CLASS FIELD THEORY

YIHANG ZHU

Contents

Date: May 11, 2021.

The main sources for the course are [Mil20], [Ser79], [CF10], [AT09]. Most of the prerequisites which we state without a proof can be found in [Neu99, §I - §II] or [Ser79, §I - §III].

1. Lecture 1, 1/26/2021

1.1. **The main ideas of class field theory, cf.** [Mil20, Introduction]**.** Let K be a global field (e.g., $\mathbb{Q}$) or a local field (e.g., $\mathbb{Q}_p$.) Class field theory is the study of abelian extensions E/K, i.e., (finite or infitnite) Galois extensions whose Galois group is abelian. The main point is that one is able to understand the structure and even classify these extensions in terms of an invariant of K itself. In the global case, this invariant is the *idele class group*

$$C_K = \mathbb{A}_K^\times / K^\times.$$

In the local case, this invariant is the multiplicative group

$$C_K = K^\times.$$

In both cases, C_K contains "all the information" about abelian extensions of K.

But why do we care?

1.1.1. *Power reciprocity.* For a prime p and an integer n not divisible by p, recall the Legendre symbol

$$(n/p) = \begin{cases} 1, & \text{if } n \text{ is a square mod } p, \\ -1, & \text{otherwise.} \end{cases}$$

Recall the quadratic reciprocity law:

$$(p/q)(q/p) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

for distinct odd primes p, q, and

$$(-1/p) = (-1)^{\frac{p-1}{2}}, \quad (2/p) = (-1)^{\frac{p^2-1}{8}}.$$

One can deduce from global CFT *power reciprocity laws* for powers greater than 2. These cannot be stated as neatly, but for powers $3, 4$ one can obtain a reasonably concrete statement. For example, one can use cubic reciprocity to quickly compute that 2 and 7 are not cubic powers modulo 61.

The more important point is that CFT puts quadratic reciprocity into a greater context. It reveals the deep link between quadratic reciprocity and many other number theoretic phenomena.

1.1.2. *A classically minded example.* As early as Fermat's time, one was interested in problems of the followg form: For a fixed integer n, find a criterion for a prime p to be expressible as

$$p = x^2 + ny^2, \quad x, y \in \mathbb{Z}.$$

For example if $n = 1$, then we know p is of the form $x^2 + y^2$ if and only if $p \equiv 1 \mod 4$. In some sense this problem is the starting point of algebraic number theory, as we know whether $p = x^2 + y^2$ is related to the *prime decomposition* of p in the field $\mathbb{Q}(\sqrt{-1})$.

Using CFT, one can obtain a complete solution to this problem. There is a whole book about this [Cox13]. To illustrate, for $n = 14$, we have:

Theorem 1.1.3. *A prime p is of the form $x^2 + 14y^2$ if and only if*

$$(*) \quad (-14/p) = 1, \quad \textit{and } (X^2+1)^2 - 8 \textit{ has a root} \mod p.$$

Here the class field theory of $K = \mathbb{Q}(\sqrt{-14})$ is at play. The condition $p = x^2 + 14y^2$ is equivalent to $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ with $\mathfrak{p}$ a *principal* prime ideal in $\mathcal{O}_K$. The condition $(*)$ is equivalent to that $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ and that $\mathfrak{p}$ splits in a certain finite abelian extension H/K, called the *Hilbert class field* of K. What CFT tells us here is an equivalence between $\mathfrak{p}$ being principal and $\mathfrak{p}$ being split in H. This relationship can be called "reciprocity", and is a recurring theme in CFT. We will soon see that quadratic reciprocity can also be understood in terms of similar philosophy.

1.1.4. *Why "class field"?* Consider a number field K. By a *modulus* of K, we mean a formal finite product

$$\mathfrak{m} = v_1^{e_1} \cdots v_k^{e_k},$$

where v_i are places of K and $e_i \in \mathbb{Z}_{\geq 0}$. This should satisfying the following conditions:

- If v is a complex place, then v does not appear in $\mathfrak{m}$.
- If v is a real place, then the power of v in $\mathfrak{m}$ is 0 or 1.

Given a modulus $\mathfrak{m}$ we define the *ray class group* $\mathrm{Cl}_{\mathfrak{m}}$ as the quotient group of the group of fractional ideals of K coprime to $\mathfrak{m}$ modulo the principal ideals generated by those $x \in K^\times$ satisfying:

- For each real place v appearing in $\mathfrak{m}$, the image of x in $K_v \cong \mathbb{R}$ is positive.
- For each finite place $\mathfrak{p}$ such that $\mathfrak{p}^e$ appears in $\mathfrak{m}$, we have f is coprime with $\mathfrak{p}$ (i.e., $f \in \mathcal{O}_{K,\mathfrak{p}}^\times$), and $f \in 1 + \mathfrak{p}^e\mathcal{O}_{K,\mathfrak{p}}$.

Then $\mathrm{Cl}_{\mathfrak{m}}$ is a finite abelian group. (The finiteness is no longer true for global fields of characteristic > 0.) The usual class group $\mathrm{Cl}(\mathcal{O}_F)$ is a special example, corresponding to $\mathfrak{m} = 1$. Another example is the *narrow class group*, corresponding to $\mathfrak{m} =$ product of all real places. This is the quotient group of all fractional ideals modulo those principal ideals generated $x \in K^\times$ such that $v(x) > 0$ for all real places v, i.e., the *totally positive* $x \in K^\times$.

For the given modulus $\mathfrak{m}$, CFT implies the existence of a *ray class field*

$$K_{\mathfrak{m}}/K.$$

This is the unique (!) finite abelian extension such that whether a prime $\mathfrak{p}$ of K splits in $K_{\mathfrak{m}}$ is equivalent to whether $\mathfrak{p}$ is trivial in $\mathrm{Cl}_{\mathfrak{m}}$, with finitely many exceptions of $\mathfrak{p}$. (The uniqueness is still true if we replace "abelian" by "Galois".) In principle, one can work out a polynomial $f(X) \in \mathcal{O}_K[X]$ such that a prime $\mathfrak{p}$ of K splits in $K_{\mathfrak{m}}$ if and only if $f(X) \mod \mathfrak{p}$ splits into linear factors in $(\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p})[X]$, with finitely many exceptions. Thus we have obtained a criterion similar to condition (*) in Theorem 1.1.3 for $\mathfrak{p}$ to be trivial in $\mathrm{Cl}_{\mathfrak{m}}$. The point is that for each $\mathfrak{m}$, there exists such a criterion.

We have a canonical isomorphism

$$\Psi : \mathrm{Cl}_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Gal}(K_{\mathfrak{m}}/K),$$

called the *Artin map.* Any $\mathfrak{p}$ coprime to $\mathfrak{m}$ is unramified in $K_{\mathfrak{m}}$, and

$$\Psi(\mathfrak{p}) = (\mathfrak{p}, K_{\mathfrak{m}}/K).$$

Here $(\mathfrak{p}, K_{\mathfrak{m}}/K)$ is the arithmetic Frobenius.[1] Clearly the above formula uniquely characterizes Ψ since the group $\mathrm{Cl}_{\mathfrak{m}}$ is generated by those $\mathfrak{p}$ that are coprime to $\mathfrak{m}$. But it is a deep statement in CFT that this formula defines a map on $\mathrm{Cl}_{\mathfrak{m}}$. In other words, if (x) is a principal ideal that is trivial in $\mathrm{Cl}_{\mathfrak{m}}$, and if we have the factorization $(x) = \prod \mathfrak{q}_i^{n_i}$, then we have

$$\prod (\mathfrak{q}_i, K_{\mathfrak{m}}/K)^{n_i} = 1$$

in $\mathrm{Gal}(K_{\mathfrak{m}}/K)$. This statement is sometimes called *Artin Reciprocity.*

Recall: Let E/K be a finite Galois extension of global fields, and let $\mathfrak{p}$ be a prime of K unramified in E. For each prime $\mathfrak{P}$ of E over $\mathfrak{p}$ we have a well-defined *arithmetic Frobenius element* $\sigma = (\mathfrak{P}, E/K) \in \mathrm{Gal}(E/K)$. This is characterized by the condition that σ stabilizes $\mathfrak{P}$, and σ acts on the residue field $k(\mathfrak{P}) = \mathcal{O}_E/\mathfrak{P}$ by the Frobenius $x \mapsto x^q$, where $q = |k(\mathfrak{p})| = |\mathcal{O}_K/\mathfrak{p}|$. When $\mathfrak{P}$ runs through the primes over $\mathfrak{p}$, the elements $(\mathfrak{P}, E/K)$ form a conjugacy class in $\mathrm{Gal}(E/K)$, denoted by $(\mathfrak{p}, E/K)$, and called the Frobenius conjugacy class of $\mathfrak{p}$. We have $(\mathfrak{p}, E/K) = \{1\}$ if and only if $\mathfrak{p}$ splits in E. More generally, if the elements of $(\mathfrak{p}, E/K)$ have order f in $\mathrm{Gal}(E/K)$, then $\mathfrak{p}$ factorizes into $[E : K]/f$ many distinct primes, with each residue degree being f. If $\mathrm{Gal}(E/K)$ is abelian, then $(\mathfrak{p}, E/K)$ reduces to a single element.

Remark 1.1.5. In the special case $\mathfrak{m} = 1$, the ray class group $\mathrm{Cl}_{\mathfrak{m}}$ is the usual class group, and the ray class field $K_{\mathfrak{m}}$ is the so-called *Hilbert class field* H. It is maximal finite abelian extension of K in which all places (including archimedean ones) are unramified. For any prime $\mathfrak{p}$ of K, we have $\mathfrak{p}$ splits in H if and only if $\mathfrak{p}$ is principal.

We have a "generalized Kronecker–Weber Theorem"[2], stating that every finite abelian extension E/K is contained in $K_{\mathfrak{m}}$ for some sufficiently large $\mathfrak{m}$. In this way we obtain a complete classification of abelian extensions, as well as understand the Galois groups and how primes factorize.

The theory sketched above is the so-called ideal-theoretic formulation of global CFT. The modern formulation using *ideles* is cleaner, and provides more insight on how the theory is functorial in K.

2. Lecture 2, 1/28/2021

2.1. **Applications of CFT.**

[1] Note that Ψ is said to have the arithmetic normalization. The negative of Ψ, which sends $\mathfrak{p}$ to the geometric Frobenius $(\mathfrak{p}, E/K)^{-1}$, is said to have the geometric normalizatoin.

[2] The original Kronecker–Weber Theorem is just for $K = \mathbb{Q}$

2.1.1. *Chebotarev Density Theorem.* Let E/K be a finite Galois extension of number fields, not necessarily abelian. Let $G = \mathrm{Gal}(E/K)$. For each prime $\mathfrak{p}$ of K that is unramified in E (which is true with only finitely many exceptions), $\mathfrak{p}$ determines a conjugacy class $(\mathfrak{p}, E/K)$ in G.

One of the classical applications of CFT is the following:

Theorem 2.1.2 (Chebotarev Density Theorem)**.** [3] *Let E/K be a finite Galois extension of number fields. Let C be a conjugacy class in $G = \mathrm{Gal}(E/K)$. The set of primes $\mathfrak{p}$ of K such that $(\mathfrak{p}, E/K) = C$ has density $|C| / |G|$ among all primes of K. In particular, this set is infinite.*

One consequence is that there are always infinitely many primes of K that split in E (corresponding to $C = \{1\}$), and also infinitely many primes that do not split in E. Another classical consequence is Dirichlet's theorem, stating that there are infinitely many prime numbers in the arithmetic progression $a+bn, n \in \mathbb{Z}$, provided that $(a, b) = 1$. See Corollary 3.1.3 below.

2.1.3. *Other applications.* There are many other applications that we do not have the time and space to survey. These include Artin L-functions, Grunwald–Wang Theorem (see [AT09, Chapter X]), and local-global principle for quadratic forms (a non-degenerate quadratic form over a number field K represents 0 if and only if its base change to K_v represents zero for each place v), just to list a few. We also mention that CFT is the GL_1-case of the Langlands program, so it is the starting point of a long long journey...

2.2. **CFT for $\mathbb{Q}$.**

2.2.1. *Review of cyclotomic extensions.* Let K be a general field. Let m be a positive integer such that $m \neq 0$ in K. Let μ_m be the group of the m-th roots of unity in $\bar{K}$, i.e., the m distinct roots of $X^m - 1$. Then μ_m is a cyclic group of order m, and its generators are called *primitive* m-th roots of unity. We often fix one primitive m-th root of unity, denoted by ζ_m. The field $K(\mu_m) = K(\zeta_m)$ is the splitting field of $X^m - 1$ over K, so the extension $K(\zeta_m)/K$ is finite Galois. This is called the m-th cyclotomic extension.

There is a natural injection

$$\alpha : \mathrm{Gal}(K(\zeta_m)/K) \longrightarrow \mathrm{Aut}(\mu_m) \cong (\mathbb{Z}/m\mathbb{Z})^\times.$$

Namely, if $\alpha(\sigma)$ is characterized by $\sigma(\zeta_m) = \zeta_m^{\alpha(\sigma)}$. In particular, $K(\zeta_m)/K$ is abelian and its degree divides $\phi(m) := |(\mathbb{Z}/m\mathbb{Z})^\times|$.

The cyclotomic extensions are closely related to *cyclotomic polynomials.* For each positive integer m, we define

$$\Phi_m(X) = \prod_{\omega} (X - \omega),$$

where ω runs through the primitive m-th roots of unity (say in $\mathbb{C}$). We have the recursive relations by

$$\Phi_1(X) = X - 1, \quad \Phi_m(X) = \frac{X^m - 1}{\prod_{d|m, 0<d<m} \Phi_d(X)}.$$

In particular $\Phi_m(X) \in \mathbb{Z}[X]$.

[3] This is also true for global function fields.

We can naturally view $\Phi_m(X)$ as a polynomial over K. Then $K(\zeta_m)/K$ is obtained by adjoining to K one root of $\Phi_m(X)$. Note that $\deg \Phi_m(X) = \phi(m)$, so we see that the following conditions are equivalent:

(i) $\alpha : \mathrm{Gal}(K(\zeta_m)/K) \to (\mathbb{Z}/m\mathbb{Z})^\times$ is an isomorphism.
(ii) $[K(\zeta_m) : K] = \phi(m)$.
(iii) $\min(\zeta_m/K) = \Phi(X)$.
(iv) $\Phi(X)$ is irrreducible in $K[X]$.

2.2.2. *Cyclotomic extensions of* $\mathbb{Q}$.

Theorem 2.2.3 (Gauss)**.** *For each $m > 0$, the cyclotomic polynomial $\Phi_m(X)$ is irreducible in $\mathbb{Q}[X]$.*

Exercise 2.2.4. We prove the theorem in steps. Assume Φ_m is not irreducible in $\mathbb{Q}[X]$. Since it is a monic polynomial in $\mathbb{Z}[X]$, it is not irreducible in $\mathbb{Z}[X]$ by Gauss's Lemma. Hence $\Phi_m = fg$, with $f, g \in \mathbb{Z}[X]$, f irreducible, and $\deg f, \deg g \geq 1$.

(i) Suppose ζ is a root of f such that ζ^p is a root of g for some prime p coprime to m. Show that f divides g^p inside $\mathbb{F}_p[X]$.
(ii) Under the above assumption, show that Φ_m has a multiple root, which is a contradiction.
(iii) Use the above results to show that every primitive m-th root of unity is a root of f, finishing the proof.

By the theorem, the injection $\alpha : \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \to (\mathbb{Z}/m\mathbb{Z})^\times$ is an isomorphism. We thus have a canonical isomorphism

$$\Psi = \alpha^{-1} : (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}),$$

where $\bar{a}$ goes to the automorphism

$$\zeta_m \mapsto \zeta_m^a.$$

Note that if $m \equiv 2 \mod 4$, then $\phi(m) = \phi(m/2)$, and hence $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{m/2})$. We shall henceforth assume $m \not\equiv 2 \mod 4$. In this case we have the following facts:

Theorem 2.2.5 (See [Was97] §2)**.** *We have $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$. A prime p ramifies in $\mathbb{Q}(\zeta_m)$ if and only if $p|m$. Moreover, the discriminant of $\mathbb{Q}(\zeta_m)$ is*

$$(-1)^{\phi(m)/2} \frac{m^{\phi(m)}}{\prod_{p|m} p^{\phi(m)/(p-1)}}$$

Recall: Let E/K be a finite extension of number fields. We recall the explicit method to find the factorization of (almost all) primes of K in E. Write $E = K(\theta)$ with $\theta \in \mathcal{O}_E$, which can always be arranged. Consider the ring $\mathcal{O}_K[\theta]$. It is a subring of $\mathcal{O}_E$ such that $\mathcal{O}_K[\theta] \otimes_{\mathbb{Z}} \mathbb{Q} = E$. Such subrings of $\mathcal{O}_E$ are called *orders.* Define the *conductor* of $\mathcal{O}_K[\theta]$ to be

$$\mathfrak{F} = \{a \in \mathcal{O}_E \mid a\mathcal{O}_E \subset \mathcal{O}_K[\theta]\}.$$

It is the largest ideal of $\mathcal{O}_E$ that is contained in $\mathcal{O}_K[\theta]$. When $\mathcal{O}_K[\theta] = \mathcal{O}_E$, $\mathfrak{F} = \mathcal{O}_E$.

Proposition 2.2.6. *Let $\mathfrak{p}$ be a prime of K that is coprime to $\mathfrak{F}$. Let $f \in \mathcal{O}_K[X]$ be the monic minimal polynomial of θ over K. Inside $k(\mathfrak{p})[X] = (\mathcal{O}_K/\mathfrak{p})[X]$, factorize $\bar{f}$ into irreducible polynomials:*

$$\bar{f}(X) = \prod_{i=1}^{g} f_i(X)^{e_i} \in k(\mathfrak{p})[X],$$

where $f_i(X)$ are irreducible polynomials in $k(\mathfrak{p})[X]$. Then the factorization of $\mathfrak{p}$ in E is given by:

$$\mathfrak{p}\mathcal{O}_E = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i},$$

where

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_E + \widetilde{f}_i(\theta)\mathcal{O}_E,$$

with $\widetilde{f}_i \in \mathcal{O}_K[X]$ a lift of f_i. Thus the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$ is e_i. Moreover, the residue extension $k(\mathfrak{P}_i)$ over $k(\mathfrak{p})$ is isomorphic to the simple extension $k(\mathfrak{p})[X]/(f_i(X))$ over $k(\mathfrak{p})$. In particular it has degree $\deg f_i$.

Proof. See [Neu99, Chapter I, Proposition 8.3]. □

Lemma 2.2.7. *For any prime p coprime to m, the map $\Psi : (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ sends p to $(p, \mathbb{Q}(\zeta_m)/\mathbb{Q})$.*

Proof. Write E for $\mathbb{Q}(\zeta_m)$. Let $\mathfrak{P}$ be a prime of E over p. Recall that $(p, E/\mathbb{Q})$ is the unique element of the decomposition group $D_{\mathfrak{P}}(E/\mathbb{Q})$ (i.e., the stabilizer of $\mathfrak{P}$ in $\mathrm{Gal}(E/\mathbb{Q})$) such that $(p, E/\mathbb{Q})$ induces $x \mapsto x^p$ on the residue field $k(\mathfrak{P}) = \mathcal{O}_K/\mathfrak{P}$. We only need to check that $\Psi(p) \in D_{\mathfrak{P}}(E/\mathbb{Q})$, because then it is clear that $\Psi(p)$ induces $x \mapsto x^p$ on $k(\mathfrak{P})$. Let

$$\overline{\Phi}_m = f_1^{e_1} \cdots f_g^{e_g} \in \mathbb{F}_p[X]$$

be the irreducible factorizatoin in $\mathbb{F}_p[X]$. Since

$$\mathcal{O}_E = \mathbb{Z}[\zeta_m] = \mathbb{Z}[X]/(\Phi_m(X)),$$

the prime factorization of $p\mathcal{O}_K$ is given by $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, where $\mathfrak{P}_i = (\widetilde{f}_i(\zeta_m), p)$, for any $\widetilde{f}_i \in \mathbb{Z}[X]$ lifting f_i. (Since we know p is unramified in E, in fact all $e_i = 1$.) Suppose $\Psi(p)(\mathfrak{P}_i) = \mathfrak{P}_j$ for some $i \neq j$. Then

$$\mathfrak{P}_j = (\widetilde{f}_i(\zeta_m^p), p) = (h(\zeta_m), p),$$

where $h(X) = \widetilde{f}_i(X^p) \in \mathbb{Z}[X]$. Since $h \equiv \widetilde{f}_i^p \mod p$, we have

$$\mathfrak{P}_j = (\widetilde{f}_i(\zeta_m)^p, p) \subset \mathfrak{P}_i,$$

a contradiction. We have thus proved that $\Psi(p)$ stabilizes each $\mathfrak{P}_i$ as desired. □

Appendix. Recall of elementary ramification theory

We recall some basic facts from ramification theory. See [Neu99, §I.9] and [Ser79, §I.7] for details.

The global case. Let E/K be a finite separable extension of number fields. Fix a prime $\mathfrak{p}$ of K (i.e., a prime $\mathfrak{p}$ of $\mathcal{O}_K$). We have the factorization

$$\mathfrak{p}\mathcal{O}_E = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i},$$

where $\mathfrak{P}_i$ are distinct primes of E, and $e_i \in \mathbb{Z}_{\geq 1}$. The integer e_i is called the *ramification index* of $\mathfrak{P}_i$ over $\mathfrak{p}$, and we also denote it by $e(\mathfrak{P}_i/\mathfrak{p})$. Define $f_i := [k(\mathfrak{P}_i) : k(\mathfrak{p})]$, called the *residue extension degree.* We also denote it by $f(\mathfrak{P}_i/\mathfrak{p})$. Then we have

$$\sum_{i=1}^{g} e_i f_i = [E : K].$$

From now on, we always assume that E/K is Galois (i.e., separable and normal). Then e_i and f_i are independent of i, i.e., they depend only on $\mathfrak{p}$. Writing e, f for them, we have

$$efg = [E : K].$$

If $e = [E : K]$ (resp. if $f = [E : K]$, resp. if $g = [E : K]$), we say that $\mathfrak{p}$ is *totally ramified* (resp. *inert*, resp. *split*) in E/K.

