Math 845 Notes
Class field theory

Lectures by Tonghai Yang
Notes by Daniel Hast

Spring 2015

Contents

1 2015-01-21: Introduction

References:

- Milne's notes on class field theory
- Lang, *Algebraic Number Theory*
- Neukirch, *Algebraic Number Theory* (very abstract)

Let k be a global field. Let K/k be a Galois extension of degree n with Galois group G. Let $\mathfrak{f} = d_{K/k}$ be the relative discriminant. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_k$. We can factor $\mathfrak{p}\mathcal{O}_K = (P_1 \cdots P_g)^e$, where $efg = n$; e is the ramification index, and $f = [\mathcal{O}_K/P_i : \mathcal{O}_k/\mathfrak{p}]$ is the residue degree. We have $e = 1 \iff \mathfrak{p} \nmid \mathfrak{f}$, in which case we say $\mathfrak{p}$ is unramified in K/k.

We have an *Artin map* $P_i \mapsto \mathrm{Frob}_{P_i} \in \mathrm{Gal}(K/k)$ such that $\mathrm{Frob}_{P_i}(x) \equiv x^{N\mathfrak{p}} \mod P_i$ for all $x \in \mathcal{O}_K - \mathfrak{p}_i$. Moreover, if $\sigma \in \mathrm{Gal}(K/k)$ such that $\sigma(P_i) = P_j$, then $\mathrm{Frob}_{P_i} = \sigma \, \mathrm{Frob}_{P_j} \, \sigma^{-1}$.

Special case: if $\mathrm{Gal}(K/k)$ is abelian, then $\mathrm{Frob}_{P_i} = \mathrm{Frob}_{P_j}$ depends only on $\mathfrak{p}$, so we denote it by $\mathrm{Frob}_{\mathfrak{p}}$.

Remark 1.1. From now on, we will deal only with abelian extensions unless otherwise specified.

Definition 1.2. Let $I(\mathfrak{f})$ denote the group of fractional ideals of $\mathcal{O}_k$ that are prime to $\mathfrak{f}$. This is a free abelian group with respect to ideal multiplication.

The Artin map is thus a homomorphism $\mathfrak{p} \mapsto \mathrm{Frob}_{\mathfrak{p}} : I(\mathfrak{f}) \to G_{K/k}$.

Aside 1.3. Let $\mathcal{D}_{K/k}$ denote the relative different, defined by

$$\mathcal{D}_{K/k}^{-1} = \left\{ x \in K \;\middle|\; \mathrm{tr}_{K/k}(xy) \in \mathcal{O}_k \ \forall y \in \mathcal{O}_K \right\}.$$

Note that $d_{K/k} = N_{K/k}\mathcal{D}_{K/k}$, and the trace map $\mathrm{tr}_{K/k}$ is a nondegenerate symmetric bilinear form.

Basic questions:

(1) What is the image of the Artin map? In fact, it's surjective.

(2) What is the kernel of the Artin map? Denote

$$\mathrm{Spl}_{K/k} = \left\{ \mathfrak{p} \in I(\mathfrak{f}) \;\middle|\; \mathrm{Frob}_{\mathfrak{p}} = 1 \right\} = \left\{ \mathfrak{p} \;\middle|\; \mathfrak{p} \text{ splits completely in } K \right\}.$$

Amazing fact: $\mathrm{Spl}_{K/k}$ determines K uniquely! More precisely, if $\mathrm{Spl}_{K/k} = \mathrm{Spl}_{L/k}$, then $K \cong L$ as k-algebras.

(3) For which subgroups N of finite index in $I(\mathfrak{f})$ is $I(\mathfrak{f})/N \cong \mathrm{Gal}(K/k)$ for some abelian extension K of k? (In other words, which subgroups of $I(\mathfrak{f})$ can be kernels of an Artin map?)

(4) How can we construct the maximal abelian extension k^{ab}/k? This is wide open even for real quadratic fields.

1.1 Quadratic reciprocity

Let $k = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ such that $d \equiv 0, 1 \pmod 4$. Then $\mathcal{O}_K = \mathbb{Z}\left[\frac{d+\sqrt{d}}{2}\right]$ and $\mathfrak{f} = d\mathbb{Z} = d$. Write $\mathrm{Gal}(K/k) = \{1, \sigma\}$. The split primes are

$$\mathrm{Spl}_{K/k} = \left\{p \text{ prime} \;\middle|\; x^2 \equiv d \pmod p \text{ has 2 solutions}\right\}.$$

Example 1.4. Does $p = 163$ split in $\mathbb{Q}(\sqrt{-3})$? It's not immediately clear how to efficiently determine whether $x^2 \equiv -3 \pmod{163}$ has two solutions.

Gauss solved this by proving the quadratic reciprocity law. Define the *Legendre symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \mid p, \\ 1 & \text{if } x^2 \equiv a \pmod p \text{ has two solutions,} \\ -1 & \text{if } x^2 \equiv a \pmod p \text{ has no solutions.} \end{cases}$$

Theorem 1.5 (Quadratic reciprocity)**.** *Let p and q be distinct odd primes. Then*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \qquad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Corollary 1.6. *Whether $p \in \mathrm{Spl}_{K/\mathbb{Q}}$ depends only on the class of p mod d. In fact, $p \in \mathrm{Spl}_{K/k} \iff \left(\frac{p}{|d|}\right) = 1$.*

Moreover, the kernel of the Artin map consists of all ideals $a\mathbb{Z}$ with $a = \prod_i p_i^{e_i} \cdot \prod_j q_j^{f_j}$, where the p_i are split, q_j are inert, and $\sum_j f_j$ is even.

1.2 Cyclotomic fields

Let $K = \mathbb{Q}(\zeta_N)$, where N is odd or $4 \mid N$. Then $d_{K/\mathbb{Q}} = N\mathbb{Z}$, and we have an isomorphism $a \mapsto \sigma_a : (\mathbb{Z}/N)^\times \xrightarrow{\simeq} G$, where $\sigma_a(\zeta_N) = \zeta_N^a$.

What does the composition with the Artin map $I(N\mathbb{Z}) \to \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/N)^\times$ look like? We have $\mathrm{Frob}_p = \sigma_p$, so $\mathrm{Spl}_{K/k} = \{p \mid p \equiv 1 \mod N\}$. Hence, the kernel of the Artin map is $\{\alpha\mathbb{Z} \mid \alpha \equiv 1 \mod N\}$.

Theorem 1.7 (Weber)**.** *Every abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field $\mathbb{Q}(\zeta_N)$, i.e., $\mathbb{Q}^{ab} = \mathbb{Q}(\zeta_\infty) := \bigcup_N \mathbb{Q}(\zeta_N)$.*

Exercise 1.8. Let $(-1)^* = -4$, $2^* = 8$, and $p^* = (-1)^{\frac{p-1}{2}}p$ if p is odd. For which N do we have $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_N)$?

2 2015-01-23: Class fields and reciprocity

Let K/k be an abelian Galois extension with Galois group G of order n, and let $\mathfrak{f} = d_{K/k}$. We want to study the Artin map $I(\mathfrak{f}) \twoheadrightarrow G_{K/k}$. What is the kernel?

Given an ideal $\mathfrak{m} \subset \mathcal{O}_k$ and a subgroup $\mathcal{K}$ of $I(\mathfrak{m})$ of finite index, is there an abelian field extension K of k such that the Artin map induces an isomorphism $I(\mathfrak{m})/\mathcal{K} \xrightarrow{\simeq} G_{K/k}$? If so, how many (up to k-isomorphism)?

2.1 Hilbert class fields

Recall the class group $\mathrm{Cl}(k) = I(\mathcal{O}_k)/P_k$, where P_k is the subgroup of all principal ideals.

Theorem 2.1 (Hilbert class field theorem)**.** *There is a unique (up to k-isomorphism) abelian extension H of k, called the* Hilbert class field *of k, such that* $\mathrm{Art} : \mathrm{Cl}(k) \xrightarrow{\simeq} G_{H/k}$ *is an isomorphism.*

Corollary 2.2. *(1) Every prime ideal of k is unramified in H.*

(2) The primes that split in H/k are exactly the principal prime ideals of k.

(3) H is the maximal abelian extension of k such that every prime ideal of k is unramified.

Remark 2.3. H may not be the maximal extension of k such that every prime ideal of k is unramified. For example, H might not have trivial class group, so we can take its class group and get a nonabelian unramified extension of k. By the Golod–Shafarevich theorem, iterating the class field construction can sometimes even result in an infinite tower.

Example 2.4. Let $k = \mathbb{Q}(\sqrt{d})$, where $d = p_1^* p_2^* \cdots p_r^*$, where $2^* = 8$, $(-1)^* = -4$, $p^* = p$ for $p \equiv 1 \pmod 4$, and $p^* = -p$ for $p \equiv -1 \pmod 4$. Then $K = \mathbb{Q}(\sqrt{p_1^*}, \sqrt{p_2^*}, \ldots, \sqrt{p_r^*})$ is unramified over k, so $K \subset H := \mathrm{Hil}(k)$, giving a surjection $\mathrm{Gal}(H/k) \twoheadrightarrow \mathrm{Gal}(K/k) \cong (\mathbb{Z}/2)^{r-1}$. This was studied by Gauss as *genus theory*.

2.2 Ray class fields

Given a number field k, we have real embeddings $\sigma : k \hookrightarrow \mathbb{R}$ and conjugate pairs of complex embeddings $\sigma, \overline{\sigma} : k \hookrightarrow \mathbb{C}$, which we think of as "primes at infinity". If σ is such an infinite prime, then we get a completion $k \hookrightarrow k_\sigma$, where k_σ is the usual completion of k with respect to the topology $|x|_\sigma = |\sigma(x)|$. (Similarly, if $\mathfrak{p}$ is a finite prime, we get a completion $k \hookrightarrow k_{\mathfrak{p}}$, the $\mathfrak{p}$-adic completion of k.)

A *cycle* of k is a formal product $\mathfrak{m} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r} \sigma_1^{\varepsilon_1} \sigma_2^{\varepsilon_2} \cdots \sigma_s^{\varepsilon_s} = \mathfrak{m}_f \mathfrak{m}_\infty$, where the σ_i are real primes, $e_i \geq 0$, and $\varepsilon_1 \in \{0, 1\}$. We denote

$$\begin{aligned} I(\mathfrak{m}) &= \{\text{fractional ideals of } k \text{ prime to } \mathfrak{m}\} = \{\text{fractions ideals of } k \text{ prime to } \mathfrak{m}_f\}, \\ P(\mathfrak{m}) &= \left\{\alpha\mathcal{O}_k \;\middle|\; \alpha \equiv 1 \pmod{^*\, \mathfrak{m}},\ \alpha \text{ prime to } \mathfrak{m}_f\right\}, \end{aligned}$$

where $\alpha \equiv 1 \pmod{^* \mathfrak{m}}$ means $\alpha \equiv 1 \pmod{\mathfrak{m}}$ for all i and $\sigma_j(\alpha) > 0$ when $\varepsilon_j = 1$.

Fact 2.5. $|I(\mathfrak{m})/P(\mathfrak{m})| < \infty$.

Theorem 2.6. *There is a unique abelian field extension $H_{\mathfrak{m}}$ of k such that* $\mathrm{Art} : I(\mathfrak{m})/P(\mathfrak{m}) \xrightarrow{\simeq} \mathrm{Gal}(H_{\mathfrak{m}}/k)$*. Again,*

$$\mathrm{Spl}_{H_{\mathfrak{m}}/k} = \left\{ \alpha\mathcal{O}_k \;\middle|\; \alpha \equiv 1 \pmod{^* \mathfrak{m}},\ \forall \mathcal{O}_k \text{ prime} \right\}.$$

Example 2.7. (1) Let $k = \mathbb{Q}$ and $\mathfrak{m} = N \cdot \infty$. Then

$$\frac{I(\mathfrak{m})}{P(\mathfrak{m})} = \frac{\{n\mathbb{Z} \mid (n, N) = 1\}}{\{n\mathbb{Z} \mid n > 0,\ n \equiv 1 \pmod{N}\}} \cong (\mathbb{Z}/N)^{\times}.$$

Thus, $H_{\mathfrak{m}} = \mathbb{Q}(\zeta_N)$.

(2) Let $\mathfrak{m} = N$. Then $I(\mathfrak{m})/P(\mathfrak{m}) = (\mathbb{Z}/N)^{\times}/\{\pm 1\}$, so $H_{\mathfrak{m}} = \mathbb{Q}(\zeta_N)^+ = \mathbb{Q}(\zeta_N + \zeta_N^{-1})$.

2.3 Reciprocity law

Theorem 2.8 (Reciprocity law of class field theory)**.** *Let L/K be a finite abelian extension of global fields, and let S be the set of primes of K ramified in L. Then there is a cycle $\mathfrak{m}$ (the* modulus*) in which the primes are exactly S, and a surjective map* $\mathrm{Art}_{L/K} : I(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ *such that:*

(1) $\ker(\mathrm{Art}_{L/K}) \supseteq P(\mathfrak{m})$*, i.e., $L \subset H_{\mathfrak{m}}$;*

(2) $\ker(\mathrm{Art}_{L/K}) = \left\{ N_{L/K}\mathcal{A} \mid \mathcal{A} \text{ is a fractional ideal of } L \text{ prime to } \mathfrak{m}_f\mathcal{O}_L \right\}$.

Moreover, given a cycle $\mathfrak{m}$ and a subgroup $P(\mathfrak{m}) \subset \mathcal{K} \subset I(\mathfrak{m})$, there is a unique finite abelian extension L of K giving an isomorphism $\mathrm{Art}_{L/K} : I(\mathfrak{m})/\mathcal{K} \xrightarrow{\simeq} \mathrm{Gal}(L/K)$.

Corollary 2.9 (Kronecker–Weber theory)**.** *Every finite abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_N)$ for some N.*

Question: How do we construct all $H_{\mathfrak{m}}$? Note that $K^{ab} = \bigcup_{\mathfrak{m}} H_{\mathfrak{m}}$.

3 2015-01-26: Local class field theory

Last time, we defined the ray class field $H_{\mathfrak{m}}$ of K. Moreover:

$$\begin{aligned} \ker(\mathrm{Art}_{L/K}) &= \left\{ N_{L/K}\mathfrak{a} \;\middle|\; \mathfrak{a} \subset L \right\} \cdot P(\mathfrak{m}), \\ \mathrm{Spl}_{L/K} &= \left\{ N_{L/K}P \;\middle|\; P \subset \mathcal{O}_L \text{ prime} \right\}, \\ P(\mathfrak{m}) &= \left\{ \alpha\mathcal{O}_K \;\middle|\; \alpha \equiv 1 \mod \mathfrak{m} \right\}. \end{aligned}$$

Note 3.1. We consider the extension $\mathbb{C}/\mathbb{R}$ to be ramified.

3.1 Local fields

Definition 3.2. A *local field* is a locally compact topological field with respect to a nontrivial valuation $|\cdot| : K \to \mathbb{R}_{\geq 0}$ such that $|1| = 1$, $|ab| = |a| \cdot |b|$, and $|a + b| \leq |a| + |b|$.

Proposition 3.3. *Every local field is one of the following:*

(1) $\mathbb{R}$ or $\mathbb{C}$ (archimedean);

(2) a finite extension of $\mathbb{Q}_p$, which is a completion of a number field;

(3) a finite extension of $\mathbb{F}_p(\!(x)\!)$, which is a completion of a global function field.

Hence, every local field arises from the following construction: Let K be a global field, let $\mathfrak{p}$ be a (finite or infinite) prime of K, and define $v_{\mathfrak{p}}(x) = a$ if $x\mathcal{O}_K = \mathfrak{p}^a \cdot \mathfrak{m}$ with $(\mathfrak{m}, \mathfrak{p}) = 1$. Then $|x|_{\mathfrak{p}} = q^{-v_{\mathfrak{p}}(x)}$ makes K into a valued field whose completion is a local field $K_{\mathfrak{p}}$.

Theorem 3.4. *Let K be a nonarchimedean local field. For any $n \geq 1$, there is a unique (up to K-isomorphism) unramified extension K_n of degree n. The maximal unramified extension of K is*

$$K^{un} = \bigcup_{n \geq 1} K_n = \bigcup_{p \nmid N} K(\mu_N),$$

where $\mu_N = \langle \zeta_N \rangle$ is the group of N-th roots of unity in K. Moreover, denote the maximal ideal of $\mathcal{O}_K$ by $\mathfrak{m}_K = \pi\mathcal{O}_K$ (where π is a uniformizer of K, i.e., a prime element of $\mathcal{O}_K$), and write $k := \mathcal{O}_K/\mathfrak{m}_K \cong \mathbb{F}_q$. Then we have an isomorphism

$$\mathrm{Gal}(K^{un}/K) \xrightarrow{\simeq} \mathrm{Gal}(\overline{k}/k) \cong \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) = \langle \mathrm{Frob}_q \rangle^{top},$$

under which the topological generator $\mathrm{Frob}_q \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ corresponds to Frob_K.

Remark 3.5. Hence, every unramified extension of a nonarchimedean local field is abelian!

3.2 Local reciprocity law

Theorem 3.6 (Local reciprocity)**.** *Let K be a nonarchimedean local field. There is a group homomorphism, the* local Artin map $\varphi_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$ *such that:*

(1) For any unramified finite extension L/K and any uniformizer π of K,

$$\varphi_K(\pi)\big|_L = \mathrm{Frob}_{L/K} = \mathrm{Frob}_K.$$

(2) For any finite abelian extension L/K, $N_{L/K}L^\times \subset \ker(\varphi_K)$, and φ_K induces an isomorphism

$$\varphi_{L/K} : K^\times/N_{L/K}L^\times \xrightarrow{\simeq} \mathrm{Gal}(L/K).$$

In particular, we have a commutative diagram

$$\begin{tikzcd} K^\times \arrow[r, "\varphi_K"] \arrow[d] & \mathrm{Gal}(K^{ab}/K) \arrow[d] \\ K^\times/N_{L/K}L^\times \arrow[r, "\simeq"] & \mathrm{Gal}(L/K). \end{tikzcd}$$

Remark 3.7. However, for topological reasons, φ_K itself is not surjective.

