x \in K^\times \cap U_{\mathfrak{m}}$.

Note that if \mathfrak{m} is trivial, then $I_S/P_{\mathfrak{m}}$ is the ideal class group. Thus, it makes sense to define

Definition (Ray class group). Let \mathfrak{m} be a modulus. The *generalized ideal class group*, or *ray class group* modulo \mathfrak{m} is

$$\text{Cl}_{\mathfrak{m}}(K) = I_S/P_{\mathfrak{m}}.$$

One can show that this is always a finite group.

Proposition. There is a canonical isomorphism

$$\frac{J_K}{K^\times U_{\mathfrak{m}}} \xrightarrow{\sim} \text{Cl}_{\mathfrak{m}}(K)$$

such that for $v \notin S \cup \Sigma_{K,\infty}$, the composition

$$K_v^\times \hookrightarrow J_K \rightarrow \text{Cl}_{\mathfrak{m}}(K)$$

sends $x \mapsto \mathfrak{p}_v^{-v(x)}$.

Thus, in particular, the Galois group $\text{Gal}(L/K)$ of the ray class field modulo \mathfrak{m} is $\text{Cl}_{\mathfrak{m}}(K)$. Concretely, if $\mathfrak{p} \notin S$ is an ideal, then $[\mathfrak{p}] \in \text{Cl}_{\mathfrak{m}}(K)$ corresponds to $\sigma_{\mathfrak{p}} \in \text{Gal}(L/K)$, the arithmetic Frobenius. This was Artin's original reciprocity law.

When $\mathfrak{m} = 0$, then this map is the inverse of the map given by content. However, in general, it is not simply (the inverse of) the prime-to- S content map, even for ideles whose content is prime to S . According to Fröhlich, this is the “*fundamental mistake of class field theory*”.

Proof sketch. Let $J_K(S) \subseteq J_K$ be given by

$$J_K(S) = \prod_{v \notin S \cup \Sigma_{K,\infty}} K_v^\times.$$

Here we do have the inverse of the content map

$$\begin{aligned} c^{-1} : J_K(S) &\rightarrow I_S \\ (x_v) &\mapsto \prod \mathfrak{p}_v^{-v(x_v)} \end{aligned}$$

We want to extend it to an isomorphism. Observe that

$$J_K(S) \cap U_{\mathfrak{m}} = \prod_{v \notin S \cup \Sigma_{K, \infty}} \mathcal{O}_v^\times,$$

which is precisely the kernel of the map c^{-1} . So c^{-1} extends uniquely to a homomorphism

$$\frac{J_K(S)U_{\mathfrak{m}}}{U_{\mathfrak{m}}} \cong \frac{J_K(S)}{J_K(S) \cap U_{\mathfrak{m}}} \rightarrow I_S.$$

We then use that $K^\times J_K(S)U_{\mathfrak{m}} = J_K$ (weak approximation), and

$$K^\times \cap V_{\mathfrak{m}} = \{x \equiv 1 \pmod{\mathfrak{m}}, x \in K^*\},$$

where

$$V_{\mathfrak{m}} = J_K(S)U_{\mathfrak{m}} = \{(x_v) \in J_K \mid \text{for all } v \text{ with } m_v > 0, x_v \in U_{\mathfrak{m}}\}. \quad \square$$

2 Hecke characters and abelian L -functions

Proposition. Let G be a profinite group, and $\rho : G \rightarrow \mathrm{GL}_n(\mathbb{C})$ continuous. Then $\ker \rho$ is open.

Of course, the kernel is always closed.

Proof. It suffices to show that $\ker \rho$ contains an open subgroup. We use the fact that $\mathrm{GL}_n(\mathbb{C})$ has “no small subgroups”, i.e. there is an open neighbourhood U of $1 \in \mathrm{GL}_n(\mathbb{C})$ such that U contains no non-trivial subgroup of $\mathrm{GL}_n(\mathbb{C})$ (exercise!). For example, if $n = 1$, then we can take U to be the right half plane.

Then for such U , we know $\rho^{-1}(U)$ is open. So it contains an open subgroup V . Then $\rho(V)$ is a subgroup of $\mathrm{GL}_n(\mathbb{C})$ contained in U , hence is trivial. So $V \subseteq \ker(\rho)$. \square

While the multiplicative group of a local field is not profinite, it is close enough, and we similarly have

Exercise. Let F be a local field. Then any continuous homomorphism $F^\times \rightarrow \mathbb{C}^\times$ has an open kernel, i.e. $\chi(1 + \mathfrak{p}_F^N) = 1$ for some $N \gg 0$.

We are ultimately interested in (continuous) representations of the idele group $\chi : J_K \rightarrow \mathbb{C}^\times$. While J_K is not profinite, it contains the group $\hat{\mathcal{O}}_K^\times$ which is profinite. Thus, $\ker \chi$ contains an open subgroup of $\hat{\mathcal{O}}_K^\times$.

In particular, if also $\chi(K_\infty^{\times,0}) = 1$, then χ has finite image.

We say χ is unramified if $\chi|_{\mathcal{O}_F^\times} = 1$.

Exercise. χ is unramified iff $\chi(x) = |x|_F^s$ for some $s \in \mathbb{C}$.

If $F \cong \mathbb{R}$, we say $\chi : F^\times \rightarrow \mathbb{C}^\times$ is unramified if $\chi(-1) = 1$ (so $\chi(x) = |x|^s$ for some s).

Going back to global fields, we have

Proposition. The set of continuous homomorphisms $\chi : J_K = \prod'_v K_v^\times \rightarrow \mathbb{C}^\times$ bijects with the set of all families $(\chi_v)_{v \in \Sigma_K}$, $\chi_v : K_v^\times \rightarrow \mathbb{C}^\times$ such that χ_v is unramified for almost all (i.e. all but finitely many) v , with the bijection given by $\chi \mapsto (\chi_v)$, $\chi_v = \chi|_{K_v^\times}$.

Proof. Given χ , we know $\chi(\hat{\mathcal{O}}_K^\times)$ is finite. So $\chi(\mathcal{O}_v^\times) = 1$ for almost all finite v . So we have a map from the LHS to the RHS. As

$$\bigoplus_{v \notin \Sigma_{K,\infty}} \mathcal{O}_v^\times \subseteq \prod_{v \nmid \infty} \mathcal{O}_v^\times$$

is dense, we know $\bigoplus_v K_v^\times \subseteq J_K$ is dense, and so this map is an inclusion.

Finally, let $(\chi_v)_v$ be an element of the RHS. So by the hypothesis,

$$\prod_{v \nmid \infty} (\ker \chi_v \cap \mathcal{O}_v^\times) \subseteq \hat{K}^\times$$

is open. So the map $\chi^\infty : \hat{K}^\times \rightarrow \mathbb{C}^\times$ given by $(x_v)_{v \nmid \infty} \mapsto \prod \chi_v(x_v)$ is well-defined. So we define

$$\chi = \chi_\infty \chi^\infty, \quad \chi_\infty = \prod_{v \mid \infty} \chi_v : K_\infty^\times \rightarrow \mathbb{C}^\times. \quad \square$$

Definition (Hecke character). A Hecke character is a continuous (not necessarily unitary) homomorphism

$$\chi : J_K/K^\times \rightarrow \mathbb{C}^\times.$$

These are also known as *quasi-characters* in some places, where character means unitary. However, we shall adopt the convention that characters need not be unitary.

By what we have just said, we can write $\chi = \chi_\infty \chi^\infty$, where $\chi_\infty : K_\infty^\times \rightarrow \mathbb{C}^\times$, and $\chi^\infty : \hat{K}^\times \rightarrow \mathbb{C}^\times$.

Example. χ has finite order iff $\chi(C_K^0) = 1$ iff $\chi_\infty(K_\infty^{\times,0}) = 1$, iff $\chi_\infty^2 = 1$, iff χ factors through $\text{Cl}_m(K)$ for some modulus m . We say χ is a *ray class character*.