If $e = 1$, then we say that $\mathfrak{p}$ is *unramified* in E/K. In this case we also say that $\mathfrak{P}_i$ is *unramified over* $\mathfrak{p}$ (for any i). We know that only finitely many primes of K ramify in K. These are precisely the prime divisors of the relative discriminant of E/K (an ideal of $\mathcal{O}_K$). See [Ser79, §III.5] or [Neu99, §III.3].

For each i, we have the *decomposition group* $D_i = D_{\mathfrak{P}_i}(E/K) \subset \mathrm{Gal}(E/K)$, which is defined to be the stabilizer of $\mathfrak{P}_i$ in $\mathrm{Gal}(E/K)$. If $\gamma \in \mathrm{Gal}(E/K)$ maps $\mathfrak{P}_i$ to $\mathfrak{P}_j$, then $\gamma D_i \gamma^{-1} = D_j$. For any i, j, such γ always exists. Hence the D_i's are conjugate inside $\mathrm{Gal}(E/K)$.

The residue extension $k(\mathfrak{P}_i)/k(\mathfrak{p})$ is an extension of finite fields, so $\mathrm{Gal}(k(\mathfrak{P}_i)/k(\mathfrak{p})) \cong \mathbb{Z}/f\mathbb{Z}$, where a generator is given by the Frobenius $x \mapsto x^{|k(\mathfrak{p})|}$. We have a natural surjective homomorphism

$$D_i \longrightarrow \mathrm{Gal}(k(\mathfrak{P}_i)/k(\mathfrak{p})).$$

Define its kernel to be the *inertia group* $I_i = I_{\mathfrak{P}_i}(E/K)$. We have $|D_i| = ef, |I_i| = e$.

Let $Z_i = E^{D_i}$ and $T_i = E^{I_i}$, called the decomposition field and inert field of $\mathfrak{P}_i$ respectively. Thus

$$E \overset{e}{\supset} T_i \overset{f}{\supset} Z_i \overset{g}{\supset} K,$$

wherethe superscripts are the degrees of the extensions. By construction E/Z_i and E/T_i are Galois with Galois groups D_i and I_i. Also, T_i/Z_i is Galois with Galois group $D_i/I_i \cong \mathrm{Gal}(k(\mathfrak{P}_i)/k(\mathfrak{p}))$. Let $\mathfrak{P}_{i,Z}$ be the prime of Z_i below $\mathfrak{P}_i$. Then

$$\mathfrak{P}_{i,Z}\mathcal{O}_E = \mathfrak{P}_i^e,$$

i.e., $\mathfrak{P}_{i,Z}$ does not decompose into distinct primes in E, thus the terminology "decomposition field". Also, $\mathfrak{P}_{i,Z}\mathcal{O}_{T_i}$ is a prime ideal of $\mathcal{O}_{T_i}$, i.e., $\mathfrak{P}_{i,Z}$ is inert in T_i, thus the terminology "inert field". Let $\mathfrak{P}_{i,T} = \mathfrak{P}_{i,Z}\mathcal{O}_{T,i}$. We have $k(\mathfrak{P}_{i,T}) = k(\mathfrak{P}_i)$, and $k(\mathfrak{P}_{i,Z}) = k(\mathfrak{p})$.

In terms of the invariants e, f, we have

$$e(\mathfrak{P}_{i,Z}/\mathfrak{p}) = f(\mathfrak{P}_{i,Z}/\mathfrak{p}) = 1$$
$$e(\mathfrak{P}_{i,T}/\mathfrak{P}_{i,Z}) = 1, f(\mathfrak{P}_{i,T}/\mathfrak{P}_{i,Z}) = f,$$
$$e(\mathfrak{P}_i/\mathfrak{P}_{i,T}) = e, f(\mathfrak{P}_i/\mathfrak{P}_{i,T}) = 1.$$

Note that $\mathfrak{P}_{i,T}$ is totally ramified in the extension E/T_i.

If E/K is abelian, then D_i, I_i, Z_i, T_i are all independent of i, and we omit the subscript i. In this case, $\mathfrak{p}$ decomposes into g distinct primes in Z. Each of them stays inert and unramified in T/Z. Each of the resulting primes in T is totally ramified inside E/T. The extension T/K is the largest subextension of E/K in which $\mathfrak{p}$ is unramified.

Finally, we remark that all the above essentially also works with number fields replaced by global function fields, which means finite separable extensions of $\mathbb{F}_q(t)$. The only modification needed is that prime ideals of $\mathcal{O}_K$ and $\mathcal{O}_E$ have to be replaced by *places* of K and E, i.e., equivalence classes of absolute values. Here two absolute values on a field are called equivalent if they differ by a positive real power. Instead of looking at the decomposition of $\mathfrak{p}\mathcal{O}_E$ into primes of $\mathcal{O}_E$, we look at how a place of K extends to different places of E. See [Neu99, §II] for details.

The local case. Recall that a non-archimedean local field is a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_q((t))$. Let E/K be a finite Galois extension of non-archimedean local fields. (In the archimedean case, the only non-trivial extension is $\mathbb{C}/\mathbb{R}$, which is of course well understood.) We write $\mathfrak{p}_K$ for the unique maximal ideal in $\mathcal{O}_K$, and write k_K for the residue field $\mathcal{O}_K/\mathfrak{p}_K$. Similarly we have $\mathfrak{p}_E$ and k_E. Everything we said in the global case holds verbatim in the local case, with the simplification that $g = 1$ always, i.e., $\mathfrak{p}_K\mathcal{O}_E = \mathfrak{p}_E^e$. (For instance, "split" never happens unless $E = K$.) The decomposition group $D_{\mathfrak{p}_E}(E/K)$ is just $\mathrm{Gal}(E/K)$, so this notion is useless in the local case.

From global to local. Let E/K be a finite Galois extension of number fields. Let $\mathfrak{P}$ be a prime of E above a prime $\mathfrak{p}$ of K. Consider the completions $E_{\mathfrak{P}}$ and $K_{\mathfrak{p}}$. The extension $E_{\mathfrak{P}}/K_{\mathfrak{p}}$ is Galois, and its Galois group is canonically identified with the decomposition group $D_{\mathfrak{P}}(E/K)$. Under this identification the inertia subgroup of $\mathrm{Gal}(E_{\mathfrak{P}}/K_{\mathfrak{p}})$ corresponds to the inertia subgroup of $D_{\mathfrak{P}}(E/K)$.

Again, everything also holds for global function fields, provided that we replace primes by places.

3. Lecture 3, 2/2/2021

3.1. CFT for $\mathbb{Q}$ continued.

Corollary 3.1.1. *For a prime p coprime to m, let g be the number of distinct prime of $\mathbb{Q}(\zeta_m)$ over p, and let f be the residue extension degree. Then $f =$ the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$, and $g = \phi(m)/f$.*

Proof. Recall that $\phi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = efg$, where e is the ramification index of p. We know $e = 1$. Now f is the order of $(p, \mathbb{Q}(\zeta_m)/\mathbb{Q})$, which is equal to the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$ by Lemma 2.2.7. □

If $\mathfrak{P}$ is a prime of $\mathbb{Q}(\zeta_m)$ above p, then $\mathbb{Q}(\zeta_m)_{\mathfrak{P}} \cong \mathbb{Q}_p(\zeta_m)$ as $\mathbb{Q}_p$-algebras. We hence deduce the following local result, which can also be proved purely locally, see [Ser79, §IV.4].

Corollary 3.1.2. *If p is coprime to m, then $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ is unramified and has degree equal to the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$.*

We can now deduce Dirichlet's theorem on primes in arithmetic progressions from the Chebotarev Density Theorem.

Corollary 3.1.3 (of Lemma 2.2.7 and Theorem 2.1.2)**.** *Let a, m be coprime positive integers. There are infinitely many primes in the arithmetic progression $a + mn, n \in \mathbb{Z}$.*

Proof. Primes in this arithmetic progression are precisely those p such that $\Psi(p) = \Psi(a) \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. Since $\{\Psi(a)\}$ is a conjugacy class in $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, the density of such primes is $1/\phi(m) > 0$. □

For $\mathbb{Q}$, a modulus $\mathfrak{m}$ is a symbol $\mathfrak{m} = m$ or $\mathfrak{m} = \infty m$, with $m \in \mathbb{Z}_{>0}$. When $\mathfrak{m} = m$, the ray class group $\mathrm{Cl}_{\mathfrak{m}}$ is defined to be the quotient group of the group of fractional deals of $\mathbb{Q}$ coprime to m modulo those principal ideals generated by

$f \in \mathbb{Q}^\times$ such that f is coprime to m (i.e., $f = a/b$ with a, b coprime to m) and $f \equiv 1 \mod m$ (i.e., $\bar{a}\bar{b}^{-1} = 1$ in $(\mathbb{Z}/m\mathbb{Z})^\times$). When $\mathfrak{m} = \infty m$, the definition of $\mathrm{Cl}_\mathfrak{m}$ is the same but with the extra condition $f > 0$.

Exercise 3.1.4. We have an isomorphim $(\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Cl}_{\infty m}$ under which each prime number p coprime to m goes to the class of the prime ideal (p). Similarly, $(\mathbb{Z}/m\mathbb{Z})^\times / \{\pm 1\} \cong \mathrm{Cl}_m$.

Theorem 3.1.5. *The extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is the ray class field corresponding to $\mathfrak{m} = \infty m$, and Ψ is the Artin map, after identifying $(\mathbb{Z}/m\mathbb{Z})^\times$ with $\mathrm{Cl}_{\infty m}$.*

Proof. For a prime p coprime to m, p splits in E if and only if $(p, E/\mathbb{Q}) = 1$, if and only if $\Psi(p) = 1$ (by Lemma 2.2.7), if and only if $p = 1$ in $(\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Cl}_\mathfrak{m}$. By the characterization of the ray class field $\mathbb{Q}_\mathfrak{m}$ we have $\mathbb{Q}_\mathfrak{m} = E$. Since $\Psi(p) = (p, E/\mathbb{Q})$, Ψ is the Artin map. □

Theorem 3.1.6 (Kronecker–Weber)**.** *Every finite abelian extension $E/\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_m)$ for sufficiently large m.*

Remark 3.1.7. Given a finite abelian extension $E/\mathbb{Q}$, one can characterize the smallest m such that $E \subset \mathbb{Q}(\zeta_m)$ as follows. Firstly, the prime divisors of m are precisely the primes that are ramified in E. Secondly, m is the smallest such that the map $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(E/\mathbb{Q})$ sending every unramified prime p to $(p, E/\mathbb{Q})$ is well defined.

Remark 3.1.8. The generalized Kronecker–Weber Theorem in CFT states that every finite abelian extension of a number field K is contained in $K_\mathfrak{m}$ for a sufficiently large modulus $\mathfrak{m}$. For $K = \mathbb{Q}$, all sufficiently large moduli are of the form $\mathfrak{m} = \infty m$ (that is, ∞ must appear), and we have seen that $\mathbb{Q}_{\infty m} = \mathbb{Q}(\zeta_m)$. In contrast, The ray class field corresponding to the modulus $\mathfrak{m} = m$ is $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$, the totally subfield of $\mathbb{Q}(\zeta_m)$. These fields are clearly not large enough for Kronecker–Weber to hold.

3.1.9. Using the Kronecker–Weber theorem and the Artin isomorphism

$$\Psi : (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}), \quad p \mapsto (p, \mathbb{Q}(\zeta_m)/\mathbb{Q}),$$

we have obtained a classification of all the abelian extensions $E/\mathbb{Q}$, as well as understood the Galois groups $\mathrm{Gal}(E/\mathbb{Q})$ and how unramified primes decompose in E (since we understand the elements $(p, E/\mathbb{Q})$, which is just $(p, \mathbb{Q}(\zeta_m)/\mathbb{Q})|_E$ if $E \subset \mathbb{Q}(\zeta_m)$). This is essentially the main content of global CFT for $\mathbb{Q}$.

3.1.10. We sketch how one can deduce quadratic reciprocity as an almost formal consequence of the above facts. For simplicity, we only consider distinct odd primes p, q with $q \equiv 1 \mod 4$. We need to show $(p/q) = 1$ if and only if $(q/p) = 1$.

Since $(\mathbb{Z}/q\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ is cyclic (as q is prime), there is a unique quadratic extension $K/\mathbb{Q}$ inside $\mathbb{Q}(\zeta_q)$. Since q is the unique finite prime that ramifies in $\mathbb{Q}(\zeta_q)$, it is also the unique finite prime that ramifies in K. Thus K has to be $\mathbb{Q}(\sqrt{q})$ (note that both q and 2 ramify in $\mathbb{Q}(\sqrt{-q})$, whose discriminant is $4q$), i.e., we have shown that $\mathbb{Q}(\sqrt{q}) \subset \mathbb{Q}(\zeta_q)$. See also the exercise below for an explicit embedding $\mathbb{Q}(\sqrt{q}) \subset \mathbb{Q}(\zeta_q)$. Now the kernel of

$$F : (\mathbb{Z}/q\mathbb{Z})^\times \xrightarrow{\Psi} \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\sqrt{q})/\mathbb{Q})$$

is precisely the subgroup of square elements, since $(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic. Hence $(p/q) = 1$ if and only if $\bar{p} \in \ker F$, if and only if $(p, \mathbb{Q}(\zeta_q)/\mathbb{Q})$ fixes $\mathbb{Q}(\sqrt{q})$, if and only if $(p, \mathbb{Q}(\sqrt{q})/\mathbb{Q}) = 1$, if and only if p splits in $\mathbb{Q}(\sqrt{q})$, if and only if $X^2 - q$ splits modulo p[4], if and only if $(q/p) = 1$.

Exercise 3.1.11. Complete the proof in the case $p \equiv q \equiv 3 \mod 4$.

Exercise 3.1.12. Let q be an odd prime number. Let

$$y = \sum_{j=1}^{q} (j/q)\zeta_q^j \in \mathbb{Q}(\zeta_q),$$

where (j/q) is the Legendre symbol. Show that $y^2 = (-1/q)q$.

3.2. **Ramification in the cyclotomic extension.** Let p be a prime. If $p|m$, then how does p behave in $\mathbb{Q}(\zeta_m)$? For simplicity we only deal with the case $m = p^r$, but see Remark 3.2.6 below.

Lemma 3.2.1. *Suppose $m = p^r$. Then p is totally ramified (i.e., ramification index = degree) in $\mathbb{Q}(\zeta_m)$.*

Proof. We have $\Phi_m(X) = (X^{p^r} - 1)/(X^{p^{r-1}} - 1)$. Modulo p this polynomial becomes $(X-1)^{p^r}/(X-1)^{p^{r-1}} = (X-1)^{p^r - p^{r-1}} = (X-1)^{\phi(m)}$. Hence $p\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathfrak{P}^{\phi(m)}$, where $\mathfrak{P}$ is generated by $\zeta_m - 1$ and p. □

As before, we immediately deduce a local statement, which again has a purely local proof as in [Ser79, §IV.4].

Corollary 3.2.2. *Let $m = p^r$. Then $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ is totally ramified, and the degree is $\phi(m)$.*

3.2.3. *Structure of $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ for general m.* Fix a prime p. To simplify notation, for each integer $m \geq 1$ we write K_m for $\mathbb{Q}_p(\zeta_m)$. Firstly, we can combine Corollary 3.1.2 and Corollary 3.2.2 as follows.

Proposition 3.2.4. *Let $m = np^r$, where $n \in \mathbb{Z}_{\geq 1}$ is coprime to p, and $r \in \mathbb{Z}_{\geq 0}$. Let e be the ramification index of $K_m/\mathbb{Q}_p$, and let f be the residue extension degree of $K_m/\mathbb{Q}_p$. Then $e = \phi(p^r)$, and $f =$ the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$. Moreover, $K_m/\mathbb{Q}_p$ is the linearly disjoint compositum of $K_n/\mathbb{Q}_p$ and $K_{p^r}/\mathbb{Q}_p$.*

Proof. We have seen the special cases $m = n$ and $m = p^r$ in Corollary 3.1.2 and Corollary 3.2.2. Note that K_m is the compositum of K_n and K_{p^r} over $\mathbb{Q}_p$, because $\zeta_n\zeta_{p^r}$ is a primitive m-th root of unity. The proposition then follows from the following general fact. □

Fact 3.2.5. *Suppose E/F is a finite Galois extension of local fields. Suppose E is the compositum of two normal subextensions E_u/F and E_r/F, where E_u/F is unramified and E_r/F is totally ramified. Then the ramification index $e(E/F)$ is equal to $[E_r : F]$, and the residue extension degree $f(E/F)$ is equal to $[E_u : F]$. In particular $[E : F] = [E_r : F][E_u : F]$, and so E_r/F and E_u/F are linearly disjoint.*

[4] Note that the conductor of $\mathbb{Z}[\sqrt{q}]$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{q})} = \mathbb{Z}[\frac{\sqrt{q}+1}{2}]$ contains 2 and is therefore coprime to p. (In fact, the conductor is $2\mathcal{O}_{\mathbb{Q}(\sqrt{q})}$.) Therefore the splitting of p is equivalent to the splitting of $X^2 - q$ modulo p.

Proof. The ramification degrees satisfy

$$e(E/F) = e(E/E_u)e(E_u/F) = e(E/E_r)e(E_r/F).$$

Since $e(E_u/F) = 1$, we have $e(E/F) = e(E/E_u) \leq [E : E_u] \leq [E_r : F] = e(E_r/F) \leq e(E/F)$. Hence equality must hold everywhere. Similarly, we have

$$f(E/F) = f(E/E_r)f(E_r/E) = f(E/E_u)f(E_u/F).$$

Since $f(E_r/E) = 1$, we have $f(E/F) = f(E/E_r) \leq [E : E_r] \leq [E_u : F] = f(E_u/F) \leq f(E/F)$. Hence equality must hold everywhere. □

Remark 3.2.6. In the global setting, if $m = np^r$ with $p \nmid n$, it is a lot easier to see that $\mathbb{Q}(\zeta_m)$ is a linearly disjoint compositum of $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_{p^r})$. Just use that $\phi(m) = \phi(n)\phi(p^r)$! In fact, using this linearly disjointness we can easily understand the behavior of p in $\mathbb{Q}(\zeta_m)$ by combining Corollary 3.1.1 and Lemma 3.2.1. For instance, we have $e = \phi(p^r)$ and $f =$ order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$. We leave the details to the reader. (Of course these formulas for e, f also follow from the local formulas in Proposition 3.2.4.)

4. Lecture 4, 2/4/2021

4.1. The local Artin map for $\mathbb{Q}_p$.

4.1.1. Fix a prime p. For each $m \in \mathbb{Z}_{\geq 1}$, write K_m for $\mathbb{Q}_p(\zeta_m)$. Write α_m for the natural injecition $\mathrm{Gal}(K_m/\mathbb{Q}_p) \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$.

Write $m = p^r n$, with $p \nmid n$. We have seen in Proposition 3.2.4 that $K_n/\mathbb{Q}_p$ is the linearly disjoint compositum of $K_{p^r}/\mathbb{Q}_p$ and $K_m/\mathbb{Q}_p$. Therefore we have a canonical isomorphism

$$\mathrm{Gal}(K_m/\mathbb{Q}_p) \cong \mathrm{Gal}(K_n/\mathbb{Q}_p) \times \mathrm{Gal}(K_{p^r}/\mathbb{Q}_p),$$

induced by the two natural projections. Under this decomposition, the injection α_m is compatible with the injections α_n and α_{p^r}, if we identify $(\mathbb{Z}/m\mathbb{Z})^\times$ with $(\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/p^r\mathbb{Z})^\times$ via the Chinese Remainder Theorem.

Since $K_n/\mathbb{Q}_p$ is unramified, its Galois group is generated by the Frobenius element. Clearly α_n sends the Frobenius to $p \in (\mathbb{Z}/n\mathbb{Z})^\times$. (This statement is strictly easier than the global statement Lemma 2.2.7.) We have also seen in Proposition 3.2.4 that α_{p^r} is surjective. Therefore the image of α_m is the subgroup

$$\langle p \rangle \times (\mathbb{Z}/p^r\mathbb{Z})^\times \subset (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/p^r\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times.$$

4.1.2. Recall that $\mathbb{Q}_p^\times \cong p^{\mathbb{Z}} \times \mathbb{Z}_p^\times$. Define the map

$$j_m : \mathbb{Q}_p^\times \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/p^r\mathbb{Z})^\times$$

by combining the maps

$$p^{\mathbb{Z}} \to (\mathbb{Z}/n\mathbb{Z})^\times, \quad p \mapsto p$$

and

$$\mathbb{Z}_p^\times \xrightarrow{x \mapsto x^{-1}} \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times/(1 + p^r\mathbb{Z}_p) \cong (\mathbb{Z}/p^r\mathbb{Z})^\times.$$

Clearly the image of j_m is equal to the image of α_m, so the composition $\alpha_m^{-1} \circ j_m$ makese sense. We thus get a surjective homomorphism:

$$\psi_m := \alpha_m^{-1} \circ j_m : \mathbb{Q}_p^\times \longrightarrow \mathrm{Gal}(K_m/\mathbb{Q}_p),$$

called the *local Artin map* for the extension $K_m/\mathbb{Q}_p$.

If l is a multiple of m, then we have commutative diagrams

$$\begin{tikzcd}
\mathrm{Gal}(K_l/\mathbb{Q}_p) \arrow[r, "\alpha_l"] \arrow[d] & (\mathbb{Z}/l\mathbb{Z})^\times \arrow[d] \\
\mathrm{Gal}(K_m/\mathbb{Q}_p) \arrow[r, "\alpha_m"] & (\mathbb{Z}/m\mathbb{Z})^\times
\end{tikzcd}$$

and

$$\begin{tikzcd}
\mathbb{Q}_p \arrow[r, "j_l"] \arrow[d, equal] & (\mathbb{Z}/l\mathbb{Z})^\times \arrow[d] \\
\mathbb{Q}_p \arrow[r, "j_m"] & (\mathbb{Z}/m\mathbb{Z})^\times
\end{tikzcd}$$

where all the vertical maps are the natural ones (noting that $K_m \subset K_l$). Therefore the following diagram commutes

$$\begin{tikzcd}
\mathbb{Q}_p^\times \arrow[r, "\psi_l"] \arrow[d, equal] & \mathrm{Gal}(K_l/\mathbb{Q}_p) \arrow[d] \\
\mathbb{Q}_p^\times \arrow[r, "\psi_m"] & \mathrm{Gal}(K_m/\mathbb{Q}_p)
\end{tikzcd}$$

In other words, we have a homomorphism

$$\psi : \mathbb{Q}_p^\times \longrightarrow \varprojlim_m \mathrm{Gal}(K_m/\mathbb{Q}_p) = \mathrm{Gal}(\mathbb{Q}_p^{cycl}/\mathbb{Q}_p),$$

where $\mathbb{Q}_p^{cycl}$ is the union of all K_m's. Since each ψ_m is surjective, we know that ψ has dense image, where $\mathrm{Gal}(\mathbb{Q}_p^{cycl}/\mathbb{Q}_p)$ is endowed with the profinite topology.