Theorem 3.8 (Existence theorem). *Let $N \leq K^\times$ be a subgroup. Then the following are equivalent:*

(1) There exists a finite abelian extension L/K such that $N_{L/K}L^\times = N$.

(2) $[K^\times : N] < \infty$ and N is open in $K^\times$.

Remark 3.9. If $\operatorname{char} K = 0$, then $[K^\times : N] < \infty$ implies N is open in $K^\times$. If $\operatorname{char} K > 0$, then the openness condition is an honest condition: there are non-open subgroups of finite index in $K^\times$.

Corollary 3.10. *Let K be a nonarchimedean local field with residue field k. If $\operatorname{char} K = 0$ and $\operatorname{char} k \neq 2$, then K has exactly 3 quadratic field extensions (up to isomorphism).*

Proof. By the existence theorem, quadratic field extensions of K correspond to subgroups $N \leq K^\times$ such that $[K^\times : N] = 2$. Fix a uniformizer π; then $K^\times = \pi^{\mathbb{Z}} \cdot \mathcal{O}_K^\times$, so

$$K^\times/(K^\times)^2 \cong \langle \pi \rangle / \langle \pi^2 \rangle \times \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 \cong (\mathbb{Z}/2) \times \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2.$$

Note that $\mathcal{O}_K^\times \cong (\mathcal{O}_K/\mathfrak{m}_K)^\times \cdot (1 + \pi\mathcal{O}_K)$, so $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 \cong (\mathbb{F}_q^\times)/(\mathbb{F}_q^\times)^2 \cong \mathbb{Z}/2$. Thus, $K^\times/(K^\times)^2 \cong (\mathbb{Z}/2) \times (\mathbb{Z}/2)$, and quadratic field extensions of K correspond to elements of order 2 in this group; there are three of these. $\square$

4 2015-01-28: Existence and Lubin–Tate fields

Exercise 4.1. (1) Let K be a nonarchimedean field. Then $1 \to 1+\mathfrak{m}_K \to \mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{m}_K)^\times \to 1$ is exact. Is it split?

(2) When is $K^\times/(K^\times)^2$ trivial in characteristic 2?

A *residue character* of K is a character of the residue field $\mathcal{O}_K/\mathfrak{m}_K$.

Let us state the existence theorem more precisely:

Theorem 4.2. *Finite abelian extensions of K correspond to open subgroups of $K^\times$ of finite index, via $L \mapsto N_{L/K}L^\times$, which is bijective. Moreover, if $L_1 \subset L_2$, then $N_{L_1/K}L_1^\times \supset N_{L_2/K}L_2^\times$, $N(L_1^\times \cap L_2^\times) = N_{L_1/K}L_1^\times \cdot N_{L_2/K}L_2^\times$, and $N(L_1L_2) = N_{L_1/K}L_1^\times \cap N_{L_2/K}L_2^\times$.*

Here are two towers of abelian extensions. Note that $K^\times = \pi^{\mathbb{Z}}\mathcal{O}_K^\times = \pi^{\mathbb{Z}}(\mathcal{O}_K/\mathfrak{m}_K)^\times \cdot (1 + \mathfrak{m}_K)$. The first tower is $K^{un} = \bigcup_{n\geq 1} K_n^{un}$, where K_n^{un} is the unique unramified extension of K of degree n. This is associated to $(\pi^n)^K \times \mathcal{O}_K^\times$. Hence, K^{un} corresponds to $\mathcal{O}_K^\times$; more precisely, $\ker(\varphi_K)|_{K^{un}} = \mathcal{O}_K^\times$.

Corollary 4.3. *$\varphi_K|_{K^{un}} : K^\times \to \operatorname{Gal}(K^{un}/K)$ has kernel $\mathcal{O}_K^\times$; this map is given by $\pi \mapsto \operatorname{Frob}_K$.*

The second tower depends on the choice of uniformizer π, and corresponds to the subgroup $\pi^{\mathbb{Z}}(1+\mathfrak{m}_K^n) < K^\times$, which is an open finite index subgroup of $K^\times$. Class field theory gives a unique field extension $K_{\pi,n}$ of K such that $\mathrm{Gal}(K_{\pi,n}/K) \cong K^\times/\pi^{\mathbb{Z}}(1+\mathfrak{m}_K^n)$. Since $\pi^{\mathbb{Z}}(1+\mathfrak{m}_K^n) = N_{K_{\pi,n}}K_{\pi,n}^\times$, there exists a uniformizer π_n of $K_{\pi,n}$ such that $N_{K_{\pi,n}}\pi_n = \pi$, so $\pi\mathcal{O}_K = \pi_n^n\mathcal{O}_{K_{\pi,n}}$.

Corollary 4.4. *The above construction gives a tower $K_{\pi,0} \subset K_{\pi,1} \subset K_{\pi,2} \subset \dots$ of totally ramified abelian extensions of K. Their union $K_\pi := \bigcup_n K_{\pi,n}$ corresponds to $\pi^{\mathbb{Z}}$ and is a maximal totally ramified abelian extension.*

Remark 4.5. If $u \in \mathcal{O}_K^\times$, then K_π might not be the same as $K_{\pi u}$. Our eventual theorem will be that $K^{ab} = K_\pi K^{un}$.

We have a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K^\times & \xrightarrow{v_p} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \varphi_K} & & \downarrow & & \\ 1 & \longleftarrow & \mathrm{Gal}(\overline{k}/k) & \longleftarrow & \mathrm{Gal}(K^{ab}/K) & \longleftarrow & I & \longleftarrow & 1 \end{array}$$

However, φ_K is surjective but not injective. One thing to do is to take a limit and get $1 \to \mathcal{O}_K^\times \to \widehat{K} \to \widehat{Z} \to 0$. The second way is via Langlands idea.

The weight group is the inverse image of the discrete group generated by the Frob_q, i.e., $W_K = I_K\,\mathrm{Frob}_K^{\mathbb{Z}}$. Put a topology so that $I_K < W_K^{ab}$ is open. Now, the one-dimensional characters of W_K are $\mathrm{Hom}(W_K^{ab}, \mathbb{C}) \cong \mathrm{Hom}(K^\times, \mathbb{C}^\times) = \mathrm{Hom}(\mathrm{GL}_1(K), \mathrm{GL}_1(\mathbb{C}))$.

5 2015-01-30: Lubin–Tate theory

The local reciprocity law gives us a morphism $\varphi_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$ such that:

(1) $\varphi_K^{(\pi)}|_{K^{un}} = \mathrm{Frob}_K$

(2) If L/K is a finite abelian extension, then $\varphi_{L/K} : K^\times \to \mathrm{Gal}(L/K)$ is surjective, and $\ker\varphi_{L/K} = N_{L/K}L^\times$.

Our goal for today: For a uniformizer π of K, construct its associated *maximal totally ramified abelian* extension $K_\pi = \bigcup_{n\geq 1} K_{\pi,n}$ such that:

(1) $K_{\pi,n} \subset K_{\pi,n+1}$

(2) $K_{\pi,n}/K$ is totally ramified of degree $[K_{\pi,n} : K] = q^{n-1}(q-1)$, where $q = |\mathcal{O}_K/\mathfrak{m}_K|$.

5.1 Lubin–Tate formal group laws

Let A be a commutative ring, and let $A[[T]]$ be the ring of formal power series over A. Given $f \in A[[T]]$ and $g \in TA[[T]]$, the composition $f \circ g$ is well-defined. If $g, h \in TA[[T]]$, then $f \circ (g \circ h) = (f \circ g) \circ h$. However, $f \circ (g + h) \neq f \circ g + f \circ h$.

Lemma 5.1. *Let $f = \sum_{i=1}^{\infty} a_i T^i \in TA[[T]]$. Then $a_1 \in A^\times \iff$ there exists $g \in TA[[T]]$ such that $f \circ g = T$. In this case, g is unique and $g \circ f = T$.*

Definition 5.2. A *one-parameter formal group law* over A is a power series $F(X,Y) \in A[[X,Y]]$ such that:

(1) $F(X,Y) = X + Y + (\text{terms of degree} \geq 2)$.

(2) $F(F(X,Y),Z) = F(X,F(Y,Z))$.

(3) $F(X,Y) = F(Y,X)$.

Proposition 5.3. *(1) $F(X,0) = X$ and $F(0,Y) = Y$.*

(2) There exists $i_F(X) \in XA[[X]]$ such that $F(X, i_F(X)) = 0$.

Proof. (1) Let $f(X) = F(X,0) = X + (\text{terms of degree} \geq 2)$. By associativity,

$$f(f(X)) = F(F(X,0),0) = F(X,F(0,0)) = F(X,0) = f(x).$$

Since $f(X) \in XA[[X]]$, there exists $g \in XA[[X]]$ such that $f \circ g = X$. Hence,

$$f = f \circ (f \circ g) = (f \circ f) \circ g = f \circ g = X.$$

(2) Suppose $G(X) = \sum_{n \geq 1} b_n X^n$ satisfies $F(X, G(X)) = 0$. Then

$$X + G(X) + \sum_{i+j=2} a_{ij} X^i G(X)^j = 0.$$

So $b_1 = -1$. Proceeding inductively, we can construct $i_F(X)$. □

Remark 5.4. For any formal group law F, we have $F(X,Y) = X + Y + XYF_1(X,Y)$ for some power series $F_1(X,Y)$.

Remark 5.5. If F is a formal group law over $\mathcal{O}_K$, for any finite extension L/K, we can define a new addition on $\mathfrak{m}_L$ by $a +_F b = F(a,b)$. This makes $(\mathfrak{m}_L, +_F)$ into an abelian group.

Example 5.6. The power series $F = X + Y$ is a formal group, called the *additive formal group*. It satisfies $(\mathfrak{m}_K, +_F) = (\mathfrak{m}_K, +)$.

Example 5.7. The power series $F = X+Y+XY = (1+X)(1+Y)-1$ is a formal group, called the *multiplicative formal group*. There is an isomorphism $a \mapsto 1 + a : (\mathfrak{m}_K, +_F) \cong (1 + \mathfrak{m}, \cdot)$.

Example 5.8. There is a formal group law associated to an elliptic curve

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We want to understand the local behavior near $0 = \infty$. Note that $\frac{y}{x}$ is a uniformizer at 0. Write $x = \sum_{i \geq -2} c_i t^i$ and $y = \sum_{i \geq -3} b_i t^i$. Given $P_1 = (x(t_1), y(t_1))$ and $P_2 = (x(t_2), y(t_2))$, we can write $P_1 + P_2 = \hat{E}(t_1, t_2)$ for some formal power series $\hat{E}$. The abelian group axioms for E imply the corresponding axioms for $\hat{E}$, which is therefore a formal group law.

6 2015-02-02: Formal groups

6.1 Morphisms of formal groups

Let F and G be formal groups over A. A morphism of formal groups $f \in \mathrm{Hom}(F, G)$ is a power series $f \in TA[\![T]\!]$ such that $f(F(X, Y)) = G(f(X), f(Y))$.

Fix a formal group F. For $f, g \in TA[\![T]\!]$, define $f +_F g = F(f(X), g(X)) \in XA[\![X]\!]$.

Lemma 6.1. *(1) $(TA[\![T]\!], +_F)$ is an additive group.*

(2) $(\mathrm{Hom}(F, G), +_G)$ is a subgroup of $(TA[\![T]\!], +_G)$.

(3) $(\mathrm{End}(F), +_F, \circ)$ is a ring.

6.2 Lubin–Tate formal group laws

Let K be a nonarchimedean local field with ring of integers $\mathcal{O}_K$ and maximal ideal $\mathfrak{m}_K = \pi\mathcal{O}_K$. Let $q = |\mathcal{O}_K/\mathfrak{m}_K|$. Define

$$\mathcal{F}_\pi = \left\{ f \in \mathcal{O}_K[\![T]\!] \;\middle|\; f(T) = \pi T + (\deg \geq 2),\ f(T) \equiv T^q \pmod{\pi} \right\}.$$

Example 6.2. $f(X) = \pi X + X^q \in \mathcal{F}_\pi$.

Example 6.3. Let $K = \mathbb{Q}$. Then $f(x) = (1 + x)^p - 1 = px + \binom{p}{2}x^2 + \cdots + x^p \in \mathcal{F}_p$.

Theorem 6.4 (Main theorem). *(1) For each $f \in \mathcal{F}_\pi$, there is a unique formal group law F_f such that $f \in \mathrm{End}(F_f)$.*

(2) F_f is an $\mathcal{O}_K$-module, i.e., the map $a \mapsto [a]_f : \mathcal{O}_K \to \mathrm{End}(F_f)$ is a ring morphism.

(3) For $f, g \in \mathcal{F}_\pi$, $\mathrm{Hom}(F_f, F_g)$ is also an $\mathcal{O}_K$-module via a map $a \mapsto [a]_{g,f} : \mathcal{O}_K \to \mathrm{Hom}(F_f, F_g)$ such that $[a]_{g,f}$ is an isomorphism $\iff$ $a \in \mathcal{O}_K^\times$. In particular, any two F_f, F_g are isomorphic.

Lemma 6.5 (Basic lemma). *Given $f, g \in \mathcal{F}_\pi$ and a linear form $\phi_1 = \sum_{i=1}^n a_i X_i$ with $a_i \in \mathcal{O}_K$, there is a unique $\phi \in \mathcal{O}_K[\![X_1, X_2, \ldots, X_n]\!]$ such that:*

(1) $\phi = \phi_1 + (\deg \geq 2)$.

(2) $f(\phi(X_1, \ldots, X_n)) = \phi(g(X_1), \ldots, g(X_n))$, i.e., $f \circ \phi = \phi \circ g$.

This lemma implies the theorem. Indeed, take $\phi_1 = X + Y$ and $g = f$. Then there is a power series $F_f \in \mathcal{O}_K[\![X, Y]\!]$ such that $F_f(X, Y) = X + Y + (\deg \geq 2)$ and $f \circ F_f = F_f \circ f$. By uniqueness and the fact that ϕ_1 is symmetric, $F_f(Y, X) = F_f(X, Y)$. Now we need to check $F_f(F_f(X, Y), Z) = F_f(X, F_f(Y, Z))$. Look at $\phi_1 = X + Y + Z$, $g = f$, and check that both sides give ϕ in the lemma, e.g. for the left side,

$$F_f(F_f(X, Y, Z)) = F_f(X, Y) + Z + (\deg \geq 2) = X + Y + Z + (\deg \geq 2)$$

and

$$f(F_f(F_f(X, Y), Z)) = F_f(f(F_f(X, Y), Z)) = F_f(F_f(f(X, Y)), Z).$$

This proves part (1) of the theorem.

For part (3), given $f, g \in \mathcal{F}_\pi$ and $a \in \mathcal{O}_K$, take $\phi_1 = ax$ in the lemma. Then there is a unique $\phi = [a]_{g,f} \in \mathcal{O}_K[[X]]$ such that $\phi = aX + (\deg \geq 2)$ and $f(\phi(X)) = \phi(g(X))$.

We need to check that $F_f \circ \phi = \phi \circ F_g$. Take $\phi_1 = aX + aY$. Then $F_f(\phi(X), \phi(Y)) = \phi(X) + \phi(Y) + (\deg \geq 2) = aX + aY + (\deg \geq 2)$, so

$$f(F_f(\phi(X), \phi(Y))) = F_f(f \circ \phi(X), f \circ \phi(Y)) = F_f(\phi \circ g(X), \phi \circ g(Y)),$$

so ϕ satisfies the conditions of the lemma. Applying the same argument to $\phi \circ F_g$ proves $F_f \circ \phi = \phi \circ F_g$.

A similar approach using the basic lemma can be used to show $[a+b]_{g,f} = [a]_{g,f} + [b]_{g,f}$, $[a]_{g,f} \circ [b]_{h,g} = [ab]_{h,f}$, and $X = [1]_f = [aa^{-1}]_{f,f} = [a]_{g,f} \circ [a^{-1}]_{f,g}$. □

7 2015-02-04: Construction of Lubin–Tate extensions

7.1 Summary of last time

Last time, we proved the following theorem:

Theorem 7.1 (Main theorem)**.** *(1) For each $f \in \mathcal{F}_\pi$, there is a unique formal group law F_f such that $f \in \operatorname{End}(F_f)$.*

(2) For $a \in \mathcal{O}_K$ and $f, g \in \mathcal{F}_\pi$, there is a unique $[a]_{g,f} \in \mathcal{O}_K[[X]]$ such that $[a]_{g,f} = ax + (\deg \geq 2)$ and $[a]_{g,f} \circ f = g \circ [a]_{g,f}$. Moreover, this gives an additive group homomorphism

$$\begin{aligned} (\mathcal{O}_K, +) &\to (\operatorname{Hom}(F_f, F_g), +_{F_g}), \\ a &\mapsto [a]_{g,f}. \end{aligned}$$

Moreover, $[a]_{h,g} \circ [b]_{g,f} = [ab]_{h,f}$, so $[a]_{g,f}$ is an isomorphism $\iff$ $a \in \mathcal{O}_K^\times$. In particular, any two F_f, F_g are isomorphic.

