ALGEBRAIC NUMBER THEORY, GR6657, SPRING 2025

GYUJIN OH

Contents

This note will freely assume the familiarity with the materials of [ANT].

- We tried to make both class field theories as formal consequences of class formation axioms. Thus, for the global class field theory, we mainly follow the approach of [AT] (with certain simplifications as we only aim to prove it for number fields), although we also used the analytic inputs for the proof of the **Second Inequality**, as it is culturally more useful to know about L-functions.

- For the local existence theorem, we chose to use Lubin–Tate theory. We tried to emphasize a theme of **Explicit class field theory**.

- For the CM theory, we completely avoid the use of algebraic geometry, and follow the complex analytic proofs of the two Main Theorems in [Deu]. A clearer exposition for the first theorem can be found in [Lan], and to a certain extent, [Cox]. We were unable to find a complete account of a complex analytic proof of the Second Main Theorem written in English (apart from an English translation of [Deu]), which we provide here.

Part 1. Class field theory

1. Ramification of local fields

We say a little more about ramification of local fields. This is to state finer properties of the local Artin reciprocity map, and how it also compares the notion of "ramification" on both sides.

Definition 1.1 (Local conductor)**.** Let K/L be a finite extension of local fields. Let $\mathfrak{p} \subset \mathcal{O}_L$ be the maximal ideal. Then, the **(local) conductor** of K/L, denoted $\mathfrak{f}_{K/L}$, is defined as

$$\mathfrak{f}_{K/L} := \begin{cases} 0 & \text{if } \mathcal{O}_L^\times = N_{K/L}(\mathcal{O}_K^\times) \\ \min\{n \geq 1 \ : \ 1 + \mathfrak{p}^n \subset N_{K/L}(\mathcal{O}_K^\times)\} & \text{otherwise.} \end{cases}$$

The slogan is that **the conductor detects how deeply ramified the extension is**. In particular, you should think in a way that $\underline{N_{K/L}(\mathcal{O}_K^\times) \text{ smaller} = K/L \text{ more ramified.}}$

Proposition 1.2. *Let K/L be an **unramified** finite extension of local fields. Then, $\mathfrak{f}_{K/L} = 0$.*

Proof. Let π be a uniformizer of L. As K/L is unramified, π is also a uniformizer of K. We do several reductions.

Consider the map $N_{K/L}(\mathcal{O}_K^\times) \hookrightarrow \mathcal{O}_L^\times \twoheadrightarrow l^\times$, where l is the residue field of L and the second map is reduction mod π map. What is the image of this map? It's easy to see that, if $x \in \mathcal{O}_K$, then $N_{K/L}(x) \pmod{\pi} \equiv N_{k/l}(x \pmod{\pi})$, where k is the residue field of K. This follows basically from that $\mathcal{O}_K$ is free over $\mathcal{O}_L$ (as $\mathcal{O}_L$ is a DVR so a PID). Therefore, the image of this map is precisely $N_{k/l}(k^\times)$. I claim that this is equal to $l^\times$. Let $l = \mathbb{F}_{p^n}$. Then $k = \mathbb{F}_{p^{nm}}$ for some $m \geq 1$. Then $k^\times$ is cyclic of order $p^{nm} - 1$ and $l^\times$ is cyclic of order $p^n - 1$. Let $a \in k^\times$ be a primitive root (i.e. a multiplicative generator). Then, $a^{\frac{p^{nm}-1}{p^n-1}} \in l^\times$, and it is a multiplicative generator of $l^\times$. Now note that $N_{k/l}(a) = \prod_{\sigma \in \mathrm{Gal}(k/l)} \sigma(a)$, but every element of $\mathrm{Gal}(k/l)$ is a power of $\mathrm{Fr}_{k/l}$, which sends x to x^{p^n}. Thus,

$$N_{k/l}(a) = a \cdot a^{p^n} \cdot a^{p^{2n}} \cdots a^{p^{(m-1)n}} = a^{1+p^n+\cdots+p^{(m-1)n}} = a^{\frac{p^{nm}-1}{p^n-1}},$$

which is as observed above is a primitive root of l. Therefore, $N_{k/l}(k^\times)$ contains a primitive root of l, so contains the whole $l^\times$. Thus, to prove that $N_{K/L}(\mathcal{O}_K^\times) = \mathcal{O}_L^\times$, it suffices to show that $N_{K/L}(\mathcal{O}_K^\times) \supset 1 + \pi\mathcal{O}_L$, or a stronger statement that $N_{K/L}(1 + \pi\mathcal{O}_K) \supset 1 + \pi\mathcal{O}_L$.

We claim that it actually suffices to show that $\left(N_{K/L}(1 + \pi^b\mathcal{O}_K)\right) \cdot (1 + \pi^{b+1}\mathcal{O}_L) = 1 + \pi^b\mathcal{O}_L$ for every $b \geq 1$ (namely, for any $1 + \pi^b x$ for $x \in \mathcal{O}_L$, there exist $1 + \pi^b y \in 1 + \pi^b\mathcal{O}_K$ and $1 + \pi^{b+1}z \in 1 + \pi^{b+1}\mathcal{O}_L$ such that $N_{K/L}(1 + \pi^b y) \cdot (1 + \pi^{b+1}z) = 1 + \pi^b x$). This is because by induction we have

$$1 + \pi\mathcal{O}_L = (1 + \pi^2\mathcal{O}_L) \cdot N_{K/L}(1 + \pi\mathcal{O}_K) = (1 + \pi^3\mathcal{O}_L) \cdot N_{K/L}(1 + \pi^2\mathcal{O}_K) \cdot N_{K/L}(1 + \pi\mathcal{O}_K)$$

$$= \cdots = (1 + \pi^{b+1}\mathcal{O}_L) \cdot N_{K/L}(1 + \pi^b\mathcal{O}_K) \cdots N_{K/L}(1 + \pi\mathcal{O}_K).$$

This means concretely that, for any $1+\pi x \in 1+\pi\mathcal{O}_L$, there exist $y_1, y_2, \cdots \in \mathcal{O}_K$ such that, for any $b \geq 1$,

$$1+\pi x \equiv N_{K/L}((1+\pi y_1)(1+\pi^2 y_2)\cdots(1+\pi^b y_b)) \pmod{\pi^{b+1}}.$$

Now note that the sequence $\{c_n\}$, with $c_n = (1+\pi y_1)(1+\pi^2 y_2)\cdots(1+\pi^n y_n)$, is a Cauchy sequence in $\mathcal{O}_K$, so it converges (by **completeness of** K) to some element $c \in K$ (or even better in $1+\pi\mathcal{O}_K$), and $1+\pi x = N_{K/L}(c)$, which is what we want.

Now we prove $\left(N_{K/L}(1+\pi^b\mathcal{O}_K)\right)\cdot(1+\pi^{b+1}\mathcal{O}_L) = 1+\pi^b\mathcal{O}_L$ for every $b \geq 1$. Let $x \in \mathcal{O}_K$, and let $h(X)$ be the characteristic polynomial of the multiplication-by-x matrix $m_x : K \to K$ (as an endomorphism of an L-vector space K), which is of the form $h(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$, where $d = [K : L]$ and $a_{d-1}, \cdots, a_1, a_0 \in \mathcal{O}_L$. Then, $g(X) = X^d + \pi^b a_{d-1}X^{d-1} + \cdots + \pi^{b(d-1)}a_1 X + \pi^{bd}a_0$ is the characteristic polynomial of the multiplication-by-$\pi^b x$. Then, $g(1) = N_{K/L}(1-\pi^b x)$. Note that $g(1) \equiv 1+\pi^b a_{d-1} \pmod{\pi^{b+1}}$. As $a_{d-1} = -\operatorname{Tr}_{K/L}(x)$, we see that $\left(N_{K/L}(1+\pi^b\mathcal{O}_K)\right)\cdot(1+\pi^{b+1}\mathcal{O}_L) = 1+\pi^b\mathcal{O}_L$ if we prove that $\operatorname{Tr}_{K/L}(\mathcal{O}_K) = \mathcal{O}_L$. Note that $\operatorname{Tr}_{K/L}(\mathcal{O}_K) \subset \mathcal{O}_L$ is an $\mathcal{O}_L$-submodule, it suffices to prove that $\operatorname{Tr}_{K/L}(\mathcal{O}_K)$ contains an element that is not in $\pi\mathcal{O}_L$. By the similar reason as above, $\operatorname{Tr}_{K/L}(x) \pmod{\pi} = \operatorname{Tr}_{k/l}(x \pmod{\pi})$. Thus, everything will follow if we show that $\operatorname{Tr}_{k/l}(k) \neq 0$. Note that $\operatorname{Tr}_{k/l}(x) = x + x^{p^n} + \cdots + q^{p^{(m-1)n}}$, so it is in particular a polynomial of degree $p^{(m-1)n}$, which has at most $(m-1)n$ roots in k. This implies that $\operatorname{Tr}_{k/l} : k \to l$ is not zero, as desired. □

Proposition 1.3. *Let K/L be a* ***tamely ramified*** *finite extension of local fields. Then, $\mathfrak{f}_{K/L} \leq 1$.*

Recall that K/L is tamely ramified if $(e_{K/L}, p) = 1$ (p is the characteristic of the residue fields of the local fields).

Proof. By transitivity of the norms, if we take $K/K_0/L$ the maximal unramified subextension of K/L, then $N_{K/L}(\mathcal{O}_K^\times) = N_{K_0/L}(N_{K/K_0}(\mathcal{O}_K^\times))$. Using this, one can easily reduce to showing the Proposition for K/K_0, i.e. we can assume that K/L is **totally tamely ramified**. We thus need to show that in this case $N_{K/L}(1+\pi_K\mathcal{O}_K) \supset 1+\pi_L\mathcal{O}_L$ where π_K, π_L are uniformizers of K, L, respectively. As $N_{K/L}(1+\pi_L\mathcal{O}_L) = (1+\pi_L\mathcal{O}_L)^{e_{K/L}}$, it follows from the fact that any element of $1+\pi_L\mathcal{O}_L$ has an $e_{K/L}$-th root in $1+\pi_L\mathcal{O}_L$ by Hensel's lemma (which needs $(e_{K/L}, p) = 1$). More precisely, for $a \in 1+\pi_L\mathcal{O}_L$, let $f(X) = X^{e_{K/L}} - a$. Then $f'(X) = e_{K/L}X^{e_{K/L}-1}$, so $f'(X)$ is not zero mod π_L. In particular, $f(X) \pmod{\pi_L} = X^{e_{K/L}} - 1$ is separable. Therefore, $f(X) = (X-1)g(X)$ mod π_L, where $(X-1, g(X)) = 1$ in $k_L[X]$. Now using Hensel's lemma, there is a root of $f(X)$ in $\mathcal{O}_L$ which is congruent to 1 mod π_L, which is exactly what we want. □

The ramification group we learned before is, more precisely, called to be in **lower numbering**.

Definition 1.4 (Ramification groups in lower numbering)**.** Let K/L be a finite Galois extension of local fields, and let $\pi_K \in K$ be a uniformizer. For $i \geq -1$ an integer, define the **i-th ramification group in lower numbering** $\operatorname{Gal}(K/L)_i \leq \operatorname{Gal}(K/L)$ (or just G_i) as

$$G_i := \{\sigma \in \operatorname{Gal}(K/L) \mid \sigma\alpha \equiv \alpha \pmod{\pi_K^{i+1}} \text{ for all } \alpha \in \mathcal{O}_K\}.$$

We call G_0 the **inertia subgroup** and G_1 the **wild inertia subgroup**.

More generally, for $s \geq -1$ a **real number**, we define $G_s := G_{\lceil s \rceil}$. This definition will come handy later when we define the ramification groups in **upper numbering**.

This definition behaves, quite obviously, very well with subgroups. Namely, if you have a subextension $K/K'/L$, then $\mathrm{Gal}(K/K') \leq \mathrm{Gal}(K/L)$, and $\mathrm{Gal}(K/K') \cap \mathrm{Gal}(K/L)_i = \mathrm{Gal}(K/K')_i$. However, this is not really what we want in view of infinite Galois theory; the infinite Galois theory requires a compatibility with respect to **quotients**, not subgroups. And it is in general not true that lower numbering is compatible with quotients of Galois group. However, if you **renumber the ramification groups**, then the ramification group becomes compatible with quotients.

Definition 1.5 (Ramification groups in upper numbering)**.** Let K/L be a finite Galois extension of local fields, and let $G = \mathrm{Gal}(K/L) = G_{-1} \supset G_0 \supset G_1 \supset \cdots$ be the ramification groups in lower numbering, as defined above. Define

$$\phi_{K/L}(s) := \int_0^s \frac{dx}{[G_0 : G_x]}.$$

This is a piecewise linear strictly increasing continuous function $\phi_{K/L} : [-1, \infty) \to [-1, \infty)$. Therefore, we can define its inverse $\psi_{K/L} : [-1, \infty) \to [-1, \infty)$ (i.e. $\psi_{K/L} \circ \phi_{K/L} = \phi_{K/L} \circ \psi_{K/L} = \mathrm{id}$). We define, for $t \geq -1$, the **t-th ramification group in upper numbering** as $G^t := G_{\psi_{K/L}(t)}$ (i.e. $G^{\phi_{K/L}(s)} = G_s$).

This is such a weird definition; for lower numbering, the "jumps" of ramification groups happen at integers (i.e. if $G_x \neq G_{x+\varepsilon}$ for $\varepsilon > 0$ small, then x is an integer), but such jumps for upper numbering seem to happen at real numbers (or if you think a bit you realize the jumps happen at rational numbers, but still not necessarily integers). But there are surprising properties of ramification groups in upper numbering.

Proposition 1.6. *If $K/L/M$ is a tower of finite Galois extension of local fields, and if $t \geq -1$, then the image of $\mathrm{Gal}(K/M)^t$ via the quotient map $\mathrm{Gal}(K/M) \twoheadrightarrow \mathrm{Gal}(L/M)$ is precisely $\mathrm{Gal}(L/M)^t$. In particular, for an infinite Galois extension X/Y of local fields and $t \geq -1$, we can define*

$$\mathrm{Gal}(X/Y)^t := \varprojlim_{Z/Y \text{ finite Galois subextension of } X/Y} \mathrm{Gal}(Z/Y)^t.$$

Proof. Omitted (tedious but elementary). □

Proposition 1.7. *Let $K/L/M$ be a tower of finite Galois extensions of local fields. Then $\phi_{K/M}(s) = \phi_{L/M}(\phi_{K/L}(s))$.*

Proof. Omitted; Exercise. □

Theorem 1.8 (Hasse–Arf theorem)**.** *Let K/L be a finite **abelian** Galois extension. Then, the jumps of ramification groups $\mathrm{Gal}(K/L)^t$ in upper numbering happen at integers. Namely, if $t \geq -1$ is such that $\mathrm{Gal}(K/L)^t \neq \mathrm{Gal}(K/L)^{t+\varepsilon}$ for arbitrarily small number $\varepsilon > 0$, then $t \in \mathbb{Z}$.*

We will later see how the Hasse–Arf theorem can prove the local Kronecker–Weber theorem.

Exercise 1.1. Compute the jumps of ramification groups in upper numbering of $\mathrm{Gal}(\mathbb{Q}_3(\zeta_9)/\mathbb{Q}_3)$ and check that the jumps happen at integers.

Now we see a surprising connection between the conductor and the ramification groups.

Theorem 1.9. *Let K/L be a finite abelian extension of degree > 1. Then,*

$$\mathfrak{f}_{K/L} = \min\{n \in \mathbb{Z} \ : \ \mathrm{Gal}(K/L)^n = \{1\}\}.$$

This will follow from the local class field theory.

2. Statements of the local class field theory

The information about ramification in the previous section gives a hint to the following connections:

size of $N_{K/L}(\mathcal{O}_K^\times) \leftrightarrow$ conductor $\mathfrak{f}_{K/L} \leftrightarrow$ ramification subgroups $\mathrm{Gal}(K/L)^t$ in upper numbering.

The local class field theory gives a connection between the first and the third entries. The local class field theory consists of two parts, the **Artin reciprocity law** and the **local existence theorem**. The Artin reciprocity law gives a connection between two totally different kinds of objects.

Theorem 2.1 (Local Artin reciprocity). *Let L be a local field. Then, there is a **unique** continuous homomorphism, called the **local Artin map***

$$\mathrm{Art}_L : L^\times \to \mathrm{Gal}(L^{\mathrm{ab}}/L),$$

satisfying the following properties.

1. *For any finite abelian subextension K/L of L^{ab}/L, the local Artin map composed with the natural map $\mathrm{Gal}(L^{\mathrm{ab}}/L) \to \mathrm{Gal}(K/L)$ defines a continuous homomorphism*

$$\mathrm{Art}_{K/L} : L^\times \to \mathrm{Gal}(K/L),$$

which is surjective with kernel $N_{K/L}(K^\times)$. In particular, there is an isomorphism

$$L^\times/N_{K/L}(K^\times) \cong \mathrm{Gal}(K/L).$$

2. *If K/L is unramified, for any uniformizer $\pi_L \in L^\times$,*

$$\mathrm{Art}_{K/L}(\pi_L) = \mathrm{Fr}_{K/L}.$$

3. *If K/L is a finite extension of local fields, the following diagram commutes, where the right vertical arrow is the restriction to L^{ab}.*

$$\begin{tikzcd}
K^\times \arrow[r, "\mathrm{Art}_K"] \arrow[d, "N_{K/L}"'] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[d, "\mathrm{res}"] \\
L^\times \arrow[r, "\mathrm{Art}_L"'] & \mathrm{Gal}(L^{\mathrm{ab}}/L)
\end{tikzcd}$$

(4) If K/L is a finite extension of local fields, the following diagram commutes, where the right vertical arrow is the transfer map $V : \mathrm{Gal}(\overline{L}/L)^{\mathrm{ab}} \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$.

$$\begin{tikzcd}
K^\times \arrow[r, "\mathrm{Art}_K"] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\
L^\times \arrow[u, hook] \arrow[r, "\mathrm{Art}_L"'] & \mathrm{Gal}(L^{\mathrm{ab}}/L) \arrow[u, "V"']
\end{tikzcd}$$

Definition 2.2 (Transfer homomorphism)**.** Let $H \leq G$ be a finite index subgroup (each G, H may or may not be infinite). The **transfer homomorphism** $V : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is defined as follows. Let $[G : H] = n$, and let us take coset representatives of G/H, so that $G = \cup_{i=1}^{n} x_i H$ for $x_1, \cdots, x_n \in G$. For $g \in G$ and $1 \leq i \leq n$, $gx_i \in x_{j_i(g)} h_i(g)$ for some $1 \leq j_i(g) \in n$ and $h_i(g) \in H$. Then we define $V(g) := \prod_{i=1}^{n} h_i(g)$ in H^{ab}.

Proposition 2.3. *The transfer homomorphism indeed defines a group homomorphism.*

Proof. Omitted (tedious but elementary). You will see this homomorphism appearing more naturally in the context of group (co)homology. □

For example, in the case of $K = \mathbb{Q}_p$, we have

$$\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mathbb{Z}_p^\times,$$

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) = \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{nr}}/\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) = \widehat{\mathbb{Z}} \times \mathbb{Z}_p^\times,$$

by the local Kronecker–Weber theorem. The local Artin reciprocity $\mathrm{Art}_{\mathbb{Q}_p}$ is then

$$\mathrm{Art}_{\mathbb{Q}_p} : \mathbb{Z} \times \mathbb{Z}_p^\times \to \widehat{\mathbb{Z}} \times \mathbb{Z}_p^\times,$$

where $\mathbb{Z} \to \widehat{\mathbb{Z}}$ is the natural map and $\mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ is the **inverse**; for more details, see [ANT, Example 15.1].

The local Artin reciprocity $\mathrm{Art}_{\mathbb{Q}_p}$ is almost an isomorphism, except the difference between $\mathbb{Z}$ and $\widehat{\mathbb{Z}}$. This is actually the case for all Art_K.

Definition 2.4. Let M be a topological group. The **profinite completion** $\widehat{M}$ is defined as

$$\widehat{M} := \varprojlim_{M \twoheadrightarrow Q,\ Q \text{ finite}} Q.$$

The profinite completion $\widehat{M}$ is regarded as a topological group, endowed with the inverse limit topology, with each finite quotient Q having the discrete topology (i.e. any subset of Q is open). There is a natural map $M \to \widehat{M}$ from definition of the inverse limit. We call M **profinite** if $M \to \widehat{M}$ is an isomorphism of topological groups.

For a rational prime $p \in \mathbb{Z}$, a profinite group M is called **pro-p** if every finite quotient of M is a p-group (i.e. of order a power of p).

Example 2.5. (1) For any Galois extension (maybe infinite) K/L, $\mathrm{Gal}(K/L)$ with its topology is a profinite group.

(2) $\widehat{\mathbb{Z}}$ is a profinite group.

(3) $\mathbb{Z}_p$ is a pro-p group.

Lemma 2.6. *A profinite group is compact, Hausdorff, and totally disconnected (i.e. every connected component is a singleton). Conversely, a compact, Hausdorff, totally disconnected topological group is a profinite group.*

Proof. Exercise. □

Theorem 2.7 (Local existence theorem)**.** *Let L be a local field. There exists an inclusion-reversing one-to-one correspondence,*

$$\left\{\textit{Open finite index subgroups of } L^\times\right\} \leftrightarrow \{\textit{Finite abelian extensions of } L\},$$

where the maps in both directions are given by

$$H \mapsto (L^{\mathrm{ab}})^{\mathrm{Art}_L(H)},$$

$$N_{K/L}(K^\times) \mapsfrom K/L.$$

If L is of characteristic 0, the adjective "open" is unnecessary.

Thus, if L is of characteristic 0, the local Artin reciprocity map $\mathrm{Art}_L : L^\times \to \mathrm{Gal}(L^{\mathrm{ab}}/L)$ becomes an isomorphism of topological groups after passing to the profinite completion:

$$\mathrm{Art}_L : \widehat{L^\times} \xrightarrow{\sim} \mathrm{Gal}(L^{\mathrm{ab}}/L).$$

From this, already we have some information about the ramification.

Corollary 2.8. *Let K/L be a finite abelian extension of local fields.*

(1) We have

$$e_{K/L} = [\mathcal{O}_L^\times : N_{K/L}(\mathcal{O}_K^\times)].$$

(2) The extension K/L is unramified if and only if $\mathfrak{f}_{K/L} = 0$.

(3) The extension K/L is tamely ramified if and only if $\mathfrak{f}_{K/L} \leq 1$.

Proof. (1) You may find the proof at [ANT, Corollary 15.15].

(2) Obvious from (1).

(3) Suppose that K/L is tamely ramified. Note that

$$\mathcal{O}_L^\times \supset 1+\pi_L\mathcal{O}_L \supset 1+\pi_L^2\mathcal{O}_L \supset \cdots,$$

is a filtration of subgroups, where π_L is a uniformizer of L. Note that $1+\pi_L\mathcal{O}_L \cong \mathcal{O}_L$ as an additive topological group, so it is a pro-p group. On the other hand, $\mathcal{O}_L^\times/(1+\pi_L\mathcal{O}_L) \cong l^\times$, where l is the residue field of L, so in particular this index is coprime to p. So we have again a filtration of subgroups

$$\mathcal{O}_L^\times \supset (1+\pi_L\mathcal{O}_L)\cdot N_{K/L}(\mathcal{O}_K^\times) \supset (1+\pi_L^2\mathcal{O}_L)\cdot N_{K/L}(\mathcal{O}_K^\times) \supset \cdots,$$

where this now stabilizes after a finitely many steps. Now any subquotient that is not the first subquotient must be a p-group, but also it is a subquotient of $\mathcal{O}_L^\times/N_{K/L}(\mathcal{O}_K^\times)$, which is of order coprime to p. Therefore, all subquotients after the first subquotient must be trivial. Thus, $(1+\pi_L\mathcal{O}_L)\cdot N_{K/L}(\mathcal{O}_K^\times) = N_{K/L}(\mathcal{O}_K^\times)$, which implies that $N_{K/L}(\mathcal{O}_K^\times) \supset 1+\pi_L\mathcal{O}_L$, or $\mathfrak{f}_{K/L} \leq 1$. The converse direction is immediate.

□

We will later see that the local Artin reciprocity precisely works as we expected with ramification subgroups.

Theorem 2.9. *Let K/L be a finite abelian extension of local fields, and let $n \geq 1$. Then,*

$$\mathrm{Art}_{K/L}(1+\pi_L^n\mathcal{O}_L) = \mathrm{Gal}(K/L)^n,$$

where π_L is a uniformizer of L. More precisely, $\mathrm{Art}_{K/L}$ gives rise to an isomorphism

$$\frac{1+\pi_L^n\mathcal{O}_L}{(1+\pi_L^n\mathcal{O}_L)\cap N_{K/L}(\mathcal{O}_K^\times)} \xrightarrow{\sim} \mathrm{Gal}(K/L)^n.$$

3. (Co)homology of groups

The construction and the proof of local Artin reciprocity law will follow a very general framework using group cohomology, where the same framework will be used for the proof of global class field theory.

3.1. G-modules.

We are interested in the following situation. Let G be a group (not necessarily abelian). Then a G-**module** is an abelian group (=$\mathbb{Z}$-module) with a left G-action. This is the same as a left $\mathbb{Z}[G]$-module, where $\mathbb{Z}[G]$ is the group ring

$$\mathbb{Z}[G] = \{\sum_{g\in G} a_g[g] \;:\; a_g \in \mathbb{Z},\ \text{only nonzero for finitely many } g\},$$

where the multiplication is given by $[gh] = [g][h]$. Note that this is a ring with unity but not necessarily commutative (commutative if and only if G is abelian). A homomorphism between G-modules (I will use the words G-**morphism** or G-**homomorphism** for such a homomorphism) is a homomorphism of abelian groups which respects the G-actions on the source and the target. For two G-modules M, N, the set of G-morphisms is denoted $\mathrm{Hom}_G(M,N)$ (or $\mathrm{Hom}_{\mathbb{Z}[G]}(M,N)$), and it is naturally an (additive) abelian group. Let Mod_G be the category of G-modules.

Example 3.1. Two typical examples of G-modules are $\mathbb{Z}$ (with the trivial G-action) and $\mathbb{Z}[G]$ (with the obvious left G-action). The trivial G-module $\mathbb{Z}$ can be also thought as $\mathbb{Z} = \mathbb{Z}[G]/I$ where I is the two-sided ideal of $\mathbb{Z}[G]$ generated by the elements of the form $[g] - 1$ for $g \in G$. This ideal I is called the **augmentation ideal**.

Proposition 3.2. *The category* Mod_G *is an abelian category, i.e. the kernel and the cokernel exist and have desired properties.*

Proof. This follows from that (left) G-modules are the same as left $\mathbb{Z}[G]$-modules. □

Recall that there are notions of **injective modules** and **projective modules** from homological/commutative algebra (see Wikipedia for example for the definitions). One way to say is that I is injective if $\mathrm{Hom}(\cdot, I)$ is exact (P is projective if $\mathrm{Hom}(P, \cdot)$ is exact, respectively).

Definition 3.3. An abelian category $\mathcal{C}$ is called to have **enough injectives** (**enough projectives**, respectively) if, for every object $X \in \mathrm{Ob}(\mathcal{C})$, there exists an injective morphism $X \hookrightarrow I$ into an injective module I (a surjective morphism $P \twoheadrightarrow X$ from a projective module P, respectively).

Given an abelian category $\mathcal{C}$ with enough injectives and an object $X \in \mathrm{Ob}(\mathcal{C})$, you can always find an **injective resolution** $X \to I^\bullet$, which is an exact sequence

$$0 \to X \to I^0 \to I^1 \to I^2 \to \cdots,$$

which may or may not extend indefinitely to the right, where each of $I^0, I^1, \cdots$ is an injective module.

Similarly, given an abelian category $\mathcal{C}$ with enough projectives and an object $X \in \mathrm{Ob}(\mathcal{C})$, you can always find an **projective resolution** $P_\bullet \to X$, which is an exact sequence

$$\cdots \to P_2 \to P_1 \to P_0 \to X \to 0,$$

which may or may not extend indefinitely to the left, where each of $P_0, P_1, \cdots$ is a projective module.

Proposition 3.4. *The category* Mod_G *has enough projectives and injectives.*

Proof. This follows from that (left) G-modules are the same as left $\mathbb{Z}[G]$-modules. □

Example 3.5. A **free G-module** is a direct sum of copies of $\mathbb{Z}[G]$, namely $\bigoplus_{i \in I} \mathbb{Z}[G]$ for some index set I (note that I may be infinite). **Any free G-module is a projective G-module.** In practice, when you look for projective G-modules, most of the time you look for free G-modules (e.g. when you find a projective resolution).

To find an example of injective G-modules, we introduce useful tools of constructing G-modules.

Definition 3.6. Let $H \leq G$ be a subgroup. The **induction** is a functor $\mathrm{Ind}_H^G : \mathrm{Mod}_H \to \mathrm{Mod}_G$ that is defined by

$$\mathrm{Ind}_H^G M := \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], M),$$

where the G-action is given by $(g \cdot \varphi)(\alpha) = \varphi(\alpha g^{-1})$ for $\varphi : \mathbb{Z}[G] \to M$ and $g \in G$. The **coinduction** (or **compact induction**) is a functor $\operatorname{coInd}_H^G : \mathrm{Mod}_H \to \mathrm{Mod}_G$ defined by

$$\operatorname{coInd}_H^G M := \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M,$$

where the left $\mathbb{Z}[G]$-module structure is given naturally by the tensor product. The **restriction** is a functor $\operatorname{Res}_H^G : \mathrm{Mod}_G \to \mathrm{Mod}_H$ that sends a G-module M into itself, M, regarded as an H-module (which is certainly possible as $H \leq G$).

Remark 3.7 (Ind vs. coInd)**.** As you will see below, oftentimes $\operatorname{Ind}_H^G M$ and $\operatorname{coInd}_H^G M$ turn out to be isomorphic. Some references therefore do not bother to distinguish between Ind_H^G and coInd_H^G. However, they are not isomorphic in a natural way (i.e. not functorial in M), and in representation theory it is ultimately important to distinguish the two.

The following are true; many of them are abstract nonsenses.

Theorem 3.8. *Let $H \leq G$ be a subgroup.*

*(1) (**Frobenius reciprocity**) For $M \in \mathrm{Ob}(\mathrm{Mod}_G)$ and $N \in \mathrm{Ob}(\mathrm{Mod}_H)$,*

$$\mathrm{Hom}_H(\operatorname{Res}_H^G M, N) \cong \mathrm{Hom}_G(M, \operatorname{Ind}_H^G N).$$

The identification is natural, i.e. is functorial in M and N.

*(2) (**Frobenius reciprocity**) For $M \in \mathrm{Ob}(\mathrm{Mod}_H)$ and $N \in \mathrm{Ob}(\mathrm{Mod}_G)$,*

$$\mathrm{Hom}_G(\operatorname{coInd}_H^G M, N) \cong \mathrm{Hom}_H(M, \operatorname{Res}_H^G N).$$

The identification is natural, i.e. is functorial in M and N.

*(3) **Suppose that H is a finite index subgroup of G.** Then, for any H-module M,*

$$\operatorname{Ind}_H^G M \cong \operatorname{coInd}_H^G M.$$

(4) Let M be a projective H-module. Then, $\operatorname{coInd}_H^G M$ is a projective G-module.

(5) Let M be an injective H-module. Then, $\operatorname{Ind}_H^G M$ is an injective G-module.

(6) The functors Ind_H^G, coInd_H^G and Res_H^G are exact.

(7) Let M be a projective (injective, respectively) G-module. Then, $\operatorname{Res}_H^G M$ is a projective (injective, respectively) H-module.

Proof. (1), (2) are consequences of tensor-hom adjunction (you have to be careful about left vs. right actions). (4), (5) are consequences of (1), (2). For example, if M is projective, $\operatorname{coInd}_H^G M$ is projective, as $\mathrm{Hom}_G(\operatorname{coInd}_H^G M, -) = \mathrm{Hom}_H(M, \operatorname{Res}_H^G(-))$ is exact; $\mathrm{Hom}_H(M, -)$ is exact by the projectivity of M, and Res_H^G is exact by (1) and (2). For (6), we use the fact that $\mathbb{Z}[G]$ is a projective H-module, as it is the same as $\operatorname{coInd}_H^G \mathbb{Z}[H]$, and $\mathbb{Z}[H]$ is a projective H-module.

Then, Ind_H^G being exact is precisely the property of $\mathbb{Z}[G]$ being a projective $\mathbb{Z}[H]$-module, and coInd_H^G being exact follows from the general abstract nonsense that projective modules are **flat** (i.e. the functor of taking a tensor product with a fixed projective module is exact). From (6), (7) follow easily from the Frobenius reciprocities, just how (4) and (5) follow from the Frobenius reciprocities.

Really the nontrivial (non-abstract-nonsense) part is (3). Let $\phi_0 : M \to \operatorname{Ind}_H^G(M)$ be an H-morphism defined by

$$\phi_0(m)(g) = \begin{cases} gm & \text{if } g \in H \\ 0 & \text{otherwise.} \end{cases}$$

This $\phi_0 \in \operatorname{Hom}_H(M, \operatorname{Res}_H^G \operatorname{Ind}_H^G(M))$ corresponds to $\phi \in \operatorname{Hom}_G(\operatorname{coInd}_H^G M, \operatorname{Ind}_H^G M)$ (which exists regardless of the assumption). On the other hand, there is a map $\psi : \operatorname{Ind}_H^G M \to \operatorname{coInd}_H^G M$ given by

$$\psi(f) = \sum_{g \in G/H} g \otimes f(g^{-1}).$$

Note that here we use that G/H is of finite order. It is now left as an exercise to the reader that

- ψ is well-defined,
- ψ is a G-morphism,
- and ϕ and ψ are inverses to each other.

□

Example 3.9. Using Theorem 3.8(5), we can now construct many injective G-modules. Firstly, when G is a trivial group, what is an injective G-module, or what is an injective $\mathbb{Z}$-module? It turns out that an abelian group = $\mathbb{Z}$-module is injective if and only if it is **divisible**; i.e., any element is divisible by any nonzero element. Standard examples of divisible groups are $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$. We can then say that $\operatorname{Ind}_{\{1\}}^G M$ for a divisible group M is an injective G-module.

3.2. Group (co)homology: definition.

As Mod_G has enough injectives/projectives, we can take right/left derived functors of left/right exact functors. We derive the following two particular functors.

Definition 3.10 (G-invariants)**.** For $M \in \operatorname{Ob}(\operatorname{Mod}_G)$, we define

$$M^G := \{m \in M \ : \ gm = m \text{ for all } g \in G\}.$$

In other words, $M^G = \operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$.

Definition 3.11 (G-coinvariants)**.** For $M \in \operatorname{Ob}(\operatorname{Mod}_G)$, we define

$$M_G := M/\langle gm - m \ : \ g \in G, m \in M\rangle.$$

In other words, $M_G = M/IM = \mathbb{Z} \otimes_{\mathbb{Z}[G]} M$ (I is the augmentation ideal, see Example 3.1).

By definition, the G-invariants functor is left exact, and the G-coinvariants functor is right exact.

Definition 3.12 (Group cohomology/homology)**.** Let $H^i(G,-) : \mathrm{Mod}_G \to \mathrm{Mod}_{\mathbb{Z}}$ be the right derived functor of the G-invariants functor $(-)^G : \mathrm{Mod}_G \to \mathrm{Mod}_{\mathbb{Z}}$, called the **$i$-th group cohomology**. Similarly, let $H_i(G,-) : \mathrm{Mod}_G \to \mathrm{Mod}_{\mathbb{Z}}$ be the left derived functor of the G-coinvariants functor $(-)_G : \mathrm{Mod}_G \to \mathrm{Mod}_{\mathbb{Z}}$, called the **$i$-th group homology**.

By the similar reason, the $\mathrm{Ext}^i_{\mathbb{Z}[G]}$ and $\mathrm{Tor}_i^{\mathbb{Z}[G]}$ exist, and

$$H^i(G,M) = \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, M), \quad H_i(G,M) = \mathrm{Tor}_i^{\mathbb{Z}[G]}(\mathbb{Z}, M).$$

Therefore, there are two major ways to compute the group (co)homology:

- For $H^i(G,M)$:
  - Take a projective resolution $P_\bullet \to \mathbb{Z}$ of $\mathbb{Z}$, and compute the i-th homology of the complex
  $$\mathrm{Hom}_{\mathbb{Z}[G]}(P_0, M) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, M) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_2, M) \to \cdots .$$
  - Take an injective resolution $M \to I^\bullet$ of M, and compute the i-th homology of the complex
  $$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, I^0) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, I^1) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, I^2) \to \cdots .$$
- For $H_i(G,M)$:
  - Take a projective resolution $P_\bullet \to \mathbb{Z}$ of $\mathbb{Z}$, and compute the i-th cohomology of the complex
  $$\cdots \to P_2 \otimes_{\mathbb{Z}[G]} M \to P_1 \otimes_{\mathbb{Z}[G]} M \to P_0 \otimes_{\mathbb{Z}[G]} M.$$
  - Take a projective resolution $P_\bullet \to M$ of M, and compute the i-th cohomology of the complex
  $$\cdots \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} P_2 \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} P_1 \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} P_0.$$

Remark 3.13 (Acyclic resolutions)**.** A posteriori, you can instead use an **acyclic resolution** to compute the group cohomology. Recall that $M \in \mathrm{Ob}(\mathrm{Mod}_G)$ is **acyclic** if $H^i(G,M) = 0$ for $i > 0$. Then, instead of an injective resolution, you may use an acyclic resolution $M \to A^\bullet$ (meaning that $0 \to M \to A^0 \to A^1 \to \cdots$ is an exact sequence, with each A^i acyclic) to compute $H^i(G,M)$. This is useful as injective modules are weird (unlike projective or acyclic modules).

Abstract nonsense pays you off:

Theorem 3.14.

(1) *The group cohomology $H^\bullet(G,-)$ and the group homology $H_\bullet(G,-)$ have the expected properties, most notably $H^0(G,-) = (-)^G$, $H_0(G,-) = (-)_G$, and the long exact sequence associated with a short exact sequence of G-modules.*

(2) *(**Shapiro's lemma**) For $H \leq G$, and for $M \in \mathrm{Ob}(\mathrm{Mod}_H)$, we have*

$$H^i(G, \operatorname{Ind}_H^G M) = H^i(H, M),$$

$$H_i(G, \operatorname{coInd}_H^G M) = H_i(H, M).$$

The identifications are functorial in M.

(3) *For any $\mathbb{Z}$-module M, $\operatorname{Ind}_{\{1\}}^G M$ is an acyclic G-module.*

Proof.

(1) This is an immediate consequence of the two functors being derived functors.

(2) Let $M \to I^\bullet$ be an injective resolution of M. Then, as Ind_H^G is exact and sends injectives to injectives (Theorem 3.8), $\operatorname{Ind}_H^G(M) \to \operatorname{Ind}_H^G(I^\bullet)$ is an injective resolution of $\operatorname{Ind}_H^G(M)$. By Frobenius reciprocity, the complex

$$\operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, \operatorname{Ind}_H^G(I^0)) \to \operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, \operatorname{Ind}_H^G(I^1)) \to \operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, \operatorname{Ind}_H^G(I^2)) \to \cdots,$$

is the same as

$$\operatorname{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}, I^0) \to \operatorname{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}, I^1) \to \operatorname{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}, I^2) \to \cdots,$$

using the fact that $\operatorname{Res}_H^G \mathbb{Z} = \mathbb{Z}$. Thus $H^i(G, \operatorname{Ind}_H^G M)$ and $H^i(H, M)$ are computed by the same complex.

Similarly, let $P_\bullet \to M$ be a projective resolution of M. Then, as coInd_H^G is exact and sends projectives to projectives, $\operatorname{coInd}_H^G(P_\bullet) \to \operatorname{coInd}_H^G(M)$ is a projective resolution of $\operatorname{coInd}_H^G(M)$. The complex

$$\cdots \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} \operatorname{coInd}_H^G(P_2) \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} \operatorname{coInd}_H^G(P_1) \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} \operatorname{coInd}_H^G(P_0),$$

is just

$$\cdots \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} (\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} P_2) \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} (\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} P_1) \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} (\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} P_0),$$

which is the same (because $\mathbb{Z} \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G] = \mathbb{Z}$) as

$$\cdots \to \mathbb{Z} \otimes_{\mathbb{Z}[H]} P_2 \to \mathbb{Z} \otimes_{\mathbb{Z}[H]} P_1 \to \mathbb{Z} \otimes_{\mathbb{Z}[H]} P_0.$$

Therefore, $H_i(G, \operatorname{coInd}_H^G M)$ and $H_i(H, M)$ are computed by the same complex.

(3) By Shapiro's lemma, it suffices to show that M is an acyclic $\mathbb{Z}$-module, i.e. $H^i(\{1\}, M) = 0$ for $i > 0$. On the other hand, as $\mathbb{Z}$ is a projective $\mathbb{Z}$-module, $H^i(\{1\}, M) = \operatorname{Ext}^i_{\mathbb{Z}}(\mathbb{Z}, M)$ must be zero if $i > 0$ ($0 \to \mathbb{Z} \to \mathbb{Z} \to 0$ is a projective resolution).

□

A general abstract nonsense gives you a further functoriality in chainging both G and M. Note that the change of G is a different direction than the change of M for $H^i(G, M)$ (i.e. "contravariant in G").

Theorem 3.15. *Let $\alpha : G' \to G$ be a group homomorphism, and let $M \in \mathrm{Ob}(\mathrm{Mod}_G)$ and $M' \in \mathrm{Ob}(\mathrm{Mod}_{G'})$. Suppose that we have a homomorphism $\beta : M \to M'$ as abelian groups. Suppose further that β respects the group actions via α: namely, if $g \in G'$, $m \in M$, we have*

$$\beta(\alpha(g) \cdot m) = g \cdot \beta(m).$$

Then, there is a natural transformation between two derived functors $H^i(G, M) \to H^i(G', M')$, extending the map $H^0(G, M) \to H^0(G', M')$ given by $M^G \to (M')^{G'}$.

Proof. This is a general abstract nonsense in homological algebra; you just check that the setup indeed gives a map $M^G \to (M')^{G'}$. □

From this, we get several new useful functors.

Definition 3.16 (Restriction)**.** Let $H \leq G$ be a subgroup and $M \in \mathrm{Ob}(\mathrm{Mod}_G)$. Then, the action of G on M is surely compatible with the action of H on M (or more precisely $\mathrm{Res}_H^G M$). Thus the functoriality gives a homomorphism called the **restriction** homomorphism,

$$\mathrm{Res} : H^i(G, M) \to H^i(H, \mathrm{Res}_H^G M).$$

Exercise 3.1. Check that $\mathrm{Res} : H^i(G, M) \to H^i(H, \mathrm{Res}_H^G M)$ coincides with the composition

$$H^i(G, M) \to H^i(G, \mathrm{Ind}_H^G \mathrm{Res}_H^G M) \xrightarrow{\sim} H^i(H, \mathrm{Res}_H^G M),$$

where the first map comes from the natural G-morphism $M \to \mathrm{Ind}_H^G \mathrm{Res}_H^G M$ corresponding to the identity in $\mathrm{Hom}_H(\mathrm{Res}_H^G M, \mathrm{Res}_H^G M) = \mathrm{Hom}_G(M, \mathrm{Ind}_H^G \mathrm{Res}_H^G M)$, and the second map is the Shapiro's lemma.

Definition 3.17 (Inflation)**.** Let $H \trianglelefteq G$ be a **normal subgroup**. For a G-module M, G/H naturally acts on M^H. Using the maps $G \to G/H$ and $M^H \to M$, we obtain the **inflation** homomorphism

$$\mathrm{Inf} : H^i(G/H, M^H) \to H^i(G, M).$$

Another perspective you can get from this functoriality is that sometimes you can give a natural group action on $H^i(G, M)$. Let's say you consider $H^0(G, M) = M^G$. Then, obviously the G-action on it is trivial. However, if M is a G-module and $H \trianglelefteq G$ is a normal subgroup, then $H^0(H, M) = M^H$ has a natural action of G/H. This extends to $H^i(H, M)$.

Definition 3.18. Let $H \trianglelefteq G$ be a normal subgroup, and M be a G-module. Then, for $g \in G$, we obtain an action $g\cdot : H^i(H, M) \to H^i(H, M)$ given by the funtoriality via $\alpha : H \to H$, $h \mapsto g^{-1}hg$ and $\beta : M \to M$, $m \mapsto gm$. One can check (exercise!) that this map is the identity if $g \in H$. Thus, this gives rise to a left G/H-action on $H^i(H, M)$.

Exercise 3.2. Show that the H-action on $H^i(H, M)$ is trivial.

Exercise 3.3. Show that, if $H \trianglelefteq G$, the image of $\mathrm{Res} : H^i(G, M) \to H^i(H, \mathrm{Res}^G_H M)$ is inside $H^i(H, \mathrm{Res}^G_H M)^{G/H}$.

There is one more functor which does not fit into the above regime but rather comes from the coincidence $\mathrm{coInd} \cong \mathrm{Ind}$ when $H \leq G$ is of finite index.

Definition 3.19 (Corestriction). Suppose that $H \leq G$ is a **finite index subgroup**. Let M be a G-module. Then the **corestriction** homomorphism is defined as the composition

$$\mathrm{Cor} : H^i(H, \mathrm{Res}^G_H M) \xrightarrow{\sim} H^i(G, \mathrm{Ind}^G_H \mathrm{Res}^G_H M) \to H^i(G, M),$$

where the first map is the Shapiro's lemma, and the second map comes from the G-morphism $\mathrm{Ind}^G_H \mathrm{Res}^G_H M \to M$ given by

$$(\varphi : \mathbb{Z}[G] \to M) \mapsto \sum_{g \in G/H} g\varphi([g^{-1}]).$$

One can check that this map is well-defined, i.e. does not depend on the choice of a representative for each coset of G/H. Note that, on H^0, Cor is the **norm map**,

$$M^H \to M^G, \quad m \mapsto \sum_{g \in G/H} gm.$$

Lemma 3.20. *Suppose that $H \leq G$ is a finite index subgroup, and let M be a G-module. Then,* $\mathrm{Cor} \circ \mathrm{Res}$ *is the same as multiplying by* $[G : H]$ *on* $H^i(G, M)$.

Proof. This comes from the fact that the composition $M \to \mathrm{Ind}^G_H \mathrm{Res}^G_H M \to M$ of the two maps appearing in the definitions of Cor and Res is multiplication by $[G : H]$, namely $m \in M$ is first sent to $\varphi : \mathbb{Z}[G] \to M$ that sends $g \mapsto gm$, and is then sent to $\sum_{g \in G/H} g \cdot (g^{-1}m) = \sum_{g \in G/H} m = [G : H]m$. □

Corollary 3.21. *If G is a finite group of order m, then for any $i > 0$, $mH^i(G, M) = 0$ for any G-module M.*

Proof. This follows from Lemma 3.20 applied to $H = \{1\}$ and the fact that $H^i(\{1\}, -)$ is zero for any $i > 0$. □

Finally, as expected for cohomology, there is a notion of **cup product**.

Definition 3.22. Let $M, N \in \mathrm{Ob}(\mathrm{Mod}_G)$, and consider $M \otimes_{\mathbb{Z}} N$ as a G-module where the action is given by $g(m \otimes n) = gm \otimes gn$. Then, there is a unique bi-$\mathbb{Z}$-linear pairing

$$\cup : H^r(G, M) \times H^s(G, N) \to H^{r+s}(G, M \otimes N),$$

which is functorial in both M and N, satisfying several properties, such as the following.

(1) When $r = s = 0$, the pairing is the obvious map $M^G \otimes N^G \to (M \otimes N)^G$.

(2) $(x \cup y) \cup z = x \cup (y \cup z)$.

(3) $x \cup y = (-1)^{rs} y \cup x$ when $x \in H^r(G, M)$, $y \in H^s(G, N)$, after identifying $M \otimes N$ with $N \otimes M$.

(4) $\mathrm{Res}(x \cup y) = \mathrm{Res}(x) \cup \mathrm{Res}(y)$.

(5) $\mathrm{Cor}(x \cup \mathrm{Res}\, y) = \mathrm{Cor}(x) \cup y$.

(6) $\mathrm{Inf}(x \cup y) = \mathrm{Inf}(x) \cup \mathrm{Inf}(y)$.

3.3. **Group (co)homology: practice.** The main computational way of approaching group (co)homology is to use a very particular projective (free, in fact) resolution of $\mathbb{Z}$.

Definition 3.23. For $r \geq 0$, let P_r be the free $\mathbb{Z}$-module with basis $(g_0, \cdots, g_r)$ for $g_0, \cdots, g_r \in G$, with a G-action given by $g(g_0, \cdots, g_r) = (gg_0, \cdots, gg_r)$. It is easy to see that P_r is a free $\mathbb{Z}[G]$-module. Let $d_r : P_r \to P_{r-1}$ be a G-morphism defined by

$$d_r(g_0, \cdots, g_r) = \sum_{i=0}^{r} (-1)^i (g_0, \cdots, \widehat{g_i}, \cdots, g_r),$$

where the notation means that g_i is omitted from the tuple in the summand.

It is a tedious yet elementary exercise to check that

$$\cdots \to P_r \xrightarrow{d_r} P_{r-1} \to \cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0,$$

is a projective resolution of $\mathbb{Z}$, where $\varepsilon : P_0 \to \mathbb{Z}$ is the map that sends $(g) \mapsto 1$ for each $g \in G$. Using this, we can compute the group cohomology (there is a similar description for group homology but we don't bother to write).

Proposition 3.24. *Let $M \in \mathrm{Ob}(\mathrm{Mod}_G)$. An r-**cochain** of G with values in M is any function $\varphi : G^r \to M$, and let $C^r(G, M)$ be the (additive) abelian group of r-cochains of G with values in M. Let $d^r : C^r(G, M) \to C^{r+1}(G, M)$ be defined by*

$$(d^r \varphi)(g_1, \cdots, g_{r+1}) :=$$

$$g_1 \varphi(g_2, \cdots, g_{r+1}) + \sum_{j=1}^{r} (-1)^j \varphi(g_1, \cdots, g_{j-1}, g_j g_{j+1}, g_{j+2}, \cdots, g_{r+1}) + (-1)^{r+1} \varphi(g_1, \cdots, g_r).$$

*Let $Z^r(G, M) = \ker d^r$ (the group of r-**cocycles**) and $B^r(G, M) = \mathrm{im}\, d^{r-1}$ (the group of r-**coboundaries**). Then, $H^r(G, M) \cong \frac{Z^r(G,M)}{B^r(G,M)}$.*

Proof. This is really just computing $H^r(G, M)$ using the projective resolution $P_\bullet \to \mathbb{Z}$, but using the fact that a morphism in $\mathrm{Hom}_G(P_r, M)$ is determined by its values at $(1, g_1, g_1 g_2, \cdots, g_1 g_2 \cdots g_{r+1})$. □

Using this, we have a more concrete description of certain things.

Example 3.25. The first cohomology $H^1(G,M)$ is computed as $\frac{B^1(G,M)}{Z^1(G,M)}$. Let's see what they parametrize:

$$B^1(G,M) = \{\varphi : G \to M \ : \ \varphi(gh) = g\varphi(h) + \varphi(g)\},$$
$$Z^1(G,M) = \{\varphi : G \to M \ : \ \text{there is } a \in M \text{ such that } \varphi(g) = ga - a \text{ for all } g \in G\}.$$

Often the elements of $B^1(G,M)$ are called **crossed homomorphisms** because the equation $\varphi(gh) = g\varphi(h) + \varphi(g)$ looks like some weird variant of a condition of being a homomorphism. In fact, if the action of G on M is trivial, then this shows that $H^1(G,M) = \mathrm{Hom}_{\mathrm{Grp}}(G,M)$ is the set of group homomorphisms $G \to M$ (notice that M is always an abelian group by definition).

Example 3.26. Given a short exact sequence of G-modules $0 \to A \to B \to C \to 0$, we can now describe what the connecting morphism $H^r(G,C) \to H^{r+1}(G,A)$ is concretely. Namely, if you have an r-cocycle $\varphi : G^r \to C$ representing an element of $H^r(G,C)$, then you can certainly lift elementwise to obtain an r-cochain $\widetilde{\varphi} : G^r \to B$. By taking arbitrary lifts, it ruins the condition of vanishing after applying d^r, but at least you know $d^r\varphi = 0$, so $d^r\widetilde{\varphi} : G^{r+1} \to B$ is an $(r+1)$-cochain whose values after projecting to C will vanish. Therefore, it follows that $d^r\widetilde{\varphi}$ has values in A, so $d^r\widetilde{\varphi} : G^{r+1} \to A$ is an $(r+1)$-cochain with values in A. As $d^{r+1} \circ d^r = 0$, this implies that $d^r\widetilde{\varphi} \in Z^{r+1}(G,A)$, which represents an element in $H^{r+1}(G,A)$. It is a routine check that this map $H^r(G,C) \to H^{r+1}(G,A)$ does not depend on any choices we made.

Example 3.27. We can describe the cup product using cocycles as follows. Let $m \in H^r(G,M)$ and $n \in H^s(G,N)$ be represented by cocycles φ and ψ, respectively. Then, $m \cup n$ is represented by the cocycle

$$(g_1, \cdots, g_{r+s}) \mapsto \varphi(g_1, \cdots, g_r) \otimes g_1 \cdots g_r \psi(g_{r+1}, \cdots, g_{r+s}).$$

Using cochains, we can show the following.

Proposition 3.28 (Inflation-restriction exact sequence)**.** *Let $H \trianglelefteq G$ be a normal subgroup, and let A be a G-module. Then,*

$$0 \to H^1(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^1(G,A) \xrightarrow{\mathrm{Res}} H^1(H,A),$$

is exact. More generally, if furthermore one knows that $H^1(H,A) = H^2(H,A) = \cdots = H^t(H,A)$ for some $t \geq 2$, then

$$0 \to H^t(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^t(G,A) \xrightarrow{\mathrm{Res}} H^t(H,A),$$

is exact.

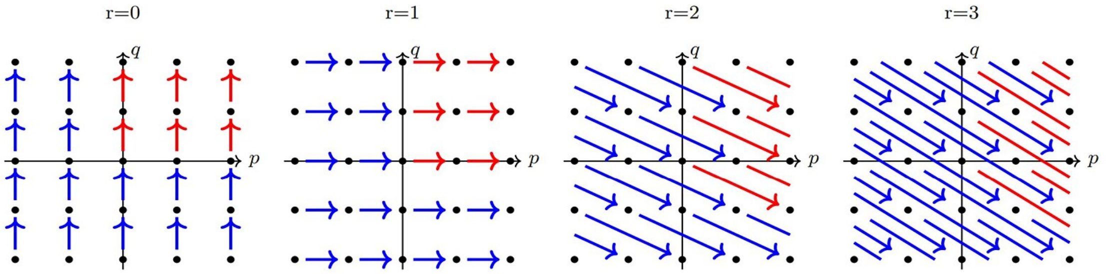
Proof. Exercise (the statement about H^1 can be easily shown using 1-cocycles, and the second statement follows from general properties of the cohomology functor). □

Remark 3.29 (Hochschild–Serre spectral sequence)**.** This result looks a bit arbitary. A better way to think about this is as a consequence of the Hochschild–Serre spectral sequence

$$E_2^{p,q} = H^p(G/H, H^q(H,A)) \Rightarrow H^{p+q}(G,A).$$

This is not actually that mysterious. The statement that “there is a spectral sequence converging to something” means something like the following (there are much more complicated versions of this, but at least in this setup, it’s explained as follows).

- A spectral sequence is a whole package of data.
  - For each $n \geq 0$, there is an n-th page of a spectral sequence $E_n^{p,q}$, for each $p, q \geq 0$ nonnegative integers.
  - Each n-th page also comes equipped with natural maps (**differentials**) $d_n^{p,q} : E_n^{p,q} \to E_n^{p+n,q-n+1}$. At each $E_n^{p,q}$, there is an arrow coming out of it ($d_n^{p,q}$) and an arrow coming into it ($d_n^{p-r,q+r-1}$), and two arrows form a complex (i.e. $d_n^{p,q} \circ d_n^{p-r,q+r-1} = 0$). Taking the homology at that (p,q)-th entry will give you the (p,q)-th entry of the next page, $E_{n+1}^{p,q}$.



- Many spectral sequences are written in the form

  $$E_2^{p,q} \Rightarrow E_\infty^{p+q}.$$

  This means the following.
  - Going from $E_n^{p,q}$ to $E_{n+1}^{p,q}$, you cut down certain parts (taking subquotients). That the spectral sequence **converges** means that eventually this stabilizes, i.e. there is some $N \gg 0$ such that $E_N^{p,q} = E_{N+1}^{p,q} = \cdots$. Sometimes you say that the spectral sequence **degenerates at n-th page**, which means that N can be taken to be n.
  - Let $E_\infty^{p,q}$ be the stabilized $E_n^{p,q}$ for large enough n. Then, E_∞^m is an object with a filtration

    $$0 = F^0 \subset F^1 \subset \cdots \subset F^m \subset F^{m+1} = E_\infty^m,$$

    such that, for $0 \leq i \leq m$, $F^{i+1}/F^i \cong E_\infty^{m-i,i}$.

Under this, the inflation-restriction exact sequence is an immediate consequence. Namely, $H^1(G, A) = E_\infty^1$. So, it sits in an exact sequence,

$$0 \to E_\infty^{1,0} \to H^1(G, A) \to E_\infty^{0,1} \to 0.$$

We see that $E_2^{1,0} = H^1(G/H, H^0(H, A)) = H^1(G/H, A^H)$, and $E_2^{0,1} = H^0(G/H, H^1(H, A)) = H^1(H, A)^{G/H}$. So let’s see how $E_\infty^{1,0}$ and $E_\infty^{0,1}$ may be different from $E_2^{1,0}$ and $E_2^{0,1}$.

- The differential from $E_n^{1,0}$ lands below the horizontal axis (when $n \geq 2$), which clearly vanishes. The differential to $E_n^{1,0}$ comes from $E_n^{1-n,n-2}$, so if $n \geq 2$, this is to the left of the vertical axis, so this also vanishes. This implies that $E_2^{1,0} = E_3^{1,0} = \cdots = E_\infty^{1,0}$.
- The differential to $E_n^{0,1}$ comes from the left of the vertical axis (when $n \geq 1$), which clearly vanishes. The differential from $E_n^{0,1}$ lands at $E_n^{n,2-n}$, so this is right on the horizontal axis when $n = 2$, and will land below the horizontal axis when $n \geq 3$. Thus, $E_3^{0,1} = \ker(d_2^{0,1} : E_2^{0,1} \to E_2^{2,0}) = E_4^{0,1} = \cdots = E_\infty^{0,1}$.

So we actually have an exact sequence

$$0 \to E_2^{1,0} \to H^1(G, A) \to E_2^{0,1} \xrightarrow{d_2^{0,1}} E_2^{2,0},$$

or

$$0 \to H^1(G/H, A^H) \to H^1(G, A) \to H^1(H, A)^{G/H} \xrightarrow{d_2^{0,1}} H^2(G/H, A^H).$$

It is a fun exercise to check that the first two maps are indeed Inf and Res (although it requires the knowledge of how spectral sequences are built). The differential $d_2^{0,1}$ is sometimes called the **transgression**. The second part of the statement of the inflation-restriction exact sequence is also a fun exercise which I will leave it to the reader.

We also have a very easy description of $H_1(G, \mathbb{Z})$.

Proposition 3.30. *We have $H_1(G, \mathbb{Z}) \cong G^{\mathrm{ab}}$, the abelianization of G.*

Proof. We have a short exact sequence $0 \to I \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$, so from this we have a long exact sequence

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

As $\mathbb{Z}[G]$ is projective, $H_i(G, \mathbb{Z}[G]) = 0$ for $i > 0$. Thus, we have an exact sequence

$$0 \to H_1(G, \mathbb{Z}) \to I/I^2 \to \mathbb{Z}[G]/I \to \mathbb{Z} \to 0.$$

As $\mathbb{Z}[G]/I \to \mathbb{Z}$ is an isomorphism, we have $H_1(G, \mathbb{Z}) \cong I/I^2$. We claim that $I/I^2 \cong G^{\mathrm{ab}}$. Let $G \to I/I^2$ be a map defined by $g \mapsto [g] - 1$. Then, it is a group homomorphism, as

$$[gh] - 1 = ([g] - 1)([h] - 1) + ([g] - 1) + ([h] - 1) \equiv ([g] - 1) + ([h] - 1) \pmod{I^2}.$$

As I/I^2 is an abelian group (additively), this map factors through $G^{\mathrm{ab}} \to I/I^2$. This map is quite obviously surjective (any element of I is a $\mathbb{Z}$-linear combination of elements of the form $[g] - 1$). To show it is injective, we form another homomorphism in the other direction. Consider $I \to G^{\mathrm{ab}}$ defined by $\sum_{g \in G} n_g[g] \mapsto g^{n_g}$, which is quite obviously a group homomorphism. Note that $([g] - 1)([h] - 1)$ is sent to $ghg^{-1}h^{-1} = \mathrm{id}$, so I^2 is in the kernel of this map, giving a group homomorphism $I/I^2 \to G/G^2$. And it is easy to see that $G^{\mathrm{ab}} \to I/I^2 \to G^{\mathrm{ab}}$ is identity, as $g \mapsto [g] - 1 \mapsto g$. Therefore, $G^{\mathrm{ab}} \to I/I^2$ is injective, thus bijective, as desired. □

We also describe a very useful technique called the **dimension shifting**.

Theorem 3.31 (Dimension shifting). *Let M be a G-module. Then, there are exact sequences of G-modules,*

$$0 \to I \otimes_{\mathbb{Z}} M \to \operatorname{coInd}_{\{1\}}^{G} M \to M \to 0,$$

where the map $\operatorname{coInd}_{\{1\}}^{G} M \to M$ *sends* $[g] \otimes m \mapsto m$, *and*

$$0 \to M \to \operatorname{Ind}_{\{1\}}^{G} M \to \operatorname{Hom}_{\mathbb{Z}}(I, M) \to 0,$$

where the map $M \to \operatorname{Ind}_{\{1\}}^{G} M$ *sends* $m \mapsto ([g] \mapsto m)$. *From this, we have, for* $n \geq 1$,

$$H^n(G, \operatorname{Hom}_{\mathbb{Z}}(I, M)) \cong H^{n+1}(G, M), \quad H_n(G, I \otimes_{\mathbb{Z}} M) \cong H_{n+1}(G, M).$$

Proof. The short exact sequences come from applying $\otimes_{\mathbb{Z}} M$ and $\operatorname{Hom}_{\mathbb{Z}}(-, M)$ to the exact sequence

$$0 \to I \to \mathbb{Z}[G] \to \mathbb{Z} \to 0,$$

which actually give you exact sequences, as $\mathbb{Z}$ is an acyclic $\mathbb{Z}$-module. The remaining statements come from Shapiro's lemma (that $H^n(G, \operatorname{Ind}_{\{1\}}^{G} M) = 0$ and $H_n(G, \operatorname{coInd}_{\{1\}}^{G} M) = 0$). □

When G is a cyclic group, $\mathbb{Z}$ has a particularly easy projective resolution.

Example 3.32. If $G = \mathbb{Z}$, then $\mathbb{Z}[G]$ can be regarded as $\mathbb{Z}[X^{\pm 1}]$. Then, $\mathbb{Z}$ has a projective resolution

$$0 \to \mathbb{Z}[X^{\pm 1}] \xrightarrow{\times (X-1)} \mathbb{Z}[X^{\pm 1}] \to \mathbb{Z} \to 0.$$

This implies that $H^i(\mathbb{Z}, M) = 0$ for $i > 1$. Furthermore, any $\mathbb{Z}[\mathbb{Z}]$-module M is an abelian group plus a group automorphism $X : M \to M$, so

$$H^0(\mathbb{Z}, M) = M^{X=1}, \quad H^1(\mathbb{Z}, M) = M / \langle Xm - m \ : \ m \in M \rangle.$$

Similarly, $H_i(\mathbb{Z}, M) = 0$ for $i > 1$, and

$$H_0(\mathbb{Z}, M) = M / \langle Xm - m \ : \ m \in M \rangle, \quad H_1(\mathbb{Z}, M) = M^{X=1}.$$

Example 3.33. When $G = \mathbb{Z}/n\mathbb{Z}$, then $\mathbb{Z}[G]$ can be regarded as $\mathbb{Z}[X]/(X^n - 1)$. Then, $\mathbb{Z}$ has a projective resolution

$$\cdots \to \mathbb{Z}[X]/(X^n - 1) \xrightarrow{\times (X^{n-1} + X^{n-2} + \cdots + 1)} \mathbb{Z}[X]/(X^n - 1) \xrightarrow{\times (X-1)} \mathbb{Z}[X]/(X^n - 1) \to \mathbb{Z} \to 0,$$

where the two maps alternate indefinitely. Note that a G-module M is an abelian group plus a group homomorphism $X : M \to M$ such that $X^n = \mathrm{id}$. Then,

$$H^i(\mathbb{Z}/n\mathbb{Z}, M) = \begin{cases} M^{X=1} & \text{if } i = 0 \\ \frac{\ker(X^{n-1} + X^{n-2} + \cdots + 1 : M \to M)}{\operatorname{im}(X - 1 : M \to M)} & \text{if } i > 0 \text{ is odd} \\ \frac{M^{X=1}}{\operatorname{im}(X^{n-1} + X^{n-2} + \cdots + 1 : M \to M)} & \text{if } i > 0 \text{ is even.} \end{cases}$$

Similarly,

$$H_i(\mathbb{Z}/n\mathbb{Z}, M) = \begin{cases} \frac{M}{\mathrm{im}(X-1:M\to M)} & \text{if } i = 0 \\ \frac{\ker(X^{n-1}+X^{n-2}+\cdots+1:M\to M)}{\mathrm{im}(X-1:M\to M)} & \text{if } i > 0 \text{ is even} \\ \frac{M^{X=1}}{\mathrm{im}(X^{n-1}+X^{n-2}+\cdots+1:M\to M)} & \text{if } i > 0 \text{ is odd.} \end{cases}$$

Note that the cohomology and homology groups have a lot in common in these cases. We will see that it is not a coincidence.

4. Galois cohomology

4.1. **Tate cohomology.** In this subsection, we assume that G is a **finite group**. In this case, given a G-module M, there is a very special operator called the **norm map** $N : M \to M$, given by $m \mapsto \sum_{g\in G} gm$. A funny thing is that the image of N is actually inside M^G, and anything in IM (recall that $I \subset \mathbb{Z}[G]$ is the augmentation ideal) is killed by N. Therefore, we have a homomorphism

$$N : H_0(G, M) \to H^0(G, M).$$

This gives a connecting bridge between the end of the homology and the end of the cohomology, and we can now "stitch together" the cohomology and the homology into one, called the **Tate cohomology**.

Definition 4.1 (Tate cohomology groups)**.** Let G be a finite group, and let M be a G-module. We define the r**-th Tate cohomology** $H_T^r(G, M)$ as

$$H_T^r(G, M) = \begin{cases} H^r(G, M) & \text{if } r > 0 \\ \mathrm{coker}(N : M_G \to M^G) & \text{if } r = 0 \\ \ker(N : M_G \to M^G) & \text{if } r = -1 \\ H_{-r-1}(G, M) & \text{if } r < -1. \end{cases}$$

Theorem 4.2 (Long exact sequence of Tate cohomology groups)**.** *Let G be a finite group, and let $0 \to A \to B \to C \to 0$ be a short exact sequence of G-modules. Then, there is a long exact sequence,*

$$\cdots \to H_T^r(G, A) \to H_T^r(G, B) \to H_T^r(G, C) \to H_T^{r+1}(G, A) \to H_T^{r+1}(G, B) \to H_T^{r+1}(G, C) \to \cdots ,$$

extending indefinitely to both sides.

Proof. The only care is required at around $r = -1, 0$ where we are stitching the ends of the two long exact sequences (homology and cohomology), and verification is very easy. □

Tate cohomology really behaves like cohomology, and the tools of cohomology extend to Tate cohomology groups as well. Note that, as G is finite, we don't have to distinguish between coinduction and induction, so we will just use induction for simplicity.

- (**Dimension shifting**) Let M be a G-module. Then,

  $$H_T^i(G, \operatorname{Ind}_{\{1\}}^G M) = 0,$$

  for all $i \in \mathbb{Z}$. We already know this for $i \neq 0, -1$. We also know that $H^0(G, \operatorname{Ind}_{\{1\}}^G M) = H_0(G, \operatorname{Ind}_{\{1\}}^G M) = M$ by Shapiro's lemma. We see that $N : M \to M$ in this case is given by the map $m \mapsto 1 \otimes m \mapsto \sum_{g \in G} g \otimes m \mapsto m$, so it is in fact an isomorphism. Thus, $H_T^{-1}(G, \operatorname{Ind}_{\{1\}}^G M) = H_T^0(G, \operatorname{Ind}_{\{1\}}^G M) = 0$.

  From this and the long exact sequence of Tate cohomology groups, we have

  $$H_T^i(G, \operatorname{Hom}_{\mathbb{Z}}(I, M)) \cong H_T^{i+1}(G, M), \quad H_T^i(G, I \otimes_{\mathbb{Z}} M) \cong H_T^{i-1}(G, M),$$

  for all $i \in \mathbb{Z}$. These will be useful for extending tools of cohomology to Tate cohomology.

- (**Shapiro's lemma**) Let $H \leq G$ be a subgroup, and let M be an H-module. Then,

  $$H_T^i(G, \operatorname{Ind}_H^G M) = H_T^i(H, M).$$

  This follows from Shapiro's lemma for $i \geq 1$ and dimension shifting for general $i \in \mathbb{Z}$.

- (**Restriction**) For $H \leq G$ and $M \in \operatorname{Ob}(\operatorname{Mod}_G)$, there is a restriction map

  $$\operatorname{Res} : H_T^i(G, M) \to H_T^i(H, \operatorname{Res}_H^G M),$$

  which is now an easy consequence of Shapiro's lemma and Frobenius reciprocity.

- (**Corestriction**) For $H \leq G$ and $M \in \operatorname{Ob}(\operatorname{Mod}_G)$, there is a corestriction map

  $$\operatorname{Cor} : H_T^i(H, \operatorname{Res}_H^G M) \to H_T^i(G, M),$$

  which exists again by Shapiro's lemma and Frobenius reciprocity.

- (**Cup product**) For $M, N \in \operatorname{Ob}(\operatorname{Mod}_G)$, we have a bi-$\mathbb{Z}$-linear pairing

  $$H_T^i(G, M) \times H_T^j(G, N) \to H_T^{i+j}(G, M \otimes N),$$

  satisfying the same kinds of properties the cohomological cup product satisfies.

We give a concrete description of Cor and Res for certain degrees of Tate cohomology groups.

Proposition 4.3. *Let G be a finite group and $H \leq G$. Let M be a G-module.*

(1) The map $\operatorname{Cor} : H_T^0(H, M) \to H_T^0(G, M)$ is induced by the map $M^H \to M^G$, $m \mapsto \sum_{g \in G/H} gm$.

(2) The map $\operatorname{Res} : H_T^{-1}(G, M) \to H_T^{-1}(H, M)$ is induced by the map $M_G \to M_H$, $m \mapsto \sum_{g \in G/H} g^{-1}m$.

(3) The map $\mathrm{Cor} : H_T^{-2}(H,\mathbb{Z}) \to H_T^{-2}(G,\mathbb{Z})$ *is the map* $H^{\mathrm{ab}} \to G^{\mathrm{ab}}$.

(4) The map $\mathrm{Res} : H_T^{-2}(G,\mathbb{Z}) \to H_T^{-2}(H,\mathbb{Z})$ *is the* ***transfer homomorphism*** $V : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ *(see Definition 2.2).*

Proof. Omitted (standard). □

Lemma 4.4. *Let* G *be a finite group of order* m. *Then, for any* G*-module* M, $mH_T^i(G,M) = 0$. *If* M *is finitely generated as an abelian group, then* $H_T^i(G,M)$ *is a finite abelian group.*

Proof. Similar to the cohomology case, the first statement follows from the fact that $\mathrm{Cor} \circ \mathrm{Res} = m$, now at all degrees of Tate cohomology. For the second statement, notice that $H_T^i(G,M)$ is, either by cochain or chain, a finitely generated abelian group. As the Tate cohomology group is a finitely generated abelian group annihilated by a nonzero integer, it is a finite abelian group. □

Just like before, the Tate cohomology has more structures when G is a finite cyclic group. Let $G = \mathbb{Z}/n\mathbb{Z}$, and let M be a G-module. This means that there is an automorphism $X : M \to M$ such that $X^n = 1$. Let $N : M \to M$ be defined by $X^{n-1} + X^{n-2} + \cdots + 1$. Then, by our previous computation,

$$H_T^i(G,M) = \begin{cases} \frac{\ker(X-1:M\to M)}{\mathrm{im}(N:M\to M)} & \text{if } i \text{ is even} \\ \frac{\ker(N:M\to M)}{\mathrm{im}(X-1:M\to M)} & \text{if } i \text{ is odd.} \end{cases}$$

This shows that $H_T^i(G,M)$ is **periodic with period** 2. In fact, given a choice of a generator $u \in H_T^2(G,\mathbb{Z})$, the cup-product with u gives an isomorphism $\cup u : H_T^i(G,M) \xrightarrow{\sim} H_T^{i+2}(G,M)$, $x \mapsto x \cup u$.

So what is $H_T^2(G,\mathbb{Z})$? Note that we have a short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$, so we have an exact sequence

$$\cdots \to H^1(G,\mathbb{Q}) \to H^1(G,\mathbb{Q}/\mathbb{Z}) \to H^2(G,\mathbb{Z}) \to H^2(G,\mathbb{Q}) \to \cdots .$$

As $\mathbb{Q}$ is divisible, by our computation, $H^1(G,\mathbb{Q}) = H^2(G,\mathbb{Q}) = 0$. Thus, $H_T^2(G,\mathbb{Z}) = H^2(G,\mathbb{Z}) = H^1(G,\mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_{\mathrm{Grp}}(G,\mathbb{Q}/\mathbb{Z}) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Taking a generator of $H_T^2(G,\mathbb{Z})$ is the same as taking a generator of G, as we can take an element of $\mathrm{Hom}_{\mathrm{Grp}}(G,\mathbb{Q}/\mathbb{Z})$ that sends a taken generator to $\frac{1}{n}$.

Using the periodicity of Tate cohomology for finite cyclic groups, we can define a numerical invariant:

Definition 4.5 (Herbrand quotient)**.** Let $G = \mathbb{Z}/n\mathbb{Z}$ and M be a G-module. Then, the **Herbrand quotient** is the rational number defined by

$$h(M) := \frac{\#H_T^0(G,M)}{\#H_T^{-1}(G,M)}.$$

Lemma 4.6. *Let* $G = \mathbb{Z}/n\mathbb{Z}$. *If* $0 \to A \to B \to C \to 0$ *is a short exact sequence of* G*-modules, then we have* $h(B) = h(A)h(C)$.