Example. The idele norm $\| \cdot \|_{\mathbb{A}} : C_K \rightarrow \mathbb{R}_{>0}^\times$ is a character not of finite order. In the case $K = \mathbb{Q}$, we have $C_{\mathbb{Q}} = \mathbb{R}_{>0}^\times \times \hat{\mathbb{Z}}^\times$. The idele norm is then the first projection onto $\mathbb{R}_{>0}^\times$. So the Hecke characters of $C_{\mathbb{Q}}$ are all of the form

$$\chi(x) = |x|_{\mathbb{A}}^s \cdot \chi'(x),$$

where χ' has finite order, i.e. is a Dirichlet character

$$C_{\mathbb{Q}} \rightarrow \hat{\mathbb{Z}}^\times \rightarrow (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$$

for some N .

For other fields, there can be more interesting Hecke characters.

For a general field K , we have finite order characters as we just saw. They correspond to characters on I_S which are trivial on P_m . In fact, we can describe all Hecke characters in terms of ideals.

2.1 Ideal-theoretic description of any Hecke character

Choose a modulus m such that χ^∞ is trivial on $\hat{K}^\times \cap U_m$. Let S be the set of finite v such that m_v is positive. Define a homomorphism $\Theta : I_S \rightarrow \mathbb{C}^\times$ as follows: if $v \notin S$, so that $\chi_v(\mathcal{O}_v^\times) = 1$, send

$$\mathfrak{p}_v \mapsto \chi_v(\pi_v)^{-1}.$$

If this were a Hecke character of finite order, then this would be trivial on P_m . Let $x \in K^\times$ with $x \equiv 1 \pmod{m}$. Then for all $v \in S$, we have $\chi_v(x) = 1$. So

$$1 = \chi(x) = \chi_\infty(x) \prod_{v \notin S \text{ finite}} \chi_v(x) = \chi_\infty(x) \prod_{\text{finite } v \notin S} \chi_v(\pi_v)^{v(x)}.$$

So by definition of Θ , we have

$$\chi_\infty(x) = \Theta(x).$$

In other words, we get a map

$$\begin{aligned} \text{Hom}_{cts}(C_K, \mathbb{C}^\times) &\rightarrow \{(\Theta, m) : \Theta : I_S \rightarrow \mathbb{C}^\times, x \equiv 1 \pmod{m} \Rightarrow \Theta(x) \\ &= \chi_\infty(x) \text{ for some } \chi_\infty : K_\infty^\times \rightarrow \mathbb{C}^\times\} / \sim \end{aligned}$$

where we quotient out by what happens when we change modulus.

It is not hard to see that this is in fact a bijection. This is Hecke's original definition of his Größencharakter.

What do general Hecke characters have to do with Galois groups?

Example. Let $K = \mathbb{Q}(i) \subseteq \mathbb{C}$. Let

$$\mathfrak{m} = 3(v_2),$$

where v_2 is a place over 2, corresponding to $(1+i)\mathcal{O}_K$. What is special about this modulus is that we in fact have

$$\mathcal{O}_{v_2}^\times = (1 + (1+i)^3\mathcal{O}_v) \times \mu_4.$$

Of course, $\text{Cl}(K) = 1$, so

$$C_K = \frac{\mathbb{C}^\times \times \hat{\mathcal{O}}_K^\times}{\mu_4 = \{\pm 1, \pm i\}}.$$

To write down characters of C_K , observe that we have a surjection

$$\hat{\mathcal{O}}_K^\times \twoheadrightarrow \mathcal{O}_{v_2}^\times = (1 + (1+i)^3\mathcal{O}_v) \times \mu_4$$

since

$$\left(\frac{\mathbb{Z}[i]}{(2+2i)} \right)^\times = \{\pm 1, \pm i\}.$$

Cancelling the μ_4 , there is a unique $\chi : C_K \rightarrow \mathbb{C}^\times$ that is trivial on

$$\prod_{v \notin \{v_2, \infty\}} \mathcal{O}_v^\times \times (1 + (1+i)^3\mathcal{O}_{v_2}),$$

such that $\chi_\infty(z) = z$. This is a Hecke character not of the form we have had before.

We can say what this is in ideal-theoretic terms. If $\mathfrak{p} \neq (1+i)$ is a prime ideal of K , then $\mathfrak{p} = (\pi)$ for $\pi \equiv 1 \pmod{(2+2i)}$ for a unique $\pi = \pi_{\mathfrak{p}}$. The associated $\Theta : I_{\{v_2\}} \rightarrow \mathbb{C}^\times$ is just given by $\Theta(\mathfrak{p}) = \pi_{\mathfrak{p}}$.

This is an example of an algebraic Hecke character.

Definition (Algebraic homomorphism). A homomorphism $K^\times \rightarrow \mathbb{C}^\times$ is *algebraic* if there exists integers $n(\sigma)$ (for all $\sigma : K \hookrightarrow \mathbb{C}$) such that

$$\varphi(x) = \prod \sigma(x)^{n(\sigma)}.$$

The first thing to note is that if φ is algebraic, then $\varphi(K^\times)$ is contained in the Galois closure of K in \mathbb{C} . In particular, it takes values in the number field. Another equivalent definition is that it is algebraic in the sense of algebraic geometry, i.e. if $K = \bigoplus \mathbb{Q}e_i$ for $i = 1, \dots, n$ as a vector space, then we can view K as the \mathbb{Q} -points of an n -dimensional affine group scheme. We can then define $R_{K/\mathbb{Q}}\mathbb{G}_m \subseteq \mathbb{A}$ to be the set on which X is invertible, and then an algebraic Hecke character is a homomorphism of algebraic groups $(T_K)/\mathbb{C} \rightarrow \mathbb{G}_m/\mathbb{C}$, where $T_K = \text{Res}_{K/\mathbb{Q}}(\mathbb{G}_m)$.

If we have a real place v of K , then this corresponds to a real embedding $\sigma_v : K \rightarrow K_v \cong \mathbb{R}$, and if v is a complex place, we have a pair of embedding $\sigma_v, \bar{\sigma}_v : K \hookrightarrow K_v \simeq \mathbb{C}$, picking one of the pair to be σ_v . So φ extends to a homomorphism

$$\varphi : K_\infty^\times \rightarrow \mathbb{C}^\times$$

given by

$$\varphi(x_v) = \prod_{v \text{ real}} x_v^{n(\sigma_v)} \prod_{v \text{ complex}} x_v^{n(\sigma_v)} \bar{x}_v^{n(\bar{\sigma}_v)}$$

Definition (Algebraic Hecke character). A Hecke character $\chi = \chi_\infty \chi^\infty : J_K/K^\times \rightarrow \mathbb{C}^\times$ is *algebraic* if there exists an algebraic homomorphism $\varphi : K^\times \rightarrow \mathbb{C}^\times$ such that $\varphi(x) = \chi_\infty(x)$ for all $x \in K_\infty^{\times,0}$, i.e. $\chi_\infty = \varphi \prod_{v \text{ real}} \text{sgn}_v^{e_v}$ for $e_v \in \{0,1\}$.

We say φ (or the tuple $(n(\sigma))_\sigma$) is the *infinite type* of χ .

Example. The adelic norm $|\cdot|_\mathbb{A} : J_K \rightarrow \mathbb{C}^\times$ has

$$\chi_\infty = \prod_v |\cdot|_v,$$

and so χ is algebraic, and the associated φ is just $N_{K/\mathbb{Q}} : K^\times \rightarrow \mathbb{Q}^\times \subseteq \mathbb{C}^\times$, with $(n_\sigma) = (1, \dots, 1)$.

Exercise. Let $K = \mathbb{Q}(i)$, and χ from the previous example, whose associated character of ideals was $\Theta : \mathfrak{p} \mapsto \pi_{\mathfrak{p}}$, where $\pi_{\mathfrak{p}} \equiv 1 \pmod{(2+2i)}$. The infinity type is the inclusion $K^\times \hookrightarrow \mathbb{C}^\times$, i.e. it has type $(1,0)$.