(3) The map

$$\begin{aligned} (\mathcal{O}_K, +, \cdot) &\to (\operatorname{End} E_f, +_{F_f}, \circ), \\ a &\mapsto [a]_f = [a]_{f,f} \end{aligned}$$

is a ring homomorphism, making F_f into a formal $\mathcal{O}_K$-module.

Example 7.2. $[1]_f = T$, $[\pi]_f = f$.

Our proof was conditional on the following lemma:

Lemma 7.3 (Basic lemma)**.** *Let $f, g \in \mathcal{F}_\pi$, and let $\phi_1 = \sum_i a_i X_i$ be a linear form. There is a unique $\phi \in \mathcal{O}_K[[X_1, \ldots, X_n]]$ such that $\phi = \phi_1 + (\deg \geq 2)$ and $\phi \circ f = g \circ \phi$.*

Example 7.4. $[a+b]_{g,f} = [a]_{g,f} +_{F_g} [b]_{g,f}$.

7.2 Proof of the "basic lemma"

Now let us prove the lemma. By induction, we'll prove that for $r \geq 1$, there is a unique polynomial ϕ_r of degree $\leq r$ such that $\phi_r = \phi_1 + (\deg \geq 2)$ and $\phi_r(f(X)) = g(\phi_r(X)) + (\deg \geq r+1)$.

For $r = 1$, this is trivial with the original ϕ_1. Suppose we have a unique such ϕ_r. Then $\phi_{r+1} = \phi_r + \psi$, where ψ is a homogeneous polynomial of degree $r+1$ such that $\phi_{r+1} \circ f = g \circ \phi_{r+1} + (\deg \geq r+2)$. So

$$\phi_r \circ f + \psi \circ f = (\phi_r + \psi) \circ f = g \circ (\phi_r + \psi) + (\deg \geq r+2).$$

Since $f(X)$ and $g(X)$ are both of the form $\pi X + (\deg \geq 2)$,

$$g(\phi_r(X) + \psi(X)) = g(\phi_r(X)) + \pi\psi(X) + (\deg \geq r+2)$$

and $\psi(f(X)) = \pi^{r+1}\psi(X) + (\deg \geq r+2)$. So we must solve

$$\phi_r(f(X)) + \pi^{r+1}\psi(X) = g(\phi_r(X)) + \pi\psi(X) + (\deg \geq r+2).$$

Hence,

$$\psi(X) = \frac{g(\phi_r(X)) - \phi_r(f(X))}{\pi(\pi^r - 1)} + (\deg \geq r+2).$$

Note that $\pi^r - 1 \in \mathcal{O}_K^\times$. Since $g(\phi_r(X)) \equiv \phi_r(X)^q$ and $\phi_r(f(X)) \equiv \phi_r(X^q) \bmod \pi$, we have $g(\phi_r(X)) - \phi_r(f(X)) \equiv \phi_r(X)^q - \phi_r(X^q) \equiv 0 \pmod{\pi}$, we can divide by π, giving us ϕ_{r+1}.

Take $\phi = \lim_{r\to\infty} \phi_r = \phi_1 + \sum_{r=2}^{\infty}(\phi_r - \phi_{r-1}) \in \mathcal{O}_K[[X]]$. $\square$

7.3 Construction of "maximal" totally ramified abelian extension

We construct a totally ramified abelian extension K_π of K associated to a uniformizer π. Let $\overline{K}$ be the algebraic closure of K. Let $x \mapsto |x| = q^{-\operatorname{ord}_\pi x} : K^\times \to \mathbb{R}_{>0}$ be the absolute value on K. The image of the absolute value is $q^{\mathbb{Z}}$.

The absolute value extends uniquely to an absolute value $|\cdot| : \overline{K}^\times \to \mathbb{R}_{>0}$ whose image is $q^{\mathbb{Q}}$. Define

$$\mathcal{O}_{\overline{K}} = \left\{ x \in \overline{K} : |x| \leq 1 \right\},$$
$$\mathfrak{m}_{\overline{K}} = \left\{ x \in \overline{K} : |x| < 1 \right\}.$$

Then $\mathfrak{m}_{\overline{K}}$ is the maximal ideal of the local ring $\mathcal{O}_{\overline{K}}$.

A formal group $f \in \mathcal{F}_\pi$ gives us a formal group F_f, which yields an $\mathcal{O}_K$-module $\Lambda = \Lambda_f = (\mathfrak{m}_{\overline{K}}, +_{F_f})$. Since all the F_f are isomorphic, this is independent of f, so we'll choose $f = \pi X + X^q$ for convenience.

Definition 7.5. Define the n-torsion of $\Lambda = \Lambda_f$ by

$$\Lambda_n \overset{\text{def}}{=} \ker[\pi^n]_f = \ker[\pi]_f^n,$$

where we denote $f^{(1)} = f$ and $f^{(n)} = f \circ f^{(n-1)}$. Note that $[\pi]_f = f$ and $[\pi^n]_f = [\pi]_f \circ \ldots \circ [\pi]_f = f^{(n)}$.

Proposition 7.6. *Λ_n is an $\mathcal{O}_K$-module give by $\Lambda_n = \left\{x \in \mathfrak{m}_{\overline{K}} : f^{(n)}(X) = 0\right\}$.*

If we take $f = \pi X + X^q$, then $f^{(n)} \equiv X^{q^n} \pmod{\pi}$. The theory of Newton polygons tells us all roots of $f^{(n)}$ have absolute value < 1.

Theorem 7.7. $K_\pi = \bigcup_{n\geq 1} K(\Lambda_n)$.

We'll prove this next time.

8 2015-02-06: Maximal totally ramified abelian extensions

Exercise 8.1. Let K be a local field and L/K a finite unramified extension. Then $N_{L/K}\mathcal{O}_L^\times = \mathcal{O}_K^\times$.

Today, we construct a totally ramified extension of K associated to π such that $K^{ab} = K_\pi K^{un}$. In particular, we will show there exists a unique map $\varphi_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$ such that:

(1) $\varphi_K^{(\pi)}|_{K^{un}} = \mathrm{Frob}_K$ for any uniformizer of K, and $\varphi_K(a)|_{K^{un}} = 1$ if $a \in \mathcal{O}_K^\times$.

(2) If L/K is a finite abelian extension, then $\varphi_{L/K} = \varphi_K|_L : K^\times \twoheadrightarrow \mathrm{Gal}(L/K)$ satisfies $\ker\varphi_{L/K} = N_{L/K}L^\times$.

Given a uniformizer π, we obtain $\mathcal{F}_\pi$, which gives an isomorphism class $F_\pi = \{F_f\}$ of formal $\mathcal{O}_K$-modules. Last time, we constructed from this a genuine $\mathcal{O}_K$-module $\Lambda = \Lambda_f = (\mathfrak{m}_{\overline{K}}, +_{F_f})$ with submodules

$$\Lambda_n = \ker([\pi^n]_f : \Lambda \to \Lambda) = \left\{x \in \mathfrak{m}_{\overline{K}} : f^{(n)}(x) = 0\right\}.$$

Lemma 8.2. *If $f = \pi X + \cdots + X^q$, then $\Lambda_n = \left\{x \in \overline{K} : f^{(n)}(x) = 0\right\}$.*

This follows from the theory of Newton polygons: given $f(x) = a_0 + a_1 X + \cdots + a_n X^n$ with $a_i \in \mathcal{O}_K$, we construct the polygon with vertices $P_i = (i, \mathrm{ord}_\pi a_i)$. The Newton polygon of f is the convex hull of these points. Each segment P_iP_j tells us there are $j - i$ roots α of f with $\mathrm{ord}_\pi \alpha = -\,\mathrm{slope}(P_iP_j)$.

If $f = \pi X + \cdots + X^q$, then the Newton polygon of $\frac{f(X)}{X} = \pi + \cdots + X^{q-1}$ has only a single edge from $(0,1)$ to $(q-1, 0)$, so f has $q-1$ roots $\alpha_1, \ldots, \alpha_{q-1}$ of order $\frac{1}{q-1}$. Hence, $K(\alpha_i)/K$ is totally ramified for each i.

Lemma 8.3. *$\Lambda_n = \mathcal{O}_K/\pi^n$ as $\mathcal{O}_K$-modules. In particular, $\mathrm{Aut}_{\mathcal{O}_K}(\Lambda_n) \cong (\mathcal{O}_K/\pi^n)^\times$.*

Proof. See Milne's notes. □

Theorem 8.4. *Let $K_{\pi,n} = K(\Lambda_n)$ and $K_\pi = \bigcup_{n\geq 1} K_{\pi,n}$.*

(1) $K_{\pi,n}/K$ is a totally ramified abelian extension of degree $(q-1)q^{n-1}$.

(2) *There are isomorphisms* $\varphi_{\pi,n} : (\mathcal{O}_K/\pi^n)^\times \xrightarrow{\simeq} \mathrm{Aut}_{\mathcal{O}_K}(\Lambda_n) \xrightarrow{\simeq} \mathrm{Gal}(K_{\pi,n}/K)$ *defined by* $\varphi_{\pi,n}(a)(\lambda) = [a]_f(\lambda)$ *for* $\lambda \in \Lambda_n$.

(3) $\pi \in N_{K_{\pi,n}/K} K_{\pi,n}^\times$.

Remark 8.5. The kernel of $\varphi_{\pi,n} : K^\times \to \mathrm{Gal}(K_{\pi,n}/K)$ is $\pi^{\mathbb{Z}} \times (1 + \pi^n \mathcal{O}_K)$. How do we know $\ker \varphi_{\pi,n} = N_{K_{\pi,n}/K} K_{\pi,n}^\times$? (Exercise: Prove this without class field theory.)

Let $f(X) = \pi X + \cdots + X^q$ as before. Choose a nonzero root π_1 such that $f(\pi_1) = 0$. Now choose π_2 such that $f(\pi_2) = \pi_1$. Continuing, choose π_n such that $f(\pi_n) = \pi_{n-1}$. Then we obtain a tower $K \subset K(\pi_1) \subset K(\pi_2) \subset \cdots \subset K(\pi_n)$ such that $[K(\pi_1) : K] = q - 1$ and $[K(\pi_{i+1}) : K(\pi_i)] = q$ for all $i \geq 1$. Moreover, $\pi_i \in \Lambda_n$, so $K(\pi_i) \subset K(\Lambda_i)$ for each i.

The Galois group $\mathrm{Gal}(K_{\pi,n}/K)$ acts on Λ_n and commutes with the $\mathcal{O}_K$-action, giving an embedding $\mathrm{Gal}(K_{\pi,n}/K) \hookrightarrow \mathrm{Aut}_{\mathcal{O}_K}(\Lambda_n) = (\mathcal{O}_K/\pi^n)^\times$. But $(\mathcal{O}_K/\pi^n)^\times$ has $(q-1)q^n$ elements, hence so does $\mathrm{Gal}(K_{\pi,n}/K)$. This proves $K_{\pi,n} = K(\Lambda_n) = K(\pi_n)$ for all n, proving (1) and (2) of the theorem.

For part (3), write $f^{[n]}(x) = \frac{f}{X} \circ f^{(n-1)}(X) = \pi + \cdots + (f^{(n-1)}(X))^q = \pi + \cdots + X^{(q-1)q^{n-1}}$. Then $f^{[n]}(\pi_n) = 0$, so by a degree argument, $f^{[n]}(x)$ is the minimal polynomial of π_n. Thus, $N_{K_{\pi,n}/K}(\pi_n) = (-1)^{(q-1)q^{n-1}} \pi = \pi$ unless q is even and $n = 1$. In the latter case, consider instead $N_{K_{\pi,1}/K}(-\pi_1)$. □

For each π, we have constructed a totally ramified abelian extension $K_\pi = \bigcup_{n \geq 1} K_{\pi,n}$ and a map

$$\begin{aligned} \varphi_\pi : K^\times &\to \mathrm{Gal}(K_\pi/K), \\ \pi &\mapsto 1, \\ u &\mapsto [u^{-1}]_f \qquad \forall u \in \mathcal{O}_K^\times. \end{aligned}$$

From this, it is clear that $K_\pi \cap K^{un} = K$, and we can extend to a map $\varphi_\pi : K^\times \to \mathrm{Gal}(K_\pi K^{un}/K)$ such that $\varphi_\pi|_{K^{un}}$ is as before, and $\varphi_\pi|_{K_\pi}$ is what we just defined.

Here's what we still need to show:

(1) $K_\pi K^{un} = K^{ab}$.

(2) $\varphi = \varphi_\pi$ does not depend on π.

(3) $\varphi|_L : K^\times \to \mathrm{Gal}(L/K)$ has kernel $N_{L/K} L^\times$.

9 2015-02-09: Local Kronecker–Weber

Note that the map φ_π mentioned last time factors as $K^\times \cong \pi^{\mathbb{Z}} \times \mathcal{O}_K^\times \twoheadrightarrow \mathcal{O}_K^\times \to \mathrm{Gal}(K_\pi K^{un}/K)$. Hence, for $a = \pi^n \cdot u$ with $u \in \mathcal{O}_K^\times$,

(1) $\varphi_\pi(a)|_{K^{un}} = (\mathrm{Frob}_K)^n$;

(2) $\varphi_\pi(a)|_{K_\pi} = \varphi_K(u)|_{K_\pi}$, where $\varphi_K(u)(\lambda) = [u^{-1}]_f(\lambda)$ for $\lambda \in \Lambda_f = \bigcup_{n \geq 1} \Lambda_n$.

Recall the statement of local class field theory: $\varphi_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$ is a map such that:

(1) $\varphi_K(a)|_{K^{un}} = (\mathrm{Frob}_K)^{\mathrm{ord}_\pi a}$.

(2) For L/K finite abelian, $\varphi_{L/K} = \varphi_K|_L : K^\times \to \mathrm{Gal}(L/K)$ is surjective with $\ker \varphi_{L/K} = N_{L/K} L^\times$.

Proposition 9.1. *Neither $K_\pi K^{un}$ nor φ_π depends on the choice of π.*

Proof. See Milne's notes. The idea is to show that, given $\varpi = \pi u$ with $u \in \mathcal{O}_K^\times$, for any $f \in \mathcal{F}_\pi$ and $g \in \mathcal{F}_\varpi$, there is an isomorphism $F_f \cong F_g$ of formal groups over $\mathcal{O}_{\widehat{K^{un}}}$. ☐

Theorem 9.2 (Local Kronecker–Weber)**.** $K^{ab} = K_\pi K^{un}$.

Example 9.3. $\mathbb{Q}_p^{ab} = \mathbb{Q}_p(\zeta_{p^\infty}) \cdot \mathbb{Q}_p(\zeta_n : (n,p) = 1)$.

Caution 9.4. We don't have this sort of theorem for global fields, not even for finite abelian extensions.

Our proof of the theorem will proceed as follows:

(I) If $K_\pi \subset L \subset K^{ab}$ with L/K_π totally ramified, then $L = K_\pi$.

(II) If $K_\pi \subset L \subset K^{ab}$ with L/K_π unramified, then $L \subset K_\pi K^{un}$.

(III) If $K_\pi \subset L \subset K^{ab}$ with L/K_π finite of degree m, then there is a totally ramified extension L_t of K_π such that $L \subset L_t K_m^{un} = L K_m^{un}$.

Granting these, if L/K is a finite abelian extension, then $LK_\pi \subset L_t K_m^{un} = L K_m^{un}$ for L_t/K_π totally ramified, so $L_t = K_\pi$. Thus, $L \subset LK_\pi \subset K_\pi K_m^{un} \subset K_\pi K^{un}$. ☐

To see (II), suppose $L = K_\pi(\alpha)$. Descend to finite level: $L'/K_{\pi,m}$ with $L = K_\pi L'$ and $L' = K_{\pi,m}(\alpha)$. Then L'/K factors into $L'/L''/K$ with L''/K unramified and L'/L'' totally ramified. Hence, $L' = K_{\pi,m} L''$, so $L = K_\pi L'' \subset K_\pi K^{un}$.

For (III), $\mathrm{Gal}(LK_m^{un}/K_\pi) \twoheadrightarrow \mathrm{Gal}(K_\pi K_m^{un}/K_\pi) = \mathrm{Gal}(K_m^{un}/K)$ corresponds to $\bigoplus \mathbb{Z}/m_i \twoheadrightarrow \mathbb{Z}/m$, where $m_i \mid m$. This map splits, i.e., $\mathrm{Gal}(LK_m^{un}/K_\pi) = \langle \tau \rangle \times H$. Take $L_t = (LK_m^{un})^{\langle \tau \rangle}$. Then $\mathrm{Gal}(LK_m^{un}/L_t) = \mathrm{Gal}(K_\pi K_m^{un}/K_\pi) = \langle \tau \rangle$.

For (I), see Milne's notes (Lemma 4.9) or the sections on higher ramification in Serre's *Local Fields*. We'll discuss this more next time.

10 2015-02-11: The global Artin map

Last time, we determined that we need the following lemma:

Lemma 10.1. *If $K_\pi \subset L \subset K^{ab}$ with L/K_π totally ramified, then $L = K_\pi$, i.e., K_π is the maximal totally ramified abelian extension of K.*

Using higher ramification groups with the upper numbering, $|G^n/G^{n+1}| \le q = |\mathcal{O}_K/\mathfrak{m}_K|$.

Example 10.2. Let $K = \mathbb{Q}_p$ and $\pi = p$. Choose $f(x) = (1+x)^p - 1 \in \mathcal{F}_p$. Then $f^{(n)}(x) = (1+x)^{p^n} - 1$, and

$$\Lambda_{f,n} = \left\{ x \in \mathfrak{m}_{\overline{\mathbb{Q}_p}} : f^{(n)}(x) = 0 \right\} = \left\{ x \in \overline{\mathbb{Q}_p} : (x+1)^{p^n} = 1 \right\},$$

$$(\mathbb{Q}_p)_{\pi,n} = \mathbb{Q}_p(\Lambda_{f,n}) = \mathbb{Q}_p(\mu_{p^n}).$$

Since $\mathbb{Q}_p^{un} = \bigcup_{p \nmid n} \mathbb{Q}_p(\mu_n)$, we obtain $\mathbb{Q}_p^{ab} = \mathbb{Q}_p(\mu_\infty) := \bigcup_{n \ge 1} \mathbb{Q}_p(\mu_n)$.