Proof. This follows from the long exact sequence of Tate cohomology and the periodicity. □

Lemma 4.7. *Let $G = \mathbb{Z}/n\mathbb{Z}$ and let M be a G-module which is also a finite abelian group. Then, $h(M) = 1$.*

Proof. Note that $H_T^0(G, M)$ and $H_T^{-1}(G, M)$ are the cokernel and the kernel of the same map $N : M_G \to M^G$. Thus, $h(M) = 1$ if we show that $\#M_G = \#M^G$. This follows again from the fact that M_G and M^G are the cokernel and the kernel of the same map $M \to M$, $m \mapsto gm - m$, where $g \in G$ is a chosen generator of G. □

4.2. **Cohomology of profinite groups.** For the group cohomology $H^i(G, M)$, we may ultimately want to put a profinite group into G. For this, we need to take topology into account. This is especially tricky because category of topological groups often fail to be abelian (when you take kernels and cokernels, what topology should you give to them?). For our purpose, we restrict the scope to very particular kinds of modules.

Definition 4.8 (Discrete G-modules)**.** Let G be a profinite group. Let M be a G-module, firstly without consideration of any topology. We say that M is a **discrete G-module** if the action map $G \times M \to M$ is continuous when M is endowed with the discrete topology. Equivalently, M is a discrete G-module if $M = \cup_{H \leq G \text{ open subgroup}} M^H$. Another equivalent condition is that, for every $m \in M$, $\{g \in G \ : \ gm = m\} \leq G$ is an open subgroup.

Example 4.9. Let $G = \mathrm{Gal}(K/L)$ for a Galois extension K/L (possibly infinite). Then, G acts on various objects such as K, $K^\times$, $\mathcal{O}_K$ (if it makes sense), $\mathcal{O}_K^\times$ (if it makes sense), etc. As stabilizer of any element $x \in K$ is $\mathrm{Gal}(K/L(x))$, and as $L(x)/L$ is a finite extension, $\mathrm{Gal}(K/L(x)) \leq \mathrm{Gal}(K/L)$ is an open subgroup. Thus, this means that all these G-modules are discrete.

As you don't have to worry too much about giving topology on the modules when they are discrete, the following holds.

Theorem 4.10. *Let G be a profinite group. Then, the category of discrete G-modules is an abelian category with enough injectives.*

Therefore, by abstract nonsense, one can right-derive a left-exact functor, and obtain the r-th cohomology functor $H^r(G, M)$ for any discrete G-module M. This cohomology fortunately has more concrete descriptions.

Theorem 4.11. *Let G be a profinite group, and let M be a discrete G-module. Then, $H^r(G, M)$ can be computed in two different ways.*

*(1) Let $C^r_{\text{cts}}(G, M)$ be the space of **continuous r-cochains** of G with values in M, i.e. $\varphi : G^r \to M$ that is continuous. Then, the differentials are defined as usual, and define $Z^r_{\text{cts}}(G, M)$ (**continuous r-cocycles**) and $B^r_{\text{cts}}(G, M)$ (**continuous r-coboundaries**). Then,*

$$H^r(G, M) \cong \frac{Z^r_{\text{cts}}(G, M)}{B^r_{\text{cts}}(G, M)}.$$

(2) The inflation morphisms give rise to a direct system $\{H^r(G/H, M^H)\}$ running over all open normal subgroups of H, and

$$H^r(G, M) \cong \varinjlim_{H \trianglelefteq G \text{ open normal}} H^r(G/H, M^H).$$

The proofs are omitted. Using these descriptions, we may still define things like $\mathrm{Cor}, \mathrm{Res}, \mathrm{Inf}$ and cup products.

Corollary 4.12. *Let G be a profinite group, and let M be a discrete G-module. Then, for $r > 0$, $H^r(G, M)$ is a torsion group.*

Proof. Any element of $H^r(G, M)$ comes from $H^r(G/H, M^H)$ for some open normal subgroup $H \trianglelefteq G$, which is necessarily of finite index, so the element is annihilated by $\#(G/H)$, thus torsion. □

4.3. **Galois cohomology.** We now compute the cohomology of Galois groups of fields.

Proposition 4.13 (Additive group case)**.** *Let K/L be a Galois extension of fields (may be infinite). Then, $H^r(\mathrm{Gal}(K/L), K) = 0$ for $r \geq 1$.*

Proof. As $H^r(\mathrm{Gal}(K/L), K) = \varinjlim_{K/M/L,\ M/L \text{ finite Galois}} H^r(\mathrm{Gal}(M/L), M)$, the general case follows from the finite extension case. So, assume that K/L is a finite Galois extension. Then, by normal basis theorem, there is $x \in K$ such that $\{\sigma(x) : \sigma \in \mathrm{Gal}(K/L)\}$ is an L-basis of K. This implies that $K \cong \mathrm{Ind}_{\{1\}}^{\mathrm{Gal}(K/L)} xL$ as $\mathrm{Gal}(K/L)$-modules. This implies that K is an acyclic $\mathrm{Gal}(K/L)$-module, which is what we want. □

More interesting is when the module is the multiplicative group; this is actually the main part of proving local class field theory.

Theorem 4.14. *Let K/L be a Galois extension of fields (may be infinite). Then, $H^1(\mathrm{Gal}(K/L), K^\times) = 0$.*

Proof. Again, as above, it suffices to assume that K/L is a finite Galois extension. Let $G = \mathrm{Gal}(K/L)$ for simplicity. Let $f : G \to K^\times$ be a 1-cocycle. Note that the Galois automorphisms of G are all linearly independent as functions over K. This implies that, as a function on K, the function $x \mapsto \left(\sum_{g \in G} f(g)g\right) x$ is not identically zero, as $f(g) \neq 0$. Let $y \in K^\times$ be the point where $z := \sum_{g \in G} f(g)gy \neq 0$. Then, for $h \in G$,

$$hz = \sum_{g \in G} hf(g) \cdot hgy = \sum_{g \in G} f(h)^{-1} f(hg) \cdot hgy = f(h)^{-1} \sum_{g' \in G} f(g') \cdot g'y = f(h)^{-1} z.$$

Thus, $f(h) = z \cdot h(z)^{-1}$, which implies that f is a 1-coboundary. □

Corollary 4.15 (Hilbert's Theorem 90)**.** *Let K/L be a finite cyclic extension with a generator $g \in \mathrm{Gal}(K/L)$. Suppose that $x \in K^\times$ is such that $N_{K/L}(x) = 1$. Then, there exists $y \in K^\times$ such that $x = y/gy$.*

Proof. By our computation of cohomology of finite cyclic groups, $H^1(\mathrm{Gal}(K/L), K^\times) = \ker(g^{n-1} + \cdots + 1)/\operatorname{im}(g-1)$, where $\mathrm{Gal}(K/L) = \mathbb{Z}/n\mathbb{Z}$. As this group is zero, this exactly implies what we want. □

Computation of $H^2(\mathrm{Gal}(K/L), K^\times)$, however, is much more complicated, and is in fact the main content of the local class field theory, when K, L are local fields.

Definition 4.16 (Brauer groups). Let K/L be a Galois extension of fields (may be infinite). Then, $\mathrm{Br}(K/L) := H^2(\mathrm{Gal}(K/L), K^\times)$ is called the **relative Brauer group** of K/L. If $K = \overline{L}$, we write $\mathrm{Br}(L)$ instead of $\mathrm{Br}(\overline{L}/L)$ and call it the **Brauer group** of L.

We have the following computation.

Proposition 4.17. *Let K be a local field.*

(1) Let L/K be an unramified extension (possibly infinite). Then, $H^r(\mathrm{Gal}(L/K), \mathcal{O}_L^\times) = 0$ for all $r > 0$.

(2) Let L/K be a finite unramified extension. Then, $\mathrm{Br}(L/K) \cong \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$.

(3) We have $\mathrm{Br}(K^{\mathrm{nr}}/K) \cong \mathbb{Q}/\mathbb{Z}$.

Proof. (1) As this is a direct limit of finite level cohomology groups of the same form, we may assume that L/K is a finite extension. Then, L/K is cyclic. Unraveling what we need to show, we need to show that $N_{L/K} : \mathcal{O}_L^\times \to \mathcal{O}_K^\times$ is surjective, and that if $N_{L/K}(x) = 1$ for $x \in \mathcal{O}_L^\times$ then $x = gy/y$ for some $y \in \mathcal{O}_K^\times$, where $g \in \mathrm{Gal}(L/K)$ is a generator. These are, respectively, Proposition 1.2 and Hilbert's Theorem 90.

(2) Consider the short exact sequence

$$0 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{v_L} \mathbb{Z} \to 0,$$

where $v_L : L^\times \to \mathbb{Z}$ is the normalized discrete valuation. By (1), we see that $H^2(\mathrm{Gal}(L/K), L^\times) \xrightarrow{H^2(v_L)} H^2(\mathrm{Gal}(L/K), \mathbb{Z})$ is an isomorphism. Now it comes from the computation of Galois cohomology of cyclic groups; namely

$$H^2(\mathrm{Gal}(L/K), L^\times) \xrightarrow{H^2(v_L)} H^2(\mathrm{Gal}(L/K), \mathbb{Z}) \xleftarrow{\sim} H^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{f \mapsto f(\mathrm{Fr}_{L/K})} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}.$$

(3) This follows from (2).

□

Definition 4.18 (Invariant map). From the proof of Proposition 4.17, we constructed a **canonical** isomorphism

$$\mathrm{inv}_{L/K} : \mathrm{Br}(L/K) \xrightarrow{\sim} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}, \quad \mathrm{inv}_{K^{\mathrm{nr}}/K} : \mathrm{Br}(K^{\mathrm{nr}}/K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z},$$

for a local field K and a finite unramified extension L/K. These are called the **invariant map**.

Lemma 4.19. *The invariant maps have the following compatibilities with changing fields.*

(1) Let K be a local field, and let $L_1 \supset L_2$ be unramified extensions of K. Then, the following diagram commutes,

$$\begin{tikzcd}
\mathrm{Br}(L_2/K) \arrow[r, "\mathrm{inv}_{L_2/K}"] \arrow[d, "\mathrm{Inf}"'] & \mathbb{Q}/\mathbb{Z} \arrow[d, equal] \\
\mathrm{Br}(L_1/K) \arrow[r, "\mathrm{inv}_{L_1/K}"'] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

(2) Let L/K be a finite extension of local fields of degree n (not necessarily unramified). Then, the following diagram commutes,

$$\begin{tikzcd}
\mathrm{Br}(K^{\mathrm{nr}}/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_{K^{\mathrm{nr}}/K}"'] & \mathrm{Br}(L^{\mathrm{nr}}/L) \arrow[d, "\mathrm{inv}_{L^{\mathrm{nr}}/L}"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "\times n"'] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

Proof. Omitted (easy). □

The core content of the local class field theory is that in fact the same description of relative Brauer group holds for **any Galois extensions**.

Theorem 4.20. *Let K be a local field. Then, there is a canonical isomorphism*

$$\mathrm{inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}.$$

*For L/K a finite Galois extension of degree n (**not necessarily unramified**), we have a canonical isomorphism*

$$\mathrm{inv}_{L/K} : \mathrm{Br}(L/K) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

The proof of this will come later (just for the sake of clarity; if we wanted we can prove it now), after we review how certain cohomological statements like this deduce class field theory abstractly. For example, for a finite Galois extension L/K of local fields, the inverse of the local Artin reciprocity map $\mathrm{Art}_{L/K}^{-1} : \mathrm{Gal}(L/K)^{\mathrm{ab}} \to K^\times/N_{L/K}(L^\times)$ is defined as the cup product with the canonical generator of $\mathrm{Br}(L/K) = H^2(\mathrm{Gal}(L/K), L^\times)$, which gives rise to an isomorphism

$$\mathrm{Gal}(L/K)^{\mathrm{ab}} = H_T^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) \xrightarrow{\sim} H_T^0(\mathrm{Gal}(L/K), L^\times) = K^\times/N_{L/K}(L^\times).$$

5. Class formations

From the previous section, we saw a hint of the idea that the reciprocity law part of the local class field theory follows from the Galois cohomology of things like $K^\times$, $\mathcal{O}_K^\times$.

Remark 5.1. The existence theorem part of the class field theory is not a cohomological consequence. The cohomological considerations can go up to the construction of reciprocity law which is **continuous**. On the other hand, the existence theorem is about the reciprocity law, after certain modification (such as passing to the profinite completion), being an **isomorphism**. Thus, the extra step that the existence theorem gives is that certain two topologies on the multiplicative group are the same, which is proved by showing that there are "fields with small enough norm groups."

The key is the following abstract theorem.

Theorem 5.2 (Tate's theorem). *Let G be a finite group, and let C be a G-module. Suppose that for all subgroups $H \leq G$, the following are true.*

- $H^1(H, C) = 0$.
- $H^2(H, C) \cong \mathbb{Z}/|H|\mathbb{Z}$.

Then, the cup product with a generator $a \in H^2(G, C) \cong \mathbb{Z}/|G|\mathbb{Z}$ gives an isomorphism $H_T^r(G, \mathbb{Z}) \xrightarrow{\sim} H_T^{r+2}(G, C)$ for every $r \in \mathbb{Z}$. In fact, the cup product with $\operatorname{Res}(a) \in H^2(H, C)$ gives an isomorphism $H_T^r(H, \mathbb{Z}) \xrightarrow{\sim} H_T^{r+2}(H, C)$ for every $H \leq G$, $r \in \mathbb{Z}$.

Proof. Choose a 2-cocycle φ representing a. Note that the cocycle condition implies that

$$g\varphi(h, i) + \varphi(g, hi) = \varphi(gh, i) + \varphi(g, h).$$

The idea is to construct an exact sequence of G-modules

$$0 \to C \to C(\varphi) \to I \to 0,$$

where I is the augmentation ideal. The construction is as follows. As a $\mathbb{Z}$-module, $C(\varphi) = C \oplus \bigoplus_{g \in G, g \neq 1} \mathbb{Z}x_g$. The action of G on $C(\varphi)$ is the same as the action of G on C on the C-part, and given by

$$gx_h = x_{gh} - x_g + \varphi(g, h),$$

where $x_1 = \varphi(1, 1)$; this matches with the action of G on $\varphi(1, 1)$: $g\varphi(1, 1) = \varphi(g, 1)$. It is easy to check that this defines a G-action on $C(\varphi)$. There is a G-morphism $C(\varphi) \to I$ given by $x_g \mapsto [g] - 1$ and the entirety of C is sent to 0. Thus $C(\varphi)$ indeed fits into the exact sequence of the form we wrote above.

The virtue of considering $C(\varphi)$ is that, when φ is considered as $\varphi \in C^2(G, C(\varphi))$, it is actually a 2-coboundary, as $\varphi = dx$, $x \in C^1(G, C(\varphi))$, defined by $x(g) = x_g$; we can check this as

$$dx(g, h) = gx(h) - x(gh) + x(g) = gx_h - x_{gh} + x_g = \varphi(g, h).$$

This implies that the map $H^2(G, C) \to H^2(G, C(\varphi))$ sends a to 0. As a generates $H^2(G, C)$, this implies that the map $H^2(G, C) \to H^2(G, C(\varphi))$ itself is zero. As $\operatorname{Cor} \circ \operatorname{Res} = [G : H]$ for any $H \leq G$, $\operatorname{Res}(a)$ generates $H^2(H, C)$ for any $H \leq G$. Therefore, for any $H \leq G$, by the same logic, $H^2(H, C) \to H^2(H, C(\varphi))$ is zero. We have a long exact sequence

$$0 = H^1(H, C) \to H^1(H, C(\varphi)) \to H^1(H, I) \to H^2(H, C) \xrightarrow{0} H^2(H, C(\varphi)) \to H^2(H, I),$$

where the first term is zero because of our assumption. Note that $H^2(H, I) = 0$, because after applying the long exact sequence to $0 \to I \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$, we have $H^2(H, I) \cong H^1(H, \mathbb{Z}) = \mathrm{Hom}_{\mathrm{Grp}}(H, \mathbb{Z}) = 0$, as $\mathbb{Z}[G]$ is an acyclic H-module. Furthermore, $H^1(H, I) \cong H^0_T(H, \mathbb{Z}) = \mathbb{Z}/|H|\mathbb{Z}$. Therefore, it follows that $H^1(H, C(\varphi)) = H^2(H, C(\varphi)) = 0$ by order considerations.

Now we claim that $H^r_T(H, C(\varphi)) = 0$ for any $H \leq G$ and $r \in \mathbb{Z}$. This follows from the following lemma.

Lemma 5.3. *Let G be a finite group, and let M be a G-module. If $H^1(H, M) = H^2(H, M) = 0$ for every $H \leq G$, then $H^r_T(H, M) = 0$ for all $H \leq G$ and $r \in \mathbb{Z}$.*

Proof. It suffices to show that $H^r_T(G, M) = 0$ for all $r \in \mathbb{Z}$. We make the initial reduction. Let $H \leq G$. For a prime p, let H_p be a Sylow p-subgroup of H. Note that $\mathrm{Cor} \circ \mathrm{Res} = [H : H_p]$, so any element $x \in H^r_T(H, M)$ of p-power order is sent to a non-identity element as long as $x \neq 1$. Therefore, $\mathrm{Res} : H^r_T(H, M)_p \to H^r_T(H_p, M)$ is injective, where $H^r_T(H, M)_p$ is the p-primary part of $H^r_T(H, M)$. So we only need to show the statement for p-subgroups $H \leq G$. In particular, we may assume that G is a p-group to start with, for some prime p. In particular, we may assume that G is solvable.

Now we can deduce this from the cyclic case, which is certainly a consequence of the periodicity of Tate cohomology. We use an induction on $|G|$. There exists a proper normal subgroup $H \trianglelefteq G$ where G/H is cyclic. By induction hypothesis, $H^r_T(H, M) = 0$ for all $r \in \mathbb{Z}$. By the inflation-restriction exact sequence, we have exact sequences

$$0 \to H^r(G/H, M^H) \to H^r(G, M) \to H^r(H, M),$$

for all $r \geq 1$. As $H^1(G, M) = H^2(G, M) = 0$, $H^1(G/H, M^H) = H^2(G/H, M^H) = 0$, so by the periodicity of Tate cohomology for the cyclic group G/H, $H^r_T(G/H, M^H) = 0$ for all $r \in \mathbb{Z}$. Therefore, $H^r(G, M) = 0$ for all $r \geq 1$. To use the dimension shifting argument, we need to show that $I \otimes_{\mathbb{Z}} M$ satisfies the conditions of the Lemma. If you check, the only thing you need to show is $H^0_T(G, M) = 0$. Suppose $x \in M^G$. Then, as $H^0_T(G/H, M^H) = 0$ by induction hypothesis, there is $y \in M^H$ such that $\sum_{g \in G/H} gy = x$. As $H^0_T(H, M) = 0$, there is $z \in M$ such that $\sum_{h \in H} hz = y$. This means that $\sum_{g \in G} gz = x$, which implies that $H^0_T(G, M) = 0$, which finishes the proof. □

Therefore, by Lemma, $H^r_T(H, C(\varphi)) = 0$ for any $H \leq G$ and $r \in \mathbb{Z}$. Therefore, by the long exact sequence of Tate cohomology, we have an isomorphism $H^{r-1}_T(H, I) \xrightarrow{\sim} H^r_T(H, C)$. Again, we already know that there is an isomorphism $H^{r-2}_T(H, \mathbb{Z}) \xrightarrow{\sim} H^{r-1}_T(H, I)$, so composing this, we get an isomorphism $H^{r-2}_T(H, \mathbb{Z}) \xrightarrow{\sim} H^r_T(H, C)$. You can show that this the cup product with $\mathrm{Res}(a)$ by using cocycles. Or, by naturality of the process, it suffices to show that the image of $1 \in H^0_T(H, \mathbb{Z})$ via this isomorphsim is $\mathrm{Res}(a) \in H^2_T(H, C)$. First, 1 is sent to a 1-cocycle in $C^1(H, I)$, $h \mapsto [h] - 1$. Then, this is sent to a 2-cocycle in $C^2(H, C)$, $h \mapsto dx$, which is exactly φ, as observed above, which is exactly what we wanted. □

Using Tate's theorem, we know exactly what we want to prove the reciprocity law in an abstract setting. The package that we need to form a class field theory is called the **class formation**.

Definition 5.4 (Class formation)**.** A **class formation** is the following package of data.

- A **base field** F, and an algebraic closure $\overline{F}$ of F. Let $G = \mathrm{Gal}(\overline{F}/F)$. In this context, every finite extension of F is regarded as a subextension of the ambient algebraic closure $\overline{F}$. For a finite extension K/F, let $G_K = \mathrm{Gal}(\overline{F}/K)$.

- A **discrete** G**-module** A. For a finite extension K/F, let $A_K = A^{G_K}$.

- For any Galois extension L/K between finite extensions of F, we demand two conditions:

Axiom 1. $H^1(\mathrm{Gal}(L/K), A_L) = 0$;

Axiom 2. there is an isomorphism $\mathrm{inv}_{L/K} : H^2(\mathrm{Gal}(L/K), A_L) \xrightarrow{\sim} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ called the **invariant map**, compatible with inflation and restriction in the following way: if $M/L/K$ is a tower of Galois extensions between finite extensions of K, the following diagrams commute,

$$\begin{tikzcd}
H^2(\mathrm{Gal}(L/K), A_L) \arrow[r, hook, "\mathrm{Inf}"] \arrow[d, "\mathrm{inv}_{L/K}"', "\sim"] & H^2(\mathrm{Gal}(M/K), A_M) \arrow[d, "\sim"', "\mathrm{inv}_{M/K}"] \\
\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \arrow[r, hook, "x\mapsto x"'] & \frac{1}{[M:K]}\mathbb{Z}/\mathbb{Z}
\end{tikzcd}
\qquad
\begin{tikzcd}
H^2(\mathrm{Gal}(M/K), A_M) \arrow[r, two heads, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_{M/K}"', "\sim"] & H^2(\mathrm{Gal}(M/L), A_M) \arrow[d, "\sim"', "\mathrm{inv}_{M/L}"] \\
\frac{1}{[M:K]}\mathbb{Z}/\mathbb{Z} \arrow[r, two heads, "x\mapsto [L:K]x"'] & \frac{1}{[M:L]}\mathbb{Z}/\mathbb{Z},
\end{tikzcd}$$

Also, from **Axiom 2**, we may form the direct limit $H^2(\mathrm{Gal}(\overline{F}/K), A) = \varinjlim_{L/K \text{ finite Galois}} H^2(\mathrm{Gal}(L/K), A_L)$, where the transition maps are inflation maps. This inherits the invariant map

$$\mathrm{inv}_K : H^2(\mathrm{Gal}(\overline{F}/K), A) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}.$$

Finally, given a Galois extension L/K of finite extensions of F, $u_{L/K} := \mathrm{inv}_{L/K}^{-1}\left(\frac{1}{[L:K]}\right) \in H^2(\mathrm{Gal}(L/K), A_L)$ is called the **fundamental class**.

Remark 5.5. From **Axiom 1** of the class formation, the inflation-restriction exact sequence already implies that the inflation map $\mathrm{Inf} : H^2(\mathrm{Gal}(L/K), A_L) \to H^2(\mathrm{Gal}(M/K), A_M)$ is injective. Also, from the construction, the following are obvious.

- If L/K is a Galois extension between finite extensions of F, then $H^2(\mathrm{Gal}(L/K), A_L) \subset H^2(\mathrm{Gal}(\overline{F}/K), A)$ is sent via inv_K isomorphically to $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$.

- If L/K is a field extension between finite extensions of F, there is a restriction map $\mathrm{Res} : H^2(\mathrm{Gal}(\overline{F}/K), A) \to H^2(\mathrm{Gal}(\overline{F}/L), A)$, and the following diagram commutes,

$$\begin{tikzcd}
H^2(\mathrm{Gal}(\overline{F}/K), A) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_K"', "\sim"] & H^2(\mathrm{Gal}(\overline{F}/L), A) \arrow[d, "\sim"', "\mathrm{inv}_L"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "x\mapsto [L:K]x"'] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

- For a Galois M/K of finite extensions of F and for an intermediate field $M/L/K$,

$$\mathrm{Res}(u_{M/K}) = u_{M/L}, \quad \mathrm{Cor}(u_{M/L}) = [L:K]u_{M/K}.$$

  Furthermore, if L/K is Galois, $\mathrm{Inf}(u_{L/K}) = [M:L]u_{M:K}$.

Example 5.6. We will see shortly that $\overline{\mathbb{Q}}_p^\times$ as a discrete $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-module is a class formation; what's left is to prove Theorem 4.20.

In the number field case, the discrete $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module that gives rise to a class formation is called the **idele class group**.

From Tate's theorem, the following is easy.

Theorem 5.7 (Abstract reciprocity law)**.** *Suppose that we are given a class formation. Then, for any Galois extension L/K of finite extensions of F, the cup product with $u_{L/K}$ gives rise to an isomorphism*

$$H_T^r(\mathrm{Gal}(L/K), \mathbb{Z}) \xrightarrow{\sim} H_T^{r+2}(\mathrm{Gal}(L/K), A_L),$$

for any $r \in \mathbb{Z}$. In particular, when $r = -2$, this gives rise to the isomorphism

$$\mathrm{Gal}(L/K)^{\mathrm{ab}} \xrightarrow{\sim} A_K/N_{L/K}(A_L),$$

where $N_{L/K} : A_L \to A_K$ is defined by $x \mapsto \sum_{g \in G} gx$. The inverse[1] of this isomorphism

$$\mathrm{rec}_{L/K} : A_K/N_{L/K}(A_L) \xrightarrow{\sim} \mathrm{Gal}(L/K)^{\mathrm{ab}},$$

is called the (relative) ***reciprocity map***[2]*.*

Furthermore, the reciprocity map has the following compatibility: if M/K is a Galois extension between finite extensions of F, and if $M/L/K$ is an intermediate extension, then the following diagrams commute,

$$\begin{tikzcd}
A_K/N_{M/K}(A_M) \arrow[r, "\mathrm{rec}_{M/K}"] \arrow[d] & \mathrm{Gal}(M/K)^{\mathrm{ab}} \arrow[d, "V"] & A_L/N_{M/L}(A_M) \arrow[r, "\mathrm{rec}_{M/L}"] \arrow[d, "N_{L/K}"'] & \mathrm{Gal}(M/L)^{\mathrm{ab}} \arrow[d] \\
A_L/N_{M/L}(A_M) \arrow[r, "\mathrm{rec}_{M/L}"'] & \mathrm{Gal}(M/L)^{\mathrm{ab}} & A_K/N_{M/K}(A_M) \arrow[r, "\mathrm{rec}_{M/K}"'] & \mathrm{Gal}(M/K)^{\mathrm{ab}},
\end{tikzcd}$$

where the left vertical arrow of the left square is induced from the natural inclusion $A_K \hookrightarrow A_L$, the right vertical arrow of the left square is the transfer homomorphism (Definition 2.2), and the right vertical arrow of the right square is induced from the natural inclusion $\mathrm{Gal}(M/L) \hookrightarrow \mathrm{Gal}(M/K)$.

Proof. This follows from Tate's theorem and the relationship between the fundamental classes and Res and Cor (and how Res and Cor behave on H_T^{-2} and H_T^0, Proposition 4.3). □

[1] Note that this is the direction of the local Artin reciprocity map; in general the treatment is clearer when you take the isomorphism in this direction.

[2] Historically this was called the norm-residue symbol, and denoted as $a \mapsto (a, L/K)$.

To obtain the absolute version of the reciprocity map, we abuse the notation and denote the composition of $\mathrm{rec}_{L/K}$ with the natural quotient map $A_K \twoheadrightarrow A_K/N_{L/K}(A_L)$ also by $\mathrm{rec}_{L/K} : A_K \twoheadrightarrow \mathrm{Gal}(L/K)^{\mathrm{ab}}$. We need another compatibility of reciprocity maps:

Proposition 5.8. *Let $M/L/K$ be a tower of Galois extensions of finite extensions of F. Then, the following diagram commutes,*

$$\begin{tikzcd}
A_K \arrow[r, "\mathrm{rec}_{M/K}"] \arrow[dr, "\mathrm{rec}_{L/K}"'] & \mathrm{Gal}(M/K)^{\mathrm{ab}} \arrow[d] \\
 & \mathrm{Gal}(L/K)^{\mathrm{ab}},
\end{tikzcd}$$

where the vertical map is induced from the natural surjection $\mathrm{Gal}(M/K) \twoheadrightarrow \mathrm{Gal}(L/K)$.

Proof. This does not immediately follow from the cohomological considerations, as we have not seen a cohomological way of defining the map $\mathrm{Gal}(M/K)^{\mathrm{ab}} \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$. On the other hand, there is a very useful criterion of telling which elements correspond to each other via the reciprocity map.

Lemma 5.9. *Let L/K be a Galois extension between finite extensions of F, and let $a \in A_K$ and $\sigma \in \mathrm{Gal}(L/K)$. Then, $\mathrm{rec}_{L/K}(a) = \sigma$ in $\mathrm{Gal}(L/K)^{\mathrm{ab}}$ if and only if, for every character $\chi \in \mathrm{Hom}_{\mathrm{Grp}}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$, the equality*

$$\mathrm{inv}_K(a \cup \delta\chi) = \chi(\sigma),$$

holds. Here, $\delta : \mathrm{Hom}_{\mathrm{Grp}}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) = H^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(\mathrm{Gal}(L/K), \mathbb{Z})$.

The Proposition immediately follows from this Lemma, so we are left with proving this Lemma.

Proof of Lemma 5.9. By definition, $\mathrm{rec}_{L/K}(a) = \sigma$ in $\mathrm{Gal}(L/K)^{\mathrm{ab}}$ if and only if $a = u_{L/K} \cup \zeta_\sigma$, where $\zeta_\sigma \in H_T^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) = H_1(\mathrm{Gal}(L/K), \mathbb{Z}) = \mathrm{Gal}(L/K)^{\mathrm{ab}}$ is the class corresponding to σ. We use the following lemma.

Lemma 5.10. *Let G be a finite group. Then, the cup product*

$$H_T^{-2}(G, \mathbb{Z}) \times H_T^2(G, \mathbb{Z}) \to H_T^0(G, \mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z},$$

is given by

$$\zeta_\sigma \cup \delta\chi = |G|\chi(\sigma),$$

for $\sigma \in G$ and $\chi \in \mathrm{Hom}_{\mathrm{Grp}}(G, \mathbb{Q}/\mathbb{Z})$. In particular, an element of $H_T^{-2}(G, \mathbb{Z})$ is determined by the values of its cup products with the elements of $H_T^2(G, \mathbb{Z})$.

Proof. Note that $\delta\chi$ is represented by a 2-cocycle $\delta\overline{\chi} : G^2 \to \mathbb{Z}$, given by

$$\delta\overline{\chi}(g, h) := s(\chi(g)) + s(\chi(h)) - s(\chi(gh)),$$

where $s : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}$ is a set-theoretic section of the quotient $\mathbb{Q} \twoheadrightarrow \mathbb{Q}/\mathbb{Z}$ (as $\chi(g)+\chi(h) = \chi(gh) \bmod \mathbb{Z}$, $\delta\overline{\chi}(g,h)$ is an integer). Unraveling the definitions, the cup product $\zeta_\sigma \cup \delta\chi$ is the class of $\sum_{\tau\in G} \delta\overline{\chi}(\tau,\sigma) \in \mathbb{Z}$ in $H^0_T(G,\mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$. Because of the formula for $\delta\overline{\chi}$, we have

$$\sum_{\tau\in G} \delta\overline{\chi}(\tau,\sigma) = |G|s(\chi(\sigma)) \in \mathbb{Z}.$$

The last statement follows from the fact that $\mathrm{Hom}_{\mathrm{Grp}}(G,\mathbb{Q}/\mathbb{Z})$ is the dual of G^{ab} and is in particular of the same order as $G^{\mathrm{ab}} = H^{-2}_T(G,\mathbb{Z})$. □

By Lemma 5.10, $a = u_{L/K} \cup \zeta_\sigma$ if and only if $a \cup \delta\chi = u_{L/K}[L : K]\chi(\sigma)$ for all $\chi \in \mathrm{Hom}_{\mathrm{Grp}}(\mathrm{Gal}(L/K),\mathbb{Q}/\mathbb{Z})$. As $\mathrm{inv}_{L/K}$ is an isomorphism, this holds if and only if $\mathrm{inv}_K(a\cup\delta\chi) = \frac{1}{[L:K]}[L : K]\chi(\sigma) = \chi(\sigma)$ for all $\chi \in \mathrm{Hom}_{\mathrm{Grp}}(\mathrm{Gal}(L/K),\mathbb{Q}/\mathbb{Z})$, which is what we want. □

□

From Proposition 5.8, we can take the inverse limit over all finite Galois extensions L/K and obtain the (absolute) **reciprocity map**

$$\mathrm{rec}_K : A_K \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}.$$

This has the similar compatibility as $\mathrm{rec}_{L/K}$ which we don't bother to write down. One also has some information about the norm groups as follows.

Theorem 5.11. *Suppose we're given a class formation. Let K be a finite extension of F.*

*(1) (**Norm limitation theorem**) For any finite extension L/K, if $L/M/K$ is the maximal abelian subextension of L/K, then*

$$N_{L/K}(A_L) = N_{M/K}(A_M).$$

In particular, $N_{L/K}(A_L)$ only depends on the Galois closure of L/K.

*(2) (**Uniqueness theorem**) If $L_1, L_2/K$ are finite abelian extensions, then*

$$N_{L_1/K}(A_{L_1}) = N_{L_2/K}(A_{L_2}) \quad \Leftrightarrow \quad L_1 = L_2.$$

Proof. (1) It is clear that $N_{L/K}(A_L) \subset N_{M/K}(A_M)$. Take a large Galois extension L'/K that contains L. Let $G = \mathrm{Gal}(L'/K)$ and $H = \mathrm{Gal}(L'/L)$. Then, $\mathrm{Gal}(L'/M) = [G,G]H$, as M is the maximal abelian extension over K contained in L. We have the following commutative diagram

$$\begin{tikzcd}
 & A_L \arrow[r, "N_{L/K}"] \arrow[d, "\mathrm{rec}_{L'/L}"'] & A_K \arrow[r, equal] \arrow[d, "\mathrm{rec}_{L'/K}"'] & A_K \arrow[d, "\mathrm{rec}_{M/K}"'] & \\
1 \arrow[r] & H/H' \arrow[r] & G/G' \arrow[r] & G/G'H \arrow[r] & 1,
\end{tikzcd}$$

where the bottom row is an exact sequence of abelian groups. Suppose $x \in N_{M/K}(A_M)$. Then, $\mathrm{rec}_{L'/K}(x) \in G/G'$ is sent to $1 \in G/G'H$. Therefore, there is an element $h \in H/H'$ whose image in G/G' is the same as $\mathrm{rec}_{L'/K}$. As $\mathrm{rec}_{L'/L}$ is surjective, there is $y \in A_L$ such that $\mathrm{rec}_{L'/K}(x) = \mathrm{rec}_{L'/K}(N_{L/K}(y))$. Thus, x and $N_{L/K}(y)$ are off by an element in $\ker \mathrm{rec}_{L'/K} = N_{L'/K}(A_{L'}) \subset N_{L/K}(A_L)$. As $N_{L/K}(y) \in N_{L/K}(A_L)$, this implies that $x \in N_{L/K}(A_L)$, which is what we want.

(2) The reverse direction is obvious. For the forward direction, let $L = L_1 L_2$, which is abelian over K. Then, under $\mathrm{rec}_{L/K} : A_K/N_{L/K}(A_L) \xrightarrow{\sim} \mathrm{Gal}(L/K)$, $N_{L_i/K}(A_{L_i})/N_{L/K}(A_L)$ correspond to $\mathrm{Gal}(L/L_i) \subset \mathrm{Gal}(L/K)$ for $i = 1, 2$. Therefore, this means $L_1 = L_2$.

□

Thus, we know exactly what kind of extra statement we need to prove to prove the existence theorem.

Theorem 5.12 (Abstract existence theorem)**.** *Suppose we're given a class formation. Suppose that the class formation further satisfies the following condition.*

(*) *For any finite extension K/F and any open finite index subgroup $U \leq A_K$, there exists a finite extension L/K such that $N_{L/K}(A_L) \subset U$.*

*Then, the **existence theorem** holds: for any finite extension K/F and any finite index subgroup $U \leq A_K$, there exists a (unique) finite **abelian** extension L/K such that $N_{L/K}(A_L) = U$.*

Proof. By (*), there exists a finite extension M/K such that $N_{M/K}(A_M) \subset U$. By the abstract reciprocity law and the norm limitation theorem, $A_K/N_{M'/K}(A_{M'}) \cong \mathrm{Gal}(M'/K)$, where M'/K is the maximal abelian subextension of M/K. Let L be the fixed field of the subgroup of $\mathrm{Gal}(M'/K)$ corresponding to $U/N_{M'/K}(A_{M'})$. By the compatibility of reciprocity maps and norms, it follows that $N_{L/K}(A_L) = U$. Uniqueness is exactly the uniqueness theorem. □

6. Adeles and ideles

To define the class formation for the global case (e.g. number fields), we need to use **adeles** and **ideles**. Before starting, we fix the terminology.

Definition 6.1 (Global fields)**.** A **global field** is a field K which is a finite extension of either $\mathbb{Q}$ or $\mathbb{F}_q(T)$. Here, $\mathbb{F}_q(T)$ is the field of rational functions in one variable with coefficients in the finite field $\mathbb{F}_q$. When K is a finite extension of $\mathbb{Q}$, we call it a **number field**. When K is a finite extension of $\mathbb{F}_q(T)$, we call it a **function field**.

Remark 6.2 (On the subtleties of the function fields)**.** There are several extra difficulties when K is a function field. Firstly, K is not perfect; $\mathbb{F}_q(T^{1/q})/\mathbb{F}_q(T)$ is a purely inseparable extension of degree q. When discussing the Galois theory of F, one must only consider separable extensions. The absolute Galois group of F is the Galois group of the maximal **separable** extension K^{sep} over K. Furthermore, there is a subtle issue with the topology of a profinite group (e.g. there are finite index subgroups that are not open). In this section, we will often give proofs only in the case when K is a number field (i.e. charcateristic 0).

Global class field theory concerns describing $\mathrm{Gal}(K^{\mathrm{sep}}/K)^{\mathrm{ab}}$ of a global field K. We want something that captures the arithmetic of the class group of K for A_K. There is another extra feature you would want, that the local and global class field theories are compatible with each other in some way, under the name of **local-global compatibility**. Remember however that the class group $\mathrm{Cl}(K)$ is defined using fractional ideals of K. **Ideles** are invented as alternatives to ideals that are expressed as elements but also exhibit clear connection with local fields.

Definition 6.3 (Places of a global field)**.** A **place** or a **prime** v of a global field K is an equivalence class of absolute values on K. Equivalently, it is either a maximal ideal of $\mathcal{O}_K$ (called a **nonarchimedean prime** or a **finite place**) or an embedding $K \hookrightarrow \mathbb{C}$ (called an **archimedean prime** or an **infinite place**); in the latter case, which happens only if K is a number field, an embedding $K \hookrightarrow \mathbb{C}$ is considered equivalent to its complex conjugate.

Let K_v be the completion of K with respect to an absolute value corresponding to v. If v is nonarchimedean, let $\mathfrak{p}_v \subset \mathcal{O}_K$ be the corresponding prime ideal (so that $K_v = \mathrm{Frac}(\mathcal{O}_{K,\mathfrak{p}_v})$). Let $\mathrm{ord}_v : K_v^\times \to \mathbb{Z}$ be the normalized discrete valuation of the cdvf K_v; namely, after choosing a uniformizer $\pi_v \in K_v$, $\mathrm{ord}_v(u\pi_v^m) = m$ for any $m \in \mathbb{Z}$, $u \in \mathcal{O}_{K_v}^\times$.

If v is archimedean, $K_v = \mathbb{R}$ if the corresponding embedding is real, and $K_v = \mathbb{C}$ if complex.

Definition 6.4 (Normalized absolute values)**.** For a local field L, there is a preferred way to normalize an absolute value (among the ones in the same equivalence class).

- If L is a p-adic field, then $|x| := \frac{1}{(\#l)^{\mathrm{ord}(x)}}$ (and $|0| := 0$), where l is the residue field of L (which is a finite field), and $\mathrm{ord} : L^\times \to \mathbb{Z}$ is the normalized discrete value as above (i.e. scaled such that ord is surjective).
- If $L = \mathbb{R}$, then $|x|$ is the usual absolute value.
- If $L = \mathbb{C}$, then $|x|$ is the square of the complex absolute value.

If K is a global field, and if v is a place of K, then let $|\cdot|_v$ be the normalized absolute value on K restricted from that of K_v under the natural inclusion $K \hookrightarrow K_v$.

We will see shortly (see Lemma 6.13) why this normalization is a useful thing to do.

Definition 6.5 (Ideles)**.** An **idele** is a collection of elements (α_v), where $\alpha_v \in K_v^\times$ for each place v of K, such that for all but finitely many places v, $\alpha_v \in \mathcal{O}_{K_v}^\times$.[3] The ideles form a multiplicative group called the **idele group** I_K.

We are regarding real/complex embddings also as primes, which is an important feature of the global class field theory. One reason why we have $\alpha_v \in \mathcal{O}_{K_v}^\times$ for all but finitely primes v is because we can think of a surjective homomorphism $I_K \twoheadrightarrow J_K$ (J_K is the multiplcative group of fractional ideals of K), defined as follows,

$$I_K \twoheadrightarrow J_K, \quad (\alpha_v) \mapsto \prod_{v \text{ nonarchimedean}} \mathfrak{p}_v^{\mathrm{ord}_v(\alpha_v)}.$$

[3] If v is archimedean, there is no good analogue of $\mathcal{O}_{K_v}$, so this statement is vacuous in that case. This is fine because we can always allow finitely many exceptions, and there are finitely many archimedean primes of K.

Note that the requirement that $\alpha_v \in \mathcal{O}_{K_v}^\times$ for all but finitely many v's is precisely the one that makes the above product a finite product (i.e. $\mathrm{ord}_v(\alpha_v) = 0$ for all but finitely many v's).

Composing this with the quotient map $J_K \twoheadrightarrow \mathrm{Cl}(K)$, we get a surjective homomorphism $I_K \twoheadrightarrow \mathrm{Cl}(K)$. Clearly we see that $(\alpha_v) \in I_K$ is in the kernel of $I_K \twoheadrightarrow \mathrm{Cl}(K)$ if there is an element $\alpha \in K^\times$ such that each α_v came from α by the embedding $K \hookrightarrow K_v$.

Definition 6.6 (Idele class group)**.** For any $\alpha \in K^\times$, we can naturally associate $(\alpha_v) \in I_K$, where for each v, α_v is the image of α by the natural embedding $K \hookrightarrow K_v$; this is well-defined as, given $\alpha \in K^\times$, $\mathrm{ord}_v(\alpha) = 0$ for all but finitely many v. Any such idele is called a **principal idele**. This defines a natural injective homomorphism $K^\times \hookrightarrow I_K$, and the quotient $C_K := I_K/K^\times$ is called the **idele class group**.

There is, therefore, a surjective homomorphism $C_K \twoheadrightarrow \mathrm{Cl}(K)$. It is the idele class group that we will use for the class formation; $A_K = C_K$.

To discuss the topology on I_K and C_K, we need to first discuss the additive analogue of ideles.

Definition 6.7 (Adeles)**.** An **adele** is a collection of elements (α_v), where $\alpha_v \in K_v$ for each place v of K, such that for all but finitely many places v, $\alpha_v \in \mathcal{O}_{K_v}$. The adeles form a ring, called the **adele ring** $\mathbb{A}_K$.

Historically, the word "idele" appeared first, and the word "adele" was introduced as an abbreviation of "additive idele." There should technically be accents (idèles, adèles), but many people drop the accents when they write (they are artificially made words anyway).

The idele group and the adele ring are related as $I_K = \mathbb{A}_K^\times$ (the unit group).

We now talk about the topologies of $\mathbb{A}_K$ and I_K, which are a bit annoying.

Definition 6.8. The ring of **finite adeles**[4] $\mathbb{A}_K^\infty$ consists of adeles (α_v) where $\alpha_v = 1$ for all archimedean primes v. More generally, if S is a finite set of places of K, then $\mathbb{A}_K^S$ consists adeles (α_v) where $\alpha_v = 1$ for all $v \in S$.

We also define $\mathbb{A}_{K,S}$, the ring of S-**adeles**, to consist of adeles (α_v) where $\alpha_v \in \mathcal{O}_{K_v}$ for all **finite places**[5] v **not contained in** S. In other words, S-adeles are the adeles where you only allow the primes in S to show up in the denominators. Similarly, $\mathbb{A}_{K,S}^\infty$, the ring of **finite** S-**adeles**, consists of finite adeles (α_v) where $\alpha_v \in \mathcal{O}_{K_v}$ for all finite places $v \notin S$. By definition, $\mathbb{A}_{K,S}$ does not change if you include/exclude some infinite places from S.

The topology of $\mathbb{A}_K$ as a topological (additive) group is generated by the subsets of the form $\prod_{v \in S} U_v \times \prod_{v \notin S} \mathcal{O}_{K_v}$, where S is a finite set of places of K, and, for each $v \in S$, $U_v \subset K_v$ is an open subset. This also makes $\mathbb{A}_K$ a topological ring (i.e. the multiplication is continuous). The topologies of $\mathbb{A}_K^\infty$, $\mathbb{A}_{K,S}$, $\mathbb{A}_{K,S}^\infty$ are induced from $\mathbb{A}_K$ as the subspace topology; note that the induced subspace topology on $\mathbb{A}_{K,S} = \prod_{v \in S \text{ or } v \text{ infinite}} K_v \times \prod_{v \notin S \text{ and } v \text{ finite}} \mathcal{O}_{K_v}$ is the product topology.

One may define similar subgroups of I_K as above, namely $I_K^\infty := I_K \cap \mathbb{A}_K^\infty$, $I_{K,S} := I_K \cap \mathbb{A}_{K,S}$, $I_K^S := I_K \cap \mathbb{A}_K^S$.

The topology of $I_K = \mathbb{A}_K^\times$ is **not** the subspace topology induced from $\mathbb{A}_K^\times$. Rather, I_K is given the topology as the multiplicative group of the topological ring $\mathbb{A}_K$; namely, you also want to

[4] The notation ∞ means that we are putting the set of all infinite places as a superscript.

[5] As noted earlier, $\mathcal{O}_{K_v}$ doesn't make sense when v is an infinite place.

take into account that the multiplicative inverse map $I_K \to I_K$ is continuous. For that matter, you use the injective (multiplicative) homomorphism $I_K \xrightarrow{x \mapsto (x, x^{-1})} \mathbb{A}_K \times \mathbb{A}_K$ and use the subspace topology induced by this homomorphism. Equivalently, the topology of I_K as a topological (multiplicative) group generated by the subsets of the form $\prod_{v \in S} U'_v \times \prod_{v \notin S} \mathcal{O}_{K_v}^\times$, where S is a finite set of places of K, and, for each $v \in S$, $U'_v \subset K_v^\times$ is an open subset[6]. The topologies of I_K^∞, $I_{K,S}$, $I_{K,S}^\infty$ are induced from I_K as the subspace topology.

Example 6.9. We have $\mathbb{A}_{\mathbb{Q}}^\infty = \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$, or in other words $\varinjlim_{n \geq 1} \frac{1}{n}\widehat{\mathbb{Z}}$ (also as topological spaces), and therefore $\mathbb{A}_{\mathbb{Q}} = \mathbb{A}_{\mathbb{Q}}^\infty \times \mathbb{R}$ (also as topological spaces).

As I said, the class formation we will use for the global class field theory will satisfy $A_K = C_K$. To define A, we need to know how C_K changes as we change K.

Proposition 6.10. *Let L/K be a finite extension of global fields.*

(1) There is a natural inclusion $\mathbb{A}_K \hookrightarrow \mathbb{A}_L$, $(\alpha_v) \mapsto (\alpha'_w)$, where $\alpha'_w := \alpha_v \in K_v \subset L_w$ for $w|v$. This restricts to a natural inclusion $I_K \hookrightarrow I_L$, and induces an injection $C_K \hookrightarrow C_L$.

(2) The natural inclusion in (1) gives rise to an isomorphism $\mathbb{A}_K \otimes_K L \xrightarrow{\sim} \mathbb{A}_L$ where $\mathbb{A}_K$ is regarded as a K-vector space via the natural inclusion $K \hookrightarrow \mathbb{A}_K$. In particular, if L/K is Galois, then $\sigma \in \mathrm{Gal}(L/K)$ acts on $\mathbb{A}_L = \mathbb{A}_K \otimes_K L$ naturally as the identity on the first factor and as σ on the second factor of the tensor product.

(3) For L/K finite Galois, $\mathbb{A}_L^{\mathrm{Gal}(L/K)} = \mathbb{A}_K$, $I_L^{\mathrm{Gal}(L/K)} = I_K$, and $C_L^{\mathrm{Gal}(L/K)} = C_K$.

Proof. (1) Only the last part is the nontrivial part, where it follows from $L^\times \cap I_K = K^\times$, which follows from $L \cap \mathbb{A}_K = K$ by (2).

(2) This follows from $K_v \otimes_K L \cong \prod_{w|v} L_w$.

(3) Only $C_L^{\mathrm{Gal}(L/K)} = C_K$ requires an explanation. Note that we have a short exact sequence of $\mathrm{Gal}(L/K)$-modules

$$1 \to L^\times \to I_L \to C_L \to 1,$$

which gives rise to a long exact sequence

$$1 \to \left(L^\times\right)^{\mathrm{Gal}(L/K)} \to I_L^{\mathrm{Gal}(L/K)} \to C_L^{\mathrm{Gal}(L/K)} \to H^1(\mathrm{Gal}(L/K), L^\times) \to \cdots .$$

By Theorem 4.14, this becomes $1 \to K^\times \to I_K \to C_L^{\mathrm{Gal}(L/K)} \to 1$, which implies that $C_L^{\mathrm{Gal}(L/K)} = C_K$.

□

[6] Note that K_v is a **topological field**, so that the topology we have for K_v is also continuous with respect to the inverse map; in particular, the topology on $K_v^\times$ is the subspace topology.

Definition 6.11. Let F be a global field. We define $C := \varinjlim_{K/F \text{ finite}} C_K$, where the transition maps are the natural inclusions. It has a natural continuous $\mathrm{Gal}(F^{\mathrm{sep}}/F)$-action that makes it a discrete $\mathrm{Gal}(F^{\mathrm{sep}}/F)$-module (as $C_K = C^{\mathrm{Gal}(F^{\mathrm{sep}}/K)}$).

Note that this **does not** mean that the natural topology on C is the discrete topology; this was not the case even in the local case. To have knowledge of the topology of C or C_K, we first want to understand how $K^\times$ sits inside I_K, or on a related note, how K sits inside $\mathbb{A}_K$; note that K is a global field, so a priori there is no preferred topology on K.

Proposition 6.12. *The subspace topology induced on $K \subset \mathbb{A}_K$ ($K^\times \subset I_K$, respectively) is the discrete topology.*

Proof. The key ingredient is the following easy observation.

Lemma 6.13 (Product formula)**.** *Let $\alpha \in K^\times$. Then, $\prod_v |\alpha|_v = 1$.*

Proof. Note that the product written above is actually a finite product, as $|\alpha_v| = 1$ for all but finitely many places v. We also note that the formula is quite obvious when $K = \mathbb{Q}$; any rational number can be written as $r = \pm \prod_p p^{n_p}$ for rational primes p (where $n_p = 0$ for all but finitely many p's), and

$$|r|_v = \begin{cases} p^{-n_p} & \text{if } v = p \\ |r| = \prod_p p^{n_p} & \text{if } v = \infty. \end{cases}$$

We would like to reduce the general statement to the case of $\mathbb{Q}$. Let v be a place of $\mathbb{Q}$ (either a rational prime or ∞). Then, $K \otimes_{\mathbb{Q}} \mathbb{Q}_v = \prod_{w|v} K_w$, running over all places w of K over v. We claim that, for any $x \in K^\times$, $\prod_{w|v} |x|_w = |N_{K/\mathbb{Q}}(x)|_v$; note that proving the claim will finish the proof. We first note that, from the decomposition $K \otimes_{\mathbb{Q}} \mathbb{Q}_v = \prod_{w|v} K_w$, $|N_{K/\mathbb{Q}}(x)|_v = \prod_{w|v} |N_{K_w/\mathbb{Q}_v}(x)|$. As any absolute value extends uniquely over a finite extension of local fields, we have $|x|_w = |N_{K_w/\mathbb{Q}_v}(x)|$, which finishes the proof of the claim. □

Now we go back to the original Proposition. As $\mathbb{A}_K$ is a topological (additive) group, it suffices to construct an open neighborhood $0 \in U \subset \mathbb{A}_K$ such that $U \cap K = \{0\}$. Given Lemma 6.13, if we take $U = \prod_{w \text{ finite}} \mathcal{O}_{K_w} \times \prod_{w \text{ infinite}} \{x \in K_w : |x| < 1\}$, then any element $(\alpha_w) \in U$ satisfy $\prod_w |\alpha_w| < 1$, unless $(\alpha_w) = 0$, which implies that $U \cap K = \{0\}$, as desired.

For I_K, note that the topology of I_K is induced as the subspace topology from $I_K \xrightarrow{x \mapsto (x, x^{-1})} \mathbb{A}_K \times \mathbb{A}_K$. So the subspace topology of $K^\times \subset I_K$ is induced as the subspace topology from $K^\times \xrightarrow{x \mapsto (x, x^{-1})} \mathbb{A}_K \times \mathbb{A}_K$. By the discreteness of $K \subset \mathbb{A}_K$, for any $x \in K^\times$, we may take an open neighborhood $x \in U \subset \mathbb{A}_K$ such that $U \cap K = \{x\}$. Then, $K^\times \cap (U \times \mathbb{A}_K) = \{x\}$, so $K^\times$ is induced the discrete topology. □

We now define the topologies on $\mathbb{A}_K/K$ and $C_K = I_K/K^\times$ to be the **quotient topology**, i.e. the finest topologies that make the quotient maps $\mathbb{A}_K \twoheadrightarrow \mathbb{A}_K/K$ and $I_K \twoheadrightarrow I_K/K^\times$ to be continuous. Remember once again that the topologies on $\mathbb{A}_K/K$ and C_K play little role when we take the cohomology of them.

Proposition 6.14 (Compactness of $\mathbb{A}_K/K$; local compactness of C_K)**.** *For a global field K, $\mathbb{A}_K/K$ is a compact group, and C_K is a locally compact group; recall that a topological space is locally compact if every point has a compact neighborhood (i.e., for all x, there is an open set U and a compact set V such that $x \in U \subset V$).*

Example 6.15. Local fields are locally compact (even $\mathbb{R}$ and $\mathbb{C}$ are locally compact), whereas the rings of integers of nonarchimedean local fields are compact (e.g. $\mathbb{Q}_p$ is locally compact vs. $\mathbb{Z}_p$ is compact).

Proof of Proposition 6.14. For the first part, by Proposition 6.10, $\mathbb{A}_K/K$ is a direct sum of copies of $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$, so it suffices to show that $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$ is compact. We note that $\mathbb{A}_\mathbb{Q} \twoheadrightarrow \mathbb{A}_\mathbb{Q}/\mathbb{Q}$ is continuous, and it is surjective even if we restrict it to $\prod_p \mathbb{Z}_p \times [0,1]$; if you have $(\alpha_v) \in \mathbb{A}_\mathbb{Q}$, then you may first add a rational number to make the finite part integral, and then you may add/subtract an integer to make the infinite part lie in $[0,1]$ while keeping the finite part integral. As $\prod_p \mathbb{Z}_p \times [0,1]$ is compact, its continuous image $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$ is also compact.

For the second part, we already see that C_K cannot be compact, as there is a surjective norm map $|\cdot| : C_K \to \mathbb{R}_{>0}$, $(\alpha_v) \mapsto \prod_v |\alpha_v|$ (this is well-defined by Lemma 6.13), and $\mathbb{R}_{>0}$ is not compact. However, this is the only source of non-compactness; if we let $C_K^1 := \ker(|\cdot| : C_K \to \mathbb{R}_{>0})$, then we will show that C_K^1 is compact. This will show that C_K is locally compact, as $\mathbb{R}_{>0}$ is locally compact.

The compactness of C_K^1 is omitted and left as an exercise. □

Exercise 6.1. Prove that C_K^1 is compact. The proof of this has a similar spirit as the proof of the finiteness of class numbers.

Note that, for example, the finiteness of class numbers is a corollary of the fact that C_K^1 is compact, as the natural quotient map $C_K^1 \to \mathrm{Cl}(K)$ is continuous, and $\mathrm{Cl}(K)$ has the discrete topology.

7. Statements of the global class field theory

The global class field theory is now easy to state, in terms of ideles. We will first state the idele version, and then translate it into practically more useful version in terms of fractional ideals.

7.1. **Idelic version of the global class field theory.**

Theorem 7.1 (Global Artin reciprocity)**.** *Let F be a global field, and fix its separable closure F^{sep}. Let $C = \varinjlim_{K/F \text{ finite}} C_K$ be the collection of idele classes over a finite extension over F. These form a class formation; namely, it satisfies Axioms 1 and 2 of Definition 5.4. More precisely, for a global field L, there is a continuous homomorphism, called the* ***global Artin map****,*

$$\mathrm{Art}_L : C_L \to \mathrm{Gal}(L^{\mathrm{ab}}/L),$$

satisfying the following properties.

(1) *For any finite abelian subextension K/L of L^{ab}/L, the global Artin map induces a continuous homomorphism*

$$\mathrm{Art}_{K/L} : C_L \to \mathrm{Gal}(K/L),$$

which is surjective with kernel $N_{K/L}(C_K)$. In particular, there is an isomorphism

$$C_L/N_{K/L}(C_K) \cong \mathrm{Gal}(K/L).$$

(2) *If K/L is a finite extension of global fields, the following diagram commutes, where the right vertical arrow is the restriction.*

$$\begin{tikzcd}
C_K \arrow[r, "\mathrm{Art}_K"] \arrow[d, "N_{K/L}"'] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[d, "\mathrm{res}"] \\
C_L \arrow[r, "\mathrm{Art}_L"'] & \mathrm{Gal}(L^{\mathrm{ab}}/L).
\end{tikzcd}$$

(3) *If K/L is a finite extension of global fields, the following diagram commutes, where the left vertical arrow is the inclusion and the right vertical arrow is the transfer homomorphism.*

$$\begin{tikzcd}
C_K \arrow[r, "\mathrm{Art}_K"] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\
C_L \arrow[r, "\mathrm{Art}_L"'] \arrow[u, hook] & \mathrm{Gal}(L^{\mathrm{ab}}/L). \arrow[u, "V"']
\end{tikzcd}$$

*Moreover, the global Artin map and the local Artin maps at various places of L are compatible with each other (**local-global compatibility**) in the following sense.*

(4) *Let K/L be an abelian extension of global fields. For each place v of L, choose a place w of K over v, and we have a local Artin map $\mathrm{Art}_{K_w/L_v} : L_v^\times \to \mathrm{Gal}(K_w/L_v)$. Regarding $\mathrm{Gal}(K_w/L_v)$ as a decomposition subgroup of $\mathrm{Gal}(K/L)$ (there is no issue of conjugacy as $\mathrm{Gal}(K/L)$ is abelian), we obtain $\mathrm{Art}_v : L_v^\times \to \mathrm{Gal}(K/L)$ for each place v of L. If v is unramified in K, then $\mathrm{Art}_v(\mathcal{O}_{L_v}^\times) = 1$ (Proposition 1.2), so taking the product of Art_v gives a map $\mathrm{Art}'_L : I_L \to \mathrm{Gal}(K/L)$.*

The conclusion is that $\mathrm{Art}'_L(L^\times) = 1$ and the induced map $\mathrm{Art}'_L : C_L \to \mathrm{Gal}(K/L)$ is precisely the global Artin map.

These properties uniquely characterize Art_L.

Remark 7.2. It is important to also consider infinite places, e.g. $\mathrm{Art}_{\mathbb{R}}$ and $\mathrm{Art}_{\mathbb{C}}$, see [ANT] for the details.

By our general discussions, we have the following corollaries for free.

Corollary 7.3 (Norm limitation theorem). *Let F be a global field. For any finite extension L/K of finite extensions of F, and if $L/M/K$ is the maximal abelian subextension of L/K, then*

$$N_{L/K}(C_L) = N_{M/K}(A_M).$$

Corollary 7.4 (Uniqueness theorem). *Let F be a global field. For any finite abelian extensions $L_1, L_2/K$ of finite extensions of F,*

$$N_{L_1/K}(C_{L_1}) = N_{L_2/K}(C_{L_2}) \quad \Leftrightarrow \quad L_1 = L_2.$$

Furthermore, this class formation also satisfies the extra condition we need for the existence theorem.

Theorem 7.5 (Global existence theorem). *Let F be a global field. Then, the class formation (F, C) satisfies the condition (*) of Theorem 5.12. In particular, for any finite extension K of F and for any open finite index subgroup $U \leq C_K$, there is a unique finite abelian extension L/K such that $N_{L/K}(C_L) = U$.*

An easy corollary of the global existence theorem is the characterization of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ for a number field K.

Corollary 7.6. *Let K be a number field (i.e. a global field of characteristic 0). Then, $\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \widehat{C_K}$, the profinite completion of C_K.*

Proof. The content of the global existence theorem is a Galois-type correspondence

$$\left\{ \begin{array}{c} \text{Finite abelian} \\ \text{extensions of } K \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Open finite index} \\ \text{subgroups of } C_K \end{array} \right\}.$$

If K is of characteristic 0, the word "open" is unnecessary, and the corollary is the immediate consequence of the above correspondence. □

Example 7.7. It is not difficult to see that $C_{\mathbb{Q}} \cong \prod_{p \text{ rational prime}} \mathbb{Z}_p^\times \times \mathbb{R}_{>0}$, so $\widehat{C_{\mathbb{Q}}} = \prod_{p \text{ rational prime}} \mathbb{Z}_p^\times \cong \widehat{\mathbb{Z}}^\times$ (there is no proper finite index subgroup of $\mathbb{R}_{>0}$). This is in accordance with $\mathbb{Q}^{\mathrm{ab}} = \bigcup_{n \geq 1} \mathbb{Q}(\zeta_n)$ so that $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) = \varprojlim_{n \geq 1} (\mathbb{Z}/n\mathbb{Z})^\times$.

7.2. **Ideal theoretic version of the global class field theory.** The above descriptions are a bit too abstract, so let us translate the statements to those about ideal class groups or their variants, as expressed in [ANT] (notations are slightly different here to match with the adelic/idelic notation).

The idea is to describe certain finite quotients of C_K in more explicit terms; after all, the global class field theory is about the finite quotients of C_K, and it suffices to have a nice description of only certain finite quotients of C_K to characterize the global Artin reciprocity map (i.e. description of C_K/U for $U \leq C_K$ open finite index subgroups generating the topology of C_K, not necessarily all open finite index subgroups). And we have observed that the class group $\mathrm{Cl}(K)$ is a finite quotient of C_K! We can similarly identify many other finite quotients of C_K with a variant of the class group, called the **ray class group**.

Definition 7.8 (Modulus)**.** Let K be a global field. A **modulus** $\mathfrak{m}$ of K is a function $\mathfrak{m} : \{\text{primes of } K\} \to \mathbb{Z}_{\geq 0}$ such that $\mathfrak{m}(\mathfrak{p}) = 0$ for all but finitely many primes $\mathfrak{p}$, $\mathfrak{m}(\mathfrak{p}) = 0$ or 1 if $\mathfrak{p}$ is real, and $\mathfrak{m}(\mathfrak{p}) = 0$ if $\mathfrak{p}$ is complex. Conventionally, one write $\mathfrak{m}$ as $\mathfrak{m} = \prod_{\mathfrak{p} \text{ primes of } K} \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$. One can write $\mathfrak{m} = \mathfrak{m}_f \mathfrak{m}_\infty$ where $\mathfrak{m}_f = \prod_{\mathfrak{p} \text{ finite primes of } K} \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$ and $\mathfrak{m}_\infty = \prod_{\mathfrak{p} \text{ infinite primes of } K} \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$. Given a modulus $\mathfrak{m}$, let $S(\mathfrak{m})$ be the finite set of primes dividing $\mathfrak{m}$.

Given two moduli $\mathfrak{m}, \mathfrak{n}$, we say $\mathfrak{m}$ divides $\mathfrak{n}$ if $\mathfrak{m}(\mathfrak{p}) \leq \mathfrak{n}(\mathfrak{p})$ for all primes $\mathfrak{p}$.

Definition 7.9 (Ray class group)**.** For a finite set of primes/places S of K, let J_K^S be the (multiplicative) group of fractional ideals generated by the prime ideals not contained in S.

For a modulus $\mathfrak{m}$ of K, let $K_{\mathfrak{m},1}$ be the set of $a \in K^\times$ such that $\mathrm{ord}_\mathfrak{p}(a-1) \geq m(\mathfrak{p})$ for all finite $\mathfrak{p}|\mathfrak{m}$, and $a_\mathfrak{p} > 0$ for all real $\mathfrak{p}|\mathfrak{m}$. This forms a (multiplicative) subgroup of $K^\times$, and for any $a \in K^{\mathfrak{m},1}$, the principal fractional ideal (a) is an element of $J_K^{S(\mathfrak{m})}$. Therefore, there is a natural embedding $K^{\mathfrak{m},1} \hookrightarrow J_K^{S(\mathfrak{m})}$. The quotient $\mathrm{Cl}^\mathfrak{m}(K) := J_K^{S(\mathfrak{m})}/K^{\mathfrak{m},1}$ is called the **ray class group with modulus** $\mathfrak{m}$.

Example 7.10. If $\mathfrak{m}$ is the modulus where $\mathfrak{m}(\mathfrak{p}) = 0$ for all $\mathfrak{p}$, then $\mathrm{Cl}^\mathfrak{m}(K) = \mathrm{Cl}(K)$. Such modulus is called the **empty modulus** and denoted $\mathfrak{m}_\emptyset$.

It turns out that the ray class groups are finite quotients of the idele class group, and they altogether can recover the idele class group.

Proposition 7.11. *Let K be a number field (for simplicity).*

(1) If $\mathfrak{m}$ is a modulus of K, the ray class group $\mathrm{Cl}^\mathfrak{m}(K)$ is a finite abelian group.

(2) For a modulus $\mathfrak{m}$ of K, let $U(\mathfrak{m}) \subset I_K$ be the open subgroup defined by

$$U(\mathfrak{m}) := \prod_{\textit{finite } \mathfrak{p} \textit{ not dividing } \mathfrak{m}} \mathcal{O}_{K_\mathfrak{p}}^\times \times \prod_{\textit{infinite } \mathfrak{p} \textit{ not dividing } \mathfrak{m}} K_\mathfrak{p}^\times \times \prod_{\textit{finite } \mathfrak{p}|\mathfrak{m}} (1 + \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}) \times \prod_{\textit{real } \mathfrak{p}|\mathfrak{m}} \mathbb{R}_{>0}.$$

Then, $I_K/K^\times U(\mathfrak{m}) \cong \mathrm{Cl}^\mathfrak{m}(K)$. Equivalently, if $\overline{U}(\mathfrak{m}) \subset C_K$ is the image of $U(\mathfrak{m}) \subset I_K \twoheadrightarrow C_K$, then $\overline{U}(\mathfrak{m}) \subset C_K$ is an open finite index subgroup such that $C_K/\overline{U}(\mathfrak{m}) \cong \mathrm{Cl}^\mathfrak{m}(K)$.

(3) If $\mathfrak{m}, \mathfrak{n}$ are two moduli of K such that $\mathfrak{m}|\mathfrak{n}$, then there is a natural map $\mathrm{Cl}^\mathfrak{n}(K) \twoheadrightarrow \mathrm{Cl}^\mathfrak{m}(K)$. Under this, we have $\varprojlim_{\mathfrak{m} \textit{ modulus of } K} \mathrm{Cl}^\mathfrak{m}(K) \cong \widehat{C_K}$.

Proof. (1) follows naturally from the finiteness of class number and (2) and (3), as the difference between $U(\mathfrak{m})$ and $U(\mathfrak{m}_\emptyset)$ is finite. Also, (3) follows easily from (2), so it remains to show (2).

Let $I_K^\mathfrak{m}$ be the group of ideles $(\alpha_\mathfrak{p})$ such that $\mathrm{ord}_\mathfrak{p}(\alpha_\mathfrak{p} - 1) \geq \mathfrak{m}(\mathfrak{p})$ for all finite $\mathfrak{p}|\mathfrak{m}$ and $\alpha_\mathfrak{p} > 0$ for all real $\mathfrak{p}|\mathfrak{m}$. Then, there is a natural surjective map $I_K^\mathfrak{m} \twoheadrightarrow J_K^{S(\mathfrak{m})}$, $(\alpha_\mathfrak{p}) \mapsto \prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(\alpha_\mathfrak{p})}$, and the kernel is precisely $U(\mathfrak{m}) \cap I^\mathfrak{m}$. Furthermore, there is a natural embedding $K^{\mathfrak{m},1} \hookrightarrow I_K^\mathfrak{m}$, $\alpha \mapsto (\alpha_\mathfrak{p})$, and not only $K^{\mathfrak{m},1} \subset \ker(I_K^\mathfrak{m} \twoheadrightarrow \mathrm{Cl}^\mathfrak{m}(K))$, but also $\mathrm{Cl}^\mathfrak{m}(K) = J_K^{S(\mathfrak{m})}/\operatorname{im}(K^{\mathfrak{m},1} \to I_K^\mathfrak{m} \to J_K^{S(\mathfrak{m})})$. From this, it follows that $\mathrm{Cl}^\mathfrak{m}(K) \cong I^\mathfrak{m}/K^{\mathfrak{m},1}(U(\mathfrak{m}) \cap I^\mathfrak{m})$. Thus, (2) will follow if we prove that the natural map $I_K^\mathfrak{m} \hookrightarrow I_K$ induces an isomorphism $I_K^\mathfrak{m}/K^{\mathfrak{m},1} \xrightarrow{\sim} I_K/K^\times$. Firstly, as $I_K^\mathfrak{m} \cap K^\times = K^{\mathfrak{m},1}$, the map $I_K^\mathfrak{m}/K^{\mathfrak{m},1} \to I_K/K^\times$ is injective. To show the surjectivity, it suffices to show $I_K = I^{\mathfrak{m}}K^\times$. The content of this in concrete terms is as follows: suppose $\mathfrak{m}$ is a modulus, and suppose, for each $\mathfrak{p}|\mathfrak{m}$, we have $\alpha_{\mathfrak{p}} \in K_{\mathfrak{p}}^\times$. Then, there exists $\alpha \in K^\times$, such that $\alpha \equiv \alpha_{\mathfrak{p}} \pmod{\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}}$ for all finite $\mathfrak{p}|\mathfrak{m}$, and α, $\alpha_{\mathfrak{p}}$ have the same sign for all real $\mathfrak{p}|\mathfrak{m}$. This follows from the following theorem: namely, this shows that however many congruence conditions and sign conditions you apply, there is an element in $K^\times$ realizing them (as long as there are finitely many conditions).

Theorem 7.12 (Weak approximation theorem). *Let F be a field, and let $|\cdot|_1, \cdots, |\cdot|_n$ be nontrivial pairwise inequivalent absolute values on F. Let F_i be the topological space where the underlying set is F and the topology is generated by $|\cdot|_i$. Then, inside the topological space $F_1 \times \cdots \times F_n$, the diagonal subset $F \subset F_1 \times \cdots \times F_n$, namely those of the form $(x, x, \cdots, x)$ for $x \in F$, is a dense subset.*

Proof. This asks you to find, for any $a_1, \cdots, a_n \in F$ and $\varepsilon > 0$, an element $b \in K$ such that $|a_i - b|_i < \varepsilon$. Note first that it is sufficient to find, for each $1 \leq m \leq n$, an element $c_m \in F$ such that $|c_m|_m > 1$ and $|c_m|_i < 1$ for all $i \neq m$. If there is such an element, then for $N \gg 0$, the element $\sum_{i=1}^n \frac{c_i^N}{1+c_i^N} a_i$ will be such an element, as

$$\lim_{N\to\infty} \frac{c_i^N}{1+c_i^N} = \begin{cases} 1 & \text{with respect to } |\cdot|_i \\ 0 & \text{with respect to } |\cdot|_j \text{ for any } j \neq i. \end{cases}$$

Thus we are reduced, by rearranging indexes, to finding an element $c \in F$ such that $|c|_1 > 1$ and $|c|_i < 1$ for all $i \geq 2$. We do an induction on n. If $n = 2$, this is basically the definition of inequivalence of two absolute values $|\cdot|_1$ and $|\cdot|_2$. For general n, by induction hypothesis, we can first find $c' \in F$ such that $|c'|_1 > 1$ and $|c'|_i < 1$ for all $2 \leq i \leq n-1$. If $|c'|_n < 1$, then we are already happy. If not, we can find $b \in F$ such that $|b|_1 > 1$ and $|b|_n < 1$. Using this, if $|c'|_n = 1$, then for $N \gg 0$, $c'^N b$ will satisfy the condition, and if $|c'|_n > 1$, then for $N \gg 0$, $\frac{c'^N}{1+c'^N} b$ will satisfy the condition. □

□

Definition 7.13 (Ray class field). By the global existence theorem and Proposition 7.11, for a global field K and a modulus $\mathfrak{m}$ of K, there exists a finite abelian extension $K(\mathfrak{m})$ of K such that $C_K/N_{K(\mathfrak{m})/K}(C_{K(\mathfrak{m})}) \cong \mathrm{Cl}^{\mathfrak{m}}(K)$ (as finite quotients of C_K). This field $K(\mathfrak{m})$ is called the **ray class field** of K for modulus $\mathfrak{m}$. In particular, if $\mathfrak{m} = \mathfrak{m}_\emptyset$, $K(\mathfrak{m}_\emptyset) =: H_K$ is called the **Hilbert class field**. If on the other hand $\mathfrak{m}$ is the product of all real places of K, then $K(\mathfrak{m})$ is called the **narrow class field**.

We can now reformulate the global class field theory in terms of ray class fields.