Observe that the image of an algebraic homomorphism $\varphi : K^\times \rightarrow \mathbb{C}^\times$ lies in the normal closure of K . More generally,

Proposition. If χ is an algebraic Hecke character, then χ^∞ takes values in some number field. We write $E = E(\chi)$ for the smallest such field.

Of course, we cannot expect χ to take algebraic values, since J_K contains copies of \mathbb{R} and \mathbb{C} .

Proof. Observe that $\chi^\infty(\hat{\mathcal{O}}_K^\times)$ is finite subgroup, so is μ_n for some n . Let $x \in K^\times$, totally positive. Then

$$\chi^\infty(x) = \chi_\infty(x)^{-1} = \varphi(x)^{-1} \in K^{cl},$$

where K^{cl} is the Galois closure. Then since $K_{>0}^\times \times \hat{\mathcal{O}}_K^\times \rightarrow \hat{K}^\times$ has finite cokernel (by the finiteness of the class group), so

$$\chi^\infty(\hat{K}^\times) = \prod_{i=1}^d z_i \chi^\infty(K_{>0}^\times \hat{\mathcal{O}}_K^\times),$$

where $z_i^d \in \chi^\infty(K_{>0}^\times \hat{\mathcal{O}}_K^\times)$, and is therefore contained inside a finite extension of the image of $K_{>0}^\times \times \hat{\mathcal{O}}_K^\times$. □

Hecke characters of finite order (i.e. algebraic Hecke characters with infinity type $(0, \dots, 0)$) are in bijection with continuous homomorphisms $\Gamma_K \rightarrow \mathbb{C}^\times$, necessarily of finite order. What we show now is how to associate to a general algebraic Hecke character χ a continuous homomorphism $\psi_\ell : \Gamma_K \rightarrow E(\chi)_\lambda^\times \supseteq \mathbb{Q}_\ell^\times$, where λ is a place of $E(X)$ over ℓ . This is continuous for the ℓ -adic topology on E_λ . In general, this will not be of finite order. Thus, algebraic Hecke characters correspond to ℓ -adic Galois representations.

The construction works as follows: since $\chi^\infty(x) = \varphi(x)^{-1}$, we can restrict the infinity type φ to a homomorphism $\varphi : K^\times \rightarrow E^\times$. We define $\tilde{\chi} : J_K \rightarrow E^\times$ as follows: if $x = x_\infty x^\infty \in K_\infty^\times K^{\infty,\times} \in J_K$, then we set

$$\tilde{\chi}(x) = \chi(x) \varphi(x_\infty)^{-1}.$$

Notice that this is not trivial on K^\times in general. Then $\tilde{\chi}_\infty$ takes values in $\{\pm 1\}$. Thus, $\tilde{\chi}$ takes values in E^\times . Thus, we know that $\tilde{\chi}$ has open kernel, i.e. it is continuous for the discrete topology on E^\times , and $\tilde{\chi}|_{K^\times} = \varphi^{-1}$.

Conversely, if $\tilde{\chi} : K^\times \rightarrow E^\times$ is a continuous homomorphism for the discrete topology on E^\times , and $\tilde{\chi}|_{K^\times}$ is an algebraic homomorphism, then it comes from an algebraic Hecke character in this way.

Let λ be a finite place of E over ℓ , a rational prime. Recall that $\varphi : K^\times \rightarrow E^\times$ is an algebraic homomorphism, i.e.

$$\varphi\left(\sum x_i e_i\right) = f(\mathbf{x}), \quad f \in E(X_1, \dots, X_n).$$

We can extend this to $K_\ell^\times = (K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^\times = \prod_{v|\ell} K_v^\times$ to get a homomorphism

$$\varphi_\lambda : K_\ell^\times \rightarrow E_\lambda^\times$$

This is still algebraic, so it is certainly continuous for the ℓ -adic topology.

Now consider the character $\psi_\lambda : J_K \rightarrow E_\lambda^\times$, where now

$$\psi_\lambda((x_v)) = \tilde{\chi}(x) \varphi_\lambda((x_v)_{v|\ell}).$$

This is then continuous for the ℓ -adic topology on E_λ^\times , and moreover, we see that $\psi_\lambda(K^\times) = \{1\}$ as $\tilde{\chi}|_{K^\times} = \varphi^{-1}$ while $\varphi_\lambda|_{K^\times} = \varphi$. Since $\tilde{\chi}(K_\infty^{\times,0}) = \{1\}$, we know that ψ_λ is in fact defined on $C_K/C_K^0 \cong \Gamma_K^{ab}$.

Obviously, ψ_λ determines $\tilde{\chi}$ and hence χ .

Fact. An ℓ -adic character $\psi : C_K/C_K^0 \rightarrow E_\lambda^\times$ comes from an algebraic Hecke character in this way if and only if the associated Galois representation is *Hodge-Tate*, which is a condition on the restriction to the decomposition groups $\text{Gal}(\bar{K}_v/K_v)$ for the primes $v \mid \ell$.

Example. Let $K = \mathbb{Q}$ and $\chi = |\cdot|_{\mathbb{A}}$, then

$$\tilde{\chi} = \text{sgn}(x_\infty) \prod_p |x_p|_p.$$

So

$$\psi_\ell((x_v)) = \text{sgn}(x_\infty) \prod_{p \neq \ell} |x_p|_p \cdot |x_\ell|_\ell \cdot x_\ell.$$

Note that $|x_\ell|_\ell x_\ell \in \mathbb{Z}_\ell^\times$. We have

$$C_{\mathbb{Q}}/C_{\mathbb{Q}}^0 \cong \hat{\mathbb{Z}}^\times.$$

Under this isomorphism, the map $\hat{\mathbb{Z}}^\times \mathbb{Q}_\ell^\times$ is just the projection onto \mathbb{Z}_ℓ^\times followed by the inclusion, and by class field theory, $\psi_\ell : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathbb{Z}_\ell^\times$ is just the cyclotomic character of the field $\mathbb{Q}(\{\zeta_{\ell^n}\})$,

$$\sigma(\zeta_{\ell^n}) = \zeta_{\ell^n}^{\psi_\ell(\sigma) \bmod \ell^n}.$$

Example. Consider the elliptic curve $y^2 = x^3 - x$ with complex multiplication over $\mathbb{Q}(i)$. In other words, $\text{End}(E/\mathbb{Q}(i)) = \mathbb{Z}[i]$, where we let i act by

$$i \cdot (x, y) \mapsto (-x, iy).$$

Its Tate module

$$T_\ell E = \lim \mathbb{E}[\ell^n]$$

is a $\mathbb{Z}_\ell[i]$ -module. If $\lambda \mid \ell$, then we define

$$V_\lambda E = T_\ell E \otimes_{\mathbb{Z}_\ell[i]} K_\lambda.$$

Then Γ_K act by $\Gamma_K : \text{Aut}_{K_\lambda} V_\lambda E = K_\lambda^\times$.

We now want to study the infinity types of an algebraic Hecke character.

Lemma. Let K be a number field, $\varphi : K^\times \rightarrow E^\times \subseteq \mathbb{C}^\times$ be an algebraic homomorphism, and suppose E/\mathbb{Q} is Galois. Then φ factors as

$$K^\times \xrightarrow{\text{norm}} (K \cap E)^\times \xrightarrow{\phi'} E^\times.$$

Note that since E is Galois, the intersection $K \cap E$ makes perfect sense.