Theorem 4.1.3 (Local Kronecker–Weber Theorem)**.** *Each finite abelian extension $E/\mathbb{Q}_p$ is contained in some K_m.*

By the theorem, $\mathbb{Q}_p^{cycl}$ is the maximal abelian extension of $\mathbb{Q}_p$ inside $\overline{\mathbb{Q}}_p$, denoted by $\mathbb{Q}_p^{\mathrm{ab}}$. (The *maximal abelian extension* makes sense, as the compositum of two finite abelian extensions is finite abelian.) Hence ψ is a homomorphism

$$\psi : \mathbb{Q}_p^\times \longrightarrow \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p).$$

This is called the *local Artin map.* One of the main goals of local CFT is to construct the analogue of ψ when $\mathbb{Q}_p$ is replaced by a general local field K. The general local Artin map is of the form

$$\psi : K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

4.2. **The idelic global Artin map.** Fix $m \in \mathbb{Z}_{\geq 1}$. For any prime p, we can identify $\mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p)$ with the decomposition group $D_p(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \subset \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. (The decomposition group does not depend on the choice of a prime of $\mathbb{Q}(\zeta_m)$ above p, since the extension is abelian.) Thus we have an embedding $\mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) \hookrightarrow$

$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. The following diagram commutes:

$$\begin{tikzcd}
\mathbb{Q}_p^\times \arrow[r, "\psi_{m,p}"] \arrow[d, "j_{m,p}"] & \mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) \arrow[d] \\
(\mathbb{Z}/m\mathbb{Z})^\times \arrow[r, "\cong"] & \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})
\end{tikzcd}$$

where the bottom map is the global Artin map, and we have written $\psi_{m,p}$ and $j_{m,p}$ for what were previously denoted by ψ_m and j_m. We denote the map $\mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ resulting from either way of composition by $\Psi_{m,p}$.

Clearly when p runs through all the primes, the images of $j_{m,p}$ generate $(\mathbb{Z}/m\mathbb{Z})^\times$. This suggests that we should think of the global Artin map more canonically as a map from "$\prod_p \mathbb{Q}_p^\times$" to $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. This map should just be the product of the maps $\Psi_{p,m} : \mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. However, we immediately see that this strategy does not make sense, because there are infinite many p's (!) and we cannot take the product of infinitely many maps into $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. This problem is solved by Chevalley's idea of using ideles. In the current example, we have the following two key observations:

(i) If $x \in \mathbb{Q}^\times$, then for almost all primes p the image of x in $\mathbb{Q}_p^\times$ lies in $\mathbb{Z}_p^\times$.

(ii) If p is a prime not dividing m, and if $x \in \mathbb{Z}_p^\times$, then the local Artin map $\psi_{m,p} : \mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p)$ kills x.

Based on observation (ii), the infinite product $\prod_p \Psi_{m,p}(x_p)$ makes sense, as long as $x_p \in \mathbb{Z}_p^\times$ for almost all p. Thus we consider the elements $(x_p)_p$ of $\prod_p \mathbb{Q}_p^\times$ such that x_p lies in $\mathbb{Z}_p^\times$ for almost all p. Such elements are called the *finite ideles*. They form a subgroup of $\prod_p \mathbb{Q}_p^\times$, denoted by $\mathbb{A}_f^\times$. Define the group of ideles to be

$$\mathbb{A}^\times := \mathbb{R}^\times \times \mathbb{A}_f^\times.$$

By the above observation (i), $\mathbb{Q}^\times$ embeds diagonally into $\mathbb{A}^\times$. That is, we map $x \in \mathbb{Q}^\times$ to the idele $(x_\infty, x_2, x_3, \cdots)$, where each x_v is just x.

The *idelic global Artin map* for the extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is a map

$$\Psi_m : \mathbb{A}^\times \longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$$

defined as follows. For $x = (x_\infty, x_p) = (x_\infty, x_2, x_3, \cdots) \in \mathbb{A}^\times$, we have

$$\Psi_m(x) = \Psi_{m,\infty}(x_\infty) \cdot \prod_p \Psi_{m,p}(x_p).$$

Here $\Psi_{m,p}$ is the map $\mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ defined before, and $\Psi_{m,\infty}$ is the map $\mathbb{R}^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ sending all positive reals to the identity and sending all negative reals to the complex conjugation in $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ (which corresponds to $-1 \in (\mathbb{Z}/m\mathbb{Z})^\times$).

Exercise 4.2.1. Check that Ψ_m is well defined, and that it is trivial on the diagonally embedded $\mathbb{Q}^\times$.

As in the local case, when m varies the global Artin maps for $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ glue together to a map

$$\Psi : \mathbb{A}^\times \longrightarrow \varprojlim_m \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}^{cycl}/\mathbb{Q}).$$

By the global Kronecker–Weber Theorem, the right hand side is $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$. By the above exercise, we can replace the left hand side by $\mathbb{A}^\times/\mathbb{Q}^\times$. Thus we have

$$\Psi : \mathbb{A}^\times/\mathbb{Q}^\times \longrightarrow \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}).$$

One of the main goals of global CFT is to generalize this map when $\mathbb{Q}$ is replaced by an arbitrary global field K. The general global Artin map is of the form

$$\Psi : \mathbb{A}_K^\times/K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

5. Lecture 5, 2/9/2021

5.1. Recall of profinite groups and inifinite Galois theory.

5.1.1. *Inverse limits.* Recall that a *directed set* is a set I equipped with a binary relation $\geq$, satisfying:

(i) $i \geq i$ for all $i \in I$.
(ii) If $i \geq j$ and $j \geq k$, then $i \geq k$.
(iii) For any $i, j \in I$, there exists k such that $k \geq i$ and $k \geq j$.

Example 5.1.2. Below are typical examples of inverse systems that we will use.

(i) $I = \mathbb{Z}_{\geq 1}$ with the natural order $\geq$.
(ii) $I = \mathbb{Z}_{\geq 1}$, where $m \geq n$ if and only if $n|m$.
(iii) Let G be a topological group. Let $I =$ the set of all finite indexed open normal subgroups of G. For $H_1, H_2 \in I$, we define $H_1 \geq H_2$ if $H_1 \subset H_2$.
(iv) Let E/K be a field extension. Let $I =$ the set of all fintie Galois extensions of K inside E. For $L_1, L_2 \in I$, we define $L_1 \geq L_2$ if $L_1 \supset L_2$.

Exercise 5.1.3. Check examples (iii) and (iv).

Let $\mathcal{C}$ be an arbitrary category, e.g., the category of sets/groups/topological groups, etc. Let I be a directed set. By an *inverse system* in $\mathcal{C}$ indexed by I, we mean a family of objects $(G_i)_{i\in I}$ in $\mathcal{C}$ together with morphisms $f_{i,j} : G_i \to G_j$ (called transition maps) defined whenever $i \geq j$. These should satisfy:

(i) For all $i \in I$, we have $f_{i,i} = \mathrm{id}_{G_i}$.
(ii) If $i \geq j \geq k$, then $f_{i,k} : G_i \to G_k$ is the composition $G_i \xrightarrow{f_{i,j}} G_j \xrightarrow{f_{j,k}} G_k$.

Example 5.1.4. Let G be a topological group. Let $I =$ the set of all finite indexed open normal subgroups of G. Then $(G/N)_{N\in I}$ is an inverse system of finite groups. Here when $N \geq N'$, the transition map $G/N \to G/N'$ is the projection (since $N \subset N'$.)

Example 5.1.5. Let E/K be a field extension. Let $I =$ the set of all fintie Galois extensions of K inside E. Then $(\mathrm{Gal}(L/K))_{L\in I}$ is an inverse system of finite groups. Here when $L \geq L'$, the transition map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(L'/K)$ is the restriction map (since $L \supset L'$.)

Let $(G_i)_{i\in I}$ be an inverse system in $\mathcal{C}$. By an *inverse limit* of $(G_i)_{i\in I}$ in $\mathcal{C}$, we mean an object G in $\mathcal{C}$ together with morphisms $p_i : G \to G_i$ for all i, satisfying:

(i) The p_i are compatible with the transition maps, i.e., whenever $i \geq j$ the composition $G \xrightarrow{p_i} G_i \xrightarrow{f_{i,j}} G_j$ is p_j.
(ii) If H is an object in $\mathcal{C}$ and if $q_i : H \to G_i$ are morphisms defined for all i compatible with the transition maps, then there is a unique morphism $u : H \to G$ such that $q_i = p_i \circ u$ for all i.

An inverse limit may not exist. If it exists, it is unique up to unique isomorphism. We denote it by $\varprojlim_{i\in I} G_i$.

Lemma 5.1.6. *Let $(G_i)_{i\in I}$ be an inverse system of topological groups. Suppose J is a cofinal subset of I, meaning that $\forall i \in I, \exists j \in J$ such that $j \geq i$. Then the inverse limit $\varprojlim_{j\in J} G_j$ exists if and only if $\varprojlim_{i\in I} G_i$ exists. When they both exist, they are naturally isomorphic.*

Proof. Exercise. □

5.1.7. *Inverse limits of topological groups.*

Theorem 5.1.8. *Let $\mathcal{C}$ be the category of topological spaces/topological groups/topological rings. Let $(G_i)_{i\in I}$ be an inverse system in $\mathcal{C}$. Then the inverse limit $\varprojlim_{i\in I} G_i$ exists.*

Proof. Define $G = (G_i)_{i\in I}$ to be the subset of $\prod_{i\in I} G_i$, consisting of $(g_i)_{i\in I}$ satisfying:

$$f_{i,j}(g_i) = g_j, \quad \forall i, j \in I \text{ s.t. } i \geq j.$$

Then G is a subgroup of $\prod_{i\in I} G_i$, and it is equipped with natural maps $p_i : G \to G_i$. We endow $\prod_{i\in I} G_i$ with the product topology[5], and endow $G = \varprojlim_{i\in I} G_i$ with the subspace topology inherited from $\prod_i G_i$. Equivalently, the topology on G is the weakest topology (i.e., the topology having the least open sets) such that each natural map $p_i : G \to G_i$ is continuous. We leave it as an exercise to check that G is the inverse limit in $\mathcal{C}$. □

Remark 5.1.9. Since the topology on $G = \varprojlim_{i\in I} G_i$ is the weakest such that each $G \to G_i$ is continuous, we know that for a topological space T and a map $f : T \to G$, the map f is continuous if and only if the composition $T \xrightarrow{f} G \to G_i$ is continuous for all $i \in I$.

Remark 5.1.10. Note that we can always view an abstract set/group/ring as a topological group/ring by considering the discrete topology. The topology on the inverse limit of discrete objects is discrete.

Now let $(G_i)_{i\in I}$ be an inverse system of finite sets/groups/rings. On each G_i we put the discrete topology. By Tychonoff's theorem, the product of arbitrarily many compact topological spaces is compact. Hence $\prod_i G_i$ is compact. It is also easy to see that $\prod_i G_i$ is Hausdorff. Clearly $\varprojlim_i G_i$ is a closed in $\prod_i G_i$. Hence it is also compact Hausdorff.

Definition 5.1.11. A *profinite group* is a topological group that is isomorphic to the topological group $\varprojlim_{i\in I} G_i$ for some inverse system of finite groups $(G_i)_{i\in I}$.

Remark 5.1.12. By definition, a profinite group is just a topological group satysfing some properties. The presentation of it as an inverse limit of finite groups is not part of the datum.

[5] A basis of open sets is given by sets of the form $\prod_{i\in I} G_i' \subset \prod_{i\in I} G_i$, where $G_i' = G_i$ for almost all i, and G_i' is open in G_i for all i

Example 5.1.13. For each prime p, the group $\mathbb{Z}_p$ with its standard topology induced by the p-adic absolute value is profinite. In fact, the natural group isomorphism $\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ is a homeomorphism. Similarly, $\mathbb{Z}_p^\times$ with the standard topology is a profinite topological group isomorphic to $\varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times$.

Theorem 5.1.14. *Let G be a Hausdorff topological group. It is profinte if and only if it is compact Hausdorff and 1 admits a neighborhood basis consisting of open subgroups.*

Remark 5.1.15. In any topological group, any open subgroup is closed, because the complement is a union of cosets of that subgroup which are all open. In a compact group, all closed subgroups are compact, and a closed subgroup is open if and only if it has finite index.

Proof. For the "only if" part, we have already seen that G is compact Hausdorff. If $G \cong \varprojlim_{i\in I} G_i$ is a presentation of G as an inverse limit of finite groups, then $(\ker(G \to G_i))_{i\in I}$ is a neighborhood basis of 1 in G consisting of open (normal) subgroups.

For the "if" part, since all open subgroups are of finite index, it is easy to see that 1 admits a neighborhood basis $\mathcal{N}$ consisting of open *normal* subgroups. (Given any open subgroup, since it is of finite index, it has only finitely many conjugates. The intersection of all the conjugates is an open normal subgroup.) For each $N \in \mathcal{N}$ we have the finite quotient group G/N. The set $\mathcal{N}$ is a directed set where $N_1 \geq N_2$ if $N_1 \subset N_2$, and $(G/N)_{N\in\mathcal{N}}$ is an inverse system of finite groups. We can thus form the profinite group $G' := \varprojlim_{N\in\mathcal{N}} G/N$.

One checks that the natural map $G \to G'$ is continuous (easy) and injective (using that the N's form a neighborhood basis of 1 and that G is Hausdorff). We claim it is surjective. Let $(g_N)_{N\in\mathcal{N}} \in G'$. For each $N \in \mathcal{N}$, the coset $g_N N$ is closed in G. Every finite subcollection of the closed sets $(g_N N)_{N\in\mathcal{N}}$, say $g_{N_1}N_1, \cdots, g_{N_k}N_k$, has non-trivial intersection. This is because we can find $N \in \mathcal{N}$ such that $N \subset N_1 \cap \cdots \cap N_k$, and we have $g_N N \subset g_{N_1}N_1 \cap \cdots \cap g_{N_k}N_k$. Since G is compact and since every finite subcollection of $(g_N N)_{N\in\mathcal{N}}$ has non-empty intersection, we hvae

$$\bigcap_{N\in\mathcal{N}} g_N N \neq \emptyset.$$

Now any element of the above set maps to $(g_N)_N \in G'$. Thus we have shown that the natural map $G \to G'$ is a continuous bijection. Since the left hand side is compact and the right hand side is Hausdorff, this map is a homeomorphism. □

Example 5.1.16. In $\mathbb{Z}_p$, 0 has a neighborhood basis consisting of open subgroups $p^n\mathbb{Z}_p$. In $\mathbb{Z}_p^\times$, 1 has a neighborhood basis consisting of open subgroups $1 + p^n\mathbb{Z}_p$.

Definition 5.1.17. A *locally profinite* topological group is a Hausdorff group such that 1 admits a neighborhood basis consisting of compact open subgroups. Equivalently, it is a Hausdorff group containing a profinite group as an open subgroup.

Example 5.1.18. The groups $\mathbb{Q}_p$ and $\mathbb{Q}_p^\times$ are locally profinite, since they contain the profinite groups $\mathbb{Z}_p$ and $\mathbb{Z}_p^\times$ as open subgroups respectively. However $\mathbb{Q}_p$ and $\mathbb{Q}_p^\times$ are not profinite, since they are not compact. Also, $\mathrm{GL}_n(\mathbb{Q}_p)$ is locally profinite, containing the profinite group $\mathrm{GL}_n(\mathbb{Z}_p)$ as an open subgroup.

We have a convenient criterion characterizing dense subsets of a profinte group.

Lemma 5.1.19. *Let G be a profinite group, and fix an isomorphism $G \xrightarrow{\sim} \varprojlim_{i\in I} G_i$, where $(G_i)_{i\in I}$ is an inverse system of finite groups. A non-empty subset $S \subset G$ is dense if and only if its image in G_i is G_i for each $i \in I$.*

Proof. If S is dense, then its image in G_i is also dense since $G \to G_i$ is continuous. But G_i is discrete, so a non-empty dense subset of G_i must be G_i.

For the converse direction, we assume without loss of generality that $G = \varprojlim_i G_i \subset \prod_i G_i$. Let $g = (g_i)_{i\in I} \in G$, and let U be an open neighborhood of g. We need to show that $S \cap U \neq \emptyset$. Up to shrinking U, we may assume that $U = \{(h_i)_i \in G \mid \forall i \in I_0,\ h_i = g_i\}$, where I_0 is a finite subset of I. (This follows from the way the product topology on $\prod_i G_i$ is defined.) Since I_0 is finite, there exists $k \in I$ that is a common upper bound of all elements of I_0. Let $s \in S$ be a preimage of $g_k \in G_k$. Then the image of s in G_i is g_i for all $i \in I_0$. Hence $s \in U$. This shows that S is dense in G. □

The following fact characterizes (locally) profinite groups topologically. We will not need it.

Fact 5.1.20. *Let G be a topological group. Then G is profinite (resp. locally profinite) if and only if it is Hausdorff, compact (resp. locally compact), and totally disconnected, meaning that every connected component is a point.*

5.1.21. *Profinite completion.* Let G be a topological group. We define its profinite completion to be

$$\widehat{G} = \varprojlim_{N} G/N,$$

where N runs through open normal finite indexed subgroups of G. (Here note that the quotient topology on each G/N is discrete, by the openness of N.) Then $\widehat{G}$ is profinite. There is a canonical continuous homomorphism $G \to \widehat{G}$, and every continuous homomorphism from G to a profinite group H factors through a unique continuous homomorphism $\widehat{G} \to H$. In general the map $G \to \widehat{G}$ is neither injective nor surjective. This map is an isomorphism if and only if G is profinite. (The only if part is trivial, and the if part is essentially proved in the proof of Theorem 5.1.14.) Note that this means when G is profinite, we have a canonical presentation of G as an inverse limit of finite groups.

Corollary 5.1.22. *Let G be a topological group. The image of $G \to \widehat{G}$ is dense in $\widehat{G}$.*

Proof. This follows immediately from Lemma 5.1.19. □

Exercise 5.1.23. Prove that there is a natural isomorphism of topological groups

$$\widehat{\mathbb{Z}} \xrightarrow{\sim} \prod_p \mathbb{Z}_p,$$

where p runs through all the primes. Here we view $\mathbb{Z}$ as a discrete topological group, and $\widehat{\mathbb{Z}}$ is its profinite completion.

5.1.24. *Infinite Galois theory.* See [Mor96, §17] Let E/K be a Galois extension (i.e., normal and separable), not necessarily of finite degree. Let I be the set of finite Galois extensions of K inside E. We have a natural isomorphism of abstract groups

$$\mathrm{Gal}(E/K) \cong \varprojlim_{L \in I} \mathrm{Gal}(L/K).$$

The right hand side has the profinite topology, so we obtain a topology on $\mathrm{Gal}(E/K)$, called the *Krull topology*. By definition, $\mathrm{Gal}(E/K)$ with the Krull topology is a profinite group. Equivalently, the Krull topology on $\mathrm{Gal}(E/K)$ is obtained by requiring $(\mathrm{Gal}(L/K))_{L\in I}$ to be an open neighborhood basis of 1.

Theorem 5.1.25. *The map $L \mapsto \mathrm{Gal}(E/L)$ is an inclusion-reversing bijection from the set of intermediate extensions of E/K to the set of* closed *subgroups of $\mathrm{Gal}(E/K)$. Under this correspondence, we have L/K is finite if and only if $\mathrm{Gal}(E/L)$ is an open subgroup of $\mathrm{Gal}(E/K)$. In this case $[L : K] = [\mathrm{Gal}(E/K) : \mathrm{Gal}(E/L)]$. We have L/K is normal if and only if $\mathrm{Gal}(E/L)$ is a normal subgroup of $\mathrm{Gal}(E/K)$. In this case, we have a topological isomorphism $\mathrm{Gal}(L/K) = \mathrm{Gal}(E/K)/\mathrm{Gal}(L/K)$, where the right hand side has the quotient topology.*

Exercise 5.1.26. Prove the above theorem using finite Galois theory.

Example 5.1.27. Let $\mathbb{F}_q$ be a finite field. For each $n \in \mathbb{Z}_{\geq 1}$, we have $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$. Taking the inverse limit in n on the two sides (with respect to divisibility), we have a topological isomorphism $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}$.

Example 5.1.28. For each $m \in \mathbb{Z}_{\geq 1}$, we have a canonical isomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. Taking the inverse limit we obtain a topological isomorphism $\varprojlim_m (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}^{cycl}/\mathbb{Q})$. The left hand side is often denoted by $\widehat{\mathbb{Z}}^\times$.

Example 5.1.29. For each $m \in \mathbb{Z}_{\geq 1}$, the local Artin map for $\mathbb{Q}_p$ gives rise to a surjective continuous map $\mathbb{Q}_p^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p)$. Taking the inerse limit we obtain a continuous map $\mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}_p^{cycl}/\mathbb{Q}_p)$. This in fact induces an isomorphism from the profinite completion of $\mathbb{Q}_p^\times$ to $\mathrm{Gal}(\mathbb{Q}_p^{cycl}/\mathbb{Q}_p)$. Recall that $\mathbb{Q}_p^\times$ is only locally profinite. If we identify it with $\mathbb{Z} \times \mathbb{Z}_p^\times$, then its profinite completion is $\widehat{\mathbb{Z}} \times \mathbb{Z}_p^\times$. We thus have two closed subgroups $\widehat{Z}$ and $\mathbb{Z}_p^\times$. Under the Galois correspondence they correspond to $\mathbb{Q}_p(\zeta_{p^\infty}) := \bigcup_r \mathbb{Q}_p(\zeta_{p^r})$ and $\bigcup_{n, p \nmid n} \mathbb{Q}_p(\zeta_n)$.