Theorem 7.14 (Ideal theoretic global class field theory). *Let L/K be a finite abelian extension of global fields. We define the modulus $\mathfrak{f}_{L/K}$ of K, called the* (global) conductor *of L/K, as $\mathfrak{f}_{L/K}(\mathfrak{p}) = \mathfrak{f}_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}$ for any prime $\mathfrak{q}$ of L dividing $\mathfrak{p}$, where $\mathfrak{f}_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}$ is the local conductor (Definition 1.1) when $\mathfrak{p}$ is a finite prime, and $\mathfrak{f}_{\mathbb{C}/\mathbb{C}} = \mathfrak{f}_{\mathbb{R}/\mathbb{R}} = 0$, $\mathfrak{f}_{\mathbb{C}/\mathbb{R}} = 1$, when $\mathfrak{p}$ is an infinite prime.*

(1) *For any modulus $\mathfrak{m}$ of K divisible by $\mathfrak{f}_{L/K}$, $L \subset K(\mathfrak{m})$. For such $\mathfrak{m}$, we may define the* ***global Artin map*** $\mathrm{Art}^{\mathfrak{m}}_{L/K} : J_K^{S(\mathfrak{m})} \to \mathrm{Gal}(L/K)$ *as $\mathfrak{p} \mapsto \mathrm{Fr}_{\mathfrak{p}}$ for any prime ideal $\mathfrak{p}$ of K not dividing $\mathfrak{m}$ (this is well-defined as all prime ideals of K ramified in L divide $\mathfrak{f}_{L/K}$). Then,* $\ker \mathrm{Art}^{\mathfrak{m}}_{L/K} \supset K^{\mathfrak{m},1}$*, giving a natural surjective map* $\mathrm{Art}^{\mathfrak{m}}_{L/K} : \mathrm{Cl}^{\mathfrak{m}}(K) \twoheadrightarrow \mathrm{Gal}(L/K)$*.*

(2) *For any modulus $\mathfrak{m}$ of K, there is a one-to-one incusion-reversing bijection*

$$\{\textit{Finite subgroups of } \mathrm{Cl}^{\mathfrak{m}}(K)\} \leftrightarrow \{\textit{Finite abelian extensions } L/K \textit{ with } \mathfrak{f}_{L/K} | \mathfrak{m}\}.$$

Proof. This follows directly from the local-global compatibility and the definition of the local conductor (and the fact that the global norm is a product of the local norms). □

This shows that $K(\mathfrak{m})$ is the maximal abelian extension of K with the "ramification bounded by $\mathfrak{m}$." For example, the Hilbert class field is the maximal abelian extension of K that is **everywhere unramified** (including infinite places; an infinite place is unramified if the real places stay real above), and the narrow class field is the maximal abelian extension of K that is **finitely everywhere unramified** (i.e. all finite primes are unramified).

Theorem 7.15 (Principal ideal theorem). *Let K be a global field, and let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal. Then, $\mathfrak{p}\mathcal{O}_{H_K}$ is a principal ideal in H_K.*

Proof. This statement follows from the compatibility of the global Artin maps with changing fields, i.e. we look at

$$\begin{tikzcd}
C_K \arrow[r, "\mathrm{Art}_K"] \arrow[d, hook] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[d, "V"] & \rightsquigarrow & \mathrm{Cl}(K) \arrow[r, "\sim"] \arrow[d] & \mathrm{Gal}(H_K/K) \arrow[d, "V"] \\
C_{H_K} \arrow[r, "\mathrm{Art}_{H_K}"'] & \mathrm{Gal}(H_K^{\mathrm{ab}}/H_K) & & \mathrm{Cl}(H_K) \arrow[r, "\sim"'] & \mathrm{Gal}(H_{H_K}/H_K).
\end{tikzcd}$$

Then this follows from a hard (yet elementary) group-theoretic fact that the transfer homomorphism $V : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is zero if $H = [G, G]$. □

Remark 7.16. One can show not just the quadratic reciprocity law but the n-ic reciprocity law using the global class field theory; see [ANT] for more classical applications of ideal-theoretic description of global class field theory.

Example 7.17. See [ANT, Exercise 16.2] for the full determination of the ray class fields of $\mathbb{Q}$ by elementary considerations.

8. Kronecker–Weber theorems: **Explicit class field theory** for $\mathbb{Q}$ and $\mathbb{Q}_p$

Before wrapping up our proofs of global/local class field theories by verifying the class formation axioms + ε, we start with a baby version, namely describing $\mathbb{Q}^{\mathrm{ab}}$ and $\mathbb{Q}_p^{\mathrm{ab}}$.

Theorem 8.1 (Kronecker–Weber theorem).

$$\mathbb{Q}^{\mathrm{ab}} = \bigcup_{n \geq 1} \mathbb{Q}(\zeta_n).$$

Theorem 8.2 (Local Kronecker–Weber theorem).

$$\mathbb{Q}_p^{\mathrm{ab}} = \bigcup_{n \geq 1} \mathbb{Q}_p(\zeta_n).$$

We will show how these follow from the elementary ramification theory. In fact, the derivation of local Kronecker–Weber theorem is related to the Lubin–Tate theory (which will be used for a proof of local existence theorem).

Remark 8.3. The whole idea of describing K^{ab} by adjoining explicit elements (or, even better, by adjoining **units**) falls under the name of **Kronecker's Jugendtraum**. In the local case, this is completely solved by the Lubin–Tate theory, which we will see in a few lectures. For number fields, we have such constructions for only certain types of number fields; for example, the theory of complex multiplication for imaginary quadratic fields, which we will also see later. There is not even a conjectural picture of what this should be for general number fields. For example, even a conjecture for the complex cubic fields was not really known until 2023, see [BCG].

Lemma 8.4. *The Kronecker–Weber theorem follows from the local Kronecker–Weber theorem.*

Proof. Let K be a finite abelian extension of $\mathbb{Q}$. There are finitely many primes $p \in \mathbb{Z}$ ramified in K. Pick a prime $\mathfrak{p}$ of K lying over p. Then, by the local Kronecker–Weber, $K_{\mathfrak{p}} \subset \mathbb{Q}_p(\zeta_{n_p})$ for some $n_p \geq 1$. Let $e_p = \mathrm{ord}_p(n_p)$ and let $n = \prod_p p^{e_p}$.

We claim that $K \subset \mathbb{Q}(\zeta_n)$. This will follow if we prove that $L = K(\zeta_n) = \mathbb{Q}(\zeta_n)$. It is firstly obvious that $L \supset \mathbb{Q}(\zeta_n)$. Let $p \in \mathbb{Z}$ be any prime tha ramifies in K, and let $\mathfrak{q}$ be a prime of L lying over p. Then, $L_{\mathfrak{q}} \subset \mathbb{Q}_p(\zeta_{n_p}, \zeta_n) = \mathbb{Q}_p(\zeta_{\mathrm{lcm}(n_p,n)})$. Let $I_p \subset \mathrm{Gal}(L_{\mathfrak{q}}/\mathbb{Q}_p) \subset \mathrm{Gal}(L/\mathbb{Q})$ be the inertia subgroup of p in L. Let $U := (L^{\mathfrak{q}})^{I_p}$, which is the maximal unramified subextension of $L^{\mathfrak{q}}/\mathbb{Q}_p$. Then, as adjoining a prime-to-p-th power root of unity gives an unramified extension, $L_{\mathfrak{q}} = U(\zeta_{p^{e_p}})$. Therefore, $I_p \subset (\mathbb{Z}/p^{e_p}\mathbb{Z})^\times$. Let $I \leq \mathrm{Gal}(L/\mathbb{Q})$ be the subgroup generated by I_p for primes $p \in \mathbb{Z}$ ramified in K. Then, $|I| \leq \prod_p |I_p| \leq \prod_p \phi(p^{e_p}) = \phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$. On the other hand, $L^I/\mathbb{Q}$ is a finitely everywhere unramified; namely, for any prime number $p \in \mathbb{Z}$, p is unramified in L^I. By Minkowski's theorem, $L^I = \mathbb{Q}$, which implies that $[L : \mathbb{Q}] = |I| \leq [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$, which implies that $L = \mathbb{Q}(\zeta_n)$, as desired.

Theorem 8.5 (Minkowski's theorem). *If a number field K satisfies that every prime number $p \in \mathbb{Z}$ is unramified in K (or $K/\mathbb{Q}$ is **finitely everywhere unramified**), then $K = \mathbb{Q}$.*

Proof. You can use the Minkowski's discriminant bound in a different way. Namely, we know that, if $[K : \mathbb{Q}] = n = r + 2s$, then each ideal class of $\mathrm{Cl}(K)$ has an integral ideal representative $\mathfrak{a}$ such that $N(\mathfrak{a}) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|}$. As $N(\mathfrak{a}) \geq 1$, we have $\sqrt{|\operatorname{disc}(K)|} \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^s \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{n/2}$. One can see that $\frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{n/2} > 1$ as long as $n \geq 2$ (the expression increases as n increases). Thus, if $n \geq 2$, then $|\operatorname{disc}(K)| \geq 2$ has a prime factor, which makes K not finitely everywhere unramified. Thus $K = \mathbb{Q}$. □

□

Thus, it remains to prove the local Kronecker–Weber theorem. The key input is the Hasse–Arf theorem.

Theorem 8.6 (Hasse–Arf theorem)**.** *Let K/L be a finite abelian extension of local fields. Then, the jumps of ramification groups $\mathrm{Gal}(K/L)^t$ in upper numbering happen at integers. Namely, if $t \geq -1$ is such that $\mathrm{Gal}(K/L)^t \neq \mathrm{Gal}(K/L)^{t+\varepsilon}$ for arbitrarily small number $\varepsilon > 0$, then $t \in \mathbb{Z}$.*

Proof. Omitted. It is still elementary but requires some clever ideas. □

Proof of the local Kronecker–Weber theorem, Theorem 8.2. We let $\mathbb{Q}_p^{\mathrm{cyc}} = \bigcup_{n\geq 1} \mathbb{Q}_p(\zeta_n)$ and $\mathbb{Q}_p(\zeta_{p^\infty}) = \bigcup_{n\geq 1} \mathbb{Q}_p(\zeta_{p^n})$. We already know $\mathbb{Q}_p^{\mathrm{nr}} = \bigcup_{(n,p)=1} \mathbb{Q}_p(\zeta_n)$, so $\mathbb{Q}_p^{\mathrm{cyc}} = \mathbb{Q}_p^{\mathrm{nr}}\mathbb{Q}_p(\zeta_{p^\infty})$, and $\mathbb{Q}_p^{\mathrm{nr}} \cap \mathbb{Q}_p(\zeta_{p^\infty}) = \mathbb{Q}_p$. Let $K/\mathbb{Q}_p$ be a finite abelian extension. Then, we have a short exact sequence

$$1 \to \mathrm{Gal}(K\mathbb{Q}_p^{\mathrm{cyc}}/\mathbb{Q}_p^{\mathrm{cyc}}) \to \mathrm{Gal}(K\mathbb{Q}_p^{\mathrm{cyc}}/\mathbb{Q}_p(\zeta_{p^\infty})) \to \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{cyc}}/\mathbb{Q}_p(\zeta_{p^\infty})) \to 1.$$

Note that $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{cyc}}/\mathbb{Q}_p(\zeta_{p^\infty})) \cong \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{nr}}/\mathbb{Q}_p) \cong \widehat{\mathbb{Z}}$, so it is a free pro-cyclic group. Therefore, by taking a lift of a topological generator $1 \in \widehat{\mathbb{Z}}$ (namely, the closure of the group generated by the element is everything; in this specific case, this says that $\mathbb{Z} \subset \widehat{\mathbb{Z}}$ is dense), this short exact sequence splits. Therefore, taking the fixed field of this lift, we obtain a field extension $F/\mathbb{Q}_p(\zeta_{p^\infty})$ such that $F \cap \mathbb{Q}_p^{\mathrm{cyc}} = \mathbb{Q}_p(\zeta_{p^\infty})$ and $F\mathbb{Q}_p^{\mathrm{cyc}} = K\mathbb{Q}_p^{\mathrm{cyc}}$. As $\mathbb{Q}_p^{\mathrm{cyc}} = \mathbb{Q}_p(\zeta_{p^\infty})^{\mathrm{nr}}$, $F \cap \mathbb{Q}_p^{\mathrm{cyc}} = \mathbb{Q}_p(\zeta_{p^\infty})$ means that $F/\mathbb{Q}_p(\zeta_{p^\infty})$ and $F/\mathbb{Q}_p$ are totally ramified[7]. Note that $K\mathbb{Q}_p^{\mathrm{cyc}}$ is abelian over $\mathbb{Q}_p$, so $F/\mathbb{Q}_p$ is also abelian.

We claim that $F = \mathbb{Q}_p(\zeta_{p^\infty})$, which will prove the local Kronecker–Weber theorem, as then $K\mathbb{Q}_p^{\mathrm{cyc}} = F\mathbb{Q}_p^{\mathrm{cyc}} = \mathbb{Q}_p^{\mathrm{cyc}}$. This will follow from the following elementary computation of ramification subgroups.

Lemma 8.7. *The jumps (in upper numbering) of ramification subgroups of $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)$ happen at all nonnegative integers (except at the 0-th ramification subgroup when $p = 2$). More precisely, for every $n \in \mathbb{Z}_{\geq 0}$,*

$$\left|\frac{\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)^n}{\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)^{n+1}}\right| = \begin{cases} p-1 & \text{if } n = 0 \\ p & \text{if } n \geq 1. \end{cases}$$

Proof. By the Hasse–Arf theorem (and the compatibility of upper numbering with taking quotients), we know that the jumps happen at some integers. Thus this boils down to calculating the jumps of $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$ for each $m \geq 1$. Note that we have an explicit uniformizer $\pi := \zeta_{p^m} - 1 \in \mathbb{Q}_p(\zeta_{p^m})$ that we can use. Recall that, if we normalize $v(\pi) = 1$, then $v(p) = \varphi(p^m) = p^{m-1}(p-1)$. For $a \in (\mathbb{Z}/p^m\mathbb{Z})^\times$, let $\sigma_a \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p)$ be such that $\sigma_a(\zeta_{p^m}) = \zeta_{p^m}^a$. Then $\sigma_a(\pi) - \pi = \zeta_{p^m}(\zeta_{p^m}^{a-1} - 1)$. Note that $\zeta_{p^m}^{a-1} - 1 = \sum_{i=1}^{a-1} \pi^i \binom{a-1}{i}$, so $v(\sigma_a(\pi) - \pi) = 1$ if $p \nmid (a-1)$. Now we can conclude what the ramification subgroups are in the case of $m = 1$ as any $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $p|(a-1)$ means $a = 1$ is the identity. Namely, $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p) = \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)_0 \supset \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)_1 = \{1\}$.

If $p|(a-1)$, then $\zeta_{p^m}^{a-1} - 1 \equiv \sum_{1\leq i\leq a-1, p|i} \pi^i \binom{a-1}{i} \pmod{p}$. So unless $\binom{a-1}{p}$ is divisible by p, we can conclude that $v(\zeta_{p^m}^{a-1} - 1) = p$. One sees elementarily that, under the assumption that

[7] For a possibly infinite extension of local fields K/L, we say K/L is totally ramified if the maximal unramified subextension is L.

$p|(a-1)$, $\binom{a-1}{p}$ is divisible by p iff $p^2|(a-1)$. Now we can finish the calculation in the case of $m=2$;

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^2})/\mathbb{Q}_p)_0 = (\mathbb{Z}/p^2\mathbb{Z})^\times,$$
$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^2})/\mathbb{Q}_p)_1 = \cdots = \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^2})/\mathbb{Q}_p)_{p-1} = \{a \in (\mathbb{Z}/p^2\mathbb{Z})^\times \ : \ a \equiv 1 \pmod p\},$$
$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^2})/\mathbb{Q}_p)_p = \cdots = \{1\}.$$

If $p^2|(a-1)$, then $\zeta_{p^m}^{a-1} - 1 \equiv \sum_{1\le i\le a-1, p^2|i} \pi^i \binom{a-1}{i} \pmod p$. We apply the same argument, and the pattern is the same. One concludes that, for a general m, we have

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p)_0 = (\mathbb{Z}/p^m)^\times,$$
$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p)_1 = \cdots = \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p)_{p-1} = \{a \in (\mathbb{Z}/p^m\mathbb{Z})^\times \ : \ a \equiv 1 \pmod p\},$$
$$\cdots,$$
$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p)_{p^{i-1}} = \cdots = \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p)_{p^i-1} = \{a \in (\mathbb{Z}/p^m\mathbb{Z})^\times \ : \ a \equiv 1 \pmod{p^i}\},$$
$$\cdots,$$
$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p)_{p^{m-1}} = \cdots = \{1\}.$$

Now we compute the upper numbering. Note that the jumps (i.e. n such that $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p)_n \neq \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p)_{n+1}$) happen exactly at $0, p-1, \cdots, p^{m-1}-1$. We compute

$$\phi_{\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p}(p^i - 1) = \frac{p-1}{p-1} + \frac{(p^2-1)-(p-1)}{p(p-1)} + \cdots + \frac{(p^i-1)-(p^{i-1}-1)}{p^{i-1}(p-1)} = i.$$

These computations altogether imply the Lemma. □

Why is this useful? It's because these numbers are optimal!

Lemma 8.8. *Let K/L be a totally ramified abelian extension. Let $\mathfrak{p} \subset \mathcal{O}_L$ be the maximal ideal, and let q be the order of the residue field of L. Then,*

$$\left|\frac{\mathrm{Gal}(K/L)^n}{\mathrm{Gal}(K/L)^{n+1}}\right| \le \begin{cases} q-1 & \textit{if } n = 0 \\ q & \textit{if } n \ge 1. \end{cases}$$

Proof. Suppose first that K/L is finite, and let π be a uniformizer of K. Then, we have a group homomorphism

$$\mathrm{Gal}(K/L)_0 \to \mathbb{F}_q^\times, \quad \sigma \mapsto \frac{\sigma(\pi)}{\pi} \pmod{\mathfrak{p}}.$$

This is a well-defined group homomorphism that does not depend on the choice of π, and the kernel is exactly $\mathrm{Gal}(K/L)_1$, which implies that $\mathrm{Gal}(K/L)_0/\mathrm{Gal}(K/L)_1$ embeds into a subgroup of $\mathbb{F}_q^\times$. For $m \ge 1$, we have a similar group homomorphism

$$\mathrm{Gal}(K/L)_m \to \mathbb{F}_q, \quad \sigma \mapsto \frac{\sigma(\pi)}{\pi} - 1 \pmod{\pi^{m+1}},$$

which is a well-defined group homomorphism that does not depend on the choice of π, and the kernel is exactly $\mathrm{Gal}(K/L)_{m+1}$. Thus, $\mathrm{Gal}(K/L)_m/\mathrm{Gal}(K/L)_{m+1}$ embeds into a subgroup of $\mathbb{F}_q$. As we already know the jumps in upper numbering happen at integers by the Hasse–Arf theorem, the Lemma follows, in the case when K/L is finite. The case of infinite extension follows from the case of finite extensions and the compatibility of upper numbering with taking quotients. □

Note that the compatibility of upper numbering with taking quotients imply that, for any $s \geq 0$,

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)^s = \frac{\mathrm{Gal}(F/\mathbb{Q}_p)^s}{\mathrm{Gal}(F/\mathbb{Q}_p)^s \cap \mathrm{Gal}(F/\mathbb{Q}_p(\zeta_{p^\infty}))}.$$

Thus, for $n \geq 0$,

$$\left|\frac{\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)^n}{\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)^{n+1}}\right| \geq \left|\frac{\mathrm{Gal}(F/\mathbb{Q}_p)^n}{\mathrm{Gal}(F/\mathbb{Q}_p)^{n+1}}\right| = \left|\frac{\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)^n}{\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)^{n+1}}\right| \left|\frac{\mathrm{Gal}(F/\mathbb{Q}_p)^n \cap \mathrm{Gal}(F/\mathbb{Q}_p(\zeta_{p^\infty}))}{\mathrm{Gal}(F/\mathbb{Q}_p)^{n+1} \cap \mathrm{Gal}(F/\mathbb{Q}_p(\zeta_{p^\infty}))}\right|,$$

which implies that $\left|\frac{\mathrm{Gal}(F/\mathbb{Q}_p)^n \cap \mathrm{Gal}(F/\mathbb{Q}_p(\zeta_{p^\infty}))}{\mathrm{Gal}(F/\mathbb{Q}_p)^{n+1} \cap \mathrm{Gal}(F/\mathbb{Q}_p(\zeta_{p^\infty}))}\right| = 1$, or $\mathrm{Gal}(F/\mathbb{Q}_p)^n \cap \mathrm{Gal}(F/\mathbb{Q}_p(\zeta_{p^\infty})) = \mathrm{Gal}(F/\mathbb{Q}_p)^{n+1} \cap \mathrm{Gal}(F/\mathbb{Q}_p(\zeta_{p^\infty}))$ for all $n \geq 0$. As $F/\mathbb{Q}_p$ is totally ramified, $\mathrm{Gal}(F/\mathbb{Q}_p(\zeta_{p^\infty})) \subset \mathrm{Gal}(F/\mathbb{Q}_p) = \mathrm{Gal}(F/\mathbb{Q}_p)^0$. Therefore, for every n, $\mathrm{Gal}(F/\mathbb{Q}_p(\zeta_{p^\infty})) \subset \mathrm{Gal}(F/\mathbb{Q}_p)^n$. This implies that $\mathrm{Gal}(F/\mathbb{Q}_p(\zeta_{p^\infty})) = \{1\}$; if there is a nontrivial element, then this comes from some finite layer, which should not be contained in an N-th ramification group (in upper numbering) for a large enough $N \gg 0$. This shows that $F = \mathbb{Q}_p(\zeta_{p^\infty})$, as desired. □

Remark 8.9. The point of the above argument was that there was an explicit totally ramified extension that has optimal numbers for the ramification subgroups. For a more general local field, a **Lubin–Tate extension** will do the job. In fact, one can use the same argument to derive the entirety of the local class field theory from the Lubin–Tate theory without using any cohomological arguments.

9. Local class field theory: verification of the class formation axioms

We now wrap up the proof of cohomological part of the local class field theory. We already verified **Axiom 1** of the two class formation axioms (Theorem 4.14), and **Axiom 2** is Theorem 4.20, which we prove here.

Proof of Theorem 4.20. We exhibit a proof that works for characteristic 0 local fields.

Let L/K be a finite Galois extension of local fields of degree n, and let M/K be an **unramified** extension of the same degree n. By Theorem 4.14 and the inflation-restriction exact sequence, we have two injective maps

$$\mathrm{Inf} : \mathrm{Br}(M/K) \hookrightarrow \mathrm{Br}(ML/K), \quad \mathrm{Inf} : \mathrm{Br}(L/K) \hookrightarrow \mathrm{Br}(ML/K).$$

Note that we already know that $\mathrm{Br}(M/K) \cong \mathbb{Z}/n\mathbb{Z}$ as M/K is unramified. We will prove Theorem 4.20 by showing that the images of two inflation maps coincide in $\mathrm{Br}(ML/K)$; in this way, we know that $\mathrm{Br}(L/K)$ not only is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ but also is canonically so via the invariant map we borrow from $\mathrm{Br}(M/K)$.

Firstly, we show that $\operatorname{im}(\mathrm{Inf} : \mathrm{Br}(L/K) \hookrightarrow \mathrm{Br}(ML/K)) \supset \operatorname{im}(\mathrm{Inf} : \mathrm{Br}(M/K) \hookrightarrow \mathrm{Br}(ML/K))$. We may use the inflation-restriction exact sequence

$$0 \to \mathrm{Br}(L/K) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(ML/K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(ML/L),$$

so the claim is equivalent to $\ker(\mathrm{Res} : \mathrm{Br}(ML/K) \to \mathrm{Br}(ML/L)) \supset \operatorname{im}(\mathrm{Inf} : \mathrm{Br}(M/K) \hookrightarrow \mathrm{Br}(ML/K))$, or that the composition $\mathrm{Br}(M/K) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(ML/K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(ML/L)$ is zero.

We first assume that L/K is totally ramified. Then, L/K and M/K are linearly disjoint, and $\mathrm{Gal}(ML/L) \cong \mathrm{Gal}(M/K)$ by restricting to M. One can check easily by hand on the level of cocycles that the composition map $\mathrm{Br}(M/K) \to \mathrm{Br}(ML/L)$ coincides with the map $H^2(\mathrm{Gal}(M/K), M^\times) \to H^2(\mathrm{Gal}(ML/L), ML^\times)$, induced by the natural inclusion $M^\times \to ML^\times$ and the canonical identification $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(ML/L)$. As $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(ML/L)$ is a finite cyclic group, this map is the same as the corresponding map in H^0_T by the periodicity. Thus, we are reduced to showing that the natural map

$$K^\times/N_{M/K}(M^\times) \to L^\times/N_{ML/L}(ML^\times),$$

is zero. We know what both sides are, as both M/K and ML/L are unramified. Namely, both are cyclic groups of order n generated by the respective uniformizers $\pi_K \in K$ and $\pi_L \in L$. However $\pi_K = u\pi_L^n$ for $u \in \mathcal{O}_L^\times$, as L/K is totally ramified. As $\mathcal{O}_L^\times \subset N_{ML/L}(ML^\times)$, this implies that π_K is sent to zero by the map, which implies that the map is zero, as desired.

In the general case of L/K, take the maximal unramified subextension U/K of L/K. Then, naturally U/K is also a subextension of M/K (as M/K is the unramified extension of degree n). By again Theorem 4.14 and the inflation-restriction exact sequence, by the inflation map, $\mathrm{Br}(U/K)$ embeds into both $\mathrm{Br}(M/K)$ and $\mathrm{Br}(L/K)$, and at least the composition $\mathrm{Br}(M/K) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(ML/K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(ML/L)$ sends those coming from $\mathrm{Br}(U/K) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(M/K)$ to zero as the composition $\mathrm{Br}(U/K) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(M/K) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(ML/K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(ML/L)$ is the same as the composition $\mathrm{Br}(U/K) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(L/K) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(ML/K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(ML/L)$ and the latter composition goes through the inflation-restriction exact sequence for $ML/L/K$. Now the veracity of whether the composition $\mathrm{Br}(M/K) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(ML/K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(ML/L)$ is zero or not can be checked by sending $\operatorname{coker}(\mathrm{Inf} : \mathrm{Br}(U/K) \to \mathrm{Br}(M/K))$ injectively into $\mathrm{Br}(M/U)$ which is again the inflation-restriction exact sequence. Namely, the claim for L/K follows from the claim for L/U, which is totally ramified, which we already showed (this requires checking various compatibilities which are left as an exercise to the reader).

Thus, we have shown one inclusion. To show the other inclusion, it suffices to show that $\#\mathrm{Br}(L/K) \leq n$. Note that, if $L/M/K$ is any subextension where M/K is Galois, then again by Theorem 4.14 and the inflation-restriction exact sequence, $0 \to \mathrm{Br}(M/K) \to \mathrm{Br}(L/K) \to \mathrm{Br}(L/M)$ implies that $\#\mathrm{Br}(L/K) \leq \#\mathrm{Br}(M/K)\,\mathrm{Br}(L/M)$. Thus, we can use an induction on n and reduce proving $\#\mathrm{Br}(L/K) \leq n$ in the case when $\mathrm{Gal}(L/K)$ has no proper nontrivial normal subgroup. However, by the consideration of the ramification subgroups, we know that the Galois group of local fields is always solvable. Thus, this means that we are reduced to proving $\#\mathrm{Br}(L/K) \leq n$ when L/K is a cyclic Galois extension of prime degree.

We now prove that $\#\operatorname{Br}(L/K) = n$ when L/K is cyclic, which will finish the proof of Theorem 4.20. As now $\mathrm{Gal}(L/K)$ is cyclic, we can use the periodicity of Tate cohomology, and in particular the Herbrand quotient. By Theorem 4.14, what we want to prove is the same as $h(L^\times) = n$. Using the short exact sequence of $\mathrm{Gal}(L/K)$-modules $1 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{\mathrm{ord}} \mathbb{Z} \to 0$, we have $h(L^\times) = h(\mathcal{O}_L^\times)h(\mathbb{Z})$. We know $H_T^0(\mathrm{Gal}(L/K), \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ and $H_T^1(\mathrm{Gal}(L/K), \mathbb{Z}) = \mathrm{Hom}_{\mathrm{Grp}}(\mathrm{Gal}(L/K), \mathbb{Z}) = 1$, so $h(\mathbb{Z}) = n$. Therefore, it suffices to show that $h(\mathcal{O}_L^\times) = 1$.

We show this in a few steps. By the normal basis theorem, there is $x \in L$ such that $\{\sigma(x) : \sigma \in \mathrm{Gal}(L/K)\}$ is a K-basis of L. We may multiply x with a nonzero element in K, so we may assume that $x \in p\mathcal{O}_K$, where p is the characteristic of the residue field of K (i.e. K is a finite extension of $\mathbb{Q}_p$). Let $V := \bigoplus_{\sigma \in \mathrm{Gal}(L/K)} \mathcal{O}_K \sigma(x) \subset \mathcal{O}_L$. Then, V as a $\mathrm{Gal}(L/K)$-module is isomorphic to $\mathrm{Ind}_{\{1\}}^{\mathrm{Gal}(L/K)} \mathcal{O}_K$, so V is acyclic. In particular, $h(V) = 1$.

Now consider the exponential and the logarithm maps

$$\exp : p\mathcal{O}_L \to 1 + p\mathcal{O}_L, \quad \log : 1 + p\mathcal{O}_L \to p\mathcal{O}_L,$$

defined as

$$\exp(x) := \sum_{i=0}^{\infty} \frac{x^i}{i!}, \quad \log(1+x) := \sum_{i=1}^{\infty} (-1)^{i-1} \frac{x^i}{i}.$$

Note that the divisibility constraints make sure that these infinite sums converge and also that $\exp \circ \log$ and $\log \circ \exp$ are identity maps. Therefore, $p\mathcal{O}_L$ and $1+p\mathcal{O}_L$ are isomorphic as $\mathrm{Gal}(L/K)$-modules ($\log$ and $\exp$ give explicit isomorphisms in both ways). In particular, $\exp(V) \subset 1 + p\mathcal{O}_L \subset \mathcal{O}_L^\times$ is also acyclic, and $h(\exp(V)) = 1$. Therefore, $h(\mathcal{O}_L^\times) = h(\exp(V))h\left(\frac{\mathcal{O}_L^\times}{\exp(V)}\right) = h\left(\frac{\mathcal{O}_L^\times}{\exp(V)}\right)$. Now $\frac{\mathcal{O}_L^\times}{\exp(V)}$, as an abelian group, is a finite abelian group, so $H^0\left(\mathrm{Gal}(L/K), \frac{\mathcal{O}_L^\times}{\exp(V)}\right)$ and $H_0\left(\mathrm{Gal}(L/K), \frac{\mathcal{O}_L^\times}{\exp(V)}\right)$ are also finite abelian groups. Therefore, $\#H_T^{-1}\left(\mathrm{Gal}(L/K), \frac{\mathcal{O}_L^\times}{\exp(V)}\right) = \#H_T^0\left(\mathrm{Gal}(L/K), \frac{\mathcal{O}_L^\times}{\exp(V)}\right)$ as they are respectively the kernel and the cokernel of the same group homomorphism $N : H_0\left(\mathrm{Gal}(L/K), \frac{\mathcal{O}_L^\times}{\exp(V)}\right) \to H^0\left(\mathrm{Gal}(L/K), \frac{\mathcal{O}_L^\times}{\exp(V)}\right)$ between finite abelian groups of the same order (they are of the same order as they are respectively the cokernel and the kernel of the same group homomorphism $\sigma - 1 : \frac{\mathcal{O}_L^\times}{\exp(V)} \to \frac{\mathcal{O}_L^\times}{\exp(V)}$, where $\sigma \in \mathrm{Gal}(L/K)$ is a generator). Therefore, $h\left(\frac{\mathcal{O}_L^\times}{\exp(V)}\right) = 1$, which finishes the proof. □

10. Lubin–Tate theory: **Explicit class field theory** for local fields

We are left with the "ε" of the local class field theory, namely the local existence theorem (and how the local class field theory detects ramification on both sides). One may abstractly verify (*), but rather than doing so, we show the local existence theorem by showing that there is an **Explicit class field theory** for all local fields. Namely, we can explicitly construct the analogues of $\mathbb{Q}_p(\zeta_{p^\infty})$ (which played an important role in the local Kronecker–Weber theorem) for all local fields. An idea is that $\mathbb{Q}_p(\zeta_{p^\infty})$ is obtained by adjoining ζ_{p^m} for $m \geq 1$, which is a solution to the equation $X^{p^m} = 1$. This has the special property that $X^{p^{m+1}} = 1$ is obtained from

$X^{p^m} = 1$ by plugging X^p into $X^{p^m} = 1$. Furthermore, the powers of ζ_{p^m} form a multiplicative group. A streamlined way of thinking about these facts is as follows.

- Let $\overline{\mathbb{Q}}_p$ be an algebraic closure of $\mathbb{Q}_p$ and let $\mathfrak{m}_{\overline{\mathbb{Q}}_p} \subset \mathcal{O}_{\overline{\mathbb{Q}}_p}$ be the maximal ideal (i.e. any element of $\overline{\mathbb{Q}}_p$ with positive valuation). Then, $1 + \mathfrak{m}_{\overline{\mathbb{Q}}_p}$ is a multiplicative group. It's more natural to think of $(1+\mathfrak{m}_{\overline{\mathbb{Q}}_p}, \times)$ instead as $\mathfrak{m}_{\overline{\mathbb{Q}}_p}$ with a multiplication law $x \cdot y = x+y+xy$ (so that $(1+x)(1+y) = 1 + (x+y+xy)$).
- Furthermore, there is a group homomorphism $\psi : (1+\mathfrak{m}_{\overline{\mathbb{Q}}_p}, \times) \to (1+\mathfrak{m}_{\overline{\mathbb{Q}}_p}, \times)$ defined by $\psi(a) = a^p$. In terms of the other multiplication law $(\mathfrak{m}_{\overline{\mathbb{Q}}_p}, \cdot)$, the formula is $\psi(x) = (x+1)^p - 1$.
- The field $\mathbb{Q}_p(\zeta_{p^\infty})$ is obtained by adjoining the roots of $\psi \circ \psi \circ \cdots \circ \psi(x) = 0$ (when ψ is regarded as an endomorphism of $(\mathfrak{m}_{\overline{\mathbb{Q}}_p}, \cdot)$).

We will see that this can be done in much general context, which is called the **Lubin–Tate theory**.

10.1. **Formal group laws.**

Definition 10.1 (Formal group law)**.** Let A be a commutative ring. Then a formal power series in two variables $F(X,Y) \in A[[X,Y]]$ is called a (commutative) **formal group law** if it behaves like a formula for a multiplication law of an abelian group, whenever the formula makes sense, and if it is not "too far from" the easiest formula $X \cdot Y \mapsto X+Y$. To be more precise, it has to satisfy the following properties.

(1) $F(X,Y) \equiv X+Y \pmod{(X^2, XY, Y^2)}$. In particular, $F(0,0) = 0$, so you can put $F(X,Y)$ as an argument into a formal power series (think about how you would compose two formal power series).

(2) (**associativity**) As elements of $A[[X,Y,Z]]$, $F(X,F(Y,Z)) = F(F(X,Y),Z)$.

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

(4) (**identity**) $F(0,Y) = Y$, $F(X,0) = X$.

(5) (**inverses**) There exists a unique $i(X) \in A[[X]]$ such that $F(X,i(X)) = 0$ (necessarily $i(X) \in XA[[X]]$).

Example 10.2. (1) $F(X,Y) = X+Y$ is a formal group law, called the **additive group law**.

(2) $F(X,Y) = X+Y+XY$ is a formal group law, called the **multiplicative group law**.

Definition 10.3. The setup that we are interested in is when $A = \mathcal{O}_K$ for a local field K (or an algebraic extension of a local field, such as K^{nr}, $\overline{K}$, K^{sep}, etc.). If $\mathfrak{m}_K \subset \mathcal{O}_K$ is the maximal ideal, then for $a, b \in \mathfrak{m}_K$, the infinite sum $F(a,b)$ converges and defines an element of $\mathfrak{m}_K$. Therefore, given a formal group law $F(X,Y)$, it defines the structure of an abelian group over the set $\mathfrak{m}_K$. We denote the abelian group defined by this procedure as $F(\mathfrak{m}_K)$.

Definition 10.4 (Homomorphism between formal group laws)**.** Continuing abstractly, given two formal group laws $F(X,Y), G(X,Y) \in A[[X,Y]]$, one can axiomatize what it means for $f(X) \in A[[X]]$ to define a formula for a homomorphism from the group defined using $F(X,Y)$ to the group defined using $G(X,Y)$. Namely, we call $f(X) \in A[[X]]$ a **homomorphism from F to G** if it satisfies

(1) $f(0) = 0$ (i.e. $f(X) \in XA[[X]]$),

(2) and, as elements of $A[[X,Y]]$, $f(F(X,Y)) = G(f(X), f(Y))$.

If $F = G$, we also call f an **endomorphism of F**. Using this, it also makes sense to define what it means for two formal group laws to be isomorphic.

Let $\mathrm{Hom}(F,G)$ be the set of all homomorphisms from F, G. This set has a natural abelian group structure, defined by $f + g := G(f(X), g(X))$. This is a homomorphism from F to G as

$$G(f(F(X,Y)), g(F(X,Y))) = G(G(f(X), f(Y)), G(g(X), g(Y)))$$
$$= G(G(f(X), g(X)), G(f(Y), g(Y))) = G((f+g)(X), (f+g)(Y)),$$

by the commutativity/associativity of $G(X,Y)$.

Let $\mathrm{End}(F)$ be the set of all endomorphisms of F. In addition to the abelian group structure defined above, it has a structure of a (not necessarily commutative) ring, defined by $f \cdot g := f \circ g$. It is easy to see that $\mathrm{End}(F)$ is closed under composition, and it gives rise to a ring structure as $f \circ (g + h) = f \circ g + f \circ h$ and $(f + g) \circ h = f \circ h + g \circ h$ ($+$ as defined above).

Exercise 10.1. Check this.

Example 10.5. (1) For the additive group law $F(X,Y) = X + Y$, $f(X) = aX$ for any $a \in A$ defines an endomorphism of F;

$$f(F(X,Y)) = a(X+Y) = F(aX, aY) = F(f(X), f(Y)).$$

(2) For the multiplicative group law $F(X,Y) = X + Y + XY$, $f(X) = (X+1)^n - 1$ for any $n \in \mathbb{N}$ defines an endomorphism of F;

$$f(F(X,Y)) = (XY+X+Y+1)^n - 1 = (X+1)^n(Y+1)^n - 1 = (f(X)+1)(f(Y)+1) - 1 = F(f(X), f(Y)).$$

(3) Actually, the example (2) also works for more general exponent $n \in A$, if we define $f(X) = (X+1)^n - 1$ as instead $\sum_{i=1}^{\infty} \binom{n}{i} X^i$, as long as we know $\binom{n}{i} \in A$ for every $i \geq 1$.

Exercise 10.2. If $A = \mathcal{O}_K$ for (an algebraic extension of) a local field K, show that $\binom{a}{k} \in \mathcal{O}_K$ for any $a \in \mathcal{O}_K$ and $k \in \mathbb{N}$.

Therefore, if $A = \mathcal{O}_K$, for the multiplicative group law F, there is an injective **ring homomorphism** $A \to \mathrm{End}(F)$ (Exercise: check that this respects addition and multiplication); there are a lot of endomorphisms of $\mathrm{End}(F)$. Having a group law with a big endomorphism ring is what we are looking for in general; see also the CM theory later in the course.

Now we restrict our attention to the case when $A = \mathcal{O}_K$. Then, there is a surprising **uniqueness** theorem for a formal group law with a particular type of an endomorphism and big endomorphism group.

Theorem 10.6 (Lubin–Tate formal group law)**.** *Let K be a local field, whose residue field is the finite field $\mathbb{F}_q$. Let $\pi \in K$ be a uniformizer. Then, there is a formal group law $F(X, Y) \in \mathcal{O}_K[[X, Y]]$, **unique up to isomorphism**, satisfying the following conditions.*

(1) There is an injective ring homomorphism $[\cdot] : \mathcal{O}_K \to \operatorname{End}(F)$, such that $[a] \equiv aX \pmod{X^2}$ for every $a \in \mathcal{O}_K$. In particular, $\operatorname{End}(F)$ is naturally an $\mathcal{O}_K$-algebra.

(2) The endomorphism $[\pi] \in \operatorname{End}(F)$, a formal power series in one variable, satisfies the congruence condition $[\pi] \equiv X^q \pmod{\pi}$.

*In fact, you can set $[\pi]$ to be any formal power series in $\mathcal{O}_K[[X]]$ satisfying $[\pi] \equiv \pi X \pmod{X^2}$ and $[\pi] \equiv X^q \pmod{\pi}$. Namely, for any $f(X) \in \mathcal{O}_K[[X]]$ satisfying these conditions, there is a **unique** (on the nose, as a formal power series) formal group law $F_f(X, Y) \in \mathcal{O}_K[[X, Y]]$ satisfying (1), (2) (and $F_f \cong F_g$ for any choices of f, g satisfying these conditions). These formal group laws are called the **Lubin–Tate formal group laws**.*

Proof. A key is the following lemma.

Lemma 10.7. *Let $f(X), g(X) \in \mathcal{O}_K[[X]]$ be two formal power series satisfying the above two congruence conditions (i.e. congruent to $\pi X \pmod{X^2}$ and $X^q \pmod{\pi}$). Let $a_1, \cdots, a_n \in \mathcal{O}_K$. Then, there exists a unique formal power series $F(X_1, \cdots, X_n) \in \mathcal{O}_K[[X_1, \cdots, X_n]]$ in n variables, such that $F(X_1, \cdots, X_n) = a_1X_1 + \cdots + a_nX_n + (\text{higher order terms})$, and, as elements of $\mathcal{O}_K[[X_1, \cdots, X_n]]$,*

$$f(F(X_1, \cdots, X_n)) = F(g(X_1), \cdots, g(X_n)).$$

Proof. The idea is simple. Namely, you inductively find the coefficients for F. For example, what are the second-order terms of F? Suppose $F(X_1, \cdots, X_n) = \sum_{i=1}^{n} a_iX_i + \sum_{1\le i\le j\le n} a_{ij}X_iX_j$ for some unknown $a_{ij} \in \mathcal{O}_K$. Let $f(X) = \sum_{i=1}^{\infty} b_iX^i$, and $g(X) = \sum_{i=1}^{\infty} c_iX^i$. Note that $b_1 = c_1 = \pi$. Then, looking at the identity $f(F(X_1, \cdots, X_n)) = F(g(X_1), \cdots, g(X_n))$ modulo third degree terms, we get

$$\pi(\sum_{i=1}^{n} a_iX_i + \sum_{1\le i\le j\le n} a_{ij}X_iX_j) + b_2(\sum_{i=1}^{n} a_iX_i)^2 = \sum_{i=1}^{n} a_i(\pi X_i + c_2X_i^2) + \sum_{1\le i\le j\le n} a_{ij}\pi^2X_iX_j.$$

The first order terms coincide, and comparing the second order terms, the coefficients of X_iX_j on both sides are

$$\pi a_{ij} + 2b_2a_ia_j = a_{ij}\pi^2,$$

if $i < j$, and

$$\pi a_{ii} + b_2a_i^2 = a_ic_2 + a_{ii}\pi^2,$$

if $i = j$. In any case, we are given an explicit formula for each a_{ij}, namely

$$a_{ij} = \begin{cases} \frac{2b_2 a_i a_j}{\pi^2 - \pi} & \text{if } i < j \\ \frac{b_2 a_i^2 - a_i c_2}{\pi^2 - \pi} & \text{if } i = j. \end{cases}$$

So indeed you can find the second order terms explicitly. You may then convince yourself that the formula for the n-th order term has $\pi^n - \pi$ as its denominator, so the formal power series can be found uniquely. □

Using Lemma 10.7, given $f(X) \in \mathcal{O}_K[[X]]$ such that $f(X) \equiv \pi X \pmod{X^2}$ and $f(X) \equiv X^q \pmod{\pi}$, one can first find a unique $F_f(X, Y) \in \mathcal{O}_K[[X, Y]]$ such that $f(F_f(X, Y)) = F_f(f(X), f(Y))$. One can use the same Lemma to show all the axioms for proving that $F_f(X, Y)$ is a formal group law. For example, the commutativity $F_f(X, Y) = F_f(Y, X)$ follows from that both $F_f(X, Y)$ and $F_f(Y, X)$ satisfy the same conditions of Lemma 10.7 so they must be equal by the uniqueness. Similarly, the associativity $F_f(X, F_f(Y, Z)) = F_f(F_f(X, Y), Z)$ follows from Lemma 10.7 applied to $f = g$ and a formal power series in three variables congruent to $X + Y + Z \pmod{\text{higher order terms}}$.

Showing the formal group law axioms is straightforward except the existence of inverse. For that, we realize that we may apply Lemma 10.7 to $f = g$ and a formal power series in one variable congruent to $-X \pmod{X^2}$. Namely, there is $[-1]_f \in \mathcal{O}_K[[X]]$ such that $[-1]_f \equiv -X \pmod{X^2}$ and $f([-1]_f(X)) = [-1]_f(f(X))$. Then, $[-1]_f$ is the desired inverses map, as $F_f(X, [-1]_f(X))$ is the unique formal power series congruent to $0 \pmod{X^2}$ and commute with f, i.e.

$$f(F_f(X, [-1]_f(X))) = F_f(f(X), f([-1]_f(X))) = F_f(f(X), [-1]_f(f(X))),$$

so by uniqueness $F_f(X, [-1]_f(X)) = 0$. This shows that $F_f(X, Y)$ defines a formal group law which has $f(X) \in \mathrm{End}(F)$. Furthermore, the same logic implies that, for each $a \in \mathcal{O}_K$, one can find $[a]_f \in \mathrm{End}(F)$, and in particular $[\pi]_f = f(X)$ by the uniqueness part of Lemma 10.7. Thus, this shows the existence and the uniqueness of F_f.

It remains to show that the isomorphism class of F_f is independent of choice of $f(X)$. Let

$$\mathcal{F}_\pi = \{g(X) \in \mathcal{O}_K[[X]] \ : \ g(X) \equiv \pi X \pmod{X^2}, \ g(X) \equiv X^q \pmod{\pi}\}.$$

We want to show that, for any $f(X), g(X) \in \mathcal{F}_\pi$, $F_f \cong F_g$. By applying Lemma 10.7 to f, g and a formal power series in one variable congruent to $aX \pmod{X^2}$ for $a \in \mathcal{O}_K$, we see that there is a unique $[a]_{f,g}(X) \in \mathcal{O}_K[[X]]$ for each $a \in \mathcal{O}_K$ such that $[a]_{f,g}(X) \equiv aX \pmod{X^2}$ and $f([a]_{f,g}(X)) = [a]_{f,g}(g(X))$. By the similar argument as above, this defines a homomorphism $[a]_{f,g} : F_g \to F_f$. Furthermore, by applying the smae Lemma in a similar way, it is easy to see that $[a + b]_{f,g} = [a]_{f,g} +_{F_f} [b]_{f,g}$ for any $a, b \in \mathcal{O}_K$, where $+_{F_f}$ is the group law for F_f. Also, for yet another $h(X) \in \mathcal{F}_\pi$, the similar reasoning shows $[ab]_{h,f} = [a]_{h,g} \circ [b]_{g,f}$ for any $a, b \in \mathcal{O}_K$. Therefore, we see that, for $a \in \mathcal{O}_K^\times$, $[a]_{f,g}$ and $[a^{-1}]_{g,f}$ are inverses to each other, as $[1]_{f,f}(X) = [1]_{g,g}(X) = X$ by the same uniqueness reasoning. Thus, $F_f \cong F_g$ for any $f, g \in \mathcal{F}_\pi$ as desired. □

We will freely use the notations used in the proof of Theorem 10.6 (e.g. $\mathcal{F}_\pi$, F_f, $[a]_f$).

10.2. **Lubin–Tate extensions.** Now we define the Lubin–Tate extensions just like you define $\mathbb{Q}_p(\zeta_{p^\infty})$ from the multiplicative formal group law over $\mathbb{Q}_p$.

Theorem 10.8 (Lubin–Tate extensions). *Let π be a uniformizer of a local field K. Let $f \in \mathcal{F}_\pi$, and let F_f be the corresponding Lubin–Tate formal group law (note that $[\pi]_f = f$). Let K^{sep} be the separable closure of K, and let $\mathfrak{m}_{K^{\mathrm{sep}}}$ be the maximal ideal of $\mathcal{O}_{K^{\mathrm{sep}}}$.*

(1) For $n \geq 1$,

$$\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}] := \{a \in \mathfrak{m}_{K^{\mathrm{sep}}} \ : \ f^{\circ n}(a) := \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}}(a) = 0\},$$

is an $\mathcal{O}_K$-submodule of $\mathfrak{m}_{K^{\mathrm{sep}}}$, and is isomorphic to $\mathcal{O}_K/(\pi^n)$.

(2) The field $K_{\pi,n} := K(\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}])$, obtained by adjoining the elements of $\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}]$ with K, is an algebraic extension of K, independent of choice of $f \in \mathcal{F}_\pi$.

*(3) The field $K_{\pi,n}$ is a totally ramified finite abelian extension over K, such that the action of $\mathcal{O}_K$ on $\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}]$ gives rise to an isomorphism $(\mathcal{O}_K/(\pi^n))^\times \xrightarrow{\sim} \mathrm{Gal}(K_{\pi,n}/K)$. The infinite extension $K_\pi := \bigcup_{n\geq 1} K_{\pi,n}$ is an abelian extension where $\mathrm{Gal}(K_\pi/K) \cong \mathcal{O}_K^\times$, and is called the **Lubin–Tate extension** (with respect to the choice of a uniformizer π).*

(4) For each $n \geq 1$, $\pi \in N_{K_{\pi,n}/K}(K_{\pi,n}^\times)$.

Proof. (1) First suppose the case $f(X) = \pi X + X^q$, which is certainly an element of $\mathcal{F}_\pi$. Then, $f^{\circ n}(X)$ is a degree q^n polynomial, so the set $\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}]$ is a finite set of order $\leq q^n$ by the fundamental theorem of algebra. We show that $\#\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}] = q^n$ by induction on n. Suppose that $\#\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ(n-1)}] = q^{n-1}$. Then, $\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}]$ consists of elements $a \in \mathfrak{m}_{K^{\mathrm{sep}}}$ such that $a^q + \pi a \in \mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ(n-1)}]$. Therefore, it suffices to show that, for each $b \in \mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ(n-1)}]$, $X^q + \pi X - b = 0$ has q distinct roots. Let $v : K^{\mathrm{sep}} \to \mathbb{Q}$ be the extension of the normalized valuation on K (so that $v(\pi) = 1$). If $v(b) > 1$, then $f(b) = \pi b + b^q$, so we have $v(f(b)) = qv(b), \cdots, v(f^{\circ(n-1)}(b)) = q^{n-1}v(b)$, which implies that $f^{\circ(n-1)}(b) \neq 0$. Therefore, $v(b) \leq 1$, which means that the polynomial $X^q + \pi X - b$ is Eisenstein (over $K(b)$), so it is irreducible, and its q roots are distinct, as desired. Therefore, $\#\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}] = q^n$. It is easy to see that $\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}]$ is stable under the $\mathcal{O}_K$-action, and it is a cyclic module generated by any element in $\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}]\backslash\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ(n-1)}]$, which implies that it is isomorphic to $\mathcal{O}_K/(\pi^n)$ as an $\mathcal{O}_K$-module.

For a general $g \in \mathcal{F}_\pi$, note that $[1]_{g,f} : \mathcal{F}_f \to \mathcal{F}_g$ gives rise to an isomorphism of formal group laws, with the inverse given by $[1]_{f,g} : \mathcal{F}_g \to \mathcal{F}_f$. So $[1]_{g,f} : \mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}] \xrightarrow{\sim} \mathfrak{m}_{K^{\mathrm{sep}}}[g^{\circ n}]$, and it's easy to see that this respects the $\mathcal{O}_K$-action on both sides.

(2) As an element of $\mathfrak{m}_{K^{\mathrm{sep}}}[g^{\circ n}]$ is obtained by applying $[1]_{g,f}$ to an element of $\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}]$, and as $[1]_{g,f} \in \mathcal{O}_K[[X]]$, any element of $\mathfrak{m}_{K^{\mathrm{sep}}}[g^{\circ n}]$ is contained in $K(\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}])$. The reverse logic gives the reverse containment, implying that $K(\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}]) = K(\mathfrak{m}_{K^{\mathrm{sep}}}[g^{\circ n}])$. We know that $K(\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}])$ is an algebraic extension for $f(X) = \pi X + X^q$.

(3) We choose $f(X) = \pi X + X^q$. Let b_1 be a nonzero root of $f(X)$, and let b_n be a root of $f(X) - b_{n-1}$ (inductively defined). Then $b_n \in \mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}] \backslash \mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ (n-1)}]$. On the other hand, as noted above, $f(X) - b_{n-1}$ is Eisenstein over $K(b_{n-1})$, so $K(b_n)/K(b_{n-1})$ is a totally ramified extension of degree q. Similarly, as b_1 is a root of $\pi + X^{q-1}$, which is again Eisenstein, $K(b_1)/K$ is totally ramified of degree $q-1$. Therefore, $K(b_n)/K$ is totally ramified of degree $q^{n-1}(q-1)$. This implies that $[K_{\pi,n} : K] \geq q^{n-1}(q-1)$. On the other hand, $K_{\pi,n}$ is the splitting field of $f^{\circ n}$ (by definition), and $K_{\pi,n}/K$ is Galois ($f^{[n]}$ is easily seen to be separable). As all group laws are defined over K, the action by any element of $\mathrm{Gal}(K_{\pi,n}/K)$ on the roots of $f^{\circ n}$ will preserve the $\mathcal{O}_K$-module structure. Therefore, $\mathrm{Gal}(K_{\pi,n}/K) \subset \mathrm{Aut}_{\mathcal{O}_K}(\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}]) = \mathrm{Aut}_{\mathcal{O}_K}(\mathcal{O}_K/(\pi^n)) = (\mathcal{O}_K/(\pi^n))^\times$, which implies that $[K_{\pi,n} : K] \leq q^{n-1}(q-1)$. Therefore, $K_{\pi,n} = K(b_{n-1})$ is totally ramified of degree $q^{n-1}(q-1)$, and we also obtain the description of the Galois group.

(4) Let $f^{[n]} := \frac{f}{X} \circ \underbrace{f \circ \cdots \circ f}_{n\,-\,1 \text{ times}}$. Then, $f^{[n]}(b_n) = 0$. As $v(b_n) = \frac{1}{q^{n-1}(q-1)}$, the degree of the minimal polynomial of b_n over K is $\geq q^{n-1}(q-1)$, so it must be the case that $f^{[n]}$ is the minimal polynomial of b_n over K. As the constant term of $f^{[n]}$ is π, $N_{K_{\pi,n}/K}(b_n) = (-1)^{(q-1)q^{n-1}}\pi$. This shows that $\pi \in N_{K_{\pi,n}/K}(K_{\pi,n}^\times)$ unless $q = 2^m$ and $n = 1$. In this exceptional case, we rather have shown that $-\pi$ is in the norm group. On the other hand, in this case, $K_{\pi,1}/K$ is totally tamely ramified and $-2 \in 1 + \pi\mathcal{O}_K$, so by Proposition 1.3, $1 - 2 = -1$ is in the norm group $N_{K_{\pi,1}/K}(K_{\pi,1}^\times)$. Therefore, π is still in the norm group. □

Example 10.9. Let $K = \mathbb{Q}_p$ and $\pi = p$. Then, there is a particularly nice choice of $f \in \mathcal{F}_\pi$: $f(X) = (X+1)^p - 1 = pX + \binom{p}{2}X^2 + \cdots + X^p$. Then $f^{\circ n}(X) = (X+1)^{p^n} - 1$, so $\mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}]$ consists of $\zeta_{p^n}^m - 1$ for $1 \leq m \leq p^n$, and $K_{\pi,n} = \mathbb{Q}_p(\zeta_{p^n})$.

Example 10.10. It is important to note that $K_{\pi,n}$ and K_π depend on the choice of π. For example, let $K = \mathbb{Q}_2$. Then, just as computed above, when you choose $\pi = 2$ and $n = 2$, $K_{2,2} = \mathbb{Q}_2(\zeta_4) = \mathbb{Q}_2(\sqrt{-1})$. On the other hand, when you choose $\pi = -2$ and $n = 2$, $K_{-2,2}$ is the splitting field of $g \circ g(X)$, where $g(X) = -2X + X^2$. Note that

$$g(g(X)) = g(X)(g(X) - 2) = X(X-2)(X^2 - 2X - 2) = X(X-2)((X-1)^2 - 3),$$

so $K_{-2,2} = \mathbb{Q}_2(\sqrt{3})$. There are many ways to see that $\mathbb{Q}_2(\sqrt{-1})$ and $\mathbb{Q}_2(\sqrt{3})$ are different; for example, $3 \notin N_{\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2}(\mathbb{Q}_2(\sqrt{-1})^\times)$, because $x^2 + y^2 \neq 3$ for any $x, y \in \mathbb{Z}_2$ by mod 4 considerations, whereas obviously $3 \in N_{\mathbb{Q}_2(\sqrt{3})/\mathbb{Q}_2}(\mathbb{Q}_2(\sqrt{3})^\times)$.

10.3. Wrapping up the proof of the local class field theory.

As promised, we will show that the Lubin–Tate extension K_π has the similar ramification properties as $\mathbb{Q}_p(\zeta_{p^\infty})$.

Theorem 10.11. *The jumps (in upper numbering) of ramification subgroups of* $\mathrm{Gal}(K_\pi/K)$ *happen at all nonnegative integers (except at the* 0*-th ramification subgroup when* $q = 2$*). More precisely, for every* $n \in \mathbb{Z}_{\geq 0}$*,*

$$\left| \frac{\mathrm{Gal}(K_\pi/K)^n}{\mathrm{Gal}(K_\pi/K)^{n+1}} \right| = \begin{cases} q - 1 & \textit{if } n = 0 \\ q & \textit{if } n \geq 1. \end{cases}$$

Proof. The pattern is very similar to the computation of the ramification subgroups in the case of $\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p$. Note that $\mathrm{Gal}(K_{\pi,n}/K) \cong (\mathcal{O}_K/(\pi^n))^\times$, and this has natural subgroups $\mathrm{Gal}(K_{\pi,n}/K_{\pi,m}) = \{x \in (\mathcal{O}_K/(\pi^n))^\times : x \equiv 1 \pmod{\pi^m}\}$. Also, we know that $K_{\pi,n} = K(b_n)$ where $b_n \in \mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}] \backslash \mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ (n-1)}]$ for a choice of $f \in \mathcal{F}_\pi$, and b_n is a uniformizer of $K_{\pi,n}$. We claim that if $\sigma \in \mathrm{Gal}(K_{\pi,n}/K_{\pi,m}) \backslash \mathrm{Gal}(K_{\pi,n}/K_{\pi,m+1})$, then $v(\sigma(b_n) - b_n) = q^m$ (where $v(b_n) = 1$, $K_{\pi,0} = K$). The same kind of computation as in the proof of local Kronecker–Weber theorem will then give you the desired conclusion. The case of $m = 0$ follows from the fact that $K_{\pi,1}$ is the maximal tamely ramified subextension of K_π by the degree reasons ($[K_{\pi,1} : K] = q - 1$ is coprime to p, when $q = p^k$ for some prime number p).

Suppose $\sigma \in \mathrm{Gal}(K_{\pi,n}/K_{\pi,m}) \backslash \mathrm{Gal}(K_{\pi,n}/K_{\pi,m+1})$. By using the identification $\mathrm{Gal}(K_{\pi,n}/K) \cong (\mathcal{O}_K/(\pi^n))^\times$, we see that σ corresponds to $1 + \pi^m u$ for $u \in \mathcal{O}_K^\times$. Then $\sigma(b_n) = [1 + \pi^m u]_f(b_n) = F_f(b_n, [\pi^m u]_f(b_n)) = F_f(b_n, [u]_f(b_{n-m}))$. Note that b_{n-m} is a uniformizer of $K_{\pi,n-m}$, and as $[u]_f$ is invertible, $[u]_f(b_{n-m})$ is also a uniformizer of $K_{\pi,n-m}$. In particular, as $K_{\pi,n-m}/K_{\pi,n}$ is totally ramified, $v([u]_f(b_{n-m})) = [K_{\pi,n-m} : K_{\pi,n}] = q^m$. Now note that $F_f(X, Y) = X + Y + XYG(X, Y)$ for some $G(X, Y) \in \mathcal{O}_K[[X, Y]]$. Therefore,

$$\sigma(b_n) - b_n = F_f(b_n, [u]_f(b_{n-m})) - b_n = [u]_f(b_{n-m}) + \underbrace{b_n[u]_f(b_{n-m})G(b_n, [u]_f(b_{n-m}))}_{\text{divisible by } b_n \cdot [u]_f(b_{n-m})}.$$

Therefore, $v(\sigma(b_n) - b_n) = v([u]_f(b_{n-m})) = q^m$, as desired. □

Theorem 10.12 (Generalized local Kronecker–Weber theorem). *For any uniformizer $\pi \in K$,*

$$K^{\mathrm{ab}} = K^{\mathrm{nr}} K_\pi.$$

Proof. The proof is exactly the same as the proof of the local Kronecker–Weber theorem. □

Remark 10.13. It is interesting to note that K^{ab} and K^{nr} does not depend on any choice but K_π does; we will see in the moment what this corresponds to on the norm group side.

We will now show that the **Explicit class field theory**, i.e. the generalized Kronecker–Weber theorem, helps with clarifying the local class field theory. In fact, our goal is to show that we can explicitly construct the local Artin reciprocity map. The key is the following lemma.

Lemma 10.14 (Lubin–Tate formal group laws become isomorphic over $\widehat{K^{\mathrm{nr}}}$). *Let $\widehat{K^{\mathrm{nr}}}$ be the completion*[8] *of K^{nr}. Then, for any uniformizers $\pi, \pi' \in K$ and $f \in \mathcal{F}_\pi$, $f' \in \mathcal{F}_{\pi'}$, F_f and $F_{f'}$ become isomorphic over $\widehat{K^{\mathrm{nr}}}$. More precisely, the following are true.*

[8] When you take an infinite extension of a local field, it generally loses the completeness property. For example, K^{nr} and $\overline{\mathbb{Q}}_p$ are **not complete**. Taking completion respects the original topology, so the infinite Galois group stays the same, e.g. $\mathrm{Gal}(\widehat{K^{\mathrm{nr}}}/K) \cong \mathrm{Gal}(K^{\mathrm{nr}}/K)$, $\mathrm{Gal}(\widehat{\overline{\mathbb{Q}}_p}/\mathbb{Q}_p) \cong \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. The completion of the algebraic closure of $\mathbb{Q}_p$, $\widehat{\overline{\mathbb{Q}}_p}$, is also called $\mathbb{C}_p$. It is not obvious but indeed true that the complete field $\mathbb{C}_p$ is also algebraically closed ($\mathbb{C}_p$ is the completion of the algebraic closure, so a priori it is not clear whether $\mathbb{C}_p$ is algebraically closed, but in fact it is). In some sense, $\mathbb{C}_p$ is the true p-adic analogue of the field of complex numbers $\mathbb{C}$.

(1) Let $v : \widehat{K^{\mathrm{nr}}} \to \mathbb{Z}$ be continuously extended from $v : K^{\mathrm{nr}} \to \mathbb{Z}$ and let $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}} = \{x \in \widehat{K^{\mathrm{nr}}} : v(x) \geq 0\}$. Then, the map $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}} \to \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}$, $b \mapsto \mathrm{Frob}_q(b) - b$, and the map $\mathcal{O}^{\times}_{\widehat{K^{\mathrm{nr}}}} \to \mathcal{O}^{\times}_{\widehat{K^{\mathrm{nr}}}}$, $b \mapsto \mathrm{Frob}_q(b)/b$, are surjective with the kernels equal to $\mathcal{O}_K$ and $\mathcal{O}_K^{\times}$, respectively.

(2) Let $\pi' = u\pi$ for $u \in \mathcal{O}_K^{\times}$, and let $\varepsilon \in \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}$ be such that $\mathrm{Frob}_q(\varepsilon) = u\varepsilon$ (which exists by (1)). Then, there exists a unique power series $\psi_\varepsilon \in \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$ satisfying the following conditions.

(a) $\psi_\varepsilon(X) \equiv \varepsilon X \pmod{X^2}$.

(b) $\mathrm{Frob}_q(\psi_\varepsilon)(X) = \psi_\varepsilon([u]_f(X))$, *where* Frob_q *acts on* $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$ *coefficientwise.*

(c) $\mathrm{Frob}_q(\psi_\varepsilon)(f(X)) = g(\psi_\varepsilon(X))$.

(d) $\psi_\varepsilon(F_f(X,Y)) = F_g(\psi_\varepsilon(X), \psi_\varepsilon(Y))$.

(e) $\psi_\varepsilon([a]_f(X)) = [a]_g(\psi_\varepsilon(X))$ *for any* $a \in \mathcal{O}_K$.

Thus, F_f and F_g are isomorphic over $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}$ by $\psi_\varepsilon : F_f \rightleftarrows F_g : \psi_{\varepsilon^{-1}}$.

Proof. (1) Let $\mathfrak{m}_{K^{\mathrm{nr}}} \subset \mathcal{O}_{K^{\mathrm{nr}}}$ and $\mathfrak{m}_K \subset \mathcal{O}_K$ be the maximal ideals. To show (1), it suffices to show that, for each $n \geq 1$, the sequences

$$0 \to \mathcal{O}_K/\mathfrak{m}_K^n \to \mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}_{K^{\mathrm{nr}}}^n \xrightarrow{b \mapsto \mathrm{Frob}_q(b) - b} \mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}_{K^{\mathrm{nr}}}^n \to 0,$$

$$1 \to (\mathcal{O}_K/\mathfrak{m}_K^n)^{\times} \to (\mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}_{K^{\mathrm{nr}}}^n)^{\times} \xrightarrow{b \mapsto \mathrm{Frob}_q(b)/b} (\mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}_{K^{\mathrm{nr}}}^n)^{\times} \to 1,$$

are exact, as $\mathcal{O}_{K^{\mathrm{nr}}} = \varprojlim_n \mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}_{K^{\mathrm{nr}}}^n$. We prove these by induction on n. In the case of $n = 1$, the sequences are $0 \to k \to \overline{k} \xrightarrow{b \mapsto b^q - b} \overline{k} \to 0$ and $1 \to k^{\times} \to \overline{k}^{\times} \xrightarrow{b \mapsto b^{q-1}} \overline{k}^{\times} \to 1$, where k is the residue field of K (=residue field of K^{nr}), and they are obviously exact. Assuming the sequences are exact for $n-1$, we consider the diagrams

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}_{K^{\mathrm{nr}}} \arrow[r] \arrow[d, "b \mapsto \mathrm{Frob}_q(b) - b"] & \mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}_{K^{\mathrm{nr}}}^n \arrow[r] \arrow[d, "b \mapsto \mathrm{Frob}_q(b) - b"] & \mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}_{K^{\mathrm{nr}}}^{n-1} \arrow[r] \arrow[d, "b \mapsto \mathrm{Frob}_q(b) - b"] & 0 \\
0 \arrow[r] & \mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}_{K^{\mathrm{nr}}} \arrow[r] & \mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}_{K^{\mathrm{nr}}}^n \arrow[r] & \mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}_{K^{\mathrm{nr}}}^{n-1} \arrow[r] & 0,
\end{tikzcd}$$

$$\begin{tikzcd}
1 \arrow[r] & (1 + \mathfrak{m}_{K^{\mathrm{nr}}}^{n-1})/\mathfrak{m}_{K^{\mathrm{nr}}}^n \arrow[r] \arrow[d] & (\mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}_{K^{\mathrm{nr}}}^n)^{\times} \arrow[r] \arrow[d, "b \mapsto \mathrm{Frob}_q(b)/b"] & (\mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}_{K^{\mathrm{nr}}}^{n-1})^{\times} \arrow[r] \arrow[d, "b \mapsto \mathrm{Frob}_q(b)/b"] & 1 \\
1 \arrow[r] & (1 + \mathfrak{m}_{K^{\mathrm{nr}}}^{n-1})/\mathfrak{m}_{K^{\mathrm{nr}}}^n \arrow[r] & (\mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}_{K^{\mathrm{nr}}}^n)^{\times} \arrow[r] & (\mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}_{K^{\mathrm{nr}}}^{n-1})^{\times} \arrow[r] & 1.
\end{tikzcd}$$

What is the left vertical map of the second diagram? It sends $1 + x$, $x \in \mathfrak{m}_{K^{\mathrm{nr}}}^{n-1}$, to $\frac{\mathrm{Frob}_q(1+x)}{1+x} = \frac{1+\mathrm{Frob}_q(x)}{1+x}$. As $(1+x)(1-x) = 1 - x^2 \equiv 1 \pmod{\mathfrak{m}_{K^{\mathrm{nr}}}}$, the left vertical map sends $1 + x$ to $(1 + \mathrm{Frob}_q(x))(1 - x) = 1 + (\mathrm{Frob}_q(x) - x) \pmod{\mathfrak{m}_{K^{\mathrm{nr}}}^n}$. Therefore, by the snake lemma, it follows that $\mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}_{K^{\mathrm{nr}}}^n \xrightarrow{b \mapsto \mathrm{Frob}_q(b) - b} \mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}_{K^{\mathrm{nr}}}^n$ and

$(\mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}^n_{K^{\mathrm{nr}}})^\times \xrightarrow{b\mapsto \mathrm{Frob}_q(b)/b} (\mathcal{O}_{K^{\mathrm{nr}}}/\mathfrak{m}^n_{K^{\mathrm{nr}}})^\times$ are surjective, and the kernels are of the order q^n and $q(q^{n-1}-q^{n-2}) = q^n - q^{n-1}$, respectively. By comparing orders, we see that the exact sequences are exact for n, as desired.

(2) We will inductively find the coefficients for $\psi_\varepsilon(X) = \sum_{n=1}^\infty a_n X^n$; we already have $a_1 = \varepsilon$. Let $[u]_f(X) = \sum_{n=1}^\infty b_n X^n$, where $b_1 = u$. Suppose that we know $a_1, \cdots, a_n$. Then, using (b), comparing the coefficients for X^{n+1}, we have

$$\mathrm{Frob}_q(a_{n+1}) = a_{n+1}u + (\text{an expression using } a_1, \cdots, a_n \text{ and } b_i\text{'s}).$$

Then, $\mathrm{Frob}_q(a_{n+1}\varepsilon^{-1}) - a_{n+1}\varepsilon^{-1} = (\text{an expression using } a_1, \cdots, a_n \text{ and } b_i\text{'s})$, so definitely you can choose a_{n+1} in the way that (a), (b) are satisfied.

Let ψ be any formal power series that satisfies (a), (b). Let $h(X) = \mathrm{Frob}_q(\psi)(f(\psi^{-1}(X)))$, where $\psi^{-1}(X)$ is the inverse of $\psi(X)$ (i.e. $\psi(\psi^{-1}(X)) = \psi^{-1}(\psi(X)) = X$), which is possible as $\psi(X) \equiv \varepsilon X \pmod{X^2}$. Note that $h(X) = \psi([u]_f(f(\psi^{-1}(X)))) = \psi(f([u]_f(\psi^{-1}(X))))$. As $f(X)$ and $[u]_f(X)$ have coefficients in $\mathcal{O}_K$, they are fixed by the action of Frob_q. Thus,

$$\mathrm{Frob}_q(h)(X) = \mathrm{Frob}_q(\psi)(f([u]_f(\mathrm{Frob}_q(\psi^{-1})(X)))).$$

Note that $\mathrm{Frob}_q(\psi)(X) = \psi([u]_f(X))$ implies that $[u]_f(\mathrm{Frob}_q(\psi^{-1})(X)) = \psi^{-1}(X)$, so

$$\mathrm{Frob}_q(h)(X) = \mathrm{Frob}_q(\psi)(f(\psi^{-1}(X))) = h(X).$$

This implies that $h(X) \in \mathcal{O}_K[[X]]$. Note that $h(X) \equiv \mathrm{Frob}_q(\varepsilon)\pi\varepsilon^{-1}X = \pi' X \pmod{X^2}$ and $h(X) \equiv \mathrm{Frob}_q(\psi)(\psi^{-1}(X)^q) \equiv \mathrm{Frob}_q(\psi)(\psi^{-1}(X^q)) \equiv X^q \pmod{\mathfrak{m}_K}$, so $h \in \mathcal{F}_{\pi'}$. Then, it is easy to see that $\psi_\varepsilon(X) := [1]_{g,h}(\psi(X))$ satisfies (a), (b), (c). Using Lemma 10.7, one can also easily show that $\psi_\varepsilon(F_f(\psi_\varepsilon^{-1}(X), \psi_\varepsilon^{-1}(Y)))$ satisfies the same characterizing properties as $F_f(X,Y)$, and that $\psi_\varepsilon([a]_f(\psi_\varepsilon^{-1}(X)))$ satisfies the same characterizing properties as $[a]_g$, so ψ_ε satisfies (4) and (5).

□

Theorem 10.15 (Explicit local class field theory via Lubin–Tate extensions)**.** *Let K be a local field, and let $\pi \in K$ be a uniformizer. Then, the local Artin map $\mathrm{Art}_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is the same as the map*

$$f_\pi : K^\times = \pi^{\mathbb{Z}} \times \mathcal{O}_K^\times \to \mathrm{Gal}(K^{\mathrm{nr}}/K) \times \mathrm{Gal}(K_\pi/K) = \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

where the two maps $\pi^{\mathbb{Z}} \to \mathrm{Gal}(K^{\mathrm{nr}}/K) \xrightarrow{\sim} \mathrm{Gal}(\overline{k}/k)$ (k is the residue field of K, $\#k = q$) and $\mathcal{O}_K^\times \xrightarrow{\sim} \mathrm{Gal}(K_\pi/K)$ are the maps $\pi \mapsto \mathrm{Frob}_q$ (i.e. $\mathrm{Frob}_q \in \mathrm{Gal}(\overline{k}/k)$ sending $x \mapsto x^q$) and the ***inverse of the** $\mathcal{O}_K$-action map, i.e. $u \mapsto [u^{-1}]_f$ (for any $f \in \mathcal{F}_\pi$), respectively. In particular, f_π does not depend on the choice of π.*

Proof. By Theorem 10.8(4), we know that $\mathrm{Art}_K(\pi)$ is trivial when sent to $\mathrm{Gal}(K^{\mathrm{ab}}/K) \twoheadrightarrow \mathrm{Gal}(K_\pi/K)$, and is $\mathrm{Frob}_q \in \mathrm{Gal}(K^{\mathrm{nr}}/K)$ when sent to $\mathrm{Gal}(K^{\mathrm{nr}}/K) \twoheadrightarrow \mathrm{Gal}(K^{\mathrm{nr}}/K)$. Therefore, $\mathrm{Art}_K(\pi) = f_\pi(\pi)$.