Proof. By definition, we can write

$$\varphi(x) = \prod_{\sigma: K \hookrightarrow \mathbb{C}} \sigma(x)^{n(\sigma)}.$$

Then since $\varphi(x) \in E$, for all $x \in K^\times$ and $\tau \in \Gamma_E$, we have

$$\prod \tau \sigma(x)^{n(\sigma)} = \prod \sigma(x)^{n(\sigma)}.$$

In other words, we have

$$\prod_{\sigma} \sigma(x)^{n(\tau^{-1}\sigma)} = \prod_{\sigma} \sigma(x)^{n(\sigma)}.$$

Since the homomorphisms σ are independent, we must have $n(\tau\sigma) = n(\sigma)$ for all embeddings $\sigma : K \hookrightarrow \bar{\mathbb{Q}}$ and $\tau \in \Gamma_E$. This implies the theorem. \square

Recall that if \mathfrak{m} is a modulus, then we defined open subgroups $U_{\mathfrak{m}} \subseteq J_K$, consisting of the elements (x_v) such that if a real $v \mid \mathfrak{m}$, then $x_v > 0$, and if $v \mid \mathfrak{m}$ for a finite v , then $v(x_v - 1) \geq m_v$. We can write this as

$$U_{\mathfrak{m}} = U_{\mathfrak{m},\infty} \times U_{\mathfrak{m}}^\infty.$$

Proposition. Let $\varphi : K^\times \rightarrow \mathbb{C}^\times$ be an algebraic homomorphism. Then φ is the infinity type of an algebraic Hecke character χ iff $\varphi(\mathcal{O}_K^\times)$ is finite.

Proof. To prove the (\Rightarrow) direction, suppose $\chi = \chi_\infty \chi^\infty$ is an algebraic Hecke character with infinity type φ . then $\chi^\infty(U_{\mathfrak{m}}^\infty) = 1$ for some \mathfrak{m} . Let $E_{\mathfrak{m}} = K^\times \cap U_{\mathfrak{m}} \subseteq \mathcal{O}_K^\times$, a subgroup of finite index. As $\chi^\infty(E_{\mathfrak{m}}) = 1 = \chi(E_{\mathfrak{m}})$, we know $\chi_\infty(E_{\mathfrak{m}}) = 1$. So $\varphi(\mathcal{O}_K^\times)$ is finite.

To prove (\Leftarrow) , given φ with $\varphi(\mathcal{O}_K^\times)$ finite, we can find some \mathfrak{m} such that $\varphi(E_{\mathfrak{m}}) = 1$. Then $(\varphi, 1) : K_\infty^\times \times U_{\mathfrak{m}}^\infty \rightarrow \mathbb{C}^\times$ is trivial on $E_{\mathfrak{m}}$. So we can extend this to a homomorphism

$$\frac{K_\infty^\times U_{\mathfrak{m}} K^\times}{K^\times} \cong \frac{K_\infty^\times U_{\mathfrak{m}}}{E_{\mathfrak{m}}} \rightarrow \mathbb{C}^\times,$$

since $E_{\mathfrak{m}} = K^\times \cap U_{\mathfrak{m}}$. But the LHS is a finite index subgroup of C_K . So the map extends to some χ . \square

Here are some non-standard terminology:

Definition (Serre type). A homomorphism $\varphi : K^\times \rightarrow \mathbb{C}^\times$ is of *Serre type* if it is algebraic and $\varphi(\mathcal{O}_K^\times)$ is finite.

These are precisely homomorphisms that occur as infinity types of algebraic Hecke characters.

Note that the unit theorem implies that

$$\mathcal{O}_K^\times \hookrightarrow K_\infty^{\times,1} = \{x \in K_\infty^\times : |x|_{\mathbb{A}} = 1\}$$

has compact cokernel. If $\varphi(\mathcal{O}_K^\times)$ is finite, then $\varphi(K_\infty^{\times,1})$ is compact. So it maps into $U(1)$.

Example. Suppose K is totally real. Then

$$K_\infty^\times = (\mathbb{R}^\times)^{\{\sigma:K \hookrightarrow \mathbb{R}\}}.$$

Then we have

$$K_\infty^{\times,1} = \{(x_\sigma) : \prod x_\sigma = \pm 1\}.$$

Then $\varphi((x_\sigma)) = \prod x_\sigma^{n(\sigma)}$, so $|\varphi(K_\infty^{\times,1})| = 1$. In other words, all the n_σ are equal. Thus, φ is just a power of the norm map.

Thus, algebraic Hecke characters are all of the form

$$|\cdot|_{\mathbb{A}}^m \cdot (\text{finite order character}).$$

Another class of examples comes from CM fields.

Definition (CM field). K is a CM field if K is a totally complex quadratic extension of a totally real number field K^+ .

This CM refers to *complex multiplication*.

This is a rather restrictive condition, since this implies $\text{Gal}(K/K^+) = \{1, c\} = \text{Gal}(K_w/K_v^+)$ for every $w \mid v \mid \infty$. So c is equal to complex conjugation for *every* embedding $K \hookrightarrow \mathbb{C}$.

From this, it is easy to see that CM fields are all contained in $\mathbb{Q}^{\text{CM}} \subseteq \bar{\mathbb{Q}} \subseteq \mathbb{C}$, given by the fixed field of the subgroup

$$\langle c\sigma\sigma^{-1} : \sigma \in \Gamma_{\mathbb{Q}} \rangle \subseteq \Gamma_{\mathbb{Q}}.$$

For example, we see that the compositum of two CM fields is another CM field.

Exercise. Let K be a totally complex S_3 -extension over \mathbb{Q} . Then K is not CM, but the quadratic subfields is complex and is equal to $K \cap \mathbb{Q}^{\text{CM}}$.

Example. Let K be a CM field of degree $2r$. Then Dirichlet's unit theorem tells us

$$\text{rk } \mathcal{O}_K^\times = r - 1 = \text{rk } \mathcal{O}_{K^+}^\times.$$

So \mathcal{O}_K^\times is a finite index subgroup of $\mathcal{O}_{K^+}^\times$. So $\varphi : K^\times \rightarrow \mathbb{C}^\times$ is of Serre type iff it is algebraic and its restriction to $K^{+, \times}$ is of Serre type. In other words, we need $n(\sigma) + n(\bar{\sigma})$ to be independent of σ .

Theorem. Suppose K is arbitrary, and $\varphi : K^\times \rightarrow E^\times \subseteq \mathbb{C}^\times$ is algebraic, and we assume E/\mathbb{Q} is Galois, containing the normal closure of K . Thus, we can write

$$\varphi(x) = \prod_{\sigma: K \hookrightarrow E} \sigma(x)^{n(\sigma)}.$$

Then the following are equivalent:

- (i) φ is of Serre type.
- (ii) $\varphi = \psi \circ N_{K/F}$, where F is the maximal CM subfield and ψ is of Serre type.
- (iii) For all $c' \in \text{Gal}(E/\mathbb{Q})$ conjugate to complex conjugation c , the map $\sigma \mapsto n(\sigma) + n(c'\sigma)$ is constant.
- (iv) (in the case $K \subseteq \mathbb{C}$ and K/\mathbb{Q} is Galois with Galois group G) Let $\lambda = \sum n(\sigma)\sigma \in \mathbb{Z}[G]$. Then for all $\tau \in G$, we have

$$(\tau - 1)(c + 1)\lambda = 0 = (c + 1)(\tau - 1)\lambda.$$

Note that in (iii), the constant is necessarily

$$\frac{2}{[K : \mathbb{Q}]} \sum_{\sigma} n(\sigma).$$

So in particular, it is independent of c' .

Proof.

- (iii) \Leftrightarrow (iv): This is just some formal symbol manipulation.
- (ii) \Rightarrow (i): The norm takes units to units.
- (i) \Rightarrow (iii): By the previous lecture, we know that if φ is of Serre type, then

$$|\varphi(K_\infty^{\times,1})| = 1.$$

Now if $(x_v) \in K_\infty^\times$, we have

$$|\varphi((x_v))| = \prod_{\text{real } v} |x_v|^{n(\sigma_v)} \prod_{\text{complex } v} |x_v|^{n(\sigma_v) + n(\bar{\sigma}_v)} = \prod_v |x_v|^{\frac{1}{2}(n(\sigma_v) + n(\bar{\sigma}_v))}.$$

Here the modulus without the subscript is the usual modulus. Then $|\varphi(K_\infty^{\times,1})| = 1$ implies $n(\sigma_v) + n(\bar{\sigma}_v)$ is constant. In other words, $n(\sigma) + n(c\sigma) = m$ is constant.