Theorem 10.3. *Every finite abelian extension of $\mathbb{Q}_p$ is contained in a local cyclotomic field $\mathbb{Q}_p(\mu_n)$ for some n.*

10.1 Global Kronecker–Weber theorem

This has a global analogue:

Theorem 10.4 (Global Kronecker–Weber)**.** *Every finite abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\mu_n)$ for some n, i.e., $\mathbb{Q}^{ab} = \mathbb{Q}(\mu_\infty)$.*

First, we prove a lemma.

Lemma 10.5. *Let $L/\mathbb{Q}$ be a finite Galois extension, let $G = \mathrm{Gal}(L/K)$, and let S be the set of prime ideals of L that are ramified in $L/\mathbb{Q}$, i.e., $S = \{\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_L : \mathfrak{p} \mid d_L\}$. For $\mathfrak{p} \in S$, let $I(\mathfrak{p})$ be its inertia group. Then $G = \langle I(\mathfrak{p}) : \mathfrak{p} \in S\rangle$.*

Proof. Let $H = \langle I(\mathfrak{p}) : \mathfrak{p} \in S\rangle$. Let $M = L^H$. Then every prime ideal of M is unramified in $M/\mathbb{Q}$. But we know any prime dividing the discriminant d_M is ramified, hence $|d_M| = 1$, i.e., $M = \mathbb{Q}$. □

Moving on to the *proof* of the theorem, let $L/\mathbb{Q}$ be a finite abelian extension. Then $D_\mathfrak{p} = D_{\mathfrak{p}'}$ if $\mathfrak{p} \cap \mathbb{Q} = \mathfrak{p}' \cap \mathbb{Q}$. Since $G = \mathrm{Gal}(L/\mathbb{Q}) = \langle I(\mathfrak{p}) : \mathfrak{p} \mid d_L\rangle$, we have $L_\mathfrak{p} \subset \mathbb{Q}_p(\zeta_{p^{S_p}}, \zeta_n)$.

Let $K = \mathbb{Q}(\zeta_{p^{S_p}} : p \mid d_L)$ and $L' = KL$. Our goal is to show $L' = K$, which implies $L \subset K$. First notice $L'_{pri'} \subset \mathbb{Q}(\zeta_{p^{S_p}}, \zeta_n)$ if $\mathfrak{p}' \cap L = \mathfrak{p}$. So we can assume $L \supset K$ by replacing L with L'. It remains to show $L = K$.

Since $K \subset L$, we have $|G| = [L : \mathbb{Q}] \geq [K : \mathbb{Q}] = \prod_{p \mid d_L} \varphi(p^{S_p})$. On the other hand, $G = \langle I(p) : p \mid d_L\rangle$, so $G \leq \prod_p |I(p)| \leq \prod_p \varphi(p^{S_p})$. Thus, $|G| = \prod_p \varphi(p^{S_p})$ and $L = K$. □

10.2 Global Artin map

Let L/K be a finite abelian extension of global fields. There is a cycle $\mathfrak{m}$ and a map

$$\varphi_\mathfrak{m} : I_K(\mathfrak{m}) \twoheadrightarrow \mathrm{Gal}(L/K),$$
$$\varphi_\mathfrak{m}(\mathfrak{p}) = (\mathrm{Frob}_\mathfrak{p})\big|_L = (\mathfrak{p}, L/K) = \left(\frac{L/K}{\mathfrak{p}}\right),$$

satisfying the following conditions:

(1) $P_K(\mathfrak{m}) = \{\alpha\mathcal{O}_K : \alpha \equiv 1 \pmod{^*\, \mathfrak{m}}\}$.

(2) $\varphi_\mathfrak{m}$ is surjective.

(3) $\ker \varphi_\mathfrak{m} = P_K(\mathfrak{m}) \cdot N_{L/K} I_L(\mathfrak{m})$.

Example 10.6. Let us describe the reciprocity law for $\mathbb{Q}$. Given a finite abelian extension $L/\mathbb{Q}$, by Kronecker–Weber, $L \subset \mathbb{Q}(\zeta_m)$ for some m. (Note that $\mathbb{Q}(\zeta_m)$ is the ray class field of m.) Take

$$\varphi_m : I_\mathbb{Q}(m) \to \mathrm{Gal}(L/\mathbb{Q}),$$
$$p \mapsto \left(\frac{L/\mathbb{Q}}{p}\right).$$

Let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Take $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ such that $\tau|_L = \sigma$. Then $\tau = \tau_a : \zeta_m \mapsto \zeta_m^a$ for some $a \in (\mathbb{Z}/m)^\times$. By Dirichlet, there are infinitely many primes p such that $p \equiv a \pmod m$. So

$$\varphi_m(p) = \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{p}\right) = \tau_p = \tau_a.$$

11 2015-02-13: Higher ramification groups

Guest lecture by Vlad Matei. A reference for higher ramification group is [S, ch. IV].

Our goal for today is to prove that, if L/K_π is totally ramified, then $L = K_\pi$.

11.1 Lower ramification groups

Definition 11.1 (Lower ramification groups)**.** Let K be a nonarchimedean local field and L/K a finite Galois extension. For $n \geq -1$, define

$$G_i = \left\{\sigma \in G : \sigma(x) \equiv x \pmod{\pi_L^{n+1}}\ \forall x \in \mathcal{O}_L\right\}.$$

Note that $G_{-1} = G$ is the whole Galois group, $G_0 = I$ is the inertia group, and $G_n \supseteq G_{n+1}$ for all n. We can also characterize these as

$$G_n = \ker(G \to \mathrm{Aut}(\mathcal{O}_L/\pi^{n+1}\mathcal{O}_L)),$$

which makes it clear that G_n is a normal subgroup of G.

Proposition 11.2. *With notation as above,*

(1) $G_n = \{\sigma \in G : v(\sigma(\pi_L) - \pi_L) > n\}$.

(2) $\bigcap_n G_n = \{1\}$.

(3) $G_0/G_1 \hookrightarrow k_L^\times$*, and for* $n \geq 1$, $G_n/G_{n+1} \cong (k_L, +)$*, where* k_L *is the residue field of* L*.*

Proof. (1) Reduce to L/K totally ramified. Then $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ for π_L a uniformizer. If $\sigma(\pi_L) \equiv \pi_L \pmod{\pi_L^{n+1}}$, then it follows for polynomials in π_L.

(2) If $\sigma \neq 1$, then $\sigma(\pi_L) \neq \pi_L$, so $v(\sigma(\pi_L) - \pi_L)$ is finite. Hence, $\sigma \notin G_n$ for sufficiently large n.

(3) See [S, IV.2.6]. $\square$

What happens for $L = K_{\pi,m}$? We have an isomorphism $\mathcal{O}_K^\times/(1+\mathfrak{m}^n) \xrightarrow{\simeq} G$ sending $(1+\mathfrak{m}^i)/(1+\mathfrak{m}^n)$ onto G_{q^i-1}.

11.2 Upper ramification groups

Define $\varphi(u) = \int_0^u \frac{dt}{(G_0:G_t)}$. This is continuous, piecewise linear, concave, strictly increasing, and satisfies $\varphi(0) = 0$ and $\varphi'(u) = \frac{1}{(G_0:G_u)}$ when φ is linear at u.

From the above, φ has an inverse map ψ, which is continuous, piecewise linear, convex, strictly increasing, and satisfies $\psi(0) = 0$ and $\psi'(u) = (G_0 : G_u)$ when ψ is linear at u. Moreover, if v is an integer, so is $\psi(v)$.

Definition 11.3 (Upper ramification groups)**.** Define $G^v = G_{\psi(v)}$, so that $G^{\varphi(u)} = u$ for all $u \geq -1$.

Proposition 11.4 ([S, IV.3.14])**.** *Let H be a normal subgroup of G. Then $(G/H)^v = G^v H/H$.*

Note 11.5. For $K_{\pi,n}$, we have $G^k = G_{q^k-1}$ for all integers $k \geq 1$, where q is the cardinality of the residue field.

The upper ramification groups of K_π are limits of higher ramification groups for $K_{\pi,n}$.

A *jump* in the filtration of G by upper ramification groups is an index j such that $G^j \neq G^{j+\varepsilon}$ for every $\varepsilon > 0$.

Theorem 11.6 (Hasse–Arf)**.** *For G abelian, jumps are integers. (This can fail for G non-abelian.)*

11.3 Main result

Let $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(L/K_\pi)$, so $G/H = \mathrm{Gal}(K_\pi/K)$. We have an exact commutative diagram

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G^{n+1} \cap H & \longrightarrow & G^{n+1} & \longrightarrow & (G/H)^{n+1} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G^n \cap H & \longrightarrow & G^n & \longrightarrow & (G/H)^n & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \frac{G^n \cap H}{G^{n+1} \cap H} & \longrightarrow & G^n/G^{n+1} & \longrightarrow & \frac{(G/H)^n}{(G/H)^{n+1}} & \longrightarrow & 1
\end{array}$$

Looking at cardinalities of the bottom row, we obtain the result. $\square$

12 2015-02-16: Global class field theory

12.1 Statement of global class field theory

Today, we begin our study of global class field theory. Let K be a global field (i.e., a finite extension of $\mathbb{Q}$ or $\mathbb{F}_q(x)$). For a modulus $\mathfrak{m}$, recall that

$$\begin{aligned} I_K(\mathfrak{m}) &= \{\text{fractional ideals of } K \text{ prime to } \mathfrak{m}\}, \\ P_K(\mathfrak{m}) &= \{\alpha\mathcal{O}_K : \alpha \equiv 1 \pmod{^* \mathfrak{m}}\} \subset I_K(\mathfrak{m}), \end{aligned}$$

where $\alpha \equiv 1 \pmod{^* \mathfrak{m}}$ means that $\operatorname{ord}_{\mathfrak{p}}(\alpha - 1) \geq 1$ if $\mathfrak{p} \mid \mathfrak{m}_f$ and $\sigma(\alpha) > 0$ for all $\sigma : K \hookrightarrow \mathbb{R}$, $\sigma \in \mathfrak{m}_\infty$.

Theorem 12.1 (Global class field theory)**.** *Let L/K be a finite abelian extension. There exists a modulus $\mathfrak{m} = \mathfrak{m}_f \cdot \mathfrak{m}_\infty$ such that:*

(1) The Artin map $\varphi_{L,\mathfrak{m}} : I_K(\mathfrak{m}) \to \operatorname{Gal}(L/K)$ is surjective, and $\ker \varphi_{L,\mathfrak{m}} = P_K(\mathfrak{m}) \cdot N_{L/K} I_L(\mathfrak{m})$.

(2) For every subgroup H of $I_K(\mathfrak{m})$ of finite index and containing $P_K(\mathfrak{m})$, there is a finite abelian extension L/K such that $H = P_K(\mathfrak{m}) \cdot N_{L/K} I_L(\mathfrak{m})$.

Fact 12.2. Suppose $\mathfrak{n} \subset \mathfrak{m}$. If the theorem works for $\mathfrak{m}$, then it also works for $\mathfrak{n}$. The biggest ideal $\mathfrak{m}$ which works for L/K is called the *conductor* of L/K, denoted $\mathfrak{f}_{L/K}$.

12.2 Hecke characters and Hecke L-functions

Definition 12.3. A *Hecke character* of K of modulus $\mathfrak{m}$ is a group homomorphism $\chi : I_K(\mathfrak{m}) \to \mathbb{C}^\times$ such that there is a continuous character

$$\chi_\infty : K_\infty^\times = \prod_{\sigma : K \hookrightarrow \mathbb{R}} K_\sigma^\times \times \prod_{\sigma, \overline{\sigma} : K \hookrightarrow \mathbb{C}} K_\sigma^\times \to \mathbb{C}^\times$$

satisfying $\chi(\alpha\mathcal{O}_K) = \chi_\infty(\alpha)^{-1}$ for $\alpha\mathcal{O}_K \in P_K(\mathfrak{m})$. (When we work with adeles later on, we will see the reason for the inverse here.)

If $\mathfrak{n} \subset \mathfrak{m}$, then any Hecke character of K of modulus $\mathfrak{m}$ is also a Hecke character of modulus $\mathfrak{n}$. The biggest modulus for which χ is a Hecke character is called the *conductor* of χ, denoted f_χ. A Hecke character χ of modulus $\mathfrak{m}$ is called *primitive* if $\mathfrak{m} = f_\chi$.

For a Hecke character χ, define the *Hecke L-function* for $\operatorname{Re} s \gg 0$ by

$$L(s, \chi) = \sum_{\substack{0 \neq \mathfrak{a} \lhd \mathcal{O}_K \\ (\mathfrak{a}, \mathfrak{f}_\chi) = 1}} \frac{\chi(\mathfrak{a})}{(N\mathfrak{a})^s} = \prod_{\mathfrak{p} \nmid \mathfrak{f}_\chi} \left(1 - \chi(\mathfrak{p})(N\mathfrak{p})^{-s}\right)^{-1}.$$

Theorem 12.4 (Hecke)**.** *$L(s, \chi)$ has meromorphic continuation to the complex plane with at most a simple pole at $s = 1$, which happens exactly when χ is the trivial character. Moreover, there exists $N \in \mathbb{C}$ and a product of Γ-functions $L_\infty(s, \chi)$ such that the* completed L-function *$\Lambda(s, \chi) = N^{s/2} L_\infty(s, \chi) L(s, \chi)$ satisfies the functional equation*

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

where $w(\chi) \in \mathbb{C}$ is the root number of χ and satisfies $|w(\chi)| = 1$.

Example 12.5. Let $\chi = \mathbb{1}$ be the trivial character $\mathfrak{a} \mapsto 1 : I_K \to \mathbb{C}^\times$. Then

$$L(s, \mathbb{1}) = \sum_{0 \neq \mathfrak{a} \lhd \mathcal{O}_K} \frac{1}{(N\mathfrak{a})^s} = \chi_K(s).$$

Example 12.6. Let $\chi : (\mathbb{Z}/N)^\times \to \mathbb{C}^\times$ be a Dirichlet character. This extends to $\tilde{\chi} : I_{\mathbb{Q}}(N) \to \mathbb{C}^\times$, defined by $n\mathbb{Z} \mapsto \chi(n)$. We define $\chi_\infty(-1) = \chi(-1)$. If $\chi(-1) = 1$, we can take the modulus $\mathfrak{m} = N\mathbb{Z}$; otherwise, if $\chi(-1) = -1$, we must use the modulus $\mathfrak{m} = (N\mathbb{Z}) \cdot \infty$.

Now let us reformulate global class field theory in terms of Hecke characters. Let L/K be a finite abelian extension, and let $\varphi_{L/K,\mathfrak{m}} : I_K(\mathfrak{m}) \twoheadrightarrow \mathrm{Gal}(L/K)$ be the Artin map. If $\rho : \mathrm{Gal}(L/K) \to \mathbb{C}^\times$ is a Galois character, then

$$\chi = \rho \circ \varphi_{L/K,\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathbb{C}^\times$$

is a group homomorphism satisfying $\chi(\alpha\mathcal{O}_K) = 1$ for $\alpha \equiv 1 \pmod{^* \mathfrak{m}}$. Hence, χ is a Hecke character of K of finite order.

Theorem 12.7 (Hecke)**.** *The above construction induces a bijection*

$$\left\{ \begin{matrix} \text{Hecke characters of} \\ K \text{ of finite order} \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{Galois characters} \\ \text{of } \mathrm{Gal}(\overline{K}/K) \end{matrix} \right\} = \left\{ \begin{matrix} \text{1-dim. rep'n of} \\ \mathrm{Gal}(\overline{K}/K) \end{matrix} \right\}.$$

13 2015-02-18: L-functions of Hecke characters

Last time, we stated the connection between Hecke characters and 1-dimensional Galois representations. Today, we explore this further.

Theorem 13.1. *Let χ be a Hecke character of finite order. Let*

$$L(s, \chi) = \prod_{\mathfrak{p} \text{ finite}} \left(1 - \chi(\mathfrak{p})(N\mathfrak{p})^{-s}\right)^{-1},$$

where we define $\chi(\mathfrak{p}) = 0$ if $\mathfrak{p} \mid \mathfrak{f}_\chi$. Then:

(1) $L(s, \chi)$ is absolutely convergent for $\mathrm{Re}\, s > 1$.

(2) $L(s, \chi)$ has analytic continuation to the complex plane, with a simple pole at $s = 1$ if and only if $\chi = \mathbb{1}$ is the trivial character, in which case

$$\operatorname*{Res}_{s=1} L(s, \mathbb{1}) = \operatorname*{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K \sqrt{|d_K|}},$$

where r_1 is the number of real places, r_2 is the number of conjugate pairs of complex places, h_K is the class number, R_K is the regulator, w_K is the root number, and d_K is the discriminant.

(3) $L(s, \chi)$ satisfies the functional equation

$$L(s, \chi) = w(\chi) \cdot (\Gamma\text{-factors}) \cdot L(1 - s, \chi).$$

(4) $L(1,\chi) \neq 0$.

Remark 13.2. One can check explicitly that $L(1,\chi) \neq 0$ by studying $\log L(s,\chi)$.