Let $\pi' \in K$ be another uniformizer. We want to show that $\mathrm{Art}_K(\pi') = f_\pi(\pi')$. As we know that they are both sent to $\mathrm{Frob}_q \in \mathrm{Gal}(K^{\mathrm{nr}}/K)$ via $\mathrm{Gal}(K^{\mathrm{ab}}/K) \twoheadrightarrow \mathrm{Gal}(K^{\mathrm{nr}}/K)$, we only need to show that $f_\pi(\pi')$ is sent to 1 via $\mathrm{Gal}(K^{\mathrm{ab}}/K) \twoheadrightarrow \mathrm{Gal}(K_{\pi'}/K)$. Let $g \in \mathcal{F}_{\pi'}$ and $\psi_\varepsilon : F_f \to F_g$ be an isomorphism over $\widehat{K^{\mathrm{nr}}}$ constructed in Lemma 10.14(2). It suffices to show that $f_\pi(\pi')(\psi_\varepsilon(b)) = \psi_\varepsilon(b)$ for every $b \in \mathfrak{m}_{K^{\mathrm{sep}}}[f^{\circ n}]$, $n \geq 1$. Note that $f_\pi(\pi') = f_\pi(u) \circ f_\pi(\pi)$. As $f_\pi(\pi)$ acts trivially on $b \in K_\pi$ and acts as Frob_q on K^{nr}, $f_\pi(\pi)(\psi_\varepsilon(b)) = \mathrm{Frob}_q(\psi_\varepsilon)(b)$, as ψ_ε has coefficients in $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}$. Therefore, $f_\pi(\pi')(\psi_\varepsilon(b)) = f_\pi(u)(\mathrm{Frob}_q(\psi_\varepsilon)(b))$. As f_ψ acts trivially on K^{nr} and acts as $[u^{-1}]_f$ on $b \in K_\pi$, we have

$$f_\pi(\pi')(\psi_\varepsilon(b)) = f_\pi(u)(\mathrm{Frob}_q(\psi_\varepsilon)(b)) = \mathrm{Frob}_q(\psi_\varepsilon)([u^{-1}]_f(b)) = \psi_\varepsilon([u]_f([u^{-1}]_f(X))) = \psi_\varepsilon(X),$$

as desired. This implies that $\mathrm{Art}_K(\pi') = f_\pi(\pi')$ for any uniformizer $\pi' \in K$. As any element of $K^\times$ is of the form $\pi'\pi^m$ for some uniformizer π' and $m \in \mathbb{Z}$, this implies that $\mathrm{Art}_K = f_\pi$. □

Remark 10.16. We see that the choice of π is reflected on the norm group side as the dependency of the splitting $K^\times = \pi^{\mathbb{Z}} \times \mathcal{O}_K^\times$ on the choice of π. Namely, there is a short exact sequence $1 \to \mathcal{O}_K^\times \to K^\times \xrightarrow{v} \mathbb{Z} \to 0$ that does not depend on any choice, but this sequence splits, and the choice of a splitting is the same as the choice of a uniformizer π, and ultimately the choice of $K^\times = \pi^{\mathbb{Z}} \times \mathcal{O}_K^\times$.

The construction of the local Artin reciprocity gives you a very clean description of the norm groups of the Lubin–Tate extensions.

Corollary 10.17. *Let K be a local field, and $\pi \in K$ be a uniformizer. Then $N_{K_{\pi,n}/K}(K_{\pi,n}^\times) = \pi^{\mathbb{Z}} \times (1 + \pi^n\mathcal{O}_K)$. In particular, for uniformizers $\pi, \pi' \in K$, $K_\pi = K_{\pi'}$ implies that $\pi = \pi'$.*

Proof. The former statement is immediate from the construction of the local Artin reciprocity. The latter follows from that $\pi^{\mathbb{Z}} = \bigcup_{n\geq 1} N_{K_{\pi,n}/K}(K_{\pi,n}^\times) = \bigcup_{n\geq 1} N_{K_{\pi',n}/K}(K_{\pi',n}^\times) = \pi'^{\mathbb{Z}}$. □

Now we can finish all the unproved claims about the local class field theory.

Proof of Theorem 2.7, the Local Existence Theorem. The Local Existence Theorem is equivalent to saying that Art_K restricted to $\mathcal{O}_K^\times$ is sent isomorphically onto the inertia $\mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{nr}}) \subset \mathrm{Gal}(K^{\mathrm{ab}}/K)$, which is obvious from Theorem 10.15. □

Proof of Theorem 2.9, on the relation between ramification and local Artin map. This follows from the calculation of the upper numbering ramification subgroups of K_π (Theorem 10.11) and the fact that ramification subgroups only care about inertia subgroup (so indifferent to unramified extensions). □

11. Analytic preliminaries for the proof of the global class field theory

The proof of the class formation axioms for global fields (let's focus on number fields) is much more convoluted. In fact, the two class formation Axioms will be proved simultaneously by much more indirect methods. A rough outline is as follows.

Step 1. For L/K a finite **cyclic** Galois extension of number fields, we will show that the Herbrand quotient $h(C_L) = [L : K]$. This implies the **First Inequality** of global class field theory,

$$\#H^2(\mathrm{Gal}(L/K), C_L) \geq [L : K].$$

Step 2. Using the analytic theory of L-functions, we will show that, for a finite Galois extension L/K of number fields, the **Second Inequality** of global class field theory,

$$\#H^0_T(\mathrm{Gal}(L/K), C_L) \leq [L : K].$$

This implies that $H^1(\mathrm{Gal}(L/K), C_L) = 0$ and $\#H^2(\mathrm{Gal}(L/K), C_L) = [L : K]$ for finite **cyclic** extensions L/K of number fields.

Step 3. One shows that $H^1(\mathrm{Gal}(L/K), C_L) = 0$ for just finite cyclic extensions L/K implies the full **Axiom 1** (i.e. the same holds for any finite Galois extensions).

Step 4. Using the Brauer group of number fields, we will show the full **Axiom 2**. This will prove the reciprocity law and the local-global compatibility.

Step 5. As usual, one proves ε more to prove the existence theorem.

The **Second Inequality** is arguably the most serious input in the proof of global class field theory. Although there is a purely algebraic proof, we will deduce this in a more classical way by using the analytic theory of L-functions.

11.1. L-functions.

Definition 11.1 (Multiplicative characters of local fields)**.** Let F be a local field. A **(multiplicative) character** of $F^\times$ is a continuous homomorphism $\psi : F^\times \to \mathbb{C}^\times$. It is called **unitary** if the image of ψ lands in $S^1 \subset \mathbb{C}^\times$ (the subgroup of complex numbers of norm 1). It is called **unramified** if ψ factors through the normalized absolute value (see Definition 6.4) $|\cdot| : F^\times \to |F^\times|$. Namely, if F is nonarchimedean, ψ is unramified if $\psi(\mathcal{O}_F^\times) = 1$; if $F = \mathbb{R}$, ψ is unramified if $\psi(\pm 1) = 1$; if $F = \mathbb{C}$, ψ is unramified if $\psi(S^1) = 1$.

The following are easy.

Lemma 11.2. *Let F be a local field.*

*(1) Every character χ of $F^\times$ is of the form $\chi = \eta|\cdot|^t$ for some unitary character η of $F^\times$ and $t \in \mathbb{C}$. The real part $\sigma := \mathrm{Re}(t)$ is uniquely determined by χ and is called the **exponent** of χ.*

(2) Every character of $\mathbb{R}^\times$ is equal to $\chi_{a,t} : \mathbb{R}^\times \to \mathbb{C}^\times$ defined by $\chi_{a,t}(x) = x^{-a}|x|^t$ for a unique pair of $a \in \{0, 1\}$ and $t \in \mathbb{C}$.

(3) Every character of $\mathbb{C}^\times$ is equal to $\chi_{a,b,t} : \mathbb{C}^\times \to \mathbb{C}^\times$ defined by $\chi_{a,b,t}(z) = z^{-a}\overline{z}^{-b}|z|^t$ for a unique triple of $a, b \in \mathbb{Z}$ with $\min(a, b) = 0$ and $t \in \mathbb{C}$.

Proof. Easy; Exercise. □

Definition 11.3 (Hecke characters)**.** Let K be a global field. A **Hecke character** (also called an **idele class character**) is a continuous homomorphism $\chi : C_K \to \mathbb{C}^\times$. Equivalently, a Hecke character is a continuous homomorphism $\chi : I_K \to \mathbb{C}^\times$ that is trivial on $K^\times \subset I_K$. For a place v of K, let $\chi_v = \chi|_{K_v^\times}$, which gives a multiplicative character $\chi_v : K_v^\times \to \mathbb{C}^\times$ of $K_v^\times$.

A Hecke character $\chi : C_K \to \mathbb{C}^\times$ is **unitary** if its image is in $S^1 \subset \mathbb{C}^\times$.

A **Dirichlet character** is a Hecke character of finite order, i.e. when the image is a finite group. By Proposition 7.11(3), any Dirichlet character χ must factor through $C_K \to \mathrm{Cl}^{\mathfrak{m}}(K)$ for some modulus $\mathfrak{m}$. The largest such modulus $\mathfrak{m}$ is called the **conductor** of χ, and denoted $\mathfrak{f}_\chi$.

Lemma 11.4. *Let K be a global field. Then, any Hecke character χ is of the form $\eta|\cdot|^t$ for some unitary Hecke character η and $t \in \mathbb{C}$ (for the definition of $|\cdot| : C_K \to \mathbb{R}_{>0}$, see the proof of Proposition 6.14). The real part $\sigma := \mathrm{Re}(t)$ is uniquely determined by χ and is called the exponent of χ.*

Proof. We have $\chi = \frac{\chi}{|\chi|}|\chi|$. □

Example 11.5. In analytic number theory, one often calls a character of $(\mathbb{Z}/m\mathbb{Z})^\times$ a Dirichlet character mod m. This fits into the general definition of Dirichlet character defined here, for $K = \mathbb{Q}$, as we already saw that $C_\mathbb{Q} = \widehat{\mathbb{Z}}^\times \times \mathbb{R}_{>0}$. Therefore, a character $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ can be regarded as a finite order character of $C_\mathbb{Q}$ by $C_\mathbb{Q} = \widehat{\mathbb{Z}}^\times \times \mathbb{R}_{>0} \twoheadrightarrow \widehat{\mathbb{Z}}^\times \twoheadrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$. One may see that, if you started with a **primitive Dirichlet character** (i.e. a character of $(\mathbb{Z}/m\mathbb{Z})^\times$ that does not come from a character of $(\mathbb{Z}/n\mathbb{Z})^\times$ for some smaller $n|m$), then the corresponding finite order Hecke character has the conductor $m\infty$.

An L-**function** of something is a holomorphic function that contains a lot of information about that thing. The definition of the L-function of a character is as follows.

Definition 11.6 (Local L-factor)**.** Let F be a local field, and let χ be a character of $F^\times$. Then, the local L-factor $L(s,\chi)$ is a holomorphic function in variable s, defined as

$$L(s,\chi) := \begin{cases} \frac{1}{1-\chi(\pi)q^{-s}} & \text{if } F \text{ is nonarchimedean (uniformizer } \pi\text{, residue field } \mathbb{F}_q\text{), } \chi \text{ is unramified} \\ 1 & \text{if } F \text{ is nonarchimedean, } \chi \text{ is ramified} \\ \pi^{-\frac{t+s}{2}}\Gamma\left(\frac{t+s}{2}\right) & \text{if } F = \mathbb{R}, \chi = \chi_{a,t} \\ 2(2\pi)^{-(t+s)}\Gamma(t+s) & \text{if } F = \mathbb{C}, \chi = \chi_{a,b,t}. \end{cases}$$

Here, $\Gamma(s)$ is the Gamma function, $\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}dt$ (or rather its analytic continuation).

This definition is somewhat mysterious, and will be justified a few lectures later. It is easy to observe that $L(s,\chi|\cdot|^t) = L(s+t,\chi)$.

Theorem 11.7 (Analytic continuation and functional equation of Hecke L-functions)**.** *Let K be a global field, and let χ be a Hecke character of K of exponent σ.*

*(1) (**Euler product**[9]) Then, the infinite product*

$$L(s, \chi) := \prod_{v \text{ place of } K} L(s, \chi_v),$$

converges and defines a holomorphic function on $\{s \in \mathbb{C} \ : \ \mathrm{Re}(s) > 1 - \sigma\}$.

*(2) (**Analytic continuation**) This admits an analytic continuation as a meromorphic function (called the **Hecke L-function** of χ) defined on the whole complex plane $s \in \mathbb{C}$. In fact, this analytic continuation is entire unless $\chi = |\cdot|^t$, in which case simple poles appear at $s = -t$ and $s = 1 - t$.*

*We also define $L_f(s, \chi) := \prod_{v \text{ finite place of } K} L(s, \chi_v)$ and call it (or rather its analytic continuation) the **finite part of the Hecke L-function** of χ.*

*(3) (**Functional equation**) Let χ^{-1} be the inverse of χ (i.e. $\chi^{-1}(x) = \frac{1}{\chi(x)}$). Then,*

$$\epsilon(s, \chi) := \frac{L(s, \chi)}{L(1 - s, \chi^{-1})},$$

*is a nowhere vanishing entire function on $s \in \mathbb{C}$, called the **global ϵ-factor**. In fact, the global ϵ-factor is given by an explicit infinite product (Euler product) of local terms, called the **local ϵ-factors**:*

$$\epsilon(s, \chi) = \prod_{v \text{ place of } K} \epsilon(s, \chi_v).$$

*In general, $\epsilon(s, \chi_v) = ae^{bs}$ for some $a, b \in \mathbb{C}$. Also, if v is a finite place at which χ_v is **unramified**, $\epsilon(s, \chi_v) = 1$ (so the above infinite product is actually a finite product).*

Remark 11.8 (Dirichlet L-functions)**.** Let χ be a Dirichlet character. In particular, the exponent $\sigma = 0$, and χ can be regarded as a character of a ray class group $\mathrm{Cl}^{\mathfrak{m}}(K)$ for some modulus $\mathfrak{m}$. By absolute convergence, if $\mathrm{Re}(s) > 1$, one can alternatively write $L_f(s, \chi)$ as

$$L_f(s, \chi) = \prod_{\mathfrak{p} \subset \mathcal{O}_K \text{ prime ideal}} (1 + \chi(\mathfrak{p})N(\mathfrak{p})^{-s} + \chi(\mathfrak{p})^2 N(\mathfrak{p})^{-2s} + \cdots) = \prod_{\mathfrak{a} \subset \mathcal{O}_K \text{ ideal}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s},$$

which is perhaps a more familiar definition of a **Dirichlet L-function**. Here $N(\mathfrak{a}) := \#\mathcal{O}_K/\mathfrak{a}$ (see [ANT]).

This is a much much more general version of the analytic continuation and the functional equation of the Riemann zeta function. One can of course give a similar proof as the Riemann zeta function case, but this can all simultaneously be proved very cleanly using Fourier analysis over the adeles (?!) and is generally called the **Tate's thesis**. We will prove Theorem 11.7 following the Tate's thesis later in the course. It does not use class field theory, so we will just assume Theorem 11.7 at the moment (alternatively, we only need the analytic inputs for Dirichlet L-functions for the proof of **Second Inequality**, and you can definitely elementarily prove the analytic continuation and functional equation for Dirichlet L-functions).

[9] An Euler product is a general term that refers to an infinite product running over each place of a global field.

Example 11.9. Let $K = \mathbb{Q}$ and χ be trivial (i.e. $\chi(x) = 1$ for all $x \in C_{\mathbb{Q}}$). Then, the Euler product in Theorem 11.7 is

$$L_f(s,\chi) = \prod_{p \text{ prime number}} \frac{1}{1-p^{-s}}, \quad L(s,\chi) = L_f(s,\chi)\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right).$$

Thus, $L_f(s,\chi)$ is the Riemann zeta function $\zeta(s)$ and $L(s,\chi)$ is the completed Riemann zeta function $\xi(s)$. The functional equation for the Riemann zeta function is $\xi(s) = \xi(1-s)$ (so the global ϵ-factor is just 1).

11.2. **Analytic inputs: nonvanishing of $L_f(1,\chi)$ and analytic class number formula.** We record the two main sources of the "analytic input." The first is

Theorem 11.10 (Nonvanishing of $L_f(1,\chi)$)**.** *If χ is a nontrivial Dirichlet character of a global field K, then $L_f(1,\chi) \neq 0$.*

We will not prove this here. This can be proved purely analytically right away (e.g. see [CF, VIII.2]). Alternatively, one can deduce this from a softer fact after showing (*) for the global existence theorem (!). For example, after showing (*), one can show Theorem 11.10 (when K is a number field) from the analytic class number formula, which is the second "analytic input".

Definition 11.11 (Dedekind zeta function)**.** Let K be a number field. The **Dedekind zeta function** is

$$\zeta_K(s) := \sum_{\mathfrak{a} \subset \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s},$$

a priori defined only for $\mathrm{Re}(s) > 1$.

Theorem 11.12 (Analytic class number formula)**.** *Let K be a number field. Then, the Dedekind zeta function $\zeta_K(s)$ has an analytic continuation to a meromorphic function on the whole complex plane $s \in \mathbb{C}$, with only simple pole at $s = 1$. Furthermore, the residue at $s = 1$ is given by*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^r(2\pi)^s R_K h_K}{\#\mu_K\sqrt{|\operatorname{disc}(K)|}},$$

where:

- *r is the number of real embeddings of K, enumerated as $\sigma_1, \cdots, \sigma_r$,*
- *s is the number of complex-conjugate pairs of complex embeddings of K, enumerated as $\{\sigma_{r+1}, \overline{\sigma_{r+1}}\}, \cdots, \{\sigma_{r+s}, \overline{\sigma_{r+s}}\}$,*
- *$h_K = \#\operatorname{Cl}(K)$ is the class number of K,*
- *μ_K is the (necessarily finite) group of roots of unity in K,*

- *R_K is the* ***regulator*** *of K, defined as*

$$R_K = \left|\det\begin{pmatrix} \log|\sigma_1(u_1)| & \log|\sigma_1(u_2)| & \cdots & \log|\sigma_1(u_{r+s-1})| \\ \cdots & \cdots & \cdots & \cdots \\ \log|\sigma_r(u_1)| & \log|\sigma_r(u_2)| & \cdots & \log|\sigma_r(u_{r+s-1})| \\ 2\log|\sigma_{r+1}(u_1)| & 2\log|\sigma_{r+1}(u_2)| & \cdots & 2\log|\sigma_{r+1}(u_{r+s-1})| \\ \cdots & \cdots & \cdots & \cdots \\ 2\log|\sigma_{r+s-1}(u_1)| & 2\log|\sigma_{r+s-1}(u_2)| & \cdots & 2\log|\sigma_{r+s-1}(u_{r+s-1})| \end{pmatrix}\right|,$$

  where $u_1, \cdots, u_{r+s-1} \in \mathcal{O}_K^\times$ is a ***fundamental system of units*** *of K, i.e. $\mathcal{O}_K^\times = \mu_K \times u_1^{\mathbb{Z}} \times \cdots \times u_{r+s-1}^{\mathbb{Z}}$ (this is the* ***Dirichlet's unit theorem****).*

Namely, you can express a certain product of $L_f(s,\chi)$'s using the Dedekind zeta function $\zeta_L(s)$ for an abelian extension L of K, and (*) will guarantee that every $L_f(s,\chi)$ appears in some such expression. The fact that there is a simple pole at $s = 1$ implies that $L_f(s,\chi)$ for $\chi \neq 1$ does not vanish at $s = 1$. We won't also prove this. The proof of the analytic class number formula is certainly "less heavy lifting" than the proof of Theorem 11.10.

11.3. **Primes in arithmetic progressions.** It is a classical topic taught in elementary analytic number theory that the non-vanishing of $L_f(1,\chi)$ for $\chi \neq 1$ implies the **Dirichlet's theorem on primes in arithmetic progressions**, namely that there are infinitely many prime numbers congruent to $a \pmod n$ for any $(a,n) = 1$ (see [ANT, Exercise 18.2]). In fact, the proof says that the prime numbers are equally distributed among each congruence class $a (\operatorname{mod} n)$ with $(a,n) = 1$ in an appropriate sense. One can deduce a similar conclusion in the current context.

Definition 11.13 (Dirichlet density)**.** Let S be a set of prime ideals of K (i.e. finite primes). If there exists $\delta \geq 0$ such that $\left(\sum_{\mathfrak{p}\in S} \frac{1}{N(\mathfrak{p})^s}\right) - \delta \log \frac{1}{s-1}$ is bounded as $s \in \mathbb{R}$ approaches $s = 1$ from the right, then we say that $\delta := \delta(S)$ and S has **Dirichlet density** δ.

Lemma 11.14. *The set of all prime ideals of K has Dirichlet density* 1.

Proof. Note that, for $\operatorname{Re}(s) > 1$ (everything is absolutely convergent so we can freely change the order of summation),

$$\log \zeta_K(s) = -\sum_{\mathfrak{p}\text{ prime ideal}} \log(1 - N(\mathfrak{p})^{-s}) = \sum_{m\geq 1}\sum_{\mathfrak{p}\text{ prime ideal}} (-1)^m \frac{N(\mathfrak{p})^{-ms}}{m}.$$

It is easy to see that $\sum_{m\geq 2}\sum_{\mathfrak{p}\text{ prime ideal}}(-1)^m\frac{N(\mathfrak{p})^{-ms}}{m}$ is bounded above by an absolute constant. Namely, this is obviously bounded by $\sum_{m\geq 2}\sum_{\mathfrak{p}\text{ prime ideal}} N(\mathfrak{p})^{-m} = \sum_{\mathfrak{p}\text{ prime ideal}} \frac{1}{N(\mathfrak{p})^2}\cdot\frac{N(\mathfrak{p})}{N(\mathfrak{p})-1} \leq 2\sum_{\mathfrak{p}\text{ prime ideal}}\frac{1}{N(\mathfrak{p})^2}$, and for each rational prime $p \in \mathbb{Z}$, there are at most $[K:\mathbb{Q}]$ many prime ideals of K dividing p, so this is bounded by $2[K:\mathbb{Q}]\sum_{p\text{ prime number}}\frac{1}{p^2} < 2[K:\mathbb{Q}]\sum_{n\geq 1}\frac{1}{n^2} = \frac{\pi^2[K:\mathbb{Q}]}{3}$. So, $\log\zeta_K(s)$ and $\sum_{\mathfrak{p}\text{ prime ideal}}\frac{1}{N(\mathfrak{p})^s}$ is off by at most this constant. By the analytic class number formula (Theorem 11.12), $\zeta_K(s)$ has a simple pole at $s = 1$, so this implies that $\log\zeta_K(s) - \log\frac{1}{s-1}$ is bounded as $s \in \mathbb{R}$ approaches $s = 1$ from the right. This shows that the set of all prime ideals of K has Dirichlet density 1. □

The following is the generalization of the Dirichlet's theorem on primes in arithmetic progressions.

Theorem 11.15 (Prime ideals in arithmetic progressions)**.** *Let K be a global field and $\mathfrak{m}$ be a modulus of K. Let $a \in \mathrm{Cl}^{\mathfrak{m}}(K)$ be an element. Then, the set of prime ideals $\mathfrak{p}$ of K such that $\mathfrak{p}$ does not divide $\mathfrak{m}$ and $[\mathfrak{p}] = a$ in $\mathrm{Cl}^{\mathfrak{m}}(K)$ has Dirichlet density $\frac{1}{\#\,\mathrm{Cl}^{\mathfrak{m}}(K)}$.*

Proof. The same argument as in Lemma 11.14 shows that, for any Dirichlet character χ of conductor $\mathfrak{m}$,

$$\log L_f(s,\chi) - \sum_{\mathfrak{p}\text{ prime ideal not dividing }\mathfrak{m}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s},$$

is bounded as $s \in \mathbb{R}$ approaches $s = 1$ from the right. We now use the elementary identity that

$$\sum_{\chi\text{ character of }\mathrm{Cl}^{\mathfrak{m}}(K)} \chi(\mathfrak{p})\chi^{-1}(a) = \begin{cases} \#\,\mathrm{Cl}^{\mathfrak{m}}(K) & \text{if } [\mathfrak{p}] = a \\ 0 & \text{if } [\mathfrak{p}] \neq a. \end{cases}$$

Thus,

$$\frac{1}{\#\,\mathrm{Cl}^{\mathfrak{m}}(K)} \left(\sum_{\chi\text{ Dirichlet character of modulus dividing }\mathfrak{m}} \chi^{-1}(a) \log L_f(s,\chi) \right) - \sum_{\mathfrak{p}\text{ prime ideal not dividing }\mathfrak{m},\ [\mathfrak{p}] = a\text{ in }\mathrm{Cl}^{\mathfrak{m}}(K)} \frac{1}{N(\mathfrak{p})^s},$$

is bounded as $s \in \mathbb{R}$ approaches $s = 1$ from the right. By the nonvanishing of $L_f(1,\chi)$ for $\chi \neq 1$ and Lemma 11.14, we see that

$$\left(\sum_{\chi\text{ Dirichlet character of modulus dividing }\mathfrak{m}} \chi^{-1}(a) \log L_f(s,\chi) \right) - \log \frac{1}{s-1},$$

is bounded as $s \in \mathbb{R}$ approaches $s = 1$ from the right. This gives the desired conclusion. □

Example 11.16. Applying this to $K = \mathbb{Q}$ and $\mathfrak{m} = n\infty$, we recover the density statement for prime numbers $\equiv a (\operatorname{mod} n)$; recall that $\mathrm{Cl}^{\mathfrak{m}}(\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$, and a prime number p gives rise to a class $p \in (\mathbb{Z}/n\mathbb{Z})^\times$. This is why Theorem 11.15 is a generalization of the Dirichlet's theorem on primes in arithmetic progressions.

Remark 11.17 (On the notion of density)**.** The notion of Dirichlet density is somewhat artificial. More natural notion of density of S (called the **natural density**) is $\lim_{n\to\infty} \frac{\#\{\mathfrak{p}\text{ prime ideals in }S,\ N(\mathfrak{p})\leq n\}}{\#\{\mathfrak{p}\text{ prime ideals, }N(\mathfrak{p})\leq n\}}$. It is indeed true that the above theorems hold even if you replace the Dirichlet density with the natural density, but the proof requires a further argument; a set with natural density δ has Dirichlet density δ (this again requires the analytic class number formula), but the converse is not necessarily true. One general tool you could use is the **Tauberian theorem**, which gives an asymptotic of $\sum_{m\leq n} a_m$ as $n \to \infty$ from the behaviour of the holomorphic function $\sum_{m=1}^{\infty} \frac{a_m}{m^s}$ as $\mathrm{Re}(s) \to 1^+$.

11.4. **Density of splitting primes, and the Second Inequality of global class field theory.** The density theorem we discussed in the previous subsection happened in the ray class group. There is an analogous density theorem in the other side of the class field theory, on the Galois side. A type of set of prime ideals whose measure we are interested in is: given a finite Galois extension of L/K and a conjugacy class $\mathcal{C} \subset \mathrm{Gal}(L/K)$, the set of prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ unramified in L and $\mathrm{Fr}_{\mathfrak{p}} = \mathcal{C}$. We will see that we have an expected answer, that the Frobenii of prime ideals are equally distributed among the elements of $\mathrm{Gal}(L/K)$. This is called the **Chebotarev density theorem**. This will follow as a consequence of global class field theory, so we are not proving it here.

A small special case of the Chebotarev density theorem, however, can be proved here, and will yield the so-called **Second Inequality** of global class field theory which is a crucial ingredient for the ultimate proof of the global class field theory. Note that, retaining the above paragraph's notations, asking $\mathrm{Fr}_{\mathfrak{p}} = \mathrm{id}$ is exactly the same as asking $\mathfrak{p}$ to split completely in L. More generally, if L/K is a finite extension and M/K is its Galois closure, then for a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ that is unramified in L, it is automatically unramified in M (this is because M is the compositum of all conjugates of L in M, and $\mathfrak{p}$ is unramified in any conjugate of L), and $\mathfrak{p}$ splitting completely in L is equivalent to $\mathfrak{p}$ splitting completely in M (by the same reasoning), so $\mathfrak{p}$ splits completely in L if and only if $\mathrm{Fr}_{\mathfrak{p}} \in \mathrm{Gal}(M/K)$ is the identity. We can now see why the following statement is a special case of the Chebotarev density theorem.

Proposition 11.18. *Let L/K be a finite extension of number fields, and let M/K be its Galois closure. Then, the set of prime ideals of K splitting completely in L has Dirichlet density $\frac{1}{[M:K]}$.*

Proof. By the paragraph right before this, we may assume that L/K is already Galois to start with. Let S be the set of prime ideals of K splitting completely in L, and let T be the set of prime ideals of L lying over those in S. Let U be the set of prime ideals $\mathfrak{q} \subset \mathcal{O}_L$ such that it is unramified over K and its residue field $\mathcal{O}_L/\mathfrak{q}$ is a prime field (i.e. $\mathbb{F}_p$ for a prime number p, not a prime power). Then, $U \subset T$; for $\mathfrak{q} \in U$, if $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$, then $f(\mathfrak{q}|\mathfrak{p}) = 1$ because there is no possibility for a residue field extension because $\mathcal{O}_L/\mathfrak{q}$ is as small as possible; as $e(\mathfrak{q}|\mathfrak{p}) = 1$ by definition and L/K is Galois, $\mathfrak{p}$ splits completely in L.

I claim that U has Dirichlet density 1. Assuming this, the statement easily follows. Namely, as U has Dirichlet density 1, T must have Dirichlet density 1. This means $\sum_{\mathfrak{q} \in T} \frac{1}{N(\mathfrak{q})^s} - \log\left(\frac{1}{s-1}\right)$ is bounded as $s \in \mathbb{R}$ appraches to $s = 1$ from the right. The sum can be written as $\sum_{\mathfrak{p} \in S} \sum_{\mathfrak{q}|\mathfrak{p}} \frac{1}{N(\mathfrak{q})^s}$. However, as each $\mathfrak{p} \in S$ splits completely in L, there are exactly $[L : K]$ many $\mathfrak{q}$ dividing $\mathfrak{p}$, and $N(\mathfrak{q}) = N(\mathfrak{p})$ for all such $\mathfrak{q}|\mathfrak{p}$. Therefore, this means $[L : K] \sum_{\mathfrak{p} \in S} \frac{1}{N(\mathfrak{p})^s} - \log\left(\frac{1}{s-1}\right)$ is bounded as $s \in \mathbb{R}$ approaches $s = 1$ from the right, or that S has Dirichlet density $\frac{1}{[L:K]}$.

Now we are left with proving the claim. As there are only finitely many ramified primes, it suffices to prove the following.

Lemma 11.19. *Let K be a number field. Then, the set B of prime ideals $\mathfrak{p}$ of K whose absolute residue degree*[10] *is > 1 has Dirichlet density 0.*

[10] For a prime ideal $\mathfrak{p}$ of K, the **absolute residue degree** is $f(\mathfrak{p}|p)$, where $p \in \mathbb{Z}$ is a prime number such that $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. For example, $\mathfrak{p}$ has absolute residue degree 1 precisely when $\mathcal{O}_K/\mathfrak{p}$ is a finite field of prime order.

Proof. Note that, for every prime number $p \in \mathbb{Z}$, there are at most $[K : \mathbb{Q}]$ many prime ideals of K dividing p. Also, for $\mathfrak{p} \in N(\mathfrak{p})$ with $\mathfrak{p}|p$ for a prime number $p \in \mathbb{Z}$, $N(\mathfrak{p}) = p^{f(\mathfrak{p}|p)} \geq p^2$. Thus,

$$\sum_{p \text{ prime number}} \sum_{\mathfrak{p} \in B, \mathfrak{p}|p} \frac{1}{N(\mathfrak{p})} \leq \sum_{p \text{ prime number}} \frac{[K : \mathbb{Q}]}{p^2} \leq \sum_{n=1}^{\infty} \frac{[K : \mathbb{Q}]}{n^2},$$

which is absolutely convergent. Thus, we may rearrange the sum on the left, and deduce that $\sum_{\mathfrak{p} \in B} \frac{1}{N(\mathfrak{p})}$ is absolutely convergent. This implies that the Dirichlet density of B is 0. □

□

Combining the two statements, we are now ready to prove the **Second Inequality**.

Theorem 11.20 (Second Inequality). *Let L/K be a finite Galois extension of number fields, and let $\mathfrak{m}$ be a modulus of K. Recall that $S(\mathfrak{m})$ is the set of primes dividing $\mathfrak{m}$. Let $S'(\mathfrak{m})$ be the set of primes of L lying over those in $S(\mathfrak{m})$. Then,*

$$[J_K^{S(\mathfrak{m})} : K^{\mathfrak{m},1} N_{L/K}(J_L^{S'(\mathfrak{m})})] \leq [L : K],$$

where $N_{L/K} : J_L^{S'(\mathfrak{m})} \to J_K^{S(\mathfrak{m})}$ is the ideal norm, i.e. $N_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f(\mathfrak{q}|\mathfrak{p})}$ for a prime ideal $\mathfrak{q}$ of L lying over a prime ideal $\mathfrak{p}$ of K.

Proof. Note that the left hand side is the index $[\mathrm{Cl}^{\mathfrak{m}}(K) : H]$ where H is the image of $J_L^{S'(\mathfrak{m})} \xrightarrow{N_{L/K}} J_K^{S(\mathfrak{m})} \twoheadrightarrow \mathrm{Cl}^{\mathfrak{m}}(K)$. By Theorem 11.15, the set A of prime ideals $\mathfrak{p}$ of K coprime to $\mathfrak{m}$ such that $[\mathfrak{p}] \in H \subset \mathrm{Cl}^{\mathfrak{m}}(K)$ has Dirichlet density $\frac{1}{[\mathrm{Cl}^{\mathfrak{m}}(K):H]}$. Let B be the set of prime ideals $\mathfrak{p}$ of K that is coprime to $\mathfrak{m}$ and splits completely in L. By Proposition 11.18, B has Dirichlet density $\frac{1}{[L:K]}$.

Note that if a prime ideal $\mathfrak{p}$ of K coprime to $\mathfrak{m}$ splits completely in L, then for any prime ideal $\mathfrak{q}$ of L lying over $\mathfrak{p}$, $N_{L/K}(\mathfrak{q}) = \mathfrak{p}$. Therefore, $B \subset A$. This implies that $\frac{1}{[\mathrm{Cl}^{\mathfrak{m}}(K):H]} \geq \frac{1}{[L:K]}$, which is equivalent to the **Second Inequality**. □

Corollary 11.21 (Second Inequality, Cohomological Version). *Let L/K be a finite Galois extension of number fields. Then,*

$$\# H_T^0(\mathrm{Gal}(L/K), C_L) \leq [L : K].$$

Proof. Note that $N_{L/K}(C_L)$ is a finite index subgroup of C_K, so it in particular contains $\overline{U(\mathfrak{m})}$ for some modulus $\mathfrak{m}$. Then for this modulus this follows from the Second Inequality in the original form. □

Remark 11.22. There is an algebraic proof (i.e. not using any analytic tools) of the **Second Inequality** due to Chevalley, e.g. [Mil, VII.6] (in *loc. cit.*, only the case of L/K cyclic of prime degree is proved, but we will see that this is enough for the verification of class formation axioms).

12. Global class field theory: verification of the class formation axioms + ε

12.1. **Relaxing the class formation axioms.** Recall the two Axioms for the class formation in our setup.

Axiom 1. For any finite Galois extension L/K of number fields, $H^1(\mathrm{Gal}(L/K), C_L) = 0$.

Axiom 2. For any finite Galois extension L/K of number fields, there is the invariant map

$$\mathrm{inv}_{L/K} : H^2(\mathrm{Gal}(L/K), C_L) \xrightarrow{\sim} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z},$$

compatible with inflation and restriction.

We only have the **Second Inequality**, which says about the upper bound on the order of H_T^0. This is very far from **Axiom 2**, because

- it is about H_T^0 and not H^2 (although if L/K is cyclic then $H_T^0 = H^2$ by periodicity),
- it is about the order and not the group structure,
- and it only gives an upper bound.

So we might say that the **Second Inequality** gives an extremely small part of **Axiom 2** for cyclic extensions. We want to leverage onto this. The first observation is as follows.

Lemma 12.1. ***Axiom 1*** *of the class formation axioms is equivalent to:*

Axiom 1'. *For any finite **cyclic** extension L/K of number fields, $H^1(\mathrm{Gal}(L/K), C_L) = 0$.*

Proof. It is obvious that **Axiom 1** implies **Axiom 1'**. Conversely, **Axiom 1'** implies that $H^1(\mathrm{Gal}(L/K), C_L) = 0$ for any finite **solvable** extension L/K, because you can find a finite filtration $L = K_0/K_1/\cdots/K_n = K$ where each K_i/K_{i+1} is cyclic, and then use the inflation-restriction exact sequence

$$0 \to H^1(\mathrm{Gal}(K_{i+1}/K), C_{K_{i+1}}) \to H^1(\mathrm{Gal}(K_i/K), C_{K_i}) \to H^1(\mathrm{Gal}(K_i/K_{i+1}), C_{K_i}) = 0,$$

to inductively show that $H^1(\mathrm{Gal}(K_i/K), C_{K_i}) = 0$ for all i.

To go from solvable to general finite Galois, we use a similar technique as in the proof of Tate's theorem (Theorem 5.2), that we use p-Sylow groups. Namely, the same argument shows that, for any finite group G and a G-module M, if we choose a p-Sylow subgroup G_p for every prime number p (we only need to do this for finitely many prime numbers p), then

$$\mathrm{Res} : H_T^r(G, M) \to \prod_{p \text{ prime number}} H_T^r(G_p, M),$$

is injective. Applying this to our setup, given a finite Galois extension L/K, we can choose $L/K_p/K$ for any prime number p such that $\mathrm{Gal}(L/K_p) \le \mathrm{Gal}(L/K)$ is a p-Sylow subgroup. As L/K_p is solvable (any p-group is solvable!), **Axiom 1'** implies that $H^1(\mathrm{Gal}(L/K_p), C_L) = 0$. The above observation then implies that $H^1(\mathrm{Gal}(L/K), C_L) = 0$, which is **Axiom 1**. □

Remark 12.2. The above proof shows that, if we wish, we can further reduce to checking $H^1 = 0$ for finite cyclic extensions of prime degree, a small improvement which we won't take advantage of.

What is interesting about this relaxation is that we can use Herbrand quotient. Namely, suppose we care only about computing the order in the cyclic case. By the **Second Inequality**, we already know that $\#H^0_T(\mathrm{Gal}(L/K), C_L) = \#H^2_T(\mathrm{Gal}(L/K), C_L) \leq [L : K]$. In addition to this, if we show that the Herbrand quotient $h(C_L) = [L : K]$, then this will simultaneously show that $\#H^1_T(\mathrm{Gal}(L/K), C_L) = 1$ and $\#H^2_T(\mathrm{Gal}(L/K), C_L) = [L : K]$, because $[L : K] \geq \#H^2_T(\mathrm{Gal}(L/K), C_L) = h(C_L)\#H^1_T(\mathrm{Gal}(L/K), C_L) \geq h(C_L) = [L : K]$, so the equality is achieved everywhere! We can summarize our findings as follows.

Lemma 12.3. *__Axiom 1__ and __Axiom 2__ of the class formation axioms, for $F = \mathbb{Q}$ and $A = C := \varprojlim_{K \text{ number field}} C_K$, are implied by the following rather different set of Axioms.*

- *(__First Inequality__[11]) For a finite cyclic extension L/K of number fields,*
$$h(C_L) = [L : K].$$
- *(__Second Inequality__) For a finite Galois extension L/K of number fields,*
$$\#H^0_T(\mathrm{Gal}(L/K), C_L) \leq [L : K].$$
- *(__"Big Regular Part"__[12]) For a Galois extension of number fields L/K, there exists a subgroup $H^2(\mathrm{Gal}(L/K), C_L)_{\mathrm{reg}} \subset H^2(\mathrm{Gal}(L/K), C_L)$, whose elements are called __regular__, and a homomorphism*
$$\mathrm{inv}_{L/K,\mathrm{reg}} : H^2(\mathrm{Gal}(L/K), C_L)_{\mathrm{reg}} \to \mathbb{Q}/\mathbb{Z},$$
such that $\mathrm{im}(\mathrm{inv}_{L/K,\mathrm{reg}}) \supset \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$. This map interacts with Inf and Res in an expected way. Namely, given a subextension $L/M/K$, Res on H^2 of C_L restricts to $\mathrm{Res} : H^2(\mathrm{Gal}(L/K), C_L)_{\mathrm{reg}} \to H^2(\mathrm{Gal}(L/M), C_L)_{\mathrm{reg}}$, and given a tower of Galois extensions $L/M/K$, Inf on H^2 restricts to $\mathrm{Inf} : H^2(\mathrm{Gal}(M/K), C_M)_{\mathrm{reg}} \to H^2(\mathrm{Gal}(L/K), C_L)_{\mathrm{reg}}$. Furthermore, the following diagrams commute,

$$\begin{tikzcd}
H^2(\mathrm{Gal}(L/K), C_L)_{\mathrm{reg}} \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_{L/K,\mathrm{reg}}"'] & H^2(\mathrm{Gal}(L/M), C_L)_{\mathrm{reg}} \arrow[d, "\mathrm{inv}_{L/M,\mathrm{reg}}"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "x \mapsto [M:K]x"'] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

$$\begin{tikzcd}
H^2(\mathrm{Gal}(M/K), C_M)_{\mathrm{reg}} \arrow[r, "\mathrm{Inf}"] \arrow[d, "\mathrm{inv}_{M/K,\mathrm{reg}}"'] & H^2(\mathrm{Gal}(L/K), C_L)_{\mathrm{reg}} \arrow[d, "\mathrm{inv}_{L/K,\mathrm{reg}}"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "x \mapsto x"'] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

[11] This statement is called an inequality because this implies that $\#H^2(\mathrm{Gal}(L/K), C_L) \geq [L : K]$ for cyclic extensions L/K.

[12] This is not a standard terminology (there is no standard short name for this result).

Proof. By the **Second Inequality** and the periodicity, for a finite cyclic extension L/K, we see that $\#H_T^2(\mathrm{Gal}(L/K), C_L) \leq [L : K]$. By the paragraph preceding this, together with the **First Inequality**, we obtain that $\#H^1(\mathrm{Gal}(L/K), C_L) = 1$ (which is **Axiom 1'**). and $\#H^2(\mathrm{Gal}(L/K), C_L) = [L : K]$. By Lemma 12.1, we have **Axiom 1**. Now that we have **Axiom 1**, we have the inflation-restriction exact sequence for H^2. By the exactly same argument as in Lemma 12.1, we see that $\#H^2(\mathrm{Gal}(L/K), C_L) \leq [L : K]$ for any finite solvable extension L/K. Furthermore, we know that $\mathrm{Res} : H^2(\mathrm{Gal}(L/K), C_L) \to \prod_{p \text{ prime}} H^2(\mathrm{Gal}(L/K_p), C_L)$ is injective, where $\mathrm{Gal}(L/K_p) \leq \mathrm{Gal}(L/K)$ is a Sylow p-group, by the solvable case, we know that

$$\#H^2(\mathrm{Gal}(L/K), C_L) \leq \prod_p \#H^2(\mathrm{Gal}(L/K_p), C_L) \leq \prod_p [L : K_p] = [L : K],$$

which shows that $\#H^2(\mathrm{Gal}(L/K), C_L) \leq [L : K]$ for any finite Galois extension L/K. On the other hand, the **"Big Regular Part"** implies that $\#H^2(\mathrm{Gal}(L/K), C_L) \geq \#H^2(\mathrm{Gal}(L/K), C_L)_{\mathrm{reg}} \geq \#\,\mathrm{im}(\mathrm{inv}_{L/K,\mathrm{reg}}) \geq [L : K]$. Therefore, we know that

$$[L : K] \geq \#H^2(\mathrm{Gal}(L/K), C_L) \geq \#H^2(\mathrm{Gal}(L/K), C_L)_{\mathrm{reg}} \geq \#\,\mathrm{im}(\mathrm{inv}_{L/K,\mathrm{reg}}) \geq [L : K],$$

so the equality is realized everywhere. This implies that $H^2(\mathrm{Gal}(L/K), C_L) = H^2(\mathrm{Gal}(L/K), C_L)_{\mathrm{reg}}$, and $\mathrm{inv}_{L/K,\mathrm{reg}}$ is an isomorphism onto $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$. The two commutative diagrams ensure that the invariant map we have satisfies the compatibilities required in **Axiom 2**. This finishes the proof. □

Remark 12.4. The above proof shows that, if we wish, we can relax the **First Inequality** and the **Second Inequality** to checking them only for finite cyclic extensions of prime degree, a small improvement which we won't take advantage of.

We have already obtained the **Second Inequality** (Corollary 11.21), so we are left with obtaining the **First Inequality** and the **"Big Regular Part"**.

12.2. The First Inequality of global class field theory.

Let L/K be a finite cyclic extension of number fields. We want to compute the Herbrand quotient $h(C_L)$. The first guess is to use the short exact sequence

$$1 \to L^\times \to I_L \to C_L \to 1,$$

and use the Herbrand quotients of $L^\times$ and I_L. However, if you try to calculate, you will realize quickly that the Herbrand quotient of $L^\times$ does not exist because the Galois cohomology groups are infinite.

Example 12.5. Let $L = \mathbb{Q}(i)$ and $K = \mathbb{Q}$. Then, $H_T^0(\mathrm{Gal}(L/K), L^\times) = \mathbb{Q}^\times / N_{\mathbb{Q}(i)/\mathbb{Q}}(\mathbb{Q}(i)^\times)$. However, you know that a prime number is a norm from $\mathbb{Q}(i)$ if and only if it is either 2 or $\equiv 1 \pmod 4$. Therefore, you see that

$$H_T^0(\mathrm{Gal}(L/K), L^\times) = \{\pm 1\} \times \prod_{p \text{ prime number} \equiv 3 \pmod 4} \mathbb{Z}/2\mathbb{Z},$$

which is an infinite group.

However, there is a surprising consequence of the finiteness of class number.

Lemma 12.6. *Let L be a number field. Then, there exists a finite set of places S of L, including all infinite places of L, such that $I_L = I_{L,S}L^\times$.*

Proof. Recall that $I_{L,S}$ is the group of ideles whose v-components are in $\mathcal{O}_{L_v}^\times$ for all $v \notin S$. Namely, $I_{L,S} = \prod_{v\notin S} \mathcal{O}_{L_v}^\times \times \prod_{v\in S} L_v^\times$. Note that, in terms of the notation introduced in Proposition 7.11, $U(\mathfrak{m}_\emptyset) = I_{L,S_\infty}$, where S_∞ is the set of all infinite places of L, and $\mathfrak{m}_\emptyset$ is the empty modulus (see Example 7.10). Therefore, $\mathrm{Cl}(L) = I_L/I_{L,S_\infty}L^\times$, which is a finite group, by the finiteness of class number. Therefore, there are finitely many ideles $\alpha_1, \cdots, \alpha_n \in I_L$ that generate $I_L/I_{L,S_\infty}L^\times$. For each idele α_i, there are only finitely many places v of L at which $|\alpha_i|_v \neq 1$. Gathering all such places for each α_i and adding to S_∞, we obtain a finite set of places S where $I_{L,S} \ni \alpha_1, \cdots, \alpha_n$. Therefore, $I_L/I_{L,S}L^\times = 1$, or $I_L = I_{L,S}L^\times$. □

Therefore, we have a short exact sequence

$$1 \to L^\times \cap I_{L,S} \to I_{L,S} \to C_L \to 1.$$

Note that $L^\times \cap I_{L,S} = \mathcal{O}_{L,S}^\times$ (i.e. $x \in L^\times$ such that $|x|_v = 1$ for all $v \notin S$, or equivalently, the prime ideal factorization of (x) only involves primes appearing in S). Now I claim that $h(I_{L,S})$ and $h(\mathcal{O}_{L,S}^\times)$ are finite numbers[13], so that we can compute $h(C_L)$ from this short exact sequence.

Proposition 12.7. *Let L/K be a finite Galois extension of number fields. Let S be a finite set of places of K that contains all infinite places of K and all places which ramify in L. Let T be the set consisting of all places of L that lies over S. Then,*

$$h(I_{L,T}) = \prod_{v\in S}[L_w : K_v],$$

where the notation means that, for each $v \in S$, we choose any place w of L that lies over v (the degree $[L_w : K_v]$ is independent of the choice of such w as L/K is Galois).

Proof. This follows from the computations of the cohomology of local fields. Namely,

$$H^i(\mathrm{Gal}(L/K), I_{L,T}) = H^i\left(\mathrm{Gal}(L/K), \prod_{w\notin T}\mathcal{O}_{L_w}^\times \times \prod_{w\in T} L_w^\times\right)$$

$$= \prod_{v\notin S} H^i\left(\mathrm{Gal}(L/K), \prod_{w|v}\mathcal{O}_{L_w}^\times\right) \times \prod_{v\in S} H^i\left(\mathrm{Gal}(L/K), \prod_{w|v} L_w^\times\right).$$

For each place v of K, choose $w|v$. Then, because L/K is Galois, any other $w'|v$ arises as a conjugate of w, so $\prod_{w|v} L_w^\times = \mathrm{Ind}_{\mathrm{Gal}(L_w/K_v)}^{\mathrm{Gal}(L/K)} L_w^\times$, and $\prod_{w|v}\mathcal{O}_{L_w}^\times = \mathrm{Ind}_{\mathrm{Gal}(L_w/K_v)}^{\mathrm{Gal}(L/K)} \mathcal{O}_{L_w}^\times$. By Shapiro's

[13] We already know $h(\mathcal{O}_{L,S}^\times)$ is a finite number by Lemma 4.4 because $\mathcal{O}_{L,S}^\times$ is a finitely generated abelian group (Theorem 12.9, Dirichlet's unit theorem for S-units).

lemma, we have

$$\prod_{v\notin S} H^i\left(\mathrm{Gal}(L/K), \prod_{w|v} \mathcal{O}_{L_w}^\times\right) \times \prod_{v\in S} H^i\left(\mathrm{Gal}(L/K), \prod_{w|v} L_w^\times\right)$$

$$= \prod_{v\notin S} H^i(\mathrm{Gal}(L_w/K_v), \mathcal{O}_{L_w}^\times) \times \prod_{v\in S} H^i(\mathrm{Gal}(L_w/K_v), L_w^\times).$$

By definition, if $v \notin S$, this means v is unramified in L. Thus, L_w/K_v is unramified, so by Proposition 4.17(1), $H^i(\mathrm{Gal}(L_w/K_v), \mathcal{O}_{L_w}^\times) = 0$ for $i > 0$ whenever $v \notin S$. Therefore, we have

$$H^i(\mathrm{Gal}(L/K), I_{L,T}) = \prod_{v\in S} H^i(\mathrm{Gal}(L_w/K_v), L_w^\times).$$

By Theorem 4.14 and Theorem 4.20,

$$H^1(\mathrm{Gal}(L/K), I_{L,T}) = 1, \quad H^2(\mathrm{Gal}(L/K), I_{L,T}) \cong \prod_{v\in S} \frac{1}{[L_w : K_v]}\mathbb{Z}/\mathbb{Z}.$$

This gives the desired result. □

We record one consequence of the above proof, which is the Galois cohomology of the ideles.

Corollary 12.8. *Let L/K be a finite Galois extension of number fields. Then,*

$$H^1(\mathrm{Gal}(L/K), I_L) = 1, \quad H^2(\mathrm{Gal}(L/K), I_L) \cong \bigoplus_{v \text{ places of } K} \mathrm{Br}(L_w/K_v) \cong \bigoplus_{v \text{ places of } K} \frac{1}{[L_w : K_v]}\mathbb{Z}/\mathbb{Z},$$

where the notation means that, for each place v of K, we choose any place w of L that lies over v.

Proof. This follows from a byproduct of the above proof,

$$H^1(\mathrm{Gal}(L/K), I_{L,T}) = 1, \quad H^2(\mathrm{Gal}(L/K), I_{L,T}) \cong \prod_{v\in S} \frac{1}{[L_w : K_v]}\mathbb{Z}/\mathbb{Z},$$

and taking the direct limit over S by making S larger and larger. Note that the direct sum appears as we are taking a direct limit ("union"), so any element in the direct limit must have nonzero entries at only finitely many places. □

Now we are reduced to computing the Herbrand quotient of unit group. We firstly record the Dirichlet's unit theorem for S-units.

Theorem 12.9 (Dirichlet's unit theorem for S-units)**.** *Let K be a number field, and let S be a finite set of places of K including all infinite places of K. Then,*

$$\mathcal{O}_{K,S}^\times \cong \mu_K \times \mathbb{Z}^{\#S-1}.$$

This is very much a direct consequence of the usual Dirichlet's unit theorem (it is a special case of the above statement when S is just the set of all infinite places of K, in which case $\#S = r+s$ in the usual notation), whose proof you may find in [ANT]. More precisely, as in the proof of the usual Dirichlet's unit theorem, you consider the following map,

$$\iota_{K,S} : \mathcal{O}_{K,S}^\times \to \mathbb{R}^{\#S}, \quad x \mapsto (\log |x|_v)_{v\in S}.$$

By the product formula, its image lies in the hyperplane $H \subset \mathbb{R}^{\#S}$ defined by

$$H := \{(t_v)_{v\in S} \ : \ \sum_{v\in S} t_v = 0\}.$$

Then, as in the case of Dirichlet's unit theorem, the image $\iota_{K,S}(\mathcal{O}_{K,S}^\times)$ is a lattice in H, and $\ker \iota_{K,S} = (\mathcal{O}_{K,S}^\times)_{\text{tors}} = \mu_K$.

Using this gadget, we are now ready to prove the following.

Proposition 12.10. *Let L/K be a finite cyclic extension of number fields, and let S be a finite set of places of K containing all infinite places. Let T be the set of all places of L lying over those in S. Then,*

$$h(\mathcal{O}_{L,T}^\times) = \frac{1}{[L:K]} \prod_{v\in S} [L_w : K_v],$$

where the notation means that, for each $v \in S$, we choose any place w of L that lies over v.

Proof. We consider the map $\iota_{L,T} : \mathcal{O}_{L,T}^\times \to \mathbb{R}^{\#T}$ defined above. Note that this map is $\mathrm{Gal}(L/K)$-equivariant (i.e. $\iota_{L,T}$ is compatible with the action of $\mathrm{Gal}(L/K)$ on the source and the target), if you define the action of $\mathrm{Gal}(L/K)$ on $\mathbb{R}^{\#T}$ by permuting the coordinates (i.e. the action of $\sigma \in \mathrm{Gal}(L/K)$ is that the v-component is sent to the σv-component). The sum-zero hyperplane $H \subset \mathbb{R}^{\#T}$ is obviously stable under the $\mathrm{Gal}(L/K)$-action, and so is the image $\iota_{L,T}(\mathcal{O}_{L,T}^\times)$, which is a lattice in H. Consider the lattice $\mathcal{L} \subset \mathbb{R}^{\#T}$ generated by $\iota_{L,T}(\mathcal{O}_{L,T}^\times)$ and the vector $(1,1,\cdots,1) \in \mathbb{R}^{\#T}$. Then, $\mathcal{L}$ is stable under the $\mathrm{Gal}(L/K)$-action (as $(1,\cdots,1)$ is obviously stable under permutation of coordinates), so you may consider $\mathcal{L}$ as a $\mathrm{Gal}(L/K)$-module. Then, $\mathcal{L} = \iota_{L,T}(\mathcal{O}_{L,T}^\times) \oplus \mathbb{Z}$ as $\mathrm{Gal}(L/K)$-modules, so $h(\mathcal{L}) = h(\mathcal{O}_{L,T}^\times)h(\mathbb{Z}) = [L:K]h(\mathcal{O}_{L,T}^\times)$. Therefore, it suffices to show that $h(\mathcal{L}) = \prod_{v\in S}[L_w : K_v]$.

Now the key is the following lemma.

Lemma 12.11. *Let G be a finite cyclic group, and V be a $\mathbb{R}[G]$-module which is also a finite-dimensional $\mathbb{R}$-vector space. Let $L_1, L_2 \subset V$ be lattices that are stable under the G-action. Then, $h(L_1) = h(L_2)$.*

Proof. Let $\dim_{\mathbb{R}} V = d$ and $G \cong \mathbb{Z}/n\mathbb{Z}$. Abstractly this means that L_1, L_2 are $\mathbb{Z}[G]$-modules such that $L_1 \otimes_{\mathbb{Z}} \mathbb{R} \cong L_2 \otimes_{\mathbb{Z}} \mathbb{R}$ as $\mathbb{R}[G]$-modules. Let $L_{i,\mathbb{Q}} := L_i \otimes_{\mathbb{Z}} \mathbb{Q}$, which is a $\mathbb{Q}[G]$-module. As G is a finite cyclic group, it is generated by a single element. Thus, upon choosing a basis of $L_{i,\mathbb{Q}}$, this being a $\mathbb{Q}[G]$-module means that there is a $d\times d$ invertible matrix T_i with coefficients in $\mathbb{Q}$ (or $T_i \in \mathrm{GL}_d(\mathbb{Q})$) such that $T_i^n = \mathrm{id}$. As $L_{1,\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{R} \cong L_{2,\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{R}$ as $\mathbb{R}[G]$-modules, this means that, based on the choice of basis on both $L_{1,\mathbb{Q}}, L_{2,\mathbb{Q}}$, there is an $d\times d$ invertible matrix M with coefficients in $\mathbb{R}$ (or $M \in \mathrm{GL}_d(\mathbb{R})$) such that $MT_1 = T_2M$. Consider the real vector space of $d \times d$ matrices with real coefficients, regarded as $\mathbb{R}^{d^2}$, with coordinates $(x_{11}, \cdots, x_{dd})$, and consider the subspace $\mathcal{S} \subset \mathbb{R}^{d^2}$ such that the matrix $(x_{ij})_{1\leq i,j\leq n}$ satisfies $(x_{ij})_{1\leq i,j\leq n}T_1 = T_2(x_{ij})_{1\leq i,j\leq n}$. This means that x_{ij}'s satisfy a system of linear equations where the coefficients are all rational numbers. Therefore, $\mathcal{S}$ has a basis $v_1, \cdots, v_m$ such that, for each v_i, all coordinates of v_i are rational numbers. Any element of $\mathcal{S}$ is expressed as $\sum_{i=1}^m y_iv_i$, $y_i \in \mathbb{R}$. Then, the determinant of the matrix $(x_{ij})_{1\leq i,j\leq n}$ is expressed as a polynomial in $y_1, \cdots, y_m$ with rational coefficients, which we denote $P(y_1, \cdots, y_m) \in \mathbb{Q}[y_1, \cdots, y_m]$. The fact that there is $M \in \mathrm{GL}_d(\mathbb{R})$ such that $MT_1 = T_2M$ means that there are real numbers $r_1, \cdots, r_m \in \mathbb{R}$ such that $P(r_1, \cdots, r_m) \neq 0$. Therefore, the set of solutions $\{P(y_1, \cdots, y_m) = 0\} \subset \mathcal{S}$ is a proper closed subset (as P is continuous). As $\{(y_1, \cdots, y_m) : y_i \in \mathbb{Q}\} \subset \mathcal{S}$ is dense, this implies that there are $q_1, \cdots, q_m \in \mathbb{Q}$ such that $P(q_1, \cdots, q_m) \neq 0$. Therefore, there exists a $d \times d$ invertible matrix N with rational coefficients such that $NT_1 = T_2N$. This implies that $L_{1,\mathbb{Q}} \cong L_{2,\mathbb{Q}}$ as $\mathbb{Q}[G]$-modules. Now, by scaling the isomorphism, it is easy to see that there is an isomorphism $f : L_{1,\mathbb{Q}} \xrightarrow{\sim} L_{2,\mathbb{Q}}$ of $\mathbb{Q}[G]$-modules such that $f(L_1) \subset L_2$ (take a random isomorphism, see what vectors you get by sending L_1, clear the denominators, and multiply the isomorphism by the common denominator). This implies that there is an injective G-module homomorphism $f : L_1 \to L_2$ whose cokernel is necessarily a finite abelian group (because L_1, L_2 are lattices of the same vector space). Therefore, $h(L_2) = h(L_1)h(\operatorname{coker} f) = h(L_1)$. □

Therefore, by Lemma 12.11, we can compute $h(\mathcal{L})$ by computing $h(\mathcal{L}')$ for any lattice $\mathcal{L}' \subset \mathbb{R}^{\#T}$ that is compatible under the $\mathrm{Gal}(L/K)$-action. One particular choice is $\mathbb{Z}^{\#T} \subset \mathbb{R}^{\#T}$, which is clearly preserved under the permutation of coordinates. Note that, as $\mathrm{Gal}(L/K)$-modules,

$$\mathbb{Z}^{\#T} = \bigoplus_{v\in S} \mathrm{Ind}_{\mathrm{Gal}(L_w/K_v)}^{\mathrm{Gal}(L/K)} \mathbb{Z},$$

(again w is chosen for each $v \in S$), so $h(\mathbb{Z}^{\#T}) = \prod_{v\in S} h(\mathrm{Ind}_{\mathrm{Gal}(L_w/K_v)}^{\mathrm{Gal}(L/K)} \mathbb{Z}) = \prod_{v\in S}[L_w : K_v]$ by Shapiro's lemma. This finishes the proof. □

Corollary 12.12 (First Inequality). *Let L/K be a finite cyclic extension of number fields. Then,*

$$h(C_L) = [L : K].$$

Proof. Let S be a finite set of primes of K containing all infinite places of K and all places which ramify in L. Let T be the set of all places of L lying over those in S. After possibly enlarging S, we may assure that $I_L = I_{L,T}L^\times$ by Lemma 12.6. Then, by Proposition 12.7 and Proposition 12.10, the short exact sequence $1 \to \mathcal{O}_{L,T}^\times \to I_{L,T} \to C_L \to 1$ implies that

$$h(C_L) = \frac{h(I_{L,T})}{h(\mathcal{O}_{L,T}^\times)} = \frac{\prod_{v\in S}[L_w : K_v]}{\frac{1}{[L:K]}\prod_{v\in S}[L_w : K_v]} = [L : K].$$

□

We have thus established the **First Inequality** and the **Second Inequality**. Note that, by the proof of Lemma 12.3, this means that **Axiom 1** is established by now.

12.3. **Brauer groups of number fields.** Similar to the local case, we also use the Brauer group of global fields. The starting point is the following.

Corollary 12.13. *Let L/K be a finite Galois extension of number fields. Then, we have the exact sequence*

$$0 \to \mathrm{Br}(L/K) \to \bigoplus_{v \text{ places of } K} \mathrm{Br}(L_w/K_v) \to H^2(\mathrm{Gal}(L/K), C_L),$$

where the notation means that, for each place v of K, we choose any place w of L that lies over v. By taking the direct limit over L (with Inf *being transition maps), we have the exact sequence*

$$0 \to \mathrm{Br}(K) \to \bigoplus_{v \text{ places of } K} \mathrm{Br}(K_v) \to H^2(\mathrm{Gal}(\overline{\mathbb{Q}}/K), C).$$

Proof. This follows from the short exact sequence $1 \to L^\times \to I_L \to C_L \to 1$, Corollary 12.8, and **Axiom 1**, which is now known because of the **First Inequality** (Corollary 12.12) and the **Second Inequality** (Corollary 11.21). The latter statement follows from the fact that taking direct limit is left exact. □

We actually precisely know what the cokernel of the map $\mathrm{Br}(K) \to \bigoplus_{v \text{ places of } K} \mathrm{Br}(K_v)$, which is the final ingredient for the proof of the (reciprocity law part of the) global class field theory.

Theorem 12.14 ("Global Invariant Zero"[14]). *Let K be a number field. Then, the composition*

$$\mathrm{Br}(K) \to \bigoplus_{v \text{ places of } K} \mathrm{Br}(K_v) \xrightarrow{\oplus_v \mathrm{inv}_{K_v}} \mathbb{Q}/\mathbb{Z},$$

is zero.

Similarly, for a Galois extension of number fields L/K, the composition

$$\mathrm{Br}(L/K) \to \bigoplus_{v \text{ places of } K} \mathrm{Br}(L_w/K_v) \xrightarrow{\oplus_v \mathrm{inv}_{L_w/K_v}} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z},$$

is zero, where the notation means that, for each place v of K, we choose any place w of L that lies over v.

We first explain why this is important.

Theorem 12.15. *The "**Global Invariant Zero**" implies the "**Big Regular Part**".*

Proof. We define $H^2(\mathrm{Gal}(\overline{\mathbb{Q}}/K), C)_{\mathrm{reg}} := \mathrm{im}(H^2(\mathrm{Gal}(\overline{\mathbb{Q}}/K), I) \to H^2(\mathrm{Gal}(\overline{\mathbb{Q}}/K), C))$, where $I = \varinjlim_{L/K \text{ finite}} I_L$. On a finite level,

$$H^2(\mathrm{Gal}(L/K), C_L)_{\mathrm{reg}} := \{\alpha \in H^2(\mathrm{Gal}(L/K), C_L) \ : \ \exists M/L/K \text{ Galois s.t.}$$

[14] This is not a standard terminology (there is no standard short name for this result).

$$\mathrm{Inf}(\alpha) \in \mathrm{im}(H^2(\mathrm{Gal}(M/K), I_M) \to H^2(\mathrm{Gal}(M/K), C_M))\}.$$

We define $\mathrm{inv}_{L/K,\mathrm{reg}} : H^2(\mathrm{Gal}(L/K), C_L)_{\mathrm{reg}} \to \mathbb{Q}/\mathbb{Z}$ as follows. Let $\alpha \in H^2(\mathrm{Gal}(L/K), C_L)_{\mathrm{reg}}$, and let $M/L/K$ be Galois such that $\mathrm{Inf}(\alpha)$ comes from $\beta \in H^2(\mathrm{Gal}(M/K), I_M)$. Then, you can take the sum of local invariants of β as the definition of $\mathrm{inv}_{L/K,\mathrm{reg}}(\alpha)$. This on one hand does not depend on the choice of β, because $\mathrm{im}(H^2(\mathrm{Gal}(M/K), I_M) \to H^2(\mathrm{Gal}(M/K), C_M))$ is the cokernel of $H^2(\mathrm{Gal}(M/K), M^\times) \to H^2(\mathrm{Gal}(M/K), I_M)$, which, by the **"Global Invariant Zero"** (Theorem 12.14), has a well-defined map to $\frac{1}{[M:K]}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$. This on the other hand does not depend on the choice of M, as the local invariants stay the same even after further inflation. As $\mathrm{im}(H^2(\mathrm{Gal}(L/K), I_L) \to H^2(\mathrm{Gal}(L/K), C_L)) \subset H^2(\mathrm{Gal}(L/K), C_L)_{\mathrm{reg}}$ admits a surjective invariant map to $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$, this implies that $\mathrm{im}(\mathrm{inv}_{L/K,\mathrm{reg}}) \supset \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$. It is an easy exercise to check that $\mathrm{inv}_{L/K,\mathrm{reg}}$ interacts in an expected way with Res and Inf by using the same properties for the local invariants. □

Thus, what is only left for the reciprocity law part of the global class field theory is to show the **"Global Invariant Zero"**.

*Proof of **"Global Invariant Zero"**, Theorem 12.14.* As the absolute Brauer group is a direct limit of the relative Brauer groups, it suffices to show the statement for the relative case. We now divide the proof into several pieces.

Step 1. Reducing to $K = \mathbb{Q}$.

Note that we know that the local invariants are not changed by Inf and Cor. Thus, if we take a large enough number field $M/L/K$ where $M/\mathbb{Q}$ is Galois, then, for any $\alpha \in \mathrm{Br}(L/K)$, the sum of local invariants of α is the same as that of $\mathrm{Inf}(\alpha) \in \mathrm{Br}(M/K)$, which is the same as that of $\mathrm{Cor}(\mathrm{Inf}(\alpha)) \in \mathrm{Br}(M/\mathbb{Q})$. Therefore, it suffices to prove the case when $K = \mathbb{Q}$.

Step 2. Proof when $L/\mathbb{Q}$ is cyclic.

We use the notation of Lemma 5.9. Note that, as $\mathrm{Gal}(L/\mathbb{Q})$ is cyclic, $H^0_T(\mathrm{Gal}(L/\mathbb{Q}), L^\times) \cong H^2_T(\mathrm{Gal}(L/\mathbb{Q}), L^\times)$, so obviously every element of $\mathrm{Br}(L/\mathbb{Q})$ is written as $a \cup \delta\chi$ for $a \in \mathbb{Q}^\times$ and $\chi \in \mathrm{Hom}_{\mathrm{Grp}}(\mathrm{Gal}(L/\mathbb{Q}), \mathbb{Q}/\mathbb{Z})$. This description is nice, because firstly $a \cup \delta\chi \in \mathrm{Br}(L/\mathbb{Q})$ is sent to $a \cup \delta\chi_p \in \mathrm{Br}(L_{v_p}/\mathbb{Q}_p)$, where v_p is a place of L that divides p, and $a \in \mathbb{Q}^\times$ gives rise to $a \in \mathbb{Q}_p^\times$ and $\chi \in \mathrm{Hom}_{\mathrm{Grp}}(\mathrm{Gal}(L/\mathbb{Q}), \mathbb{Q}/\mathbb{Z}) \mapsto \chi_p \in \mathrm{Hom}_{\mathrm{Grp}}(\mathrm{Gal}(L_{v_p}/\mathbb{Q}_p), \mathbb{Q}/\mathbb{Z})$ as $\mathrm{Gal}(L_{v_p}/\mathbb{Q}_p) \subset \mathrm{Gal}(L/\mathbb{Q})$. Then, by Lemma 5.9, $\mathrm{inv}_{L_{v_p}/\mathbb{Q}_p}(a \cup \delta\chi_p) = \delta_p(\mathrm{Art}_{L_{v_p}/\mathbb{Q}_p}(a))$. We want to show that $\sum_p \mathrm{inv}_{L_{v_p}/\mathbb{Q}_p}(a \cup \delta\chi_p) = 0$. For this, it suffices to show that $\prod_p \mathrm{Art}_{L_{v_p}/\mathbb{Q}_p}(a) = 1$ as an element of $\mathrm{Gal}(L/\mathbb{Q})$ (here, $\mathrm{Art}_{L_{v_p}/\mathbb{Q}_p}(a) \in \mathrm{Gal}(L_{v_p}/\mathbb{Q}_p) \subset \mathrm{Gal}(L/\mathbb{Q})$). Note that, by Proposition 5.8, the relative local reciprocity map is compatible under enlarging the larger field. As $L/\mathbb{Q}$ is cyclic, it is abelian, so by the Kronecker–Weber theorem (Theorem 8.1, which we already proved!), we may enlarge L and reduce to checking this when $L = \mathbb{Q}(\zeta_n)$ is a cyclotomic field.

By Theorem 10.15, we know explicitly what the Artin local reciprocity map is. Using this, we know an explicit recipe of what $\mathrm{Art}_{\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p}(a)$ is as an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong$

$(\mathbb{Z}/n\mathbb{Z})^\times$; if $a = p^{e_p}u$ for some $u \in \mathbb{Z}_p^\times$ and if $n = p^{f_p}m$ for $(p, m) = 1$, then $\mathrm{Art}_{\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p}(a) \in (\mathbb{Z}/n\mathbb{Z})^\times$ is the congruence class that is $\equiv p^{e_p} \pmod m$ and $\equiv u^{-1} \pmod{p^{f_p}}$.

Exercise 12.1. Convince yourself that this is the correct recipe.

We want to show that $\prod_p \mathrm{Art}_{\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p}(a) = 1$. As the left hand side is multiplicative in a, it suffices to show this when either $a = q$ is a prime number or $a = -1$. Let $n = \prod_{i=1}^k p_i^{f_i}$, and consider $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{f_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{e_k}\mathbb{Z})^\times$, and write a class in $(\mathbb{Z}/n\mathbb{Z})^\times$ as $(c_1, \cdots, c_k)$ in accordance with the decomposition. Then, if either $a = -1$ or $a = q$ for a prime number $q \neq p_1, \cdots, p_k$, we have

$$\mathrm{Art}_{\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p}(a) = \begin{cases} (1, 1, \cdots, \underbrace{a^{-1}}_{i\text{-th entry}}, \cdots, 1) & \text{if } p = p_i \\ (a, a, \cdots, a) & \text{if } p = a \text{ (in the case of } a = -1\text{, this is meant to be } p = \infty) \\ (1, 1, \cdots, 1) & \text{if } p \neq p_1, \cdots, p_k, a. \end{cases}$$

Thus, it is apparent that $\prod_p \mathrm{Art}_{\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p}(a) = 1$ in these cases. On the other hand, if $a = p_i$, then

$$\mathrm{Art}_{\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p}(p_i) = \begin{cases} (p_i, p_i, \cdots, \underbrace{1}_{i\text{-th entry}}, \cdots, p_i) & \text{if } p = p_i \\ (1, 1, \cdots, \underbrace{p_i^{-1}}_{j\text{-th entry}}, \cdots, 1) & \text{if } p = p_j,\ j \neq i \\ (1, 1, \cdots, 1) & \text{if } p \neq p_1, \cdots, p_k. \end{cases}$$

Thus, again $\prod_p \mathrm{Art}_{\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p}(p_i) = 1$ in these cases. These altogether proves the **"Global Invariant Zero"** for $L/\mathbb{Q}$ cyclic.

Step 3. Reducing the problem to an elementary number theory problem.

Now we want to prove that, for any finite Galois $L/\mathbb{Q}$ and $\alpha \in \mathrm{Br}(L/\mathbb{Q})$,

$$\sum_{p \text{ rational prime}} \mathrm{inv}_{L_v/\mathbb{Q}_p}(\alpha) = 0,$$

where v is chosen to be any place in L over p (here, a rational prime means either a prime number or ∞). As taking inflation does not change the local invariants, we may check this by possibly enlarging the field. Suppose that there is a cyclic field extension $M/\mathbb{Q}$ such that $\mathrm{Inf}(\alpha) \in \mathrm{Br}(ML/\mathbb{Q})$ satisfies that $\mathrm{Res}(\mathrm{Inf}(\alpha)) \in \mathrm{Br}(ML/M)$ is zero. Then, this means that $\mathrm{Inf}(\alpha) \in \ker(\mathrm{Res} : \mathrm{Br}(ML/\mathbb{Q}) \to \mathrm{Br}(ML/M))$. By the inflation-restriction, this is the same as $\mathrm{Inf}(\alpha) \in \mathrm{im}(\mathrm{Inf} : \mathrm{Br}(M/\mathbb{Q}) \to \mathrm{Br}(ML/\mathbb{Q}))$. As again the inflation does not change the local invariants, and as we have shown the **"Global Invariant Zero"** for M in Step 2, this will finish the **"Global Invariant Zero"** for α. Therefore, we will be done if we can find, for each $\alpha \in \mathrm{Br}(L/\mathbb{Q})$, a cyclic field extension $M/\mathbb{Q}$ such that $\mathrm{Res}(\mathrm{Inf}(\alpha)) = 0$ in $\mathrm{Br}(ML/M)$.