But if $\tau \in \text{Gal}(E/\mathbb{Q})$, and $\varphi' = \tau \circ \varphi$, $n'(\sigma) = n(\tau^{-1}\sigma)$, then this is also of Serre type. So

$$m = n'(\sigma) + n'(c\sigma) = n(\tau^{-1}\sigma) + n(\tau^{-1}c\sigma) = n(\tau^{-1}\sigma) + n((\tau^{-1}c\tau)\tau^{-1}\sigma).$$

- (iii) \Rightarrow (ii): Suppose $n(\sigma) + n(c'\sigma) = m$ for all σ and all $c' = \tau c \tau^{-1}$. Then we must have

$$n(c'\sigma) = n(c\sigma)$$

for all σ . So

$$n(\sigma) = n(c\tau c\tau^{-1}\sigma)$$

So n is invariant under $H = [c, \text{Gal}(E/\mathbb{Q})] \leq \text{Gal}(E/\mathbb{Q})$, noting that c has order 2. So φ takes values in the fixed field $E^H = E \cap \mathbb{Q}^{\text{CM}}$. By the proposition last time, this implies φ factors through $N_{K/F}$, where $F = E^H \cap K = K \cap \mathbb{Q}^{\text{CM}}$. \square

Recall that a homomorphism $\varphi : K^\times \rightarrow \mathbb{C}^\times$ is algebraic iff it is a character of the commutative algebraic group $T_K = R_{K/\mathbb{Q}}\mathbb{G}_m$, so that $T_K(\mathbb{Q}) = K^\times$, i.e. there is an algebraic character $\varphi' : T_K/\mathbb{C} \rightarrow \mathbb{G}_m/\mathbb{C}$ such that φ' restricted to $T_K(\mathbb{Q})$ is φ .

Then φ is of Serre type iff φ is a character of ${}^K S^0 = T_K/\mathcal{E}_K^0$, where \mathcal{E}_K is the Zariski closure of \mathcal{O}_K^\times in T_K and \mathcal{E}_K^0 is the identity component, which is the same as the Zariski closure of $\Delta \subseteq \mathcal{O}_K^\times$, where Δ is a sufficiently small finite-index subgroup.

The group ${}^K S^0$ is called the *connected Serre group*. We have a commutative diagram (with exact rows)

$$\begin{array}{ccccccc} 1 & \longrightarrow & K^\times & \longrightarrow & J_K & \longrightarrow & J_K/k^\times & 1 \\ & & \downarrow & & \downarrow & & \downarrow \pi_0 & \\ 1 & \longrightarrow & {}^K S^0 & \longrightarrow & {}^K S & \longrightarrow & \Gamma_K^{ab} & 1 \end{array}$$

This ${}^K S$ is a projective limit of algebraic groups over \mathbb{Q} . We have

$$\text{Hom}({}^K S, \mathbb{C}^\times) = \text{Hom}({}^K S, \mathbb{G}_m/\mathbb{C}) = \{\text{algebraic Hecke characters of } K\}$$

The infinity type is just the restriction to ${}^K S^0$.

Langlands created a larger group, the *Taniyama group*, an extension of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ by ${}^K S^0$, which is useful for abelian varieties with CM and conjugations and Shimura varieties.

3 Abelian L -functions

We are now going to define L -functions for Hecke characters. Recall that L -functions have a complex parameter s , and some other thing. However, given any s and Hecke character, we can multiply by $|\cdot|_{\mathbb{A}}^s$ to get a new Hecke character. So we don't have to include an s in the definition.

Let $\chi : C - K \rightarrow \mathbb{C}^\times$ be any Hecke character. For any $v \in \Sigma_K$, we define L -factors $L(\chi_v)$ as follows:

- If v is non-Archimedean and χ_v unramified, i.e. $\chi_v|_{\mathcal{O}_{K_v}^\times} = 1$, we set

$$L(\chi_v) = \frac{1}{1 - \chi_v(\pi_v)}.$$

- If v is non-Archimedean and χ_v is ramified, then we set

$$L(\chi_v) = 1.$$

- If v is a real place, if

$$\chi_v(x) = x^{-N}|x|_v^s,$$

where $N = 0, 1$, then

$$L(\chi_v) = \Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2).$$

- If v is complex, if

$$\chi_v(x) = \sigma(x)^{-N}|x|_v^s,$$

where $\sigma \in \text{Isom}(K_v, \mathbb{C})$ and $N \geq 0$, then

$$L(\chi_v) = \Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$$

We then define

$$L(\chi, s) = L(\chi_v \cdot |\cdot|_v^s).$$

So for finite unramified v , we have

$$L(\chi_v, s) = \frac{1}{1 - \chi_v(\pi_v)q_v^{-s}},$$

where $q_v = |\mathcal{O}_{K_v}/(\pi_v)|$.

Recall that the kernel of the idelic norm $|\cdot|_{\mathbb{A}} : C_K \rightarrow \mathbb{R}_{>0}^\times$ is compact. It is then not hard to see that for every χ , there is some $t \in \mathbb{R}$ such that $\chi \cdot |\cdot|_{\mathbb{A}}^t$ is unitary. In particular,

$$\Lambda(\chi, s) = \prod_v L(\chi_v, s)$$

converges absolutely on some right half-plane. Observe that

$$\Lambda(\chi| \cdot |_{\mathbb{A}}^t, s) = \Lambda(\chi, t + s).$$

Theorem (Hecke–Tate).

- (i) $\Lambda(\chi, s)$ has a meromorphic continuation to \mathbb{C} , entire unless $\chi = |\cdot|_{\mathbb{A}}^t$ for some $t \in \mathbb{C}$, in which case there are simple poles at $s = 1 - t, -t$.

(ii) There is some function, the *global ε -factor*,

$$\varepsilon(\chi, s) = AB^s$$

for some $A \in \mathbb{C}^\times$ and $B \in \mathbb{R}_{>0}$ such that

$$\Lambda(\chi, s) = \varepsilon(\chi, s)\Lambda(\chi^{-1}, 1-s).$$

(iii) There is a factorization

$$\varepsilon(\chi, s) = \prod_v \varepsilon_v(\chi_v, \mu_v, \psi_v, s),$$

where $\varepsilon_v = 1$ for almost all v , and ε_v depends only on χ_v and certain auxiliary data ψ_v, μ_v . These are the *local ε -factors*.

Traditionally, we write

$$L(\chi, s) = \prod_{\text{finite } v} L(\chi_v, s),$$

and then

$$\Lambda(\chi, s) = L(\chi, s)L_\infty(\chi, s).$$

However, Tate (and others, especially the automorphic people) use $L(\chi, s)$ for the product over all v .

At first, Hecke proved (i) and (ii) using global methods, using certain Θ functions. Later, Tate proved (i) to (iii) using local-global methods and especially Fourier analysis on K_v and \mathbb{A}_K . This generalizes considerably, e.g. to automorphic representations.

We can explain some ideas of Hecke's method. We have a decomposition

$$K_\infty = K \otimes \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{C}^n,$$

and this has a norm $\|\cdot\|$ induced by the Euclidean metric on \mathbb{R}^n . Let $\Delta \subseteq \mathcal{O}_{K,+}^\times$ be a subgroup of totally positive units of finite index, which is $\cong \mathbb{Z}^{r_1+r_2-1}$. This has an embedding $\Delta = K_\infty^{\times,1}$, which extends to a continuous homomorphism $\Delta \otimes \mathbb{R} \rightarrow K_\infty^{\times,1}$. The key fact is

Proposition. Let $x \in K^\times$. Pick some invariant measure du on $\Delta \otimes \mathbb{R}$. Then

$$\int_{\Delta \otimes \mathbb{R}} \frac{1}{\|ux\|^{2s}} du = \frac{\text{stuff}}{|N_{K/\mathbb{Q}}(x)|^{2s/n}},$$

where the stuff is some ratio of Γ factors and powers of π (and depends on s).