6. Lecture 6, 2/11/2021

6.1. **Recall of local fields.**

6.1.1. *Discretely valued fields.* Let K be a field. Recall that a *discrete valuation* on K is a surjective function $v : K \to \mathbb{Z} \cup \{\infty\}$, satisfying

- $v(x) = \infty$ if and only if $x = 0$
- $v(xy) = v(x + y)$
- $v(x + y) \geq \min(v(x), v(y))$

for all $x, y \in K$. The pair (K, v) is called a *discretely valued field.*

Remark 6.1.2. Some authors define a discretely valuation without requiring that v is surjective. Then either the image of v is $\{0, \infty\}$ (in which case v is called *trivial*), or there exists a unique $n \in \mathbb{Z}_{\geq 1}$ such that nv is a discrete valuation in our sense. In the latter case the difference in the two definitions is just a matter of normalization.

Example 6.1.3. Let $K = \mathbb{Q}$, and let p be a prime. We obtain a discrete valuation v_p on $\mathbb{Q}$ as follows. For any non-zero integer a we define $v_p(a) \in \mathbb{Z}_{\geq 0}$ such that $p^{v_p(a)}$ is the precise power of p dividing a. For $x = a/b \in \mathbb{Q}^\times$, we define $v_p(x) = v_p(a) - v_p(b)$. Finally we define $v_p(0) = \infty$ (of course!).

By Ostrowski's theorem, every discrete valuation on $\mathbb{Q}$, when canonically normalized, is of the form v_p for a unique prime p.

Example 6.1.4. Let $K = \mathbb{F}_q(t)$. For $f \in K^\times$, define $v_t(f)$ to be the "order of zero or pole" of f at $t = 0$. Then v_t is a discrete valuation on K.

Let (K, v) be a discretely valued field. Define

$$\mathcal{O}_K = \mathcal{O}_{K,v} := \{x \in K \mid v(x) \geq 0\}$$

$$\mathfrak{m}_K = \mathfrak{m}_{K,v} := \{x \in K \mid v(x) > 0\} .$$

Then $\mathcal{O}_K$ is a subring of K, called the *valuation ring of* v, and $\mathfrak{m}_K$ is the unique maximal ideal of $\mathcal{O}_K$. In fact, $\mathcal{O}_K$ is a DVR, namely a PID with a unique prime ideal. (See [Ser79, §§I.1, I.2] for various characterizations of a DVR.)

Any generator of $\mathfrak{m}_K$ is called a *uniformizer*. The uniformizers are precisely the elements $\pi \in K$ satisfying $v(\pi) = 1$.

We have

$$\mathcal{O}_K^\times = \{x \in K \mid v(x) = 0\} .$$

The non-zero ideals of $\mathcal{O}_K$ are of the form $\mathfrak{m}_K^n, n \in \mathbb{Z}_{\geq 1}$. Among these, only $\mathfrak{m}_K$ is prime. The field $\mathcal{O}_K/\mathfrak{m}_K$ is called the *residue field* of (K, v), which we will denote by k_K.

If we fix a uniformizer $\pi \in \mathcal{O}_K$, then for any $x \in K^\times$ we recover $v(x)$ as the unique integer n such that $\pi^{-n}x \in \mathcal{O}_K^\times$. Note that the notion of a uniformizer, as well as the subset $\mathcal{O}_K^\times \subset \mathcal{O}_K$, depend only on the ring structure of $\mathcal{O}_K$. This way we recover v from the subring $\mathcal{O}_K \subset K$. In fact, we have a bijection

(6.1.4.1)
$$\{\text{discrete valuations on } K\} \longleftrightarrow \{\text{subrings } \mathcal{O} \subset K \text{ s.t. } \mathcal{O} \text{ is DVR and } K = \operatorname{Frac} \mathcal{O}\} .$$

Thus in a sense, the theory of discretely valued fields is equivalent to the theory of DVR's.

Let (K, v) be a discretely valued field. Pick a real number $0 < \alpha < 1$ and define the corresponding absolute value

$$|x|_v := \alpha^{v(x)}$$

for $x \in K$. (Here $\alpha^\infty = 0$.) Then $|\cdot|_v$ is a nonarchimedean absolute value, i.e., a function $|\cdot| : K \to \mathbb{R}\geq 0$ satisfying

(i) $|x| = 0$ if and only if $x = 0$.
(ii) $|xy| = |x| \, |y|$.
(iii) $|x + y| \leq \max(|x|, |y|)$.

(Conversely, every non-archimedean absolute value $|\cdot|$ on K such that $|K^\times|$ is a *discrete* subgroup of $\mathbb{R}_{>0}$ comes from a discrete valuation and a choice of α.) We then obtain a metric on K by

$$d(x, y) = |x - y|_v ,$$

and hence a topology on K. Under this topology K is a Hausdorff topological field. (Recall that a topological field is a topological ring which is also a field, and on which the multiplicative inverse is continuous.) Clearly the topology depends only on v, not on the choice of α.

An equivalent way to define the topology on K is to declare that for each $x \in K$, we have a neighborhood basis of x given by $\{x + \mathfrak{m}_K^n\}_{n \geq 1}$.

6.1.5. *Completion.* Let R be a noetherian local ring, with unique maximal ideal $\mathfrak{m}$. Recall that the *completion* of R (as a local ring) is defined to be the ring

$$R^\wedge = \varprojlim_{n \in \mathbb{Z}_{\geq 1}} R/\mathfrak{m}_R^n.$$

There is a natural ring homomorphism $R \to R^\wedge$. We call R *complete*, if the natural map $R \to R^\wedge$ is an isomorphism. It is a fact that $R^\wedge$ itself is a Noetherian complete local ring. Its maximal ideal is generated by the image of $\mathfrak{m}$.

Lemma 6.1.6. *Let (K, v) be a discretely valued field. The following conditions are equivalent:*

- *(i) K is complete w.r.t. the metric $d(x, y) = |x - y|_v$, where $|\cdot|_v = \alpha^{v(\cdot)}$ for some $0 < \alpha < 1$. (Recall that a metric space is complete if all Cauchy sequences converge.)*
- *(ii) $\mathcal{O}_K$ is comlete w.r.t. the metrix $d(x, y)$.*
- *(iii) $\mathcal{O}_K$ is a complete local ring.*

If the above conditions are satisfied we say that (K, v) is complete*.*

Proof. For (i) ⇔ (ii), use that $\mathcal{O}_K$ is open in K, that multiplication by π^{-1} is a homeomorphism on K, and that $\{\pi^{-n}\mathcal{O}_K\}_{n \geq 0}$ is an open covering of K, where π is a uniformizer. For (ii) ⇔ (iii), use that $\{\mathfrak{m}^n\}_{n \geq 0}$ is a neighborhood basis of 0 in $\mathcal{O}_K$. □

Let (K, v) be a discretely valued field. The completion $\mathcal{O}_K^\wedge$ of $\mathcal{O}_K$ is again a DVR, and if π is a uniformizer in $\mathcal{O}_K$ then the image of π in $\mathcal{O}_K^\wedge$ is a uniformizer. Let $K^\wedge$ be the fraction field of $\mathcal{O}_K^\wedge$. Then there is a unique discrete valutation $v^\wedge$ on $K^\wedge$ corresponding to the subring $\mathcal{O}_K^\wedge$ under the correspondence (6.1.4.1). We have a natural embedding $K \to K^\wedge$ extending the natural map $\mathcal{O}_K \to \mathcal{O}_K^\wedge$. This map has dense image, and is compatible with the valuations v on K and $v^\wedge$ on $K^\wedge$. The discretely valued field $(K^\wedge, v^\wedge)$ is called the *completion* of (K, v). By construction, $(K^\wedge, v^\wedge)$ is complete. Recall that $\mathcal{O}_K/\mathfrak{m}_K^n \cong \mathcal{O}_K^\wedge/\mathfrak{m}_{K^\wedge}^n$ (which is a general property of the completion of a local ring). In particular, $(K^\wedge, v^\wedge)$ has the same residue field as (K, v).

(Alternatively, one obtains $K^\wedge$ by completing the metric space K in the usual sense as in analysis. One then checks that the metric on $K^\wedge$ comes from a discrete valuation, and that the corresponding valuation ring can be identified wtih $\mathcal{O}_K^\wedge$.)

Example 6.1.7. The completion of $(\mathbb{Q}, v_p)$ is $(\mathbb{Q}_p, v_p)$. The valuation rings are $\mathbb{Z}_{(p)}$ and $\mathbb{Z}_p$ respectively, and the residue fields are both $\mathbb{F}_p$.

Example 6.1.8. The completion of $(\mathbb{F}_q(t), v_t)$ is the Laurent series field $\mathbb{F}_q((t)) = \left\{\sum_{i \geq n} a_i t^i \mid n \in \mathbb{Z}, a_i \in \mathbb{F}_q\right\}$. The valutation v_t extends to $\mathbb{F}_q((t))$ as follows. For each $f = \sum a_i t^i \in \mathbb{F}_q((t))$, $v_t(f)$ is the least i such that $a_i \neq 0$. The valuation rings in $\mathbb{F}_q(t)$ and $\mathbb{F}_q((t))$ are $\mathbb{F}_q[t]$ and $\mathbb{F}_q[[t]]$ respectively. The residue fields are both $\mathbb{F}_q$.

6.1.9. *Local fields.*

Definition 6.1.10. By a *non-archimedean local field*, we mean a complete discretely valued field whose residue field is finite.

There are also archimedean local fields, which turn out to be just $\mathbb{R}$ and $\mathbb{C}$. We shall not pay too much attention to them.

To simplify the language, we simply say "local fields" when we mean non-archimedean local fields.

Lemma 6.1.11. *Let (K, v) be a discretely valued field whose reside field k is finite. Then $\mathfrak{m}_K^n$ is a finite-index subgroup of $\mathcal{O}_K$. The index is $|k|^n$.*

Proof. For each $n \in \mathbb{Z}_{\geq 1}$, we have a short exact sequence

$$1 \longrightarrow \mathfrak{m}_K^n/\mathfrak{m}_K^{n+1} \longrightarrow \mathcal{O}_K/\mathfrak{m}_K^{n+1} \longrightarrow \mathcal{O}_K/\mathfrak{m}_K^n \longrightarrow 1.$$

The term $\mathfrak{m}_K^n/\mathfrak{m}_K^{n+1}$ is a 1-dimensional k-vector space. (Use that $\mathfrak{m}_K$ is principal.) Also $\mathcal{O}_K/\mathfrak{m}_K^1 = k$. Hence by induction each $\mathcal{O}_K/\mathfrak{m}_K^n$ is a finite ring, whose cardinality is $|k|^n$. □

Now let (K, v) be a discretely valued field with finite reside field. We know that $\{\mathfrak{m}_K^n\}_{n\geq 1}$ form a neighborhood basis of 0 in $\mathcal{O}_K$. By the above lemma, each $\mathfrak{m}_K^n$ is an open subgroup of finite index. Therefore the natural map

$$\mathcal{O}_K \longrightarrow \mathcal{O}_K^{\wedge} = \varprojlim_{n\in\mathbb{Z}_{\geq 1}} \mathcal{O}_K/\mathfrak{m}_K^n$$

can be identified with the natural map from the topological group $\mathcal{O}_K$ to its profinite completion. Hence $\mathcal{O}_K$ is complete if and only if $\mathcal{O}_K$ is profinite. We conclude that if (K, v) is a local field, then $(\mathcal{O}_K, +)$ is profinite (and hence compact), and $(K, +)$ is locally profinite (and hence locally compact).

Conversely, by similar considerations, every discretely valued field that is locally compact is a local field ([Ser79, §II.1]).

7. Lecture 7, 2/16/2021

7.1. Recall of local fields, continued.

7.1.1. *Structure of* $(K, +)$ *and* $(K^\times, \times)$. Let (K, v) be a discretely valued field, with residue field k.

Inside $(K, +)$, we have open subgroups

$$K \supset \mathcal{O}_K \supset \mathfrak{m}_K \supset \mathfrak{m}_K^2 \supset \cdots \supset \mathfrak{m}_K^n \supset \cdots$$

They form a neighborhood basis of 0. The successive quotients $\mathfrak{m}_K^n/\mathfrak{m}_K^{n+1}$ are all 1-dimensional k-vecotr spaces, for all $n \geq 0$.

After fixing a uniformizer π, we have an (topological) isomorphism

$$\mathbb{Z} \times \mathcal{O}_K^\times \xrightarrow{\sim} (K^\times, \times), \quad (n, x) \mapsto \pi^n x.$$

Let $U = \mathcal{O}_K^\times$, and $U_n = 1 + \mathfrak{m}_K^n$ for $n \geq 1$. Then inside U we have open subgroups

$$U \supset U_1 \supset U_2 \supset \cdots \supset U_n \supset \cdots$$

which form an open neighborhood basis of 1. We have group isomorphisms $U/U_1 \cong k^\times$, and $U_n/U_{n+1} \cong \mathfrak{m}_K^n/\mathfrak{m}_K^{n+1}$ induced by $x \mapsto x - 1$. In particular, $U_n/U_{n+1} \cong k$.

If (K,v) is assumed to be complete, then by definition

$$\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\mathfrak{m}_K^n,$$

i.e., the group structure of $\mathcal{O}_K$ is determined by the quotients $\mathcal{O}_K/\mathfrak{m}_K^n$, which are successive extensions of copies of k. If we further assume that (K,v) is a local field (i.e., k is finite), then U is profinite since it is compact (because $U = \mathcal{O}_K - \mathfrak{m}_K$ is a closed subset of $\mathcal{O}_K$) Hausdorff and 1 has a neighborhood basis consisting of open subgroups (i.e., the U_n's). It follows that

$$U \cong \varprojlim_n U/U_n.$$

In this case we also know that $K^\times \cong \mathbb{Z} \times U$ is a locally profinite group.

Finally, when we assume (K,v) is complete and is of **characteristic zero**, there exists n (which depends on K) such that the exponential map

$$x \longmapsto \sum_{m\geq 0} x^m/m!$$

defines an isomorphism of topological groups

$$(\mathfrak{m}_K^n, +) \xrightarrow{\sim} (U_n, \times).$$

(Here we need n to be sufficiently large for the exponential series and the logarithmic series to converge on $\mathfrak{m}_K^n$ and U_n respectively.) This restricts to an isomorphism $\mathfrak{m}_K^{n'} \xrightarrow{\sim} U_{n'}$ for all $n' \geq n$. Note that the exponential map does not make sense when $\mathrm{char}(K) > 0$, as $1/n!$ does not exists when $\mathrm{char}(K)|n$.

Lemma 7.1.2. *Let (K,v) be a complete discretely valued field of characteristic zero. Then every finite index subgroup of $(\mathcal{O}_K, +)$ is open, and every finite index subgroup of $K^\times$ is open.*

Proof. Let H be a subgroup of $\mathcal{O}_K$ of index $j \in \mathbb{Z}_{\geq 1}$. Then H contains $j\mathcal{O}_K = \mathfrak{m}_K^{v(j)}$, which is an open subgroup of $\mathcal{O}_K$. Here when writing $v(j)$ we view j as an element of $\mathcal{O}_K$. Since $j \neq 0$ in $\mathcal{O}_K$ (because $\mathrm{char}(K) = 0$), we have $0 \leq v(j) < \infty$. Since H contains an open subgroup of $\mathcal{O}_K$, it is open itself.

Now let H be a subgroup of $K^\times$ of index $j \in \mathbb{Z}_{\geq 1}$. Fix a uniformizer π, and identify $K^\times$ with $\pi^{\mathbb{Z}} \times U$. Then H contains $(K^\times)^j \cong \pi^{j\mathbb{Z}} \times U^j$. It suffices to show that $j\mathbb{Z} \times U^j$ is open inside $\mathbb{Z} \times U$. Since $\mathbb{Z}$ is discrete, we only need to show that U^j is open in U. Find n large enough such that $(U_n, \times) \cong (\mathfrak{m}_K^n, +)$. Then we have a topological isomorphism $(U_n, \times) \cong (\mathcal{O}_K, +)$. Under this isomorphism U_n^j corresponds to $j\mathcal{O}_K = \mathfrak{m}_K^{v(j)}$, which is open in $\mathcal{O}_K$.[6] Hence U_n^j is open in U_n. Now $U^j \supset U_n^j$, and U_n^j is open in U_n which is also open in U. Therefore U^j is open in U, as desired. □

[6] Note that the exponents in the notations U_n^j and $\mathfrak{m}_K^{v(j)}$ have different meanings: U_n^j is the subgroup of U_n consisting of the j-th poweres, whereas $\mathfrak{m}_K^{v(j)}$ is the ideal of $\mathcal{O}_K$ generated by the $v(j)$-fold products of elements of $\mathfrak{m}_K$, or equivalently $\mathfrak{m}_K^{v(j)} = \pi^{v(j)}\mathcal{O}_K$.

7.1.3. *Series expansion.* Let (K, v) be a local field, or more generally a complete discretely valued field. Then an infinite series $\sum_{n\geq 0} a_n$ in K converges (w.r.t. the absolute value $|x| = \alpha^{v(x)}$, where $0 < \alpha < 1$) if and only if $v(a_n) \to +\infty$. Algebraically, the sum of this series can be understood as follows. Up to dropping finitely many terms, we may assume that $a_n \in \mathcal{O}_K$ for all n. Then inside each $\mathcal{O}_K/\mathfrak{m}_K^l$, the images of a_n's are almost all zero, since for almost all n we have $v(a_n) \geq l$. Let $\gamma_n \in \mathcal{O}_K/\mathfrak{m}_K^l$ be the sum of the images of all a_n's, which is a finite sum. Then $(\gamma_n)_n$ is an element of $\varprojlim_n \mathcal{O}_K/\mathfrak{m}_K^n$. By completeness this inverse limit is isomorphic to $\mathcal{O}_K$ itself, so $(\gamma_n)_n$ corresponds to an element $\gamma \in \mathcal{O}_K$. This γ is equal to $\sum a_n$.

From now on we assume that (K, v) is a local field. If we fix a uniformizer $\pi \in K$, then a series of the form $\sum_{n\geq m} a_n\pi^n$, where $m \in \mathbb{Z}$ and $a_n \in \mathcal{O}_K^\times$, converges. We can represent an arbitrary element of K by such a series, where a_n are required to be *Teichmüller representatives*, which we recall as follows.

Let k be the residue field, and let p be the characteristic of k. The surjective homomorphism $\mathcal{O}_K^\times \to k^\times$ has a unique multiplicative section $x \mapsto [x]$, called the *Teichmüller section* or *Teichmüller lift.* Concretely, for each $x \in k^\times$, we define $[x]$ to be

$$\lim_{n\to+\infty} y_n^{p^n}, \tag{7.1.3.1}$$

where $y_n \in \mathcal{O}_K^\times$ is an arbitrary lift of $x^{p^{-n}} = \sqrt[p^n]{x} \in k^\times$. (Note that $x \mapsto x^p$ is an automorphism of $k^\times$, so it makes sense to take p-th roots.) The image of $[\cdot]$ is precisely the set of $(q-1)$-th roots of unity in $\mathcal{O}_K^\times$, where $q = |k|$.

Exercise 7.1.4. Show that the limit (7.1.3.1) converges by checking that $(y_n^{p^n})$ is a Cauchy sequence. Also show that the limit is independent of the choices of y_n. Show that $[\cdot]$ is indeed a multiplicative section of $\mathcal{O}_K^\times \to k^\times$. Finally, show that any other multiplicative section of $\mathcal{O}_K^\times \to k^\times$ must equal $[\cdot]$.

Example 7.1.5. Let $K = \mathbb{Q}_5$. The Teichmüller lift of $\bar{4} \in \mathbb{F}_5$ is $-1 \in \mathbb{Z}_5$.

Remark 7.1.6. The map $[\cdot]$ is additive if and only if $\mathrm{char}(K) > 0$. In this chase $\mathrm{char}(K) = \mathrm{char}(k) = p$, and $[\cdot]$ extends to a field embedding $k \to K$.

Proposition 7.1.7. *Let (K, v) be a local field. Fix a uniformizer π. For each $y \in K^\times$, there is a unique sequence $(a_n)_{n\geq v(y)}$ where each $a_n \in \{0\} \cup [k^\times] \subset \{0\} \cup \mathcal{O}_K^\times$ such that*

$$y = \sum a_n\pi^n.$$

This is called the Teichmüller expansion of y with respect to π.

Proof. Exercise. □

Remark 7.1.8. If $\mathrm{char}(K) > 0$, we have seen that the subset $\{0\} \cup [k^\times]$ is in fact a subfield of K isomorphic to k. In this case the Teichmüller expansion gives a field isomorsphim $K \cong k((t)), \pi \mapsto t$, where $k((t))$ is formal Laurent series field. The valuation v on K corresponds to the valuation v_t on $k((t))$.

Remark 7.1.9. If L is a complete discretely valued field whose residue field l is of characteristic 0, then there is still a unique multiplicative section of $\mathcal{O}_L^\times \to l^\times$, and this section extends to a field embedding $l \to L$. We again have an isomorphism $L \cong l((t))$. In this course we will not study such fields.

Remark 7.1.10. Let (K, v) be a local field with $\mathrm{char}(K) = 0$. Suppose $y, z \in K^\times$ have Teichmüller expansions $\sum a_n\pi^n$ and $\sum b_n\pi^n$ respectively. Then we have $y + z = \sum(a_n + b_n)\pi^n$, but this is in general not the Teichmüller expansion of $y + z$. If π can be and is taken to be p (i.e., K is "absolutely unramified"), then the coefficients of the Teichmüller expansion of $y + z$ is given by certain universal polyonimals called Witt polynomials evaluated at $(a_n, b_n)_n$. There is a similar story for multiplying two Teichmüller expansions. See [Ser79, §§II.5, II.6] for more details.