What do we concretely need for M? Note that $\operatorname{inv}_{L_v/\mathbb{Q}_p}(\alpha) \neq 0$ for finitely many places p of $\mathbb{Q}$ (p can be ∞). For such a place p, let d_p be the denominator of $\operatorname{inv}_{L_v/\mathbb{Q}_p}(\alpha)$. Suppose that $M/\mathbb{Q}$ is a cyclic extension such that, for each place p with $\operatorname{inv}_{L_v/\mathbb{Q}_p}(\alpha) \neq 0$, d_p divides $[M_w : \mathbb{Q}_p]$, where w is any place in M dividing p. We claim that this choice of M will satisfy $\operatorname{Res}(\operatorname{Inf}(\alpha)) = 0$ in $\operatorname{Br}(ML/M)$. To check this, note that by Corollary 12.13, $\operatorname{Br}(ML/M) \to \bigoplus_{w \text{ place of } M} \operatorname{Br}((ML)_{w'}/M_w)$ is injective, where for each place w of M, any place w' of ML above w is chosen. Therefore, it suffices to show that $\operatorname{inv}_{(ML)_{w'}/M_w}(\operatorname{Res}(\operatorname{Inf}(\alpha))) = 0$ for all places w of M. However, we know that

$$\operatorname{inv}_{(ML)_{w'}/M_w}(\operatorname{Res}(\operatorname{Inf}(\alpha))) = [M_w : \mathbb{Q}_p] \operatorname{inv}_{(ML)_{w'}/\mathbb{Q}_p}(\operatorname{Inf}(\alpha)) = [M_w : \mathbb{Q}_p] \operatorname{inv}_{L_v/\mathbb{Q}_p}(\alpha),$$

where w is the place of M that w'' divides, v is the place of L that w'' divides, and p is the place of $\mathbb{Q}$ that w'' divides. This is always zero, as either $\operatorname{inv}_{L_v/\mathbb{Q}_p}(\alpha) = 0$ or $[M_w : \mathbb{Q}_p] \operatorname{inv}_{L_v/\mathbb{Q}_p}(\alpha)$ is an integer (which is equivalent to zero mod 1). This implies that $\operatorname{Res}(\operatorname{Inf}(\alpha)) = 0$ if you find such an M.

Step 4. Finishing the proof.

Thus, the problem becomes an elementary number theory problem.

Lemma 12.16. *Let $p_1, \cdots, p_h$ be distinct places of $\mathbb{Q}$, and let $r_1, \cdots, r_h \in \mathbb{N}$ be integers, with the restriction that $r_i \in \{1, 2\}$ if $p_i = \infty$. Then, there exists a cyclic extension $M/\mathbb{Q}$ such that, for every $1 \leq i \leq h$ and every place v of M dividing p_i, $[M_v : \mathbb{Q}_{p_i}]$ is divisible by r_i.*

Proof. It is annoying to think about the infinite place, but the condition on the infinite place will be always satisfied if we find M which is totally complex (i.e. all archimedean embeddings are complex embeddings). So, we will assume that all $p_1, \cdots, p_h$ are finite prime numbers, and instead find M that is a totally complex number field. We may arrange p_i's so that $p_1 < \cdots < p_h$. Let $\operatorname{lcm}(r_1, \cdots, r_h) = \prod_{i=1}^{s} \ell_i^{\nu_i}$ be the prime factorization (so $\ell_1, \cdots, \ell_s$ are distinct primes). Note that, if p is a prime number and $(n, p) = 1$, then $[\mathbb{Q}_p(\zeta_n) : \mathbb{Q}_p] = \operatorname{ord}(p \pmod n)$, and in particular $\operatorname{ord}(p \pmod n) \geq \log_p(n)$.

Let $T > p_h$ be a big integer. For $1 \leq i \leq s$, let $x_i \geq \frac{\ell_i^{\nu_i}(\ell_i - 1)}{\log_T(\ell_i)}$ be a positive integer (i.e. $\log_T(\ell_i^{x_i}) \geq \ell_i^{\nu_i}(\ell_i - 1)$). Then, as $\operatorname{Gal}(\mathbb{Q}(\zeta_{\ell_i^{x_i}})/\mathbb{Q}) \cong (\mathbb{Z}/\ell_i^{x_i}\mathbb{Z})^\times \cong (\mathbb{Z}/\ell_i^{x_i-1}\mathbb{Z}) \times (\mathbb{Z}/(\ell_i - 1)\mathbb{Z})$, there is a cyclic subextension $\mathbb{Q}(\zeta_{\ell_i^{x_i}})/M_i/\mathbb{Q}$ such that $[M_i : \mathbb{Q}] = \ell_i^{x_i - 1}$ (there are many such cyclic extensions inside $\mathbb{Q}(\zeta_{\ell_i^{x_i}})$, and we just choose one). For $1 \leq j \leq h$, for any place v of M_i dividing p_j,

$$[(M_i)_v : \mathbb{Q}_{p_j}] \geq \frac{[\mathbb{Q}_{p_j}(\zeta_{\ell_i^{x_i}}) : \mathbb{Q}_{p_j}]}{\ell_i - 1} = \frac{\operatorname{ord}(p_j \pmod{\ell_i^{x_i}})}{\ell_i - 1} \geq \frac{\log_{p_j}(\ell_i^{x_i})}{\ell_i - 1} \geq \frac{\log_T(\ell_i^{x_i})}{\ell_i - 1} \geq \ell_i^{\nu_i}.$$

As $M_1, \cdots, M_s$ are cyclic extensions of $\mathbb{Q}$ with coprime degrees, their compositum $C = M_1 \cdots M_s$ is also cyclic. Furthermore, as each $[(M_i)_v, \mathbb{Q}_{p_j}]$ is a divisor of $[M_i : \mathbb{Q}]$, which is a power of ℓ_i, $[C_{v'} : \mathbb{Q}_{p_j}] = \prod_{i=1}^{s} [(M_i)_{v_i} : \mathbb{Q}_{p_j}]$ where $v', v_1, \cdots, v_s$ are places of

$C, M_1, \cdots, M_s$ dividing p_j. Therefore, for each $1 \leq j \leq h$, $[C_{v'} : \mathbb{Q}_{p_j}]$ is divisible by $\operatorname{lcm}(r_1, \cdots, r_h)$, so in particular by r_j.

Now the only issue is whether C is totally complex or not. If $\operatorname{lcm}(r_1, \cdots, r_h)$ is odd, then we may just take the compositum of C with $\mathbb{Q}(i)$ and get a totally complex cyclic extension satisfying the same properties (this works because $[C : \mathbb{Q}]$ is odd). If $\operatorname{lcm}(r_1, \cdots, r_h)$ is even, then by our convention $p_1 = 2$. Then, in the process of choosing M_1, it does not matter which maximal cyclic subextension of $\mathbb{Q}(\zeta_{2^{x_1}})$ we choose. We can in particular always make x_1 larger so that $x_1 \geq 3$, and take $M_1 = \mathbb{Q}(\zeta_{2^{x_1}} - \zeta_{2^{x_1}}^{-1})$. The claim is:

For any $N \geq 3$, $\mathbb{Q}(\zeta_{2^N} - \zeta_{2^N}^{-1})$ is a totally complex cyclic extension of $\mathbb{Q}$ of degree 2^{N-2}.

Let $F_1 = \mathbb{Q}(\zeta_{2^N})$ and $F_2 = \mathbb{Q}(\zeta_{2^N} - \zeta_{2^N}^{-1})$. We know that $\operatorname{Gal}(F_1/\mathbb{Q}) \cong (\mathbb{Z}/2^N\mathbb{Z})^\times$. We claim that $\operatorname{Gal}(F_1/F_2)$ is the order 2 subgroup generated by $2^{N-1}-1$; indeed $(2^{N-1}-1)^2 = 2^{2N-2} - 2^N + 1 \equiv 1 \pmod{2^N}$ as $2N-2 \geq N$. This is because the element $\sigma \in \operatorname{Gal}(F_1/\mathbb{Q})$ corresponding to $2^{N-1} - 1$ acts on $\xi := \zeta_{2^N} - \zeta_{2^N}^{-1}$ as

$$\sigma(\xi) = \zeta_{2^N}^{2^{N-1}-1} - \zeta_{2^N}^{-(2^{N-1}-1)} = \zeta_{2^N}^{2^{N-1}-1} - \zeta_{2^N}^{2^{N-1}+1} = -\zeta_{2^N}^{-1} + \zeta_{2^N} = \xi.$$

As $[F_1 : F_2] \leq 2$ (ζ_{2^N} is a root of a quadratic polynomial over F_2), this implies that $\operatorname{Gal}(F_1/F_2) = \langle 2^{N-1} - 1 \rangle$. Now among any archimedean embedding of F_1, you see that ξ is never a real number, so F_2 is a totally complex number field. Furthermore, let $H := \ker((\mathbb{Z}/2^N\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times)$, which is a cyclic group ($(\mathbb{Z}/2^N\mathbb{Z})^\times$ is not cyclic, but $(\mathbb{Z}/2^N\mathbb{Z})^\times \cong (\mathbb{Z}/2^{N-2}\mathbb{Z}) \times \{\pm 1\}$, so given any element $u \in (\mathbb{Z}/2^N\mathbb{Z})^\times$ of order 2^{N-2}, you may take $\pm u$ to make it an element of H). As $H \cdot \langle 2^{N-1} - 1 \rangle = (\mathbb{Z}/2^N\mathbb{Z})^\times$ (as $2^{N-1} - 1 \equiv -1 \pmod 4$), this implies that $H \hookrightarrow (\mathbb{Z}/2^N\mathbb{Z})^\times \twoheadrightarrow \frac{(\mathbb{Z}/2^N\mathbb{Z})^\times}{\langle 2^{N-1}-1 \rangle} = \operatorname{Gal}(F_2/\mathbb{Q})$ is an isomorphism, so $F_2/\mathbb{Q}$ is cyclic. Thus, by taking M_1 as above, we can guarantee that C is totally complex if $\operatorname{lcm}(r_1, \cdots, r_h)$ is even. This finishes the proof. □

Thus we are done! □

Remark 12.17. In the above proof, we did not actually need the Kronecker–Weber theorem in Step 2, because the extension M constructed in Step 4 is a cyclic extension which is a subextension of a cyclotomic field. So proving $L/\mathbb{Q}$ for cyclic extension which is a subextension of a cyclotomic field in Step 2 is enough.

Corollary 12.18. *The pair $F = \mathbb{Q}$ and $A = C$ is a class formation. Therefore, the global Artin reciprocity (Theorem 7.1) holds.*

Proof. We proved the **First Inequality** (Corollary 12.12), the **Second Inequality** (Corollary 11.21), and the **"Big Regular Part"** (Theorem 12.14 + Theorem 12.15). Therefore Lemma 12.3 gives you the verification of class formation axioms.

Now that we know $(\mathbb{Q}, C)$ is a class formation, we can use Lemma 5.9 to also establish the local-global compatibility, because the invariant of an idele class is by construction the sum of the local invariants of its local components. □

Corollary 12.19 (Fundamental Exact Sequence)**.** *The maps in "**Global Invariant Zero**" form short exact sequences, i.e.*

$$0 \to \mathrm{Br}(K) \to \bigoplus_{v \text{ places of } K} \mathrm{Br}(K_v) \xrightarrow{\oplus_v \mathrm{inv}_{K_v}} \mathbb{Q}/\mathbb{Z} \to 0,$$

$$0 \to \mathrm{Br}(L/K) \to \bigoplus_{v \text{ places of } K} \mathrm{Br}(L_w/K_v) \xrightarrow{\oplus_v \mathrm{inv}_{L_w/K_v}} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \to 0,$$

are exact.

Proof. The proof of Lemma 12.3 show that the sum of local invariants map gives you an identification of the cokernel of the global Brauer group with the direct sum of local Brauer groups. Thus we get the result. □

12.4. **Global existence theorem.** Thus, we only need to show the global existence theorem (Theorem 7.5), for which we need to show (*).

Proof of the global existence theorem, Theorem 7.5. As we know, we need to show the statement (*): for a number field K and an open subgroup $U \leq C_K$ of finite index, there exists a finite extension L/K such that $N_{L/K}(C_L) \leq U$. We will show (*) by induction on the number of divisors of $[C_K : U]$.

There is nothing to prove if $[C_K : U] = 1$ (take $L = K$), so the base cases are when $[C_K : U]$ is a prime number. Before proving the base cases, let us first explain the induction step. Suppose that we have K and $U \leq C_K$ with $[C_K : U] = N$ which has D divisors, and suppose we know (*) for any K' and $U' \leq C_{K'}$ with the number of divisors of $[C_{K'} : U']$ less than D. If N is a prime, this is a base case. If not, then you can find a subgroup $U \lneq V \lneq C_K$. By the induction hypothesis, $V \supset N_{L/K}(C_L)$ for some finite extension L/K. Let $N := N_{L/K}(C_L)$. Take $W = N_{L/K}^{-1}(N \cap U) \subset C_L$. Then,

$$[C_L : W] = [N : N \cap U] = [UN : U],$$

which clearly divides $[V : U]$. Therefore, by the induction hypothesis, there exists a finite extension M/L such that $W \supset N_{M/L}(C_M)$. Then,

$$U \supset N \cap U = N_{L/K}(W) \supset N_{L/K}(N_{M/L}(C_M)) = N_{M/K}(C_M),$$

as desired.

Thus, we only need to prove (*) for the base cases when $[C_K : U] = p$ is a prime number. One observation is that we can always enlarge the field K. Suppose there is a counterxample to (*) for the prime index case so that there is $[C_K : U] = p$ where U does not contain any $N_{L/K}(C_L)$. Then, for any L/K, if we take $U' := N_{L/K}^{-1}(U \cap N_{L/K}(C_L))$, then by the similar computations as above, $[C_L : U'] = [UN_{L/K}(C_L) : U]$ which divides $[C_K : U] = p$, so it is either p or 1. However, as U does not contain $N_{L/K}(C_L)$, $UN_{L/K}(C_L) \neq U$, so $[C_L : U'] = p$. If L and U' is not a counterexample to (*), then there exists M/L such that $N_{M/L}(C_M) \subset U'$, which means

$$N_{M/K}(C_M) = N_{L/K}(N_{M/L}(C_M)) \subset N_{L/K}(U') = U \cap N_{L/K}(C_L) \subset U,$$

which contradicts with the assumption that K and U give rise to a counterexample. Using this observation, we may reduce the problem to the cases where $K \supset \mathbb{Q}(\zeta_p)$.

Now we only need to prove (*) for $[C_K : U] = p$ a prime number and $K \supset \mathbb{Q}(\zeta_p)$. By Lemma 12.6, we may find a finite set S of places of K, containing all infinite places of K, such that $I_K = K^\times I_{K,S}$. We may always enlarge S such that S also contains all places of K above p. Let $J \subset I_K$ be the preimage of $U \leq C_K$ under the projection $I_K \twoheadrightarrow C_K$. Then, as $J \leq I_K$ is open, by possibly enlarging S, we may ensure that J contains a subgroup of the form $\prod_{v \in S}\{1\} \times \prod_{v \notin S} \mathcal{O}_{K_v}^\times$. Moreover, as $J \subset I_K$ is of index p, $I_K^p \subset J$. This implies that, for any place v of K, $(K_v^\times)^p \subset J$. This implies that

$$J \supset W_S := \prod_{v \in S}(K_v^\times)^p \times \prod_{v \notin S} \mathcal{O}_{K_v}^\times.$$

Note that, as $K \supset \mathbb{Q}(\zeta_p)$, by the Dirichlet's theorem for S-units (Theorem 12.9), $\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^p \cong (\mathbb{Z}/p\mathbb{Z})^{\#S}$. Therefore, if we define L to be obtained from K by adjoining all p-th roots of $u \in \mathcal{O}_{K,S}^\times$, then $[L : K] = p^s$ and L/K is Galois (because $K \subset \mathbb{Q}(\zeta_p)$). More concretely, if $u_1, \cdots, u_{\#S-1}$ is a fundamental system of S-units, then $L = K(\zeta_{p^N}, u^{1/p}, \cdots, u_{\#S-1}^{1/p})$ for some $N > 0$ (so that $\zeta_{p^{N-1}} = \zeta_{p^N}^p \in K$). By the global Artin reciprocity (Theorem 7.1), $C_K/N_{L/K}(C_L) \cong (\mathbb{Z}/p\mathbb{Z})^{\#S}$.

We claim that $N_{L/K}(I_L) \supset W_S$. To show this, we need to show that, for $v \in S$, $(K_v^\times)^p \leq N_{L/K}(I_L)$, and for $v \notin S$, $\mathcal{O}_{K_v}^\times \subset N_{L/K}(I_L)$.

- For $v \in S$: note that for any place w of L over v, $N_{L_w/K_v}(L_w^\times) \subset N_{L/K}(I_L)$. By the local Artin reciprocity (Theorem 2.1), $K_v^\times/N_{L_w/K_v}(L_w^\times) \cong \mathrm{Gal}(L_w/K_v)$ (L/K is abelian to start with). As $\mathrm{Gal}(L_w/K_v)$ is a subgroup of $\mathrm{Gal}(L/K)$, $\mathrm{Gal}(L_w/K_v)$ has exponent p. Therefore, $(K_v^\times)^p \subset N_{L_w/K_v}(L_w^\times) \subset N_{L/K}(I_L)$.

- For $v \notin S$: note that v is unramified in L. This is because $\mathrm{disc}(L/K)$ divides the discriminant computed using a power basis of $\zeta_{p^N}, u_1^{1/p}, \cdots, u_{\#S-1}^{1/p}$, which divides a product of powers of discriminants computed using $\{1, \cdots, \zeta_{p^N}^{p-1}\}$, $\{1, \cdots, u_1^{(p-1)/p}\}, \cdots, \{1, \cdots, u_{\#S-1}^{(p-1)/p}\}$, respectively, and each such discriminant has prime ideal factors of those in S because u_i's are S-units (namely, $\mathrm{disc}(1, \cdots, u_i^{(p-1)/p}) = \pm N_{L/\mathbb{Q}}(pu_i^{(p-1)/p})$, and S contains all primes dividing p). This implies that, for $v \notin S$, $\mathcal{O}_{K_v}^\times \subset N_{L/K}(I_L)$ by Proposition 1.2.

These imply that $N_{L/K}(I_L) \supset W_S$, so in particular $N_{L/K}(C_L) \supset K^\times W_S/K^\times$. Note that $N_{L/K}(C_L)$ is of index $p^{\#S}$ inside C_K. We claim that $[C_K : K^\times W_S/K^\times] = p^{\#S}$, which will show that $N_{L/K}(C_L) = K^\times W_S/K^\times$. This will imply that $N_{L/K}(C_L) = K^\times W_S/K^\times \subset K^\times J/K^\times = U$, proving the base cases for (*).

Thus our only remaining task is to prove that $[C_K : K^\times W_S/K^\times] = p^{\#S}$. From the exact sequence $1 \to \mathcal{O}_{K,S}^\times \to I_{K,S} \to C_K \to 1$, and as $W_S \subset I_{K,S}$, we have a short exact sequence

$$1 \to \frac{\mathcal{O}_{K,S}^\times}{\mathcal{O}_{K,S}^\times \cap W_S} \to \frac{I_{K,S}}{W_S} \to \frac{C_K}{K^\times W_S/K^\times} \to 1.$$

So we can compute $[C_K : K^\times W_S/K^\times]$ by computing the orders of the other two groups in the short exact sequence.

- For $\#\frac{\mathcal{O}_{K,S}^\times}{\mathcal{O}_{K,S}^\times \cap W_S}$: I claim that $\mathcal{O}_{K,S}^\times \cap W_S = (\mathcal{O}_{K,S}^\times)^p$. This will show that

$$\frac{\mathcal{O}_{K,S}^\times}{\mathcal{O}_{K,S}^\times \cap W_S} = \frac{\mathcal{O}_{K,S}^\times}{(\mathcal{O}_{K,S}^\times)^p} \cong (\mathbb{Z}/p\mathbb{Z})^{\#S},$$

  so that $[\mathcal{O}_{K,S}^\times : \mathcal{O}_{K,S}^\times \cap W_S] = p^{\#S}$.

  One inclusion is clear; it is obvious that $(\mathcal{O}_{K,S}^\times)^p \subset \mathcal{O}_{K,S}^\times \cap W_S$. Conversely, if $y \in \mathcal{O}_{K,S}^\times \cap W_S$, I claim that y is a global p-th power (if so, its p-th root will necessarily be an element of $\mathcal{O}_{K,S}^\times$). This is the same as showing $K(y^{1/p}) = K$. Let $L = K(y^{1/p})$. Then, L/K is Galois (as $K \supset \mathbb{Q}(\zeta_p)$), every place $v \in S$ splits completely in L, and every place $v \notin S$ is unramified in L (because every place over p is already contained in S). Let T be the set of all places of L over S. Then, by Proposition 1.2, $N_{L/K}(I_{L,T}) = I_{K,S}$. As $I_{K,S} \to C_K$ is surjective, this implies that $N_{L/K}(C_L) = C_K$. By the local Artin reciprocity (Theorem 2.1), this implies that $L = K$, as desired.

- For $\#\frac{I_{K,S}}{W_S}$: note that quite obviously

$$\frac{I_{K,S}}{W_S} = \frac{\prod_{v\in S} K_v^\times \times \prod_{v\notin S} \mathcal{O}_{K_v}^\times}{\prod_{v\in S}(K_v^\times)^p \times \prod_{v\notin S}\mathcal{O}_{K_v}^\times} = \prod_{v\in S}\frac{K_v^\times}{(K_v^\times)^p}.$$

  I claim that $[K_v^\times : (K_v^\times)^p] = \frac{p^2}{|p|_v}$.

  - If v is real, then $K \supset \mathbb{Q}(\zeta_p)$ means that this is possible only if $p = 2$. Then $[K_v^\times : (K_v^\times)^p] = [\mathbb{R}^\times/(\mathbb{R}^\times)^2] = 2 = \frac{2^2}{|2|_v}$.
  - If v is complex, then $[K_v^\times : (K_v^\times)^p] = [\mathbb{C}^\times : (\mathbb{C}^\times)^p] = 1 = \frac{p^2}{|p|_v}$.
  - If v is a finite place not above p, then note that $K_v^\times \cong \pi_v^{\mathbb{Z}} \times (\mathcal{O}_{K_v}/(\pi_v))^\times \times (1+\pi_v\mathcal{O}_{K_v})$, where $\pi_v \in K_v$ is a uniformizer. As $1+\pi_v\mathcal{O}_{K_v}$ is pro-ℓ, where $\ell \in \mathbb{Z}$ a prime number which v divides, $1+\pi_v\mathcal{O}_{K_v} = (1+\pi_v\mathcal{O}_{K_v})^p$. Furthermore, as $\zeta_p \in K_v$, this implies that $p|\ell - 1$, and $\frac{(\mathcal{O}_{K_v}/(\pi_v))^\times}{((\mathcal{O}_{K_v}/(\pi_v))^\times)^p} \cong \mathbb{Z}/p\mathbb{Z}$. Therefore, $[K_v^\times : (K_v^\times)^p] = p^2 = \frac{p^2}{|p|_v}$.
  - If v is a finite place above p, let $e = e(K_v/\mathbb{Q}_p)$ and $f = f(K_v/\mathbb{Q}_p)$. Then $\frac{1+\pi_v\mathcal{O}_{K_v}}{(1+\pi_v\mathcal{O}_{K_v})^p} = \frac{\pi_v\mathcal{O}_{K_v}}{p\pi_v\mathcal{O}_{K_v}} \cong \mathcal{O}_{K_v}/p\mathcal{O}_{K_v}$, so $[1+\pi_v\mathcal{O}_{K_v} : (1+\pi_v\mathcal{O}_{K_v})^p] = \#(\mathcal{O}_{K_v}/p\mathcal{O}_{K_v}) = p^{ef}$. Moreover, $(\mathcal{O}_{K_v}/(\pi_v))^\times = \mathbb{F}_{p^f}^\times$, and as $\zeta_p \in K$, this implies that $f \geq 2$. Therefore, $\mathbb{F}_{p^f}^\times/(\mathbb{F}_{p^f}^\times)^p \cong \mathbb{Z}/p\mathbb{Z}$. Therefore, $[K_v^\times : (K_v^\times)^p] = p^{ef+2}$. Note on the other hand that $\frac{p^2}{|p|_v} = \frac{p^2}{|\pi_v|_v^e} = \frac{p^2}{p^{-ef}} = p^{ef+2}$, so they are the same.

  This implies that

$$[I_{K,S} : W_S] = \prod_{v\in S}\frac{p^2}{|p|_v} = \frac{p^{2\#S}}{\prod_{v\in S}|p|_v} = p^{2\#S},$$

  as S contains all places of K above p.

Thus

$$[C_K : K^\times W_S/K^\times] = \frac{[I_{K,S} : W_S]}{[\mathcal{O}_{K,S}^\times : \mathcal{O}_{K,S}^\times \cap W_S]} = \frac{p^{2\#S}}{p^{\#S}} = p^{\#S},$$

and we are done! □

This concludes the proof of the global class field theory. Before we move on to the next topic, we record the Galois analogue of Theorem 11.15, and a generalization of Proposition 11.18: Chebotarev density theorem!

Theorem 12.20 (Chebotarev density theorem). *Let L/K be a finite Galois extension of number fields, and let $\mathcal{C} \subset \mathrm{Gal}(L/K)$ be a conjugacy class. Then, the set of prime ideals $\mathfrak{p}$ of K such that $\mathfrak{p}$ is unramified in L and $\mathrm{Fr}_\mathfrak{p} = \mathcal{C}$ has Dirichlet density $\frac{|\mathcal{C}|}{|\mathrm{Gal}(L/K)|}$ in the set of all prime ideals of K.*

Proof. If L/K is abelian, then this is literally Theorem 11.15; namely, we choose a modulus $\mathfrak{m}$ such that $K(\mathfrak{m}) \supset L$, and then this set is (up to a finite difference) the set of prime ideals of K whose class in $\mathrm{Cl}^\mathfrak{m}(K)$ lands in $\mathcal{C} + H$ where $H \leq \mathrm{Cl}^\mathfrak{m}(K)$ corresponds to $\mathrm{Cl}^\mathfrak{m}(K)/H \cong C_K/N_{L/K}(C_L) \cong \mathrm{Gal}(L/K)$. This has density, by Theorem 11.15, $\frac{1}{[\mathrm{Cl}^\mathfrak{m}(K):H]} = \frac{1}{|\mathrm{Gal}(L/K)|}$ (note that $\mathcal{C}$ is a singleton if L/K is abelian).

In general, let $\sigma \in \mathcal{C}$, and let $M = L^{\langle\sigma\rangle}$. Then L/M is a cyclic extension of order f, where f is the order of σ. Now we set several sets of primes.

- Let T be the set of prime ideals $\mathfrak{p}$ of K such that $\mathfrak{p}$ is unramified in L and $\mathrm{Fr}_\mathfrak{p} = \mathcal{C}$ in $\mathrm{Gal}(L/K)$.

- Let T' be the set of prime ideals $\mathfrak{q}$ of M such that $\mathfrak{q}$ is unramified in L, $\mathrm{Fr}_\mathfrak{q} = \sigma$ in $\mathrm{Gal}(L/M)$ and $f(\mathfrak{q}|\mathfrak{q} \cap \mathcal{O}_K) = 1$. By the abelian case as done above, the Dirichlet density of T' is $\frac{1}{f}$.

- Let T'' be the set of prime ideals $\mathfrak{P}$ of L such that $\mathfrak{P}$ is unramified over K and $\mathrm{Fr}_\mathfrak{P} = \sigma$ in $\mathrm{Gal}(L/K)$.

Note that $T'' \to T'$, $\mathfrak{P} \mapsto \mathfrak{P} \cap \mathcal{O}_M$, is a well-defined map, as $f(\mathfrak{P}|\mathfrak{P} \cap \mathcal{O}_K) = f = f(\mathfrak{P}|\mathfrak{P} \cap \mathcal{O}_M)$ which implies that $f(\mathfrak{P} \cap \mathcal{O}_M|\mathfrak{P} \cap \mathcal{O}_K) = 1$. We claim that $T'' \to T'$ is injective and its image misses only finitely many primes of T'. It is injective because $f(\mathfrak{P}|\mathfrak{P} \cap \mathcal{O}_M) = f$ implies that $\mathfrak{P} \cap \mathcal{O}_M$ is inert in L, so that $\mathfrak{P}$ is the only prime in L above $\mathfrak{P} \cap \mathcal{O}_M$. Furthermore, if $\mathfrak{q} \in T'$ is such that $\mathfrak{q}$ is unramified over K, then the order of σ being f means $\mathfrak{q}$ is inert in L, so we take $\mathfrak{P}$ of L lying over $\mathfrak{q}$, then $\mathrm{Fr}_\mathfrak{P}$ in $\mathrm{Gal}(L/M)$ is $\mathrm{Fr}_\mathfrak{P}$ in $\mathrm{Gal}(L/K)$ raised to the power of $f(\mathfrak{P}|\mathfrak{q}) = 1$, which means $\mathrm{Fr}_\mathfrak{P}$ in $\mathrm{Gal}(L/K)$ is just σ. Note that for $\mathfrak{P} \in T''$, $N(\mathfrak{P}) = N(\mathfrak{P} \cap \mathcal{O}_M)^f$, so

$$\sum_{\mathfrak{P} \in T''} \frac{1}{N(\mathfrak{P})^{s/f}} - \frac{1}{f} \log\left(\frac{1}{s-1}\right)$$

is bounded as $s \to 1$ from the right.

We now construct another map $T'' \to T$, $\mathfrak{P} \mapsto \mathfrak{P} \cap \mathcal{O}_K$. Note that it is quite obviously surjective, and each element in T is hit by exactly $\frac{[L:K]}{f|C|}$ elements in T'' (there are $\frac{[L:K]}{f}$ primes in L above a prime in T). Again, for $\mathfrak{P} \in T''$, $N(\mathfrak{P}) = N(\mathfrak{P} \cap \mathcal{O}_K)^f$, so

$$\frac{[L:K]}{f|C|}\sum_{\mathfrak{p}\in T}\frac{1}{N(\mathfrak{p})^s} = \sum_{\mathfrak{P}\in T''}\frac{1}{N(\mathfrak{P})^{s/f}}.$$

Therefore,

$$\sum_{\mathfrak{p}\in T}\frac{1}{N(\mathfrak{p})^s} - \frac{|C|}{[L:K]}\log\left(\frac{1}{s-1}\right),$$

is bounded as $s \to 1$ from the right. This is exactly what we wanted. □

Corollary 12.21. *Let K be a number field, and let $L_1, L_2/K$ be finite extensions of K. Let $\mathcal{S}(L_i/K)$ be the set of primes of K that split completely in L_i. Suppose that L_1 is Galois over K.*

(1) Then, $L_1 \subset L_2$ if and only if $\mathcal{S}(L_1/K)$ contains $\overline{\mathcal{S}}(L_2/K) - S$ for a finite subset $S \subset \overline{\mathcal{S}}(L_2/K)$, where $\overline{\mathcal{S}}(L_2/K)$ is the set of prime ideals $\mathfrak{p}$ of K such that $\mathfrak{p}$ is unramified in L_2 and $f(\mathfrak{q}|\mathfrak{p}) = 1$ for some prime ideal $\mathfrak{p}$ of L_2 lying over K.

(2) Then, $L_2 \subset L_1$ if and only if $\mathcal{S}(L_2/K)$ contains $\mathcal{S}(L_1/K) - S$ for a finite subset $S \subset \mathcal{S}(L_1/K)$.

Proof. (1) The forward direction is obvious. For the reverse direction, let N be a Galois extension of K containing both L_1 and L_2. We want to show that $\mathrm{Gal}(N/L_2) \subset \mathrm{Gal}(N/L_1)$. Let $\sigma \in \mathrm{Gal}(N/L_2)$. Let $\mathfrak{p}$ be a prime ideal of K unramified in N such that $\mathrm{Fr}_\mathfrak{p}$ in $\mathrm{Gal}(N/K)$ is the conjugacy class of σ. Let $\mathfrak{P}$ be a prime of N such that $\mathrm{Fr}_\mathfrak{P} = \sigma$ in $\mathrm{Gal}(N/K)$. Let $\mathfrak{P}' = \mathfrak{P} \cap \mathcal{O}_{L_2}$. Then, for $\alpha \in \mathcal{O}_{L_2}$, $\alpha = \sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}'}$. Therefore, $f(\mathfrak{P}'|\mathfrak{p}) = 1$. Therefore, $\mathfrak{p} \in \overline{\mathcal{S}}(L_2/K)$. Therefore, there are infinitely many primes $\mathfrak{p}$ of K unramified in N such that $\mathrm{Fr}_\mathfrak{p}$ in $\mathrm{Gal}(N/K)$ is the conjugacy class of σ such that it splits completely in L_1. We choose such $\mathfrak{p}$. Then let $\mathfrak{P}$ be a prime of N lying over such $\mathfrak{p}$ such that $\mathrm{Fr}_\mathfrak{P} = \sigma$ in $\mathrm{Gal}(N/K)$. Then $\mathrm{Fr}_{\mathfrak{P}\cap\mathcal{O}_{L_1}} = \sigma|_{L_1}$ in $\mathrm{Gal}(L_1/K)$. However as $\mathfrak{p}$ splits completely in L_1, $\sigma|_{L_1} = 1$. Therefore, $\sigma \in \mathrm{Gal}(N/L_1)$, for any $\sigma \in \mathrm{Gal}(N/L_2)$, which implies that $L_1 \subset L_2$.

(2) The forward direction is obvious. For the reverse direction, let N be the Galois closure of L_2. Then $\mathcal{S}(N/K) = \mathcal{S}(L_2/K)$. Note that $\overline{\mathcal{S}}(L_1/K) = \mathcal{S}(L_1/K)$. Therefore this case is (1) for $L_1 = N$ and $L_2 = L_1$. This implies that $N \subset L_1$, which implies $L_2 \subset L_1$.

□

Part 2. The theory of complex multiplication

All instances of **Explicit class field theory** we have seen so far are all of the form as, given a field K, describing K^{ab} by adjoining explicit elements. Furthermore, these explicit elements have been torsion elements in some group where the multiplication law is given by some explicit polynomial/power series. Furthermore, the group had a large endomorphism ring containing $\mathcal{O}_K$, so that it becomes an $\mathcal{O}_K$-module. We will show that a similar story exists when K is an imaginary quadratic field, where the corresponding group is given by a so-called "**elliptic curve with complex multiplication**". As this course does not assume a prior knowledge of algebraic geometry, we try to develop the theory as elementarily as possible.

13. Lattices in $\mathbb{C}$ (or, in other words, elliptic curves over $\mathbb{C}$)

13.1. Elliptic functions for lattices in $\mathbb{C}$ (=elliptic curves over $\mathbb{C}$).

Definition 13.1 (Lattices in $\mathbb{C}$ = elliptic curves over $\mathbb{C}$)**.** A **lattice** (or an **elliptic curve over** $\mathbb{C}$) $\Lambda \subset \mathbb{C}$ is a free rank 2 abelian subgroup which discretely sits inside $\mathbb{C}$ (i.e. the subspace topology on Λ given by $\Lambda \subset \mathbb{C}$ is the discrete topology). A **fundamental parallelogram** of Λ is a parallelogram formed by $z, z+\omega_1, z+\omega_2, z+\omega_1+\omega_2$ for some $z \in \mathbb{C}$ and a $\mathbb{Z}$-basis $\omega_1, \omega_2 \in \Lambda$ (Warning: there are many fundamental parallelograms for a given lattice).

Two lattices (=elliptic curves over $\mathbb{C}$) $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ are **isomorphic** if there exists a complex number $c \in \mathbb{C}^\times$ such that $\Lambda_2 = c\Lambda_1$. An **isogeny** between two lattices (=elliptic curves over $\mathbb{C}$) $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ is a homomorphism $f : \Lambda_1 \to \Lambda_2$ where there is $c \in \mathbb{C}^\times$ such that $f(x) = cx$. The **degree** of an isogeny $f : \Lambda_1 \to \Lambda_2$ is $\deg f := \#\operatorname{coker} f$. Given two lattices (=elliptic curves over $\mathbb{C}$) $\Lambda_1, \Lambda_2 \subset \mathbb{C}$, let

$$\operatorname{Hom}(\Lambda_1, \Lambda_2) := \{\text{isogenies } \Lambda_1 \to \Lambda_2\} \cup \{0\}.$$

It is easy to check that the addition of complex numbers gives an additive abelian group structure on $\operatorname{Hom}(\Lambda_1, \Lambda_2)$. Two lattices (=elliptic curves over $\mathbb{C}$) $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ are called **isogenous** if there is an isogeny from Λ_1 to Λ_2, i.e. if $\operatorname{Hom}(\Lambda_1, \Lambda_2) \neq 0$.

For a lattice (=elliptic curve over $\mathbb{C}$) $\Lambda \subset \mathbb{C}$, $\operatorname{End}(\Lambda) := \operatorname{Hom}(\Lambda, \Lambda)$ further has a commutative ring structure, where the multiplication is given by the multiplication of complex numbers, or equivalently, the composition of isogenies. Given $f \in \operatorname{End}(\Lambda)$, we define $\deg f := \#\operatorname{coker} f$ (and $\deg 0 = 0$). This defines a multiplicative homomorphism $\deg : \operatorname{End}(\Lambda) \to \mathbb{Z}_{\geq 0}$. It is easy to see that, if $f(x) = cx$ for $c \in \mathbb{C}^\times$, then $\deg f = |c|^2$.

Example 13.2.

(1) If $\Lambda \subset \mathbb{C}$ is any lattice (=elliptic curve over $\mathbb{C}$), for $n \in \mathbb{N}$, there is an isogeny $[n] : \Lambda \to \Lambda$ given by $[n](x) = nx$. Its degree is $\deg[n] = n^2$. This implies that there is a natural ring homomorphism $\mathbb{Z} \xrightarrow{n \mapsto [n]} \operatorname{End}(\Lambda)$.

(2) Let K be an imaginary quadratic field, and choose an embedding $\iota : K \hookrightarrow \mathbb{C}$. Then $\iota(\mathcal{O}_K) \subset \mathbb{C}$ is a lattice (=elliptic curve over $\mathbb{C}$). For each $\alpha \in \mathcal{O}_K \backslash \{0\}$, there is an isogeny $[\alpha] : \iota(\mathcal{O}_K) \to \iota(\mathcal{O}_K)$ given by $[\alpha](\iota(x)) = \iota(\alpha)\iota(x)$. Its degree is $\deg[\alpha] = N_{K/\mathbb{Q}}(\alpha)$. This implies that there is a natural ring homomorphism $\mathcal{O}_K \xrightarrow{\alpha \mapsto [\alpha]} \operatorname{End}(\iota(\mathcal{O}_K))$.

We want to classify lattices in $\mathbb{C}$ (=elliptic curves over $\mathbb{C}$) up to isomorphism. Let $\Lambda \subset \mathbb{C}$ be a lattice (=elliptic curve over $\mathbb{C}$), and choose a basis $v_1, v_2 \in \Lambda$. Then, we can multiply Λ with v_1^{-1} so that $v_1 = 1$. We may thus assume that $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$ for some $\tau \in \mathbb{C}$. The requirement of Λ being a lattice means that $\tau \notin \mathbb{R}$ (Exercise: check this). Furthermore, by possibly replacing τ

with $-\tau$, we may only consider $\tau \in \mathbb{C}$ with $\mathrm{Im}(\tau) > 0$. Let $\mathbb{H} = \{\tau \in \mathbb{C} \ : \ \mathrm{Im}(\tau) > 0\}$, which is called the **upper half plane**. The observation so far means that the map of sets

$$\mathbb{H} \to \{\text{lattices in } \mathbb{C} \text{ (=elliptic curves over } \mathbb{C})\}/\text{isomorphisms}, \quad \tau \mapsto \mathbb{Z} \oplus \mathbb{Z}\tau,$$

is surjective. What are the fibers of this map?

Proposition 13.3. *Let* $\mathrm{SL}_2(\mathbb{Z})$ *be the group of* 2×2 *matrices with integer entries with determinant* 1*. There is an action of* $\mathrm{SL}_2(\mathbb{Z})$ *on* $\mathbb{H}$ *given by*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau := \frac{a\tau + b}{c\tau + d}.$$

Furthermore, for $\tau_1, \tau_2 \in \mathbb{C}$*, two lattices (=elliptic curves over* $\mathbb{C}$*)* $\mathbb{Z} \oplus \mathbb{Z}\tau_1, \mathbb{Z} \oplus \mathbb{Z}\tau_2 \subset \mathbb{C}$ *are isomorphic if and only if there exists* $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ *such that* $\tau_1 = \gamma \cdot \tau_2$*.*

Proof. See the proof of [ANT, Theorem 10.22]. The calculations in *loc. cit.* carry over in our setup in the same way. □

So we know that we have an isomorphism of sets,

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \xrightarrow{\sim} \{\text{lattices in } \mathbb{C} \text{ (=elliptic curves over } \mathbb{C})\}/\text{isomorphisms}, \quad \tau \mapsto \mathbb{Z} \oplus \mathbb{Z}\tau.$$

This is nice, but the set $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is still a bit mysterious, so it will be desirable to have more structures.

Remark 13.4. One way to proceed is to realize $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ as a **Riemann surface**, which in fact has a complex algebraic structure whose defining equations can be taken even over $\mathbb{Q}$[15]. Such a Riemann surface obtained in this way is called a **modular curve**. As, again, we do not assume algebraic geometry in this course, we use a different perspective.

Another remark is that one can always move a chosen $\tau \in \mathbb{H}$ by the action of $\mathrm{SL}_2(\mathbb{Z})$ so that you find a unique representative in the **fundamental domain**

$$\mathcal{F} = \{z \in \mathbb{H} \ : \ -1/2 \leq \mathrm{Re}(z) \leq 1/2 \text{ and } |z| \geq 1, \text{ and if } \mathrm{Re}(z) > 0, |z| > 1\}.$$

Namely, for any $\tau \in \mathbb{H}$, $\mathrm{SL}_2(\mathbb{Z})\tau \cap \mathcal{F}$ is a singleton. For the proof, see [ANT, Theorem 10.28]. This is also useful for other purposes (see [ANT, §10] for example).

There is a holomorphic function $j : \mathbb{H} \to \mathbb{C}$ such that $j(\tau_1) = j(\tau_2)$ if and only if τ_1, τ_2 give rise to the isomorphic lattices (=elliptic curves over $\mathbb{C}$), and this specific function is called the j**-function**. Along the way, we will also see a hint of how to really see $\mathbb{C}$ modulo a lattice as an algebraic curve[16], i.e. the graph of a polynomial equation in two variables.

[15] In general, given a complex algebraic structure, there are a lot of ways to find its defining equations over $\mathbb{Q}$ (if there is one). Namely, for example, the algebraic sets of points $\{(x, y) \in \mathbb{C}^2 \ : \ y = 2x^2\}$ and $\{(x, y) \in \mathbb{C}^2 \ : \ y = x^2\}$ are "isomorphic over $\mathbb{C}$" because you get $y = 2x^2$ from $y = x^2$ after putting $\sqrt{2}x \mapsto x$, but they are "not isomorphic over $\mathbb{Q}$" because this substitution $\sqrt{2}x \mapsto x$ is not allowed in the realm of $\mathbb{Q}$-coefficients. In fact, however, the modular curve has in some sense a "canonical" way of being defined over $\mathbb{Q}$, called the **canonical model**, and this notion is very much related to the Main Theorem of complex multiplication we will see in a moment.

[16] The terminology of "curve" may be confusing. We are following the calculus-like

Definition 13.5 (Weierstrass $\wp$-function)**.** Let $\Lambda \subset \mathbb{C}$ be a lattice (=elliptic curve over $\mathbb{C}$). Then, for $z \notin \Lambda$, we define the **Weierstrass $\wp$-function**

$$\wp(z) := \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right).$$

Lemma 13.6. *For a lattice $\Lambda \subset \mathbb{C}$ (=elliptic curve over $\mathbb{C}$), $\wp(z)$ defines a meromorphic function in $\mathbb{C}$ where the poles are at $z \in \Lambda$, where all the poles are of order 2. Furthermore, $\wp(z)$ is periodic for the translation by any element in Λ, i.e. $\wp(z) = \wp(z+\lambda)$ for any $\lambda \in \Lambda$.*

Similarly, its derivative $\wp'(z) = -2\sum_{\lambda \in \Lambda} \frac{1}{(z-\lambda)^3}$ is a meromorphic function in $\mathbb{C}$ where the poles are at $z \in \Lambda$ (all the poles are of order 3), periodic for the translation by any element in Λ, i.e. $\wp'(z) = \wp'(z+\lambda)$ for any $\lambda \in \Lambda$.

Proof. It is easy to see that the infinite sum converges uniformly absolutely on any compact set away from Λ, so it defines a holomorphic function on $\mathbb{C}\setminus\Lambda$. It also has order 2 poles at every $z \in \Lambda$ as the infinite sum defining $\wp(z) - \frac{1}{(z-\lambda)^2}$ is uniformly absolutely convergent on a compact set around λ. The sum is unchanged if you translate by an element in Λ, so $\wp(z)$ is periodic in Λ. The same logic applies to $\wp'(z)$. □

This means that $\wp(z)$ is an **elliptic function**.

Definition 13.7 (Elliptic function)**.** Let $\Lambda \subset \mathbb{C}$ be a lattice (=elliptic curve over $\mathbb{C}$). An **elliptic function** for Λ is a meromorphic function $f(z)$ for $z \in \mathbb{C}$ such that $f(z)$ is periodic with translation by Λ, i.e. $f(z+\lambda) = f(z)$ for any $\lambda \in \Lambda$.

Definition 13.8 (Eisenstein series)**.** Let $\Lambda \subset \mathbb{C}$ be a lattice (=elliptic curve over $\mathbb{C}$). For $k \geq 2$, the **Eisenstein series** is defined as

$$G_{2k} := \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^{2k}}.$$

We may want to write $G_{2k}(\Lambda)$ to indicate its dependency on Λ. It is elementary to check that $G_{2k}(c\Lambda) = c^{-2k}G_{2k}(\Lambda)$ for $c \in \mathbb{C}^\times$.

You may also see this as a holomorphic function $G_{2k} : \mathbb{H} \to \mathbb{C}$, $\tau \mapsto G_{2k}(\tau)$ which is the infinite sum for the lattice (=elliptic curve over $\mathbb{C}$) $\mathbb{Z} \oplus \mathbb{Z}\tau$.

Remark 13.9. The reason why we only take even powers is because the infinite sum is trivially zero for odd powers (if $\lambda \in \Lambda$, $-\lambda \in \Lambda$). The Eisenstein series $G_{2k}(\tau)$ is an example of a **modular form** (of weight $2k$ and level 1).

The following is an algebraic geometry in disguise.

Proposition 13.10. *Let $\Lambda \subset \mathbb{C}$ be a lattice (=elliptic curve over $\mathbb{C}$).*

(1) Then, $\wp(z)$ satisfies a differential equation,

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2\wp(z) - g_3,$$

where $g_2 = 60G_4$, and $g_3 = 140G_6$.

(2) *Any elliptic function $p(z)$ for Λ is expressed as a rational function in $\wp(z)$ and $\wp'(z)$. If $p(z)$ is holomorphic outside Λ, it is expressed as a polynomial in $\wp(z)$ and $\wp'(z)$. Namely, if E (H, respectively) is the ring of elliptic functions (the ring of elliptic functions holomorphic outside Λ), then $H \cong \mathbb{C}[X,Y]/(Y^2-(4X^3-g_2X-g_3))$ and $E = \mathrm{Frac}(H)$.*

If $p(z)$ is furthermore even (i.e. $p(z)=p(-z)$), then you only need to use $\wp(z)$ to express $p(z)$ as above.

(3) *If $f \in \mathrm{End}(\Lambda)$ is $x \mapsto cx$ for $c \in \mathbb{C}^\times$ (i.e. $c\Lambda \subset \Lambda$), then $\wp(cz)$ is expressed as a rational function in $\wp(z)$. Conversely, if $c \in \mathbb{C}^\times$ is such that $\wp(cz)$ is expressed as a rational function in $\wp(z)$, then $c\Lambda \subset \Lambda$.*

(4) *For the rational function appearing in (3), you may take $\wp(cz) = \frac{A(\wp(z))}{B(\wp(z))}$ for $A(X), B(X) \in \mathbb{C}[X]$ such that $\deg A = \deg B + 1 = \deg f$.*

Proof. (1) Just by expanding the infinite sum formally into Laurent series, we obtain the Laurent series expansion of $\wp(z)$ at $z=0$,

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}z^{2n}.$$

This implies that $\wp'(z)$ has the Laurent series expansion at $z=0$

$$\wp'(z) = -\frac{2}{z^3} + \sum_{n=1}^{\infty}(2n+1)2nG_{2n+2}z^{2n-1}.$$

Thus, $(\wp'(z))^2$ has the Laurent series expansion at $z=0$

$$\begin{aligned}(\wp'(z))^2 &= \frac{4}{z^6} - \frac{4}{z^3}\cdot(6G_4z+20G_6z^3) + (\text{holomorphic part, vanishing at } z=0)\\ &= \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + (\text{holomorphic part, vanishing at } z=0).\end{aligned}$$

Similarly, $4(\wp(z))^3 - g_2\wp(z) - g_3$ has the Laurent series expansion at $z=0$

$$\begin{aligned}&4(\wp(z))^3 - g_2\wp(z) - g_3\\ &= \frac{4}{z^6} + \frac{12}{z^4}(3G_4z^2+5G_6z^4) - \frac{g_2}{z^2} - g_3 + (\text{holomorphic part, vanishing at } z=0)\\ &= \frac{4}{z^6} + \frac{36G_4-60G_4}{z^2} + (60G_6-140G_6) + (\text{holomorphic part, vanishing at } z=0)\\ &= \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + (\text{holomorphic part, vanishing at } z=0).\end{aligned}$$

Therefore, $(\wp'(z))^2 - (4(\wp(z))^3 - g_2\wp(z) - g_3)$ is a meromorphic function with possible poles at Λ, periodic in Λ and is actually holomorphic and vanishing at $z=0$. By periodicity, this function is holomorphic everywhere. By periodicity, the values of this function are taken at a compact domain (e.g. fundamental parallelogram), so in particular bounded. Therefore, by Liouville's theorem, this function is a constant function. As we know its value at $z = 0$ is zero, this function is zero, proving the identity (the difference is everywhere zero).

(2) If $p(z)$ is an even elliptic function holomorphic outside Λ, its Laurent series expansion at $z = 0$ would look like $\sum_{n=M}^{\infty} a_{2n}z^{2n}$ for $M \in \mathbb{Z}$. If $M \geq 0$, then by Liouville's theorem, $p(z)$ is constant. If $M < 0$, then you may inductively find a polynomial $q(X) \in \mathbb{C}[X]$ such that $q(\wp(z))$ and $p(z)$ has the matching tail of Laurent series expansion; for example, $p(z) - a_{2M}\wp(z)^{-M}$ would have a lower order pole at $z = 0$, and you can continue the process until you eliminate all poles. This implies that again $p(z)$ is expressed as a polynomial in $\wp(z)$.

Now let $p(z)$ be an elliptic function holomorphic outside Λ. As any function is a sum of an even function and an odd function, we only need to show that an odd elliptic function holomorphic outside Λ can be expressed as a polynomial in $\wp(z)$ and $\wp'(z)$. By using the same strategy as above, we can eliminate any odd-order poles of order ≥ 3. For the simple pole, we claim that there is actually no elliptic function with just a simple pole at each $\lambda \in \Lambda$. This is because, if we let $\Lambda = \mathbb{Z}\tau_1 \oplus \mathbb{Z}\tau_2$, if you compute the contour integral $\int_S f(z)dz$ along a parallelogram S with four vertices $\frac{\pm\tau_1\pm\tau_2}{2}$, then this would be equal to $2\pi i$ times the residue of the simple pole, but the two parallel sides of S are in different directions for S, so $\int_S f(z)dz = 0$, contradicting the assumption that $f(z)$ has a simple pole at $z = 0$ and nowhere else outside Λ.

The above two paragraphs and (1) show that there is a surjective map $\mathbb{C}[X, Y]/(Y^2 - (4X^3 - g_2X - g_3)) \twoheadrightarrow H, X \mapsto \wp(z), Y \mapsto \wp'(z)$. As any element of $\mathbb{C}[X, Y]/(Y^2 - (4X^3 - g_2X - g_3))$ is uniquely expressed as $a_0(X) + Ya_1(X)$ for $a_0(X), a_1(X) \in \mathbb{C}[X]$, if there is $a_0(X) + Ya_1(X)$ in the kernel of the surjective map $\mathbb{C}[X, Y]/(Y^2 - (4X^3 - g_2X - g_3)) \twoheadrightarrow H$, then $a_0(\wp(z)) + \wp'(z)a_1(\wp(z)) = 0$, or $a_0(\wp(z)) = -\wp'(z)a_1(\wp(z))$. As $a_0(\wp(z))$ is even and $-\wp'(z)a_1(\wp(z))$ is odd, this means that $a_0 = a_1 = 0$. Therefore, the surjective map $\mathbb{C}[X, Y]/(Y^2 - (4X^3 - g_2X - g_3)) \twoheadrightarrow H$ is an isomorphism.

If $p(z)$ is an elliptic function, it has finitely many poles up to translation by $\Lambda = \mathbb{Z}\tau_1 \oplus \mathbb{Z}\tau_2$. Let $z_0, \cdots, z_n$ be the poles of $p(z)$ (up to translation by Λ), with multiplicities $m_0, \cdots, m_n$. Suppose that we manually include $z_0 = 0$, in the list of poles by allowing m_0 to be possibly 0. Then, the function

$$q(z) = p(z)\prod_{i=1}^{n}(\wp(z) - \wp(\lambda))^{m_i},$$

is an elliptic function whose poles are only at Λ. This is because $\wp(z) - \wp(\lambda)$ is an elliptic function whose poles are only at Λ, and has at least a simple zero at $z = \lambda$, so multiplying $\prod_{i=1}^{n}(\wp(z) - \wp(\lambda))^{m_i}$ with $p(z)$ will cancel out all non-Λ poles (it may introduce more zeros, but that is fine). Thus, $q(z)$ is a polynomial in $\wp(z)$ and $\wp'(z)$. Therefore, $p(z)$ is a rational function in $\wp(z)$ and $\wp'(z)$. It is clear that if $p(z)$ is even then you don't need to use $\wp'(z)$ because $q(z)$ will be an even elliptic function holomorphic outside Λ.

(3) If $c\Lambda \subset \Lambda$, then $\wp(cz)$ is definitely an even elliptic function, so by (2), $\wp(cz)$ is expressed as a rational function in $\wp(z)$. Conversely, if $\wp(cz)$ is expressed as a rational function in $\wp(z)$, this means that $\wp(cz)$ is an elliptic function, i.e. $\wp(cz) = \wp(c(z+\lambda))$ for $\lambda \in \Lambda$. Therefore, by scaling cz to z, we have $\wp(z) = \wp(z + c\lambda)$ for $\lambda \in \Lambda$. As $\wp(z)$ has poles only at $z \in \Lambda$, this means that $c\lambda \in \Lambda$. Therefore, $c\Lambda \subset \Lambda$.

(4) Let us take $A(X), B(X)$ so that A, B have no common factors (=common zeros, as $\mathbb{C}$ is algebraically closed). Note that there is a double pole of $\wp(cz)$ at $z = 0$. On the other hand, the order of a pole of $A(\wp(z))$ at $z = 0$ is $2\deg A$, and similarly the order of a pole of $B(\wp(z))$ at $z = 0$ is $2\deg B$. Thus, $2 = 2\deg A - 2\deg B$, or $\deg A = \deg B + 1$.

Note also that $\wp(cz)$ satisfies $\wp\left(c\left(z+\frac{\lambda}{c}\right)\right) = \wp(cz+\lambda) = \wp(cz)$, so it is actually invariant under translation by a finer lattice (=elliptic curve over $\mathbb{C}$) $\frac{1}{c}\Lambda$. In particular, inside a fundamental parallelogram of Λ, there are $\deg f$ different poles, and all poles are double poles. Therefore, the number of poles of $\wp(cz)$ in a fundamental parallelogram of Λ (counted with multiplicities) is $2\deg f$. On the other hand, $A(\wp(z))$ has only one pole at $z = 0$, of order $2\deg A$, in a fundamental parallelogram of Λ containing $z = 0$. Also, $B(\wp(z))$ has only one pole at $z = 0$, of order $2\deg B$, in the same fundamental parallelogram, and by the argument principle, there are $2\deg B$ many zeros (counted with multiplicities) in the same fundamental parallelogram. Thus, if $A(\wp(z))$ and $B(\wp(z))$ do not share a common zero, then the number of poles of $\frac{A(\wp(z))}{B(\wp(z))}$ counted with multiplicities will be $2\deg A - 2\deg B + 2\deg B = 2\deg A$. This will then show that $\deg A = \deg f$. However, if $A(\wp(z)) = B(\wp(z)) = 0$, then $\wp(z)$ will be a common zero of $A(X)$ and $B(X)$, which do not exist by our assumption. Thus, $\deg A = \deg f$.

□

Remark 13.11. Given a lattice $\Lambda \subset \mathbb{C}$ (=elliptic curve over $\mathbb{C}$), we can now give an algebraic equation defining $\mathbb{C}/\Lambda$, which is as a topological manifold a 2-torus. Consider the map

$$\mathbb{C}/\Lambda - \{0\} \to \mathbb{C}^2, \quad z \mapsto (\wp(z), \wp'(z)).$$

Its image is contained in $\{(x,y) \in \mathbb{C}^2 \ : \ y^2 = 4x^3 - g_2x - g_3\} \subset \mathbb{C}^2$ by Proposition 13.10(1). It turns out that the induced map $\mathbb{C}/\Lambda - \{0\} \to \{(x,y) \in \mathbb{C}^2 \ : \ y^2 = 4x^3 - g_2x - g_3\}$ is a **biholomorphism**, i.e. bijective, holomorphic, and its inverse is also holomorphic. You can add the "point at infinity" ∞ in a certain way and let $0 \in \mathbb{C}/\Lambda$ be sent to ∞, so that $\mathbb{C}/\Lambda$ is, as a "complex manifold", isomorphic to $\{(x,y) \in \mathbb{C}^2 \ : \ y^2 = 4x^3 - g_2x - g_3\} \cup \{\infty\}$, which is a complex curve defined by a polynomial equation, a **complex algebraic curve**. The equation $y^2 = 4x^3 - g_2x - g_3$ is a typical equation that defines an **elliptic curve**.

13.2. j-invariants of lattices in $\mathbb{C}$ (=elliptic curves over $\mathbb{C}$).

Definition 13.12 (j-invariant)**.** We may think of $g_2 = 60G_4$ and $g_3 = 140G_6$ as a holomorphic function on $\mathbb{H}$. The j-function $j : \mathbb{H} \to \mathbb{C}$ is a function defined as

$$j(\tau) := 1728\frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2}.$$

Given a lattice $\Lambda \subset \mathbb{C}$ (=elliptic curve over $\mathbb{C}$), isomorphic to $\mathbb{Z} \oplus \mathbb{Z}\tau$, we define the j-invariant of the lattice (=elliptic curve over $\mathbb{C}$) as $j(\tau)$. Similarly, for a lattice (=elliptic curve over $\mathbb{C}$) $\Lambda \in \mathbb{C}$, $j(\Lambda)$ is defined using the same formula with $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$. It is elementary to check that $j(\Lambda) = j(c\Lambda)$ for any $c \in \mathbb{C}^\times$.

Remark 13.13. There is a good reason why you want to put 1728 in the definition of j-function, which we will see a bit later.

Proposition 13.14.

(1) *The j-function is a holomorphic function, i.e.* $g_2(\tau)^3 - 27g_3(\tau)^2 \neq 0$ *for* $\tau \in \mathbb{H}$.

(2) *The j-function is invariant under the* $\mathrm{SL}_2(\mathbb{Z})$*-action on* $\mathbb{H}$*. Namely, for* $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ *and* $\tau \in \mathbb{H}$, $j(\gamma \cdot \tau) = j(\tau)$*. In particular, the j-invariant of a lattice (=elliptic curve over* $\mathbb{C}$*) is well-defined.*

(3) *Conversely, for* $\tau_1, \tau_2 \in \mathbb{H}$, $j(\tau_1) = j(\tau_2)$ *if and only if* $\tau_1 = \gamma\tau_2$ *for some* $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

(4) *The j-function defines a bijective holomorphic function* $j : \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \xrightarrow{\sim} \mathbb{C}$.

(5) *For any* $a, b \in \mathbb{C}$ *such that* $a^3 - 27b^2 \neq 0$*, there exists a lattice (=elliptic curve over* $\mathbb{C}$*)* $\Lambda \subset \mathbb{C}$ *such that* $g_2(\Lambda) = a$ *and* $g_3(\Lambda) = b$.

Proof. (1) By Proposition 13.10(1), $X = \wp(z)$ is a root of a cubic polynomial $4X^3 - g_2X - g_3$ if $\wp'(z) = 0$. Let $\omega_1, \omega_2 \in \Lambda$ be a $\mathbb{Z}$-basis. Then, there are three points, $\lambda = \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$, in $\mathbb{C}$, up to translation by Λ, such that $\lambda \notin \Lambda$ but $2\lambda \in \Lambda$. At those points λ, using that $\wp(z)$ is an even function, we have

$$\wp(z+\lambda) = \wp(-z-\lambda) = \wp(-z-\lambda+2\lambda) = \wp(-z+\lambda).$$

Therefore, if you take the power series expansion at $z = \lambda$, then the power series will be even, so $\wp'(\lambda) = 0$. Consider the function $f(z) = \wp(z) - \wp(\lambda)$. This is also a holomorphic function periodic in Λ, that has double poles at $z \in \Lambda$ (and no other poles) and double zeros at $z \in \lambda + \Lambda$ (because $f(\lambda) = 0$ and $f'(\lambda) = 0$). By the residue theorem, this implies that there are no more zeros. In particular, $\wp(\lambda)$ is distinct from any other value of $\wp$ as long as it is not the translate by Λ. Therefore, $\wp\left(\frac{\omega_1}{2}\right)$, $\wp\left(\frac{\omega_2}{2}\right)$, $\wp\left(\frac{\omega_1+\omega_2}{2}\right)$ are three distinct numbers. As $4X^3 - g_2X - g_3$ has at most three roots, these numbers are exactly the three roots. Now the expression $g_2^3 - 27g_3^2$ is $\frac{1}{16}$ of the discriminant of the polynomial $4X^3 - g_2X - g_3$, so we know that

$$g_2^3 - 27g_3^2 = \frac{1}{16}\left(\wp\left(\frac{\omega_1}{2}\right) - \wp\left(\frac{\omega_2}{2}\right)\right)^2\left(\wp\left(\frac{\omega_1}{2}\right) - \wp\left(\frac{\omega_1+\omega_2}{2}\right)\right)^2\left(\wp\left(\frac{\omega_2}{2}\right) - \wp\left(\frac{\omega_1+\omega_2}{2}\right)\right)^2 \neq 0.$$

(2) For this, we clarify what we meant by that the the Eisenstein series G_{2k} is a modular form of weight $2k$ and level 1. This means that, for any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, $G_{2k}(\gamma \cdot \tau) = (c\tau + d)^{2k} G_{2k}(\tau)$. To prove this, we use that $\mathrm{SL}_2(\mathbb{Z})$ as a group is generated by $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. It is easy to check that showing $G_{2k}(\gamma \cdot \tau) = (c\tau + d)^{2k} G_{2k}(\tau)$ only needs to be checked for generators of $\mathrm{SL}_2(\mathbb{Z})$. Thus, we only need to show that $G_{2k}(\tau + 1) = G_{2k}(\tau)$, and $G_{2k}\left(-\frac{1}{\tau}\right) = \tau^{2k} G_{2k}(\tau)$. The first relation is obvious as $\mathbb{Z} \oplus \mathbb{Z}\tau = \mathbb{Z} \oplus \mathbb{Z}(\tau + 1)$, so the sum defining the Eisenstein series is the same for both lattices (=elliptic curves over $\mathbb{C}$). For the second relation, we note that $\mathbb{Z} \oplus \mathbb{Z}\left(-\frac{1}{\tau}\right) = \mathbb{Z} \oplus \mathbb{Z}\left(\frac{1}{\tau}\right) = \frac{1}{\tau}\left(\mathbb{Z} \oplus \mathbb{Z}\tau\right)$, so you get the same sum for $G_{2k}\left(-\frac{1}{\tau}\right)$ as $G_{2k}(\tau)$ except that you multiply every term by $\frac{1}{\frac{1}{\tau^{2k}}} = \tau^{2k}$, which gives the desired relation.

This implies the $\mathrm{SL}_2(\mathbb{Z})$-invariance of the j-function, because, for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$,

$$j(\gamma \cdot \tau) = 1728 \frac{(c\tau + d)^{12} g_2(\tau)^3}{(c\tau + d)^{12} g_2(\tau)^3 - 27(c\tau + d)^{12} g_3(\tau)^2} = 1728 \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27 g_3(\tau)^2} = j(\tau).$$

(3) If $j(\tau) = j(\tau')$, it's easy to see that this means $\frac{G_4(\tau)^3}{G_6(\tau)^2} = \frac{G_4(\tau')^3}{G_6(\tau')^2}$. You may find $\lambda \in \mathbb{C}$ such that $\lambda^4 G_4(\tau') = G_4(\tau)$ and $\lambda^6 G_6(\tau) = G_6(\tau)$. This means that the two lattices (=elliptic curves over $\mathbb{C}$) $\Lambda_1 := \mathbb{Z} \oplus \mathbb{Z}\tau'$ and $\Lambda_2 := \lambda(\mathbb{Z} \oplus \mathbb{Z}\tau)$ give rise to the same infinite sum G_4 and G_6.

Let $\wp_{\Lambda_1}(z)$ and $\wp_{\Lambda_2}(z)$ be the Weierstrass $\wp$-function obtained by using the two lattices (=elliptic curves over $\mathbb{C}$) Λ_1, Λ_2. By the proof of Proposition 13.10(1), we see that the Laurent series expansion at $z = 0$ of $\wp_{\Lambda_1}(z)$ and that of $\wp_{\Lambda_2}(z)$ coincide up to the z^4-term. Moreover, by differentiating the differential equation in Proposition 13.10(1), we obtain

$$2\wp'(z)\wp''(z) = 12\wp'(z)(\wp(z))^2 - g_2\wp'(z),$$

or

$$\wp''(z) = 6\wp(z)^2 - g_2/2.$$

This means that, by comparing the Laurent series expansion on both side,

$$\frac{6}{z^4} + \sum_{n=1}^{\infty}(2n+1)2n(2n-1)G_{2n+2}z^{2n-2} = 6\left(\frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}z^{2n}\right)^2 - 30G_4.$$

Comparing the coefficients, we get the identities

$$z^{-4}\text{-term:} \quad 6 = 6,$$

$$1\text{-term:} \quad 6G_4 = 36G_4 - 30G_4,$$

$$z^2\text{-term:} \quad 60G_6 = 60G_6,$$

z^{2n}-term, $n \geq 2$: $\quad (2n{+}3)(2n{+}2)(2n{+}1)G_{2n+4} = 12(2n{+}3)G_{2n+4}{+}6\sum_{i=0}^{n-2}(2i{+}3)(2n{-}2i{+}1)G_{2i+4}G_{2n-2i}$.

The first three equations are obviously identities, and the last equation is, after rearranging,

$$\frac{(n-1)(2n+3)(2n+5)}{3}G_{2n+4} = \sum_{i=0}^{n-2}(2i+3)(2n-2i+1)G_{2i+4}G_{2n-2i} \quad \text{for } n \geq 2,$$

and the coefficient on the left hand side is not zero for $n \geq 2$. In particular, every G_{2n}, $n \geq 2$, is determined by G_4 and G_6 via a recurrence relation. This implies that $\wp_{\Lambda_1}(z)$ and $\wp_{\Lambda_2}(z)$ have the same Laurent expansion at $z = 0$, which means $\wp_{\Lambda_1}(z) = \wp_{\Lambda_2}(z)$. As they have the same set of poles, this implies that $\Lambda_1 = \Lambda_2$.

We claim that $\mathbb{Z} \oplus \mathbb{Z}\tau' = \lambda(\mathbb{Z} \oplus \mathbb{Z}\tau)$ for some $\lambda \in \mathbb{C}^\times$ implies that $\tau' = \gamma \cdot \tau$ for some $\tau \in \mathrm{SL}_2(\mathbb{Z})$. If $\mathbb{Z} \oplus \mathbb{Z}\tau' = \lambda(\mathbb{Z} \oplus \mathbb{Z}\tau)$, $1 = \lambda(c\tau + d)$ and $\tau' = \lambda(a\tau + b)$ for $a, b, c, d \in \mathbb{Z}$. Then, $\tau' = \frac{\tau'}{1} = \frac{a\tau+b}{c\tau+d}$. As τ' and 1 are not real multiples of one another, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has nonzero determinant. By doing this the other way around, we see that $\tau = \frac{a'\tau'+b'}{c'\tau'+d'}$ for $a', b', c', d' \in \mathbb{Z}$, which implies that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$. As $\mathbb{Z}^\times = \{\pm 1\}$, $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm 1$. On the other hand, one can check that, if $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = -1$, then $\mathrm{Im}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau\right) < 0$. Therefore, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, as desired.

(4) By (3), we know that $j : \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}$ is injective. Thus what we really need to show is that j is surjective. By Open Mapping Theorem of complex analysis, we know that $j(\mathbb{H}) \subset \mathbb{C}$ is an open subset. To conclude that $j(\mathbb{H}) = \mathbb{C}$, it suffices to show that $j(\mathbb{H})$ is also a closed subset of $\mathbb{C}$ as $\mathbb{C}$ is connected. Suppose that $\tau_1, \tau_2, \cdots$ is a sequence of points in $\mathbb{H}$ such that $j(\tau_1), j(\tau_2), \cdots$ converge to some $w \in \mathbb{C}$. We may translate τ_i's by $\mathrm{SL}_2(\mathbb{Z})$ so that we can put $\tau_i \in \mathcal{F}$, the fundamental domain (Remark 13.4).

Before we proceed, we need to know one more qualitative fact about $j(\tau)$. Note that

$$g_2(\tau) = 60 \sum_{m,n\in\mathbb{Z},(m,n)\neq(0,0)} \frac{1}{(m+n\tau)^4} = 60\left(2\sum_{m=1}^{\infty}\frac{1}{m^4} + \sum_{n,m\in\mathbb{Z},n\neq 0}\frac{1}{(m+n\tau)^4}\right).$$

In this expression, the second sum goes to 0 as $\mathrm{Im}\,\tau \to +\infty$. Therefore, $\lim_{\mathrm{Im}\,\tau\to+\infty} g_2(\tau) = 120\zeta(4) = 120\frac{\pi^4}{90} = \frac{4\pi^4}{3}$. Similarly,

$$g_3(\tau) = 140 \sum_{m,n\in\mathbb{Z},(m,n)\neq(0,0)} \frac{1}{(m+n\tau)^6} = 140\left(2\sum_{m=1}^{\infty}\frac{1}{m^6} + \sum_{n,m\in\mathbb{Z},n\neq 0}\frac{1}{(m+n\tau)^6}\right),$$

and by the same reason, $\lim_{\operatorname{Im}\tau\to+\infty} g_3(\tau) = 280\zeta(6) = 280\frac{\pi^6}{945} = \frac{8\pi^6}{27}$ (for the values of $\zeta(2n)$, see for example [ANT, Example 18.18]). In fact, the convergence of the function as $\operatorname{Im}\tau \to +\infty$ is another requirement for $g_2(\tau)$ and $g_3(\tau)$ to be modular forms.

Anyhow, the denominator of $j(\tau)$ goes to $(4\pi^4/3)^3 - 27(8\pi^6/27)^2 = 0$ as $\operatorname{Im}\tau \to +\infty$. This implies that $|j(\tau)| \to \infty$ as $\operatorname{Im}\tau \to +\infty$. This means that $\operatorname{Im}\tau_1, \operatorname{Im}\tau_2, \cdots$ remains bounded below a certain bound M. Therefore, $\tau_i \in \mathcal{F} \cap \{\tau \in \mathbb{H} : \operatorname{Im}(\tau) < M\} \subset \{x + yi \in \mathbb{H} : x \in [-1/2, 1/2],\ y \in [1/2, M]\}$. Therefore, the infinite sequence $\tau_1, \cdots$ has a limit point τ' inside this box. By the continuity of j, $j(\tau') = w$. This shows that $j(\mathbb{H}) \subset \mathbb{C}$ is closed.

(5) By (4), there exists $\tau \in \mathbb{H}$ such that $j(\tau) = 1728\frac{a^3}{a^3-27b^2}$. This implies that $\frac{g_2(\tau)^3}{g_3(\tau)^2} = \frac{a^3}{b^2}$. This implie that there exists $c \in \mathbb{C}^\times$ such that $g_2(\tau) = c^4 a$ and $g_3(\tau) = c^6 b$. Then the lattice (=elliptic curve over $\mathbb{C}$) $c(\mathbb{Z} \oplus \mathbb{Z}\tau)$ will do the job.

□

Remark 13.15. The quotient $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} =: Y(1)$ is an example of the **modular curves**. Even though Proposition 13.14(4) tells you that j function is a bijection between $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ and $\mathbb{C}$, it does not quite identify $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ with $\mathbb{C}$ as a complex manifold, because the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ is not free. There are two reasons for this problem, one easy and one subtle. The easy reason is that $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ acts trivially on the whole $\mathbb{H}$. However, even though you consider the action of $\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\left\{\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$ on $\mathbb{H}$, the action is not free, which is a more subtle source of the problem. For example,

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot i = \frac{-1}{i} = i, \quad \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \cdot e^{2\pi i/3} = \frac{-e^{2\pi i/3} - 1}{e^{2\pi i/3}} = -1 - e^{-2\pi i/3} = e^{2\pi i/3}.$$

In fact, these are the only two points in the fundamental domain $\mathcal{F}$ (see Remark 13.4) with a nontrivial stabilizer in $\mathrm{PSL}_2(\mathbb{Z})$.