Exercise. Prove this when $K = \mathbb{Q}[\sqrt{d}]$ for $d > 0$. Then $\Delta = \langle \varepsilon \rangle$, and then

$$\begin{aligned} \text{LHS} &= \int_{-\infty}^{\infty} \frac{1}{|\varepsilon^t x + \varepsilon^{-t} x'|^{2s}} dt \\ \text{RHS} &= \frac{\text{stuff}}{|xx'|^s}. \end{aligned}$$

The consequence of this is that if $\mathfrak{a} \subseteq K$ is a fractional ideal, then

$$\begin{aligned} \sum_{0 \neq x \in \mathfrak{a} \bmod \Delta} \frac{1}{|N_{K/\mathbb{Q}}(x)|^s} &= \text{stuff} \cdot \sum_{0 \neq x \in \mathfrak{a} \bmod \Delta} \int_{\Delta \otimes \mathbb{R}} \frac{1}{\|ux\|^{ns}} du \\ &= \text{stuff} \cdot \int_{\Delta \otimes \mathbb{R}/\Delta} \left(\sum_{0 \neq x \in \mathfrak{a}} \frac{1}{\|ux\|^{ns}} \right) du \end{aligned}$$

The integrand has a name, and is called the *Epstein ζ -function* of the lattice $(\mathfrak{a}, \|u \cdot \|^2)$. By the Poisson summation formula, we get an analytic continuity and functional equation for the epsilon ζ function. On the other hand, taking linear combinations of the left gives $L(\chi, s)$ for $\chi : \text{Cl}(K) \rightarrow \mathbb{C}^\times$. For more general χ , we modify this with some extra factors. When the infinity type is non-trivial, this is actually quite subtle.

Note that if χ is unramified outside S and ramified at S , recall we had a homomorphism $\Theta : I_S \rightarrow \mathbb{C}^\times$ sending $\mathfrak{p}_v \mapsto \chi_v(\pi_v)^{-1}$. So

$$L(\chi, s) = \prod_{\text{finite } v \notin S} \left(\frac{1}{1 - \Theta(\mathfrak{p}_v)^{-1} (N\mathfrak{p}_v)^{-s}} \right) = \sum_{\mathfrak{a} \in \mathcal{O}_K \text{ prime to } S} \frac{\Theta(\mathfrak{a})^{-1}}{(N\mathfrak{a})^s}.$$

This was Hecke's original definition of the Hecke character.

If $K = \mathbb{Q}$ and $\chi : C_{\mathbb{Q}} \rightarrow \mathbb{C}^\times$ is of finite order, then it factors through $C_{\mathbb{Q}} \rightarrow C_{\mathbb{Q}}/C_{\mathbb{Q}}^0 \cong \hat{\mathbb{Z}}^\times \rightarrow (\mathbb{Z}/N\mathbb{Z})^\times$, and so χ is just some Dirichlet character $\varphi : (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$. The associated L -functions are just Dirichlet L -functions. Indeed, if $p \nmid N$, then

$$\chi_p(p) = \chi(1, \dots, 1, p, 1, \dots) = \chi(p^{-1}, \dots, p^{-1}, 1, p^{-1}, \dots) = \varphi(p \bmod N)^{-1}.$$

In other words, $L(\chi, s)$ is the Dirichlet L -series of φ^{-1} (assuming N is chosen so that χ ramifies exactly at $v \mid N$).

Tate's method uses local ε -factors $\varepsilon(\chi_v, \mu_v, \psi_v, s)$, where $\psi_v : K_v \rightarrow \text{U}(1)$ is a non-trivial additive character, e.g. for v finite,

$$K_V \xrightarrow{\text{tr}} \mathbb{Q}_p \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \cong \mathbb{Z}[v_p]/\mathbb{Z} \xrightarrow{e^{2\pi i x}} \mathbb{C}^\times,$$

which we needed because Fourier transforms take in additive measures, and μ_v is a Haar measure on K_v . The condition for (iii) to hold is

$$\prod \psi_v : \mathbb{A}_K \rightarrow \text{U}(1)$$

is well-defined and trivial on $K \subseteq \mathbb{A}_K$, and $\mu_{\mathbb{A}} = \prod \mu_v$ is a well-defined measure on \mathbb{A}_K , i.e. $\mu_v(\mathcal{O}_v) = 1$ for all v and

$$\int_{\mathbb{A}_K/K} \mu_{\mathbb{A}} = 1.$$

There exists explicit formulae for these ε_v 's. If χ_v is unramified, then it is just $A_v B_v^s$, and is usually 1; for ramified finite v , they are given by Gauss sums.

4 Non-abelian L-functions

Let K be a number field. Then we have a reciprocity isomorphism

$$\text{Art}_K : C_K/C_K^0 \xrightarrow{\sim} \Gamma_K^{\text{ab}}.$$

If $\chi : C - K \rightarrow C_K^0 \rightarrow \mathbb{C}^\times$ is a Hecke character of finite order, then we can view it as a map $\psi = \chi \circ \text{Art}_K^{-1} : \Gamma_K \rightarrow \mathbb{C}^\times$. Then

$$L(\chi, s) = \prod_{\text{finite } v \text{ unramified}} \frac{1}{1 - \chi_v(\pi_v)q_v^{-s}}^{-1} = \prod \frac{1}{1 - \psi(\text{Frob}_v)q_v^{-s}},$$

where $\text{Frob}_v \in \Gamma_{K_v}/I_{K_v}$ is the geometric Frobenius, using that $\psi(I_{K_v}) = 1$. Artin generalized this to arbitrary complex representations of Γ_K .

Let $\rho : \Gamma_K \rightarrow \text{GL}_n(\mathbb{C})$ be a representation. Define

$$L(\rho, s) = \prod_{\text{finite } v} L(\rho_v, s),$$

where ρ_v is the restriction to the decomposition group at v , and depends only on the isomorphism class of ρ . We first define these local factors for non-Archimedean fields:

Definition. Let F be local and non-Archimedean. Let $\rho : W_F \rightarrow \text{GL}_{\mathbb{C}}(V)$ be a representation. Then we define

$$L(\rho, s) = \det(1 - q^{-s}\rho(\text{Frob}_F)|_{V^{I_F}})^{-1},$$

where V^{I_F} is the invariants under I_F .

Note that for all this section, representations will be finite-dimensional and continuous for the complex topology (so in the case of W_F , we require $\ker \sigma$ to be open).

Proposition.

(i) If

$$0 \rightarrow (\rho', V') \rightarrow (\rho, V) \rightarrow (\rho'', V'') \rightarrow 0$$

is exact, then

$$L(\rho, s) = L(\rho', s) \cdot L(\rho'', s).$$

(ii) If E/F is finite separable, $\rho : W_E \rightarrow \text{GL}_{\mathbb{C}}(V)$ and $\sigma = \text{Ind}_{W_E}^{W_F} \rho : W_F \rightarrow \text{GL}_{\mathbb{C}}(U)$, then

$$L(\rho, s) = L(\sigma, s).$$

Proof.

(i) Since ρ has open kernel, we know $\rho(I_F)$ is *finite*. So

$$0 \rightarrow (V')^{I_F} \rightarrow V^{I_F} \rightarrow (V'')^{I_F} \rightarrow 0$$

is exact. Then the result follows from the multiplicativity of det.