7.2. **Extensions of local fields.**

Theorem 7.2.1. *Let (K, v) be a complete discretely valued field, and let E/K be a finite extension of fields. Then there is a unique discrete valuation w on E and a unique $e \in \mathbb{Z}_{\geq 1}$ (called the* ramification index*) such that*

$$w(x) = ev(x), \quad \forall x \in K.$$

(In other words, w is the unique discrete valuation on E that extends v up to scaling.) Moreover, (E, w) is complete, $\mathcal{O}_E$ is the integral closure of $\mathcal{O}_K$ in E, and the residue field $\mathcal{O}_E/\mathfrak{m}_E$ is an extension of $\mathcal{O}_K/\mathfrak{m}_K$ of degree $f = [E : K]/e$. In fact we have the following formula for w:

$$w(y) = v(N_{E/K}(y))/f, \quad \forall y \in E.$$

Proof. See [Ser79, §II.2]. □

By the theorem, every finite extension of a local field has the canonical structure of a non-archimedan local field. When we consider a finite extension of local fields E/K, it is always understood that the discrete valuations on E and K are related as in the theorem.

Fact 7.2.2. *Every local field is isomorphic to a finite extension of $\mathbb{Q}_p$ (if the characteristic is zero), or isomorphic to $\mathbb{F}_q((t))$ for some finite field $\mathbb{F}_q$ (if the characteristic is positive).*

8. Lecture 8, 2/23/2021

8.1. **Unramified extensions.** Let (K, v) be a local field, with residue field k. Recall that a finite extension E/K is called *unramified*, if it is separable and the ramification index $e = 1$, i.e., E/K is separable and a uniformizer in K stays to be a uniformizer in E. In this case, E/K is Galois, and the natural homomorphism $\mathrm{Gal}(E/K) \to \mathrm{Gal}(k_E/k)$ is an isomorphism. (Here k_E denotes the residue field of E.) Let $n = [E : K] = [k_E : k]$. We always identify $\mathrm{Gal}((k_E/k)$ with $\mathbb{Z}/n\mathbb{Z}$, where $\bar{1} \in \mathbb{Z}/n\mathbb{Z}$ corresponds to the Frobenius $x \mapsto x^{|k|}$ in $\mathrm{Gal}(k_E/k)$. The corresponding generator of $\mathrm{Gal}(E/K)$ is again callled the Frobenius, usually denoted by σ.

Fact 8.1.1 (See [Ser79, §III.5]). *The natural functor*

$$\{\text{finite unramified extensions of } K\} \longrightarrow \{\text{finite extensions of } k\},$$
$$E \longmapsto k_E$$

is an equivalence of categories. Here the morphisms in the two categories are K-algebra maps and k-algebra maps respectively. Moreover, if E/K is a finite unramified extension and L/K is an arbitrary finite extension, then the set of K-algebra maps $E \to L$ is in natural bijection with the set of k-algebra maps $k_E \to k_L$.

Let L/K be a finite extension. By Fact 8.1.1, subextensions of L/K that are unramified over K are in bijection with subextensions of k_L/k. The one corresponding to k_L is the maxmal unramified extension of K inside L.

If we fix a separable closure K^s of K, then it follows easily from Fact 8.1.1 that for each $n \in \mathbb{Z}_{\geq 1}$ there is a unique unramified extension K_n/K of degree n inside K^s. (The uniqueness boils down to the fact that in a fixed extension of finite fields, there is at most one subextension of each given degree.) We have

$$K_n \subset K_m$$

whenever $n|m$. Let

$$K^{\mathrm{ur}} = \bigcup_{n\geq 1} K_n.$$

This is a field extension of K inside K^s such that every unramified extension of K inside K^s is contained in K^{ur}.

Then the discrete valuation v on K extends to a discrete valuation on K^{ur} (but K^{ur} is not complete). The residue field of K^{ur} is an algebraic closure $\bar{k}$ of k. The extension K^{ur}/K is Galois, and $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ is topologically isomorphic to $\mathrm{Gal}(\bar{k}/k) \cong \widehat{\mathbb{Z}}$. Under this identification, the image of $1 \in \mathbb{Z}$ in $\widehat{\mathbb{Z}}$ corresponds to the Frobenius $\sigma \in \mathrm{Gal}(K^{\mathrm{ur}}/K)$, i.e., the element σ which restricts to the Frobenius in every $\mathrm{Gal}(K_n/K)$.

Denote by G_K the infinite Galois grouip $\mathrm{Gal}(K^s/K)$. Under the Galois correspondence, K^{ur}/K corresponds to a closed subgroup of G_K, denoted by I_K, called the *inerta group* of K. This can also be built from finite inertia groups as follows. For each finite Galois extension L/K inside K^s, we have the inertia group $I(L/K) \subset \mathrm{Gal}(L/K)$ corrresponding to the maximal unramified extension of K inside L. Under the map $G_K \to \mathrm{Gal}(L/K)$, I_K maps to $I(L/K)$. This induces a map

$$I_K \longrightarrow \varprojlim_L I(L/K)$$

where the inverse limit is taken over all finite Galois extensions L/K inside K^s. This map is a topological isomorphism.

By Galois theory we have a short exact sequence

$$1 \longrightarrow I_K \longrightarrow G_K \longrightarrow \mathrm{Gal}(K^{\mathrm{ur}}/K) \cong \widehat{\mathbb{Z}} \longrightarrow 1.$$

8.2. **The Local Reciprocity.**

8.2.1. *Maximal abelian extension.* Let E/K be a separable extension of fields. Given any two finite abelian (i.e., finite Galois with abelian Galois group) extensions $L_1/K, L_2/K$ inside E, the compositum L_1L_2/K is still finite abelian. The compositum of all such extensions is called the *maximal abelian extension* of K in E. This is in general infinite over K.

We often fix a separable closure K^s of K. Then we write K^{ab} for the maximal abelian extension of K inside K^s.

Exercise 8.2.2. The natural map $\mathrm{Gal}(K^s/K) \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ identifies $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ with the maximal Hausdorff abelian quotient of $\mathrm{Gal}(K^s/K)$. The kernel is the closure of the derived subgroup of $\mathrm{Gal}(K^s/K)$.

From now on we fix a local field K, and fix a separable closure K^s. All finite separable extensions of K are assumed to be inside K^s. Note that $K^{\mathrm{ab}} \supset K^{\mathrm{ur}}$. We now state the first main theorem of local class field theory.

Theorem 8.2.3 (Local Reciprocity). *There exists a unique homomorphism*

$$\phi_K : K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

satisfying the following conditions. For every subextension L/K inside K^{ab}, we write $\phi_{L/K}$ for the composite map $K^\times \xrightarrow{\phi_K} \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K)$.

(i) For any uniformizer $\pi \in K$, the image of π under $\phi_{K^{\mathrm{ur}}/K} : K^\times \to \mathrm{Gal}(K^{\mathrm{ur}}/K)$ is the Frobenius σ.
(ii) Let L/K be a finite abelian extension (always assumed to be inside the fixed K^s, and hence inside K^{ab}). Then $\phi_{L/K}$ is surjective, and its kernel is $N_{L/K}(L^\times)$. In particular, we have an induced isomorphism : $K^\times/\mathrm{N}_{L/K}(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K)$, which we still denote by $\phi_{L/K}$.

Note that every $x \in \mathcal{O}_K^\times$ can be written as $x = \pi/\pi'$ for two different uniformizers π and π'. It immediately follows from condition (i) that $x \in \ker \phi_{K^{\mathrm{ur}}/K}$. Thus $\phi_{K^{\mathrm{ur}}/K}$ factors as $K \xrightarrow{v} \mathbb{Z} \xrightarrow{f} \mathrm{Gal}(K^{\mathrm{ur}}/K)$. If we identify $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ with $\widehat{\mathbb{Z}}$ as usual, then clearly $f : \mathbb{Z} \to \mathrm{Gal}(\mathfrak{K}^{\mathrm{ur}}/K)$ is just the canonical map $\mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}}$.

8.3. Consequences of Local Reciprocity.

Definition 8.3.1. A *norm subgroup* of $K^\times$ is a subgroup of the form $\mathrm{N}_{L/K}(L^\times)$ for some finite abelian extension L/K. For brevity, we write N_L for $N_{L/K}(L^\times)$ when K is fixed.

Remark 8.3.2. By a result called the "norm limitation theorem", the set of norm subgroups of $K^\times$ does not change if in the definition we allow arbitrary finite extensions L/K. For the moment we will not use this result.

Corollary 8.3.3. *Every norm subgroup is of finite index in $K^\times$.*

Proof. If L/K is a finite abelian extension, then the index of N_L in $K^\times$ is equal to the size of $\mathrm{Gal}(L/K)$, which is finite. □

Corollary 8.3.4. *Every subgroup of $K^\times$ containing a norm subgroup is itself a norm subgroup.*

Proof. Say N is a subgroup of $K^\times$ containing a norm subgroup N_L. Recall that we have the isomorphism $\phi_{L/K} : K^\times/N_L \xrightarrow{\sim} \mathrm{Gal}(L/K)$. Let $\mathrm{Gal}(L/L')$ be the image of N in $\mathrm{Gal}(L/K)$. Then N is equal to the kernel of $\phi_{L'/K} : K^\times \to \mathrm{Gal}(L'/K)$, which is $N_{L'}$. □

Corollary 8.3.5. *Let L, L' be finite abelian extensions of K (inside K^{ab}). The following statements hold.*

(i) $L \subset L'$ if and only if $N_L \supset N_{L'}$.
(ii) $N_{L\cdot L'} = N_L \cap N_{L'}$.

Proof. By $N_{L'/K} = N_{L/K} \circ N_{L'/L}$, we have the "only if" in (i). This also implies the containment $\subset$ in (ii). For the containment $\supset$ in (ii), use that N_L is the kernel of $\phi_{L/K} : K^\times \to \mathrm{Gal}(L/K)$, and similarly for $N_{L'}$ and $N_{L\cdot L'}$. It suffices to show that the map $\mathrm{Gal}(L \cdot L'/K) \to \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K)$ is injective. But this is true by general Galois theory.

We now use (ii) to prove the "if" in (i). By (ii) and by the assumption $N_L \supset N_{L'}$, we have $N_{L \cdot L'} = N_{L'}$. But then $[L \cdot L' : K] = [L' : K]$, and so $L \subset L'$. □

9. Lecture 9, 2/25/2021

9.1. **Consequences of Local Reciprocity, continued.**

Corollary 9.1.1. *The map $L \mapsto N_L$ is an inclusion-reversing bijection from the set of finite abelian extensions of K (inside K^{ab}) to the set of norm subgroups of $K^\times$.*

Proof. By part (i) of Corollary 8.3.5, this map is inclusion reversing and injective. Surjectivity follows from the definition of norm groups. □

Corollary 9.1.2. *Let L, L' be finite abelian extensions of K. Then $N_{L \cap L'} = N_L \cdot N_{L'}$.*

Proof. We know that $L \cap L'$ is the largest abelian extension of K contained in both L and L'. On the other hand $N_L \cdot N_{L'}$ is a norm subgroup (since it contains a norm subgroup), and it is clearly the smallest norm subgroup containing both N_L and $N_{L'}$. The assertion then follows from Corollary 9.1.1. □

Lemma 9.1.3. *Let L/K be a finite extension of K (not necessarily abelian). If $N_{L/K}(L^\times)$ is of finite index in $K^\times$, then it is open.*

Proof. We know that $\mathcal{O}_L^\times$ is compact, so $N_{L/K}(\mathcal{O}_L^\times)$ is closed in $K^\times$. Also note that $N_{L/K}(\mathcal{O}_L^\times) = N_{L/K}(L^\times) \cap \mathcal{O}_K^\times$. (For $x \in L$ we have $v_K(N_{L/K}(x)) = f v_L(x)$.) Therefore $N_{L/K}(\mathcal{O}_L^\times)$ is closed and of finite index in $\mathcal{O}_K^\times$, and hence open in $\mathcal{O}_K^\times$. It follows that $N_{L/K}(L^\times)$ contains an open subgroup of $K^\times$, and is therefore itself open. □

Remark 9.1.4. In fact, by the norm limitation theorem, we have $N_{L/K}(L^\times) = N_{E/K}(E^\times)$, where E is the maximal abelian extension of K in L. Hence $N_{L/K}(L^\times)$ is automatically of finite index in $K^\times$.

Remark 9.1.5. If K has characteristic zero, then the lemma is superfluous as every finite index subgroup of $K^\times$ is open.

Corollary 9.1.6. *Every norm subgroup of $K^\times$ is open and of finite index.*

Note that the six Corollaries 8.3.3, 8.3.4, 8.3.5, 9.1.1, 9.1.2, 9.1.6 are all consequences of the existence of the local Artin map ϕ_K. We haven't used the uniqueness.

9.2. **The Local Existence Theorem.**

We now state the second main theorem of local class field theory.

Theorem 9.2.1 (Local Existence Theorem)**.** *The norm subgroups of $K^\times$ are precisely the open finite index subgroups of $K^\times$.*

Corollary 9.2.2. *The map $L \mapsto N_{L/K}(L^\times)$ is a bijection from the set of finite abelian extensions of K to the set of open finite index subgroups of $K^\times$.*

Proof. Combine Corollary 9.1.1 with Theorem 9.2.1. □

Corollary 9.2.3. *The map ϕ_K induces an isomorphism from the profinite completion of $K^\times$ to* $\mathrm{Gal}(K^{\mathrm{ab}}/K)$.

Proof. Exercise. (Use that $\mathrm{Gal}(K^{\mathrm{ab}}/K) = \varprojlim_L \mathrm{Gal}(L/K)$, where L runs through the finite abelian extensions of K.) □

Example 9.2.4. Let p be an odd prime. The degree p-extensions of $\mathbb{Q}_p$ are all abelian, and they correspond to index p (and open, which is automatic) subgroups of $\mathbb{Q}_p^\times$. We have

$$\mathbb{Q}_p^\times \cong p^{\mathbb{Z}} \times \mathbb{Z}_p^\times \cong \mathbb{Z} \times \mathbb{F}_p^\times \times (1+\mathbb{Z}_p) \cong \mathbb{Z} \times \mathbb{F}_p^\times \times \mathbb{Z}_p,$$

where we used the exponential map for $(1+\mathbb{Z}_p, \times) \cong (\mathbb{Z}_p, +)$. The index p subgroups of $\mathbb{Q}_p^\times$ are in bijection with the index p subgroups of $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^p$, and the latter is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Thus we have $p+1$ such extensions. Among them, one is unramified, and the other p extensions are totally ramified. Note that for $m = (p^p-1)p^2$, we have $\mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) \cong \mathbb{Z}/p\mathbb{Z} \times (\mathbb{Z}/p^2\mathbb{Z})^\times \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Denoting this group by G, we have $G/G^p \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Therefore inside $\mathbb{Q}_p(\zeta_m)$ we find all the $p+1$ extensions of $\mathbb{Q}_p$ of degree p.

Example 9.2.5. Recall that K_n/K denotes the unramified extension of degree n. Let π be a uniformizer of K. The map $\phi_{K_n/K} : K^\times \to \mathrm{Gal}(K_n/K)$ sends π to σ which has order n, and sends $\mathcal{O}_K^\times$ to 1. Hence the kernel of it is $\pi^{n\mathbb{Z}}\mathcal{O}_K^\times$. (Note that this subgroup of $K^\times$ is independent of the choice of π.) We conclude that $N_{K_n} = \pi^{n\mathbb{Z}}\mathcal{O}_K^\times$. After some reduction steps, this fact boils down to the surjectivity of the norm map between two finite fields, which can be proved elementarily. (For instance, use that the non-zero elements of a finite field form a cyclic group.)

9.3. The field K_π.

In the following discussion, we assume the existence of the local Artin map ϕ_K as in Theorem 8.2.3. Fix a uniformizer $\pi \in K^\times$. Let $K_\pi \subset K^{\mathrm{ab}}$ be the fixed field of $\phi_K(\pi) \in \mathrm{Gal}(K^{\mathrm{ab}}/K)$. The next lemma gives an intrinsic characterization of K_π.

Lemma 9.3.1. *The field K_π is the union of finite abelian extensions L/K such that $\pi \in N_L$.*

Proof. We know that K_π is the union of finite abelian extensions L/K such that π lies in the kernel of $\phi_{L/K} : K^\times \to \mathrm{Gal}(L/K)$. But the last condition is equivalent to $\pi \in N_L$. □

Remark 9.3.2. If L/K is any finite Galois extension such that $\pi \in N_{L/K}(L^\times)$, then L/K must be totally ramified. To see this, use the formula $v_K(N_{L/K}(x)) = f(L/K)v_L(x), \forall x \in L^\times$. Since the left hand side can assume 1, we must have $f(L/K) = 1$.

Recall that $K^\times$ has a tower of subgroups

$$K^\times \supset U \supset U_1 \supset U_2 \supset \cdots,$$

where $U = \mathcal{O}_K^\times$ and $U_n = 1 + \mathfrak{m}_K^n$. For any choice of uniformizer π, we have $K^\times = \pi^{\mathbb{Z}} \times U$.

Proposition 9.3.3. *Assume the existence of ϕ_K as in the Local Reciprocity Theorem (Theorem 8.2.3), and assume the Local Existence Theorem (Theorem 9.2.1). Choose a uniformizer $\pi \in K$. The following statements hold.*

(i) For each $n \geq 1$, let $K_{\pi,n}$ be the finite abelian extension of K characterized by the condition

$$N_{K_{\pi,n}} = \pi^{\mathbb{Z}} \times U_n.$$

(This exists by the Local Existence Theorem, since $\pi^{\mathbb{Z}} \times U_n$ is an open finite index subgroup of $K^\times$.) Then $K_\pi = \bigcup_n K_{\pi,n}$.

(ii) We have $K^{\mathrm{ab}} = K_\pi K^{\mathrm{ur}}$.

Proof. Clearly $K_{\pi,n} \subset K_\pi$. To show that $K_\pi = \bigcup_n K_{\pi,n}$, we need to show that an arbitrary finite abelian extension L/K satisfying $\pi \in N_L$ is contained in $K_{\pi,n}$ for some n. We know that N_L is open, so it must contain an open neighborhood of π in $K^\times$. But $(\{\pi\} \times U_n)_{n\geq 1}$ form a neighborhood basis of π. Hence N_L contains $\{\pi\} \times U_n$ for suitable n. Since N_L is a group, it also contains $N_{K_{\pi,n}}$. But then we have $L \subset K_{\pi,n}$.

We now show that $K^{\mathrm{ab}} = K_\pi K^{\mathrm{ur}}$. For this we need to show that an arbitrary finite abelian extension L/K is contained in $K_{\pi,n}K^{\mathrm{ur}}$ for some n. We know that N_L is an open finite index subgroup of $K^\times$. Since N_L is open, it must contain U_n for some n. Since N_L is of finite index in $K^\times$, it cannot be contained inside U, i.e., there exists $x \in N_L$ with $v(x) \neq 0$. Write $x = \pi^{v(x)}y$, with $y \in U$. Note that a suitable power of y lies in U_n, since $[U : U_n] < \infty$. Hence after raising x to a power we may assume that $x = \pi^{v(x)}y$ with $y \in U_n$. But then N_L contains $\pi^{v(x)}$. Therefore

$$N_L \supset \pi^{v\mathbb{Z}} \times U_n$$

for some integers $v, n \geq 1$. Note that

$$\pi^{v\mathbb{Z}} \times U_n = (\pi^{v\mathbb{Z}} \times U) \cap (\pi^{\mathbb{Z}} \times U_n) = N_{K_v} \cap N_{K_{\pi,n}} = N_{K_{\pi,n}\cdot K_v}.$$

(Recall that K_v denotes the degree v unramified extension of K.) Hence $L \subset K_{\pi,n} \cdot K_v \subset K_{\pi,n} \cdot K^{\mathrm{ur}}$. □

10. Lecture 10, 3/2/2021

10.1. **The Local Existence Theorem, continued.** In the proof of Proposition 9.3.3, we essentially showed the following fact: Let U be a profinite group. Then every open finite index subgroup of $\mathbb{Z} \times U$ contains $v\mathbb{Z} \times U'$ for some $v \geq 1$ and some open subgroup $U' \subset U$. In particular, the profinte completion of $\mathbb{Z} \times U$ is $\widehat{\mathbb{Z}} \times U$. Using this, we can give a more conceptual (but essentially the same) proof of the fact $K^{\mathrm{ab}} = K_\pi K^{\mathrm{ur}}$ using infinite Galois theory and Corollary 9.2.3 as follows. (Note that Corollary 9.2.3) still assumes the Local Existence Theorem.)

Alternative proof of Proposition 9.3.3 (ii). Since $K^\times \cong \pi^{\mathbb{Z}} \times U$ as a topological group and U is profinite, the profinite completion $\widehat{K^\times}$ of $K^\times$ is isomorphic to $\pi^{\widehat{\mathbb{Z}}} \times U$ (by the preceding paragraph). When we identify this with $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ as in Corollary 9.2.3, the subgroup $\pi^{\widehat{\mathbb{Z}}}$ corresponds to $\mathrm{Gal}(K^{\mathrm{ab}}/K_\pi)$ and the subgroup U corresponds to $\mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}})$. Since the intersection of these two subgroups is trvial, we have $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{ur}}$. □

Note that U is a canonical subgroup of $\widehat{K^\times}$, but $\pi^{\widehat{\mathbb{Z}}}$ is not canonical as it depends on π. (Rather, we have a canonical quotient map $\widehat{K^\times} \to \widehat{\mathbb{Z}}$ induced by $v : K^\times \to \mathbb{Z}$.) This corresponds to the fact that K^{ur}/K is canonical and K_π/K is not.

From the above alternative proof, we easily see that ϕ_K restricts to an isomorphism of topological groups $U \xrightarrow{\sim} \mathrm{Gal}(K_\pi/K)$.

Proposition 10.1.1. *Assume the Local Existence Theorem. Then ϕ_K in the Local Reciprocity Theorem is unique.*

Proof. Suppose ϕ'_K is another choice. For any uniformizer $\pi \in K$, use ϕ_K to define K_π, and use ϕ'_K to define K'_π. Note that $K_\pi = K'_\pi$, since they are both the union of finite abelian extensions L/K such that $\pi \in N_L$. We have $K^{\mathrm{ab}} = K_\pi K^{\mathrm{ur}}$. We have $\phi_K(\pi)$ acts via the identity on K_π, and acts via σ on K^{ur}. Ditto for $\phi'_K(\pi)$. Therefore $\phi_K(\pi) = \phi'_K(\pi)$. Now note that the set of all possible uniformizers of K actually generate $K^\times$. (Clearly $K^\times$ is generated by one uniformizer and U, but any element of U is a ratio of two uniformizers.) Hence $\phi_K = \phi'_K$. □

Remark 10.1.2. In the above proof, we needed the Local Existence Theorem only for the knowledge that $K = K_\pi K^{\mathrm{ur}}$.