Definition 13.3 (Dirichlet density)**.** Let A be a set of prime ideals of K. The *Dirichlet density* of A is

$$d(A) = \lim_{s\to 1^+} = \frac{\log \prod_{\mathfrak{p}\in A}(1-(N\mathfrak{p})^{-s})^{-1}}{\log \zeta_K(s)}.$$

Theorem 13.4 (Chebotarev density theorem)**.** *Let L/K be a finite Galois extension. Then*

$$\mathrm{Spl}_{L/K} = \left\{\mathfrak{p} \in M_K^f : \mathfrak{p} \textit{ splits completely in } L\right\}$$

has Dirichlet density $[L:K]^{-1}$. In particular, $\mathrm{Spl}_{L/K}$ is infinite.

Proof. Observe that

$$\begin{aligned}
\log \zeta_L(s) &= \sum_{\mathfrak{P}}\sum_{m} \frac{1}{m(N\mathfrak{P})^{ms}} = \sum_{\mathfrak{P}} \frac{1}{(N\mathfrak{P})^s} + \mathrm{O}(1) \\
&= \sum_{\mathfrak{p}} \sum_{f_{\mathfrak{P}/\mathfrak{p}}=1} \frac{1}{(N\mathfrak{p})^s} + \sum_{\mathfrak{p}} \sum_{f=f_{\mathfrak{P}/\mathfrak{p}}\geq 2} \frac{1}{(N\mathfrak{p})^{fs}} + \mathrm{O}(1) \\
&= [L:K] \sum_{\substack{\mathfrak{p} \\ f_{\mathfrak{P}/\mathfrak{p}}=1}} \frac{1}{(N\mathfrak{p})^s} + \mathrm{O}(1) \\
&= [L:K] \sum_{\mathfrak{p}\in \mathrm{Spl}_{L/K}} \frac{1}{(N\mathfrak{p})^s} + \mathrm{O}(1).
\end{aligned}$$

Thus,

$$d(\mathrm{Spl}_{L/K}) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in \mathrm{Spl}_{L/K}} (N\mathfrak{p})^{-s}}{\log \zeta_K(s)} = \frac{1}{[L:K]} \lim_{s\to 1^+} \frac{\log \zeta_L(s)}{\log \zeta_K(s)} = \frac{1}{[L:K]}. \qquad \square$$

Corollary 13.5. *Let L/K and M/K be two finite Galois extensions of global fields. If $\mathrm{Spl}_{L/K} = \mathrm{Spl}_{M/K}$, then $L = M$.*

Proof. Apply the Chebotarev density theorem to LM. $\square$

Theorem 13.6. *Let L/K be a finite abelian extension with Galois group G. Then*

$$\zeta_L(s) = \prod_{\chi\in\hat{G}} L(s,\chi),$$

where $\hat{G} = \mathrm{Hom}(G,\mathbb{C}^\times)$ is the group of characters of G.

Corollary 13.7. *$\zeta_L(s)/\zeta_K(s)$ is holomorphic and is neither 0 nor ∞ at $s=1$.*

Proof. Observe that $\dfrac{\zeta_L(s)}{\zeta_K(s)} = \displaystyle\prod_{\substack{\chi\in\hat{G}\\ \chi\neq \mathbb{1}}} L(s,\chi)$, which has the desired properties. $\square$

Theorem 13.8 (Dirichlet density theorem)**.** *For $\sigma \in \mathrm{Gal}(L/K)$, define*

$$A(\sigma) = \left\{ \mathfrak{p} \in M_K^f : e_{L/K}(\mathfrak{p}) = 1,\ \varphi_{L/K}(\mathfrak{p}) = \sigma \right\}.$$

Then $d(A(\sigma)) = [L : K]^{-1}$.

Example 13.9. Let $L = \mathbb{Q}(\zeta_m)$, $K = \mathbb{Q}$, and $\sigma = \sigma_a : \zeta_m \mapsto \zeta_m^a$. Then we recover the original Dirichlet density theorem:

$$\begin{aligned}
\log \prod_{\mathfrak{p} \in A(\sigma)} (1 - N\mathfrak{p})^{-s} &= \sum_{\mathfrak{p} \in A(\sigma)} (N\mathfrak{p})^{-s} + \mathrm{O}(1) = \frac{1}{n} \sum_{\mathfrak{p}} \sum_{\chi \in \hat{G}} \chi^{-1}(\sigma)\chi(\mathfrak{p})(N\mathfrak{p})^{-s} \\
&= \frac{1}{n} \sum_{\chi \in \hat{G}} \chi^{-1}(\sigma) \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{(N\mathfrak{p})^s} = \frac{1}{n} \sum_{\chi \in \hat{G}} \chi^{-1}(\sigma) \log L(s, \chi) \\
&= \frac{1}{n} \log \zeta_K(s) + \frac{1}{n} \sum_{\mathbb{1} \neq \chi \in \hat{G}} \chi^{-1}(\sigma) \log L(s, \chi).
\end{aligned}$$

14 2015-02-20: Character version of CFT

Recall the classical statement of class field theory:

Theorem 14.1 (Global class field theory)**.** *For each finite abelian Galois extension L/K of number fields, there is a cycle $\mathfrak{m}$ of K such that*

$$\begin{aligned}
\varphi_{L/K,\mathfrak{m}} : I_K(\mathfrak{m}) &\to \mathrm{Gal}(L/K), \\
\mathfrak{p} &\mapsto \mathrm{Frob}_{\mathfrak{p},L/K}
\end{aligned}$$

is surjective and has kernel $P_K(\mathfrak{m}) \cdot N_{L/K} I_L(\mathfrak{m})$, where $P_K(\mathfrak{m}) = \{\alpha \mathcal{O}_K : \alpha \equiv 1 \pmod{^*\ \mathfrak{m}}\}$.

We reformulate this in the language of Hecke characters. There is a bijective correspondence

$$\begin{gathered}
\left\{ \begin{matrix} \text{Hecke characters of} \\ K \text{ of finite order} \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{1-dim. representations} \\ \text{of } \mathrm{Gal}(\overline{K}/K) \end{matrix} \right\}, \\
\chi \longleftrightarrow \rho, \\
\chi(\mathfrak{p}) = \rho(\mathrm{Frob}_{\mathfrak{p},L/K}).
\end{gathered}$$

Theorem 14.2. *We have $\zeta_L(s) = \prod_{\chi \in \mathrm{Gal}(L/K)^\wedge} L(s, \chi)$. Hence, $\zeta_L(s)/\zeta_K(s)$ is holomorphic on $\mathbb{C}$.*

14.1 Density theorems

Theorem 14.3. *Let L/K be a finite abelian Galois extension, and let $\sigma \in \mathrm{Gal}(L/K)$. Then*

$$A(\sigma) = \left\{ \mathfrak{p} \in M_K^f : \mathrm{Frob}_{\mathfrak{p},L/K} = \sigma \right\}$$

has Dirichlet density $[L : K]^{-1}$.

More generally:

Theorem 14.4 (Chebotarev density theorem)**.** *Let L/K be a finite Galois extension with $G = \mathrm{Gal}(L/K)$. Let C be a conjugacy class in G. Then*

$$A(C) = \left\{ \mathfrak{p} \in M_K^f : \mathrm{Frob}_{\mathfrak{p},L/K} = C \right\}$$

has Dirichlet density $\frac{|C|}{|G|}$.

Proof. See [M, VIII.7.4]. □

14.2 Higher-dimensional Galois representations

To understand a group, we should study its representations. In particular, we can study Galois representations $\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(V) = \mathrm{GL}_n(\mathbb{C})$, where V is a finite-dimensional $\mathbb{C}$-vector space. For topological reasons, such representations factor through a finite quotient $\mathrm{Gal}(L/K)$, so we can study representations $\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}(V)$.

Let $\mathfrak{B}$ be a prime of L unramified over a prime $\mathfrak{p}$ of K. We obtain a conjugacy class $\mathrm{Frob}_{\mathfrak{B}/\mathfrak{p}}$, and $\rho(\mathrm{Frob}_{\mathfrak{B}/\mathfrak{p}}$ is a linear operator on V. Define

$$L_{\mathfrak{p}}(s,\rho) = \det\left(1 - (N\mathfrak{p})^{-s}\rho(\mathrm{Frob}_{\mathfrak{B}/\mathfrak{p}})\right)^{-1}.$$

This depends only on $\mathfrak{p}$. In general, to account for ramification, let $I = I_{\mathfrak{B}/\mathfrak{p}}$ be the inertia group. Then define

$$L_{\mathfrak{p}}(s,\rho) = \det\left(1 - (N\mathfrak{p})^{-s}\rho(\mathrm{Frob}_{\mathfrak{B}/\mathfrak{p}})\big|_{V^I}\right)^{-1}.$$

Multiplying these local factors, we obtain the *Artin L-function*

$$L(s,\rho) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(s,\rho).$$

15 2015-02-23: Artin L-functions and adeles

15.1 Artin L-functions

Last time, we defined the L-function $L(s,\rho)$ associated to an n-dimensional Galois representation $\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(V)$.

Theorem 15.1 (Artin)**.** *$L(s,\rho)$ has meromorphic continuation to the whole complex plane and satisfies a functional equation $L(s,\rho) = (\Gamma$-factor$) \cdot L(1-s,\rho)$.*

Conjecture 15.2 (Artin)**.** *IF ρ is irreducible and nontrivial, then $L(s,\rho)$ is holomorphic.*

Conjecture 15.3 (Langlands correspondence)**.** *There exists an irreducible cuspidal automorphic representation π of $\mathrm{GL}_n(K)$ such that $L(s,\rho) = L(s,\pi)$.*

Remark 15.4. Galois representations for which Langlands' conjecture is true are called *modular*. Modularity is known for representations $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$.

15.2 Adelic language

Let K be a global field, and let M_K be the set of primes (finite or infinite) of K. For $v \in M_K$, let K_v be the completion of K at v. More explicitly, each prime v is associated with an absolute value:

- If $\sigma : K \hookrightarrow \mathbb{R}$ is a real prime, then $|x|_\sigma = |\sigma(x)|$.
- If $\sigma, \overline{\sigma} : K \hookrightarrow \mathbb{C}$ is a complex prime, then $|x|_\sigma = |\sigma(x)|^2$.
- If $\mathfrak{p}$ is a finite prime, then $|x|_\mathfrak{p} = (N\mathfrak{p})^{-\operatorname{ord}_\mathfrak{p} x}$.

Proposition 15.5 (Product formula)**.** $\displaystyle\prod_{v \in M_K} |x|_v = 1$ *for all* $x \in K^\times$*.*

Definition 15.6 (Restricted products)**.** Let $(R_i)_{i \in I}$ be a family of rings, and for each $i \in I$, let $\mathcal{O}_{R_i}$ be a subring of R_i. The *restricted product* $\coprod\!\!\coprod_{i \in I}(R_i, \mathcal{O}_{R_i})$ is the ring of all $(x_i)_i \in \prod_{i \in I} R_i$ such that $x_i \in \mathcal{O}_{R_i}$ for all but finitely many $i \in I$.

If each R_i is a topological ring, then we give the restricted product the topology generated by the open basis of sets of the form $U = \prod_i U_i$, where $U_i \subset R_i$ is open and $U_i = \mathcal{O}_{R_i}$ for almost all i.

Definition 15.7. The *ring of adeles* of K is the restricted product

$$\mathbb{A}_K = \coprod\!\!\coprod_v (K_v, \mathcal{O}_{K_v}).$$

Fact 15.8. $K \hookrightarrow \mathbb{A}_K$ is discrete, and $\mathbb{A}_K = K + \widehat{\mathcal{O}}_K + K_\infty$ (or $K \cdot \widehat{\mathcal{O}}_K \cdot K_\infty$), where $K_\infty = \prod_{v \mid \infty} K_v$, $\widehat{\mathcal{O}}_K = \prod_{v \nmid \infty} \mathcal{O}_{K_v}$, and $K_f = \mathbb{A}_{K,f} = \coprod\!\!\coprod_{v \nmid \infty} K_v$.

Moreover, $\mathbb{A}_K$ is locally compact, and admits a Haar measure $dx = \prod_v dx_v$, where $dx_v = |dx|$ on $\mathbb{R}$, $dx_v = |dz \wedge d\overline{z}|$ on $\mathbb{C}$, and $\int_{\mathcal{O}_{K_\mathfrak{p}}} dx_\mathfrak{p} = 1$ on $K_\mathfrak{p}$.

Definition 15.9. The *group of ideles* of K is $\mathbb{A}_K^\times$, the group of units of $\mathbb{A}_K$. We give $\mathbb{A}_K^\times$ the topology induced by the open basis of $U = \prod_v U_v$ with $U_v \subset K_v^\times$ open and $U_v = \mathcal{O}_v^\times$ for almost all v.

16 2015-02-25: Adeles and ideles

Recall that K embeds into $\mathbb{A}_K$ as a discrete subspace. Moreover, the quotient $K \backslash \mathbb{A}_K$ is compact.

Theorem 16.1. *Let* $\psi : K \backslash \mathbb{A}_K \to \mathbb{C}^1$ *be a nontrivial additive character. Then*

$$\operatorname{Hom}(K \backslash \mathbb{A}_K, \mathbb{C}^\times) = \{\psi_a : a \in K\},$$

where $\psi_a(x) = \psi(ax)$*.*

16.1 Ideles

We defined the group of ideles to be $\mathbb{A}_K^\times$, the group of units of $\mathbb{A}_K$. We equip this with a Haar measure $d^\times x = \prod_v d^\times x_v$, where

$$d^\times x_v = \begin{cases} (1-(N\mathfrak{p}_v)^{-1})\,\frac{dx_v}{|x_v|_v} & \text{if } v \nmid \infty, \\ \frac{dx_v}{|x_v|_v} & \text{if } v \mid \infty. \end{cases}$$

Hence, we have $\mathrm{vol}(\mathcal{O}_v^\times, d^\times x_v) = 1$.

If $\mathcal{O}_K$ is the ring of integers in $\mathbb{A}_K$, then $\mathcal{O}_K^\times$ is the maximal compact open subgroup of $(\mathbb{A}_K^\times)_f = K_f^\times$.

Lemma 16.2. *Let $\mathbb{A}_K^1 = \left\{x = (x_v) \in \mathbb{A}_K^\times : |x|_{\mathbb{A}} = \prod_v |x_v|_v = 1\right\}$. Then $K^\times \hookrightarrow \mathbb{A}_K^1$ is discrete and $K^\times\backslash\mathbb{A}_K^1$ is compact. Moreover, we have an exact sequence*

$$1 \to K^\times\backslash\mathbb{A}_K^1 \to K^\times\backslash\mathbb{A}_K^\times \to \mathbb{R}_{>0} \to 1.$$

Definition 16.3. The group $K^\times\backslash\mathbb{A}_K^\times$ is called the *idele class group*. It is a locally compact abelian group, so we can do Fourier analysis on $K^\times\backslash\mathbb{A}_K^\times$.

We have a map

$$\mathbb{A}_K^\times \to I_K = \{\text{fractional ideals of } K\},$$
$$x = (x_v) \mapsto (x) = x\mathcal{O}_K = x_f\widehat{\mathcal{O}}_K \cap K = \prod_{v\nmid\infty} \mathfrak{p}_v^{\mathrm{ord}_v x_v}$$

which restricts to $x \mapsto (x) = x\mathcal{O}_K : K^\times \to P_K$.

Proposition 16.4. *The above maps induce an isomorphism $K^\times\backslash\mathbb{A}_K^\times/\widehat{\mathcal{O}}_K^\times K_\infty^\times \xrightarrow{\simeq} \mathrm{Cl}(K)$, where $\mathrm{Cl}(K)$ is the ideal class group of K.*

Theorem 16.5. *Let $\mathfrak{m}$ be a cycle of K. Then we have a natural isomorphism*

$$K^\times\backslash\mathbb{A}_K^\times/\mathcal{U}_{\mathfrak{m},f}\mathcal{U}_{\mathfrak{m},\infty} \xrightarrow{\simeq} \mathrm{Cl}_K(\mathfrak{m}) = I_K(\mathfrak{m})/P_K(\mathfrak{m}),$$

where

$$\mathcal{U}_{\mathfrak{m},f} = \prod_{v\nmid\infty}(1+\mathfrak{m}_v)\cap\mathcal{O}_v^\times = \prod_{v\nmid\mathfrak{m}}\mathcal{O}_v^\times \prod_{v\mid\mathfrak{m}_f}(1+\mathfrak{p}_v^{\mathrm{ord}_v \mathfrak{m}_f}),$$
$$\mathcal{U}_{\mathfrak{m},\infty} = \prod_{v\mid\mathfrak{m}_\infty}(K_v^\times)^+ \prod_{\substack{v\nmid\mathfrak{m}_\infty \\ v\mid\infty}} K_v^\times,$$

where $(K_v^\times)^+$ denotes the connected component of $1 \in K_v^\times$ (i.e., $\mathbb{R}_{>0}$ for real places and $\mathbb{C}^\times$ for complex places).

Define $\lambda_v : K_v^\times \to \mathrm{Cl}_K(\mathfrak{m})$ for $v \nmid \mathfrak{m}$ by $\lambda_v(x_v) = \mathfrak{p}_v^{\mathrm{ord}_v x_v}$ for $v \nmid \infty$, and $\lambda_v(x_v) = \mathcal{O}_K$ for $v \mid \infty$.

Fact 16.6 (Approximation theorem). Let S be a finite set of primes and $K_S^\times = \prod_{v\in S} K_v^\times$. Then $K^\times \hookrightarrow K_S^\times$ is dense. In particular, for any open subgroup U_S of $K_S^\times$, $K^\times U_S = K_S^\times$. Consequently, $\mathbb{A}_K^\times = K^\times U_S \coprod_{v\notin S} K_v^\times = (\mathbb{A}_K^S)^\times$.