(ii) We can write

$$U = \{\varphi : W_F \rightarrow V : \varphi(gx) = \rho(g)\varphi(x) \text{ for all } g \in W_E, x \in W_F\}.$$

where W_F acts by

$$\sigma(g)\varphi(x) = \varphi(xg).$$

Then we have

$$U^{I_F} = \{\varphi : W_F/I_F \rightarrow V : \dots\}.$$

Then whenever $\varphi \in U^{I_F}$ and $g \in I_E$, then

$$\sigma(g)\varphi(x) = \varphi(xg) = \varphi((xgx^{-1})x) = \varphi(x).$$

So in fact φ takes values in V^{I_E} . Therefore

$$U^{I_F} = \text{Ind}_{W_E/I_E}^{W_F/I_F} V^{I_E}.$$

Of course, $W_F/I_F \cong \mathbb{Z}$, which contains W_E/I_E as a subgroup. Moreover,

$$\text{Frob}_F^d = \text{Frob}_E,$$

where $d = [k_E : k_F]$. We note the following lemma:

Lemma. Let $G = \langle g \rangle \supseteq H = \langle h = g^d \rangle$, $\rho : H \rightarrow \text{GL}_{\mathbb{C}}(V)$ and $\sigma = \text{Ind}_H^G \rho$. Then

$$\det(1 - t^d \rho(h)) = \det(1 - t \sigma(g)).$$

Proof. Both sides are multiplicative for exact sequences of representations of H . So we can reduce to the case of $\dim V = 1$, where $\rho(h) = \lambda \in \mathbb{C}^\times$. We then check it explicitly. \square

To complete the proof of (ii), take $g = \text{Frob}_F$ and $t = q_F^{-s}$ so that $t^d = q_E^{-s}$. \square

For Archimedean F , we define $L(\rho, s)$ in such a way to ensure that (i) and (ii) hold, and if $\dim V = 1$, then

$$L(\rho, s) = L(\chi, s),$$

where if $\rho : W_F^{\text{ab}} \rightarrow \mathbb{C}^\times$, then χ is the corresponding character of F^\times under the Artin map.

If $F \simeq \mathbb{C}$, then this is rather easy, since every irreducible representation of $W_F \cong \mathbb{C}^\times$ is one-dimensional. We then just define for ρ 1-dimensional using $W_F^{\text{ab}} \cong F^\times$ and extend to all ρ by (i). The Jordan–Hölder theorem tells us this is well-defined.

If $F \simeq \mathbb{R}$, then recall that

$$W_{\mathbb{R}} = \langle \mathbb{C}^\times, s : s^2 = -1 \in \mathbb{C}^\times, szs^{-1} = \bar{z} \rangle.$$

Contained in here is $W_{\mathbb{R}}^{(1)} = \langle \text{U}(1), s \rangle$. Then

$$W_{\mathbb{R}} = W_{\mathbb{R}}^{(1)} \times \mathbb{R}_{>0}^\times.$$

It is then easy to see that the irreducible representations of $W_{\mathbb{R}}$ are

- (i) 1-dimensional $\rho_{W_{\mathbb{R}}}$; or
- (ii) 2-dimensional, $\sigma = \text{Ind}_{\mathbb{C}}^{W_{\mathbb{R}}} \rho$, where $\rho \neq \rho^s : \mathbb{C}^{\times} \rightarrow \mathbb{C}^{\times}$.

In the first case, we define

$$L(\rho, s) = L(\chi, s)$$

using the Artin map, and in the second case, we define

$$L(\sigma, s) = L(\rho, s)$$

using (ii).

To see that the properties are satisfied, note that (i) is true by construction, and there is only one case to check for (ii), which is if $\rho = \rho^s$, i.e.

$$\rho(z) = (z\bar{z})^t.$$

Then $\text{Ind}_{\mathbb{C}^{\times}}^{W_{\mathbb{R}}} \rho$ is reducible, and is a sum of characters of $W_{\mathbb{R}}^{\text{ab}} \cong \mathbb{R}^{\times}$, namely $x \mapsto |x|^t$ and $x \mapsto \text{sgn}(x)|x|^t = x^{-1}|x|^{t+1}$. Then (ii) follows from the identity

$$\Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1) = \Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s).$$

Now let K be global, and let $\rho : \Gamma_K \rightarrow \text{GL}_{\mathbb{C}}(V)$. For each $v \in \Sigma_K$, choose \bar{k} of \bar{K} over v . Let $\Gamma_v \cong \Gamma_{K_v}$ be the decomposition group at \bar{v} . These contain I_V , and we have the geometric Frobenius $\text{Frob}_v \in \Gamma_v/I_V$. We define $\rho_v = \rho|_{\Gamma_v}$, and then set

$$\begin{aligned} L(\rho, s) &= \prod_{v \nmid \infty} L(\rho_v, s) = \prod_{v \nmid \infty} \det(1 - q_v^{-s} \text{Frob}_v|_{V^{I_v}})^{-1} \\ \Lambda(\rho, s) &= LL_{\infty} \\ L_{\infty} &= \prod_{v | \infty} L(\rho_v, s). \end{aligned}$$

This is well-defined as the decomposition groups $\bar{v} | v$ are conjugate. If $\dim V = 1$, then $\rho = \chi \circ \text{Art}_K^{-1}$ for a finite-order Hecke character χ , and then

$$L(\rho, s) = L(\chi, s).$$

The facts we had for local factors extend to global statements

Proposition.

- (i) $L(\rho \oplus \rho', s) = L(\rho, s)L(\rho', s)$.
- (ii) If L/K is finite separable and $\rho : \Gamma_L \rightarrow \text{GL}_{\mathbb{C}}(V)$ and $\sigma = \text{Ind}_{\Gamma_L}^{\Gamma_K}(\rho)$, then

$$L(\rho, s) = L(\sigma, s).$$

The same are true for $\Lambda(\rho, s)$.

Proof. (i) is clear. For (ii), we saw that if $w \in \Sigma_L$ over $v \in \Sigma_K$ and consider the local extension L_w/K_v , then

$$L(\rho_w, s) = L(\text{Ind}_{\Gamma_{L_w}}^{\Gamma_{K_v}} \rho_w).$$

In the global world, we have to take care of the splitting of primes. This boils down to the fact that

$$\left(\mathrm{Ind}_{\Gamma_L}^{\Gamma_K} \rho\right)\Big|_{\Gamma_{K_v}} = \bigoplus_{w|v} \mathrm{Ind}_{\Gamma_{L_w}}^{\Gamma_{K_v}}(\rho|_{\Gamma_{L_w}}). \quad (*)$$

We fix a valuation \bar{v} of \bar{K} over v . Write $\Gamma_{\bar{v}/v}$ for the decomposition group in Γ_K . Write \bar{S} for the places of \bar{K} over v , and S the places of L over v .

The Galois group acts transitively on \bar{S} , and we have

$$\bar{S} \cong \Gamma_K / \Gamma_{\bar{v}/v}.$$

We then have

$$S \cong \Gamma_L \backslash \Gamma_K / \Gamma_{\bar{v}/v},$$

which is compatible with the obvious map $\bar{S} \rightarrow S$.

For $\bar{w} = g\bar{v}$, we have

$$\Gamma_{\bar{w}/v} = g\Gamma_{\bar{v}/v}g^{-1}.$$

Conjugating by g^{-1} , we can identify this with $\Gamma_{\bar{v}/v}$. Similarly, if $w = \bar{w}|_L$, then this contains

$$\Gamma_{\bar{w}/w} = g\Gamma_{\bar{v}/v}g^{-1} \cap \Gamma_L,$$

and we can identify this with $\Gamma_{\bar{v}/v} \cap g^{-1}\Gamma_Lg$.

There is a theorem, usually called Mackey's formula, which says if $H, K \subseteq G$ are two subgroups of finite index, and $\rho : H \rightarrow \mathrm{GL}_{\mathbb{C}}(V)$ is a representation of H . Then

$$\left(\mathrm{Ind}_H^G V\right)|_K \cong \bigoplus_{g \in H \backslash G/K} \mathrm{Ind}_{K \cap g^{-1}Hg}^K(g^{-1}V),$$

where $g^{-1}V$ is the $K \cap g^{-1}Hg$ -representation where $g^{-1}xg$ acts by $\rho(x)$. We then apply this to $G = \Gamma_K, H = \Gamma_L, K = \Gamma_{\bar{v}/v}$. \square

Example. If ρ is trivial, then

$$L(\rho, s) = \prod_v (1 - q_v^{-s})^{-1} = \sum_{\mathfrak{a} \in \mathcal{O}_K} \frac{1}{N\mathfrak{a}^s} = \zeta_K(s).$$

This is just the Dedekind ζ -function of K .