10.2. **Idea of Lubin–Tate theory.**

Lubin–Tate theory gives a self-contained explicit construction of $K_{\pi,n}$, for any uniformizer π of K. It also constructs an isomorphism $U \xrightarrow{\sim} \mathrm{Gal}(K_\pi/K)$, as predicted in by the Local Reciprocity Theorem and Local Existence Theorem.

Example 10.2.1. Let $K = \mathbb{Q}_p, \pi = p$. Then $K_{\pi,n} = \mathbb{Q}_p(\zeta_{p^n})$.

The construction of $\mathbb{Q}_p(\zeta_{p^n})$ can be interpreted as follows. Let $\Lambda = \bigcup_L \mathfrak{m}_L$, where L runs through finite extensions of $\mathbb{Q}_p$ inside $\overline{\mathbb{Q}}_p$. For each L, we transport the multiplicative group structure on $1 + \mathfrak{m}_L$ to a group structure on $\mathfrak{m}_L$ via the bijection $1 + \mathfrak{m}_L \xrightarrow{\sim} \mathfrak{m}_L, x \mapsto x - 1$. Then for $x, y \in \mathfrak{m}_L$, we have

$$x +' y = (1 + x)(1 + y) - 1 = x + y + xy$$

where $+'$ is the group operation. We can think of $+'$ as a deformation of the usual group operation $+$ on $\mathfrak{m}_L$, where the difference is only in "higher order terms". Since the formula defining $+'$ is independent of L, we get a group structure $+'$ on Λ. Let

$$\Lambda_n = \left\{ x \in \Lambda \mid \underbrace{x +' \cdots +' x}_{p^n \text{ times}} = 0 \right\}$$

Then $\mathbb{Q}_p(\zeta_{p^n}) = \mathbb{Q}_p(\Lambda_n)$.

The $\mathbb{Z}$-module Λ_n is a free $\mathbb{Z}/p^n\mathbb{Z}$-module of rank 1. The action of $\mathrm{Gal}(\mathbb{Q}_p(\Lambda_n)/\mathbb{Q}_p)$ on Λ_n gives rise to a homomorphism $\mathrm{Gal}(\mathbb{Q}_p(\Lambda_n)/\mathbb{Q}_p) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$. Taking the inverse limit in n we get a homomorphism $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \to \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times$. This is an isomorphism, and the inverse ismorpism $\mathbb{Z}_p^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty}), \mathbb{Q}_p)$ is equal to the *negative* of the local Artin map.

How do we generalize this to construct $K_{\pi,n}$ for general K and π? We define the set Λ in the same way, and we need a group structure $+'$ on Λ (which depends on π) deforming the usual $+$. This time, $x +' y$ will no longer be given by a polynomial in x, y. It is rather a power series in x, y of the form

$$x + y + \text{higher degree terms},$$

and the coefficients are in $\mathcal{O}_K$. Lubin and Tate figured out the suitable power series to be used here, and this is called the *Lubin–Tate formal group law.* One of the key features in the construction is that $\mathcal{O}_K$-acts on this group via endomorphisms, Thus we have a ring homomorphism $\mathcal{O}_K \to \mathrm{End}(\Lambda, +')$, which we will denote by $a \mapsto [a]$. Define

$$\Lambda_n := \{x \in \Lambda \mid [\pi]^n x = 0\}$$

The Λ_n is an $\mathcal{O}_K$-submodule of Λ, and it is in fact an $\mathcal{O}_K/\pi^n$-module. It turns out to be a free $\mathcal{O}_K/\pi^n$-module of rank 1. Define

$$K_{\pi,n} = K(\Lambda_n).$$

Then we have a natural homomorphism $\mathrm{Gal}(K_{\pi,n}/K) \to (\mathcal{O}_K/\pi^n)^\times$. Take $K_\pi = \bigcup_n K_{\pi,n}$. The map $\mathrm{Gal}(K_\pi/K) \to \varprojlim_n (\mathcal{O}_K/\pi^n)^\times = \mathcal{O}_K^\times$ is an isomorphism, and its inverse is the negative of the restriction of the local Artin map.

11. Lecture 11, 3/4/2021

11.1. **Formal group laws.** We closely follow [Mil20, §I.2]

11.1.1. *Formal power series.* Fix a commutative ring A with 1. (We will set $A = \mathcal{O}_K$.) Let $A[[X_1, \cdots, X_n]]$ be the formal power series ring, and let $A[[X_1, \ldots, X_n]]_+$ be the subset consisting of power series whose constant terms are zero.

Let $f(X_1, \cdots, X_n) \in A[[X_1, \cdots, X_n]]$, and let $g_1(Y_1, \cdots, Y_m), \cdots g_n(Y_1, \cdots, Y_m) \in A[[Y_1, \cdots, Y_m]]$. The substitution

$$f(g_1(Y_1, \cdots, Y_m), \cdots, g_n(Y_1, \cdots, Y_m))$$

does not make sense in general. For instance, if $f = f(X_1) = X_1 + X_1^2 + \cdots, g = g(X_1) = 1$, then $f(g)$ does not make sense. It makes sense whenever each g_i has zero constant term, i.e., $g_i \in A[[Y_1, \cdots, Y_m]]_+$. In this case, we have $f(g_1, \cdots, g_n) \in A[[Y_1, \cdots, Y_m]]$. If we know that $f \in A[[X_1, \cdots, X_n]]_+$ in addition, then $f(g_1, \cdots, g_n) \in A[[Y_1, \cdots, Y_m]]_+$.

Lemma 11.1.2. *(i) Let $f \in A[[T]], g, h \in A[[T]]_+$. The two interpretations of $f(g(h))$ are the same.*

(ii) Let $f \in A[[T]]_+$. Then f admits a composition right-inverse $g \in A[[T]]_+$, i.e., $f(g(T)) = T$, if and only if the linear term of f is aT for some $a \in A^\times$. In this case we also have $g(f(T)) = T$.

Proof. Part (i) is obvious, so we only prove (ii). Write $f(T) = \sum_{i\geq 1} a_i T^i$. If $f(g(T)) = T$, then

$$a_1 g(T) + a_2 g(T)^2 + \cdots = T. \qquad (11.1.2.1)$$

The linear coefficient on the LHS is divisible by a_1, so $a_1 \in R^\times$.

Conversely, assume $a_1 \in R^\times$. Write $g = \sum_{i\geq 1} b_i T^i$. We solve for b_i consecutively from (11.1.2.1). The linear coefficient of both sides is $a_1 b_1 = 1$, so $b_1 = a_1^{-1}$. The quadratic coefficient is $a_1 b_2 + a_2 b_1^2 = 0$, from which $b_2 = -a_1^{-1}(a_2 b_1^2)$. In general, the n-th coefficient is $a_1 b_n +$ polynomial in $(a_2, \cdots, a_n, b_1, \cdots, b_{n-1}) = 0$, so we can solve for b_n.

Now assume $f(g(T)) = T$, and we show that $g(f(T)) = T$. Clearly the linear coefficient of g is also in $A^\times$. Thus there exists $h \in A[[T]]_+$ such that $g(h(T)) = T$. Then $f(T) = f(g(h(T))) = h(T)$, so $g(f(T)) = g(h(T)) = T$. □

Exercise 11.1.3. Part (ii) of the above lemma can be viewed as a version of the Inverse Function Theorem. State and prove a multi-variable version.

Example 11.1.4. Assume that A contains $\mathbb{Q}$. Then we can define

$$f(T) = \log(1+T) = -\sum_{n\geq 1} (-T)^n/n,$$

and

$$g(T) = e^T - 1 = \sum_{n\geq 1} T^n/n!.$$

We have $f(g(T)) = g(f(T)) = T$.

11.1.5. *Axioms for a formal group law.*

Definition 11.1.6. A *formal group law* over A is a power series $F(X,Y) \in A[[X,Y]]_+$ satisfying certain axioms. For $f, g \in A[[Z_1, \cdots, Z_n]]_+$, we write $f +_F g$ for $F(f,g) \in A[[Z_1, \cdots, Z_n]]_+$. (In particular, we write $X +_F Y$ for $F(X,Y)$ itself.) The axioms are as follows:

(i) (Associativity.) We have

$$X +_F (Y +_F Z) = (X +_F Y) +_F Z \in A[[X,Y,Z]]_+.$$

(i.e., $F(X, F(Y,Z)) = F(F(X,Y),Z)$.)

(ii) (Commutativity.) We have

$$X +_F Y = Y +_F X \in A[[X,Y]]_+.$$

(i.e., $F(X,Y) = F(Y,X)$.)

(iii) (Identity.) We have

$$X +_F 0 = X.$$

(i.e., $F(X,0) = X$.)

(iv) (Inverse.) There exists $i(X) \in A[[X]]_+$ such that

$$X +_F i(X) = 0.$$

(i.e., $F(X, i(X)) = 0$.)

We immediately observe that by axioms (ii) and (iii), we have

$$F(X,Y) = X + Y + \text{higher degree terms},$$

and none of these higher degree terms is a pure power of X or Y. By this and by axiom (iv), we have

$$i(X) = -X + \text{higher degree terms}.$$

We think of $+_F$ as a deformation of the usual $+$, and think of $i(X)$ as a deformation of the usual $-$.

Exercise 11.1.7. Show that $i(X)$ is uniquely determined by $F(X,Y)$.

Lemma 11.1.8. *Suppose $F \in A[[X,Y]]_+$ is of the form $F(X,Y) = X+Y+$ higher degree terms, and suppose F satisfies axiom (i). Then F satisfies axiom (iii).*

Proof. Let $f(X) = F(X,0)$. We need to show that $f(X) = X$. Note that $F(0,0) = 0$. In axiom (i), taking $Y = Z = 0$, we get $f(X) = F(f(X),0) = f(f(X))$. Now note that $f(X) = X+$ higher degree terms, so there exists a composition inverse g of f. Then $f(X) = g(f(f(X))) = g(f(X)) = X$. □

Remark 11.1.9. What we call "formal group laws" are actually the commutative one-dimensional formal group laws. Only such formal group laws will appear in the course.

Example 11.1.10. The additive formal group law $F(X,Y) = X + Y$. In this case clearly $i(X) = -X$. This makes sense over $A = \mathbb{Z}$, and hence over arbitrary A.

Example 11.1.11. The multiplicative formal group law $F(X,Y) = (X+1)(Y+1)-1$. We can compute the inversion $i(X)$ as follows. We have

$$(X+1)(i(X)+1) - 1 = 0,$$

so

$$i(X) + 1 = (X+1)^{-1} = \sum_{n\geq 0}(-X)^n.$$

We get

$$i(X) = \sum_{n\geq 1}(-X)^n.$$

This makes sense over $A = \mathbb{Z}$, and hence over arbitrary A.

Example 11.1.12. For simplicity assume A is a field. One can get a formal group law over A from an elliptic curve E over A, by expanding the group law of E near the identity. See [Sil09, Chapter IV] for more details.

Example 11.1.13. Let $f, g \in A[[T]]_+$ be composition-inverses of each other. Suppose $F(X,Y)$ is a formal group law. Then $g(F(f(X), f(Y)))$ is another formal group law. For instance, $f(T) = \log(1+T)$, $g(T) = e^T - 1$, and $F(X,Y) = X+Y$. Then

$$g(F(f(X), f(Y))) = g(f(X)+f(Y)) = g(\log((1+X)(1+Y))) = (1+X)(1+Y)-1.$$

This is the multiplicative formal group law.

11.1.14. *Homomorphisms and endomorphisms.* Let F and G be two formal group laws over A. By a homomorphism $F \to G$, we mean a power series $h(T) \in A[[T]]_+$ satisfying

$$h(X +_F Y) = h(X) +_G h(Y),$$

or equivalently $h(F(X,Y)) = G(h(X), h(Y))$. If we have homomorphisms $h : F \to G$ and $h' : G \to H$, then we define their composition to be $h'(h(T))$, which is a homomorphism $F \to H$.

Example 11.1.15. The power series $h(T) = \log(1+T)$ is a homomorphism from the multiplicative formal group to the additive formal group.

The endomorphisms of a formal group law F form a ring, where addition is given by $(h_1(T), h_2(T)) \mapsto h_1(T) +_F h_2(T)$, and multiplication is given by composition. We denote this ring by $\mathrm{End}(F)$. This ring has multiplicative identity, given by $h(T) = T$.

Appendix. Formal group laws as group objects in a category. We explain how to define formal group laws as group objects in a certain category of *coordinated formal Lie varieties.* Throughout we fix a commutative ring A with 1.

11.1.16. *Coordinated formal Lie varieties.* The category $\mathcal{L}$ of *coordinated formal Lie varieties* is defined as follows. The objects are labeled by the positive integers: $L^1, L^2, \cdots$. We think of L^n as an infinitesimal neighborhood of the origin in A^n. A morphism from L^n to L^m is an m-tuple of elements of $A[[X_1, \cdots, X_n]]_+$. Here is the informal way to think of it: The morphism given by $(f_1, \cdots, f_m)$ sends the point

$$(X_1, \cdots, X_n) \in L^n$$

to the point

$$(f_1(X_1, \cdots, X_n), \cdots, f_m(X_1, \cdots, X_n)) \in L^m.$$

If $(f_1, \cdots, f_m)$ is a morphism $L^n \to L^m$, and $(g_1, \cdots, g_k)$ is a morphism $L^m \to L^k$, we get the composite morphism $L^n \to L^k$ given by

$$(g_1(f_1, \cdots, f_m), \cdots, g_k(f_1, \cdots, f_m)).$$

This definition of composition indeed satisfies the usual associativity requirement. The identity map $L^n \to L^n$ is given by

$$(X_1, \cdots, X_n).$$

For technical convenience we also include an object L^0 in the category $\mathcal{L}$. By definition, there is a unique homomorphism $L^n \to L^0$ for each n. Also, there is a unique homomorphism $L^0 \to L^n$ given by the n-tuple $(0, \cdots, 0)$. Note that L^0 is simultaneously an initial object and a final object in $\mathcal{L}$. For arbitrary m and n, we define the composite morphism $L^m \to L^0 \to L^n$ to be $(0, \cdots, 0)$.

The category $\mathcal{L}$ admits finite products. Given m, n, define

$$\mathrm{pr}_{\leq m} = (X_1, X_2, \cdots, X_m) : L^{m+n} \longrightarrow L^m$$

and

$$\mathrm{pr}_{>m} = (X_{m+1}, X_{m+2}, \cdots, X_{m+n}) : L^{m+n} \longrightarrow L^n.$$

It is easy to see that $(L^{m+n}, \mathrm{pr}_{\leq m}, \mathrm{pr}_{>m})$ is the product of L^m and L^n. In fact, given morphisms

$$f = (f_1, \cdots, f_m) : L^k \longrightarrow L^m$$

and

$$g = (g_1, \cdots, g_n) : L^k \longrightarrow L^n,$$

we define $f \times g : L^k \to L^{m+n}$ by

$$f \times g = (f_1, \cdots, f_m, g_1, \cdots, g_n).$$

Then $f \times g$ is the unique morphism $L^k \to L^{m+n}$ such that $\mathrm{pr}_{\leq m} \circ (f \times g) = f$ and $\mathrm{pr}_{>m} \circ (f \times g) = g$.

11.1.17. *Group objects.* Let $\mathcal{C}$ be a category that contains a final object denoted by pt (the notation stands for "point"). We assume that $\mathcal{C}$ admits finite products. By *a group object in* $\mathcal{C}$, we mean an object G in $\mathcal{C}$ together with a group structure on $\mathrm{Hom}(S, G)$ for each $S \in \mathcal{C}$. This should satisfy the property that whenever $f : S \to T$ is a morphism, the induced map $f^* : \mathrm{Hom}(T, G) \to \mathrm{Hom}(S, G)$ is a homomorphism. Similarly we define an abelian group object.

Given a group object G, we can produce a multiplication map $m : G \times G \to G$, an identity section $e : pt \to G$, and an inversion map $i : G \to G$ as follows. In $\mathrm{Hom}(G \times G, G)$, we have two elements pr_1 and pr_2. We define m to be $\mathrm{pr}_1 \cdot \mathrm{pr}_2$, where $\cdot$ is the group operation on $\mathrm{Hom}(G \times G, G)$. Similarly, we define e to be the neutral element in the group $\mathrm{Hom}(pt, G)$, and define i to be the inverse element of $\mathrm{id}_G \in \mathrm{Hom}(G, G)$ with respect to the group structure on $\mathrm{Hom}(G, G)$.

It is easy to see that the group structure on $\mathrm{Hom}(S, G)$, for any S, can be recovered from m, e, i. For instance, given $f_1, f_2 \in \mathrm{Hom}(S, G)$, we recover $f_1 \cdot f_2$ as the composition

$$S \xrightarrow{(f_1, f_2)} G \times G \xrightarrow{m} G.$$

In fact, we can equivalently define a group object by just specifying m, e, i satisfying certain axioms that are analogous to the usual axioms for a group.

11.1.18. *Formal group laws.*

Definition 11.1.19. By an n-dimensional commutative formal group law over A, we mean an abelian group object in $\mathcal{L}$ supported on L^n. In our course, a "formal group law" simply refers to a 1-dimensional commutative formal group law.

To give a one-dimensional commutative formal group law, it is the same as to give morphisms $m : L^1 \times L^1 = L^2 \to L^1, e : L^0 \to L^1$, and $i : L^1 \to L^1$ satisfying certain axioms. Note that m is just given by a power series in two variables $F(X_1, X_2) \in A[[X_1, X_2]]_+$. The morphism e must be given by (0), and the morphism i is given by a power series in one variable $i(X_1) \in A[[X_1]]_+$. We shall write $F(X_1, X_2)$ also as $X_1 +_F X_2$. The general axioms for an abelian group object satisfed by m, e, i translate to the axioms in Definition 11.1.6.

11.1.20. *Homomorphism and endomorphisms.* In a general category (with a final object pt and admitting finite products), a *homomorphism* between two group objects G_1, G_2 is a morphism $h : G_1 \to G_2$ that is compatible with the multiplication maps $G_1 \times G_1 \to G_1$ and $G_2 \times G_2 \to G_2$, and compatible with the identity sections $pt \to G_1$ and $pt \to G_2$.

In our situation, a homomorphism between two formal group laws F and G should be a morphism $L^1 \to L^1$, i.e., an element $h \in A[[X]]_+$, that is compatible with the multiplication maps, i.e.,

$$h(X +_F Y) = h(X) +_G h(Y),$$

or equivalently $h(F(X, Y)) = G(h(X), h(Y))$. The composition of homomorphisms $h : F \to G$ and $h' : G \to H$ is simply given by $h'(h(X))$. (This is how we compose two morphisms $L^1 \to L^1$.)

The endomorphisms of a formal group F form a ring, where $+$ is the "pointwise addition" and $\times$ is the composition. We denote this ring by $\mathrm{End}(F)$. For $h_1, h_2 \in \mathrm{End}(F)$, the pointwise sum $h_1 + h_2$ is really just

$$h_1 +_F h_2 = F(h_1(X), h_2(X)) \in \mathrm{End}(F).$$

The ring structure on $\mathrm{End}(F)$ is characterized categorically as follows. For each $L^n \in \mathcal{L}$, we have a natural map from $\mathrm{End}(F)$ to $\mathrm{End}(\mathrm{Hom}(L^n, F))$, where the latter is the usual endomorphism ring of the abelian group $\mathrm{Hom}(L^n, F)$. We require this map to be a ring homomorphism. This condition uniquely characterizes the ring structure on $\mathrm{End}(F)$. (This essentially follows from Yoneda's Lemma.)

12. Lecture 12, 3/9/2021

12.1. **Lubin–Tate formal group laws.** We now construct certain formal group laws called *Lubin–Tate formal group laws.* We follow [Mil20, §I.2]. The original source is [LT65], which is extremely well written and readable.

From now on, we fix a non-archimedian local field K and fix a uniformizer π. Let q be the cardinality of the residue field. Let $A = \mathcal{O}_K$.

Definition 12.1.1. Let $\mathcal{F}_\pi$ denote the set of $f(X) \in A[[X]]$ satisfying

(i) $f(X) = \pi X + O(X^2)$.
(ii) $f(X) \equiv X^q \mod \pi$.

Example 12.1.2. We have $f(X) = \pi X + X^q \in \mathcal{F}_\pi$.

Example 12.1.3. Assume $K = \mathbb{Q}_p$ and $\pi = p$. Let $f(X) = (1+X)^p - 1$. Then $f(X) = pX + \sum_{i=2}^{p-1} \binom{p}{i} X^i + X^p$, where all the binomial coefficients are divisible by p. Hence $f \in \mathcal{F}_p$.

Lemma 12.1.4 (Key Lemma)**.** *Let $f, g \in \mathcal{F}_\pi$. Let $n \geq 1$. Then there exists $\phi \in A[[X_1, \cdots, X_n]]_+$ such that*

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

Moreover, ϕ is uniquely determined by its linear part, which can be an arbitrary linear form $a_1X_1 + \cdots a_nX_n$.

Proof. We write X for $(X_1, \cdots, X_n)$, and write $g(X)$ for $(g(X_1), \cdots, g(X_n))$. Suppose we want the linear part of ϕ to be some arbitrary $\phi_1(X) = a_1X_1 + \cdots a_nX_n$. We prove by induction on $r \geq 1$ that there exists a degree r polynomial $\phi_r(X) = \phi_r(X_1, \cdots, X_n)$, whose linear part is ϕ_1, satisfying

$$f(\phi_r(X)) = \phi_r(g(X)) + O(X^{r+1}). \tag{12.1.4.1}$$

Here $O(X^{r+1})$ denotes a sum of monomials in $X_1, \cdots, X_n$ of degrees $\geq r+1$. Moreover, we require that $\phi_{r+1} - \phi_r$ is a homogeneous polynomial of degree $r+1$.

If $r = 1$, take ϕ_r to be ϕ_1. Then (12.1.4.1) holds because on both sides the linear part is $\sum_i \pi a_i X_i$.