Exercise 13.1. Verify this claim. More precisely, show that, if $\tau \in \mathcal{F}$ is such that the stabilizer of τ in $\mathrm{PSL}_2(\mathbb{Z})$ is not trivial, then $\tau = i$ or $\tau = e^{2\pi i/3}$. Show that the stabilizer of i in $\mathrm{PSL}_2(\mathbb{Z})$ is the order 2 cyclic group $\left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$, and the stabilizer of $e^{2\pi i/3}$ in $\mathrm{PSL}_2(\mathbb{Z})$ is the order 3 cyclic group $\left\langle \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$.

The easy reason can be resolved by taking the quotient of $\mathbb{H}$ by a slightly smaller subgroup of $\mathrm{SL}_2(\mathbb{Z})$ (basically any subgroup that does not contain $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$), but the subtle reason can never be resolved by this trick. This is a manifestation of a very subtle fact that the modular curves are actually **(complex) orbifolds**, or in algebraic geometry language, **(complex) algebraic stacks**.

As we will see, the j-function is a remarkable holomorphic function that is crucial for the **Explicit class field theory** for imaginary quadratic fields.

13.3. **Lattices in $\mathbb{C}$ (=elliptic curves over $\mathbb{C}$) with complex multiplication.** We saw in the previous section that, given a lattice (=elliptic curve over $\mathbb{C}$) $\Lambda \subset \mathbb{C}$, $\mathrm{End}(\Lambda)$ is a commutative ring that contains $\mathbb{Z}$ in it. We also saw an example where $\mathrm{End}(\Lambda)$ is bigger than $\mathbb{Z}$, equal to $\mathcal{O}_K$ for an imaginary quadratic field K.

Definition 13.16 (Lattices in $\mathbb{C}$ (=elliptic curves over $\mathbb{C}$) with complex multiplication)**.** Let $\Lambda \subset \mathbb{C}$ be a lattice (=elliptic curve over $\mathbb{C}$). We say that Λ has **complex multiplication** (or **CM**) if $\mathrm{End}(\Lambda) \neq \mathbb{Z}$.

The reason why we call it to have complex multiplication is because the shape of $\mathrm{End}(\Lambda)$ is extremely restricted, so that if $\mathrm{End}(\Lambda) \neq \mathbb{Z}$, then it has to be not too far from the ring of integers of an imaginary quadratic field. This is because $\mathrm{End}(\Lambda)$ has a lot more structures than expected.

Lemma 13.17. *Let $\Lambda, \Lambda' \subset \mathbb{C}$ be lattices (=elliptic curves over $\mathbb{C}$).*

*(1) Let $f : \Lambda \to \Lambda'$, $x \mapsto cx$, be an isogeny. Then, its **dual** $\widehat{f} : \Lambda' \to \Lambda$, given by $x \mapsto \frac{\deg f}{c} x$, is also an isogeny. In particular, two lattices (=elliptic curves over $\mathbb{C}$) being isogenous is an equivalence condition. If $\Lambda = \Lambda'$, this map gives a ring involution (i.e. a ring homomorphism which is an involution) $\widehat{\cdot} : \mathrm{End}(\Lambda) \to \mathrm{End}(\Lambda)$ called the **Rosati involution**.*

(2) For $n \in \mathbb{Z}$, $\widehat{[n]} = [n]$.

(3) For $f \in \mathrm{Hom}(\Lambda, \Lambda')$, $\deg f = \deg \widehat{f}$, $f \circ \widehat{f} = [\deg f]$ in $\mathrm{End}(\Lambda')$ and $\widehat{f} \circ f = [\deg f]$ in $\mathrm{End}(\Lambda)$.

*(4) Let the **trace** of $f \in \mathrm{End}(\Lambda)$ be defined as $\mathrm{tr}\, f := f + \widehat{f}$. Then, $\mathrm{tr}\, f \in \mathbb{Z} \subset \mathrm{End}(\Lambda)$.*

(5) Let $\mathrm{End}^0(\Lambda) = \mathrm{End}(\Lambda) \otimes_{\mathbb{Z}} \mathbb{Q}$. Then, $\mathrm{End}^0(\Lambda)$ is either $\mathbb{Q}$ or an imaginary quadratic field.

(6) If $\mathrm{End}^0(\Lambda) = \mathbb{Q}$, then $\mathrm{End}(\Lambda) = \mathbb{Z}$.

*(7) If $\mathrm{End}^0(\Lambda) = K$ is an imaginary quadratic field, then $\mathrm{End}(\Lambda) \subset K$ is, as a $\mathbb{Z}$-module, a free rank 2 $\mathbb{Z}$-module. In this case, we say that Λ **has complex multiplication by the ring** $\mathrm{End}(\Lambda)$.*

Proof. (1) The statement is invariant under replacing c and Λ' by cd and $d\Lambda'$ for any $d \in \mathbb{C}^\times$. In particular, we may assume that $c = 1$, i.e. $\Lambda \subset \Lambda'$ is just a sublattice. Then, $\deg f = \#\frac{\Lambda'}{\Lambda}$, so multiplying by $\deg f$ will kill anything in this quotient, i.e. $x \mapsto (\deg f)x$ sends an element in Λ' to an element in Λ, which makes it an isogeny. This also shows the reflexivity of the relation of two lattices (=elliptic curves over $\mathbb{C}$) being isogenous despite the apparent asymmetry in the definition.

If $\Lambda = \Lambda'$, then $\deg f = |c|^2$, so the dual isogeny $\widehat{f}$ is $x \mapsto \frac{\deg f}{c} x = \overline{c}x$. Therefore, it is clear that taking the dual isogeny is an involution.

(2) Obvious.

(3) Obvious from (1) and (2).

(4) Obvious.

(5) Suppose that $f : \Lambda \to \Lambda$, $x \mapsto cx$, is an isogeny. We may scale Λ so that $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$ for some $\tau \in \mathbb{H}$. Then, $x \mapsto cx$ being an isogeny means that $c, c\tau \in \mathbb{Z} \oplus \mathbb{Z}\tau$. Therefore, $c = m + n\tau$ and $c\tau = a + b\tau$. Combining, we obtain $m\tau + n\tau^2 = a + b\tau$, or $n\tau^2 + (m-b)\tau - a = 0$. This implies that τ is a solution to a quadratic polynomial in $\mathbb{Q}[X]$. Therefore, $\mathbb{Q}(\tau)$ is either $\mathbb{Q}$ or a quadratic field. As $\tau \in \mathbb{H}$, τ is not real, so $\mathbb{Q}(\tau)$ is either $\mathbb{Q}$ or an imaginary quadratic field. As $\mathrm{End}(\Lambda)$ is naturally a subring of $\mathbb{Q}(\tau)$, this implies that $\mathrm{End}^0(\Lambda)$ is also a subring of $\mathbb{Q}(\tau)$. Thus, we get the result.

(6) Let us scale Λ so that $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$. If $x \mapsto cx$, $c \in \mathbb{Q}$, is a self-isogeny of Λ, this means that $c, c\tau \in \Lambda$. However, as $\mathrm{Im}(\tau) > 0$, $c \in \Lambda$ means that $c \in \mathbb{Z}$. Therefore, $\mathrm{End}(\Lambda) \subset \mathbb{Z}$. As $\mathbb{Z} \subset \mathrm{End}(\Lambda)$, we get the result.

(7) Let us scale Λ so that $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$. If $x \mapsto cx$ is a self-isogeny of Λ, then certainly $c \in \mathbb{Z} \oplus \mathbb{Z}\tau$. Therefore, $\mathrm{End}(\Lambda)$ is a $\mathbb{Z}$-submodule of $\mathbb{Z} \oplus \mathbb{Z}\tau$. This implies that $\mathrm{End}(\Lambda)$ is a free $\mathbb{Z}$-module of rank ≤ 2. As there exists highly divisible large enough $N \gg 0$ such that $N, N\tau \in \mathrm{End}(\Lambda)$, this implies that the rank of $\mathrm{End}(\Lambda)$ is ≥ 2, so exactly 2.

□

By Lemma 13.17, for a lattice (=elliptic curve over $\mathbb{C}$) $\Lambda \subset \mathbb{C}$, we know that either $\mathrm{End}(\Lambda) = \mathbb{Z}$ is or $\mathrm{End}(\Lambda)$ is a free rank 2 $\mathbb{Z}$-submodule of an imaginary quadratic field, or an **order** in an imaginary quadratic field.

Definition 13.18 (Order)**.** Given a $\mathbb{Q}$-algebra K of finite dimension as a $\mathbb{Q}$-vector space, an **order** $\mathcal{O}$ in K is a subring of K that is a free $\mathbb{Z}$-module rank $\dim_{\mathbb{Q}} K$. Equivalently, it is a subring $\mathcal{O} \subset K$ which is finitely generated as a $\mathbb{Z}$-module, and $K = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$.

Lemma 13.19. *Let K be an imaginary quadratic field. If $\mathcal{O} \subset K$ is an order, then $\mathcal{O} = \mathbb{Z} + N\mathcal{O}_K$ for $N = [\mathcal{O}_K : \mathcal{O}] \in \mathbb{N}$. In particular, any order $\mathcal{O}$ is contained in $\mathcal{O}_K$ (making $\mathcal{O}_K$ the* ***maximal order*** *in K). We call N the* ***conductor*** *of the order $\mathcal{O}$.*

Proof. We first show that $\mathcal{O} \subset \mathcal{O}_K$. Let $\alpha \in \mathcal{O}$. If $\alpha \in \mathbb{Z}$, then obviously $\alpha \in \mathcal{O}_K$. If not, then, $\mathbb{Z}[\alpha] \subset \mathcal{O}$ is a $\mathbb{Z}$-submodule, so it is a free $\mathbb{Z}$-module of rank exactly 2 (it is ≥ 2 because it contains $\mathbb{Z} \oplus \mathbb{Z}\alpha$, it is ≤ 2 because it is contained in $\mathcal{O}$). Let β_1, β_2 be a $\mathbb{Z}$-basis of $\mathbb{Z}[\alpha]$. Then, β_1 and β_2 are $\mathbb{Z}$-linear combinations of certain powers of α. Let α^N be the power of α with a larger exponent than any powers of α appearing in β_1, β_2. Then, $\alpha^N = m_1\beta_1 + m_2\beta_2$ for $m_1, m_2 \in \mathbb{Z}$. This means that α is a root of a monic polynomial with integer coefficients, so α is an algebraic integer, or $\alpha \in \mathcal{O}_K$. This shows that $\mathcal{O} \subset \mathcal{O}_K$.

Now let $N = [\mathcal{O}_K : \mathcal{O}]$. Then, $N\mathcal{O}_K \subset \mathcal{O}$. Therefore, $\mathbb{Z} + N\mathcal{O}_K \subset \mathcal{O}$. Now it suffices to show that $[\mathcal{O}_K : \mathbb{Z} + N\mathcal{O}_K] = N$. Note that $[\mathcal{O}_K : N\mathcal{O}_K] = N^2$, so it suffices to show that $[\mathbb{Z} + N\mathcal{O}_K : N\mathcal{O}_K] = N$. But this is obvious because $\frac{\mathbb{Z}+N\mathcal{O}_K}{N\mathcal{O}_K} = \frac{\mathbb{Z}}{\mathbb{Z}\cap N\mathcal{O}_K} = \frac{\mathbb{Z}}{N\mathbb{Z}}$. We are done. □

We now know quite precisely what can possibly be $\mathrm{End}(\Lambda)$ for a lattice (=elliptic curve over $\mathbb{C}$) $\Lambda \subset \mathbb{C}$. We also know that, for "most" lattices (=elliptic curves over $\mathbb{C}$), $\mathrm{End}(\Lambda) = \mathbb{Z}$, because, if you scale to express $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$ for $\tau \in \mathbb{H}$, $\mathrm{End}(\Lambda) \neq \mathbb{Z}$ if and only if τ is an imaginary quadratic number, and almost all complex numbers are even transcendental. So a lattice (=elliptic curve over $\mathbb{C}$) having complex multiplication is quite a special property[17].

We may then ask – given an order $\mathcal{O} \subset K$ in an imaginary quadratic field, what are the lattices (=elliptic curves over $\mathbb{C}$) Λ having complex multiplication by $\mathcal{O}$ (i.e. $\mathrm{End}(\Lambda) = \mathcal{O}$)? It is quite clear that $\mathrm{End}(\mathcal{O}) = \mathcal{O}$, but there can be other possibilities, because Λ need not have a ring structure. It turns out that there is a very precise description of the list of Λ's realizing the given $\mathcal{O}$ as their endomorphism algebras, and, in particular, the list is finite! From here we start to see a connection between the lattices (=elliptic curves over $\mathbb{C}$) with complex multiplication and the class field theory of an imaginary quadratic field.

Definition 13.20 (Proper $\mathcal{O}$-ideal)**.** Let $\mathcal{O}$ be an order in an imaginary quadratic field K. For an ideal $\mathfrak{a} \subset \mathcal{O}$, let

$$\mathcal{O}(\mathfrak{a}) := \{\alpha \in K \ : \ \alpha\mathfrak{a} \subset \mathfrak{a}\}.$$

By definition, $\mathcal{O} \subset \mathcal{O}(\mathfrak{a})$, and $\mathcal{O}(\mathfrak{a}) = \mathrm{End}(\mathfrak{a})$ when $\mathfrak{a}$ is seen as a lattice in $\mathbb{C}$ (=elliptic curve over $\mathbb{C}$), so $\mathcal{O}(\mathfrak{a})$ is also an order in K by Lemma 13.19. An $\mathcal{O}$-ideal $\mathfrak{a}$ is a **proper $\mathcal{O}$-ideal** if $\mathcal{O}(\mathfrak{a}) = \mathcal{O}$. Similarly, a fractional $\mathcal{O}$-ideal $\mathfrak{b} \subset K$ (i.e. a finitely generated $\mathcal{O}$-submodule) is a **proper fractional $\mathcal{O}$-ideal** if $\mathcal{O}(\mathfrak{b}) := \{\alpha \in K \ : \ \alpha\mathfrak{b} \subset \mathfrak{b}\}$ is equal to $\mathcal{O}$. Again, $\mathcal{O}(\mathfrak{b}) = \mathrm{End}(\mathfrak{b})$ when $\mathfrak{b}$ is seen as a lattice in $\mathbb{C}$ (=elliptic curve over $\mathbb{C}$), so $\mathcal{O}(\mathfrak{b})$ is an order in K.

Example 13.21. Not all ideals of an order are proper. For example, let $K = \mathbb{Q}(\sqrt{-3})$. Then, $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, so that $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$ is the order of conductor 2 in K. Let $\mathfrak{a} = (2, 1+\sqrt{-3}) \subset \mathcal{O}$ be an ideal of $\mathcal{O}$. Then, we see that $\mathcal{O}(\mathfrak{a}) = \mathcal{O}_K \neq \mathcal{O}$, because $\frac{1+\sqrt{-3}}{2} \in \mathcal{O}(\mathfrak{a})$.

Remark 13.22. The failure of some ideals being proper is related to the fact that an order is not necessarily a Dedekind domain (specifically, not normal; for example, [ANT, Lemma 6.9] does not hold for orders). In particular, all ideals of the maximal order $\mathcal{O}_K$ are proper, as $\mathcal{O}_K$ is normal (by definition, for an ideal $\mathfrak{a} \subset \mathcal{O}_K$, $\mathcal{O}(\mathfrak{a}) = \mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$).

Definition 13.23 (Ideal norm)**.** Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and let $\mathfrak{a} \subset \mathcal{O}$ be an $\mathcal{O}$-dieal. Then, the **ideal norm** of $\mathfrak{b}$ is $N(\mathfrak{a}) := [\mathcal{O} : \mathfrak{a}]$. More generally, for a fractional $\mathcal{O}$-ideal $\mathfrak{b} \subset K$, which is always of the form $\lambda\mathfrak{a}$ for some $\lambda \in K^\times$ and $\mathfrak{a} \subset \mathcal{O}$ an $\mathcal{O}$-ideal, $N(\mathfrak{b}) := N_{K/\mathbb{Q}}(\lambda)N(\mathfrak{a})$, which can be easily seen to be well-defined.

Remark 13.24. The norm is not necessarily multiplicative, which is also another manifestation of the fact that fractional $\mathcal{O}$-ideals are not neceesarily invertible. It is however multplicative for proper (i.e. invertible) fractional $\mathcal{O}$-ideals.

Lemma 13.25. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and let $\mathfrak{a} \subset K$ be a fractional $\mathcal{O}$-ideal. Then, $\mathfrak{a}$ is a proper fractional $\mathcal{O}$-ideal if and only if $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal (i.e. there is a fractional $\mathcal{O}$-ideal $\mathfrak{b} \subset K$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$).*

[17] Imaginary quadratic numbers in $\mathbb{H}$ are therefore sometimes called **special points**, or **CM points**.

Proof. Let $\mathfrak{a}$ be an invertible fractional $\mathcal{O}$-ideal. Then, there is a fractional $\mathcal{O}$-ideal $\mathfrak{b} \subset K$ such that $\mathfrak{ab} = \mathcal{O}$. If $\alpha \in \mathcal{O}(\mathfrak{a})$, then $\alpha\mathcal{O} = \alpha\mathfrak{ab} \subset \mathfrak{ab} = \mathcal{O}$, which implies that $\alpha \in \mathcal{O}$. Thus, $\mathcal{O}(\mathfrak{a}) \subset \mathcal{O}$, which implies that $\mathcal{O}(\mathfrak{a}) = \mathcal{O}$, or $\mathfrak{a}$ is proper.

Conversely, let $\mathfrak{a} \subset K$ be a proper fractional $\mathcal{O}$-ideal. We may multiply $\mathfrak{a}$ by an appropriate element in K so that we may assume that $\mathfrak{a} \subset \mathcal{O}$ (being proper or being invertible is invariant under multiplication by an element in K).

Let $\overline{\mathfrak{a}}$ be the $\mathcal{O}$-ideal obtained by applying the nontrivial Galois element of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathfrak{a}$; this is an $\mathcal{O}$-ideal as $\overline{\mathcal{O}} = \mathcal{O}$ (every order is of the form $\mathbb{Z} + N\mathcal{O}_K$ for $N \in \mathbb{N}$). We claim that $\mathfrak{a}\overline{\mathfrak{a}} = (N(\alpha))$ (the principal ideal of $\mathcal{O}$ generated generated by $N(\alpha)$). Then, $\mathfrak{a}^{-1} := \frac{1}{N(\alpha)}\overline{\mathfrak{a}}$ will give you the inverse, making $\mathfrak{a}$ invertible. Let $\alpha, \beta \in \mathfrak{a}$ be a $\mathbb{Z}$-basis. Let $\tau = \frac{\beta}{\alpha}$, so that $\mathfrak{a} = \alpha(\mathbb{Z} \oplus \mathbb{Z}\tau)$, and $\mathcal{O} = \mathcal{O}(\mathfrak{a}) = \mathcal{O}(\mathbb{Z} \oplus \mathbb{Z}\tau)$. Let $aX^2 + bX + c$ be the minimal polynomial of τ over $\mathbb{Z}$, so that $a, b, c \in \mathbb{Z}$, with $a > 0$ and $\gcd(a, b, c) = 1$. Note that $a\tau \in \mathcal{O}(\mathbb{Z} \oplus \mathbb{Z}\tau)$. Therefore, $\mathcal{O} \supset \mathbb{Z} \oplus \mathbb{Z}a\tau$. If $\gamma \in \mathcal{O}(\mathbb{Z} \oplus \mathbb{Z}\tau)$, $\gamma, \gamma\tau \in \mathbb{Z} \oplus \mathbb{Z}\tau$, so in particular $\mathbb{Z} \oplus \mathbb{Z}\tau \supset \mathcal{O}$. This implies that $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}a'\tau$ for $a'|a$. If $a'\tau \in \mathcal{O}(\mathbb{Z} \oplus \mathbb{Z}\tau)$, then $a'\tau^2 \in \mathbb{Z} \oplus \mathbb{Z}\tau$. As $a^2X + bX + c$ is the minimal polynomial of τ, $a' = a$. Therefore, $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}a\tau$. So,

$$N(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}] = [\mathbb{Z} \oplus \mathbb{Z}a\tau : \alpha(\mathbb{Z} \oplus \mathbb{Z}\tau)] = \frac{[\mathbb{Z} \oplus \mathbb{Z}a\tau : \alpha(\mathbb{Z} \oplus \mathbb{Z}a\tau)]}{[\alpha(\mathbb{Z} \oplus \mathbb{Z}\tau) : \alpha(\mathbb{Z} \oplus \mathbb{Z}a\tau)]} = \frac{N_{K/\mathbb{Q}}(\alpha)}{a}.$$

Consider $\mathfrak{a}\overline{\mathfrak{a}}$, which is the $\mathbb{Z}$-module generated by $\{\alpha\overline{\alpha}, \alpha\overline{\beta}, \beta\overline{\alpha}, \beta\overline{\beta}\} = N_{K/\mathbb{Q}}(\alpha)\{1, \tau, \overline{\tau}, \tau\overline{\tau}\}$. Note that $\tau\overline{\tau} = \frac{c}{a}$ and $\tau + \overline{\tau} = -\frac{b}{a}$, so $\mathfrak{a}\overline{\mathfrak{a}}$ is the $\mathbb{Z}$-module generated by $N_{K/\mathbb{Q}}(\alpha)\{1, \tau, \frac{b}{a}, \frac{c}{a}\} = N(\mathfrak{a})\{a, a\tau, b, c\}$. As $\{a, b, c\}$ generate $\mathbb{Z}$, we see that $\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})(\mathbb{Z} \oplus \mathbb{Z}a\tau) = N(\mathfrak{a})\mathcal{O} = (N(\mathfrak{a}))$. □

Definition 13.26 (Ring class group). Let $\mathcal{O}$ be an order in an imaginary quadratic field. Let $\mathrm{Cl}(\mathcal{O})$, called the **ring class group** of $\mathcal{O}$, be the group of proper (=invertible) fractional $\mathcal{O}$-ideals modulo the principal ideals in $\mathcal{O}$.

Proposition 13.27. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. There is a one-to-one correspondence*

$$\mathrm{Cl}(\mathcal{O}) \leftrightarrow \{\textit{lattices } \Lambda \subset \mathbb{C} \textit{ (=elliptic curves over } \mathbb{C}\textit{) with } \mathrm{End}(\Lambda) = \mathcal{O}\}/\textit{isomorphisms},$$

$$\mathfrak{a} \mapsto \mathfrak{a} \subset \mathbb{C}.$$

Proof. The only remaining verification is, if $\Lambda \subset \mathbb{C}$ is a lattice (=elliptic curve over $\mathbb{C}$) with $\mathrm{End}(\Lambda) = \mathcal{O}$, then $\Lambda = \lambda\mathfrak{a}$ for $\lambda \in \mathbb{C}^\times$ and $\mathfrak{a}$ an $\mathcal{O}$-ideal. You may take $\lambda \in \mathbb{C}^\times$ so that $\lambda^{-1}\Lambda \subset \mathcal{O}$. So we just assume that $\Lambda \subset \mathcal{O}$. Then $\mathcal{O}(\Lambda) = \mathcal{O}$ by definition, and Λ is an $\mathcal{O}$-ideal as Λ is stable under multiplication by an element in $\mathcal{O}$. □

Example 13.28. As all fractional ideals of $\mathcal{O}_K$ are invertible, $\mathrm{Cl}(\mathcal{O}_K) = \mathrm{Cl}(K)$.

We may guess that the ring class groups, just like the (ray) class groups, are natural objects in the idele/ideal side of the global class field theory. In particular, it must arise as a quotient of the ray class group of a certain modulus. This is in fact true.

Theorem 13.29 (Ring class groups and ray class groups)**.** *Let K be an imaginary quadratic field, and let $\mathcal{O} = \mathbb{Z} + N\mathcal{O}_K$ be the order in K of conductor N.*

*(1) An $\mathcal{O}$-ideal $\mathfrak{a} \subset \mathcal{O}$ is said to be **coprime to** N if $\mathfrak{a} + N\mathcal{O} = \mathcal{O}$. Then, this is equivalent to that $N(\mathfrak{a})$ is coprime to N.*

(2) Any $\mathcal{O}$-ideal coprime to the conductor N is a proper $\mathcal{O}$-ideal.

(3) The ring class group $\mathrm{Cl}(\mathcal{O})$ is generated by the $\mathcal{O}$-ideal classes of the $\mathcal{O}$-ideals coprime to the conductor N. More precisely,

$$\mathrm{Cl}(\mathcal{O}) \cong \frac{\{\textit{fractional } \mathcal{O}\textit{-ideals coprime to } N\}}{\{\textit{principal fractional ideals } \alpha\mathcal{O} \textit{ where } N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q} \textit{ is coprime to } N\}},$$

where a fractional $\mathcal{O}$-ideal coprime to N is a fractional ideal of the form $\frac{\mathfrak{a}}{\mathfrak{b}}$ where $\mathfrak{a}, \mathfrak{b}$ are $\mathcal{O}$-ideals coprime to N.

(4) Any $\mathcal{O}_K$-ideal $\mathfrak{a} \subset \mathcal{O}_K$ coprime to N gives rise to an $\mathcal{O}$-ideal $\mathfrak{a} \cap \mathcal{O} \subset \mathcal{O}$ coprime to N. Conversely, any $\mathcal{O}$-ideal $\mathfrak{a} \subset \mathcal{O}$ coprime to N gives rise to an $\mathcal{O}_K$-ideal $\mathfrak{a}\mathcal{O}_K \subset \mathcal{O}_K$ coprime to N. This gives a one-to-one correspondence between the $\mathcal{O}_K$-ideals coprime to N and the $\mathcal{O}$-ideals coprime to N. Accordingly, $\mathrm{Cl}(\mathcal{O}) \cong J_K^{S(N)}/K^{N,\mathcal{O}}$, where $S(N)$ is the set of places of K dividing N, and $K^{N,\mathcal{O}}$ is the subgroup of $K^\times$ generated by $\alpha \in \mathcal{O}_K$ such that $\alpha \equiv a \pmod{N\mathcal{O}_K}$ for some $a \in \mathbb{Z}$ with $\gcd(a, N) = 1$.

(5) Consider N as a modulus in K (note that K has no real place, so there is no infinite modulus to worry about). There is a natural quotient map $\mathrm{Cl}^N(K) \twoheadrightarrow \mathrm{Cl}(\mathcal{O})$ with kernel $(\mathbb{Z}/N\mathbb{Z})^\times$ (principal ideals generated by the integers coprime to N). In particular, the ring class group $\mathrm{Cl}(\mathcal{O})$ is finite.

Proof. (1) Note that $\mathfrak{a} + N\mathcal{O} = \mathcal{O}$ is equivalent to that multiplication by N is surjective on $\mathcal{O}/\mathfrak{a}$, which is equivalent to the order of $\mathcal{O}/\mathfrak{a}$ being coprime to N.

(2) Let $\mathfrak{a}$ be an $\mathcal{O}$-ideal coprime to N. Let $\alpha \in \mathcal{O}(\mathfrak{a}) \subset \mathcal{O}_K$. Then $\alpha\mathfrak{a} \subset \mathfrak{a}$, so in particular $\alpha\mathcal{O} = \alpha(\mathfrak{a} + N\mathcal{O}) \subset \mathfrak{a} + N\alpha\mathcal{O} \subset \mathfrak{a} + N\mathcal{O}_K = \mathcal{O}$. This implies that $\alpha \in \mathcal{O}$, so $\mathcal{O}(\mathfrak{a}) \subset \mathcal{O}$, which means that $\mathfrak{a}$ is a proper $\mathcal{O}$-ideal.

(3) We first show that, for every proper $\mathcal{O}$-ideal $\mathfrak{b} \subset \mathcal{O}$, there is a fractional $\mathcal{O}$-ideal $\mathfrak{a} \subset K$ coprime to N such that $\mathfrak{b}\mathfrak{a}^{-1}$ is a principal fractional $\mathcal{O}$-ideal (recall that $\mathfrak{a}$ is invertible by (2), so $\mathfrak{a}^{-1}$ makes sense). Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_n \subset \mathcal{O}$ be the prime ideals of $\mathcal{O}$ containing either $N\mathcal{O}$ or $\mathfrak{b}$; there are finitely many such prime ideals as both $N\mathcal{O}$ and $\mathfrak{b}$ are of finite index in $\mathcal{O}$. In particular, if $\mathfrak{p} \subset \mathcal{O}$ is a prime ideal not equal to any $\mathfrak{p}_i$, then $\mathfrak{b}\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$.

We claim that, even at $\mathfrak{p}_i$, $\mathfrak{b}\mathcal{O}_{\mathfrak{p}_i} = \beta_i\mathcal{O}_{\mathfrak{p}_i}$ for some $\beta_i \in K^\times$ (i.e. $\mathfrak{b}$ is locally principal[18]); this is not obvious because $\mathcal{O}_{\mathfrak{p}_i}$ now is not necessarily a PID (remember, for the ring of integers case, we used that a local Dedekind domain is a discrete valuation ring, thus a

[18] In fact, the converse is true, that a locally principal ideal is invertible. See [Neu, Proposition I.12.4].

PID). Indeed, as $\mathfrak{b}\mathfrak{b}^{-1} = \mathcal{O}$, which means that $1 = \sum_{i=1}^{r} x_i y_i$ for $x_i \in \mathfrak{b}$, $y_i \in \mathfrak{b}^{-1}$. Note that each $x_i y_i \in \mathcal{O}$ by definition, and as the sum of $x_1 y_1, \cdots, x_r y_r$ is 1, not all of them, as elements of $\mathcal{O}_{\mathfrak{p}}$, are contained in the maximal ideal $\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ of $\mathcal{O}_{\mathfrak{p}}$. After rearranging, suppose that $x_1 y_1$ as an element of $\mathcal{O}_{\mathfrak{p}}$ is not contained in $\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$. As $\mathcal{O}_{\mathfrak{p}}$ is still a local ring, $x_1 y_1 \in \mathcal{O}_{\mathfrak{p}}^{\times}$. Then, for any $x \in \mathfrak{b}\mathcal{O}_{\mathfrak{p}_i}$, $xy_1 \in \mathfrak{b}\mathfrak{b}^{-1}\mathcal{O}_{\mathfrak{p}_i} = \mathcal{O}_{\mathfrak{p}_i}$, and $xy_1(x_1y_1)^{-1}x_1 \in x_1\mathcal{O}_{\mathfrak{p}_i}$, which shows tat $\mathfrak{b}\mathcal{O}_{\mathfrak{p}_i} \subset x_1\mathcal{O}_{\mathfrak{p}_i}$. As $x_1 \in \mathfrak{b}$, this in fact implies that $\mathfrak{b}\mathcal{O}\mathfrak{p}_i = x_1\mathcal{O}_{\mathfrak{p}_i}$, as desired.

We now let $\mathfrak{q}_i \subset \mathcal{O}_K$ be any maximal ideal containing $\mathfrak{p}_i\mathcal{O}_K$. By the Weak Approximation Theorem (Theorem 7.12), there exists $\beta \in K^{\times}$ such that $|\beta - \beta_i|_{\mathfrak{q}_i} < |\beta|_{\mathfrak{q}_i}$ (to apply the Weak Approximation Theorem, think of this condition as $|\beta_i^{-1} - \beta^{-1}|_{\mathfrak{q}_i} < |\beta_i^{-1}|_{\mathfrak{q}_i}$; it is finding an element of the diagonal close to the point $(\beta_1^{-1}, \cdots, \beta_n^{-1})$) for all $1 \leq i \leq n$. We claim that $\mathfrak{a} = \beta^{-1}\mathfrak{b}$ does the job; i.e. $\beta^{-1}\mathfrak{b}$ is a fractional $\mathcal{O}$-ideal coprime to N, or $\beta^{-1}\mathfrak{b}\mathcal{O}_{\mathfrak{p}_i} = \mathcal{O}_{\mathfrak{p}_i}$ for every $1 \leq i \leq n$. Note that $\beta^{-1}\mathfrak{b}\mathcal{O}_{\mathfrak{p}_i} = \beta^{-1}\beta_i\mathcal{O}_{\mathfrak{p}_i}$, so it suffices to show that $\beta^{-1}\beta_i$ is a unit in $\mathcal{O}_{\mathfrak{p}_i}$. By construction, $|1 - \beta^{-1}\beta_i|_{\mathfrak{q}_i} < 1$, so $\beta^{-1}\beta_i$ is a unit in $\mathcal{O}_{K,\mathfrak{q}_i}$. Note that $\mathfrak{q}_i \cap \mathcal{O} \supset \mathfrak{p}_i$, so it is in fact $\mathfrak{q}_i \cap \mathcal{O} = \mathfrak{p}_i$, because $\mathfrak{q}_i \cap \mathcal{O} \neq \mathcal{O}$ (i.e. $\mathfrak{q}_i$ cannot contain $\mathcal{O}$). This implies that $\mathcal{O}_{K,\mathfrak{q}_i}$ is the integral closure of $\mathcal{O}_{\mathfrak{p}_i}$ in K. This implies that $\mathcal{O}_{K,\mathfrak{q}_i}^{\times} \cap \mathcal{O}_{\mathfrak{p}_i} = \mathcal{O}_{\mathfrak{p}_i}^{\times}$, so in particular $\beta^{-1}\beta_i$ is a unit in $\mathcal{O}_{\mathfrak{p}_i}$.

What we proved so far is that there is a natural surjection

$$\{\text{fractional } \mathcal{O}\text{-ideals coprime to } N\} \twoheadrightarrow \mathrm{Cl}(\mathcal{O}).$$

Certainly any principal fractional ideal $\alpha\mathcal{O}$ with $N_{K/\mathbb{Q}}(\alpha)$ coprime to N is contained in the kernel. Conversely, if $\alpha\mathcal{O}$ is a principal fractional ideal coprime to N, then it is invertible, so by Remark 13.24, its norm is also coprime to N, which is equal to $N_{K/\mathbb{Q}}(\alpha)$.

(4) For an $\mathcal{O}_K$-ideal $\mathfrak{a} \subset \mathcal{O}_K$ coprime to N, $\mathcal{O}/\mathfrak{a}\cap\mathcal{O} \hookrightarrow \mathcal{O}_K/\mathfrak{a}$ is injective. As $N\mathcal{O}_K \subset \mathcal{O}$, and as multiplying by N is invertible on $\mathcal{O}_K/\mathfrak{a}$, it means that $\mathcal{O}/\mathfrak{a} \cap \mathcal{O} \to \mathcal{O}_K/\mathfrak{a}$ is surjective. Therefore, $N(\mathfrak{a}) = N(\mathcal{O} \cap \mathfrak{a})$, so $\mathfrak{a} \cap \mathcal{O}$ is an $\mathcal{O}$-ideal coprime to N.

Conversely, for an $\mathcal{O}$-ideal $\mathfrak{a} \subset \mathcal{O}$ coprime to N, we have

$$\mathfrak{a}\mathcal{O}_K + N\mathcal{O}_K = (\mathfrak{a} + N\mathcal{O})\mathcal{O}_K = \mathcal{O}\mathcal{O}_K = \mathcal{O}_K,$$

which means that $\mathfrak{a}\mathcal{O}_K$ is coprime to N.

To show that these are inverses to each other, we first show that, given an $\mathcal{O}$-ideal $\mathfrak{a} \subset \mathcal{O}$ coprime to N, $\mathfrak{a}\mathcal{O}_K \cap \mathcal{O} = \mathfrak{a}$. Obviously $\mathfrak{a}\mathcal{O}_K \cap \mathcal{O} \supset \mathfrak{a}$. For the other inclusion, note that

$$\mathfrak{a}\mathcal{O}_K \cap \mathcal{O} = (\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})(\mathfrak{a} + N\mathcal{O}) \subset \mathfrak{a} + N\mathfrak{a}\mathcal{O}_K \subset \mathfrak{a} + \mathfrak{a}\mathcal{O} = \mathfrak{a}.$$

We then show that, given an $\mathcal{O}_K$-ideal $\mathfrak{a} \subset \mathcal{O}_K$ coprime to N, $(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K = \mathfrak{a}$. Obviously $(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K \subset \mathfrak{a}$. For the other inclusion, note that

$$\mathfrak{a} = \mathfrak{a}\mathcal{O} = \mathfrak{a}(\mathfrak{a} \cap \mathcal{O} + N\mathcal{O}) \subset (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K + N\mathfrak{a} \subset (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K + \mathfrak{a} \cap \mathcal{O} = (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K,$$

because obviously $N\mathfrak{a} \subset \mathfrak{a}$ and $N\mathfrak{a} \subset N\mathcal{O}_K \subset \mathcal{O}$. This shows that the two operations are inverses to each other.

Finally, to show that $\mathrm{Cl}(\mathcal{O}) \cong J_K^{S(N)}/K^N$, it suffices to show that, for $\alpha \in \mathcal{O}_K$, $\alpha \equiv a \pmod{N\mathcal{O}_K}$ for some $a \in \mathbb{Z}$ with $\gcd(a, N) = 1$ if and only if $\alpha \in \mathcal{O}$ and $\gcd(N_{K/\mathbb{Q}}(\alpha), N) = 1$, which is almost by the definition of the conductor obvious.

(5) This follows from (4) and the finiteness of the ray class group.

□

Definition 13.30 (Ring class field)**.** Let K be an imaginary quadratic field, and let $\mathcal{O}$ be an order in K. Then, the **ring class field** $K(\mathcal{O})$ is the abelian extension of K which, by the global Artin reciprocity, corresponds to $\mathrm{Cl}(\mathcal{O})$ as the natural quotient of the idele class group C_K (because it is the natural quotient of the ray class group $\mathrm{Cl}^N(K)$, where N is the conductor of $\mathcal{O}$). By definition, $\mathrm{Gal}(K(\mathcal{O})/K) \cong \mathrm{Cl}(\mathcal{O})$, and $K(\mathcal{O})$ is the subfield of the ray class field $K(N)$ where $\mathrm{Gal}(K(N)/K(\mathcal{O})) \cong (\mathbb{Z}/N\mathbb{Z})^\times$.

14. Modular functions

14.1. Modular functions for $\mathrm{SL}_2(\mathbb{Z})$.

For the **Explicit class field theory** for imaginary quadratic fields, we need to develop some theory of **modular functions**, which are meromorphic modular forms of weight 0.

Definition 14.1 (Congruence subgroups)**.** For $N \geq 1$, we define certain finite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$ as follows.

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv 0 \pmod{N} \right\}.$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv 0 \pmod{N}, \ a, d \equiv 1 \pmod{N} \right\}.$$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ b, c \equiv 0 \pmod{N}, a, d \equiv 1 \pmod{N} \right\}.$$

Obviously, $\Gamma(N) \leq \Gamma_1(N) \leq \Gamma_0(N) \leq \mathrm{SL}_2(\mathbb{Z})$.

A finite index subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ is a **congruence subgroup** if $\Gamma \supset \Gamma(N)$ for some $N \geq 1$.

Remark 14.2. As the definition suggests, there are finite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$ that are not congruence subgroups.

Definition 14.3 (Modular functions)**.** Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. A **modular function** for Γ is a meromorphic function $f : \mathbb{H} \to \mathbb{C}$ that satisfies the following.

- For $\gamma \in \Gamma$, $f(\tau) = f(\gamma \cdot \tau)$.
- "As τ escape to infinity, $f(\tau)$ is meromorphic".

  We explain in detail what this means.

- Firstly, this includes the statement that $f(\tau)$ is meromorphic as $\operatorname{Im}\tau \to +\infty$, which is reminiscent of what we analyzed about $j(\tau)$ above. Let $N(\mathbb{Z}) = \left\{\begin{pmatrix} 1 & n \\ 0 & 1\end{pmatrix} : n \in \mathbb{Z}\right\} \leq \mathrm{SL}_2(\mathbb{Z})$, and let $N_\Gamma := N(\mathbb{Z}) \cap \Gamma$. Note that as Γ is a congruence subgroup, $\Gamma \supset \Gamma(M)$ for some $M \geq 1$, and $\Gamma(M) \cap N(\mathbb{Z}) = \left\{\begin{pmatrix} 1 & Mn \\ 0 & 1\end{pmatrix} : n \in \mathbb{Z}\right\}$, so $N_\Gamma = \left\{\begin{pmatrix} 1 & M'n \\ 0 & 1\end{pmatrix} : n \in \mathbb{Z}\right\}$ for some $M'|M$. This implies that $\begin{pmatrix} 1 & M' \\ 0 & 1\end{pmatrix} \in \Gamma$, so $f(\tau) = f(\tau + M')$. Therefore, if you consider the map $\mathbb{H} \to D^\times$, $\tau \mapsto e^{2\pi i\tau/M'}$, where $D^\times := \{0 < |z| < 1\}$, then f factors through this map, and therefore gives rise to a holomorphic map on $D^\times$. Then, $f(\tau)$ being meromorphic as $\operatorname{Im}\tau \to +\infty$ means that the corresponding holomorphic function on $D^\times$ has a pole at $z = 0$, and the Fourier expansion of $f(\tau)$ at ∞ is of the form

$$f(\tau) = \sum_{n=K}^{\infty} a_n q^n, \quad q = e^{\frac{2\pi i\tau}{M'}},$$

  for some $K \in \mathbb{Z}$ (i.e. the Laurent series in q has a finite meromorphic tail). This is called the q-**expansion** of $f(\tau)$ at ∞.
- A **cusp** is an element of $\mathbb{P}^1_{\mathbb{Q}} := \mathbb{Q} \cup \{\infty\}$. The same formula for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ applies to $\mathbb{P}^1_{\mathbb{Q}}$ (where, for $q \in \mathbb{Q}$, $\begin{pmatrix} a & b \\ c & d\end{pmatrix} \cdot q =$ "$\frac{aq+b}{cq+d}$" $= \infty$ if $cq + d = 0$, and $\begin{pmatrix} a & b \\ c & d\end{pmatrix} \cdot \infty =$ "$\frac{a\infty+b}{c\infty+d}$" $= \frac{a}{c}$, which is ∞ if $c = 0$). Note that $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1_{\mathbb{Q}}$. Two cusps $q_1, q_2 \in \mathbb{P}^1_{\mathbb{Q}}$ are Γ-**equivalent** if $q_1 = \gamma \cdot q_2$ for $\gamma \in \Gamma$.

  For each cusp $q \in \mathbb{P}^1_{\mathbb{Q}}$, you may choose $\gamma_q \in \mathrm{SL}_2(\mathbb{Z})$ such that $q = \gamma_q \cdot \infty$. If $f : \mathbb{H} \to \mathbb{C}$ satisfies $f(\tau) = f(\gamma \cdot \tau)$ for $\gamma \in \Gamma$, then if we let $f_q(\tau) := f(\gamma_q \cdot \tau)$, then $f_q(\gamma \cdot \tau) = f_q(\tau)$ if $\gamma \in \gamma_q^{-1}\Gamma\gamma_q$. Note that $\gamma_q^{-1}\Gamma\gamma_q$ is also a congruence subgroup as $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

  Now, this requirement of meromorphic as τ escape to infinity is actually $f_q(\tau)$ being meromorphic as $\operatorname{Im}\tau \to +\infty$ for every $q \in \mathbb{P}^1_{\mathbb{Q}}$. Note that you only need to check one cusp per a Γ-equivalence class of cusps. As $\mathbb{P}^1_{\mathbb{Q}}/\Gamma$ is a finite set (reason: $\mathbb{P}^1_{\mathbb{Q}}/\mathrm{SL}_2(\mathbb{Z})$ is just a singleton, and $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ is finite), this is a finite check.

Clearly, if $\Gamma' \leq \Gamma$, a modular function for Γ is automatically a modular function for Γ'.

Lemma 14.4. *The j-function is a modular function for* $\mathrm{SL}_2(\mathbb{Z})$*. Its q-expansion is* $j(\tau) = q^{-1} + 744 + 196884q + \cdots \in \mathbb{Z}[[q]](q^{-1})$.

This is the reason why we put 1728 in the definition of j; we want the coefficients of the q-expansion to be in $\mathbb{Z}$, and the lowest order term to be just q^{-1}.

Proof. We first compute the q-expansions of $G_4(\tau)$ and $G_6(\tau)$; indeed, they have a slightly different transformation formula for the action of $\mathrm{SL}_2(\mathbb{Z})$, but the extra factor is just 1 when you act by any element in $N(\mathbb{Z})$, so there are by the same reason the q-expansions of G_4 and G_6. Note that, for $k \geq 2$, we have

$$G_{2k}(\tau) = 2\zeta(2k) + 2\sum_{m\geq 1}\sum_{n\in\mathbb{Z}} \frac{1}{(m\tau+n)^{2k}} = 2\zeta(2k) + 2\sum_{m\geq 1} f_{2k}(m\tau),$$

where $f_{2k}(z) = \sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^{2k}}$. As $f_{2k}(z) = f_{2k}(z+1)$, it should also have a Fourier expansion, as $\operatorname{Im} z \to +\infty$. As $\lim_{\operatorname{Im} z\to+\infty} f_{2k}(z) = 0$, this implies that $f_{2k}(z) = \sum_{m=1}^{\infty} a_m e^{2\pi imz}$. Each coefficient a_m can be computed by

$$a_m = \int_{Ni}^{1+Ni} f_{2k}(z)e^{-2\pi imz}dz, \quad N > 0.$$

As $2k \geq 4$, the sum is absolutely convergent and we have

$$\begin{aligned} a_m &= \int_{Ni}^{1+Ni} \left(\sum_{n\in\mathbb{Z}} \frac{e^{-2\pi imz}}{(z+n)^{2k}}\right) dz = \sum_{n\in\mathbb{Z}} \int_{Ni}^{1+Ni} \frac{e^{-2\pi imz}}{(z+n)^{2k}}dz \\ &= \sum_{n\in\mathbb{Z}} \int_{n+Ni}^{1+n+Ni} \frac{e^{-2\pi imz}}{z^{2k}}dz = \int_{-\infty+Ni}^{\infty+Ni} \frac{e^{-2\pi imz}}{z^{2k}}dz. \end{aligned}$$

Let $I_{M,N} := \int_{-M+Ni}^{M+Ni} \frac{e^{-2\pi imz}}{z^{2k}}dz$, so that $a_m = \lim_{M\to+\infty} I_{M,N}$. Consider the contour integral

$$\frac{1}{2\pi i}\int_{S_{X,M,N}} \frac{e^{-2\pi imz}}{z^{2k}}dz = \frac{1}{2\pi i}\left(\int_{M+Ni}^{-M+Ni} + \int_{-M+Ni}^{-M-Xi} + \int_{-M-Xi}^{M-Xi} + \int_{M-Xi}^{M+Ni}\right) \frac{e^{-2\pi imz}}{z^{2k}}dz,$$

where $S_{X,M,N}$ is the rectangle with four corners $-M+Ni$, $M+Ni$, $-M-Xi$, $M-Xi$ for $M, N, X > 0$ (counterclockwise). By the residue theorem,

$$\frac{1}{2\pi i}\int_{S_{X,M,N}} \frac{e^{-2\pi imz}}{z^{2k}}dz = \frac{(-2\pi im)^{2k-1}}{(2k-1)!} = -\frac{(2\pi i)^{2k-1}m^{2k-1}}{(2k-1)!}.$$

Therefore,

$$I_{M,N} = \frac{(2\pi i)^{2k}m^{2k-1}}{(2k-1)!} + \left(\int_{-M+Ni}^{-M-Xi} + \int_{-M-Xi}^{M-Xi} + \int_{M-Xi}^{M+Ni}\right) \frac{e^{-2\pi imz}}{z^{2k}}dz.$$

We claim that $a_m = \lim_{N\to+\infty} I_{M,N} = \frac{(2\pi i)^{2k}m^{2k-1}}{(2k-1)!}$. For this, we give a bound on the other three integrals appearing in the above expression.

- For z on the vertical line connecting $-M-Xi$ and $-M+Ni$, i.e. for $z = -M+yi$ with $-X \leq y \leq N$, we have

  $$\left|\frac{e^{-2\pi imz}}{z^{2k}}\right| = \frac{e^{2\pi my}}{|z|^{2k}} \leq \frac{e^{2\pi mN}}{M^{2k}},$$

  so

  $$\left|\int_{-M+Ni}^{-M-Xi} \frac{e^{-2\pi imz}}{z^{2k}}dz\right| \leq (N+X)\frac{e^{2\pi mN}}{M^{2k}}.$$

- For z on the horizontal line connecting $M - Xi$ and $-M - Xi$, i.e. for $z = x - Xi$ with $-M \leq x \leq M$, we have
$$\left|\frac{e^{-2\pi imz}}{z^{2k}}\right| = \frac{e^{-2\pi mX}}{|z|^{2k}} \leq \frac{e^{-2\pi mX}}{X^{2k}},$$
so
$$\left|\int_{-M-Xi}^{M-Xi} \frac{e^{-2\pi imz}}{z^{2k}} dz\right| \leq 2M\frac{e^{-2\pi mX}}{X^{2k}}.$$

- For z on the vertical line connecting $M - Xi$ and $M + Ni$, i.e. for $z = M + yi$ with $-X \leq y \leq N$, we have
$$\left|\frac{e^{-2\pi imz}}{z^{2k}}\right| = \frac{e^{2\pi my}}{|z|^{2k}} \leq \frac{e^{2\pi mN}}{M^{2k}},$$
so
$$\left|\int_{M-Xi}^{M+Ni} \frac{e^{-2\pi imz}}{z^{2k}} dz\right| \leq (N+X)\frac{e^{2\pi mN}}{M^{2k}}.$$

Therefore,
$$\left|I_{M,N} - \frac{(2\pi i)^{2k} m^{2k-1}}{(2k-1)!}\right| \leq 2(N+X)\frac{e^{2\pi mN}}{M^{2k}} + 2M\frac{e^{-2\pi mX}}{X^{2k}}.$$
Let $X = M$. Then,
$$\left|I_{M,N} - \frac{(2\pi i)^{2k} m^{2k-1}}{(2k-1)!}\right| \leq 2(N+M)\frac{e^{2\pi mN}}{M^{2k}} + 2M\frac{e^{-2\pi mM}}{M^{2k}}.$$

The right hand side goes to 0 as $M \to +\infty$, so this implies that $a_m = \frac{(2\pi i)^{2k} m^{2k-1}}{(2k-1)!}$, as desired.

This implies that
$$f_{2k}(z) = \sum_{m=1}^{\infty} \frac{(2\pi i)^{2k} m^{2k-1}}{(2k-1)!} e^{2\pi imz}.$$
Therefore,
$$G_{2k}(\tau) = 2\zeta(2k) + 2\sum_{m\geq 1}\sum_{j=1}^{\infty} \frac{(2\pi i)^{2k} j^{2k-1}}{(2k-1)!} e^{2\pi ijm\tau} = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{r=1}^{\infty} \sigma_{2k-1}(r) e^{2\pi ir\tau},$$
where $\sigma_{2k-1}(r) = \sum_{d|r} d^{2k-1}$. Therefore,
$$g_2(\tau) = 60G_4(\tau) = \frac{4\pi^4}{3} + 120\frac{(2\pi i)^4}{3!}\sum_{r=1}^{\infty} \sigma_3(r)e^{2\pi ir\tau} = \frac{4\pi^4}{3} + 320\pi^4 \sum_{r=1}^{\infty} \sigma_3(r)e^{2\pi ir\tau},$$
$$g_3(\tau) = 140G_6(\tau) = \frac{8\pi^6}{27} + 280\frac{(2\pi i)^6}{5!}\sum_{r=1}^{\infty} \sigma_5(r)e^{2\pi ir\tau} = \frac{8\pi^6}{27} - \frac{448\pi^6}{3}\sum_{r=1}^{\infty} \sigma_5(r)e^{2\pi ir\tau}.$$

In particular, $g_2(\tau) = \frac{4\pi^4}{3}(1 + 240qP(q))$ and $g_3(\tau) = \frac{8\pi^6}{27}(1 - 504qQ(q))$ for $q = e^{2\pi i\tau}$ and $P(X), Q(X) \in \mathbb{Z}[[X]]$ with $P(0) = Q(0) = 1$. Therefore,

$$j(\tau) = 1728\frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2} = 1728\frac{\frac{64\pi^{12}}{27}(1 + 240qP(q))^3}{\frac{64\pi^{12}}{27}(1 + 240qP(q))^3 - \frac{64\pi^{12}}{27}(1 - 504qQ(q))^2}$$

$$= 1728\frac{(1 + 240qP(q))^3}{(1 + 240qP(q))^3 - (1 - 504qQ(q))^2}.$$

To show that the Laurent series expansion of $j(\tau)$ is in $\mathbb{Z}[[q]](q^{-1})$ with the first term starting with q^{-1}, what we need to show is that

$$\frac{(1 + 240qP(q))^3 - (1 - 504qQ(q))^2}{1728} = q + \cdots \in \mathbb{Z}[[q]].$$

Note that

$$\frac{(1 + 240qP(q))^3 - (1 - 504qQ(q))^2}{1728}$$

$$= \frac{(1 + 720qP(q) + 172800q^2P(q)^2 + 13824000q^3P(q)^3) - (1 - 1008qQ(q) + 254016q^2Q(q)^2)}{1728}$$

$$= q\frac{5P(q) + 7Q(q)}{12} + 100q^2P(q)^2 + 8000q^3P(q)^3 - 147q^2Q(q)^2.$$

We know that $P(0) = Q(0) = 1$ and as the q-term only appears in the first part of the above expression, we know that the q-series for the above expression starts with $q + \cdots$. To show that the above expression has integer coefficients, we need to show that the coefficients of $5P(q) + 7Q(q)$ are divisible by 12, or the coefficients of $5(P(q) - Q(q))$ are divisible by 12. Thus, we want to show that $P(q) \equiv Q(q) \pmod{12}$. This is the same as $\sigma_3(n) \equiv \sigma_5(n) \pmod{12}$. As $\sigma_k(n)$ is multiplicative (i.e. $\sigma_k(mn) = \sigma_k(m)\sigma_k(n)$ as long as $\gcd(m, n) = 1$), we only need to show the congruence when n is a prime power, $n = p^s$. Thus we want to show that $1 + p^3 + \cdots + p^{3s} \equiv 1 + p^5 + \cdots + p^{5s} \pmod{12}$ for any $s \geq 1$ and prime p. By Chinese Remainder Theorem, we need to show this for $(\mathrm{mod}\, 3)$ and $(\mathrm{mod}\, 4)$ separately.

- For $(\mathrm{mod}\, 3)$: if $p = 3$, then $1 + p^3 + \cdots + p^{3s} \equiv 1 \equiv 1 + p^5 + \cdots + p^{5s} \pmod{3}$. If $p \neq 3$, then $p^2 \equiv 1 \pmod{3}$, so $p^{3t} \equiv p^{5t} \pmod{3}$ for any $t \geq 0$.
- For $(\mathrm{mod}\, 4)$: if $p = 2$, then $1 + p^3 + \cdots + p^{3s} \equiv 1 \equiv 1 + p^5 + \cdots + p^{5s} \pmod{4}$. If $p \neq 2$, then $p^2 \equiv 1 \pmod{4}$, so $p^{3t} \equiv p^{5t} \pmod{4}$ for any $t \geq 0$.

I will leave to the reader checking that the next terms of the q-expansion of $j(\tau)$ after q^{-1} are $q^{-1} + 744 + 196884q + \cdots$. □

Theorem 14.5. *The modular functions for* $\mathrm{SL}_2(\mathbb{Z})$ *are precisely the rational functions in* $j(\tau)$. *In other words, the field of modular fuctions for* $\mathrm{SL}_2(\mathbb{Z})$, *denoted* $K(Y(1))$, *is given by* $K(Y(1)) = \mathbb{C}(j)$.

Among those, the modular functions for $\mathrm{SL}_2(\mathbb{Z})$ *that are holomorphic on* $\mathbb{H}$ *are precisely the polynomials in* $j(\tau)$. *Namely, the ring of modular functions for* $\mathrm{SL}_2(\mathbb{Z})$ *holomorphic on* $\mathbb{H}$, *denoted* $\mathcal{O}(Y(1))$, *is given by* $\mathcal{O}(Y(1)) = \mathbb{C}[j]$.

Proof. It is clear that a rational function in $j(\tau)$ is a modular function for $\mathrm{SL}_2(\mathbb{Z})$. Conversely, suppose that you are given a modular function $f(\tau)$ for $\mathrm{SL}_2(\mathbb{Z})$. Suppose that $f(\tau)$ has a q-expansion with some meromorphic tail, starting with $a_N q^{-N}$ for $N > 0$. Then, you may consider $f(\tau) - a_N j(\tau)^N$, which is a modular function with the meromorphic tail of the q-expansion starting with a lower order term. By repeating this, we may assume that the q-expansion of $f(\tau)$ has no meromorphic tail. This means that there is $C \in \mathbb{C}$ such that $\lim_{\mathrm{Im}\,\tau\to+\infty} f(\tau) = C$. This implies that $f(\tau)$ has no poles in the region $\{\mathrm{Im}\,\tau > B\}$ for some $B \gg 0$. This implies that there are only finitely many poles of $f(\tau)$ up to $\mathrm{SL}_2(\mathbb{Z})$-action, as such poles must appear in the box $\{x + yi \in \mathbb{H} \ : \ x \in [-1/2, 1/2],\ y \in [1/2, B]\}$ and there are only finitely many poles of a meromorphic function in a compact set in $\mathbb{C}$. Let $z_1, \cdots, z_m$ be the poles of $f(\tau)$ up to $\mathrm{SL}_2(\mathbb{Z})$-action, of order $n_1, \cdots, n_m$. Then, we consider

$$f(\tau)\prod_{i=1}^{m}(j(\tau) - j(z_i))^{n_i}.$$

Note that $j(\tau)$ is holomorphic on the whole $\mathbb{H}$, so this function is now holomorphic on $\mathbb{H}$. On the other hand, this process introduces yet another meromorphic tail of the q-expansion at ∞. We then go through the same reduction as above to eliminate the meromorphic tail of the q-expansion (which does not introduce new poles in $\mathbb{H}$, as $j(\tau)$ is holomorphic on $\mathbb{H}$). Thus we arrive at a modular function $f(\tau)$ which is holomorphic on $\mathbb{H}$ and has no meromorphic tail in its q-expansion. But this implies that $f(\tau)$ is bounded, as $\lim_{\mathrm{Im}\,\tau\to+\infty} f(\tau) = C'$ for some $C' \in \mathbb{C}$, and the rest of the values are realized by $f(\tau)$ for some τ in the box $[-1/2, 1/2] \times [1/2, B']$ as above for some $B' \gg 0$. Therefore, by Liouville's theorem, $f(\tau)$ is a constant function, which is obviously a rational function in $j(\tau)$. It is clear from the proof that we also showed that a modular function for $\mathrm{SL}_2(\mathbb{Z})$ holomorphic on $\mathbb{H}$ is a polynomial in $j(\tau)$. □

Remark 14.6 (Canonical model of the modular curve $Y(1)$; for those who know algebraic geometry)**.** This implies that the modular curve $Y(1)$ in the algebraic geometry context can be defined as the affine line $\mathbb{A}^1_{\mathbb{C}} = \mathrm{Spec}\,\mathbb{C}[j]$ where you treat j just as a symbol representing a variable of a polynomial. Furthermore, you can give a $\mathbb{Q}$-model of $Y(1)$ by dictating that $\mathrm{Spec}\,\mathbb{Q}[j] =: Y(1)_{\mathbb{Q}}$ is "the cannocial model" of $Y(1)$ over $\mathbb{Q}$. You can even try to do this with $\mathbb{Z}$ instead of $\mathbb{Q}$; for the modular curve $Y(1)$, it turns out that this is the correct thing to do[19], but in general you need to ask yourself what is the meaning of "canonical model over $\mathbb{Z}$".

14.2. **Modular functions for $\Gamma_0(N)$.** Now we consider a variant of $j(\tau)$.

Definition 14.7. For $N \in \mathbb{N}$, let $j_N(\tau) := j(N\tau)$.

Proposition 14.8. *The function $j_N(\tau) : \mathbb{H} \to \mathbb{C}$ is a modular function for $\Gamma_0(N)$.*

Proof. Note that $N\tau = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \cdot \tau$ (we only talked about the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$, but really any 2×2 matrix with real entries and positive determinant acts on $\mathbb{H}$ by the same formula). Thus,

[19] Someone may argue otherwise and may want to exclude $2, 3$, i.e. it's a correct thing to do over $\mathbb{Z}[1/6]$. This is related to the fact that the action of $\mathrm{PSL}_2(\mathbb{Z})$ on $\mathbb{H}$ is not free at precisely the orbits of i and $e^{2\pi i/3}$ where the stabilizers are of order 2 and 3, respectively.

for $\gamma \in \Gamma_0(N)$ and $\tau \in \mathbb{H}$,

$$N\gamma \cdot \tau = \left(\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \gamma \begin{pmatrix} N^{-1} & 0 \\ 0 & 1 \end{pmatrix} \right) N\tau.$$

Therefore, we show that $j_N(\gamma \cdot \tau) = j_N(\tau)$ if we show that $\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \gamma \begin{pmatrix} N^{-1} & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. If we let $\gamma = \begin{pmatrix} a & b \\ Nc & d \end{pmatrix}$, then

$$\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \begin{pmatrix} N^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} Na & Nb \\ Nc & d \end{pmatrix} \begin{pmatrix} N^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & Nb \\ c & d \end{pmatrix}.$$

This is obviously in $\mathrm{SL}_2(\mathbb{Z})$ (determinant 1 is obvious because we are conjugating). To see if $j_N(\tau)$ is meromorphic at the cusps, we first enumerate all $\Gamma_0(N)$-equivalence classes of the cusps. This is the same as asking the representatives of the set of right cosets $\Gamma_0(N)\backslash \mathrm{SL}_2(\mathbb{Z})$. Let

$$C(N) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \ : \ ad = N, \ a > 0, \ 0 \leq b < d, \ \gcd(a, b, d) = 1 \right\}.$$

We claim that a right coset of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$ is of the form $[\gamma] := \left(\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} \mathrm{SL}_2(\mathbb{Z})\gamma \right) \cap \mathrm{SL}_2(\mathbb{Z})$ for a unique $\gamma \in C(N)$. Note first that such a set is stable under the action of $\Gamma_0(N)$ from the left; if $\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} A\gamma \in [\gamma]$ for $A \in \mathrm{SL}_2(\mathbb{Z})$, then for any $M \in \Gamma_0(N)$, as $\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} M \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} \in \mathrm{SL}_2(\mathbb{Z})$,

$$M \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} A\gamma = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} \left(\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} M \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} \right) A\gamma \in [\gamma].$$

Furthermore, if $\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} A_1\gamma, \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} A_2\gamma \in [\gamma]$, then

$$\left(\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} A_1\gamma \right) \left(\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} A_2\gamma \right)^{-1} = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} A_1 A_2^{-1} \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N),$$

as $\Gamma_0(N) = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} \mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \cap \mathrm{SL}_2(\mathbb{Z})$. This implies that $[\gamma]$ is a right $\Gamma_0(N)$-coset.

Now the claim is that, given any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, you may find a unique $\gamma \in C(N)$ such that there is $M \in \mathrm{SL}_2(\mathbb{Z})$ such that $M \begin{pmatrix} Na & Nb \\ c & d \end{pmatrix} = \gamma$. Firstly we show that we can make it an upper traingular matrix. This is the same as asking whether there exist $z, w \in \mathbb{Z}$ with

$\gcd(z, w) = 1$ such that $Naz + wc = 0$. Let $M = \gcd(c, N)$. Then we let $z = \frac{c}{M}$ and $w = -\frac{N}{M}a$. As $\gcd(a, c) = 1$ and $\gcd\left(\frac{c}{M}, \frac{N}{M}\right) = 1$, we have $\gcd(z, w) = 1$, as desired. Now we find $x, y \in \mathbb{Z}$ such that $xw - yz = 1$we have

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} Na & Nb \\ c & d \end{pmatrix} = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix},$$

where by the determinant consideration we have $AD = N$. By possibly negating x, y, z, w, we can assure that $A, D > 0$. Now by multiplying further on the left, we may perform a row operation of adding a multiple of one row to another, so we may assure that $0 \leq B < D$. We also have $\gcd(A, B, D) = 1$ as otherwise the original matrix $\begin{pmatrix} Na & Nb \\ c & d \end{pmatrix}$ would also have a nontrivial common divisor among its entries, which is impossible as $\gcd(c, d) = 1$. We have thus shown that there is some $\gamma \in C(N)$. The only thing we are left with showing for the right cosets is that, no two different elements of $C(N)$ are related by multiplication by an element in $\mathrm{SL}_2(\mathbb{Z})$ on the left. If $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \in C(N)$, and if $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$, then firstly $z = 0$, and as $xw = 1$ by the determinant condition, $x = w = \pm 1$. As $a, a' > 0$, we have $x = w = 1$. Then it is just about multiplying with $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ on the left, which do not give a new element in $C(N)$ by the exactly same reason as above (it is an elementary row operation as alluded above).

From what we have shown is, if $M \in \mathrm{SL}_2(\mathbb{Z})$, then $j_N(M \cdot \tau) = j\left(\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} M \cdot \tau\right) = j(\gamma\tau)$ for some $\gamma \in C(N)$. Let $\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. Then, from $j(\tau) = e^{-2\pi i\tau} + \sum_{n=0}^{\infty} a_n e^{2\pi in\tau}$, $a_n \in \mathbb{Z}$, as $\gamma \cdot \tau = \frac{a\tau+b}{d}$, we have

$$j(\gamma \cdot \tau) = e^{-2\pi ib/d} e^{-2\pi ia\tau/d} + \sum_{n=0}^{\infty} a_n e^{2\pi inb/d} e^{2\pi ina\tau/d} = e^{-2\pi ib/d} q^{-a/d} + \sum_{n=0}^{\infty} a_n e^{2\pi inb/d} q^{an/d}.$$

Thus this is a meromorphic Laurent q-expansion at the cusp (i.e. has a finite meromorphic tail). so we have finished showing that $j_N(\tau)$ is a modular function for $\Gamma_0(N)$. □

Obviously, $j(\tau)$ is also a modular function for $\Gamma_0(N)$. It turns out that all the modular functions for $\Gamma_0(N)$ are obtained as the rational functions in $j(\tau)$ and $j_N(\tau)$. The obvious question is: is there an algebraic relation between $j(\tau)$ and $j_N(\tau)$? It turns out that there is one.

Definition 14.9 (Modular equation). For $N \in \mathbb{N}$, we define the function $\Phi_N(X, \tau)$ as

$$\Phi_N(X, \tau) := \prod_{\gamma \in \Gamma_0(N) \backslash \mathrm{SL}_2(\mathbb{Z})} (X - j_N(\gamma \cdot \tau)).$$

This is a degree $|C(N)|$ polynomial in X with coefficients in holomorphic functions on $\mathbb{H}$.

Theorem 14.10. *Let $N \in \mathbb{N}$.*

(1) *The function $\Phi_N(X,\tau)$ is a polynomial in X with coefficients in* ***modular functions for*** $\mathrm{SL}_2(\mathbb{Z})$ ***holomorphic on*** $\mathbb{H}$*. Therefore, by Theorem 14.5, there exists a polynomial $\Phi_N(X,Y) \in \mathbb{C}[X,Y]$ in two variables X, Y such that $\Phi_N(X,\tau) = \Phi_N(X, j(\tau))$. We call $\Phi_N(X,Y)$ the* ***modular polynomial*** *for $\Gamma_0(N)$.*

(2) *The modular polynomial $\Phi_N(X,Y)$ is, as a polynomial in X, irreducible of degree $|C(N)| = N\prod_{p|N}\left(1+\frac{1}{p}\right)$.*

(3) *The modular functions for $\Gamma_0(N)$ are precisely the rational functions in $j(\tau)$ and $j_N(\tau)$. Namely, the field of modular functions for $\Gamma_0(N)$, denoted $K(Y_0(N))$, is given by $K(Y_0(N)) = \mathbb{C}(j, j_N) = \mathbb{C}(j)[T]/(\Phi_N(T,j))$.*

Among those, the modular functions for $\Gamma_0(N)$ that are holomorphic on $\mathbb{H}$ are precisely the polynomials in $j(\tau)$ and $j_N(\tau)$. Namely, the ring of modular functions for $\Gamma_0(N)$ holomorphic on $\mathbb{H}$, denoted $\mathcal{O}(Y_0(N))$, is given by $\mathcal{O}(Y_0(N)) = \mathbb{C}[j, j_N] = \mathbb{C}[j][T]/(\Phi_N(T,j))$.

(4) *For $N > 1$, we have $\Phi_N(X,Y) = \Phi_N(Y,X)$.*

(5) *The modular polynomial $\Phi_N(X,Y)$ has* ***integer coefficients****, i.e. $\Phi_N(X,Y) \in \mathbb{Z}[X,Y]$.*

(6) *If N is not a perfect square, then $\Phi_N(X,X)$ is a polynomial of degree > 1 whose leading coefficient is ± 1.*

(7) *If $N = p$ is a prime, then $\Phi_p(X,Y) \equiv (X^p - Y)(X - Y^p) \pmod{p}$.*

Proof. (1) We need to show that the coefficients of $\Phi_N(X,\tau)$ are holomorphic on $\mathbb{H}$, invariant under $\mathrm{SL}_2(\mathbb{Z})$-action, and is meromorphic at the cusps. Being holomorphic on $\mathbb{H}$ is obvious (already $j_N(\gamma\cdot\tau)$ is). Similarly, being meromorphic at the cusps is obvious (already $j_N(\gamma\cdot\tau)$ is). Finally, for the invariance under $\mathrm{SL}_2(\mathbb{Z})$-action, if we choose $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, then if we enumerate the right cosets of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$ as $\Gamma_0(N)\gamma_i$, $1 \le i \le |C(N)| = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$, then the invariance under the action of σ is the same as asking whether the right cosets $\Gamma_0(N)\gamma_i\sigma$ are precisely the right cosets in $\Gamma_0(N)\backslash \mathrm{SL}_2(\mathbb{Z})$, which is obvious.

(2) Firstly, it is quite easy to see that the analogue of Chinese Remainder Theorem for $\mathrm{SL}_2(\mathbb{Z})$ is true, i.e. for any tuple of pairwise coprime integers $(N_1, \cdots, N_m)$, the map $\mathrm{SL}_2(\mathbb{Z}) \to \prod_{i=1}^m \mathrm{SL}_2(\mathbb{Z}/N_i\mathbb{Z})$ is surjective. This implies that, if $(N,M) = 1$, then $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(NM)] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)][\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(M)]$. Thus, to show that $|C(N)| = N\prod_{p|N}\left(1+\frac{1}{p}\right)$, it suffices to show when $N = p^k$ is a prime power. In that case, we can just enumerate the matrices in $C(p^k)$. Namely, if $a = p^{k-i}$ and $d = p^i$, then unless either $i = 0$ or $i = k$, $0 \le b < d$ is such that $\gcd(a,b,d) = \gcd(b,p) = 1$, so there are $\frac{d(p-1)}{p}$ many choices for b. Therefore,

$$|C(p^k)| = 1 + \sum_{i=1}^{k-1} \frac{p^i(p-1)}{p} + p^k = p^k + p^{k-1},$$

which is what we want.

To show that $\Phi_N(X,Y)$ is irreducible as a polynomial in X, it suffices to show that $\Phi_N(X,j(\tau))$ is the minimal polynomial of $j_N(\tau)$ over $\mathbb{C}(j)$, the field of all modular functions for $\mathrm{SL}_2(\mathbb{Z})$. Let $\mathscr{M}$ be the field of all meromorphic functions on $\mathbb{H}$, and let $\mathscr{M}_N = \mathbb{C}(j,j_N)$, which is a subfield of $\mathscr{M}$. For $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, we obtain a homomorphism $\iota_\sigma : \mathscr{M}_N \to \mathscr{M}$, $f(\tau) \mapsto f(\sigma\cdot\tau)$. This is automatically injective as it is a field homomorphism. Furthermore, if $f \in \mathbb{C}(j)$, then obviously $\iota_\sigma(f) = f$. Now note that, from the proof of Proposition 14.8, the meromorphic tail of the q-expansion of $j_N(\sigma\cdot\tau)$ tells you which $\gamma \in C(N)$ does $\sigma \in [\gamma]$. Therefore, if σ, σ' are in different right cosets of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$, then $j_N(\sigma\cdot\tau) \neq j_N(\sigma'\cdot\tau)$. Therefore, there are at least $|C(N)|$ many distinct field embeddings of $\mathscr{M}_N$ into $\mathscr{M}$ fixing $\mathbb{C}(j)$. This implies that $[\mathscr{M}_N : \mathbb{C}(j)] \geq |C(N)|$. As the degree of $\Phi_N(X,Y)$ is of degree $|C(N)|$ as a polynomial in N, this implies that $\Phi_N(X,j(\tau))$ must be the minimal polynomial of $j_N(\tau)$ over $\mathbb{C}(j)$.

(3) Let $f(\tau)$ be a modular function for $\Gamma_0(N)$. As above, we enumerate the right cosets of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$ as $\Gamma_0(N)\gamma_i$, $1 \leq i \leq |C(N)|$. Consider the function

$$G(X,\tau) := \sum_{i=1}^{|C(N)|} f(\gamma_i\cdot\tau)\prod_{j\neq i}(X - j_N(\gamma_j\cdot\tau)).$$

This is a polynomial in X with coefficients being meromorphic functions on $\mathbb{H}$ with meromorphic q-expansion at cusps. We claim that the coefficients of $G(X,\tau)$ are actually modular functions for $\mathrm{SL}_2(\mathbb{Z})$. For this, we only need to show that $G(X,\tau) = G(X,\sigma\cdot\tau)$ for $\sigma \in \mathrm{SL}_2(\mathbb{Z})$. As we already know $\Phi_N(X,j(\tau))$ has coefficients being modular functions for $\Gamma_0(N)$, it suffices to show that $H(X,\tau) = H(X,\sigma\cdot\tau)$, where

$$H(X,\tau) := \sum_{i=1}^{|C(N)|} \frac{f(\gamma_i\cdot\tau)}{X - j_N(\gamma_i\cdot\tau)}.$$

However, we know that both f and j_N are modular functions for $\Gamma_0(N)$, so $H(X,\tau) = H(X,\sigma\cdot\tau)$ follows from the fact that $\Gamma_0(N)\gamma_i\sigma$ runs over all right cosets of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. As $G(X,\tau)$ has coefficients being modular functions for $\mathrm{SL}_2(\mathbb{Z})$, by Theorem 14.5, $G(X,\tau) \in \mathbb{C}(j)[X]$.

We can arrange γ_i's so that $\gamma_1 = 1$. Then, $\frac{\partial\Phi_N}{\partial X}(j_N(\tau),j(\tau)) = \prod_{j\neq 1}(j_N(\tau) - j_N(\gamma_i\cdot\tau))$. Thus,

$$G(j_N(\tau),\tau) = f(\tau)\frac{\partial\Phi_N}{\partial X}(j_N(\tau),j(\tau)).$$

As $\Phi_N(X,j(\tau))$ is irreducible over $\mathbb{C}(j)$, and as $j_N(\tau)$ is a root of $\Phi_N(X,j(\tau))$, we have $\frac{\partial\Phi_N}{\partial X}(j_N(\tau),j(\tau)) \neq 0$. Therefore, $f(\tau) = \frac{G(j_N(\tau),\tau)}{\frac{\partial\Phi_N}{\partial X}(j_N(\tau),j(\tau))}$. As both the numerator and the denominator are in $\mathbb{C}(j,j_N)$, we get that $f(\tau) \in \mathbb{C}(j,j_N)$.