Example. Let L/K be a finite Galois extension with Galois group G . Consider the regular representation $r_{L/K}$ on $\mathbb{C}[G]$. This decomposes as $\bigoplus \rho_i^{d_i}$, where $\{\rho_i\}$ run over the irreducible representations of G of dimension d_i . We also have

$$r_{L/K} = \mathrm{Ind}_{\Gamma_L}^{\Gamma_K}(1).$$

So by the induction formula, we have

$$\zeta_L(s) = L(r_{L/K}, s) = \prod_i L(\rho_i, s)^{d_i}.$$

Example. For example, if $L/K = \mathbb{Q}(\zeta_N)/\mathbb{Q}$, then

$$\zeta_{\mathbb{Q}(\zeta_N)}(s) = \prod_{\chi} L(\chi, s),$$

where the product runs over all primitive Dirichlet characters mod $M | N$. Since $\zeta_{\mathbb{Q}(\zeta_N)}, \zeta_{\mathbb{Q}}$ have simple poles at $s = 1$, we know that $L(\chi, 1) \neq 0$ if $\chi \neq \chi_0$.

Theorem (Brauer induction theorem). Suppose $\rho : G \rightarrow \mathrm{GL}_N(\mathbb{C})$ is a representation of a finite group. Then there exists subgroups $H_j \subseteq G$ and homomorphisms $\chi_j : H_j \rightarrow \mathbb{C}^\times$ and integers $m_j \in \mathbb{Z}$ such that

$$\mathrm{tr} \rho = \sum_j m_j \mathrm{tr} \mathrm{Ind}_{H_j}^G \chi_j.$$

Note that the m_j need not be non-negative. So we cannot quite state this as a statement about representations.

Corollary. Let $\rho : \Gamma_K \rightarrow \mathrm{GL}_N(\mathbb{C})$. Then there exists finite separable L_j/K and $\chi_j : \Gamma_{L_j} \rightarrow \mathbb{C}^\times$ of finite order and $m_j \in \mathbb{Z}$ such that

$$L(\rho, s) = \prod_j L(\chi_j, s)^{m_j}.$$

In particular, $L(\rho, s)$ has meromorphic continuation to \mathbb{C} and has a functional equation

$$\Lambda(\rho, s) = L \cdot L_\infty = \varepsilon(\rho, s) L(\tilde{\rho}, 1 - s)$$

where

$$\varepsilon(\rho, s) = AB^s = \prod \varepsilon(\chi_j, s)^{m_j},$$

and $\tilde{\rho}(g) = {}^t \rho(g^{-1})$.

Conjecture (Artin conjecture). If ρ does not contain the trivial representation, then $\Lambda(\rho, s)$ is entire.

This is closely related to the global Langlands conjecture.

In general, there is more than one way to write ρ as an sum of virtual induced characters. But when we take the product of the ε factors, it is always well-defined. We also know that

$$\varepsilon(\chi_j, s) = \prod \varepsilon_v(\chi_{j,v}, s)$$

is a product of local factors. It turns out the local decomposition is not independent of the decomposition, so if we want to write

$$\varepsilon(\rho, s) = \prod_v \varepsilon_v(\rho_v, s),$$

we cannot just take $\varepsilon_v(\rho_v, s) = \prod \varepsilon_v(\chi_{j,v}, s)$, as this is not well-defined. However, Langlands proved that there exists a unique factorization of $\varepsilon(\rho, s)$ satisfying certain conditions.

We fix F a non-Archimedean local field, $\chi : F^\times \rightarrow \mathbb{C}^\times$ and local ε factors

$$\varepsilon(\chi, \psi, \mu),$$

where μ is a Haar measure on F and $\psi : F \rightarrow \mathrm{U}(1)$ is a non-trivial character. Let $n(\psi)$ be the least integer such that $\psi(\pi_F^n \mathcal{O}_F) = 1$. Then

$$\varepsilon(\chi, \psi, \mu) = \begin{cases} \mu(\mathcal{O}_F) & \chi \text{ unramified, } n(\psi) = 0 \\ \int_{F^\times} \chi^{-1} \cdot \psi \, d\mu & \chi \text{ ramified} \end{cases}$$

Since χ and ψ are locally constant, the integral is actually sum, which turns out to be finite (this uses the fact that χ is ramified).

For $a \in F^\times$ and $b > 0$, we have

$$\varepsilon(\chi, \psi(ax), b\mu) = \chi(a)|a|^{-1}b\varepsilon(\chi, \psi, \mu).$$

Theorem (Langlands–Deligne). There exists a unique system of local constants $\varepsilon(\rho, \psi, \mu)$ for $\rho : W_F \rightarrow \mathrm{GL}_{\mathbb{C}}(V)$ such that

- (i) ε is multiplicative in exact sequences, so it is well-defined for virtual representations.
- (ii) $\varepsilon(\rho, \psi, b\mu) = b^{\dim V} \varepsilon(\rho, \psi, \mu)$.
- (iii) If E/F is finite separable, and ρ is a virtual representation of W_F of degree 0 and $\sigma = \mathrm{Ind}_{W_E}^{W_F} \rho$, then

$$\varepsilon(\sigma, \psi, \mu) = \varepsilon(\rho, \psi \circ \mathrm{tr}_{E/F}, \mu').$$

Note that this is independent of the choice of μ and μ' , since “ $\dim V = 0$ ”.

- (iv) If $\dim \rho = 1$, then $\varepsilon(\rho)$ is the usual abelian $\varepsilon(\chi)$.

Index

- C_K^0 , 13
- F^{ur} , 5
- I_F , 5
- I_S , 18
- J_K , 12
- K^{ab} , 4
- P_F , 5
- Art_F , 6
- Frob_q , 5
- Γ_K , 4
- $\Lambda(\chi, s)$, 29
- Σ_K^∞ , 11
- $\Sigma_{K, \infty}$, 11
- \bar{K} , 4
- $\mathbb{Z}_\ell(1)(\bar{k})$, 6
- \mathbb{A}_K , 12
- \mathbb{A}_K^\times , 12
- $\mathfrak{a}(\infty)$, 17
- $\mu_n(\bar{k})$, 5
- k_F , 5
- $v \mid \infty$, 11
- $v \nmid \infty$, 11
- adele, 12
- algebraic Hecke character, 23
- algebraic homomorphism, 22
- Archimedean local field, 4
- arithmetic Frobenius, 5
- Artin map
 - global, 13
 - local, 6
- Artin reciprocity law, 14
- Brauer group, 9
- CM field, 26
- conductor, 18
- connected Serre group, 28
- content homomorphism, 16
- decomposition group, 13
- existence theorem, 7
- finite place, 11
- fundamental mistake of class field theory, 18
- generalized ideal class group, 18
- geometric Frobenius, 5
- global ε -factor, 30
- global Artin map, 13
- global field, 11
- Hecke character, 21
- idele, 12
- idele class group, 12
- inertia group, 5
- infinite place, 11
- infinite type, 23
- Kronecker–Weber theorem, 17
- Krull topology, 4
- local ε -factors, 30
- local Artin map, 6
- local class field theory, 6
- local field, 4
- maximal tamely ramified extension, 6
- maximal unramified extension, 5
- modulus, 17
- non-Archimedean local field, 4
- place, 11
- product formula, 11
- profinite group, 4
- quasi-characters, 21
- ramification
 - real place, 15
- ray class character, 21
- ray class field, 18
- ray class group, 18
- relative Weil group, 9
- residue field, 5
- Serre type, 26
- tame mod n character, 5
- Tamiyama group, 28
- Tate module, 6
- uniformizer, 4
- valuation ring, 4
- Weil group, 8
- wild inertia group, 5