Suppose ϕ_r has been constructed. Set $\phi_{r+1}(X) = \phi_r(X) + Q(X)$, where $Q(X)$ is a homogeneous polynomial of degree $r+1$, to be determined. We have

$$\begin{aligned} f(\phi_{r+1}(X)) = f(\phi_r(X) + Q(X)) &= f(\phi_r(X)) + f'(\phi_r(X))Q(X) + O(X^{2r+2}) \\ &= f(\phi_r(X)) + \pi Q(X) + O(X^{r+2}). \end{aligned}$$

(We used that $f'(X) = \pi + O(X)$ and $Q(X) = O(X^{r+1})$.) On the other hand, we have

$$\phi_{r+1}(g(X)) = \phi_r(g(X)) + Q(g(X)) = \phi_r(g(X)) + Q(g(X_1), \cdots, g(X_n))$$
$$= \phi_r(g(X)) + Q(\pi X_1, \cdots, \pi X_n) + O(X^{r+2}) = \phi_r(g(X)) + \pi Q(X) + O(X^{r+2}).$$

(We used that Q is homogeneous of degree $r+1$.) Thus we want

$$Q(\pi X_1, \cdots, \pi X_n) - \pi Q(X_1, \cdots, X_n) = f(\phi_r(X)) - \phi_r(g(X)) + O(X^{r+2}).$$

Note that LHS is $(\pi^{r+1} - \pi)Q(X)$, so we want

$$Q(X) = \frac{f(\phi_r(X)) - \phi_r(g(X))}{\pi^{r+1} - \pi} + O(X^{r+2}). \tag{12.1.4.2}$$

Note that the numerator in the fraction is $O(X^{r+1})$, so as long as we can show that the fraction has coefficients in $A = \mathcal{O}_K$ we can (and must) take $Q(X)$ to be the homogeneous degree $r+1$ part of the fraction. Since the denominator $\pi^{r+1} - \pi$ has valuation 1 in $\mathcal{O}_K$, we only need

$$f(\phi_r(X)) \equiv \phi_r(g(X)) \mod \pi.$$

But $f(\phi_r(X)) \equiv \phi_r(X)^q \equiv \phi_r(X_1^q, \cdots, X_r^q) \equiv \phi_r(g(X_1), \cdots, g(X_r)) \mod \pi$, so we are done.

Now define ϕ to be $\lim_{r\to\infty} \phi_r \in A[[X]]$. (Note that this limit is well defined, because ϕ_r agrees with ϕ_{r+1} in all degree $\leq r$ terms.) Then we have

$$f(\phi(X)) = f(\phi_r(X)) + O(X^{r+1}) = \phi_r(g(X)) + O(X^{r+1}) = \phi(g(X)) + O(X^{r+1}),$$

where for the first equality we used that $f \in A[[X]]_+$, and for the last equality we used that $g \in A[[X]]_+$. Since this holds for all r, we have $f(\phi_r(X)) = \phi_r(g(X))$.

Finally, we show the uniqueness of ϕ when the linear part is fixed. Suppose ϕ solves the problem in the lemma. Define ϕ_r to be the truncation of ϕ where we throw away terms of degree larger than r. Then ϕ_r must satisfy (12.1.4.1), and also $\phi_{r+1} - \phi_r$ is homogeneous of degree r. As the proof above shows, the difference $Q = \phi_{r+1} - \phi_r$ must be determined by (12.1.4.2). Thus each ϕ_r, and hence ϕ itself, is uniquely determined by the linear part ϕ_1. □

Proposition 12.1.5. *For every $f \in \mathcal{F}_\pi$, there exists a unique formal group law F_f over A such that $f \in \mathrm{End}(F_f)$.*

Proof. Let $F = F_f$ be the unique power series in $A[[X,Y]]_+$ whose linear part is $X + Y$, satisfying

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

(The existence and uniqueness of F follows from the Key Lemma applied to $n = 2$ and $f = g$.) We only need to show that F is a formal group law.

To show associativity, let $G_1(X,Y,Z) = F(F(X,Y),Z)$ and $G_2(X,Y,Z) = F(X, F(Y,Z))$. Then G_1 and G_2 both have linear part $X + Y + Z$. We have

$$f(G_1(X,Y,Z)) = f(F(F(X,Y),Z)) = F(f(F(X,Y)), f(Z)) = F(F(f(X), f(Y)), f(Z))$$

$$= G_1(f(X), f(Y), f(Z)).$$

Similarly, $f(G_2(X,Y,Z)) = G_2(f(X), f(Y), f(Z))$. By the uniqueness in the Key Lemma, we have $G_1 = G_2$.

Similary, we have $F(X,Y) = F(Y,X)$, because $F(X,Y)$ and $G(X,Y) := F(Y,X)$ both have linear part $X+Y$, and they both solve the problem in the Key Lemma with $f = g$.

By Lemma 11.1.8, we have $F(X, 0) = X$.

Finally, we show the existence of $i(X) \in A[[X]]_+$ such that $F(X, i(X)) = 0$. Let $i(X)$ be the unique element of $A[[X]]_+$ whose linear part is $-X$ and such that $f(i(X)) = i(f(X))$. Set $G(X) = F(X, i(X))$. Then

$$f(G(X)) = f(F(X, i(X))) = F(f(X), f(i(X))) = F(f(X), i(f(X))) = G(f(X)).$$

Note that the linear part of G is 0. On the other hand, clearly 0 is a power series in one variable with linear part 0 such that it intertwines with f (since $f(0) = 0$). Thus the uniqueness in the Key Lemma implies that $G = 0$. □

13. Lecture 13, 3/11/2021

13.1. **Lubin–Tate formal group laws, continued.**

Example 13.1.1. Let $K = \mathbb{Q}_p$ and $\pi = p$. We have $f(X) = (1+X)^p - 1 \in \mathcal{F}_p$. Note that f is an endomorphism of the multiplicative formal group law $F(X,Y) = (X+1)(Y+1)-1$. Hence $F = F_f$.

For every $f \in \mathcal{F}_\pi$, the formal group law F_f is called a *Lubin–Tate formal group law.* The set of all Lubin–Tate formal group laws (corresponding to all choices of π and $f \in \mathcal{F}_\pi$) are characterized as those formal group laws that admit an endomorphism whose linear coefficient is a uniformizer in $\mathcal{O}_K$ and whose reduction modulo $\mathfrak{m}_K$ is the Frobenius $X \mapsto X^q$. (Over $\mathbb{F}_q$, every formal group law admits an endomorphism of the form $h(X) = X^q$.)

We continue fixing a uniformizer $\pi \in K$, and writing A for $\mathcal{O}_K$.

Proposition 13.1.2. *Let $f, g \in \mathcal{F}_\pi$. For each $a \in A$, there is a unique homomorphism $[a]_{g,f} : F_f \to F_g$ whose linear coefficient is a and which intertwines the endomorphisms $f \in \mathrm{End}(F_f)$ and $g \in \mathrm{End}(F_g)$, i.e., $g \circ [a]_{g,f} = [a]_{g,f} \circ f$.*

Proof. Let h be the unique element of $A[[X]]_+$ whose linear part is aX and satisfying $h(f(X)) = g(h(X))$. We see that the intertwining condition forces $[a]_{g,f}$ to be equal to h. We only need to show that h is indeed a homomorphism $F_f \to F_g$, i.e., $h(F_f(X,Y)) = F_g(h(X), h(Y))$. Call the two sides $G_1(X,Y)$ and $G_2(X,Y)$. Then G_1 and G_2 both have linear part $aX + aY$. We then compute

$$G_1(f(X), f(Y)) = h(f(X) +_{F_f} f(Y)) = h(f(X +_{F_f} Y)) = g(h(X +_{F_f} Y)) = g(G_1(X,Y)).$$

Similarly, $G_2(f(X), f(Y)) = g(G_2(X,Y))$. Hence $G_1 = G_2$ by the uniqueness in the key lemma. □

Proposition 13.1.3. *Let $f, g, h \in \mathcal{F}_\pi$. Let $a, b \in A$. We have $[a]_{g,f} +_{F_g} [b]_{g,f} = [a+b]_{g,f}$, and $[a]_{g,f} \circ [b]_{f,h} = [ab]_{g,h}$. Moreover $[1]_{f,f}$ is the identity on F_f, and $[\pi]_{f,f} = f$.*

Proof. This follows easily from the uniqueness in the previous proposition. □

Corollary 13.1.4. *Let $f \in \mathcal{F}_\pi$. There is a unique (injective) ring homomorphism $[\cdot] : a \to \mathrm{End}(F_f)$ such that for each $a \in \mathcal{O}_K$, the linear coefficient of $[a]$ is a, and such that $[\pi] = f$.*

Proof. For the existence, take $[\cdot]$ to be $[\cdot]_{f,f}$. This is indeed a ring homomorphism sending π to f, by the previous proposition. For the uniqueness, note that $[a]$ must intertwine with $[\pi] = f$ since $\mathcal{O}_K$ is a commutative ring. Hence we must have $[a] = [a]_{f,f}$. □

By the above discussion, for each $f \in \mathcal{F}_\pi$ we obtain a canonical ring homomorphism $A \to \mathrm{End}(F_f), a \mapsto [a]_{f,f}$. To simply notation we write $[a]_f$ for it. This means that F_f has the canonical structure of a *formal A-module.* For $f, g \in \mathcal{F}_\pi$, we have a canonical A-linear isomorphism $[1]_{g,f} : F_f \xrightarrow{\sim} F_g$. (Here A-linearity follows from $[a]_{g,g} \circ [1]_{g,f} = [a]_{g,f} = [1]_{g,f}[a]_{f,f}$.) We can characterize $[1]_{g,f}$ as the unique A-linear isomorphism whose linear coefficient is 1. Thus we know that the formal A-module F_f is independent of the choice of f up to canonical isomorphism. (However, the isomorphism class of the A-module F_f depends on π.)

Example 13.1.5. Let $K = \mathbb{Q}_p, \pi = p, f = (1+X)^p - 1 \in \mathcal{F}_p$. We know that F_f is the multiplicative formal group law $F_f(X,Y) = (1+X)(1+Y) - 1$. What is $[a]_{f,f}$ for $a \in \mathbb{Z}_p$? We know that it is the unique power series $h(X)$ with linear coefficient a satisfying $f(h(X)) = h(f(X))$. Take

$$h(X) = (1+X)^a := \sum_{m \geq 0} \binom{a}{m} X^m,$$

where $\binom{a}{m}$ is by definition

$$a(a-m) \cdots (a-m+1)/m! \in \mathbb{Q}_p.$$

We first need to check that these coefficients $\binom{a}{m}$ are actually in $\mathbb{Z}_p$. To see this, let $(a_i)_i$ be a sequence in $\mathbb{N}$ converging to a in $\mathbb{Z}_p$. (For instance, take $a_i \in \mathbb{N}$ to be any postive lift of the image of a in $\mathbb{Z}_p/p^i\mathbb{Z}_p \cong \mathbb{Z}/p^i\mathbb{Z}$.) Then the sequence $\binom{a_i}{m}$ converges to $\binom{a}{m}$ inside $\mathbb{Q}_p$. It follows that $\binom{a}{m} \in \mathbb{Z}_p$ since each $\binom{a_i}{m} \in \mathbb{N} \subset \mathbb{Z}_p$ and since $\mathbb{Z}_p$ is closed in $\mathbb{Q}_p$. Now the linear coefficient of h is indeed a, and the desired identity $f(h(X)) = h(f(X))$ boils down to the fact that

$$((1+X)^a)^p = ((1+X)^p)^a = (1+X)^{ap}.$$

Again, this is true because it is true when a is replaced by a_i.

13.2. **Lubin–Tate extensions.** The discrete valuation v on K extends uniquely to a (non-discrete) valuation on the algebraic closure $\bar{K}$, which we now explain. If L/K is a finite extension, then recall that there is a unique discrete valuation w on L such that $w(x) = e(L/K)v(x), \forall x \in K$. Now for $x \in L$, we define $v(x)$ to be

$$w(x)/e(L/K).$$

In this way we have extended the function $v : K \to \mathbb{Z} \cup \{+\infty\}$ to a function $v : L \to \mathbb{Q} \cup \{+\infty\}$. Since w is unique, it is easy to see that this extension of v is also unique, i.e., it must be given by $v(x) = w(x)/e(L/K)$. By writing $\bar{K}$ as a union of such finite extensions L/K, we obtain a function

$$v : \bar{K} \longrightarrow \mathbb{Q} \cup \{+\infty\},$$

which extends $v : K \to \mathbb{Z} \cup \{+\infty\}$ and is independent of any choices. The well definedness of v on $\bar{K}$ follows from the uniqueness of the extension of v to each finite extension L/K.

We define

$$\Lambda = \left\{x \in \bar{K} \mid v(x) > 0\right\}.$$

Then Λ is the union of $\mathfrak{m}_L$, where L runs over all finite extensions of K (inside $\bar{K}$).

We now fix a uniformizer $\pi \in K$ and fix $f \in \mathcal{F}_\pi$. We then have the formal group law $F_f \in \mathcal{O}_K[[X,Y]]_+$.

Note that for any $x_1, \cdots, x_n \in \Lambda$ and any $H(X_1, \cdots, X_n) \in \mathcal{O}_K[[X_1, \cdots, X_n]]_+$, the power series $H(x_1, \cdots, x_n)$ converges in Λ. More precisely, if $x_1, \cdots, x_n \in \mathfrak{m}_L$ for some finite extension L/K, then $H(x_1, \cdots, x_n) \in \mathfrak{m}_L$. Indeed, if

$$H(X_1, \cdots, X_n) = \sum_{i_1 \geq 0, \cdots, i_n \geq 0} a_{i_1, \cdots, i_n} X_1^{i_1} \cdots X_n^{i_n}, \quad \text{(with } a_{0,\cdots,0} = 0)$$

then the individual terms of the series $H(x_1, \cdots, x_n)$, namely $a_{i_1,\cdots,i_n} x_1^{i_1} \cdots x_n^{i_n}$, tend to zero in L. Thus the series converges in L. Since all the partial sums are inside $\mathfrak{m}_L$, the limit is also in $\mathfrak{m}_L$ (by the closedness of $\mathfrak{m}_L$ in L).

Thus the formal group law F_f together with the formal A-module structure gives rise to an A-module structure on Λ. We denote this A-module by Λ_f. By definition, the underlying set of Λ_f is just Λ, addition in Λ_f is given by

$$(x, y) \longmapsto F_f(x, y) = x +_{F_f} y, \quad \forall x, y \in \Lambda$$

and scalar multiplication is given by

$$(a, x) \mapsto [a]_f(x), \quad \forall a \in \mathcal{O}_K, x \in \Lambda.$$

(Recall that $[a]_f \in \mathcal{O}_K[[X]]_+$.)

14. Lecture 14, 3/23/2021

14.1. **Lubin–Tate extensions, continued.** Let K be a local field. We continue writing A for $\mathcal{O}_K$. We denote by π a uniformizer in A. Recall that for any $f \in \mathcal{F}_\pi$, we have an A-module Λ_f, whose underlying set is $\Lambda = \{x \in \bar{K} \mid v(x) > 0\}$, and the A-module structure is defined via the formal A-module F_f.

Definition 14.1.1. Let M be an A-module. We denote by M_n the submodule $\{x \in M \mid \pi^n x = 0\}$. Note that the definition of M_n is independent of the choice of the uniformizer π.

For $f, g \in \mathcal{F}_\pi$, we have a canonical A-module isomorphism $\Lambda_f \xrightarrow{\sim} \Lambda_g$ given by $x \mapsto [1]_{g,f}(x)$. In particular, for $x \in \Lambda$, we have $x \in \Lambda_{f,n}$ if and only if $[1]_{g,f}(x) \in \Lambda_{g,n}$. Note that x and $[1]_{g,f}(x)$ generate the same finite extension of K, because whenever $x \in L$ we have $[1]_{g,f}(x) \in L$, for any finite extension L/K, and vice versa (since $x = [1]_{f,g}([1]_{g,f}(x))$). Thus the extension $K(\Lambda_{f,n})/K$ is independent of the choice of f. We denote it by $K_{\pi,n}$.

For instance, we can take $f(X) = X^q + \pi X \in \mathcal{F}_\pi$, and consider the n-fold composition $f^{(n)}(X) = f(f(\cdots f(X)))$, which is a degree q^n polynomial. Then $K_{\pi,n}$ is generated over K by the roots of $f^{(n)}(X)$ inside Λ.

Proposition 14.1.2. *Let $f(X) = X^q + \pi X$. All the roots of $f^{(n)}$ in $\bar{K}$ are in Λ.*

Recall the Newton polygon method to determine valuations of roots.

Theorem 14.1.3 (See [Neu99, §2.6])**.** *Let $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathcal{O}_K[X]$. Define the* Newton polygon *to be the (lower) convex hull of the points $(i, v(a_i))$. Suppose it has k different edges, of horizontal distances $l_1, \cdots, l_k$ and slopes $s_1, \cdots, s_k$. Then among the n roots of f inside $\bar{K}$ (with multiplicities), there are precisely l_j roots α such that $v(\alpha) = -s_j$, for $j = 1, \cdots, k$.*

Example 14.1.4. We say that $f(X) = a_n X^n + \cdots + a_0 \in \mathcal{O}_K[X]$ is Eisenstein if $v(a_n) = 0, v(a_i) > 0$ for $i < n$, and $v(a_0) = 1$. Then the Newton polygon is the straight edge from $(0, 1)$ to $(n, 0)$. Hence all n roots have valuation $1/n$.

Proof of Proposition 14.1.2. The polynomial $f^{(n)}(X)$ is of the form $X^{q^n} + \cdots + \pi^n X$. Moreover, since $f(X) \equiv X^q \mod \pi$, we have $f(f(X)) \equiv f(X)^q \equiv X^{q^2} \mod \pi$, and by induction $f^{(n)}(X) \equiv X^{q^n} \mod \pi$. Hence all the middle coefficients of $f^{(n)}$ have positive valuation. It follows that all the edges in the Newton polygon have strictly negative slopes. Thus all the roots of $f^{(n)}$ in $\bar{K}$ lie in Λ. □

In conclusion, $K_{\pi,n}/K$ is generated by *all* the roots of $f^{(n)}(X)$ in $\bar{K}$, where $f(X) = X^q + \pi X$. In particular, we have

Corollary 14.1.5. *The extension $K_{\pi,n}/K$ is finite and normal.*

Lemma 14.1.6. *For any $f \in \mathcal{F}_\pi$, the set $\Lambda_{f,1}$ has q distinct elements. The map $\pi : \Lambda_f \to \Lambda_f$ (i.e., the map sending $x \in \Lambda$ to $[\pi]_f(x) = f(x) \in \Lambda$) is surjective.*

Proof. The isomorphism class of the A-module Λ_f is independent of f, so we may assume that $f(X) = X^q + \pi X$. For the first statement, we need to show that $f(X)$ has q distinct roots in Λ. We have already seen that all the roots of $f(X)$ in $\bar{K}$ lie in Λ. Since $\deg f = q$, we only need to check that f and f' are coprime. We have $f'(X) = qX^{q-1}+\pi$, so any root α of $f'(X)$ in $\bar{K}$ satisfies $v(q)+(q-1)v(\alpha) = v(-\pi)$, i.e., $v(\alpha) = (1 - v(q))/q - 1$. On the other hand, by a similar computation, every root of $f(X)$ is either zero, or has valuation $1/(q - 1)$. Since $v(q) \neq 0$, we see that f and f' do not have common roots in $\bar{K}$, i.e., they are coprime.

We now prove the second statement. We need to show that for any $\lambda \in \Lambda$, there exists $\alpha \in \Lambda$ such that $f(\alpha) = \lambda$. Namely, the polynomial $f(X)-\lambda = X^q+\pi X - \lambda$ has a root in Λ. Using the Newton polygon, we see that all the roots of this polynomial in $\bar{K}$ have positive valuations. □

15. Lecture 15, 3/25/2021

15.1. Lubin–Tate extensions, continued.

Lemma 15.1.1. *For any $f \in \mathcal{F}_\pi$, the extension $K_{\pi,n}/K$ is separable, and hence Galois in view of Corollary 14.1.5.*

Proof. As usual we may assume that $f = X^q + \pi X$. We prove the lemma by induction on n. For $n = 1$, we have seen that $\Lambda_{f,1}$ is the set of the q distinct roots of $f(X) \in K[X]$. Hence the elements of $\Lambda_{f,1}$ are all separable over K. Now suppose $K_{\pi,n}/K$ is separable. Let $\alpha \in \Lambda_{f,n+1}$. Then $\beta := f(\alpha) \in \Lambda_{f,n}$, and α is a root of $f(X) - \beta \in K_{\pi,n}[X]$. The derivative of this polynomial is again $qX^{q-1} + \pi$, and every root of it has valuation equal to $(1 - v(q))/q - 1 \leq 0$. Hence α is not root of $(f(X) - \beta)'$, and not a multiple root of $f(X) - \beta$. Therefore α is separable over $K_{\pi,n}$. Since $K_{\pi,n}/K$ is separable, we have α is separable over K. □

Proposition 15.1.2. *For any $f \in \mathcal{F}_\pi$ and any $n \geq 1$, the A-module $\Lambda_{f,n}$ is isomorphic to $A/(\pi)^n$. In particular, it has q^n elements.*

Proof. We first show that $\Lambda_{f,n}$ has exactly q^n elements. Consider the short exact sequence

$$0 \to \Lambda_{f,n} \to \Lambda_{f,n+1} \xrightarrow{\pi} \Lambda_{f,n} \to 0.$$

Here, the surjectivity of the last map follows from Lemma 14.1.6. Since we know $\Lambda_{f,1}$ has q elements, the claim follows from induction.