Returning to the theorem, take $S = \{v : v \mid \mathfrak{m}\}$, and denote $S_f = \{v \in S : v \nmid \infty\}$ and $S_\infty = \{v \in S : v \mid \infty\}$. Then

$$\mathcal{U}_S := (\mathcal{U}_{\mathfrak{m},f}\mathcal{U}_{\mathfrak{m},\infty} \cap K_S^\times = \prod_{v\in S_f} (1 + \mathfrak{p}_v^{\operatorname{ord}_v \mathfrak{m}_f}) \prod_{v\in S_\infty} (K_v^\times)^+.$$

Hence, $\mathbb{A}_K^\times = K^\times \mathcal{U}_S \coprod_{v\notin S} K_v^\times$. Define $\lambda : \mathbb{A}_K^\times \to \mathrm{Cl}_K(\mathfrak{m})$ to satisfy $\lambda|_{K^\times \mathcal{U}_S} = 1$ and $\lambda|_{K_v^\times} = \lambda_v$. One can check that this is well-defined, after which bijectivity is clear. □

17 2015-02-27: Adelic reciprocity law

Recall that $K^\times \hookrightarrow \mathbb{A}_K^\times$ is discrete. The approximation theorem tells us that, for any finite set of primes S and any open compact subgroup U of $K_S^\times$, $\mathbb{A}_K^\times = K^\times U (\mathbb{A}_K^S)^\times$, where $\mathbb{A}_K^S = \coprod_{v\notin S} K_V$.

Proposition 17.1 (Strong approximation)**.** *For any prime v_0, the map $K^\times \hookrightarrow (\mathbb{A}_K^{(v_0)})^\times := \coprod_{v\neq v_0} K_v^\times$ is discrete. However, for any set of* at least two *primes S, the map $K^\times \hookrightarrow (\mathbb{A}_K^S)^\times$ is dense.*

Last time, we asserted that the map

$$\lambda : K^\times \backslash \mathbb{A}_K^\times / \mathcal{U}_\mathfrak{m} \xrightarrow{\simeq} \mathrm{Cl}_K(\mathfrak{m}) = I_K(\mathfrak{m})/P_K(\mathfrak{m})$$

is an isomorphism. The map is constructed as follows:

(1) Construct the map $\lambda_v : K_v^\times \to I_K(\mathfrak{m})/P_K(\mathfrak{m})$ for unramified primes $v \nmid \mathfrak{m}$.

(2) Use the approximation theorem to extend the map to $K^\times \backslash \mathbb{A}_K^\times$.

(3) Define the map $\lambda : \mathbb{A}_K^\times \to K^\times \backslash \mathbb{A}_K^\times \to I_K(\mathfrak{m})/P_K(\mathfrak{m})$.

(4) Define $\lambda_v : K_v^\times \to I_K(\mathfrak{m})/P_K(\mathfrak{m})$ for *all* v (not just unramified primes).

Theorem 17.2 (Adelic version of the reciprocity law)**.** *Let K be a global field. There exists a unique continuous group homomorphism $\varphi_K : \mathbb{A}_K^\times \to \mathrm{Gal}(K^{ab}/K)$ such that:*

(1) $\ker \varphi_K = \overline{K^\times \cdot (K_\infty^\times)^0} \supset K^\times$.

(2) For any finite abelian extension L/K, the composition

$$\varphi_{L/K} : \mathbb{A}_K^\times \xrightarrow{\varphi_K} \mathrm{Gal}(K^{ab}/K) \twoheadrightarrow \mathrm{Gal}(L/K)$$

is surjective, and $\ker \varphi_{L/K} = K^\times \cdot N_{L/K}\mathbb{A}_L^\times$.

(3) If $\mathfrak{p}$ is unramified in L/K, then $\varphi_{L/K}(\pi_\mathfrak{p}) = \mathrm{Frob}_{\mathfrak{p},L/K}$ for any local uniformizer $\pi_\mathfrak{p}$ of $K_\mathfrak{p}$.

Remark 17.3 (Open subgroups). For $v \nmid \infty$, $K_v^\times$ has a basis near 1 of compact open subgroups

$$\mathcal{O}_{K_v}^\times \supset 1 + \mathfrak{p}_v \supset 1 + \mathfrak{p}_v^2 \supset \dots .$$

If π_v is a uniformizer for $\mathcal{O}_{K_v}^\times$, we have $\mathfrak{p}_v = \pi_v \mathcal{O}_{K_v}$.

For $v \mid \infty$, this is not the case: $\mathbb{R}^\times$ has only two open subgroups, $\mathbb{R}^\times$ and $\mathbb{R}_{>0}$, while $\mathbb{C}^\times$ has no proper open subgroups.

Theorem 17.4 (Adelic existence theorem). *Let U_f be a compact open subgroup of $\mathbb{A}_f^\times$ of finite index. Let U_∞ be an open subgroup of $K_\infty^\times$. There is a unique finite abelian extension L/K such that $K^\times \cdot U_f \cdot U_\infty = K^\times \cdot N_{L/K}\mathbb{A}_L^\times$, i.e., $\varphi_{L/K}$ gives an isomorphism $K^\times \backslash \mathbb{A}_K^\times / U_f U_\infty \xrightarrow{\simeq} \mathrm{Gal}(L/K)$.*

To recover the classical formulation of global class field theory, observe that we have a commutative diagram

$$\begin{tikzcd}
K^\times \backslash \mathbb{A}_K^\times \arrow[r, "\varphi_K = \lim_{\mathfrak{m}} \varphi_{K,\mathfrak{m}}"] \arrow[d] \arrow[dr, "\varphi_{K,\mathfrak{m}}"] \arrow[ddr, "\varphi_{K,\mathfrak{n}}"'] & \mathrm{Gal}(K^{ab}/K) \arrow[r, equal] \arrow[d] & \lim\limits_{\mathfrak{m}} \mathrm{Gal}(H_K(\mathfrak{m})/K) \\
I_K(\mathfrak{m})/P_K(\mathfrak{m}) \arrow[r] \arrow[d, "\pi_{\mathfrak{m},\mathfrak{n}}"] & \mathrm{Gal}(H_K(\mathfrak{m})/K) \arrow[d] & \\
I_K(\mathfrak{n})/P_K(\mathfrak{n}) \arrow[r] & \mathrm{Gal}(H_K(\mathfrak{n})/K) &
\end{tikzcd}$$

The connection between global and local class field theory is expressed by commutativity of

$$\begin{tikzcd}
K_v^\times \arrow[r, "\varphi_{K_v}"] \arrow[d] & \mathrm{Gal}(K_v^{ab}/K_v) \arrow[d] \\
\mathbb{A}_K^\times \arrow[r, "\varphi_K"] & \mathrm{Gal}(K^{ab}/K),
\end{tikzcd}$$

where v is a prime of K, the vertical arrows are the natural injections, and φ_{K_v} and φ_K are the maps given by the reciprocity laws.

18 2015-03-02: Idele class characters

We have formulated global class field in three equivalent ways: the classical version, the adelic version, and as an equivalence between Hecke characters and 1-dimensional Galois representations.

Now let us discuss an adelic version of the formulation via Hecke characters. An *idele class character* of a global field K is a continuous group homomorphism $\chi : K^\times \backslash \mathbb{A}_K^\times \to \mathbb{C}^\times$, i.e., a continuous group homomorphism $\chi = \prod \chi_v : \mathbb{A}_K^\times \to \mathbb{C}^\times$ such that:

(1) There is a compact open subgroup U of $\mathbb{A}_f^\times = \coprod_{v \nmid \infty} K_v^\times$ such that $\chi(gu) = \chi(g)$ for all $u \in U$.

(2) $\chi_\infty = \prod_{v \mid \infty} \chi_v$ is continuous (and hence real-analytic).

(3) $\chi(K^\times) = 1$.

Condition (1) is equivalent to both of the following being true:

(a) Each χ_v is continuous, i.e., there is a compact open subgroup $U_v = 1 + \pi_v^{n_v}\mathcal{O}_v$ of $K_v^\times$ such that $\chi_v|_{U_v} = 1$.

(b) For almost all v, $\chi_v|_{\mathcal{O}_v^\times} = 1$ (i.e., χ_v is unramified).

Here is what condition (2) means: When v is real, $\chi_v : \mathbb{R}^\times \to \mathbb{C}^\times$ must be given by $\chi_v(x) = (\operatorname{sign} x)^\varepsilon |x|^{s_0}$ for some $\varepsilon \in \{0,1\}$ and $s_0 \in \mathbb{C}$. When v is complex, $\chi_v : \mathbb{C}^\times \to \mathbb{C}^\times$ must be given by $z \mapsto z^n |z|^{s_0}$ for some $n \in \mathbb{N}$ and $s_0 \in \mathbb{C}$.

Theorem 18.1. *There is a natural bijective correspondence*

$$\{\textit{Hecke characters of } K\} \longleftrightarrow \{\textit{idele class characters of } K\}.$$

For any idele class character $\chi = \prod \chi_v : \mathbb{A}_K^\times \to \mathbb{C}^\times$, let $\mathfrak{m}_f = \prod_v (1 + \pi_v^{n_v}\mathcal{O}_v) \cap \mathcal{O}_v$ so that $\chi(gu) = \chi(g)$ for all $u \in \mathfrak{m}_f$. Then the corresponding Hecke character $\chi_c : I_K(\mathfrak{m}_f) \to \mathbb{C}^\times$ is given by $\chi_c(\mathfrak{a}) = \chi(\prod \pi_v^{\operatorname{ord}_v \mathfrak{a}}) = \prod_{v \nmid \mathfrak{m}_f} \chi_v(\pi_v^{\operatorname{ord}_v \mathfrak{a}})$ for any ideal $\mathfrak{a} \in I_K(\mathfrak{m}_f)$.

Conversely, given a Hecke character $\chi_c : I_K(\mathfrak{m}) \to \mathbb{C}^\times$, the corresponding idele class character $\chi_{\mathbb{A}} = \prod_v \tilde{\chi}_v$ is characterized by the following properties:

(1) For $v \nmid \mathfrak{m}_f\infty$, $\tilde{\chi}_v(\pi_v) = \chi(\mathfrak{p}_v)$, where $\mathfrak{p}_v$ is the prime ideal associated to v and π_v is any uniformizer of K. In particular, $\tilde{\chi}_v(\mathcal{O}_v^\times) = 1$.

(2) For v real, $\tilde{\chi}_v|_{\mathbb{R}>0} = \chi_v|_{\mathbb{R}>0}$.

(3) For v complex, $\tilde{\chi}_v = \chi_v$.

(4) For $v \mid \mathfrak{m}_f$, let $n_v = \operatorname{ord}_{\mathfrak{p}_v} \mathfrak{m}_f$. Then $\tilde{\chi}_v|_{1+\pi_v^{n_v}\mathcal{O}_v} = 1$.

Since $\chi_v(\mathcal{O}_v^\times) = 1$ for all $v \nmid \mathfrak{m}_f\infty$, the Hecke character χ_c is well-defined. It remains to check $\chi_c(\alpha\mathcal{O}_K) = 1$ for any $\alpha \equiv 1 \pmod{^* \mathfrak{m}}$. Take $\mathfrak{m} = \mathfrak{m}_f \cdot \prod_{v \text{ real}} \mathfrak{m}_v$. Since $\alpha_v = \pi_v^{\operatorname{ord}_v \alpha} u_v$ for some $u_v \in \mathcal{O}_v^\times$, we have $\chi_v(\alpha_v) = \chi_v(\pi_v^{\operatorname{ord}_v \alpha}\chi_v(u_v)$. But $\chi_v(u_v) = 1$ for all $v \nmid \mathfrak{m}_f\infty$, so

$$1 = \chi(\alpha) = \prod_v \chi_v(\alpha_v) = \prod_{v \nmid \mathfrak{m}_f\infty} \chi_v(\alpha_v) \cdot \prod_{v \mid \mathfrak{m}_f} \chi_v(\alpha_v) \cdot \prod_{v \mid \infty} \chi_v(\alpha_v) = \chi_c(\alpha\mathcal{O}_K) \cdot \prod_{v \mid \infty} \chi_v(\alpha_v).$$

So $\chi_c(\alpha\mathcal{O}_K) = \prod_{v \mid \infty} \chi_v(\alpha_v)^{-1} = \chi_\infty(\alpha)^{-1}$.

19 2015-03-04: Reciprocity for idele class characters

Continuing from last time, we want to construct an idele class character $\chi_{\mathbb{A}}$ from a Hecke character χ of K.

(1) For $v \nmid \infty\mathfrak{m}$, define $\tilde{\chi}_v : K_v^\times \to \mathbb{C}^\times$ by $\tilde{\chi}_v(\mathcal{O}_v^\times) = 1$ and $\tilde{\chi}_v(\pi_v) = \chi(\mathfrak{p}_v)$.

(2) For $v \mid \infty$ and $v \nmid \mathfrak{m}_\infty$, define $\tilde{\chi}_v = \chi_v$.

(3) For $v \mid \mathfrak{m}_\infty$, define $\tilde{\chi}_v|_{(K_v^\times)^+} = \chi_v$.

(4) $\chi_{\mathbb{A}}(K^\times \cdot \mathcal{U}_{\mathfrak{m}_f}) = 1$.

To check this is well-defined, it suffices to show that $a \in K^\times \cap \mathcal{U}_{\mathfrak{m}_f}\mathcal{U}_{\mathfrak{m}_\infty} \prod_{v \nmid \infty\mathfrak{m}} K_v^\times$, we have $a \equiv 1 \pmod{^* \mathfrak{m}}$. Indeed,

$$\chi_{\mathbb{A}}(a) = 1 \cdot \prod_{v \mid \infty} \chi_v(a_v) \cdot \prod_{v \nmid \infty\mathfrak{m}} \chi_v(a_v) = \chi_\infty(a)\chi(a\mathcal{O}_K) = \chi_\infty(a)\chi_\infty^{-1}(\alpha) = 1.$$

Example 19.1. A Hecke character of $\mathbb{Q}$ of finite order is a Dirichlet character $\chi : (\mathbb{Z}/N)^\times \to \mathbb{C}^\times$. The corresponding idele class character $\chi_{\mathbb{A}} = \prod_{p \le \infty} \tilde{\chi}_p : \mathbb{A}_{\mathbb{Q}}^\times \to \mathbb{C}^\times$ is defined by

(1) $\tilde{\chi}_p : \mathbb{Q}_p^\times \to \mathbb{C}^\times$ for p unramified is defined by $\tilde{\chi}_p(p) = \chi(p)$.

(2) $\tilde{\chi}_\infty : \mathbb{R}^\times \to \mathbb{C}^\times$ is defined by $\tilde{\chi}_\infty(a) = 1$ for all $a > 0$, and $\tilde{\chi}_\infty(-1) = \chi(-1)$.

Proposition 19.2. *For $p \mid N$, the character $\tilde{\chi}_p : \mathbb{Q}_p^\times \cong p^{\mathbb{Z}} \times \mathbb{Z}_p^\times \to \mathbb{C}^\times$ is defined by $\tilde{\chi}_p(a) = \chi_p(a)$, and factors through $\mathbb{Z}_p^\times/(1 + p^e\mathbb{Z}_p) \to (\mathbb{Z}_p/p^e)^\times \xrightarrow{\chi_p} \mathbb{C}^\times$. Moreover, $\tilde{\chi}_{p_i}(p_i) = \prod_{j \ne i} \chi_{p_j}^{-1}(p_i)$.*

Remark 19.3. What could go wrong if we replace $\mathbb{Q}$ by an arbitrary number field? First, Dirichlet characters are defined on elements, but Hecke characters are defined on ideals; this only works because $\mathbb{Z}$ is a PID. Second, if there are several real primes, how do we determine the values at $-1 \in \mathbb{R}$?

Now we state yet another version of the reciprocity law, this time in terms of idele class characters.

Theorem 19.4 (Global reciprocity law)**.** *There is a natural bijective correspondence*

$$\left\{ \begin{array}{c} \textit{idele class characters} \\ \textit{of } K \textit{ of finite order} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} 1\textit{-dim. representations} \\ \textit{of } \mathrm{Gal}(\overline{K}/K) \end{array} \right\}.$$

More generally, there is a group called the Weil group of K such that

$$\left\{ \begin{array}{c} \textit{idele class characters} \\ \textit{of } K \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} 1\textit{-dim. representations} \\ \textit{of Weil group} \end{array} \right\}.$$

19.1 The Langlands correspondence

It is natural to ask what happens when we look at higher-dimensional representations of $\mathrm{Gal}(\overline{K}/K)$. Langlands conjectured:

Conjecture 19.5. *There are natural bijective correspondences*

$$\left\{ \begin{array}{c} \textit{Automorphic representations of} \\ \mathrm{GL}_n(K)\backslash \mathrm{GL}_n(\mathbb{A}_K) \textit{ of some} \\ \textit{special algebraic type} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} n\textit{-dimensional} \\ \textit{representations of} \\ \mathrm{Gal}(\overline{K}/K) \end{array} \right\}$$

and

$$\left\{ \begin{array}{c} \textit{Automorphic representations of} \\ \mathrm{GL}_n(K)\backslash \mathrm{GL}_n(\mathbb{A}_K) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} n\textit{-dimensional} \\ \textit{representations of} \\ \textit{some Langlands group} \end{array} \right\}.$$

More generally, if G is a reductive algebraic group over $\mathbb{Q}$, then there is a similar correspondence involving automorphic representations of G.

There is also a local Langlands correspondence, which has been proved for GL_n.

20 2015-03-06: Complex multiplication

Now we begin our study of complex multiplication. For a reference, see [Sil].

Definition 20.1. Let F be a field. An *elliptic curve* over F is a smooth projective curve over F of genus 1 with a fixed F-point O.