Suppose now that f is holomorphic on $\mathbb{H}$. Then, the coefficients of $G(X,\tau)$ are the modular functions holomorphic on $\mathbb{H}$, so $G(X,\tau) \in \mathbb{C}[j][X]$. Therefore, it suffices to show that

$\frac{\partial \Phi_N}{\partial X}(j_N(\tau), j(\tau)) \neq 0$ for any $\tau \in \mathbb{H}$, or that $j_N(\tau) \neq j_N(\gamma_i \cdot \tau)$ for any $\tau \in \mathbb{H}$. Supopse the contrary that $j_N(\tau) = j_N(\gamma_i \cdot \tau)$ for some $i \geq 2$ and $\tau \in \mathbb{H}$. As $j : \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}$ is bijective, this means that there exists $M \in \mathrm{SL}_2(\mathbb{Z})$ such that $M \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \gamma_i$. This means that $\gamma_i \in \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} \mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \cap \mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(N)$, which contradicts the assumption that $\Gamma_0(N)\gamma_i \neq \Gamma_0(N)$. Thus, we see that $f(\tau)$ is a polynomial in $j(\tau)$ and $j_N(\tau)$.

(4) Note that $\Phi_N(X, j(\tau))$ can be expressed alternatively as

$$\Phi_N(X, j(\tau)) = \prod_{\gamma \in C(N)} (X - j(\gamma \cdot \tau)).$$

As $\begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix} \in C(N)$ and as $\begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix} \cdot \tau = \frac{\tau}{N}$, this implies that $\Phi_N(j(\tau/N), j(\tau)) = 0$, or $\Phi_N(j(\tau), j_N(\tau)) = 0$. Therefore, the polynomial $\Phi_N(j(\tau), X) \in \mathbb{C}[j][X]$ is divisible by the minimal polynomial of $j_N(\tau)$ over $\mathbb{C}[j]$ which is $\Phi_N(X, j(\tau))$. Therefore, $\Phi_N(j(\tau), X) = g(X)\Phi_N(X, j(\tau))$ for $g(X) \in \mathbb{C}(j)[X]$. By the Gauss Lemma, we know that $g(X) \in \mathbb{C}[j][X]$, i.e. there is $G(X, Y) \in \mathbb{C}[X, Y]$ such that $g(X) = G(X, j(\tau))$. Thus,

$$\Phi_N(j(\tau), X) = G(X, j(\tau))\Phi_N(X, j(\tau)) = G(X, j(\tau))G(j(\tau), X)\Phi_N(j(\tau), X),$$

so $G(X, j(\tau))G(j(\tau), X) = 1$. As $j(\tau)$ is not an algebraic function (otherwise it would not have a q-expansion), this implies that $G(X, Y)G(Y, X) = 1$ as polynomials in $\mathbb{C}[X, Y]$. This implies that $G(X, Y) = G(Y, X) = \pm 1$. If $G(X, Y) = -1$, then $\Phi_N(j(\tau), X) = -\Phi_N(X, j(\tau))$, so in particular $\Phi_N(j(\tau), j(\tau)) = 0$. However, as $\Phi_N(X, j(\tau))$ is irreducible over $\mathbb{C}(j)$, this is impossible if $|C(N)| > 1$, which is the case when $N > 1$. Therefore, $G(X, Y) = 1$, and we have $\Phi_N(X, j(\tau)) = \Phi_N(j(\tau), X)$, or $\Phi_N(X, Y) = \Phi_N(Y, X)$ as again $j(\tau)$ is not algebraic.

(5) We know that the q-expansion of $j(\gamma \cdot \tau)$ for $\gamma \in C(N)$ has coefficients in $\mathbb{Z}[\zeta_N]$. Therefore, the coefficients of $\Phi_N(X, j(\tau))$, which are the symmetric functions in $j(\gamma \cdot \tau)$, γ ranging over $C(N)$, are polynomials in $j(\tau)$ whose q-expansions have coefficients in $\mathbb{Z}[\zeta_N]$. We want to show that these coefficients are in fact integers. Let $\sigma_x \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ be the Galois element that sends $\zeta_N \mapsto \zeta_N^x$. Then, after applying σ_x to the coefficients of the q-expansion of $j(\gamma \cdot \tau)$, $\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(N)$, we have

$$\sigma_x\left(j(\gamma \cdot \tau)\right) = e^{-2\pi i b x/d} q^{-a/d} + \sum_{n=0}^{\infty} a_n e^{2\pi i n b x/d} q^{na/d}.$$

This is however the q-expansion of $j(\gamma_x \cdot \tau)$ where $\gamma_x = \begin{pmatrix} a & bx \pmod{d} \\ 0 & d \end{pmatrix} \in C(N)$ where $bx \pmod{d}$ is the integer in between 0 and $d - 1$ congruent to bx mod d (note that $\gcd(a, bx \pmod d, d) = \gcd(a, bx, d) = 1$ as $\gcd(x, N) = 1$ and a, d divide N). Therefore, $\sigma_x(\gamma) := \gamma_x$ gives a permutation of $C(N)$. Therefore, the action of σ_x on the coefficients of the q-expansion of a symmetric function in $j(\gamma \cdot \tau)$, γ ranging over $C(N)$, makes no change of the coefficients. This implies that the q-expansions of the coefficients of $\Phi_N(X, j(\tau))$ have integer coefficients. This implies that the coefficients of $\Phi_N(X, j(\tau))$ are integer polynomials in $j(\tau)$ (this just follows from the same argument that you eliminate meromorphic tails one by one, and each process the difference is an integer monomial in $j(\tau)$), or $\Phi_N(X, j(\tau)) \in \mathbb{Z}[j][X]$, or $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$.

(6) If N is not a perfect square, then for any $\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(N)$, $a \neq d$. Therefore, the q-expansion of $j(\tau) - j(\gamma \cdot \tau)$ has the meromorphic tail $q^{-1} - e^{-2\pi i b/d} q^{-a/d}$, so the lowest order term of the meromorphic tail is either q^{-1} or $-e^{-2\pi i b/d} q^{-a/d}$. In particular, the coefficient of the lowest order term of the meromorphic tail is always a root of unity. Now the lowest order term of the meromorphic tail of the q-expansion of $\Phi_N(j(\tau), j(\tau))$ is a product of such terms, so its coefficient is again a root of unity. On the other hand, $\Phi_N(j(\tau), j(\tau))$ is a polynomial in $j(\tau)$, so its coefficient of the lowest order term of the q-expansion is an integer. Therefore, this coefficient must be ± 1. This implies that $\Phi_N(X, X)$ has the leading coefficient ± 1.

(7) Let $N = p$ be a prime. Then $C(p) = \{\sigma_0, \cdots, \sigma_{p-1}, \sigma_p\}$, where $\sigma_k = \begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix}$ for $0 \leq k \leq p-1$ and $\sigma_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. Therefore, we have

$$j(\sigma_k \cdot \tau) = e^{-2\pi i k/p} q^{-1/p} + \sum_{n=0}^{\infty} a_n e^{2\pi i n k/p} q^{n/p}, \quad 0 \leq k \leq p-1,$$

and

$$j(\sigma_p \cdot \tau) = q^{-p} + \sum_{n=0}^{\infty} a_n q^{np}.$$

We use $\zeta_p = e^{2\pi i/p}$ and $\pi = \zeta_p - 1$. Then,

$$j(\sigma_k \cdot \tau) = \zeta^{-k} q^{-1/p} + \sum_{n=0}^{\infty} a_n \zeta_p^{nk} q^{n/p} \equiv q^{-1/p} + \sum_{n=0}^{\infty} a_n q^{n/p} \pmod{\pi}, \quad 0 \leq k \leq p-1.$$

Therefore, if we look at $\Phi_N(X, j(\tau))$ as an element of polynomials in X with coefficients in meromorphic q-expansions with integer coefficients (i.e. $\Phi_N(X, j(\tau)) \in \mathbb{Z}[[q]](q^{-1})[X]$), we have

$$\Phi_N(X, j(\tau)) \equiv \left(X - \left(q^{-1/p} + \sum_{n=0}^{\infty} a_n q^{n/p} \right) \right)^p \left(X - \left(q^{-p} + \sum_{n=0}^{\infty} a_n q^{np} \right) \right) \pmod{\pi},$$

where the congruence is first seen in a slightly bigger ring $\mathbb{Z}[\zeta_p][[q^{1/p}]](q^{-1/p})[X]$. Note that, in characteristic p, we have $(Y+Z)^p = Y^p + Z^p$, and also for any integer M, $M^p = M$. Therefore,

$$\left(X - \left(q^{-1/p} + \sum_{n=0}^{\infty} a_n q^{n/p}\right)\right)^p \equiv X^p - \left(q^{-1/p} + \sum_{n=0}^{\infty} a_n q^{n/p}\right)^p \equiv X^p - \left(q^{-1} + \sum_{n=0}^{\infty} a_n q^{n}\right) \pmod{\pi},$$

which means that

$$\Phi_N(X, j(\tau)) = \left(X^p - \left(q^{-1} + \sum_{n=0}^{\infty} a_n q^n\right)\right)\left(X - \left(q^{-p} + \sum_{n=0}^{\infty} a_n q^{np}\right)\right) \pmod{\pi}.$$

As both sides are now in $\mathbb{Z}[[q]](q^{-1})[X]$ and $\pi\mathbb{Z}[\zeta_p] \cap \mathbb{Z} = p\mathbb{Z}$, this implies that

$$\Phi_N(X, j(\tau)) = \left(X^p - \left(q^{-1} + \sum_{n=0}^{\infty} a_n q^n\right)\right)\left(X - \left(q^{-p} + \sum_{n=0}^{\infty} a_n q^{np}\right)\right) \pmod{p}.$$

As $q^{-1} + \sum_{n=0}^{\infty} a_n q^n$ is the q-expansion of the j-function, this means that

$$\Phi_N(X, j(\tau)) = (X^p - j(\tau))(X - j(\tau)^p) \pmod{p}.$$

Therefore, $\Phi_N(X, Y) = (X^p - Y)(X - Y^p) \pmod{p}$.

□

Remark 14.11 (Canonical model of the modular curve $Y_0(N)$; for those who know algebraic geometry)**.** This first means that the modular curve $Y_0(N) =: \Gamma_0(N)\backslash\mathbb{H}$ of level $\Gamma_0(N)$ is algebraically identified with $\operatorname{Spec} \mathbb{C}[j][T]/(\Phi_N(T, j))$. And then, you can define "the canonical model" of $Y_0(N)$ over $\mathbb{Q}$ as $Y_0(N)_{\mathbb{Q}} := \operatorname{Spec} \mathbb{Q}[j][T]/(\Phi_N(T, j))$. As before, you may want to do this for $\mathbb{Z}$ instead of $\mathbb{Q}$, but in general this is not the philosophically corect thing to do. Namely, bad things can happen at certain "bad" primes; here, a "bad" prime is a prime p that divides N.[20] For example, $\Phi_N(X, Y)$ mod p for $p|N$ may not give a "correct" modular equation mod p. However, it is actually OK if p^2 does not divide N. Therefore, $\operatorname{Spec} \mathbb{Z}[1/M][j][T]/(\Phi_N(T, j))$ is the correct integral model over $\mathbb{Z}[1/M]$ for $M = \prod_{p^2|N} p$. In particular, Theorem 14.10(7) is related to what's called the **Eichler–Shimura congruence relation**.

We also need the following result that connects the modular polynomial Φ_N with the lattices in $\mathbb{C}$ (=elliptic curves over $\mathbb{C}$).

Definition 14.12. Let $\Lambda, \Lambda' \subset \mathbb{C}$ be lattices (=elliptic curves over $\mathbb{C}$). An isogeny $f : \Lambda' \to \Lambda$ is called a **cyclic isogeny** of order N if $\operatorname{coker} f \cong \mathbb{Z}/N\mathbb{Z}$.

Proposition 14.13. *Let $N \in \mathbb{N}$ and $\tau \in \mathbb{H}$. Let $\mathbb{Z} \oplus \mathbb{Z}\tau \subset \mathbb{C}$ be the corresponding lattice (=elliptic curve over $\mathbb{C}$). Then there are one-to-one bijections between the following sets:*

(1) the roots of the polynomial $\Phi_N(X, j(\tau)) \in \mathbb{C}[X]$;

[20] Again, someone may also want to include 2 and 3 in the list of "bad" primes.

(2) the points $\gamma \cdot \tau \in \mathbb{H}$ for $\gamma \in C(N)$;

(3) the lattices (=elliptic curves over $\mathbb{C}$) $\Lambda \subset \mathbb{C}$, up to isomorphism, admitting a cyclic isogeny $f : \Lambda \to \mathbb{Z} \oplus \mathbb{Z}\tau$ of order N.

The bijections between (1), (2), (3) are $j(\gamma \cdot \tau) \leftrightarrow \gamma \cdot \tau \leftrightarrow \mathbb{Z} \oplus \mathbb{Z}(\gamma \cdot \tau)$ (for $\gamma \in C(N)$).

Proof. The correspondence between (1) and (2) is an immediate consequence of the definition of Φ_N and Theorem 14.10(2). For (3), this is classifying the sublattices $\Lambda \subset \mathbb{Z} \oplus \mathbb{Z}\tau$ such that $\frac{\mathbb{Z} \oplus \mathbb{Z}\tau}{\Lambda} \cong \mathbb{Z}/N\mathbb{Z}$ up to isomorphism. Note that if Λ is an index N sublattice of $\mathbb{Z} \oplus \mathbb{Z}\tau$, then this must contain $N\mathbb{Z} \oplus N\mathbb{Z}\tau$. Thus, without worrying about isomorphisms, we are just finding the subgroups of $(\mathbb{Z}/N\mathbb{Z})^2 = \frac{\mathbb{Z} \oplus \mathbb{Z}\tau}{N\mathbb{Z} \oplus N\mathbb{Z}\tau}$ whose quotient is $\mathbb{Z}/N\mathbb{Z}$. This is just parametrized by the surjective homomorphisms $(\mathbb{Z}/N\mathbb{Z})^2 \twoheadrightarrow \mathbb{Z}/N\mathbb{Z}$, or where $(1,0)$ and $(0,1)$ go to in $\mathbb{Z}/N\mathbb{Z}$. Let $(1,0) \mapsto x$ and $(0,1) \mapsto y$. Then this homomorphism being surjective is the same as $\gcd(x, y, N) = 1$. The corresponding sublattice $\Lambda \subset \mathbb{Z} \oplus \mathbb{Z}\tau$ is

$$\Lambda = \{m + n\tau \ : \ m, n \in \mathbb{Z},\ mx + ny \equiv 0 \pmod{N}\}.$$

Let $a = \gcd(x, N)$ and $d = \frac{N}{a}$. Then, by definition, $\gcd(a, y) = 1$. Therefore, if $mx + ny \equiv 0 \pmod{N}$, then $N|ny$, so $a|n$. Let $n = an'$ and $x = ax'$. Then,

$$\Lambda = \{m + an'\tau \ : \ m, n' \in \mathbb{Z},\ mx' + n'y \equiv 0 \pmod{d}\}.$$

As $\gcd(x', d) = 1$, this congruence condition can be simplified into $m \equiv -\frac{n'y}{x'} \pmod{d}$. Let b be the integer such that $0 \leq b \leq d-1$ and $b \equiv -\frac{y}{x'} \pmod{d}$. Then,

$$\Lambda = \{m + an'\tau \ : \ m, n' \in \mathbb{Z},\ m \equiv n'b \pmod{d}\} = d\mathbb{Z} \oplus (a\tau + b)\mathbb{Z} = d\left(\mathbb{Z} \oplus \frac{a\tau + b}{d}\mathbb{Z}\right).$$

Note that what we have found so far implies that $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(N)$. Conversely, this also shows that $d\left(\mathbb{Z} \oplus \frac{a\tau+b}{d}\mathbb{Z}\right)$ for $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(N)$ gives rise to a sublattice with quotient $\cong \mathbb{Z}/N\mathbb{Z}$. Thus, this implies that a map from (2) to (3) is well-defined and surjective. Injectivity follows from the fact that no two elements of $C(N)$ are $\mathrm{SL}_2(\mathbb{Z})$-translates of one another. □

15. **Explicit class field theory** for imaginary quadratic fields

15.1. **First Main Theorem: from j-invariants to ring class fields.**

The first main point of the **Explicit class field theory** of K is that the ring class field $K(\mathcal{O})$ can be obtained by adjoining K with explicit values of the j-function (!).

Theorem 15.1 (First Main Theorem of Complex Multiplication). *Let $\tau \in \mathbb{H}$ be a quadratic number, corresponding to a lattice (=elliptic curve over $\mathbb{C}$) $\mathbb{Z} \oplus \mathbb{Z}\tau \subset \mathbb{C}$ with complex multiplication by an order $\mathcal{O} = \mathrm{End}(\mathbb{Z} \oplus \mathbb{Z}\tau)$ in an imaginary quadratic field $K = \mathbb{Q}(\tau)$. Then, $j(\tau)$ is an algebraic integer (!) and $K(\mathcal{O}) = K(j(\tau))$ (!!).*

Proof. Suppose that $\alpha \in \mathcal{O}$ such that $[\alpha] : \mathbb{Z} \oplus \mathbb{Z}\tau \to \mathbb{Z} \oplus \mathbb{Z}\tau$, $x \mapsto \alpha x$, is a cyclic isogeny (necessarily of order $N_{K/\mathbb{Q}}(\alpha)$). Then, by Proposition 14.13, $j(\tau)$ is a root of $\Phi_{N_{K/\mathbb{Q}}(\alpha)}(X, j(\tau))$. Therefore, $j(\tau)$ is a root of the polynomial $\Phi_{N_{K/\mathbb{Q}}(\alpha)}(X, X) \in \mathbb{Z}[X]$. If we also know that $N_{K/\mathbb{Q}}(\alpha)$ is not a perfect square, then Theorem 14.10(6) will imply that $j(\tau)$ is an algebraic integer.

Thus, the proof that $j(\tau)$ is an algebraic integer for quadratic τ will be done if we show the following.

Lemma 15.2. *Let $\mathcal{O} \subset K$ be an order in an imaginary quadratic field, and let $\mathfrak{a} \subset \mathcal{O}$ be a proper $\mathcal{O}$-ideal. Then, there exists $\alpha \in \mathcal{O}$ such that*

- $N = N_{K/\mathbb{Q}}(\alpha)$ *is not a perfect square, and*
- $\mathfrak{a}/\alpha\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}$ *(as abelian groups).*

Proof. We know that $\mathcal{O} = \mathbb{Z} \oplus f\mathcal{O}_K$ for the conductor $f \in \mathbb{N}$ of $\mathcal{O}$. Let $d = \operatorname{disc}(K)$. Then, $\beta = \frac{d+\sqrt{d}}{2}$ is always in $\mathcal{O}_K$ (in fact $\mathcal{O}_K = \mathbb{Z}[\beta] = \mathbb{Z} \oplus \mathbb{Z}\beta$; note that $\beta^2 = d\beta + \frac{d-d^2}{4}$). We claim that, unless $K = \mathbb{Q}(\sqrt{-2})$, $\alpha = f\beta$ satisfies the two properties. Firstly, $N_{K/\mathbb{Q}}(\alpha) = f^2\frac{d^2-d}{2}$. If this is a perfect square, then as $\gcd(d-1, d) = 1$, either $d-1 = -2a^2$ and $d = -b^2$ or $d-1 = -a^2$ and $d = -2b^2$. Note that either $d = n$ for a negative square-free number $n \equiv 1 \pmod 4$ or $d = 4n$ for a negative square-free number $n \not\equiv 1 \pmod 4$. In the former case, d is odd, so it must be that $d - 1 = -2a^2$ and $d = -b^2$, but as d is square-free, $b = 1$, so $d = -1$, which is not congruent to $1 \pmod 4$. In the latter case, d is even, so it must be $d - 1 = -a^2$ and $d = -2b^2$. As $d = 4n$ for a negative square-free number $n \not\equiv 1 \pmod 4$, this implies that $2|b$, so $d = -8c^2$ for some $c \in \mathbb{Z}$, and this implies that $2|n$. As n is square-free, it turns out that $c = 1$, so $d = -8$, which is what we are excluding at the moment. Thus, the first condition is satisfied (as long as $K \neq \mathbb{Q}(\sqrt{-2})$). For the second condition, consider the short exact sequence

$$0 \to \mathfrak{a}/\alpha\mathfrak{a} \to \mathcal{O}/\alpha\mathfrak{a} \to \mathcal{O}/\mathfrak{a} \to 0.$$

As $\#\mathfrak{a}/\alpha = \frac{[\mathcal{O}:\alpha\mathfrak{a}]}{[\mathcal{O}:\mathfrak{a}]} = N$, we know that $\mathfrak{a}/\alpha\mathfrak{a}$ has the correct order. If it is not cyclic, then by the structure theorem for finite abelian groups, there is a subgroup of $\mathfrak{a}/\alpha\mathfrak{a}$ isomorphic to $(\mathbb{Z}/h\mathbb{Z})^2$ for some $h > 1$. Therefore, there exists $\alpha\mathfrak{a} \subset \mathfrak{b} \subset \mathfrak{a}$ such that $\mathfrak{b}/\alpha\mathfrak{a} \cong (\mathbb{Z}/h\mathbb{Z})^2$. As abelian groups, $\mathfrak{b}$ is free of rank 2, and as $\mathfrak{b}/\alpha\mathfrak{a}$ is of exponent h, $h\mathfrak{b} \subset \alpha\mathfrak{a}$. On the other hand, as $[\mathfrak{b} : h\mathfrak{b}] = h^2$, this implies that $h\mathfrak{b} = \alpha\mathfrak{a}$. This implies that $\mathfrak{b} = h^{-1}\alpha\mathfrak{a}$ is an $\mathcal{O}$-ideal, and $\alpha\mathcal{O} = h\mathfrak{b}\mathfrak{a}^{-1}$. On the other hand, as $\mathfrak{b} \subset \mathfrak{a}$, so $\mathfrak{b}\mathfrak{a}^{-1} \subset \mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. Therefore, $\alpha\mathcal{O} \subset h\mathcal{O}$, which implies that $\frac{\alpha}{h} \in \mathcal{O}$. On the other hand, $\alpha = f\beta$ and $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}f\beta$, so $\frac{\alpha}{h} \in \mathcal{O}$ implies that $h = 1$, contradicting the assumption.

The only exclusion we made was $K = \mathbb{Q}(\sqrt{-2})$. Then $\mathcal{O} = \mathbb{Z} \oplus f\sqrt{-2}\mathbb{Z}$. What we did above shows that the second condition $\mathfrak{a}/\alpha\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}$ can be replaced with the condition that $\frac{\alpha}{h} \in \mathcal{O}$ for $h \in \mathbb{N}$ implies $h = 1$. Now here you could choose $\alpha = f\sqrt{-2}$, then $N = 2f^2$ is not a square, and the second condition is also clearly satisfied. □

To show $K(\mathcal{O}) = K(j(\tau))$, we will use Corollary 12.21. Note that we already know $K(\mathcal{O})$ is Galois over K, but not necessarily for $K(j(\tau))$. Moreover, as $K/\mathbb{Q}$ is Galois, $K(\mathcal{O})/\mathbb{Q}$ is Galois. Therefore, we want to show that all but finitely many primes of $\mathcal{S}(K(\mathcal{O})/\mathbb{Q})$ are contained in

$\mathcal{S}(K(j(\tau))/\mathbb{Q})$, and all but finitely many primes of $\overline{\mathcal{S}}(K(j(\tau))/\mathbb{Q})$ are contained in $\mathcal{S}(K(\mathcal{O})/\mathbb{Q})$. Note first that $p \in \mathcal{S}(K(\mathcal{O})/\mathbb{Q})$ if and only if $p = \mathfrak{p}\overline{\mathfrak{p}}$ splits completely in K (with $\mathfrak{p} \neq \overline{\mathfrak{p}}$) and $\mathfrak{p}$ splits completely in $K(\mathcal{O})$, but $\mathfrak{p}$ splitting completely in $K(\mathcal{O})$ is the same as $[\mathfrak{p}] = 1$ in $\mathrm{Cl}(\mathcal{O})$, or $\mathfrak{p} = \alpha\mathcal{O}_K$ for $\alpha \in \mathcal{O}$. Therefore, up to a finite difference, $\mathcal{S}(K(\mathcal{O})/\mathbb{Q})$ is the set of primes p such that $p = N_{K/\mathbb{Q}}(\alpha)$ for $\alpha \in \mathcal{O}$.

- For $\mathcal{S}(K(\mathcal{O})/\mathbb{Q}) - S \subset \mathcal{S}(K(j(\tau))/\mathbb{Q})$, for a finite set S.

  Let $p \in \mathcal{S}(K(\mathcal{O})/\mathbb{Q})$ such that p is unramified in $K(j(\tau))$. Then, up to a finite difference, $p = N_{K/\mathbb{Q}}(\alpha)$ for $\alpha \in \mathcal{O}$. Then $\mathbb{Z} \oplus \mathbb{Z}\tau \to \mathbb{Z} \oplus \mathbb{Z}\tau$, $x \mapsto \alpha x$, is a cyclic isogeny of order p (cyclic because p is a prime). Therefore, $\Phi_p(j(\tau), j(\tau)) = 0$. This implies that $(j(\tau)^p - j(\tau))^2$ is divisible by p. Let $\mathfrak{P}$ be a prime of $K(j(\tau))$ lying over p. Then $j(\tau)^p \equiv j(\tau) \pmod{\mathfrak{P}}$. Note that $\mathcal{O}_{K(j(\tau))} \supset \mathbb{Z}[j(\tau)]$ may not be the same, but it is of finite index, and as long as p does not divide $[\mathcal{O}_{K(j(\tau))} : \mathbb{Z}[j(\tau)]]$ (which excludes finitely many priems), $\alpha^p \equiv \alpha \pmod{\mathfrak{P}}$ for every $\alpha \in \mathcal{O}_{K(j(\tau))}$. Thus $f(\mathfrak{P}|p) = 1$ for any $\mathfrak{P}$ over p. This implies that p splits completely in $K(j(\tau))$ up to a finite difference.

  This implies that $K(\mathcal{O}) \supset K(j(\mathfrak{a}))$ for all proper fractional $\mathcal{O}$-ideals $\mathfrak{a}$. Let $\mathfrak{a}_1, \cdots, \mathfrak{a}_{\#\,\mathrm{Cl}(\mathcal{O})}$ be the classes of $\mathrm{Cl}(\mathcal{O})$. Then $\Delta = \prod_{i<j}(j(\mathfrak{a}_i) - j(\mathfrak{a}_j))$ is a nonzero element of $\mathcal{O}_{K(\mathcal{O})}$.

- For $\overline{\mathcal{S}}(K(j(\tau))/\mathbb{Q}) - S \subset \mathcal{S}(K(\mathcal{O})/\mathbb{Q})$, for a finite set S.

  Let $p \in \overline{\mathcal{S}}(K(j(\tau))/\mathbb{Q})$. This in particular implies that p splits completely in K, so $p = N(\mathfrak{p})$ for some prime ideal $\mathfrak{p}$ of K. As long as p does not divide the conductor of $\mathcal{O}$, then $p = N(\mathfrak{p}) = N(\mathfrak{p} \cap \mathcal{O})$. We want to show that for all but finitely many such p, $\mathfrak{p} \cap \mathcal{O} = \alpha\mathcal{O}$ for some $\alpha \in \mathcal{O}$, which will show that $p = N_{K/\mathbb{Q}}(\alpha)$, so that $p \in \mathcal{S}(K(\mathcal{O})/\mathbb{Q})$. We can exclude finitely many p at any point, so we further assume that j is coprime to Δ.

  Let $\mathfrak{a}$ be the proper $\mathcal{O}$-ideal corresponding to $\mathbb{Z} \oplus \mathbb{Z}\tau$. Let $\mathfrak{a}' = (\mathfrak{p} \cap \mathcal{O})\mathfrak{a}$. Then it is of index p inside $\mathfrak{a}$, so $\mathfrak{a}' \to \mathfrak{a}$ is a cyclic isogeny of order p. Thus, $\Phi_p(j(\mathfrak{a}'), j(\mathfrak{a})) = 0$. Let $\mathfrak{P}$ be a prime of $K(j(\tau))$ above p such that $f(\mathfrak{P}|p) = 1$ (which exists as $p \in \overline{\mathcal{S}}(K(j(\tau))/\mathbb{Q})$). Let $\mathfrak{P}'$ be a prime of $K(\mathcal{O})$ above $\mathfrak{P}$. Then $\Phi_p(j(\mathfrak{a}'), j(\mathfrak{a})) = 0$ implies that $(j(\mathfrak{a}')^p - j(\mathfrak{a}))(j(\mathfrak{a}') - j(\mathfrak{a})^p) \equiv 0 \pmod{\mathfrak{P}'}$. As $f(\mathfrak{P}|p) = 1$, we have $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\mathfrak{P}}$, so in any case $j(\mathfrak{a})^p \equiv j(\mathfrak{a}') \pmod{\mathfrak{P}'}$. As p is coprime to Δ, this means that $j(\mathfrak{a}) = j(\mathfrak{a}')$. This means that $\mathfrak{p} \cap \mathcal{O}$ is a principal $\mathcal{O}$-ideal, which is what we wanted.

□

We also know how $\mathrm{Gal}(K(\mathcal{O})/K)$ acts on $j(\tau)$, in the sense of reciprocity law.

Theorem 15.3 (Reciprocity law for j-invariants)**.** *Let $\mathcal{O}$ be an order in an imaginary quadratic field K. Let $\mathfrak{a}$ be a proper $\mathcal{O}$-ideal, so that $j(\mathfrak{a}) \in K(\mathcal{O})$ by Theorem 15.1. For $\alpha \in C_K$, we have*

$$\mathrm{Art}_K(\alpha)(j(\mathfrak{a})) = j(\mathfrak{a}_\alpha^{-1}\mathfrak{a}),$$

where $\mathfrak{a}_\alpha$ is a proper $\mathcal{O}$-ideal representing the image of α by the natural quotient map $C_K \twoheadrightarrow \mathrm{Cl}(\mathcal{O})$ obtained in Theorem 13.29(4).

To deduce this, we divert our attention slightly to the **(meromorphic) modular forms**.

Definition 15.4 (Modular forms)**.** Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup, and let $k \in \mathbb{Z}$ be an integer. A **meromorphic modular form** of weight k and level Γ is a meromorphic function $f : \mathbb{H} \to \mathbb{C}$ such that the following conditions hold.

(1) (**Modularity**) For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, $f(\gamma \cdot \tau) = (c\tau + d)^k f(\tau)$.

(2) (**Meromorphy at cusps**) At each cusp $c \in \mathbb{P}^1_{\mathbb{Q}}$, $f(\tau)$ is meromorphic at c.

A **weakly holomorphic modular form** is a **holomorphic** function $f : \mathbb{H} \to \mathbb{C}$ which is a meromorphic modular form.

A **modular form** is a weakly holomorphic modular form satisfying a stronger condition, **Holomorphy at cusps**.

(2)' (**Holomorphy at cusps**) At each cusp $c \in \mathbb{P}^1_{\mathbb{Q}}$, $f(\tau)$ is holomorphic at c, i.e. the q-expansion has no meromorphic tail.

A **cusp form** is a modular form satisfying a stronger condition, **Cuspidality at cusps**.

(2)' (**Cuspidality at cusps**) At each cusp $c \in \mathbb{P}^1_{\mathbb{Q}}$, $f(\tau)$ is holomorphic at c and furthermore $f(c) = 0$. Namely, the q-expansion of f at c has no nonpositive powers of q in it.

It is clear that any type of the above forms is closed under addition and scalar multiplication. Furthermore, if you multiply two forms of the same type with the same level and weights k and ℓ, then the product is of the same level and weight $k + \ell$. If $\Gamma = \Gamma(N)$, then we simply say that a form is of level N.

Example 15.5.

(1) For a congruence group Γ, the modular functions for Γ are precisely the meromorphic modular forms of weight 0 and level Γ. The modular functions for Γ holomorphic on $\mathbb{H}$ (e.g. $j(\tau)$) are precisely the weakly holomorphic modular forms of weight 0 and level Γ.

(2) As seen in the proof of Proposition 13.14(2), the Eisenstein series $G_{2k}(\tau)$ is a modular form of weight $2k$ and level 1. As its q-expansion at ∞ has a constant term some nonzero multiple of $\zeta(2k)$, it is nonzero, so $G_{2k}(\tau)$ is not a cusp form.

(3) As seen in the proof of Lemma 14.4, the q-expansion of $g_2(\tau)^3 - 27g_3(\tau)^2$ at ∞ starts with the q-term. Furthermore, both $g_2(\tau)^3$ and $g_3(\tau)^2$ are of level 1 and weight 12 ($12 = 4\times 3 = 6\times 2$). Thus, $g_2(\tau)^3 - 27g_3(\tau)^3$ is a cusp form of weight 12 and level 1. This function $\Delta(\tau) := g_2(\tau)^3 - 27g_3(\tau)^2$ is called the **modular dicriminant**. As shown in Proposition 13.14(4), $\Delta(\tau) \neq 0$ for every $\tau \in \mathbb{H}$ (on the other hand, by cuspidality, "$\Delta(\infty) = 0$").

We are particularly interested in integrality properties of ratios of values of Δ.

Theorem 15.6. *Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a 2×2 matrix with integer entries such that $\deg \gamma = N$ is a positive integer. Let*

$$\varphi_\gamma(\tau) := N^{12} \frac{\Delta(\gamma \cdot \tau)}{(c\tau + d)^{12}\Delta(\tau)}.$$

1. *The function φ_γ is integral over $\mathbb{Z}[j]$.*
2. *For $\tau \in \mathbb{H}$ quadratic, $\varphi_\gamma(\tau)$ is an algebraic integer that divides N^{12}.*
3. *Let $\tau \in \mathbb{H}$ be a quadratic number with $\mathcal{O} = \operatorname{End}(\mathbb{Z} \oplus \mathbb{Z}\tau)$ and $\mathfrak{a} \cong \mathbb{Z} \oplus \mathbb{Z}\tau$ for a proper $\mathcal{O}$-ideal $\mathfrak{a}$. Suppose that p is a prime number splitting completely in K such that p does not divide the conductor of $\mathcal{O}$. Let $p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}}$ be the factorization into $\mathcal{O}$-ideals (i.e. $p\mathcal{O} = (\mathfrak{p}' \cap \mathcal{O})(\overline{\mathfrak{p}'} \cap \mathcal{O})$ where $p\mathcal{O}_K = \mathfrak{p}'\overline{\mathfrak{p}'}$). Let γ be a 2×2 matrix with integer entries with $\det \gamma = p$ such that $\mathbb{Z} \oplus \mathbb{Z}\tau \cong \mathfrak{a}$ sends $\gamma(\mathbb{Z} \oplus \mathbb{Z}\tau) \cong \mathfrak{p}\mathfrak{a}$. Then, in a sufficiently big number field L, $\varphi_\gamma(\tau)\mathcal{O}_L = \overline{\mathfrak{p}}^{12}\mathcal{O}_L$ (e.g. you can take $L = K(\varphi_\gamma(\tau))$).*
4. *Retain the same notation as (3). If δ is a 2×2 matrix with integer entries with $\det \delta = p$ such that, under the isomorphism $\mathbb{Z} \oplus \mathbb{Z}\tau \cong \mathfrak{a}$, $\delta(\mathbb{Z} \oplus \mathbb{Z}\tau)$ is sent to neither $\mathfrak{p}\mathfrak{a}$ nor $\overline{\mathfrak{p}}\mathfrak{a}$, then $\varphi_\delta(\tau)$ is a unit.*

Proof. (1) Note that from the proof of Proposition 14.8, we can deduce that

$$C(N) = \mathrm{SL}_2(\mathbb{Z}) \backslash \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \; : \; a, b, c, d \in \mathbb{Z}, \; ad - bc = N \right\}.$$

This is because the proof shows that $\left(\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} \mathrm{SL}_2(\mathbb{Z})\gamma \right) \cap \mathrm{SL}_2(\mathbb{Z})$ is a right $\Gamma_0(N)$-coset for any γ which is an integer 2×2 matrix with $\det \gamma = N$, and because the formula clearly shows that this coset only depends on the right $\mathrm{SL}_2(\mathbb{Z})$-coset of γ, so the bijection $C(N) \xrightarrow{\sim} \{\text{right } \Gamma_0(N)\text{-cosets}\}$ factors through

$$C(N) \to \mathrm{SL}_2(\mathbb{Z}) \backslash \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \; : \; a, b, c, d \in \mathbb{Z}, \; ad - bc = N \right\} \to \{\text{right } \Gamma_0(N)\text{-cosets}\}$$

whose composition is a bijection. Here the first map is just the natural map (any element of $C(N)$ is an integer 2×2 matrix with determinant N). Thus the first map is injective. To show that the first map is surjective, we also notice that any integer 2×2 matrix with determinant N can be modified by left multiplying by an element of $\mathrm{SL}_2(\mathbb{Z})$ to arrive at an element of $C(N)$, but everything just works in the same way (you can always make the matrix upper triangular in this way, and everything else is verbatim the same).

As Δ is a modular form of weight 12 and level 1, if $\gamma' = M\gamma$ for $M \in \mathrm{SL}_2(\mathbb{Z})$, $\varphi_{\gamma'}(\tau) = \varphi_\gamma(\tau)$. Let $\gamma_1, \cdots, \gamma_{|C(N)|}$ be all the elements of $C(N)$. Suppose that $\sigma \in \mathrm{SL}_2(\mathbb{Z})$. Then, for each $1 \leq i \leq |C(N)|$, there is unique $1 \leq j_i \leq |C(N)|$ such that $\mathrm{SL}_2(\mathbb{Z})\gamma_i\sigma =$

$\mathrm{SL}_2(\mathbb{Z})\gamma_{j(i)}$. We claim that $\varphi_{\gamma_i}(\sigma \cdot \tau) = \varphi_{\gamma_{j_i}}(\tau)$. Indeed, for $\gamma_i = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\sigma = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$,

$$\varphi_{\gamma_i}(\sigma \cdot \tau) = N^{12} \frac{\Delta(\gamma_i \sigma \cdot \tau)}{(c\sigma \cdot \tau + d)^{12} \Delta(\sigma \cdot \tau)} = N^{12} \frac{\Delta(\gamma_i \sigma \cdot \tau)}{(c\frac{x\tau+y}{z\tau+w} + d)^{12}(z\tau + w)^{12}\Delta(\tau)}$$

$$= N^{12} \frac{\Delta(\gamma_i \sigma \cdot \tau)}{((cx+dz)\tau + (cy+dw))^{12}\Delta(\tau)} = \varphi_{\gamma_{j_i}}(\tau).$$

Therefore, if $f(\tau)$ is a symmetric function in $\varphi_{\gamma_i}(\tau)$'s, then it is a modular function of level 1 (meromorphy at cusps is obvious) that is holomorphic on $\mathbb{H}$. Therefore, the polynomial $\prod_{i=1}^{|C(N)|}(X - \varphi_{\gamma_i}(\tau))$ is a polynomial in X with coefficients in $\mathbb{C}[j]$.

To show that $\varphi_\gamma(\tau)$ is integral over $\mathbb{Z}[j]$, we want to show that symmetric polynomials in $\varphi_{\gamma_i}(\tau)$ have q-expansions in $\mathbb{Z}[[q]](q^{-1})$. Note that, by the proof of Proposition 14.8, it is easy to see that the q-expansion of $\varphi_{\gamma_i}(\tau)$ is in $\mathbb{Z}[\zeta_N][[q^{1/N}]](q^{-1/N})$, and applying $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ on the coefficients will permute the q-expansions of $\varphi_{\gamma_i}(\tau)$'s. Therefore, this shows that a symmetric polynomial in $\varphi_{\gamma_i}(\tau)$'s has q-expansion in $\mathbb{Z}[[q]](q^{-1})$.

(2) From (1) and Theorem 15.1, $\varphi_\gamma(\tau)$ is an algebraic integer for a quadratic $\tau \in \mathbb{H}$. Let $\operatorname{adj}\gamma = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, so that $\gamma \operatorname{adj}\gamma = \begin{pmatrix} N & 0 \\ 0 & N \end{pmatrix}$. Then

$$\varphi_\gamma(\tau)\varphi_{\operatorname{adj}\gamma}(\gamma \cdot \tau) = N^{24} \frac{\Delta(\gamma \cdot \tau)}{(c\tau + d)^{12}\Delta(\tau)} \frac{\Delta(((\operatorname{adj}\gamma)\gamma) \cdot \tau)}{\left(-c\frac{a\tau+b}{c\tau+d} + a\right)^{12} \Delta(\gamma \cdot \tau)} = \frac{N^{24}}{(ad-bc)^{12}} = N^{12}.$$

As $\varphi_{\operatorname{adj}\gamma}(\gamma \cdot \tau)$ is also an algebraic integer, $\varphi_\gamma(\tau)$ divides N^{12}.

(3) We choose a proper $\mathcal{O}$-ideal $\mathfrak{b}$ such that $\mathfrak{b}\mathfrak{p} = \lambda\mathcal{O}$ is a principal $\mathcal{O}$-ideal and $\mathfrak{b}$ is coprime to p (this is always possible because $\mathrm{Cl}(\mathcal{O})$ is generated by proper $\mathcal{O}$-ideals coprime to M for any choice of M). Then $\mathfrak{b}\mathfrak{p}\mathfrak{a}$ is a sublattice of $\mathfrak{p}\mathfrak{a}$, so there exists a 2×2 matrix γ' with integer entries such that $\gamma(\mathbb{Z} \oplus \mathbb{Z}\tau) \cong \mathfrak{p}\mathfrak{a}$ sends $\gamma'\gamma(\mathbb{Z} \oplus \mathbb{Z}\tau) \cong \mathfrak{b}\mathfrak{p}\mathfrak{a}$. Then by definition $\det \gamma' = [\mathfrak{p}\mathfrak{a} : \mathfrak{b}\mathfrak{p}\mathfrak{a}] = N(\mathfrak{b})$. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. We then have

$$\varphi_{\gamma'}(\gamma \cdot \tau)\varphi_\gamma(\tau) = N(\mathfrak{b})^{12} p^{12} \frac{\Delta(\gamma'\gamma \cdot \tau)}{(c'\frac{a\tau+b}{c\tau+d} + d')^{12}\Delta(\gamma \cdot \tau)} \frac{\Delta(\gamma \cdot \tau)}{(c\tau + d)^{12}\Delta(\tau)}$$

$$= N(\mathfrak{b})^{12} p^{12} \frac{1}{((c'a + d'c)\tau + (c'b + d'd))^{12}}.$$

It is easy to see that $\lambda = (c'a + d'c)\tau + (c'b + d'd)$. Therefore, $\varphi_{\gamma'}(\gamma \cdot \tau)\varphi_\gamma(\tau) = \frac{N(\mathfrak{b})^{12}p^{12}}{\lambda^{12}}$. Note that (2) tells us that $\varphi_{\gamma'}(\gamma \cdot \tau)$ divides $N(\mathfrak{b})^{12}$, so $\varphi_\gamma(\tau)$ is divisible by $\frac{p^{12}}{\lambda^{12}}$. Note also that, as $\mathfrak{b}$ is coprime to p, the prime factorization of $\lambda\mathcal{O}_K$ has exactly one appearance of $\mathfrak{p}'$ and no appearance of $\overline{\mathfrak{p}'}$. Therefore, $\varphi_\gamma(\tau)\mathcal{O}_L$ is divisible by $\overline{\mathfrak{p}'}^{12}\mathcal{O}_L = \overline{\mathfrak{p}}^{12}\mathcal{O}_L$. On the other hand, by (2), $\varphi_\gamma(\tau)$ divides p^{12}, and as $N(\mathfrak{b})$ is coprime to p, it turns out that $\frac{N(\mathfrak{b})^{12}}{\varphi_{\gamma'}(\gamma\cdot\tau)}$ is coprime to $\varphi_\gamma(\tau)$. Therefore, $\varphi_{\gamma'}(\gamma\cdot\tau)$ must be off by a unit, and $\varphi_\gamma(\tau)\mathcal{O}_L = \overline{\mathfrak{p}}^{12}\mathcal{O}_L$.

(4) Recall that in the proof of Theorem 14.10(7) we observed that $C(p) = \{\sigma_0, \cdots, \sigma_p\}$ where $\sigma_k = \begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix}$, $0 \leq k \leq p-1$, and $\sigma_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. Suppose that $0 \leq r \neq s \leq p$ be such that the isomorphism $\mathbb{Z}\oplus\mathbb{Z}\tau \cong \mathfrak{a}$ sends $\sigma_r(\mathbb{Z}\oplus\mathbb{Z}\tau) \cong \mathfrak{p}\mathfrak{a}$ and $\sigma_s(\mathbb{Z}\oplus\mathbb{Z}\tau) \cong \overline{\mathfrak{p}}\mathfrak{a}$. Then, by (3), we know that $\varphi_{\sigma_r}(\tau)\varphi_{\sigma_s}(\tau)$ is a unit times p^{12}. What we want to show is that $\varphi_{\sigma_i}(\tau)$ is a unit as long as $i \neq r, s$. As each $\varphi_{\sigma_i}(\tau)$ is an algebraic integer, to achieve what we want, it suffices to show that $\prod_{k=0}^{p} \varphi_{\sigma_k}(\tau)$ is a unit times p^{12}. Note that the function $F(z) := \prod_{k=0}^{p} \varphi_{\sigma_k}(z)$ for $z \in \mathbb{H}$ is a modular function in $\mathrm{SL}_2(\mathbb{Z})$ holomorphic on $\mathbb{H}$, so it is a polynomial in j. Furthermore, if we look at the lowest order term of the q-expansions of $\varphi_{\sigma_k}(z)$, it's easy to see that we get $e^{2\pi ik/p}q^{-\frac{p-1}{p}}$ for $0 \leq k \leq p-1$, and $p^{12}q^{p-1}$ for $k = p$. Therefore, the lowest order term of the q-expansion of F is $e^{2\pi i(0+1+\cdots+(p-1))/p}p^{12}q^{(p-1)-(p-1)} = e^{2\pi i(p-1)/2}p^{12} = (-1)^{p-1}p^{12}$. Therefore, F is in fact a modular function for $\mathrm{SL}_2(\mathbb{Z})$ that is also holomorphic at infinity. By Liouville's theorem, this must be a constant, so $F(\tau) = (-1)^{p-1}p^{12}$, which is what we wanted.

□

Proof of Theorem 15.3. By Artin reciprocity, $\mathrm{Art}_K(\alpha)|_{K(\mathcal{O})}$ depends only on the image $[\mathfrak{a}_\alpha] \in \mathrm{Cl}(\mathcal{O})$ of α along $C_K \twoheadrightarrow \mathrm{Cl}(\mathcal{O})$. By Theorem 13.29(3) and (4), for any choice of modulus $\mathfrak{m}$ divisible by the conductor N of $\mathcal{O}$, we know that $\mathrm{Cl}(\mathcal{O})$ is generated by the prime $\mathcal{O}$-ideals of $\mathcal{O}$ which are of the form $\mathfrak{p} \cap \mathcal{O}$ for a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ coprime to $\mathfrak{m}$. We in particular add a few more primes to $\mathfrak{m}$ so that it is divisible also by the primes ramified in $K(\mathcal{O})$ and the primes ramified over $\mathbb{Q}$. Then, it suffices to show the identity for α such that $\mathfrak{a}_\alpha = \mathfrak{p} \cap \mathcal{O}$ for a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ coprime to $\mathfrak{m}$. Now for such α, we know by the local Artin reciprocity and the local-global compatibility that $\mathrm{Art}_K(\alpha)|_{K(\mathcal{O})} = \mathrm{Fr}_{\mathfrak{p}}$. Thus, we need to show that, for each prime $\mathfrak{p}$ unramified over $\mathbb{Q}$ and unramified in $K(\mathcal{O})$, if $\mathfrak{P}$ is a prime of $K(\mathcal{O})$ lying over $\mathfrak{p}$, then $j(\mathfrak{a})^{N(\mathfrak{p})} \equiv j((\mathfrak{p} \cap \mathcal{O})^{-1}\mathfrak{a}) \pmod{\mathfrak{P}}$.

Let p be a prime number in $\mathbb{Z}$ such that $p\mathbb{Z} = \mathbb{Z} \cap \mathfrak{p}$. If p is inert in K, then $\mathfrak{p} = p\mathcal{O}_K$. On the other hand, $[\mathfrak{p}] = 1$ in $\mathrm{Cl}(\mathcal{O})$ because it is a principal ideal and $(p, N) = 1$. Therefore, we know that $p\mathcal{O}_K$ splits completely in $K(\mathcal{O})$. Therefore, $N(\mathfrak{P}) = p^2 = N(\mathfrak{p})$ and the congruence we want to show is $j(\mathfrak{a})^{p^2} \equiv j(\mathfrak{a}) \pmod{\mathfrak{P}}$ which is obvious.

We are left with the case when p splits completely in K, $p = \mathfrak{p}'\overline{\mathfrak{p}'}$ with $\mathfrak{p}' \neq \overline{\mathfrak{p}'}$. Then, we want to show that $j(\mathfrak{a})^p \equiv j(\mathfrak{p}^{-1}\mathfrak{a}) \pmod{\mathfrak{P}}$ where $\mathfrak{p} = \mathfrak{p}' \cap \mathcal{O}$.

Recall that in the proof of Theorem 14.10(7) we observed that $C(p) = \{\sigma_0, \cdots, \sigma_p\}$ where $\sigma_k = \begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix}$, $0 \leq k \leq p-1$, and $\sigma_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. We consider the polynomial in two variables

$$F(X, Y) := \left(\prod_{i=0}^{p}(Y - \varphi_{\sigma_i}(\tau))\right)\sum_{i=0}^{p}\frac{X - j(\sigma_i \cdot \tau)}{Y - \varphi_{\sigma_i}(\tau)}.$$

Its coefficients are holomorphic functions on $\mathbb{H}$ meromorphic at cusps. Furthermore, it's easy to see that the coefficients are invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$. Therefore, $F \in \mathbb{C}[X, Y, j]$. By looking at the q-expansions, we see immediately that in fact $F \in \mathbb{Z}[\zeta_p][X, Y, j]$. It is also easy to see that the q-expansions are invariant under the conjugation by any element of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, so $F \in \mathbb{Z}[X, Y, j]$. Since the first p terms (i.e. those corresponding to $\sigma_0, \cdots, \sigma_{p-1}$) have the q-expansiosn of the same form except that they use different p-th roots of unity (including 1), these terms are all congruent to each other mod $1 - \zeta_p$. As there are p such terms, the sum of these p terms will vanish mod $1 - \zeta_p$. Therefore,

$$F(X, Y) \equiv \left(\prod_{i=0}^{p} (Y - \varphi_{\sigma_i}(\tau)) \right) \frac{X - j(\sigma_p \cdot \tau)}{Y - \varphi_{\sigma_p}(\tau)} \pmod{1 - \zeta_p}.$$

As $j(\sigma_p \cdot \tau) = j(\tau)^p$, we see that $F(j(\tau)^p, Y) \in p\mathbb{Z}[Y, j]$.

We let $\tau \in \mathbb{H}$ be such that $\mathbb{Z} \oplus \mathbb{Z}\tau \cong \mathfrak{a}$. Let α, β be two 2×2 integer matrices such that the isomorphism $\mathbb{Z} \oplus \mathbb{Z}\tau \cong \mathfrak{a}$ sends $\alpha(\mathbb{Z} \oplus \mathbb{Z}\tau) \cong \mathfrak{p}\mathfrak{a}$ and $\beta(\mathbb{Z} \oplus \mathbb{Z}\tau) \cong \overline{\mathfrak{p}}\mathfrak{a}$. We can then see that $F(j(\tau)^p, \varphi_\beta(\tau)) \equiv 0 \pmod{\mathfrak{p}\mathcal{O}_L}$ for a big enough number field L that contains all these values. Note that $\det \alpha = \det \beta = p$. Therefore, if we let $\sigma_u \in C(p)$ be such that $\mathrm{SL}_2(\mathbb{Z})\beta = \mathrm{SL}_2(\mathbb{Z})\sigma_u$, then we see that only the u-th term of the original sum for the definition of $F(X, Y)$ survives when we put $Y = \varphi_\beta(\tau)$, so that we obtain

$$(j(\tau)^p - j(\sigma_u \cdot \tau)) \prod_{0 \leq i \leq p, i \neq u} (\varphi_\beta(\tau) - \varphi_{\sigma_i}(\tau)) \equiv 0 \pmod{\mathfrak{p}\mathcal{O}_L}.$$

As $j(\sigma_u \cdot \tau) = j(\overline{\mathfrak{p}}\mathfrak{a}) = j(\mathfrak{p}^{-1}\mathfrak{a})$, to get what we want, it suffices to show that $\varphi_\beta(\tau) \not\equiv \varphi_{\sigma_i}(\tau) \pmod{\mathfrak{p}\mathcal{O}_L}$ for $i \neq u$. By Theorem 15.6(3), it follows that $\varphi_\beta(\tau)\mathcal{O}_L = \mathfrak{p}^{12}\mathcal{O}_L$. Therefore, it suffices to show that $\varphi_{\sigma_i}(\tau) \not\equiv 0 \pmod{\mathfrak{p}\mathcal{O}_L}$. If $\mathrm{SL}_2(\mathbb{Z})\sigma_i = \mathrm{SL}_2(\mathbb{Z})\alpha$, then again Theorem 15.6(3) shows that $\varphi_{\sigma_i}(\tau)\mathcal{O}_L = \overline{\mathfrak{p}}^{12}\mathcal{O}_L$, so in particular $\varphi_{\sigma_i}(\tau) \not\equiv 0 \pmod{\mathfrak{p}\mathcal{O}_L}$. If not, then Theorem 15.6(4) shows that $\varphi_{\sigma_i}(\tau)$ is a unit, which also implies that $\varphi_{\sigma_i}(\tau) \not\equiv 0 \pmod{\mathfrak{p}\mathcal{O}_L}$. □

Corollary 15.7. *For an imaginary quadratic field K, $H_K = K(j(\mathcal{O}_K))$.*

This is a remarkable property of the j-function. In fact, the j-function assumes transcendental values at algebraic, non-quadratic points on $\mathbb{H}$.

Theorem 15.8 (Schneider). *If $\tau \in \mathbb{H}$ is an algebraic number such that $j(\tau)$ is also an algebraic number, then τ is a quadratic number. In other words, if $\tau \in \mathbb{H}$ is algebraic and not quadratic, $j(\tau)$ is a transcendental number.*

For the proof, see [Sil, Chapter II.6].

15.2. **Second Main Theorem: from ring class fields to ray class fields.** Note that $K(N)$ (ray class field of conductor N) and $K(\mathbb{Z} \oplus N\mathcal{O}_K)$ (ring class field of order of conductor N) are different, and $\mathrm{Gal}(K(N)/K(\mathbb{Z} \oplus N\mathcal{O}_K)) = (\mathbb{Z}/N\mathbb{Z})^\times$. How do we reach the ray class field from the ring class field? We need to adjoin more specific elements to ring class fields.

Definition 15.9 (Weber functions)**.** Let $\mathcal{O}$ be an order in an imaginary quadratic field K. We define the **Weber function** of the order $\mathcal{O}$, which is a function on three variables $(z,\tau) \in \mathbb{C} \times \mathbb{H}$, as

$$\tau_{\mathcal{O}}(z,\tau) := g^{(\#\mu_{\mathcal{O}})}(\tau)\wp(z, \mathbb{Z} \oplus \mathbb{Z}\tau)^{\frac{\#\mu_{\mathcal{O}}}{2}},$$

where $\wp(z, \mathbb{Z} \oplus \mathbb{Z}\tau)$ is the Weierstrass $\wp$-function for the lattice $\mathbb{Z} \oplus \mathbb{Z}\tau \subset \mathbb{C}$ (=elliptic curve over $\mathbb{C}$), $\mu_{\mathcal{O}}$ is the group of roots of unity in $\mathcal{O}$ (which can be either $\langle -1 \rangle$ (order 2), $\langle \zeta_4 \rangle$ (order 4, only happens when $K = \mathbb{Q}(i)$ and $\mathcal{O} = \mathcal{O}_K$) or $\langle \zeta_6 \rangle$ (order 6, only happens when $K = \mathbb{Q}(\sqrt{-3})$ and $\mathcal{O} = \mathcal{O}_K$)), and

$$g^{(2)}(\tau) := -2^7 \cdot 3^5 \frac{g_2(\tau)g_3(\tau)}{\Delta(\tau)},$$

$$g^{(4)}(\tau) := 2^8 \cdot 3^4 \frac{g_2(\tau)^2}{\Delta(\tau)^2},$$

$$g^{(6)}(\tau) := -2^9 \cdot 3^6 \frac{g_3(\tau)}{\Delta(\tau)}.$$

Again, there are good reasons why you want to multiply with those powers of 2 and 3, which you will see in a moment.

Remark 15.10. The reason why we take the units into account is precisely because the stabilizer of the $\mathrm{SL}_2(\mathbb{Z})$-action on $\mathbb{H}$ is not $\{\pm 1\}$ precisely at two orbits, namely the orbit of i and the orbit of $e^{2\pi i/3}$. Note that the case of order 4 stabilizer is precisely when the corresponding lattice (=elliptic curve over $\mathbb{C}$) is $\mathbb{Z} \oplus \mathbb{Z}i = \mathcal{O}_{\mathbb{Q}(i)}$, and the case of order 6 stabilizer is precisely when the corresponding lattice (=elliptic curve over $\mathbb{C}$) is $\mathbb{Z} \oplus \mathbb{Z}e^{2\pi i/3} = \mathbb{Z} \oplus \mathbb{Z}\frac{-1+\sqrt{-3}}{2} = \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$!

Similar to the j-function, we are interested in special values of the Weber functions. The algebraic properties of the special values are studied by an analouge of the modular polynomial.

Definition 15.11 (Division polynomial, torsion points)**.** Let $N \in \mathbb{N}$. Consider the function

$$T_{N,\mathcal{O}}(X,\tau) := \prod_{x_1,x_2 \in \mathbb{Z}/N\mathbb{Z},\ \gcd(x_1,x_2,N)=1} \left(X - \tau_{\mathcal{O}}\left(\frac{x_1 + x_2\tau}{N}, \tau \right) \right).$$

This is called the N**-th order division polynomial** for the Weber function $\tau_{\mathcal{O}}$. The points $\frac{x_1+x_2\tau}{N}$ for $\gcd(x_1, x_2, N) = 1$ are exactly the points $z \in \mathbb{C}$ such that $Nz \in \mathbb{Z} \oplus \mathbb{Z}\tau$ and $nz \notin \mathbb{Z} \oplus \mathbb{Z}\tau$ for $0 < n < N$. Such a z is called a **torsion point of $\mathbb{Z} \oplus \mathbb{Z}\tau$ of exact order** N. A **torsion point** of $\mathbb{Z} \oplus \mathbb{Z}\tau$ is a point $z \in \mathbb{C}$ such that $nz \in \mathbb{Z} \oplus \mathbb{Z}\tau$ for some $n \in \mathbb{N}$.

Theorem 15.12. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K. Let $N \in \mathbb{N}$.*

(1) The division polynomial $T_{N,\mathcal{O}}(X,\tau)$ is a polynomial in X with coefficients being polynomials in $j(\tau)$. Thus, we may think of $T_{N,\mathcal{O}}(X,\tau) = T_{N,\mathcal{O}}(X, j(\tau))$ for a two-variable polynomial $T_{N,\mathcal{O}}(X,Y)$.

(2) The two-variable polynomial $T_{N,\mathcal{O}}(X,Y) \in \mathbb{Q}[X,Y]$. Furthermore, if N is not a prime power, $T_{N,\mathcal{O}}(X,Y) \in \mathbb{Z}[X,Y]$. If N is a power of a prime number p, then $p^{\#\mu_{\mathcal{O}}}T_{N,\mathcal{O}}(X,Y) \in \mathbb{Z}[X,Y]$.

Proof. (1) It is clear that the action of $\mathrm{SL}_2(\mathbb{Z})$ on τ preserves $T_{N,\mathcal{O}}(X,\tau)$, as the enumeration of the $\mathbb{Z} \oplus \mathbb{Z}\tau$-orbits of $\frac{x_1+x_2\tau}{N}$ running over $x_1, x_2 \in \mathbb{Z}/N\mathbb{Z}$, $\gcd(x_1, x_2, N) = 1$ only depend on the lattice $\mathbb{Z} \oplus \mathbb{Z}\tau$. It is also clear that the coefficients are actual values and do not blow up for any $\tau \in \mathbb{H}$. The result follows.

(2) We need to discuss the Fourier expansions, so let us start with $\wp(z,\tau)$. Namely, $\wp(z,\tau)$ is $\mathrm{SL}_2(\mathbb{Z})$-invariant at τ-variable, and periodic with periods 1 and τ at z-variable. Let $U = e^{2\pi i z}$. Then, we claim that, for $|\operatorname{Im}(z)| > \operatorname{Im}\tau > 0$, the following formula holds,

$$\wp(z,\tau) = -\frac{\pi^2}{3}\left(1 + \frac{12U}{(1-U)^2} + 12\sum_{n,m=1}^{\infty} nq^{nm}(U^n + U^{-n} - 2)\right).$$

The way that this formula is obtained is a variant of the argument we used to compute the Fourier expansion of the Eisenstein series $G_{2k}(\tau)$ (this is like the "weight 2" version, except that there are a lot more decorations to make the infinite sum converge). Namely,

$$\wp(z,\tau) = f(z) + \sum_{m\in\mathbb{Z}, m\neq 0} g(z, m\tau),$$

where

$$f(z) = \frac{1}{z^2} + \sum_{n\in\mathbb{Z}, n\neq 0}\left(\frac{1}{(z-n)^2} - \frac{1}{n^2}\right),$$

$$g(z,\tau) = \sum_{n\in\mathbb{Z}}\left(\frac{1}{(z-n-\tau)^2} - \frac{1}{(n+\tau)^2}\right).$$

Note that this is an OK rearrangement, because the infinite sum for the definition of $\wp(z)$ is absolutely convergent as long as you don't pull terms out of the parentheses (the whole series disregarding the grouping is not absolutely convergent, but $\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} = \frac{2z\lambda - z^2}{\lambda^2(z-\lambda)^2}$ which is $\sim \frac{1}{\lambda^3}$). Now each of $f(z)$ and $g(z,\tau)$ have an absolutely convergent infinite sum, so dealing with each of these functions, we can rearrange the terms as we wish.

- For $f(z)$: note that $f(z) = \sum_{n\in\mathbb{Z}} \frac{1}{(z-n)^2} - 2\zeta(3) = \sum_{n\in\mathbb{Z}} \frac{1}{(z-n)^2} - \frac{\pi^2}{3}$. Note also that $\sum_{n\in\mathbb{Z}} \frac{1}{(z-n)^2}$ is periodic with period 1, so we may expect a Fourier expansion in terms of U. In fact, it is one of the standard infinite series proved in complex analysis that

  $$\csc^2(z) = \sum_{n\in\mathbb{Z}} \frac{1}{(z-n\pi)^2},$$

  so that

  $$\pi^2\csc^2(\pi z) = \sum_{n\in\mathbb{Z}} \frac{1}{(z-n)^2}.$$

  Note that $\sin^2(\pi z) = \frac{1-\cos(2\pi z)}{2} = \frac{2-U-U^{-1}}{4}$. Therefore, $f(z) = -\frac{\pi^2}{3} - \frac{4\pi^2}{U-2+U^{-1}} = -\frac{\pi^2}{3}\left(1 + \frac{12U}{(1-U)^2}\right)$. This identity holds as long as $U \neq 1$.

- For $g(z,\tau)$: note that, using the identity we discussed above, $g(z,\tau) = \pi^2\csc^2(\pi(z-\tau)) - \pi^2\csc^2(\pi\tau)$. Thus,

  $$g(z,\tau) = -\frac{4\pi^2}{\frac{U}{q} - 2 + \frac{q}{U}} + \frac{4\pi^2}{q - 2 + q^{-1}}.$$

  Note that

  $$\frac{4\pi^2}{q-2+q^{-1}} = \frac{4\pi^2 q}{q^2-2q+1} = 4\pi^2 q(1-q)^{-2} = 4\pi^2 q\sum_{n=0}^{\infty}\binom{-2}{n}(-1)^n q^n$$
  $$= 4\pi^2 q\sum_{n=0}^{\infty}(n+1)q^n = 4\pi^2\sum_{n=1}^{\infty} nq^n.$$

  Therefore, similarly,

  $$\frac{4\pi^2}{\frac{U}{q} - 2 + \frac{q}{U}} = 4\pi^2\sum_{n=1}^{\infty} nq^n U^{-n}.$$

  These identities hold when $|q| < 1$ and $\left|\frac{q}{U}\right| < 1$, which is when $\mathrm{Im}(z) > \mathrm{Im}(\tau) > 0$. Note however that we are also planning to plug $m\tau$ into τ for $m < 0$. In those cases, we need to rather use

  $$\frac{4\pi^2}{q-2+q^{-1}} = 4\pi^2 q^{-1}(1-q^{-1})^{-2} = 4\pi^2\sum_{n=1}^{\infty} nq^{-n},$$
  $$\frac{4\pi^2}{\frac{U}{q} - 2 + \frac{q}{U}} = 4\pi^2\sum_{n=1}^{\infty} nq^{-n}U^n.$$

  These identities hold when $|q^{-1}| < 1$ and $\left|\frac{U}{q}\right| < 1$, which is when $\mathrm{Im}(z) < \mathrm{Im}(\tau) < 0$.

So all in all, if we gather the Fourier expansions, we get

$$\wp(z,\tau) = -\frac{\pi^2}{3}\left(1+\frac{12U}{(1-U)^2}\right) + 4\pi^2\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}\left(nq^{nm} - nq^{nm}U^{-n}\right) + 4\pi^2\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}\left(nq^{nm} - nq^{nm}U^{n}\right).$$

This after rearrangement is precisely what we wanted. Now, we can easily compute the q-expansions of $g^{(2)}$, $g^{(4)}$, $g^{(6)}$, so that $\tau_{\mathcal{O}}(z,\tau)$ has the Fourier expansion

$$\tau_{\mathcal{O}}(z,\tau) = P(q)\left(1 + \frac{12U}{(1-U)^2} + 12\sum_{n,m=1}^{\infty} nq^{nm}(U^n + U^{-n} - 2)\right)^{\#\mu_{\mathcal{O}}/2},$$

for some q-expansion $P(q) \in \mathbb{Z}[[q]]$ with the lowest term starting with $q^{-\#\mu_{\mathcal{O}}/2}$ (this includes that the lowest order coefficient is 1; this is why we multiplied those funny numbers in the definitions of $g^{(2)}$, $g^{(4)}$, $g^{(6)}$).

Now we can conclude. Note that, for $0 \leq x_1, x_2 < N$, then $U = \zeta_N^{x_1} q^{x_2/N}$, where $\zeta_N = e^{2\pi i/N}$. Thus

$$\tau_{\mathcal{O}}\left(\frac{x_1 + x_2\tau}{N}, \tau\right) = (q^{-\#\mu_{\mathcal{O}}/2} + \cdots)\left(1 + \frac{12\zeta_N^{x_1} q^{x_2/N}}{\left(1 - \zeta_N^{x_1} q^{x_2/N}\right)^2} + 12\sum_{n,m=1}^{\infty} nq^{nm}\left(\zeta_N^{x_1 n} q^{x_2 n/N} + \zeta_N^{-x_1 n} q^{-x_2 n/N} - 2\right)\right)^{\#\mu_{\mathcal{O}}/2}.$$

Note that there are only finitely many appearances of negative powers of q in the above series because $x_2/N < 1$. This shows that the coefficients of the above q-expansion are in $\mathbb{Q}(\zeta_N)$. Furthermore, the coefficients are actually in $\mathbb{Z}[\zeta_N]$ unless $x_2 = 0$ (in which case the middle term would just be $\frac{12\zeta_N^{x_1}}{(1-\zeta_N^{x_1})^2}$.). Now note that the Galois conjugation $\zeta_N \mapsto \zeta_N^r$ sends the q-expansion for $\tau_{\mathcal{O}}\left(\frac{x_1+x_2\tau}{N}, \tau\right)$ to $\tau_{\mathcal{O}}\left(\frac{rx_1+x_2\tau}{N}, \tau\right)$, so it follows that $T_{N,\mathcal{O}}(X, Y) \in \mathbb{Q}[X, Y]$. Furthermore, we know exactly how much we need to multiply to make it integral; namely, we need to multiply by

$$\prod_{x \in \mathbb{Z}/N\mathbb{Z},\ \gcd(x,N)=1} (1 - \zeta_N^x)^{\#\mu_{\mathcal{O}}} = \begin{cases} 1 & \text{if } N \text{ is not a prime power} \\ p^{\#\mu_{\mathcal{O}}} & \text{if } N = p^k \text{ is a prime power.} \end{cases}$$

Thus we are done.

□

Definition 15.13. Let $\mathcal{O}$ be an order in an imaginary quadratic field K. Let $N \in \mathbb{N}$. Let p be a prime number coprime to N. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a 2×2 matrix with integer entries such that $\det\gamma = p$. We define, for $x_1, x_2 \in \mathbb{Z}$ with $\gcd(x_1, x_2, N) = 1$,

$$\delta_{\gamma,\mathcal{O},N}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}; \tau\right) := \tau_{\mathcal{O}}\left(\frac{x_1 + x_2\tau}{N}, \tau\right)^p - \tau_{\mathcal{O}}\left(\frac{px_1 + px_2\tau}{N(c\tau + d)}, \gamma \cdot \tau\right).$$

Note that this definition makes sense as $p\mathbb{Z} \oplus p\mathbb{Z}\tau \subset (c\tau + d)(\mathbb{Z} \oplus \mathbb{Z}\gamma \cdot \tau)$. We furthermore define

$$S_{\gamma,\mathcal{O},N}(X, \tau) := \prod_{x_1, x_2 \in \mathbb{Z}/N\mathbb{Z},\ \gcd(x_1,x_2,N)=1} \left(X - \delta_{\gamma,\mathcal{O},N}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}; \tau\right)\right).$$

For $k \geq 0$, the X^k-coefficient of $S_{\gamma,\mathcal{O},N}(\tau)$ is denoted as $D^{(k)}_{\gamma,\mathcal{O},N}(\tau)$.

Theorem 15.14. *We retain the notations of Definition 15.13.*

(1) The functions $D^{(k)}_{\gamma,\mathcal{O},N}(\tau)$ are modular functions for $G_\gamma := \mathrm{SL}_2(\mathbb{Z}) \cap \gamma^{-1}\,\mathrm{SL}_2(\mathbb{Z})\gamma$, holomorphic on $\mathbb{H}$.

(2) The q-expansion of $D^{(k)}_{\gamma,\mathcal{O},N}(\tau)$ at infinity has rational coefficients that are p-integers (i.e. can be written as $\frac{m}{n}$ with $\gcd(n, p) = 1$). If $\gamma = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$, all coefficients of the q-expansion are divisible by p (except the leading coefficient case where $D^{(k)}_{\gamma,\mathcal{O},N}(\tau) = 1$).

(3) *Let $\tau' \in \mathbb{H}$ be a quadratic number such that $\operatorname{End}(\mathbb{Z} \oplus \mathbb{Z}\tau') \cong \mathcal{O}$. Let $\mathfrak{a}$ be a proper $\mathcal{O}$-ideal such that $\mathbb{Z} \oplus \mathbb{Z}\tau' \cong \mathfrak{a}$. Suppose that $p = \mathfrak{p}'\overline{\mathfrak{p}'}$ splits completely in K and p does not divide the conductor of $\mathcal{O}$. Then, $D^{(k)}_{\gamma,\mathcal{O},N}(\tau')$ is algebraic. Furthermore, if γ is such that $\mathbb{Z} \oplus \mathbb{Z}\tau' \cong \mathfrak{a}$ sends $\gamma(\mathbb{Z} \oplus \mathbb{Z}\tau') \cong \mathfrak{p}'\mathfrak{a}$, then $D^{(k)}_{\gamma,\mathcal{O},N}(\tau')$ is divisible by $\overline{\mathfrak{p}'}$.*

(4) *Let $\tau' \in \mathbb{H}$ be a quadratic number such that $\operatorname{End}(\mathbb{Z} \oplus \mathbb{Z}\tau') \cong \mathcal{O}$. Let $\mathfrak{a}$ be a proper $\mathcal{O}$-ideal such that $\mathbb{Z} \oplus \mathbb{Z}\tau' \cong \mathfrak{a}$. Suppose that p is inert in K, $p > 12$, p does not divide the conductor of $\mathcal{O}$, and p is unramified in $\mathbb{Q}(j(\tau'))$. Then, $D^{(k)}_{\gamma,\mathcal{O},N}(\tau')$ is algebraic and is divisible by p.*

(5) *Let $\mathcal{O} = \mathcal{O}_K$. Let z be a torsion point of $\mathbb{Z} \oplus \mathbb{Z}\tau$ of exact order N. Under the isomorphism $\mathbb{Z} \oplus \mathbb{Z}\tau \cong \mathfrak{a}$, let z be sent to z' (as an element of $\frac{1}{N}\mathfrak{a}$). Then, $Nz\mathfrak{a}^{-1} = \mathfrak{r}$ is an integral ideal of $\mathcal{O}_K$ coprime to N, and $\tau_{\mathcal{O}_K}(z, \tau)$ only depends on the ray class $[\mathfrak{r}^{-1}] \in \mathrm{Cl}^N(K)$. For $\alpha \in \mathrm{Cl}^N(K)$, we will define $\tau_{\mathcal{O}_K}(\alpha) := \tau_{\mathcal{O}_K}(z, \tau)$ for any z as above such that $[\mathfrak{r}^{-1}] = \alpha$.*

(6) *For any prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ such that the prime number p divisible by $\mathfrak{p}$ satisfies $p > 12$ and $\gcd(p, N\operatorname{disc}(K)) = 1$. Then, for any prime ideal $\mathfrak{P}$ above $\mathfrak{p}$ in a big enough number field and $\alpha \in \mathrm{Cl}^N(K)$,*

$$\tau_{\mathcal{O}_K}(\alpha[\mathfrak{p}]^{-1}) \equiv \tau_{\mathcal{O}_K}(\alpha)^{N(\mathfrak{p})} \pmod{\mathfrak{P}}.$$

Proof. (1) Note that, for any $M \in \mathrm{SL}_2(\mathbb{Z})$, $M = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$, as $\delta M = \begin{pmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{pmatrix}$,

$$\delta_{\gamma,\mathcal{O},N}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}; M \cdot \tau\right) = \tau_{\mathcal{O}}\left(\frac{x_1 + x_2 M \cdot \tau}{N}, M \cdot \tau\right)^p - \tau_{\mathcal{O}}\left(\frac{px_1 + px_2 M \cdot \tau}{N(cM \cdot \tau + d)}, \gamma M \cdot \tau\right)$$

$$= \tau_{\mathcal{O}}\left(\frac{x_1(z\tau + w) + x_2(x\tau + y)}{N}, \tau\right)^p - \tau_{\mathcal{O}}\left(\frac{px_1(z\tau + w) + px_2(x\tau + y)}{N(c(x\tau + y) + d(z\tau + w))}, \gamma M \cdot \tau\right)$$

$$= \tau_{\mathcal{O}}\left(\frac{(x_1 w + x_2 y) + (x_1 z + x_2 x)\tau}{N}, \tau\right)^p - \tau_{\mathcal{O}}\left(\frac{p(x_1 w + x_2 y) + p(x_1 z + x_2 x)\tau}{N((cx + dz)\tau + (cy + dw))}, \gamma M \cdot \tau\right)$$

$$= \delta_{\gamma M,\mathcal{O},N}\left(M\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}; \tau\right).$$

This is why $\delta_{\gamma,\mathcal{O},N}$ was notated vertically in the first place. Note also that, if $M \in G_\gamma$, then $\mathrm{SL}_2(\mathbb{Z})\gamma = \mathrm{SL}_2(\mathbb{Z})\gamma M$, so $\binom{x_1}{x_2} \mapsto M\binom{x_1}{x_2}$ permutes the pairs $\binom{x_1}{x_2}$ such that $x_1, x_2 \in \mathbb{Z}/N\mathbb{Z}$, $\gcd(x_1, x_2, N) = 1$. This implies that $S_{\gamma,\mathcal{O},N}(X, \tau)$ is invariant under the action of G_γ on τ. It is clear that the coefficients are holomorphic on $\mathbb{H}$ and meromorphic at cusps, so we get the desired result.

(2) Note that the q-expansion of $\tau_{\mathcal{O}}\left(\frac{x_1 + x_2\tau}{N}, \tau\right)$ already have p-integral coefficients. Moreover, as noted in the proof of Theorem 15.12, the q-expansion of $D^{(k)}_{\gamma,\mathcal{O},N}(\tau)$ has coefficients in $\mathbb{Q}(\zeta_N)$, and the action of an element in $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, $\zeta_N \mapsto \zeta_N^r$, permutes

$\delta_{\gamma,\mathcal{O},N}\left(\binom{x_1}{x_2};\tau\right)$ for $x_1, x_2 \in \mathbb{Z}/N\mathbb{Z}$, $\gcd(x_1, x_2, N) = 1$, so the q-expansion of $D^{(k)}_{\gamma,\mathcal{O},N}(\tau)$ has coefficients actually in $\mathbb{Q}$.

If $\gamma = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$,

$$\delta_{\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix},\mathcal{O},N}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix};\tau\right) = \tau_{\mathcal{O}}\left(\frac{x_1 + x_2\tau}{N}, \tau\right)^p - \tau_{\mathcal{O}}\left(\frac{px_1 + px_2\tau}{N}, p\tau\right).$$

Note that the q-expansion of $\tau_{\mathcal{O}}\left(\frac{px_1+px_2\tau}{N}, p\tau\right)$ is obtained from that of $\tau_{\mathcal{O}}\left(\frac{x_1+x_2\tau}{N}, \tau\right)$ by replacing q by q^p and ζ_N by ζ_N^p, so it follows that $\tau_{\mathcal{O}}\left(\frac{x_1+x_2\tau}{N}, \tau\right)^p \equiv \tau_{\mathcal{O}}\left(\frac{px_1+px_2\tau}{N}, p\tau\right) \pmod p$, which is what we want.

(3) By using the exactly same arguments as Theorem 14.10(3), one can show that the field of modular functions for G_γ, denoted $K(Y(G_\gamma))$, is precisely $\mathbb{C}(j, \varphi_\gamma)$ (in particular, φ_γ is a modular function for G_γ, with the minimal polynomial of φ_γ over $\mathbb{C}(j)$ of degree p). Furthermore, we know that the q-expansion of φ_γ has integral coefficients. This implies that, by (2), $D^{(k)}_{\gamma,\mathcal{O},N}(\tau) = F(j(\tau), \varphi_\gamma(\tau))$, where $F(X, Y) \in \mathbb{Q}(\zeta_p)[X, Y]$ has p-integral coefficients. Therefore, by Theorem 15.6(2), $D^{(k)}_{\gamma,\mathcal{O},N}(\tau')$ is an algebraic number. Furthermore, if γ is such that $\gamma(\mathbb{Z} \oplus \mathbb{Z}\tau') \cong \mathfrak{p}'\mathfrak{a}$, then we have

$$D^{(k)}_{\gamma,\mathcal{O},N}(\tau) \prod_{\sigma\in C(p),\sigma\neq\gamma} (\varphi_\gamma(\tau) - \varphi_\sigma(\tau)) = a_0(j(\tau)) + a_1(j(\tau))\varphi_\gamma(\tau) + \cdots + a_p(j(\tau))\varphi_\gamma(\tau)^p,$$

for $a_0(Y), \cdots, a_p(Y) \in \mathbb{Q}[Y]$ with p-integral coefficients. We claim that $a_0(j(\tau'))$ is divisible by p. Indeed, note that for any $\delta \in C(p)$, we have

$$D^{(k)}_{\delta,\mathcal{O},N}(\tau) \prod_{\sigma\in C(p),\sigma\neq\delta} (\varphi_\delta(\tau) - \varphi_\sigma(\tau)) = a_0(j(\tau)) + a_1(j(\tau))\varphi_\delta(\tau) + \cdots + a_p(j(\tau))\varphi_\delta(\tau)^p,$$

so our claim follows from the fact from (2) and the fact that $\varphi_{\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}}(\tau')$ is divisible by p^{12}, as proved in Theorem 15.6(4).

On the other hand, $\prod_{\sigma\in C(p),\sigma\neq\gamma}(\varphi_\gamma(\tau') - \varphi_\sigma(\tau'))$ is not divisible by $\overline{\mathfrak{p}'}$, as $\varphi_\gamma(\tau')$ is divisible by $\overline{\mathfrak{p}'}$ by Theorem 15.6(3) and $\varphi_\sigma(\tau')$ is not divisible by $\overline{\mathfrak{p}'}$ by Theorem 15.6(3), (4). Therefore, $D^{(k)}_{\gamma,\mathcal{O},N}(\tau')$ is divisible by $\overline{\mathfrak{p}'}$.

(4) Let $C(p) = \{\sigma_0, \cdots, \sigma_p\}$, as usual, and $F(X, \tau) = \prod_{i=0}^p (X - D^{(k)}_{\sigma_i,\mathcal{O},N}(\tau))$. It is easy to see that $F(X, \tau) = F(X, j(\tau))$ for $F(X, Y) \in \mathbb{Q}[X, Y]$ with p-integral coefficients, by comparing q-expansions and showing that the q-expansion is fixed under the Galois conjugation by $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. This implies that $D^{(k)}_{\sigma_i,\mathcal{O},N}(\tau')$ is algebraic for $0 \leq i \leq p$.

By the same reason as the proof of Theorem 14.10(7), combined with (2), we obtain that

$$F(X,j(\tau)) \equiv X\left(X^p - D^{(k)}_{\begin{pmatrix}1 & 0\\0 & p\end{pmatrix},\mathcal{O},N}(\tau)^p\right) \pmod{1-\zeta_p}.$$

Therefore, $F(X,Y) \equiv X(X^p - a_1(Y)) \pmod{p}$, where $a_1(Y)$ is the coefficient of the X-term of $F(X,Y)$. Here, $\bmod p$ congruence makes sense as the coefficients are already known to be p-integral. In particular, the constant term is divisible by p, and therefore there exists $0 \le i \le p$ such that $D^{(k)}_{\sigma_i,\mathcal{O},N}(\tau')$ is divisible by p. To be more precise, let $\mathfrak{P}$ be a prime ideal of $L := \mathbb{Q}(j(\tau'), D^{(k)}_{\sigma_0,\mathcal{O},N}(\tau'), \cdots, D^{(k)}_{\sigma_p,\mathcal{O},N}(\tau'))$ above p. Then, $\prod_{0\le j\le p, j\ne i}(X - D^{(k)}_{\sigma_j,\mathcal{O},N}(\tau')) \equiv X^p - Q_1(j(\tau')) \pmod{\mathfrak{P}}$. Therefore, $D^{(k)}_{\sigma_j,\mathcal{O},N}(\tau')^p \equiv Q_1(j(\tau')) \pmod{\mathfrak{P}}$ for all $0 \le j \le p$, $j \ne i$.

If $D^{(k)}_{\sigma_i,\mathcal{O},N}(\tau')$ is a multiple zero of $F(X,j(\tau'))$, then this implies that $Q_1(j(\tau')) \equiv 0 \pmod{\mathfrak{P}}$, so that $D^{(k)}_{\sigma_j,\mathcal{O},N}(\tau') \equiv 0 \pmod{\mathfrak{P}}$ for every j, which is what we wanted.

If $D^{(k)}_{\sigma_i,\mathcal{O},N}(\tau')$ is a simple zero of $F(X,j(\tau'))$, then $D^{(k)}_{\sigma_i,\mathcal{O},N}(\tau)$ is a simple zero of $F(X,j(\tau))$. This implies that $D^{(k)}_{\sigma_i,\mathcal{O},N}$ generates $K(Y(G_{\sigma_i}))/K(Y(1))$, as $F(X,j(\tau'))$ is of the same degree as $[K(Y(G_{\sigma_i})) : K(Y(1))] = p+1$. This implies that

$$\frac{\partial F}{\partial X}(D^{(k)}_{\sigma_i,\mathcal{O},N}(\tau), j(\tau))\varphi_{\sigma_i}(\tau) = c_0(j(\tau)) + c_1(j(\tau))D^{(k)}_{\sigma_i,\mathcal{O},N}(\tau) + \cdots + c_p(j(\tau))D^{(k)}_{\sigma_i,\mathcal{O},N}(\tau)^p.$$

As $\frac{\partial F}{\partial X}(D^{(k)}_{\sigma_i,\mathcal{O},N}(\tau'), j(\tau')) \ne 0$, $\varphi_{\sigma_i}(\tau') \in \mathbb{Q}(j(\tau'), D^{(k)}_{\sigma_i,\mathcal{O},N}(\tau'))$. Note that $\prod_{j=0}^p \varphi_{\sigma_j}(\tau') = \pm p^{12}$, as proved in Theorem 15.6(4). We claim that $\varphi_{\sigma_j}(\tau')$ and $\varphi_{\sigma_{j'}}(\tau')$ for $j \ne j'$ are off by a unit (i.e. $\frac{\varphi_{\sigma_{j'}}(\tau')}{\varphi_{\sigma_j}(\tau')}$ is a unit). Indeed, as p does not divide the conductor of $\mathcal{O}$, which we denote by M, if $\mathbb{Z}\oplus\mathbb{Z}\tau' \cong \mathfrak{a}$ for a proper $\mathcal{O}$-ideal $\mathfrak{a}$, then for any $\sigma_{j''}$ for $0 \le j'' \le p$, $\sigma_{j''}(\mathbb{Z}\oplus\mathbb{Z}\tau') \cong \mathfrak{a}_{j''}$ is a proper $\mathcal{O}_p$-ideal, where $\mathcal{O}_p = \mathbb{Z}\oplus pM\mathcal{O}_K$ is the order of conductor pM (it is easy that the $\mathcal{O}_p$-action stabilizes $\mathfrak{a}_{j''}$ as p is coprime to M, and it is a proper ideal as it is invertible; the inverse is either $p\sigma_{j''}$ or $\frac{1}{p}\sigma_{j''}$ applied to $\mathfrak{a}^{-1}$).

Our claim will be proved if we show that $\frac{\varphi_{\sigma_{j'}}(\tau')}{\varphi_{\sigma_j}(\tau')}$ is coprime to any prime number ℓ. Let $\mathfrak{c}$ be a proper $\mathcal{O}_p$-ideal in the same class as $\mathfrak{a}_{j'}\mathfrak{a}_j^{-1}$ which is coprime to $pM\ell$. Then there is $\gamma \in \mathcal{O}_p$ such that $\mathfrak{a}_{j'}\gamma = \mathfrak{a}_j\mathfrak{c}$. As $\mathfrak{c}$ is coprime to $pM\ell$, it is of the form $\mathfrak{c}'\cap\mathcal{O}_p$ for an ideal $\mathfrak{c}' \subset \mathcal{O}_K$ of order coprime to $pM\ell$. Then, by taking the associated $\mathcal{O}$-ideal, we get

$$\mathfrak{a}\gamma = \mathfrak{a}(\mathfrak{c}'\cap\mathcal{O}),$$

so $\mathfrak{c}'\cap\mathcal{O}$ is a principal ideal generated by γ. Therefore, there is an integer 2×2 matrix $A = \begin{pmatrix} x & y \\ z & w\end{pmatrix}$ of determinant $N_{K/\mathbb{Q}}(\gamma)$ such that

$$\sigma_{j'}(\gamma\mathbb{Z}\oplus\gamma\mathbb{Z}\tau') = A(\sigma_j(\mathbb{Z}\oplus\mathbb{Z}\tau')),$$

where furthermore the two basis vectors correspond to each other (i.e. $\gamma \leftrightarrow 1$, $\gamma\tau' \leftrightarrow \tau'$). This implies that

$$\frac{\varphi_{\sigma_{j'}}(\tau')}{\varphi_{\sigma_j}(\tau')} = \frac{\Delta(\sigma_{j'} \cdot \tau')}{\Delta(\sigma_j \cdot \tau')} = \frac{\Delta\left(\frac{A\sigma_j \cdot \tau'}{\gamma}\right)}{\Delta(\sigma_j \cdot \tau')} = \frac{\varphi_A(\sigma_j \cdot \tau')(z\sigma_j \cdot \tau' + w)^{12}\Delta\left(\frac{A\sigma_j \cdot \tau'}{\gamma}\right)}{N_{K/\mathbb{Q}}(\gamma)^{12}\Delta(A\sigma_j \cdot \tau')}$$

$$= \frac{\varphi_A(\sigma_j \cdot \tau')\gamma^{12}}{N_{K/\mathbb{Q}}(\gamma)^{12}}.$$

We know that $\varphi_A(\sigma_j \cdot \tau')$ is a factor of a power of $N_{K/\mathbb{Q}}(\gamma)$ by Theorem 15.6(2), so this quantity is coprime to ℓ, as desired.

As $\varphi_{\sigma_i}(\tau')^{p+1}$ and p^{12} are off by a unit, $p + 1 > 12$, and $\mathfrak{p}$ is unramified in $\mathbb{Q}(j(\tau'))$, it follows that $\mathfrak{P}$ is ramified over $\mathbb{Q}(j(\tau'))$. Let $\mathfrak{q} = \mathfrak{P} \cap \mathcal{O}_{\mathbb{Q}(j(\tau'))}$. Then, $I(\mathfrak{P}|\mathfrak{q}) \cap \mathrm{Gal}(L/\mathbb{Q}(j(\tau'), D^{(k)}_{\sigma_i,\mathcal{O},N}(\tau'))) \neq \{1\}$. Let λ be a nontrivial element in the intersection. Then, $\lambda(D^{(k)}_{\sigma_i,\mathcal{O},N}(\tau')) = D^{(k)}_{\sigma_{i'},\mathcal{O},N}(\tau')$ for $i \neq i'$, and the divisibility by $\mathfrak{P}$ stays the same, so $D^{(k)}_{\sigma_{i'},\mathcal{O},N}(\tau')$ is divisible by $\mathfrak{P}$. Therefore, $Q_1(j(\tau'))$ is also divisible by $\mathfrak{P}$, so $D^{(k)}_{\sigma_j,\mathcal{O},N}(\tau')$ is divisible by all j, as desired.

(5) This is easy; exercise.

(6) This is an easy consequence of (3), (4) and the definition of $D^{(k)}_{\gamma,\mathcal{O},N}$, proved just as Theorem 15.3.

□

Now we are ready to prove the reciprocity law and the Second Main Theorem of complex multiplication.

Theorem 15.15 (Second Main Theorem of Complex Multiplication). *Let K be an imaginary quadratic field, and let $\tau \in \mathbb{H}$ be a quadratic number such that $\mathrm{End}(\mathbb{Z} \oplus \mathbb{Z}\tau) = \mathcal{O}_K$. Let $N \in \mathbb{N}$. Then, the ray class field K with modulus N is given by*

$$K(N) = K(j(\tau), \{\tau_{\mathcal{O}_K}(z, \tau) \ : \ z \in \frac{1}{N}(\mathbb{Z} \oplus \mathbb{Z}\tau)/(\mathbb{Z} \oplus \mathbb{Z}\tau)\}).$$

Proof. Let the number field on the right hand side by denoted L. As in the proof of the First Main Theorem, we use the splitting primes. The nicer thing is that Theorem 15.12 already tells you that the values $\tau_{\mathcal{O}}(z, \tau)$'s are conjugates to each other, so L/K is Galois.

Therefore, as per the density argument, we only need to show that $\mathcal{S}(K(N)/K)$ and $\mathcal{S}(L/K)$ have the same Dirichlet density. If $\mathfrak{p} \in \mathcal{S}(K(N)/K)$ that is unramified over $\mathbb{Q}$, then by Theorem 15.3 and Theorem 15.14(6), $\mathfrak{p}$ has to split completely in L. Conversely, if $\mathfrak{p} \in \mathcal{S}(L/K)$ that is unramified over $\mathbb{Q}$ and any difference $j(\tau) - j(\tau')$ for $\mathrm{End}(\mathbb{Z} \oplus \mathbb{Z}\tau) = \mathrm{End}(\mathbb{Z} \oplus \mathbb{Z}\tau') = \mathcal{O}_K$, then exactly as in the proof of Theorem 15.1, we see that $\mathfrak{p}$ is principal. Here comes the reason why the Weber function is defined in such a weird way: it is invariant under any automorphism of the lattice (=elliptic curve). Namely, if $\tau_{\mathcal{O}_K}(\alpha) = \tau_{\mathcal{O}_K}(\beta)$ for $\alpha, \beta \in \mathrm{Cl}^N(K)$ that arise to the same class in $\mathrm{Cl}(K)$ (i.e. $\frac{\alpha}{\beta}$ is a principal ideal, although maybe not congruent to 1 mod N), then α/β is congruent to a unit of $\mathcal{O}_K^\times$ mod N, and this is if and only if. Therefore, any difference $\tau_{\mathcal{O}_K}(\alpha)-\tau_{\mathcal{O}_K}(\beta)$ for $\alpha \neq \beta \in \mathrm{Cl}^N(K)$ with their images being the same in $\mathrm{Cl}(K)$ is nonzero, and we can exclude the prime ideals dividing any such difference. Then, the congruence in Theorem 15.14(6) plus $\mathfrak{p}$ avoiding the differences imply that $\mathfrak{p}$ has to be 1 mod N, so it must split completely in $K(N)$, as desired. □

Exercise 15.1. Formulate and prove the reciprocity law for the values of the Weber function $\tau_{\mathcal{O}_K}(z,\tau)$, in the similar way as Theorem 15.3.

Remark 15.16. The analogous statement to Second Main Theorem holds for $K(\mathfrak{m})$ for a general modulus $\mathfrak{m}$ of K, where now we need to take the values of the Weber function at the "$\mathfrak{m}$-torsion points".

Remark 15.17. The Second Main Theorem describes $K(N)$ by using the j-invariants of the lattices (=elliptic curves over $\mathbb{C}$) with complex multiplication by $\mathcal{O}_K$ and the associated Weber functions. On the other hand, the First Main Theorem describes the ring class field using the j-invariants of those having complex multiplication by a possibly non-maximal order. There is a way to connect these two, describing $K(N)$ in terms of those having complex multiplication by a general order.

Example 15.18 (Comparing **Explicit Class Field Theories**). We have seen three types of **Explicit Class Field Theory**, for $\mathbb{Q}$ (Kronecker–Weber theorem), for local fields (Lubin–Tate theory), and for imaginary quadratic field (Second Main Theorem of complex multiplication). They all have the same theme: for the explicit class field theory for a field F, you must find a group structure with a large endomorphism by $\mathcal{O}_F$, and the ray class fields are obtained by adjoining to the maximal unramified extension of F the torsion points of the group you found. To write more concisely:

- $F = \mathbb{Q}$ (Kronecker–Weber Theorem, Theorem 8.1)
  - Group: the multiplicative group $\overline{\mathbb{Q}}^\times$.
  - Torsion points: $X^N = 1$, so the powers of ζ_N.
  - $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\{\zeta_N \ : \ N \geq 1\})$.
- F is a local field (Lubin–Tate theory, §10)
  - Group: $(\mathfrak{m}_{F^{\mathrm{sep}}}, F_f)$ where F_f is a Lubin–Tate formal group law (Theorem 10.6).
  - Torsion points: $\mathfrak{m}_{F^{\mathrm{sep}}}[f^{\circ n}]$ (Theorem 10.8).
  - $F^{\mathrm{ab}} = F^{\mathrm{nr}}F_\pi = F^{\mathrm{nr}}(\mathfrak{m}_{F^{\mathrm{sep}}}[f^{\circ n}])$ (Theorem 10.12).
- F is an imaginary quadratic field (CM theory, §15)
  - Group: Lattice $\Lambda \subset \mathbb{C}$ (=elliptic curve over $\mathbb{C}$) with complex multiplication by $\mathcal{O}_F$ (Definition 13.16).

  - Torsion points: $\frac{1}{N}\Lambda$ (Definition 15.11).
  - $F^{\mathrm{ab}} = F(j(\mathcal{O}_F), \{\tau_{\mathcal{O}_K}(z, \Lambda) : z \in \frac{1}{N}\Lambda\}) = H_F(\{\tau_{\mathcal{O}_K}(z, \Lambda) : z \in \frac{1}{N}\Lambda\})$ (Second Main Theorem of Complex Multiplication, Theorem 15.15).

There is also a slightly more vague analogy between the role of the j-function and the exponential; namely, both are functions where the input and the output being both algebraic is extremely rare, and the maximal unramified extensions are obtained by the values of the function in those very rare cases.

- For $F = \mathbb{Q}$, $H_{\mathbb{Q}} = \mathbb{Q}$ (Minkowski's theorem, Theorem 8.5) and there is nothing to talk about. There is no bigger everywhere unramified extension because the multiplicative group is unique.
- For F a p-adic local field, $F^{\mathrm{nr}} = \cup_{(n,p)=1} F(\zeta_n)$, and $\zeta_n = e^{2\pi i \frac{1}{n}} \in \overline{\mathbb{Q}}^{\times}$. Let's define a function $f : \mathbb{R} \to \mathbb{C}$ by $f(x) = e^{2\pi i x}$. Then it is an easy exercise to see that, for $x \in \mathbb{R}$, both x and $f(x)$ are algebraic if and only if $x \in \mathbb{Q}$. Note also that there are many non-isomorphic Lubin–Tate formal group laws over F, and that they become all isomorphic over F^{nr} (Lemma 10.14).
- For F an imaginary quadratic field, $H_F = F(j(\mathcal{O}_F))$ (Corollary 15.7). We also know that, for $\tau \in \mathbb{H}$, both τ and $j(\tau)$ are algebraic if and only if τ is a quadratic number (Theorem 15.1, Theorem 15.8).

Part 3. **Class field theory as the Langlands correspondence for** $\mathrm{GL}(1)$

16. Setup and local theory

16.1. **Weil groups.** Let F be a local field. Then, we explained that the local Artin map

$$\mathrm{Art}_F : F^{\times} \to \mathrm{Gal}(F^{\mathrm{ab}}/F) = \mathrm{Gal}(\overline{F}/F)^{\mathrm{ab}},$$

is never an isomorphism (here $\overline{F}$ is the separable closure of F), because there is a "difference between $\mathbb{Z}$ and $\widehat{\mathbb{Z}}$." One way to resolve this into establishing an isomorphism is to demote $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ to a smaller group, called the **Weil group**.

Definition 16.1 (Weil group)**.** For a local field F, consider the short exact sequence of groups

$$1 \to I_F \to \mathrm{Gal}(\overline{F}/F) \to \mathrm{Gal}(F^{\mathrm{nr}}/F) \to 1,$$

where $I_F := \mathrm{Gal}(\overline{F}/F^{\mathrm{nr}})$ is the inertia group. Note also that $\mathrm{Gal}(F^{\mathrm{nr}}/F) \cong \widehat{\mathbb{Z}}$ naturally by identifying the Frobenius of $\mathrm{Gal}(F^{\mathrm{nr}}/F)$ with $1 \in \widehat{\mathbb{Z}}$. Let $\iota : \mathrm{Gal}(\overline{F}/F) \to \mathrm{Gal}(F^{\mathrm{nr}}/F)$ be the natural surjective map of the short exact sequence. Then, $W_F := \iota^{-1}(\mathbb{Z})$ is the **Weil group** of F. It sits in a natural short exact sequence

$$1 \to I_F \to W_F \xrightarrow{\iota} \mathbb{Z} \to 1.$$

The topology of W_F is such that $I_F \leq W_F$ is an open subgroup and the subspace topology on I_F is the same as the natural topology on I_F as an infinite Galois group.

The last part on topology is making the topology to look like something like $F^\times$ where there is a profinite part and a discrete part. Note that W_F is a subgroup of $\mathrm{Gal}(\overline{F}/F)$ but the topology of W_F is not the subspace topology of $\mathrm{Gal}(\overline{F}/F)$.

The local Artin map then can be demoted to an isomorphism of topological groups

$$\mathrm{Art}_F : F^\times \xrightarrow{\sim} W_F^{\mathrm{ab}},$$

which is actually much more frequent way of thinking about local class field theory in practice. This also has an advantage of working for local fields of positive characteristic.

From the local class field theory, we obviously have the following. Let E be a topological field (a field with topology). Then, there is a one-to-one bijection,

$$\left\{\begin{matrix}\text{Continuous homomorphisms}\\ F^\times \to E^\times\end{matrix}\right\} \leftrightarrow \left\{\begin{matrix}\text{Continuous homomorphisms}\\ W_F^{\mathrm{ab}} \to E^\times\end{matrix}\right\}.$$

Because $E^\times$ is abelian, this gives a one-to-one bijeciton

$$\left\{\begin{matrix}\text{Continuous homomorphisms}\\ F^\times \to E^\times\end{matrix}\right\} \leftrightarrow \left\{\begin{matrix}\text{Continuous homomorphisms}\\ W_F \to E^\times\end{matrix}\right\}.$$

The subject of local Langlands correspondence is when we use $E = \overline{\mathbb{Q}}_\ell$ for $\ell \neq p$ (or we also sometimes use any finite extension of $\mathbb{Q}_\ell$).

$$\left\{\begin{matrix}\text{Continuous homomorphisms}\\ F^\times \to \overline{\mathbb{Q}}_\ell^\times\end{matrix}\right\} \leftrightarrow \left\{\begin{matrix}\text{Continuous homomorphisms}\\ W_F \to \overline{\mathbb{Q}}_\ell^\times\end{matrix}\right\}.$$

This is called the **local Langlands correspondence for** $\mathrm{GL}_1(F)$.

16.2. **Smooth representations of algebraic groups.** We will briefly mention how this bijection is generalized in more general Langlands program. Firstly we need to understand what we mean by $\mathrm{GL}_1(F)$. For $n \geq 1$, we let $\mathrm{GL}_n(F)$ be the group of invertible $n \times n$ matrices with entries in F. There is a natural way to give a topology on this group; consider the injective map $\mathrm{GL}_n(F) \to \mathrm{Mat}_{n\times n}(F) \times \mathrm{Mat}_{n\times n}(F)$, $X \mapsto (X, X^{-1})$, where $\mathrm{Mat}_{n\times n}(F)$ is the set of $n \times n$ matrices with entries in F; as $\mathrm{Mat}_{n\times n}(F) \cong F^{n^2}$, this set is naturally topologized by the topology of F, and we let $\mathrm{GL}_n(F)$ to be inherited the subspace topology along the said embedding.

In particular, $\mathrm{GL}_1(F) = F^\times$ (with the matching topology). So the local Langlands correspondence for $\mathrm{GL}_1(F)$ can be rewritten as

$$\left\{\begin{matrix}\text{Continuous homomorphisms}\\ \mathrm{GL}_1(F) \to \overline{\mathbb{Q}}_\ell^\times\end{matrix}\right\} \leftrightarrow \left\{\begin{matrix}\text{Continuous homomorphisms}\\ W_F \to \mathrm{GL}_1(\overline{\mathbb{Q}}_\ell)\end{matrix}\right\}.$$

The **local Langlands correspondence for** $\mathrm{GL}_n(F)$ for $n \geq 1$ is actually a bijection

$$\left\{\begin{matrix}\text{Smooth admissible}\\ \text{irreducible representations}\\ \text{of } \mathrm{GL}_n(F)\end{matrix}\right\} \leftrightarrow \left\{\begin{matrix}\text{Frobenius-semisimple continuous}\\ \text{homomorphisms } W_F \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)\end{matrix}\right\},$$

plus a bunch of conditions. Our modest goal is to explain what modifications were made so that this is truly a generalization of the local Langlands correspondence for $\mathrm{GL}_1(F)$ (i.e. when $n = 1$ this general statement specializes to what we know).

- The right side ("**Galois side**"): other than 1 becoming n, there is only one change, namely there is an additional adjective **"Frobenius-semisimple"**. What does this mean? A **Frobenius element** of W_F is any element $g \in W_F$ such that $\iota(g) = 1$ in $\mathbb{Z}$. We want this to be **semisimple**, i.e. sent to a matrix that is **diagonalizable**. This additional adjective did not appear in the case when $n = 1$, as any 1×1 matrix is diagonalizable.

- The left side ("**automorphic side**"[21]): other than 1 becoming n, there are quite a few changes.

  - **Smooth admissible irreducible representations of** $\mathrm{GL}_n(F)$. We explain in four parts.

    * $\cdots$ **representations of** $\mathrm{GL}_n(F)$. This is just a vector space V over $\overline{\mathbb{Q}}_\ell$ together with a linear action of $\mathrm{GL}_n(F)$. Note that for this we **do not assume that** V **is finite-dimensional**. In fact most representations appearing on the left side ("automorphic side") will actually be infinite dimensional.
    * **Smooth** $\cdots$. Given a representation of $\mathrm{GL}_n(F)$ (acting on V), a vector $v \in V$ is a **smooth vector** if the stabilizer of v in $\mathrm{GL}_n(F)$ (i.e. the subgroup $\{g \in \mathrm{GL}_n(F) \ : \ gv = v\}$) is an open subgroup. A representation is **smooth** if every vector is a smooth vector.
    * $\cdots$ **admissible** $\cdots$. This means that, for any open subgroup $U \leq \mathrm{GL}_n(F)$, the U-fixed vectors V^U are finite-dimensional.
    * $\cdots$ **irreducible** $\cdots$. A representation is irreducible if there is no nonzero proper subspace stable under the action by $\mathrm{GL}_n(F)$.

  - **Why is there no $\overline{\mathbb{Q}}_\ell$ in the left side?** This is because the notion of smoothness **does not care about the topology of the vector space** (Exercise: look through the above definitions and convince yourself of this). In particular, the notion only cares about the field $\overline{\mathbb{Q}}_\ell$ without caring about its topology. The point now is that an algebraically closed field with the same cardinality and characteristic is unique up to isomorphism, so as fields (without caring about topology) $\overline{\mathbb{Q}}_\ell \cong \overline{\mathbb{Q}}_p \cong \mathbb{C} \cong \cdots$. Therefore, as long as you use any of these fields as base fields for the vector spaces, the notion does not change!

So why did all these not appear when $n = 1$? We need to show that continuous homomorphisms $\mathrm{GL}_1(F) \to \overline{\mathbb{Q}}_\ell^\times$ are precisely the smooth admissible irreducible representations of $\mathrm{GL}_1(F)$.

  - Let $\mathrm{GL}_1(F) \to \overline{\mathbb{Q}}_\ell^\times$ be a continuous homomorphism. Then this is obviously irreducible (being a one-dimensional representation) and admissible (representation is already finite-dimensional). For the smoothness, we need to look at what kind of representation this is. Let $\pi \in F$ be a uniformizer. Then $F^\times = \pi^{\mathbb{Z}} \times \mathcal{O}_F^\times$, so firstly you

[21] The reason why it's called the automorphic side will be clarified later.

decide where π goes, which can be arbitrary element in $\overline{\mathbb{Q}}_\ell^\times$ (this does not affect continuity). So what is a continuous homomorphism $\psi : \mathcal{O}_F^\times \to \overline{\mathbb{Q}}_\ell^\times$? Well, $\mathcal{O}_F^\times \supset 1+\pi\mathcal{O}_F$, and this subgroup is pro-p, when F is a p-adic field. On the other hand, $\overline{\mathbb{Q}}_\ell^\times$ is locally a pro-ℓ group (i.e. there is an open subgroup of $\overline{\mathbb{Q}}_\ell^\times$ that is pro-ℓ). Let $V \subset \overline{\mathbb{Q}}_\ell^\times$ be pro-ℓ. Then by possibly shrinking V, $U := \psi^{-1}(V)$ must be a pro-p group. Then $U \xrightarrow{\psi} V$ is a continuous homomorphism from a pro-p group to a pro-ℓ-group, which actually must be zero (Exercise: check this). Therefore, this implies that ψ factors through a finite quotient of $\mathcal{O}_F^\times$.

From this, we see that any vector of the 1-dimensional representation is fixed by $\ker \psi$, which is an open finite index subgroup of $\mathcal{O}_F^\times$. So in any case the stabilizer will be open.

- Conversely, let's say we have a smooth admissible irreducible representation of $\mathrm{GL}_1(F) = F^\times$ (with base field $\overline{\mathbb{Q}}_\ell$), acting on V. Take a nonzero vector $v \in V$. Then the stabilizer is an open subgroup of $F^\times$. Let G be this stabilizer. Then, V^G is finite-dimensional by admissibility. Note that $\pi^n \cdot v$ is fixed by G, as $F^\times$ is abelian. Therefore, $\pi : V^G \to V^G$ is a linear endomorphism, and by the finite-dimensionality of V^G and as $\overline{\mathbb{Q}}_\ell$ is algebraically closed, it follows that there is $w \in V^G$ such that $\pi w = \lambda w$ for some $\lambda \in \overline{\mathbb{Q}}_\ell$. Let W be the span of all vectors of the form $g \cdot w$ for $g \in \mathcal{O}_F^\times$. By smoothness, we know that W is finite-dimensional. Moreover, as $F^\times$ is abelian, π acts on W by the scalar λ. Therefore, W is stable under the action of $F^\times$, so $V = W$, and in particular V is finite-dimensional. Now we can use that a finite-dimensional irreducible representation of an abelian group must be one-dimensional, to deduce that such a representation must be at least a homomorphism $\mathrm{GL}_1(F) \to \overline{\mathbb{Q}}_\ell^\times$. By smoothness, it follows that this homomorphism restricted to $\mathcal{O}_F^\times$ must factor through a finite quotient, so this must be continuous.

Remark 16.2. (1) It is interesting that the left side evolves to an infinite-dimensional representation theory of $\mathrm{GL}_n(F)$ that does not care about topology of coefficient field, whereas the right side evolves to a finite-dimensional representation theory of W_F that cares about the topology of the coefficient field. In fact, the independence of the RHS on ℓ is an interesting result on its own right.

(2) In fact, the adjective "admissible" is unnecessary, as any smooth irreducible representations of $\mathrm{GL}_n(F)$ are automatically admissible. This is not an easy result and is first proved by Jacquet.

(3) There are several desiderata on the bijection so that there is a unique bijection satisfying the desiderata. These include the compatibility with the local class field theory, and the matching of L-factors and ϵ-factors.

16.3. **Local Hecke algebra.** There is a ring that encodes everything about the smooth representation theory of $\mathrm{GL}_n(F)$, which is called the **(local) Hecke algebra**.

Definition 16.3. For a finite index subgroup K of $\mathrm{GL}_n(\mathcal{O}_F)$, let

$$\mathcal{H}(K) = \{f : \mathrm{GL}_n(F) \to \overline{\mathbb{Q}}_\ell \ : \ f \text{ is smooth, bi-}K\text{-invariant and compactly supported}\}.$$

Here, f is **smooth** if f is locally constant, is **bi-K-invariant** if $f(gxh) = f(x)$ for $g, h \in K$, $x \in \mathrm{GL}_n(F)$, and is **compactly supported** if there is a compact subset $C \subset \mathrm{GL}_n(F)$ such that $f(x) = 0$ for $x \notin C$. Let $\mathcal{H} = \bigcup_{K \leq \mathrm{GL}_n(\mathcal{O}_F)} \mathcal{H}(K)$. This $\mathcal{H}$ is called the **(local) Hecke algebra**.

Example 16.4. For a finite index subgroup $K \leq \mathrm{GL}_n(\mathcal{O}_F)$, the characteristic function $\mathbf{1}_K \in \mathcal{H}(K)$. Recall that the definition of $\mathbf{1}_K$ is

$$\mathbf{1}_K(x) = \begin{cases} 1 & \text{if } x \in K \\ 0 & \text{otherwise.} \end{cases}$$

The reason why $\mathcal{H}$ is called an algebra is because there is a multiplication defined on it. Namely, for $f_1, f_2 \in \mathcal{H}$, we define the **convolution product**

$$f_1 * f_2(g) = \int_{\mathrm{GL}_n(F)} f_1(gh^{-1}) f_2(h) dh.$$

Exercise 16.1. Check that $f_1, f_2 \in \mathcal{H}(K)$ implies $f_1 * f_2 \in \mathcal{H}(K)$.

Exercise 16.2. If we define, for a finite index subgroup $K \leq \mathrm{GL}_n(\mathcal{O}_F)$, $e_K := \frac{1}{\mathrm{vol}(K)} \mathbf{1}_K \in \mathcal{H}$, check that $e_K * e_K = e_K$ (i.e. $e_K \in \mathcal{H}$ is an idempotent).

This big ring acts on any smooth representation V of $\mathrm{GL}_n(F)$; if $f \in \mathcal{H}$, then, for $v \in V$,

$$f \cdot v := \int_{\mathrm{GL}_n(F)} f(g)(g \cdot v) dg.$$

This integral is well-defined because f is locally constant and compactly supported. Thus, any smooth representation of $\mathrm{GL}_n(F)$ can be seen as an $\mathcal{H}$-module. In fact, there is a reverse direction, that "smooth" $\mathcal{H}$-modules are smooth representations of $\mathrm{GL}_n(F)$, but we won't need this.

17. Automorphic representations

To describe how the global class field theory is massaged into something that can be generalized into the global Langlands correspondence for GL_n, it requires a lot more work to do. Again, our starting point is the global Artin map: for a number field L, the map

$$\mathrm{Art}_L : C_L \to \mathrm{Gal}(\overline{L}/L)^{\mathrm{ab}}.$$

In the context of Langlands program, one writes $C_L = L^\times \backslash I_L = L^\times \backslash \mathbb{A}_L^\times$. This is not an isomorphism, but the difference between $L^\times \backslash \mathbb{A}_L^\times$ and $\mathrm{Gal}(\overline{L}/L)^{\mathrm{ab}}$ is more subtle than the local case. Rather than massaging this to an isomorphism, we investigate in which situations the characters of $L^\times \backslash \mathbb{A}_L^\times$ can be related to the characters of $\mathrm{Gal}(\overline{L}/L)$.

17.1. **Automorphic forms.** The main players in the "automorphic side" are **automorphic representations**, which will be defined shortly. Automorphic representations are roughly speaking a collection of **automorphic forms**. Before giving you a definition of automorphic forms, keep the following examples in mind.

- Hecke characters for L (i.e. characters of the idele class group C_L) are automorphic forms for GL_1 over L.
- Modular forms are automorphic forms for GL_2 over $\mathbb{Q}$.

Modular forms are holomorphic functions on the upper half plane, while Hecke characters involve adeles. They look quite different; it amounts to the fact that automorphic forms can be defined in two related but different ways. Some features we see in either example are:

- they have a transformation law with respect to some group (both Hecke characters and modular forms);
- they are related to adeles (Hecke characters);
- they are related to some geometric space associated to the group (modular forms);
- they do not grow too fast at infinity (modular forms);
- they satisfy a differential equation (modular forms are holomorphic functions = satisfies the Cauchy–Riemann equation).

We will eventually connect these pictures and see that they all talk about the same thing.

Let me give you a first definition of automorphic forms, for GL_n over L. The convention is that when you talk about automorphic forms/representations of GL_n over a number field K, you say they are for $\mathrm{GL}_n(\mathbb{A}_L)$.

Definition 17.1 (Adelic automorphic forms for $\mathrm{GL}_n(\mathbb{A}_L)$)**.** An **adelic automorphic form** for $\mathrm{GL}_n(\mathbb{A}_L)$ is a function

$$f : \mathrm{GL}_n(\mathbb{A}_L) \to \mathbb{C},$$

such that

(1) it is **left**-$\mathrm{GL}_n(L)$-**invariant**,

(2) it is **smooth**,

(3) it has a **central character** $\omega : L^\times \backslash \mathbb{A}_L^\times \to S^1$,

(4) it is K^∞-**finite for all open compact subgroups** $K^\infty \leq \mathrm{GL}_n(\mathbb{A}_L^\infty)$,

(5) it is K_∞-**finite**,

(6) it is $Z(\mathfrak{gl}_n(L_\infty))$-**finite**,

(7) and it has **moderate growth**.

We let $\mathcal{A}(\mathrm{GL}_n(\mathbb{A}_L), \omega)$ be the vector space of adelic automorphic forms for $\mathrm{GL}_n(\mathbb{A}_L)$ with a central character ω.

It has a lot of terms. Let me explain them, where some of them I will be intentionally hand-wavy as it would take too much time to explain it properly.

(1) (Left-$\mathrm{GL}_n(L)$-invariance) This just means that the function f is invariant under multiplying an element of $\mathrm{GL}_n(L)$ on the left, i.e. $f(gx) = f(x)$ for any $x \in \mathrm{GL}_n(\mathbb{A}_L)$ and $g \in \mathrm{GL}_n(L)$ (recall that $L \subset \mathbb{A}_L$, so naturally $\mathrm{GL}_n(L) \subset \mathrm{GL}_n(\mathbb{A}_L)$). Therefore, it is also natural to see f as a function

$$f : \mathrm{GL}_n(L) \backslash \mathrm{GL}_n(\mathbb{A}_L) \to \mathbb{C}.$$

(2) (Smoothness) This is the same "smoothness" (or "niceness" as I called in the lectures) as in Tate's thesis. Namely, over $\mathbb{R}$ or $\mathbb{C}$, this is the same as the usual smoothness in analysis, whereas over p-adic fields, this is "locally constant."

More concretely, this means as follows. Let $x \in \mathrm{GL}_n(\mathbb{A}_L)$. Let v be a place of L. Then $L_v \hookrightarrow \mathbb{A}_L$ gives a natural embedding $\mathrm{GL}_n(L_v) \hookrightarrow \mathrm{GL}_n(\mathbb{A}_L)$. Then f being smooth means that the "orbit map"

$$\mathrm{GL}_n(L_v) \to \mathbb{C}, \quad g \mapsto f(xg),$$

is smooth in the above sense. More precisely, if $L_v = \mathbb{R}$ or $\mathbb{C}$, then this means the corresponding map $\mathrm{GL}_n(\mathbb{R}) \to \mathbb{C}$ or $\mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}$ is a real-analytically smooth map. If L_v is a p-adic field, then there is an open subgroup $\Gamma \leq \mathrm{GL}_n(L_v)$ such that $f(x) = f(xg)$ for $g \in \Gamma$.

(3) (Central character) The group $\mathrm{GL}_n(\mathbb{A}_L)$ has the center given by the diagonal matrices with entries in $\mathbb{A}_L^\times$. Then f having the central character ω means that $f(xg) = \omega(g)f(x)$ for any $g \in L^\times \backslash \mathbb{A}_L^\times$ (seen as the diagonal matrix) and $x \in \mathrm{GL}_n(\mathbb{A}_L)$.

(4) (K^∞-finiteness) Recall first that $\mathbb{A}_L^\infty$ is the space of **finite adeles**, i.e. the adeles where the entries at infinite places are all 1. We want f to behave in a way that you do not need the whole complicated group $\mathrm{GL}_n(\mathbb{A}_L^\infty)$ (the finite adele part of $\mathrm{GL}_n(\mathbb{A}_L)$), but rather its discrete quotient. Note that $\mathrm{GL}_n(\widehat{\mathcal{O}_L})$ is an open (compact) subgroup of $\mathrm{GL}_n(\mathbb{A}_L^\infty)$ where $\widehat{\mathcal{O}_L}$ is the profinite completion of $\mathcal{O}_L$. Thus this condition really means that the vector space spanned by the functions $f_g(x) := f(xg)$ for $g \in \mathrm{GL}_n(\widehat{\mathcal{O}_L})$ is finite-dimensional.

(5) (K_∞-finiteness) This is a similar condition but at infinite place. An analogue of the "open compact subgroup" is a **maximal connected compact subgroup** (i.e. a connected compact subgroup such that it is maximal among such subgroups) $K_\infty \leq \mathrm{GL}_n(L_\infty)$, where $L_\infty = L \otimes_{\mathbb{Q}} \mathbb{R} = \prod_{v \text{ infinite places of } L} L_v$. Note that $\mathrm{GL}_n(L_\infty)$ is a real-analytic manifold which is also a group, which is often called a **Lie group**. It is a theorem (called the **Cartan–Iwasawa–Malcev theorem**) that **any maximal connected compact subgroup of a connected Lie group is unique up to conjugation**.

In practice, in our case, $\mathrm{GL}_n(L_\infty)$ is a product of $\mathrm{GL}_n(\mathbb{R})$'s and $\mathrm{GL}_n(\mathbb{C})$'s, so we only need to know what maximal compact subgroups are for $\mathrm{GL}_n(\mathbb{R})$ and $\mathrm{GL}_n(\mathbb{C})$.

Exercise 17.1. Show that the **special orthogonal group** $\mathrm{SO}(n) \subset \mathrm{GL}_n(\mathbb{R})$ (i.e. the group of $n \times n$ orthogonal matrices with determinant 1) is a maximal connected compact subgroup, i.e. $\mathrm{SO}(n)$ is compact and connected and that there is no bigger compact and connected group containing $\mathrm{SO}(n)$ inside $\mathrm{GL}_n(\mathbb{R})$.

Exercise 17.2. Show that the **unitary group** $\mathrm{U}(n) \subset \mathrm{GL}_n(\mathbb{C})$ (i.e. the group of $n \times n$ unitary matrices) is a maximal connected compact subgroup, i.e. $\mathrm{U}(n)$ is compact and connected and that there is no bigger compact and connected group containing $\mathrm{U}(n)$ inside $\mathrm{GL}_n(\mathbb{C})$.

As per the above Exercises, we can take K_∞ to be a product of $\mathrm{SO}(n)$'s and $\mathrm{U}(n)$'s accordingly. Then, the condition of K_∞-finiteness is similar: the vector space spanned by the functions $f_g(x) := f(xg)$for $g \in K_\infty$ is finite-dimensional.

(6) ($Z(\mathfrak{gl}_n(L_\infty))$-finiteness) This is a bit too involved to explain, so we have to be hand-wavy. This is another condition at infinite place which basically says that f satisfies a certain explicit partial differential equation.

(7) (Moderate growth) This is also a bit too involved to explain; this is a similar condition to "meromorphic at cusps" condition for modular forms.

So what do these mean when $n = 1$?

Lemma 17.2. *Let L be a number field and $\omega : L^\times \backslash \mathbb{A}_L^\times \to S^1$ be a unitary Hecke character. Then, an adelic automorphic form $f : \mathrm{GL}_1(\mathbb{A}_L) \to \mathbb{C}$ for $\mathrm{GL}_1(\mathbb{A}_L)$ with central character ω is uniquely of the form*

$$f(x) = c\omega(x),$$

for some fixed $c \in \mathbb{C}$.

Proof. That it should be of the said form is easy because of the central character condition, so $f(x)$ is determined by $f(1)$, i.e. $f(x) = \omega(x)f(1)$. Thus the task is to see whether ω satisfies the said conditions. The left $L^\times$ invariance is obvious, and the smoothness is dealt in the discussion of Tate's thesis. The central character condition is given. The K^∞-finiteness and K_∞-finiteness are also obvious, as any action by such groups will give you a constant multiple of ω, so the vector space spanned by those translates will always be one-dimensional.

For the last two conditions, as the conditions were given hand-wavily, we can only justify them hand-wavily. We know exactly the unitary characters of $\mathbb{R}^\times$ and $\mathbb{C}^\times$: for $\mathbb{R}^\times$, the unitary characters are either $x \mapsto |x|^{it}$ for some $t \in \mathbb{R}$ or $x \mapsto \mathrm{sgn}(x)|x|^{it}$ for some $t \in \mathbb{R}$; for $\mathbb{C}^\times$, the unitary characters are of the form $z \mapsto \left(\frac{z}{\bar{z}}\right)^n |z|^{it}$ for some $n \in \mathbb{Z}$ and $t \in \mathbb{R}$. Now it is believable that these functions satisfy certain differential equations (note that for $\mathbb{C}$, you see $z = x + iy$ and ask for a differential equation in terms of x and y). □

We can abstractly define what an automorphic representation is.

Definition 17.3 (Automorphic representation)**.** Recall that $\mathcal{A}(\mathrm{GL}_n(\mathbb{A}_L),\omega)$ is the space of adelic automorphic forms with a central character ω. This has the right action of $\mathrm{GL}_n(\mathbb{A}_L)$ (i.e. for $g \in \mathrm{GL}_n(\mathbb{A}_L)$ and $f \in \mathcal{A}(\mathrm{GL}_n(\mathbb{A}_L),\omega)$, $(g \cdot f)(x) := f(xg)$ is also an adelic automorphic form). An **automorphic representation** is an irreducible $\mathrm{GL}_n(\mathbb{A}_L)$-representation which arises as a subquotient (i.e. a quotient representation of a subrepresentation, or a Jordan–Holder constituent) of $\mathcal{A}(\mathrm{GL}_n(\mathbb{A}_L),\omega)$.

We are actually slightly lying here, because we need some more language to properly deal with the infinite places[22], but the main concept is there.

The reason why we want to consider automorphic **representations** instead of a single automorphic **form** is because of the following theorem.

Theorem 17.4 (Flath)**.** *Every automorphic representation π of $\mathrm{GL}_n(\mathbb{A}_L)$ is of the form*

$$\text{“}\pi = \bigotimes_{v \textit{ places of } L} \pi_v \text{”},$$

where π_v is an irreducible smooth admissible representation of $\mathrm{GL}_n(L_v)$.

We've put a quotation mark as some care is required; $\mathrm{GL}_n(\mathbb{A}_L)$ is not a literal product of $\mathrm{GL}_n(L_v)$'s[23].

We can now state a rough idea of what a **global Langlands correspondence for** $\mathrm{GL}_n(\mathbb{A}_L)$ should look like.

Conjecture 17.5 (Global Langlands correspondence for $\mathrm{GL}_n(\mathbb{A}_L)$, weak form)**.** *Let L be a number field, and let ℓ be a prime number. Let $\pi = \bigotimes_v \pi_v$ be an automorphic representation of $\mathrm{GL}_n(\mathbb{A}_L)$ that is also “nice at infinite places” (we are constantly hand-waving things at infinite places). Then, there exists a continuous homomorphism $\rho_\pi : \mathrm{Gal}(\overline{L}/L) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ such that, for any place v of L, π_v corresponds to the restriction of ρ_π to the Weil group W_{L_v} inside the decomposition group at v, seen as $\mathrm{Gal}(\overline{L_v}/L_v)$.*

A mnemonic is that

$$\pi = \bigotimes_v \pi_v \quad \leftrightarrow \quad \rho_\pi|_{\mathrm{Gal}(\overline{L_v}/L_v)} = \rho_{\pi_v}.$$

There are more compatibilities that this correspondence should satisfy, and also a conjectural description of what the image of this correspondence should be (i.e. characterization of continuous homomorphisms $\mathrm{Gal}(\overline{L}/L) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ that should arise as ρ_π for some π), but these are beyond our scope.

[22] Instead of asking for a $\mathrm{GL}_n(\mathbb{A}_L)$-representation, which is the same as the data of a $\mathrm{GL}_n(\mathbb{A}_L^\infty)$-representation and a $\mathrm{GL}_n(L_\infty)$-representation with commuting actions, we should really ask for the data of a $\mathrm{GL}_n(\mathbb{A}_L^\infty)$-representation and a $(\mathfrak{gl}_n(L), K_\infty)$-**module** with commuting actions. Whenever we talk about representations at infinite places, we will be constantly lying about this issue from now on.

[23] For all but finitely many v's, π_v has a specific 1-dimensional line, and one can take it as a “basepoint” of taking infinite products in a “restricted way”.

17.2. **Symmetric spaces.** We will rather try to explain why modular forms can be interpreted as automorphic forms for $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$. The key is that there is a different version of the definition of automorphic forms, called the **classical automorphic forms**, which is more evidently tied with the geometry of certain manifolds with a group action. To have an aesthetically satisfying complete picture, we focus on the case when the number field L has narrow class number 1 (e.g. $L = \mathbb{Q}$)[24].

Assumption. Let $\mathfrak{m}_\infty$ be the modulus of all real places of L. Then, $\mathrm{Cl}^{\mathfrak{m}_\infty}(L) = 1$.

Then, the "manifold" that we work with is the quotient[25]

$$X_{\mathrm{GL}_n(L_\infty)^0} := \mathrm{GL}_n(L_\infty)^0 / \mathbb{R}_{>0} K_\infty,$$

which is called the **symmetric space** for the connected Lie group $\mathrm{GL}_n(L_\infty)^{0}$[26], which is the connected component of the identity $1 \in \mathrm{GL}_n(L_\infty)$. Here, $K_\infty \subset \mathrm{GL}_n(L_\infty)^0$ is the maximal connected compact subgroup, and $\mathbb{R}_{>0} \subset \mathrm{GL}_n(L_\infty)^0$ corresponds to the diagonal matrices whose entries are in $\mathbb{R}_{>0}$, where $\mathbb{R}_{>0} \subset \mathbb{R}$ embeds canonically into L_∞ via tensoring $\mathbb{Q} \hookrightarrow L$ with $\otimes_{\mathbb{Q}} \mathbb{R}$. More precisely, there exists a Riemannian manifold $X_{\mathrm{GL}_n(L_\infty)^0}$ with an isometric action by $\mathrm{GL}_n(L_\infty)^0$ (on the left, by our convention).

Example 17.6.

(1) If $n = 1$, then $\mathrm{GL}_1(L_\infty)^0 = (\mathbb{R}_{>0})^r \times (\mathbb{C}^\times)^s$ where r and s are the numbers of real and (pairs of) complex embeddings of L, respectively. Then, K_∞ under this decomposition can be taken to be $\{1\}^r \times (S^1)^s$. Therefore, $X_{\mathrm{GL}_1(L_\infty)^0} \cong \mathbb{R}_{>0}^{r+s-1}$ (we see $r + s - 1$ again!!!) where $\mathrm{GL}_1(L_\infty)^0$ acts by real/complex norms.

(2) If $n = 2$ and $L = \mathbb{Q}$, then the associated symmetric space is

$$\mathrm{GL}_2(\mathbb{R})^0 / \mathbb{R}_{>0} \,\mathrm{SO}(2).$$

What is this? It is easy to see that this is the same as $\mathrm{SL}_2(\mathbb{R}) / \mathrm{SO}(2)$.

Exercise 17.3. Consider the usual action of $\mathrm{SL}_2(\mathbb{R})$ on the upper half plane $\mathbb{H}$. Show that the stabilizer of $i \in \mathbb{H}$ is precisely $\mathrm{SO}(2)$, the special orthogonal group (i.e. 2×2 orthogonal matrices with determinant 1).

Thus, $X_{\mathrm{GL}_2(\mathbb{R})^0}$ is the **upper half plane** $\mathbb{H}$.

Now we can define the **classical automorphic forms**, firstly as functions on $\mathrm{GL}_n(L_\infty)^0$.

Definition 17.7 (Classical automorphic forms, version 1)**.** Let $\Gamma \leq \mathrm{GL}_n(L_\infty)^0$ be a discrete subgroup. Let $\omega : L_\infty^\times \to S^1$ be a unitary character. Then, a **classical automorphic form** with level Γ and central character ω is

[24] In general, you need to consider a finite disjoint union of the picture described below.

[25] We are making the picture simpler by killing all the centers, which is not what people would want to do in practice.

[26] One may try to do this without taking the connected component of the identity. This is possible, at the cost of dealing with manifolds with several connected components. For example, even for $\mathrm{GL}_2(\mathbb{R})$, the symmetric space would then by the union of the lower and the upper half plane.

(1) a smooth (i.e. real analytic) function $f : \mathrm{GL}_n(L_\infty)^0 \to \mathbb{C}$ such that,

(2) $f(\gamma g) = f(g)$ for $\gamma \in \Gamma$,

(3) $f(gz) = \omega(z)f(g)$ for $z \in L_\infty^\times$, seen as the diagonal matrix,

(4) that is K_∞-finite (i.e. the space of functions $f_k(g) := f(gk)$ for $k \in K_\infty$ is finite-dimensional),

(5) $Z(\mathfrak{gl}_n(L_\infty))$-finite (roughly speaking, satisfies certain partial differential equations),

(6) and has moderate growth (roughly speaking, analogous to “meromorphic at cusps”).

To relate this with functions on $X_{\mathrm{GL}_n(L_\infty)^0}$, we need a final ingredient, a **factor of automorphy**. Somehow the above picture seems to be **invariant under Γ-action** but transforms under the action of K_∞. On the other hand, a modular form is a function on $\mathbb{H}$, so it should be **invariant under K_∞-action** but transforms under the action of Γ. This trade-off comes from the following kind of procedure.

Example 17.8. Let $f : \mathbb{H} \to \mathbb{C}$ be a modular form of weight k and level $\mathrm{SL}_2(\mathbb{Z})$. This means that $f(\gamma \cdot z) = (cz+d)^k f(z)$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Using that $\mathrm{GL}_2(\mathbb{R})^0/\mathbb{R}^\times \mathrm{SO}(2) \cong \mathbb{H}$ with $1 \in \mathrm{GL}_2(\mathbb{R})^0$ corresponding to $i \in \mathbb{H}$, we define $\varphi_f : \mathrm{GL}_2(\mathbb{R})^0 \to \mathbb{C}$ as

$$\varphi_f(g) = (\det g)^{k/2}(ci+d)^{-k} f(g \cdot i), \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})^0.$$

Then by the factor $(ci+d)^{-k}$, φ_f is no longer right-$\mathrm{SO}(2)$-invariant, but it is now left-$\mathrm{SL}_2(\mathbb{Z})$-invariant!

The key is coming up with the factor $(cz+d)^k$, which is called a **factor of automorphy**.

Definition 17.9 (Factor of automorphy)**.** A **factor of automorphy** is a function $j : \mathrm{GL}_n(L_\infty)^0 \times X_{\mathrm{GL}_n(L_\infty)^0} \to \mathbb{C}$ such that, for each $\gamma \in \Gamma$, $j(\gamma, \cdot)$ is a smooth function on $X_{\mathrm{GL}_n(L_\infty)^0}$ and the **cocycle condition** holds,

$$j(\gamma\delta, z) = j(\gamma, \delta \cdot z) j(\delta, z).$$

A factor of automorphy corresponds to what happens at the infinite places. I won't go deep into details, but just remark that this is related to the K_∞-finiteness, so in particular associated to a **finite dimensional representation of** K_∞.

Example 17.10. For $n = 2$, $L = \mathbb{Q}$ and $k \in \mathbb{Z}$, for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})^0$ and $z \in \mathbb{H} = X_{\mathrm{GL}_2(\mathbb{R})^0}$, it is easy to check that $j(\gamma, z) := (\det \gamma)^{-k/2}(cz+d)^k$ is a factor of automorphy.

The way that this is related to a finite dimensional representation of K_∞ is as follows. Note that in this case $K_\infty = \mathrm{SO}(2)$, and as a matrix group this is given by the rotation matrices,

$$\mathrm{SO}(2) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbb{R} \right\}.$$

In particular, $\mathrm{SO}(2) \cong S^1$ as topological groups. Now if we apply the same formula for $\gamma \in \mathrm{SO}(2)$ and $z = i$ (the "basepoint" of $\mathbb{H}$), then we get

$$j\left(\begin{pmatrix}\cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{pmatrix}, i\right) = (i\sin\theta + \cos\theta)^k = e^{ik\theta}.$$

This gives rise to a **character** $\mathrm{SO}(2) \to S^1$, so a one-dimensional representation of the circle group $\mathrm{SO}(2) \cong S^1$.

As you might have guessed, there is a way to reverse this procedure, using the so-called **Iwasawa decomposition**. Moreover, as K_∞ in general is not abelian, the correct generality for the factor of automorphy should be a function $j : \Gamma \times X_{\mathrm{GL}_n(L_\infty)^0} \to \mathrm{GL}_N(\mathbb{C})$ for some $N > 0$; the below definition then will give you the so-called **vector-valued automorphic forms**.

Definition 17.11 (Classical automorphic forms, version 2)**.** Let $\Gamma \leq \mathrm{GL}_n(L_\infty)^0$ be a discrete subgroup. Let $\omega : L_\infty^\times \to S^1$ be a unitary charcater that is trivial on $\mathbb{R}_{>0} \subset L_\infty^\times$. Let $j : \mathrm{GL}_n(L_\infty)^0 \times X_{\mathrm{GL}_n(L_\infty)^0} \to \mathbb{C}$ be a factor of automorphy. Then, a **classical automorphic form** with level Γ, central character ω and weight j is

(1) a smooth (i.e. real analytic) function $f : X_{\mathrm{GL}_n(L_\infty)^0} \to \mathbb{C}$ such that,

(2) $f(\gamma x) = j(\gamma, x) f(x)$ for $\gamma \in \Gamma$, $x \in X_{\mathrm{GL}_n(L_\infty)^0}$,

(3) $f(gz) = \omega(z) f(g)$ for $z \in L_\infty^\times$, seen as the diagonal matrix,

(4) that is $Z(\mathfrak{g}_n(L_\infty))$-finite (roughtly speaking, satisfies certain partial differential equations),

(5) and has moderate growth (roughly speaking, analogous to "meromorphic at cusps").

Now the procedure is clear: given a classical automorphic form $f : X_{\mathrm{GL}_n(L_\infty)^0} \to \mathbb{C}$ in the "version 2" sense, we obtain a classical automorphic form $\varphi_f : \mathrm{GL}_n(L_\infty)^0 \to \mathbb{C}$ in the "version 1" sense by setting

$$\varphi_f(g) = j(g, 1)^{-1} f(1),$$

where $1 \in X_{\mathrm{GL}_n(L_\infty)^0}$ is the point whose stabilizer is $K_\infty \leq \mathrm{GL}_n(L_\infty)^0$.

To obtain an adelic automorphic form from a classical automorphic form in the "version 1" sense, the key is the following.

Theorem 17.12 (Strong approximation)**.** *Any element $g \in \mathrm{GL}_n(\mathbb{A}_L)$ can be written as $g = g_1 g_2 g_3$, where $g_1 \in \mathrm{GL}_n(L)$, $g_2 \in \mathrm{GL}_n(L_\infty)^0$, and $g_3 \in \mathrm{GL}_n(\widehat{\mathcal{O}_L})$. In short,*

$$\mathrm{GL}_n(\mathbb{A}_L) = \mathrm{GL}_n(L)\,\mathrm{GL}_n(L_\infty)^0\,\mathrm{GL}_n(\widehat{\mathcal{O}_L}).$$

Example 17.13. In the case of $n = 1$, this is precisely the statement that the narrow class group $\mathrm{Cl}^{\mathfrak{m}_\infty}(L) = 1$. In general, the difference between the left and the right hand sides is precisely the narrow class group. Alternatively, one can use SL_n instead of GL_n and do not worry about this issue (although there are other more subtle complications when you use SL_n instead of GL_n).

Corollary 17.14. *Let $K^\infty \leq \mathrm{GL}_n(\widehat{\mathcal{O}_L})$ be a finite index subgroup. Let $\Gamma_{K^\infty} := \mathrm{GL}_n(\mathcal{O}_L)^0 \cap K^\infty$, where $\mathrm{GL}_n(\mathcal{O}_L)^0 = \mathrm{GL}_n(\mathcal{O}_L) \cap \mathrm{GL}_n(L_\infty)^0$ is the $n \times n$ invertible matrices with entries in $\mathcal{O}_L$ whose determinant is positive under every real embedding of L. Then, the natural map*

$$\Gamma_{K^\infty} \backslash \mathrm{GL}_n(L_\infty)^0 \to \mathrm{GL}_n(L) \backslash \mathrm{GL}_n(\mathbb{A}_L)/K^\infty,$$

is a bijection.

Example 17.15. If $L = \mathbb{Q}$ and $n = 2$, then $\mathrm{GL}_2(\mathbb{Z})^0 = \mathrm{SL}_2(\mathbb{Z})$ because the determinant is a unit in $\mathbb{Z}$ which is positive in every real embedding, so must be 1.

By this Corollary, we see that a classical automorphic form with level Γ_{K^∞} gives rise to an adelic automorphic form (which is right-K^∞-invariant).

17.3. **When does an automorphic form generate an automorphic representation?** We now know that modular forms give rise to an adelic automorphic form.

$$\{\text{Modular forms}\} \to \{\text{Automorphic forms for } \mathrm{GL}_2(\mathbb{A}_\mathbb{Q})\}.$$

The question is: when does an adelic automorphic form give you an automorphic representation? You want to produce an irreducible representation, and for that, what is crucial is to see the representation as a module over the (local) Hecke algebras. The action of the (local) Hecke algebras can be encoded in the language of classical automorphic forms in terms of **Hecke operators**, and one sufficient (and necessary for modular forms) condition for a modular form to give rise to an automorphic representation is that it is an eigenvector for the Hecke operators, called a **Hecke eigenform** (I won't be explaining more about this; you may find a lot of references about what a Hecke operator for a modular form is).

$$\{\text{Hecke eigenforms}\} \to \{\text{Automorphic representations of } \mathrm{GL}_2(\mathbb{A}_\mathbb{Q})\}.$$

Given an automorphic representation, there are many automorphic forms contained in it as a vector. Correspondingly, there are many Hecke eigenforms that give rise to the same automorphic representation of $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$. One such occasion is that, given a Hecke eigenform $f : \mathbb{H} \to \mathbb{C}$, for $N > 1$, $f_N : \mathbb{H} \to \mathbb{C}$ given by $f_N(z) := f(Nz)$ is also a Hecke eigenform, and it turns out that f and f_N are two different vectors of the same automorphic representation. However, given an automorphic representation, there is a **unique** modular form (up to scaling by a nonzero complex number) which cannot be written as f_N for $N > 1$, and such a modular form is called **new**. Thus if we restrict to Hecke eigenforms that are new, and if we ignore multiplying the modular form by a nonzero scalar, this correspondence becomes injective.

$$\{\text{Hecke eigenforms that are new}\}/\mathbb{C}^\times \hookrightarrow \{\text{Automorphic representations of } \mathrm{GL}_2(\mathbb{A}_\mathbb{Q})\}.$$

18. Galois representations

A weak form of the global Langlands correspondence for $\mathrm{GL}_n(\mathbb{A}_L)$ attaches a Galois representation (i.e. a continuous homomorphism $\mathrm{Gal}(\overline{L}/L) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$) to an automorphic representation of $\mathrm{GL}_n(\mathbb{A}_L)$. Specifying what representations should appear as such is more delicate, especially regarding the data at archimedean places and at ℓ-adic places. What I will say is that for all but finitely many places v of L, the inertia group $I_v \subset D_v \subset \mathrm{Gal}(\overline{L}/L)$ is sent to the identity element, i.e. the representation is **unramified** at v. This already is a very big restriction.

18.1. **Shimura–Taniyama conjecture and Fermat's Last Theorem.** As now we know that certain modular forms give rise to automorphic representations of $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$, one may ask if there is a more down-to-earth expectation on what Galois representations arise as those corresponding to modular forms. In fact, there is a precise conjecture, which is now almost known (called the **Fontaine–Mazur conjecture**). A particular case of this, called the **Shimura–Taniyama conjecture**, is a crucial ingredient in the proof of Fermat's Last Theorem.

Theorem 18.1 (Shimura–Taniyama conjecture, Wiles, Taylor–Wiles, Breuil–Conrad–Diamond–Taylor)**.** *There is a bijective correspondence*

$$\{\textit{Cuspidal new normalized Hecke eigenforms of weight } 2 \textit{ with rational } q\textit{-expansion coefficients}\}$$

$$\leftrightarrow$$

$$\{\textit{Elliptic curves (=lattices) over } \mathbb{Q}\}/\textit{isogenies.}$$

Some explanation of the words.

- **Cuspidal**$\cdots$: This means that the constant term of the q-expansion is 0 (to exclude the likes of Eisenstein series).
- $\cdots$**normalized**$\cdots$: This means that the q-term of the q-expansion is 1 (to eliminate the effect of scaling by a nonzero scalar).
- $\cdots$**with rational q-expansion coefficients**: This means that the q-expansion has coefficients in $\mathbb{Q}$.
- **Elliptic curves over $\mathbb{Q}$**: These are **lattices** whose j-invariants are in $\mathbb{Q}$.

So what is the correspondence? Objects in two sides match when they **give rise to the same Galois representation**. We already mentioned that a new Hecke eigenform gives an automorphic representation and thus a Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_\ell)$; this part of global Langlands correspondence is already known long before. The way that a Galois representation is associated with an elliptic curve over $\mathbb{Q}$ is as follows.[27]

Step 1 Up to isomorphism, the Weierstrass $\wp$-function associate to an elliptic curve satisfies the differential equation $(\wp'(z))^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$ for $g_2, g_3 \in \mathbb{Q}$.

Step 2 Consider the set $T = \{x, y \in \overline{\mathbb{Q}} \ : \ y^2 = 4x^3 - g_2x - g_3\}$. As $g_2, g_3 \in \mathbb{Q}$, the set T has an action by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (acting on x, y). Furthermore, the fact that this arises from an elliptic curve (=lattice) implies that there is a natural abelian group structure on T. This abelian group structure is compatible with the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (i.e. T is a $\mathbb{Z}[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module).

Step 3 For $N > 1$, let $T[\ell^N] := \{t \in T \ : \ \ell^N t = 0\}$, which is a $(\mathbb{Z}/\ell^N\mathbb{Z})[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module. It turns out that $T[\ell^N]$ as a $\mathbb{Z}/\ell^N\mathbb{Z}$-module is free of rank 2 (i.e. as an abelian group, $T[\ell^N] \cong (\mathbb{Z}/\ell^N\mathbb{Z})^{\oplus 2}$). Thus, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ gives a continuous homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/\ell^N\mathbb{Z})$.

[27] The actual Galois representation matching those arising from modular forms should be

Step 4 Take the inverse limit $N \to \infty$ and obtain $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$. As $\mathbb{Z}_\ell \subset \mathbb{Q}_\ell \subset \overline{\mathbb{Q}}_\ell$, this gives a Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$.

The crucial ingredient of the above theorem is the so-called **modularity lifting theorem**, which we will explain later.

Theorem 18.2 (Fermat's Last Theorem). *Let $p > 2$ be a prime number. Then, there is no $a, b, c \in \mathbb{Z}$ with $abc \neq 0$ such that $a^p + b^p = c^p$.*

The proof goes like: if Fermat's Last Theorem is false, then a nontrivial solution will give you a very peculiar elliptic curve over $\mathbb{Q}$, which, under the Shimura–Taniyama conjecture (which is a theorem), corresponds to a weight 2 cusp form of level 2, which does not exist.

18.2. **Galois deformation theory.** One direction of Shimura–Taniyama conjecture has been known for a while, namely constructing an elliptic curve from a modular form. Although this is also quite nontrivial, it is not too crazy (you know exactly where you should look for such elliptic curves, using modular curves). The difficult direction is that **every elliptic curve** over $\mathbb{Q}$ arises in this fashion. In other words, we often say an elliptic curve over $\mathbb{Q}$ is **modular** if it arises from a certain modular form, and the Shimura–Taniyama conjecture says that every elliptic curve over $\mathbb{Q}$ is modular.

The idea of the proof for the conjecture is to use congruences. Namely, we can talk about when two elliptic curves E_1, E_2 over $\mathbb{Q}$ are **congruent modulo** p, for a prime p. Then, the proof strategy breaks down to two steps.

(1) (Modularity lifting theorem) Show that, if E is modular, then any elliptic curve congruent to E mod p is modular.

(2) For any given E, find a small prime p and a particularly simple elliptic curve E' congruent to E mod p such that you already know E' is modular.

It turns out that in (2), either $p = 3$ or $p = 5$ works in every case ($p = 2$ is excluded because things break down at 2). Either $p = 3$ or $p = 5$ works in (2) requires the modularity lifting theorem, too (often called the 3-5 **switch**).

19. Modularity lifting theorems

19.1. **Basic proof strategy of $R = \mathbb{T}$ theorems.** Taylor–Wiles method. Minimal level, non-minimal level.

19.2. **Finding Taylor–Wiles primes.**

19.3. **The case of $\mathrm{GL}_1(\mathbb{A}_L)$.**

References

[ANT] Gyujin Oh, Notes for Algebraic Number Theory, GU4043, Spring 2024.

[AT] Emil Artin, John Tate, Class Field Theory.

[BCG] Nicholas Bergeron, Pierre Charollois, Luis E. García, *Elliptic units for complex cubic fields.* arXiv:2311.04110.

[CF] *Algebraic Number Theory*, Proceedings of an instructional conference organized by the London Mathematical Society. Edited by J. W. S. Cassels and A. Fröhlich.

[Cox] David A. Cox, Prime of the form $x^2 + ny^2$.

[Deu] Max Deuring, *Die Klassenkörper der komplexen Multiplikation.*

[GZ] Benedict Gross, Don Zagier, *On singular moduli.* Crelle's Journal **355** 191-220, 1984.

[Lan] Serge Lang, Elliptic Functions.

[Mil] James Milne, Class Field Theory.

[Neu] Jurgen Neukirch, Algebraic Number Theory.

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

Department of Mathematics, Columbia University, 2990 Broadway, New York, NY 10027
E-mail address: gyujinoh@math.columbia.edu