By Riemann–Roch, any elliptic curve over F is isomorphic to one of the form $E : y^2 + a_1xy + a_3y = x^3 + ax + b$. If $\operatorname{char} F \neq 2, 3$, we may take $a_1 = a_3 = 0$ without loss of generality, and such a curve E is smooth if and only if $\Delta 4a^3 - 27b^2 \neq 0$.

Given such a realization as a plane curve, define an addition law on E by $P + Q + R = 0$, where P, Q, R are collinear points on E. This is independent of the embedding, and can also be defined intrinsically in terms of the Picard group.

Over $\mathbb{C}$, smooth projective curves correspond to smooth compact Riemann surfaces of the same genus, so complex elliptic curves are complex tori. Any elliptic curve over $\mathbb{C}$ corresponds to to $E_\Lambda = \mathbb{C}/\Lambda$ for some lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, and the group structure is induced by addition in $\mathbb{C}$.

Definition 20.2. Morphisms $\mathrm{Hom}(E_1, E_2)$ of elliptic curves are defined to be group homomorphisms which are also regular maps. A morphism $f \in \mathrm{Hom}(E_1, E_2)$ is called an *isogeny* provided that $\ker f$ and $\operatorname{coker} f$ are both finite.

Let $\mathrm{End}(E)$ be the ring of endomorphisms $E \to E$ which are either isogenies or zero. Note that $\mathbb{Z} \subset \mathrm{End}(E)$: for $n > 0$, the map $P \mapsto [n]P = P + \cdots + P : E \mapsto E$ is an isogeny, as is $P \mapsto [-1]P = -P$.

We study the situation over $\mathbb{C}$, which will be representative of the characteristic zero case in general. Given a map $\tilde{f} = f_\alpha : \mathbb{C} \to \mathbb{C}$ given by $z \mapsto \alpha z$, we may descend to $f : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ if $\tilde{f}(z) = \alpha z \in \Lambda_2$ for all $z \in \Lambda_1$, where Λ_1 and Λ_2 are free $\mathbb{Z}$-lattices of rank 2.

Lemma 20.3. $\mathrm{Hom}(E_{\Lambda_1}, E_{\Lambda_2}) = \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\}$.

Lemma 20.4. *Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \omega_1(\mathbb{Z} + \mathbb{Z}\frac{\omega_2}{\omega_1})$ be a lattice with $\tau := \frac{\omega_2}{\omega_1} \in \mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$. Then $E_\Lambda \cong E_\tau := \mathbb{C}/\Lambda_\tau$, where $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$. This gives a surjection $\tau \mapsto E_\tau : \mathbb{H} \twoheadrightarrow \{$elliptic curves over $\mathbb{C}\}/\cong$.*

When is $\alpha \in \mathrm{Hom}(E_{\tau_1}, E_{\tau_2})$ an isomorphism? Choose $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_{\tau_1} = \Lambda_{\tau_2}$. Let $a, b, c, d \in \mathbb{Z}$ such that

$$\alpha \begin{pmatrix} \tau_1 \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tau_2 \\ 1 \end{pmatrix}.$$

Then α is an isomorphism if and only if $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$. In fact, since $\tau_1, \tau_2 \in \mathbb{H}$, we have $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ if and only if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. To summarize:

Proposition 20.5. *Let $\alpha \in \mathbb{C}$ and $\tau_1, \tau_2 \in \mathbb{H}$.*

(1) $\alpha \in \mathrm{Hom}(E_{\tau_1}, E_{\tau_2}) \iff \alpha \begin{pmatrix} \tau_1 \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tau_2 \\ 1 \end{pmatrix}$.

(2) α is an isomorphism $\iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

Theorem 20.6. *This yields a bijective correspondence between $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ and isomorphism classes of elliptic curves over $\mathbb{C}$.*

Thus, we refer to $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ as a *moduli space of elliptic curves*. More generally, let $X(K)$ be the moduli space of (isomorphism classes of) elliptic curves over a field K. This is a "scheme" (actually a stack) over $\mathbb{Q}$.

Definition 20.7. We say an element $[\tau] \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is defined over $F \subset \mathbb{C}$ if E_τ can be defined over F.

Theorem 20.8. *Let $\tau \in \mathbb{H} \cap \overline{\mathbb{Q}}$. Then $[\tau]$ is defined over $\overline{\mathbb{Q}}$ if and only if τ is imaginary quadratic.*

Proposition 20.9. *Let $\tau \in \mathbb{H}$. Then*

$$\mathrm{End}(E_\tau) = \begin{cases} \text{an order in } \mathbb{Q}(\tau) & \text{if } \tau \text{ is imaginary quadratic,} \\ \mathbb{Z} & \text{otherwise.} \end{cases}$$

Proof. Let $\alpha \in \mathrm{End}(E_\tau)$. Then $\alpha \in \mathbb{C}$ such that $\alpha = c\tau + d$ and $\alpha\tau = a\tau + b$. If $\alpha \in \mathbb{Q}(\tau)$, then $(c\tau + d)\tau = a\tau + b$, so $c\tau^2 + (d - a)\tau - b = 0$, so τ is imaginary quadratic.

Conversely, if τ is imaginary quadratic, write $k = \mathbb{Q}(\tau)$. We have $\alpha \in \mathrm{End}(E_\tau)$ if and only if $\alpha\Lambda_\tau = \Lambda_\tau$, and $\mathcal{O}_\tau = \{\alpha \in k : \alpha\Lambda_\tau \subset \Lambda_\tau\}$ is always an order of k. $\square$

21 2015-03-09: CM and the class group

The j-invariant

$$j(\tau) = j(E_\tau) = 1728 \frac{E_4^3}{\Delta(\tau)}$$

gives a bijection between $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ and the set of isomorphism classes of elliptic curves over $\mathbb{C}$. Here, for even $k \geq 4$,

$$E_k(\tau) = \sum_{\gamma \in \Gamma_\infty \backslash \mathrm{SL}_2(\mathbb{Z})} (c\tau + d)^{-k},$$

where $\Gamma_\infty = \left\{ \pm \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z} \right\}$, is a modular form of weight k for $\mathrm{SL}_2(\mathbb{Z})$. Also,

$$\Delta(\tau) = \frac{1}{1728}(E_4^3 - E_6^2) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

is the unique weight 12 cusp form for $\mathrm{SL}_2(\mathbb{Z})$.

Theorem 21.1. *E_τ can be defined over F if and only if $j(\tau) \in F$, in which case we write $[\tau] \in F$.*

Let E be an elliptic curve over $\mathbb{C}$. Recall from last time that $\mathrm{End}(E)$ is either $\mathbb{Z}$ or an order $\mathcal{O}$ of an imaginary quadratic field. In the latter case, we say E has *complex multiplication* (CM) by $\mathcal{O}$.

Let $k = \mathbb{Q}(\sqrt{d})$ be the field of fractions of $\mathcal{O} = \mathcal{O}_k$, and denote

$$\mathcal{E}\ell\ell(k) = \{\text{elliptic curves } E/\mathbb{C} \text{ with CM by } \mathcal{O}_k, \text{ up to } \mathbb{C}\text{-isomorphism}\}.$$

Proposition 21.2. *The map $[\mathfrak{a}] \mapsto E_{\mathfrak{a}} = \mathbb{C}/\mathfrak{a}$ induces a bijection $\mathrm{Cl}(k) \to \mathcal{E}\ell\ell(k)$.*

The group $\mathrm{Aut}(\mathbb{C})$ acts on elliptic curves over $\mathbb{C}$ as follows:

$$\begin{array}{ccc} E^\sigma & \longrightarrow & E \\ \downarrow & & \downarrow \\ \mathrm{Spec}\,\mathbb{C} & \xrightarrow{\sigma} & \mathrm{Spec}\,\mathbb{C} \end{array}$$

In coordinates, $E : y^2 = x^3 + ax + b$ is sent to $E^\sigma : y^2 = x^3 + \sigma(a)x + \sigma(b)$.

Lemma 21.3. *This induces an isomorphism $f \mapsto f^\sigma : \mathrm{End}(E) \xrightarrow{\simeq} \mathrm{End}(E^\sigma)$, where $f^\sigma(p^\sigma) = f(p)^\sigma$. (If $p \in E(\mathbb{C})$, then $p^\sigma \in E^\sigma(\mathbb{C})$.)*

Corollary 21.4. *If $E \in \mathcal{E}\ell\ell(k)$, then $E^\sigma \in \mathcal{E}\ell\ell(k)$. In particular, $\mathrm{Aut}(\mathbb{C})$ acts on $\mathcal{E}\ell\ell(k)$.*

Hence, there exists a number field $F \subset \overline{\mathbb{Q}} \subset \mathbb{C}$ such that $\mathrm{Aut}(\mathbb{C}/F)$ acts trivially on $\mathcal{E}\ell\ell(k)$ and $[F : \mathbb{Q}] \mid h_k = \#\,\mathcal{E}\ell\ell(k)$.

Proposition 21.5. *For each $E \in \mathcal{E}\ell\ell(k)$, we have $j(E^\sigma) = j(E)^\sigma$ and $[\mathbb{Q}(j(E)) : \mathbb{Q}] \le h_k$.*

Example 21.6. The elliptic curve $E : y^2 = x^3 + x$ has an endomorphism $f : (x, y) \mapsto (-x, iy)$ of order 4. This gives an inclusion $i \mapsto f : \mathbb{Z}[i] \subset \mathrm{End}(E)$, so $\mathrm{End}(E) = \mathbb{Z}[i]$. Thus, E has CM by $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a PID, $\mathcal{E}\ell\ell(\mathbb{Q}(i)) = \{E_i\}$, so $E_i \cong E$. Thus, $j(i) = j(E_i) = j(z) = 1728$.

Example 21.7. The elliptic curve $E : y^2 = x^3 + 1$ has an endomorphism $(x, y) \mapsto (\zeta_3 x, y)$, where $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$. Thus, E has CM by $\mathbb{Z}[\zeta_3]$, which is a PID, so $E = E_{\zeta_3}$ and $j(\zeta_3) = j(E) = 0$.

Theorem 21.8. *Let $E \in \mathcal{E}\ell\ell(k)$. Let $H = k(j(E))$ and $L = k(j(z), E_{\mathrm{tor}})$, where $E_{\mathrm{tor}} = \bigcup_{m \ge 1} E[m]$ is the set of torsion $\mathbb{C}$-points of E. Then $\mathrm{Gal}(L/H)$ is abelian.*

Proof. Define a map $\sigma \mapsto \rho(\sigma) : \mathrm{Gal}(L/H) \to \mathrm{Aut}(E_{\mathrm{tor}})$, where $\rho(\sigma)P = P^\sigma$. This is well-defined as $E^\sigma = E$ since $j(z) \in H$ is fixed by σ and E is defined over H.

Let $L_m = H(E[m])$. Then ρ induces an injection $\mathrm{Gal}(L_m/H) \hookrightarrow \mathrm{Aut}(E[m])$. Notice that $E[m]$ is actually an $\mathcal{O}_k$-module. So $\mathrm{Im}\,\rho \subset \mathrm{Aut}_{\mathcal{O}_k} E[m]$, which is abelian as $E[m]$ is $\mathcal{O}_k$-principal. □

This is analogous to the construction of totally ramified abelian extensions in local class field theory.

22 2015-03-11: CM and Hilbert class fields

Recall from last time that we have the space of CM elliptic curves $\mathcal{E}\ell\ell(k) \cong \mathrm{Cl}(k)$ with an action of $\mathrm{Aut}(\mathbb{C})$.

Lemma 22.1. *Fix $i : K \hookrightarrow \mathbb{C}$ and $E \in \mathcal{E}\ell\ell(k)$. There exists a unique $\iota : \mathcal{O}_K \xrightarrow{\simeq} \mathrm{End}(E)$ such that $\iota(a)^*\omega = i(a)\omega$ for all $\omega \in \Omega_{E/\mathbb{C}}$.*

Today, we give a proof of the theorem from last time.

Theorem 22.2. *Let $E \in \mathcal{E}\ell\ell(k)$, $H_E = K(j(E))$, and $L = K(j(z), E_{\mathrm{tor}})$. Then L is abelian over H_E.*

Definition 22.3. If $E \in \mathcal{E}\ell\ell(k)$ and $\mathfrak{a} \subset \mathcal{O}_K$ is an ideal, the group of $\mathfrak{a}$-torsion points of E is

$$E[\mathfrak{a}] = \{P \in E(\mathbb{C}) : \iota(\alpha)P = 0 \ \forall \alpha \in \mathfrak{a}\}.$$

Lemma 22.4. *Let $E \in \mathcal{E}\ell\ell(k)$. Then $E[\mathfrak{a}]$ is an $\mathcal{O}_K$-module and $E[\mathfrak{a}] \cong \mathcal{O}_K/\mathfrak{a}$.*

Proof. Since $E \in \mathcal{E}\ell\ell(k)$, $E \cong E_{\mathfrak{b}}$ for some fractional ideal $\mathfrak{b}$ of k. So

$$E[\mathfrak{a}] = \{[z] \in \mathbb{C}/\mathfrak{b} : \alpha z \in \mathfrak{b} \ \forall \alpha \in \mathfrak{a}\} = \mathfrak{a}^{-1}\mathfrak{b}/\mathfrak{b} \cong \mathcal{O}_K/\mathfrak{a}.$$

□

Proof of the theorem. We have $L = \bigcup_{m \geq 1} L_m$, where $L_m = H_E(E[m])$. Define a homomorphism $\rho : \mathrm{Gal}(L_m/H_E) \hookrightarrow \mathrm{Aut}(E[m])$ by $\rho(\sigma)\cdot P := P^\sigma$. One can check that $\rho(\sigma)$ is $\mathcal{O}_K$-linear for all $\sigma \in \mathrm{Gal}(L_m/H_E)$, and hence lands in $\mathrm{Aut}_{\mathcal{O}_K}(E[m])$, which by the lemma is isomorphic to $\mathrm{Aut}_{\mathcal{O}_K}(\mathcal{O}_K/m) = (\mathcal{O}_K/m)^\times$, an abelian group. □

Example 22.5. We have $\mathbb{Q}^{ab} = \mathbb{Q}(\mathbb{G}_{m,\mathrm{tor}}) = \mathbb{Q}(\zeta_\infty)$ and $\mathbb{G}_m(\mathbb{C}) = \mathbb{C}^\times$, with $\mathbb{Z}$ acting on $\mathbb{C}^\times$ by $n \cdot z = z^n$.

Recall our setup from local class field theory: Let K be a local field, and let π be a uniformizer of K. Choosing $f = \pi X + X^q$, let F_f be the corresponding formal group law over $\mathcal{O}_K$. Then $\Lambda_n = \{x \in \mathfrak{m}_{\overline{K}} : [\pi^n]_f \cdot x = 0\}$ is also an $\mathcal{O}_K$-module, and we proved:

(1) $K_\pi = K(\bigcup_{n \geq 1} \Lambda_n)$ is a maximal totally ramified abelian extension of K.

(2) $K^{ab} = K_\pi K^{un} = K_\pi \cdot K(\mu_n : \mathfrak{p} \nmid n)$.

We have a similar picture for $H_E = K(j(E))$:

(1) H_E is independent of $E \in \mathcal{E}\ell\ell(k)$ and is the Hilbert class field of K: every prime of K is unramified in $H = H_E$, and $\mathrm{Gal}(H_E/K) \cong \mathrm{Cl}(K)$.

(2) $k^{ab} = k(j(E), h(E_{\mathrm{tor}}))$, where if we write $E : y^2 = x^3 + ax + b$ (with $a, b \in H$) and $P = (x, y) \in E(\mathbb{C})$, then

$$h(P) = \begin{cases} x & \text{if } ab \neq 0, \\ x^2 & \text{if } b = 0 \text{ (when } j(E) = 1728), \\ x^3 & \text{if } a = 0 \text{ (when } j(E) = 0). \end{cases}$$

We have defined two actions on $\mathcal{E}\ell\ell(k)$:

(1) $\mathrm{Gal}(\overline{K}/K) \circlearrowleft \mathcal{E}\ell\ell(k) \cong \mathrm{Cl}(k)$

(2) $\mathrm{Cl}(k) \circlearrowleft \mathcal{E}\ell\ell(k)$ simply-transitively by $[\mathfrak{a}] * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$.

Definition 22.6. Fix $E \in \mathcal{E}\ell\ell(k)$. Define a map

$$\begin{aligned} F = F_E : \mathrm{Gal}(\overline{K}/K) &\to \mathrm{Cl}(k), \\ \sigma &\mapsto F(\sigma), \end{aligned}$$

where $F(\sigma)$ is defined by $F(\sigma) * E = E^\sigma$.

Proposition 22.7. *(1) F_E is independent of the choice of E.*

(2) $F = F_E$ is a group homomorphism.

Proof. Choose another $E_1 \in \mathcal{E}\ell\ell(k)$. Since $\mathrm{Cl}(k)$ acts simply-transitively on $\mathcal{E}\ell\ell(k)$, there exists $[\mathfrak{b}] \in \mathrm{Cl}(k)$ such that $E_1 = [\mathfrak{b}] * E$. Write $F_{E_1}(\sigma) = [\mathfrak{a}_1]$ and $F_E(\sigma) = [\mathfrak{a}]$. Then $E_1^\sigma = [\mathfrak{a}_1] * E_1$, so

$$[\mathfrak{a}_1\mathfrak{b}] * E = [\mathfrak{a}_1] * [\mathfrak{b}] * E = ([\mathfrak{b}] * E)^\sigma = [\mathfrak{b}] * E^\sigma = [\mathfrak{b}] * [\mathfrak{a}] * E = [\mathfrak{b}\mathfrak{a}] * E.$$

(We should check $([\mathfrak{b}] * E)^\sigma = [\mathfrak{b}] * E^\sigma$.) This implies $[\mathfrak{a}_1\mathfrak{b}] = [\mathfrak{b}\mathfrak{a}]$, so $[\mathfrak{a}_1] = [\mathfrak{a}]$. ☐

We'll finish the proof of the theorem next time. As a final remark, note that the following diagram commutes:

$$\begin{tikzcd} \mathrm{Gal}(\overline{K}/K) \arrow[r, "F"] \arrow[d, equal] & \mathrm{Cl}(K) \arrow[d, "\simeq"] \\ \mathrm{Gal}(\overline{K}/K) \arrow[r] & \mathrm{Gal}(H/K), \end{tikzcd}$$

where the right arrow is the isomorphism given by class field theory.

23 Several missing lectures

[I don't have notes for a few weeks of lectures at this point. See [Sil, chapter 2] for an exposition of the theory of complex multiplication, the subject of these lectures.]

24 2015-04-13: Rank and modularity of elliptic curves

Theorem 24.1 (Mordell–Weil)**.** *Let L be a number field. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over L, where $a, b \in \mathcal{O}_L$. Then $E(L)$ is a finitely-generated abelian group.*

Remark 24.2. Due to work of Mazur, the torsion part of $E(L)$ is known to be one of a finite list of possibilities. The rank $r(E(L))$ of $E(L)$ is called the *Mordell–Weil rank* of E, and is more mysterious.

Let $\mathfrak{p}$ be a prime of L such that E has good reduction modulo $\mathfrak{p}$. Let $q_\mathfrak{p} = |k_\mathfrak{p}|$, where $k_\mathfrak{p} = |\mathcal{O}_L/\mathfrak{p}|$. Let $a_\mathfrak{p}$ be the trace of $\sigma_\mathfrak{p}$ on $H^1(\tilde{E})$. Then $a_\mathfrak{p} = q_\mathfrak{p} + 1 - \left|\tilde{E}(k_\mathfrak{p})\right|$.

Define the local L-factor

$$L_\mathfrak{p}(s, E) = \left(1 - a_\mathfrak{p} q_\mathfrak{p}^{-s} + q_\mathfrak{p}^{1-2s}\right)^{-1}.$$

The global L-function of E is defined by

$$L(s, E) = \prod_\mathfrak{p} L_\mathfrak{p}(s, E)$$

(note: the definition of $L_\mathfrak{p}$ at bad primes is slightly different), which is absolutely convergent if $\operatorname{Re} s > \frac{3}{2}$. Also, by the Weil bound, $|a_\mathfrak{p}| \le 2\sqrt{q_\mathfrak{p}}$.

Conjecture 24.3. *$L(s, E)$ has holomorphic continuation to the whole complex s-plane and has functional equation*

$$N^s L(s, E) L_\infty(s, E) = w_E N^{2-s} L(2 - s, E) L_\infty(2 - s, E),$$

where $w_E = \pm 1$. (The most interesting part is for $s = 1$.)

Conjecture 24.4 (Birch–Swinnerton-Dyer)**.** *The algebraic rank and analytic rank are equal: $r(E(L)) = \operatorname{ord}_{s=1} L(s, E)$. Moreover,*

$$\frac{L^{(1)}(1, E)}{r!} = \frac{|\text{Ш}(E)|\, R_{E/L}}{|E(L)_{\mathrm{tor}}|^2}.$$

Theorem 24.5 (Wiles, Taylor–Wiles)**.** *If $L = \mathbb{Q}$, then $L(s, E)$ has holomorphic continuation and functional equation as conjectured above. Moreover, $L(s, E) = L(s, f)$ for some modular form f of weight 2.*

Theorem 24.6 (Deuring)**.** *Suppose E has CM by $\mathcal{O}_K$.*

(1) If $K \subset L$, then

$$L(s, E/L) = L(s, \chi_{E/L}) \cdot L(s, \overline{\chi}_{E/L}).$$

(2) If $K \not\subset L$, write $L' = KL$. Then

$$L(s, E/L) = L(s, \chi_{E/L'}).$$

In particular, holomorphic continuation and the functional equation hold for E/L.

24.1 Final project

Take your favorite imaginary quadratic field k. (Easy choice: class number one.) Choose a CM elliptic curve E/H. Find $\chi_{E/H}$ and $L(s, E/H)$.

25 2015-04-17: CM elliptic curves and Heegner points

Let $\mathbb{H}$ be the upper half plane, and define $Y_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathbb{H}$, the moduli space of degree-N cyclic isogenies $\varphi : E \to E'$ of elliptic curves up to isomorphism. The variety $Y_0(N)$ is defined over $\mathbb{Q}$. For any number field F,

$$Y_0(N)(F) = \left\{E \xrightarrow{\varphi} E' : E, E', \varphi \text{ defined over } F\right\} / (F\text{-isomorphism}).$$

Take $k = \mathbb{Q}(\sqrt{d})$ such that every $p \mid N$ splits in k (the *Heegner condition*). Write $N\mathcal{O}_k = \mathfrak{n} \cdot \overline{\mathfrak{n}}$. For each fraction ideal $\mathfrak{a}$, define

$$P_{\mathfrak{a}} = \begin{pmatrix} E_{\mathfrak{a}} = \mathbb{C}/\mathfrak{a} \xrightarrow{\varphi} \mathbb{C}/\mathfrak{n}^{-1}\mathfrak{a} = E_{\mathfrak{n}^{-1}\mathfrak{a}} \\ [z] \mapsto [z] \end{pmatrix}.$$

The kernel $\ker P_{\mathfrak{a}} = \mathfrak{n}^{-1}\mathfrak{a}/\mathfrak{a}$ is cyclic of order N. Let H be the Hilbert class field of k.

Define the compactification $X(N)$ by

$$X(N)(\mathbb{C}) = Y_0(N) \cup \{\text{cusps}\} = \Gamma_0(N)\backslash(\mathbb{H} \cup \mathbb{Q} \cup \{\infty\}).$$

This is a compact $\mathbb{C}$-curve, and $X_0(N)/\mathbb{Q}$ is a projective smooth curve.

Theorem 25.1 (Wiles, Taylor–Wiles)**.** *For every elliptic curve $E/\mathbb{Q}$ with conductor N, there is a surjective map*

$$\begin{aligned} X_0(N) &\xrightarrow{\pi} E \\ P_{[\mathfrak{a}]} &\mapsto \pi(P_{[\mathfrak{a}]}) \in E(H). \end{aligned}$$

Moreover, $L(s, E/k) = L(s, E/\mathbb{Q}) \cdot L(s, E^d/\mathbb{Q})$, where $E : y^2 = x^3 + ax + b$ and $E^d : dy^2 = x^3 + ax + b$ and $k = \mathbb{Q}(\sqrt{d})$.

The Heegner condition also implies that the functional equation takes the form

$$L(s, E/k) = -(\Gamma\text{-factors})L(2 - s, E/k)$$

since $w_{E,k} = -1$. Hence, $L(1, E/k) = 0$.

Theorem 25.2 (Gross–Zagier formula)**.** *Let $y_k = \sum_{[\mathfrak{a}] \in \mathrm{Cl}(k)} \pi(P_{[\mathfrak{a}]}) \in E(k)$. Then*

$$L'(1, E/k) = C \langle y_k, y_k \rangle_{\mathrm{NT}}$$

for some $C > 0$, where

$$\langle \cdot, \cdot \rangle_{\mathrm{NT}} : E(F)/E(F)_{\mathrm{tor}} \times E(F)/E(F)_{\mathrm{tor}} \to \mathbb{R}_{\geq 0}$$

is the Neron–Tate height, which is bilinear, symmetric, and positive-definite.

Corollary 25.3. *$L'(1,E/k) \neq 0 \iff y_k \in E(k)$ has infinite order, in which case $\operatorname{rank} E(k) \geq 1$.*

Kolyvagin developed the notion of *Euler system* to prove:

Theorem 25.4 (Kolyvagin)**.** *If $y_k \in E(k)$ has infinite order, then $\operatorname{rank} E(k) = 1$.*

(If y_k has finite order, nothing is known; the BSD conjecture implies $\operatorname{rank} E(k) \geq 3$.)

Theorem 25.5 (Gross–Zagier, Kolyvagin)**.** *If $L'(1,E/k) \neq 0$, then $\operatorname{rank} E(k) = 1$ and $\operatorname{rank} E(\mathbb{Q}) = \operatorname{ord}_{s=1} L(s,E/\mathbb{Q})$.*

25.1 Class numbers

Let $k = \mathbb{Q}(\sqrt{d})$ and $h_d = |\mathrm{Cl}(k)|$.

Theorem 25.6 (Siegel)**.** *We have*

$$\frac{|d|^{1/2}}{\log|d|} \ll h_d \ll |d|^{1/2} \log|d| \,.$$

This is not effective, but can be made effective if we assume the Riemann hypothesis.

Theorem 25.7 (Goldfeld 1979)**.** *If there is an elliptic curve $E/\mathbb{Q}$ such that $\operatorname{ord}_{s=1} L(s,E) \geq 3$, then*

$$h_d \geq \kappa(\varepsilon)\, |d|^{\frac{1}{2}-\varepsilon}$$

for every $\varepsilon > 0$, where $\kappa(\varepsilon)$ is an explicit constant.

Example 25.8. Consider the elliptic curve $E : -139y^2 = x^3 + 10x^2 - 20x + 8$. Then y_k is torsion, so $L'(1,E/k) = 0$, which implies $\operatorname{ord}_{s=1} L(s,E) \geq 3$. This proves the hypothesis of Goldfeld's theorem.

26 2015-04-24: Galois cohomology

Theorem 26.1. *Let L/K be a finite Galois extension of fields with $G = \mathrm{Gal}(L/K)$. Then $H^1(G, L^\times) = 0$.*

Corollary 26.2 (Hilbert 90)**.** *IF $G = \langle\sigma\rangle$ is cyclic and $N_{L/K} x = 1$, then $x = \frac{\sigma y}{y}$ for some y.*

Theorem 26.3. *Let M be a G-module and $\varphi \in Z^2(G,M)$. Then φ gives rise to a group extension*

$$0 \to M \to E \xrightarrow{\pi} G \to 1$$

such that:

(1) The G-module M associated to the above short exact sequence coincides with the original G-module structure on M.

(2) The 2-cocycle associated to the sequence is equivalent to φ.

27 2015-04-27: Galois homology

Let G be a group and M a G-module. Define $H_r(G,M) := \mathrm{Tor}_r^G(\mathbb{Z},M)$. Equivalently, $H^r(G,-)$ is the derived functor of the coinvariants functor $M \mapsto M_G$, where M_G is the maximal quotient on which M acts trivially.

Theorem 27.1. *$H_1(G,\mathbb{Z}) = G^{ab}$.*

Let I_G be the augmentation ideal of the group algebra $\mathbb{Z}[G]$.

Lemma 27.2. *$\mathbb{Z} \otimes_G M = \mathbb{Z}[G]/I_G \otimes_{\mathbb{Z}[G]} M = M/I_G M$, which is by definition M_G.*

Lemma 27.3. *M if G-flat iff $H_r(G,M) = 0$ for all $r > 0$.*

Proposition 27.4. *$H_1(G,\mathbb{Z}) = I_G/I_G^2$.*

Proof. Taking coinvariants of the short exact sequence

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

yields a long exact sequence

$$H_1(\mathbb{Z}[G]) \to H_1(\mathbb{Z}) \to H_0(I_G) \to H_0(\mathbb{Z}[G]) \to H_0(\mathbb{Z}) \to 0.$$

Since $H_1(\mathbb{Z}[G]) = 0$ and $H_0(\mathbb{Z}[G]) = H_0(\mathbb{Z}) = \mathbb{Z}$, we obtain an isomorphism $H_1(\mathbb{Z}[G]) \cong H_0(I_G) = I_G/I_G^2$. $\square$

Lemma 27.5. *$I_G/I_G^2 \cong G^{ab} = G/[G,G]$.*

Tate defined a "very long" exact sequence that glues together both homology and cohomology. Define a norm map

$$\begin{aligned} N_G : M &\to M^G \\ m &\mapsto N_G(m) = \sum_{g \in G} gm. \end{aligned}$$

Lemma 27.6. *$I_G M \subset \ker N_G$ and $\operatorname{im} N_G \subset M_G$.*

Definition 27.7. For $r \in \mathbb{Z}$, define

$$H_T^r(G,M) = \begin{cases} H^r(G,M), & r \geq 1, \\ M^G/(\operatorname{im} N_G), & r = 0, \\ (\ker N_G)/I_G M, & r = -1, \\ H_{-r+1}, & r \leq -2. \end{cases}$$

Proposition 27.8 (Tate)**.** *Given a short exact sequence*

$$0 \to M_1 \to M_2 \to M_3 \to 0,$$

we obtain a doubly-infinite long exact sequence

$$\cdots \to H_T^r(G,M_1) \to H_T^r(G,M_2) \to H_T^r(G,M_3) \to H_T^{r+1}(G,M_1) \to \dots$$

Theorem 27.9. *Let L/K be a finite Galois extension of fields. Then $H_T^r(G,\mathbb{Z}) \xrightarrow{\simeq} H_T^{r+2}(G,L^\times)$ for all r, and the isomorphism is "canonical", depending only on a choice of generator of $H_T^2(G,L^\times)$, which is cyclic of order $|G|$.*

28 2015-05-06: Brauer groups

The *Brauer group* of a field is the group of central division algebras over K with the operation of tensor product.

Proposition 28.1. *Let K be any field. Then* $\mathrm{Br}(K) \cong H^2(G_K, \overline{K}^\times)$.

29 2015-05-08: Brauer groups of local fields

Today, we will prove that the Brauer group of a nonarchimedean local field is $\mathbb{Q}/\mathbb{Z}$, which implies local class field theory.

Let $x \mapsto |x| = q^{-\mathrm{ord}_K x} : K \to \mathbb{R}_{>0}$ be the valuation of K. Let $\mathcal{O}_K$ be the ring of integers, $\mathfrak{p} = \pi\mathcal{O}_K \subset \mathcal{O}_K$ the maximal ideal with a uniformizer π, and $k = \mathcal{O}_K/\mathfrak{p}$ the residue field of order q.

Let D be a central division algebra over K of index $[D : K] = n^2$. Then there is a unique norm $|\cdot| : D \to \mathbb{R}_{>0}$ such that $|xy| = |x|\,|y|$ and $|x + y| \le \max\{|x|, |y|\}$ for all $x, y \in D$.

The subring $\mathcal{O}_D = \{x \in D : |x| \le 1\}$ is the unique maximal order in D. This ring has unique maximal ideal $\mathfrak{m}_D = \{x \in D : |x| < 1\}$. The quotient $\ell = \mathcal{O}_D/\mathfrak{m}_D$ is a finite field extension of k of index $f = [\ell : k] \le n$. Moreover, $\mathfrak{p}\mathcal{O}_D = \mathfrak{m}_D^e$.

Lemma 29.1. $e = f = n$.

Corollary 29.2. *Let D be a central division algebra over K of rank n^2. Let $L = K_n^{un}$ be the unique unramified extension of K of degree n. Then $K_n^{un} \hookrightarrow D$, and K_n^{un} splits D in the sense that $D \otimes_K K_n^{un} \cong M_n(K_n^{un})$. In other words, $[D] \in \mathrm{Br}(K_n^{un}/K)$, i.e., $[D] = 1 \in \mathrm{Br}(K_n^{un})$.*

Theorem 29.3. *Let K be a nonarchimedean local field. Then* $\mathrm{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$.

Proof. Let K^{un} be the maximal unramified extension of K. We have an exact sequence

$$1 \to \mathrm{Br}(K^{un}/K) \to \mathrm{Br}(K) \to \mathrm{Br}(K^{un}).$$

Assume D is a central division K^{un}-algebra of degree n^2. There is a finite unramified extension K'/K such that $D = D' \otimes_{K'} K^{un}$. By the corollary, $D' \otimes_{K'} L \cong M_n(L)$, where L is the unramified extension of K' of degree n. So

$$D = D' \otimes_{K'} K^{un} = (D' \otimes_{K'} L) \otimes_L K^{un} \cong M_n(K^{un}).$$

Thus, $\mathrm{Br}(K^{un}) = 0$. Hence,

$$\begin{aligned}\mathrm{Br}(K) &\cong \mathrm{Br}(K^{un}/K) \cong H^2(\mathrm{Gal}(K^{un}/K), K^{un\times}) \cong H^2(\mathrm{Gal}(K^{un}/K), \mathbb{Z}) \\ &\cong H^1(\mathrm{Gal}(K^{un}/K), \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(\mathrm{Gal}(K^{un}/K), \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Q}/\mathbb{Z}.\end{aligned}$$

□

Let us explicitly construct the isomorphism $\mathrm{Inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$. Let D be a central division K-algebra of rank n^2. Let $\sigma_{K_n^{un}/K}$ be the Frobenius automorphism, which generates $\mathrm{Gal}(K_n^{un}/K)$. There exists $e \in D^\times$ such that $\sigma_{K_n^{un}/K}(x) = exe^{-1}$. Then $\mathrm{Inv}_K([D]) = \mathrm{ord}_K\, e \pmod{\mathbb{Z}}$.

Theorem 29.4. *Every quadratic extension of K is inside the unique quaternion division algebra D.*

References

[CF] Cassels and Fröhlich, *Algebraic Number Theory*.

[L] S. Lang, *Algebraic Number Theory*.

[M] J. Milne, *Class Field Theory*, online notes.

[N] J. Neukirch, *Algebraic Number Theory*.

[S] J.P. Serre, *Local Fields*.

[Sil] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*.

Index