Now by the classification of finitely generated modules over a PID, we have $\Lambda_{f,n} \cong A/(\pi^{m_1}) \oplus \cdots \oplus A/(\pi^{m_k})$ for a unique sequence of integers $m_1 \leq \cdots \leq m_k$. Note that $\Lambda_{f,1}$ is equal to the π-torsion in $\Lambda_{f,n}$. If $k \geq 2$, then $|\Lambda_{f,1}| \geq q^2$, contradicting Lemma 14.1.6. Hence $\Lambda_{f,n} \cong A/(\pi^m)$ for some m. Since it has q^n elements, we have $m = n$. □

As an immediate consequence of the above corollary, the endomorphism ring of the A-module $\Lambda_{f,n}$ is naturally isomorphic to A/π^n, and the automorphism group of the A-module $\Lambda_{f,n}$ is naturally isomorphic to $(A/\pi^n)^\times$. Now $\mathrm{Gal}(K_{\pi,n}/K)$ acts on $\Lambda_{f,n}$ via A-module automorphisms. In fact, the condition that an element $x \in \mathfrak{m}_{K_{\pi,n}}$ lies in $\Lambda_{f,n}$ is expressed in a power series equation in x with coefficients in A. The group $\mathrm{Gal}(K_{\pi,n}/K)$ acts continuously on $\mathfrak{m}_{K_{\pi,n}}$, so it preserves such a power series equation. We thus obtain a homomorphism

$$\rho_{\pi,n} : \mathrm{Gal}(K_{\pi,n}/K) \longrightarrow \mathrm{Aut}_{A\text{-mod}}(\Lambda_{f,n}) \cong (A/\pi^n)^\times.$$

We call it the *Lubin–Tate* homomorphism.

Implicitly, the definition of $\rho_{\pi,n}$ involves the choice of $f \in \mathcal{F}_\pi$, but it is easy to see that $\rho_{\pi,n}$ is in fact indepedent of that choice. The point is that for $f, g \in \mathcal{F}_\pi$, the isomorphism $\Lambda_{f,n} \xrightarrow{\sim} \Lambda_{g,n}$ induced by $[1]_{g,f}$ is $\mathrm{Gal}(K_{\pi,n}/K)$-equivariant, since it is given by a power series with coefficients in K.

Theorem 15.1.3. *The following statements hold.*

(i) The extension $K_{\pi,n}/K$ is totally ramified, of degree $(q-1)q^{n-1}$.
(ii) $\rho_{\pi,n}$ is an isomorphism.
(iii) π is a norm from $K_{\pi,n}$.

Proof. Take $f(X) = X^q - \pi X$. Let π_1 be a non-zero root of $f(X)$ in $\bar{K}$. For $i \geq 2$, inductively choose π_i to be a non-zero root of $f(X) - \pi_{i-1} = 0$ in $\bar{K}$. Using Newton polygons, we have $v(\pi_1) = 1/(q-1)$ and $v(\pi_i) = 1/(q-1)q^{i-1}$ for $i \geq 2$. Note that $\pi_n \in \Lambda_{f,n}$, so we have $\pi_n \in K_{\pi,n}$. Thus $e(K_{\pi,n}/K) \geq (q-1)q^{n-1}$.

Now ρ is clearly injective. Hence $[K_{\pi,n} : K] \leq |(A/\pi^n)^\times| = (q-1)q^{n-1}$. For the last equality, see the exercise below.

Combining the two inequalities, we get (i) (ii).

We now show (iii). Let $g(T) = f(T)/T = T^{q-1}+\pi$, and let $u_n(T) = g(f(\cdots f(T)))$, where f appears $n-1$ times. Then $\deg u_n = (q-1)q^{n-1}$, and

$$u_n(\pi_n) = u_{n-1}(\pi_{n-1}) = \cdots = g(\pi_1) = 0.$$

By part (i) and the fact that $v(\pi_n) = 1/(q-1)q^{n-1}$, we know that π_n has degree $(q-1)q^{n-1}$ over K, and that $K_{\pi,n} = K(\pi_n)$. Hence u_n is the monic minimal polynomial of π_n over K. Thus the norm of $\pi_n \in K_{\pi,n}$ down to K is $(-1)^{\deg u_n}$ times the constant term of u_n, which is π. If $(-1)^{\deg u_n} = 1$ then we are done. Otherwise, $-\pi$ is a norm, and the extension $K_{\pi,n}/K$ has odd degree and therefore -1 is a norm. Hence π is a norm. □

Exercise 15.1.4. Show that $|(A/\pi^n)^\times| = (q-1)q^{n-1}$. Hint: first show that $(A/\pi^n)^\times \cong A^\times/(1+\pi^n A)$.

Exercise 15.1.5. Let $K = \mathbb{Q}_p$ and $\pi = p$. We have $K_{\pi,n} = \mathbb{Q}_p(\zeta_{p^n})$, and the isomorphism $\rho : \mathrm{Gal}(K_{\pi,n}/K) \xrightarrow{\sim} (\mathbb{Z}_p/p^n)^\times = (\mathbb{Z}/p^n)^\times$ is the usual isomorphism, i.e., $\rho^{-1}(\bar{a})$ maps ζ_{p^n} to $\zeta_{p^n}^a$.

16. Lecture 16, 3/30/2021

16.1. **Explicit local reciprocity map.** Fix a uniformizer $\pi \in K$. Recall from Theorem 15.1.3 that the Lubin–Tate homomorphism $\rho_{\pi,n} : \mathrm{Gal}(K_{\pi,n}/K) \to (A/\pi^n)^\times$ is an isomorphism. It will turn out that the **negative** of $\rho_{\pi,n}^{-1}$, which is an isomorphism

$$\begin{aligned}(A/\pi^n)^\times &\xrightarrow{\sim} \mathrm{Gal}(K_{\pi,n}/K),\\ a &\longmapsto (-\rho_{\pi,n}^{-1}(a) : x \mapsto [a^{-1}]_f(x), \forall x \in \Lambda_{f,n})\end{aligned}$$

is induced by the local Artin map $\phi_{K_{\pi,n}/K} : K^\times \xrightarrow{\phi} \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(K_{\pi,n}/K)$. Let

$$K_\pi = \bigcup_n K_{\pi,n}$$

(where the union is inductive), and let

$$K^{\mathrm{LT}} = K_\pi \cdot K^{\mathrm{ur}}.$$

It will enventually turn out that $K^{\mathrm{LT}} = K^{\mathrm{ab}}$, but we cannot use it for now. Since each $K_{\pi,n}/K$ is totally ramified, the fields K_π and K^{ur} are linearly disjoint over K. Thus

$$\mathrm{Gal}(K^{\mathrm{LT}}/K) \cong \mathrm{Gal}(K_\pi/K) \times \mathrm{Gal}(K^{\mathrm{ur}}/K) \cong \varprojlim_n \mathrm{Gal}(K_{\pi,n}/K) \times \widehat{\mathbb{Z}} \cong A^\times \times \widehat{\mathbb{Z}}.$$

Here in the last isomorphism we used ρ to identify $\mathrm{Gal}(K_{\pi,n}/K)$ with $(A/\pi^n)^\times$, and used the (obvious) fact that the natural map $\mathrm{Gal}(K_{\pi,m}/K) \to \mathrm{Gal}(K_{\pi,n}/K)$ corresponds to the natural projection $(A/\pi^m)^\times \to (A/\pi^n)^\times$ when $n \le m$. If we know $K^{\mathrm{LT}} = K^{\mathrm{ab}}$, then we can *define* the local Artin map by the formula

$$K^\times = \pi^{\mathbb{Z}} \times A^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K) \cong A^\times \times \widehat{\mathbb{Z}},$$
$$\pi^b \cdot a \longmapsto (a^{-1}, b).$$

One approach to local class field theory is to try and show $K^{\mathrm{LT}} = K^{\mathrm{ab}}$ directly (using the Hasse–Arf Theorem), and then to define the local Artin map in the above way. We will however not take this approach.

Without knowing $K^{\mathrm{LT}} = K^{\mathrm{ab}}$, we can still use the formula $\pi^b \cdot a \mapsto (a^{-1}, b)$ to define a homomorphism

$$\phi_\pi : K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{LT}}/K).$$

16.2. **Independence of the uniformizer.**

Theorem 16.2.1. *The subfield $K^{\mathrm{LT}} \subset \bar{K}$ is independent of the choice of π. The map ϕ_π is independent of the choice of π.*

The discrete valuation v on K extends to a discrete valuation v on K^{ur}, making K^{ur} a discretely valued field. We know that (K^{ur}, v) is not complete, and denote the completion by $\breve{K}$. The unique extension of v to $\breve{K}$ is again denoted by v. Let $B = \mathcal{O}_{\breve{K}} = \left\{ x \in \breve{K} \mid v(x) \ge 0 \right\}$. The Frobenius $\sigma \in \mathrm{Gal}(K^{\mathrm{ur}}/K)$ extends uniquely to a K-automorphism σ of $\breve{K}$. Then σ preserves v on $\breve{K}$, and in particular acts on B.

Lemma 16.2.2. *The homomorphisms $B \to, b \mapsto b - \sigma(b)$ and $B^\times \to B^\times, b \mapsto b\sigma(b)^{-1}$ are surjective, with kernels A and $A^\times$ respectively. These homomorphisms are often called* Lang isogenies*.*

Proof. Let R be the valuation ring of K^{ur}, whose maximal ideal is πR and residue field is $\bar{k}$, the algebraic closure of the residue field k of K. By the definition of completion we have $B = \varprojlim_n R/\pi^n$. We show by induction that the sequence

$$0 \to A/\pi^n \to R/\pi^n \xrightarrow{f_n} R/\pi^n \to 0 \tag{16.2.2.1}$$

is exact, where $f_n(x) = x - \sigma(x)$. When $n = 1$, the sequence becomes

$$0 \to k \to \bar{k} \xrightarrow{\sigma - 1} \bar{k},$$

which is obviously exact. Assuming the sequence is exact for $n-1$, we can apply the snake lemma to the diagram

$$\begin{tikzcd}
0 \arrow[r] & R/\pi \arrow[r, "\pi^{n-1}"] \arrow[d, "f_1"] & R/\pi^n \arrow[r] \arrow[d, "f_n"] & R/\pi^{n-1} \arrow[r] \arrow[d, "f_{n-1}"] & 0 \\
0 \arrow[r] & R/\pi \arrow[r, "\pi^{n-1}"] & R/\pi^n \arrow[r] & R/\pi^{n-1} \arrow[r] & 0
\end{tikzcd}$$

(The exactness of the two rows is obvious, and the commutativity folows from the fact that $\sigma(\pi) = \pi$.) Then f_n is surjective, and $\ker(f_n)$ is an extension of $\ker(f_{n-1}) = A/\pi^{n-1}$ by $\ker(f_1) = A/\pi$. Thus $\ker(f_n)$ has q^n elements, and since it contains A/π^n it must be equal to A/π^n. We have thus shown that (16.2.2.1) is exact.

Recall the following general fact: Suppose I is directed set, and we have inverse systems $(A_i)_{i\in I}, (B_i)_{i\in I}, (C_i)_{i\in I}$ of abelian groups. For each i, suppose we have a short exact sequence $0 \to A_i \to B_i \to C_i \to 0$, and suppose that the maps $A_i \to B_i$ and $B_i \to C_i$ are compatible with the transition maps. Then we have an exact sequence

$$0 \to \varprojlim_i A_i \to \varprojlim_i B_i \to \varprojlim_i C_i.$$

The last map is surjective when I is countable and $(A_i)_{i\in I}$ is Mittag-Leffler, i.e., for each $i \in I$ the system $\mathrm{im}(A_j \to A_i)$ of subgroups of A_i stabilizes as j gets sufficiently large. Applying this to our situation, from (16.2.2.1) we get a short exact sequence

$$0 \to A \to B \xrightarrow{\sigma-1} B \to 0,$$

since the inverse system $(A/\pi^n)_n$ (with the obvious transition maps) is Mittag-Leffler.

The case with $B^\times \to B^\times, b \mapsto b\sigma(b)^{-1}$ is proved similarly. We replace A/π^n and R/π^n by $A^\times/(1+\pi^n A)$ and $R^\times/(1+\pi^n R)$ respectively. Note that $A^\times \cong \varprojlim_n A^\times/(1+\pi^n A)$, and $B^\times \cong \varprojlim_n (R/\pi^n)^\times \cong \varprojlim_n R^\times/(1+\pi^n R)$. (The isomorphism $(R/\pi^n)^\times \cong R^\times/(1+\pi^n R)$ is similar to the one in Exercise 15.1.4.) □

Remark 16.2.3. When $\mathrm{char}(K) = 0$, the surjectivity in Lemma 16.2.2 can be generalized when B or $B^\times$ is replaced by $G(B)$, where G is a smooth affine group scheme over $\mathcal{O}_K$ with connected special fiber [Gre63, Proposition 3].

We now let π, ϖ be two uniformizers in K, and write $\varpi = \pi u$, with $u \in A^\times$. Let $f \in \mathcal{F}_\pi$ and $g \in \mathcal{F}_\varpi$.

Proposition 16.2.4. *The formal A-modules F_f and F_g over $\mathcal{O}_K$ become isomorphic after base changing from $\mathcal{O}_K$ to B. (Here we write $\mathcal{O}_K$ instead of A to emphasize that it is the ring of coefficients of the power series defining the formal group; after base changing from $\mathcal{O}_K$ to B, we obtain two formal A-modules over B. They are defined by simply viewing all the power series over $\mathcal{O}_K$ involved in the definitions of F_f and F_g as power series over B.) More precisely, fix $\epsilon \in B^\times$ such that $\sigma(\epsilon) = \epsilon u$. There exists $\theta(T) \in B[[T]]_+$ such that*

(i) The linear coefficient of $\theta(T)$ is ϵ.
(ii) $\sigma(\theta(T)) = \theta([u]_f(T))$.
(iii) $\theta(F_f(X,Y)) = F_g(\theta(X), \theta(Y))$.
(iv) $\theta([a]_f(X)) = [a]_g(\theta(X)), \forall a \in A$.

Note that conditions (i) (iii) (iv) imply that θ is an isomorphism between formal A-modules over B. Indeed, by condition (i) and Lemma 11.1.2 (the Inverse Function Theorem), we know that θ has a composition inverse.

Proof. We leave it as an exercise to prove the existence of $\theta(T)$ satisfying (i) and (ii), using Lemma 16.2.2. We now show that such $\theta(T)$ can be modified to satisfy $g = \sigma\theta \circ f \circ \theta^{-1}$. (Here θ^{-1} is the composition inverse of θ.) In fact, let $h = \sigma\theta \circ f \circ \theta^{-1} \in B[[T]]_+$. Then

$$h = \theta \circ [u]_f \circ f \circ \theta^{-1} = \theta \circ f \circ [u]_f \circ \theta^{-1}.$$

Since f and $[u]_f$ have coefficients in A, we have

$$\sigma h = \sigma\theta \circ f \circ [u]_f \circ \sigma\theta^{-1} = \sigma\theta \circ f \circ \theta^{-1} = h.$$

Hence

$$h \in A[[T]]_+.$$

The linear coefficient of h is $\epsilon u \pi \epsilon^{-1} = u\pi = \varpi$. Modulo $\mathfrak{m}_K$, we have

$$h \equiv \sigma\theta \circ (X \mapsto X^q) \circ \theta^{-1},$$

so

$$h(X) \equiv \sigma\theta(\theta^{-1}(X)^q) \equiv \theta(\theta^{-1}(X))^q = X^q.$$

(For the second congruence we used $(\sigma\theta)(Y^q) \equiv (\theta(Y))^q$.) Thus $h \in \mathcal{F}_\varpi$, and we can consider $[1]_{g,h}$. Replace θ by $\theta' = [1]_{g,h} \circ \theta$. Then θ' still satisfies conditions (i) and (ii), and we have

$$\sigma\theta' \circ f \circ \theta'^{-1} = [1]_{g,h} \circ h \circ [1]_{h,g} = g.$$

We now assume that $g = \sigma\theta \circ f \circ \theta^{-1}$. It is then easy to prove conditions (iii) and (iv) using the Key Lemma (Lemma 12.1.4). □

Exercise 16.2.5. Finish the above proof.

17. Lecture 17, 4/1/2021

Proof of Theorem 16.2.1. We first show that K^{LT} is independent of π. Let π, ϖ be two uniformizers of K. We shall show that $K^{\mathrm{ur}} \cdot K_{\pi,n} = K^{\mathrm{ur}} \cdot K_{\varpi,n}$ for each $n \geq 1$. Let $f = X^q - \pi X \in \mathcal{F}_\pi$ and $g = X^q - \varpi X \in \mathcal{F}_\varpi$. Let θ be as in Proposition 16.2.4, with respect to π, ϖ, f, g. Let C be the completion of $\bar{K}$, with respect to the topology defined by v. By the functoriality of completion there is a natural embedding $\breve{K} \to C$. We can make the set $\Lambda' = \{x \in C \mid v(x) > 0\}$, which is analogous to Λ, into A-modules Λ'_f and Λ'_g according to F_f and F_g respectively. Note that the π^n-torsion in Λ'_f, denoted by $\Lambda'_{f,n}$, is actually equal to $\Lambda_{f,n}$, because both sets consist of all the roots of the polynomial $f^{(n)}$ in $\bar{K}$. Similarly, $\Lambda'_{g,n} = \Lambda_{g,n}$. Clearly θ induces an A-module isomorphism $\Lambda'_f \xrightarrow{\sim} \Lambda'_g, x \mapsto \theta(x)$, and hence a bijection $\Lambda'_{f,n} \xrightarrow{\sim} \Lambda'_{g,n}$. (Recall that the π^n-torsion and ϖ^n-torsion in an A-module are the same.) Hence we have $\Lambda_{g,n} = \theta(\Lambda_{f,n})$. Note that $\theta(\Lambda_{f,n})$ is a subset of the completion of $K^{\mathrm{ur}} \cdot K_{\pi,n}$ (viewed as a subfield of C), since every element of $\theta(\Lambda_{f,n})$ is the limit of a sequence of elements of $K^{\mathrm{ur}} \cdot K_{\pi,n}$. By symmetry, the completions of $K^{\mathrm{ur}} \cdot K_{\pi,n}$ and $K^{\mathrm{ur}} \cdot K_{\varpi,n}$ are equal, as subfields of C. By Lemma 17.0.1 below, we can recover $K^{\mathrm{ur}} \cdot K_{\pi,n}$ from its completion by taking algebraic elements over K, and similarly for $K^{\mathrm{ur}} \cdot K_{\varpi,n}$. Hence $K^{\mathrm{ur}} \cdot K_{\pi,n} = K^{\mathrm{ur}} \cdot K_{\varpi,n}$ as desired, and so K^{LT} is independent of π.

We now show that ϕ_π is indepedent of π. Note that we only need to show that $\phi_\pi(\varpi) = \phi_\varpi(\varpi)$ whenever π, ϖ are two uniformizers. In fact, if we know this, then for any uniformizer π' we have $\phi_\pi(\varpi) = \phi_{\pi'}(\varpi)$, since they are both equal to $\phi_\varpi(\varpi)$. Keeping π and π' fixed and letting ϖ vary, we conclude that $\phi_\pi = \phi_{\pi'}$ since the set of all uniformizers generate the group $K^\times$.

We now show that $\phi_\pi(\varpi) = \phi_\varpi(\varpi)$. Recall that $\phi_\varpi(\varpi)$ acts as the Frobenius on K^{ur} and fixes $K_{\varpi,n}$ for all n. Write $\varpi = \pi u$. Now $\phi_\pi(\varpi) = \phi_\pi(\pi u)$ also acts as the Frobenius on K^{ur}, and it sends $x \in \Lambda_{f,n}$ to $[u^{-1}]_f(x)$. Thus it sends $\theta(x) \in \Lambda_{g,n}$ to $(\sigma\theta)([u^{-1}]_f(x))$, since it acts on the coefficients of θ, which are in $\check{K}$, as σ. By property (ii) in Proposition 16.2.4, $(\sigma\theta)([u^{-1}]_f(x)) = \theta(x)$. Thus $\phi_\pi(\varpi)$ fixes $\theta(x)$ for every $x \in \Lambda_{f,n}$. Since θ induces a bijection $\Lambda_{f,n} \xrightarrow{\sim} \Lambda_{g,n}$, we see that $\phi_\pi(\varpi)$ fixes $\Lambda_{g,n}$. Hence $\phi_\pi(\varpi)$ agrees with $\phi_\varpi(\varpi)$ on $K_{\varpi,n}$ for all n. □

Lemma 17.0.1. *Let L be an intermediate extension of $\bar{K}/K$ such that $v(L^\times) = \frac{1}{e}\mathbb{Z} \subset \mathbb{Q}$ for some $e \in \mathbb{Z}_{\geq 1}$. Let $\widehat{L}$ be the completion of L with respect to the discrete valuation $w := e \cdot v$. Then L is algebraically closed inside $\widehat{L}$.*

Proof. Suppose not. Then there is a non-trivial finite extension L_1/L inside $\widehat{L}$. Let $\widehat{w}$ be the unique discrete valuation on $\widehat{L}$ extending w on L. Note that on any algebraic extension of K, there is at most one (in fact, exactly one) $\mathbb{Q}$-valued valuation extending v on K, since this is the case on any finite extension of K. It follows that $\widehat{w}|_{L_1}$ is the unique discrete valuation on L_1 that extends w on L up to a scalar. Let $\widehat{L}_1$ be the completion of L_1 with respect to this discrete valuation. By functoriality we have a canonical map $\widehat{L} \to \widehat{L}_1$, and by [Ser79, §II.3, Theorem 1 (iii)] the $\widehat{L}$-dimension of $\widehat{L}_1$ is equal to $[L_1 : L] > 1$. It follows that the canonical map $\widehat{L} \to \widehat{L}_1$ is non-surjective, and so L is not dense in L_1. But $L \subset L_1 \subset \widehat{L}$ and L is dense in $\widehat{L}$, a contradiction. □

Remark 17.0.2. In Lemma 17.0.1, we crucially used that (L, w) is algebraic over a *complete* discretely valued field. For instance $\mathbb{Q}$ is not algebraically closed inside its p-adic completion $\mathbb{Q}_p$.

17.1. **Group (co)homology.**

17.1.1. *G-modules.* Let G be a group. By a *G-module*, we mean an abelian group equipped with a left G-action via group automorphisms. Let $\mathbb{Z}[G]$ be the group algebra of G over $\mathbb{Z}$. Then a G-module is the same as a left $\mathbb{Z}[G]$-module. Morphisms between G-modules are group homomorphisms which are G-equivariant. (We shall also call these morphisms *G-homomorphisms.*) The category of G-modules is abelian.

If X, Y are G-modules, we write $\mathrm{Hom}(X, Y)$ for the group of homomorphisms $X \to Y$, and write $\mathrm{Hom}_{\mathbb{Z}[G]}(X, Y) = \mathrm{Hom}_G(X, Y)$ for the group of G-homomorphisms $X \to Y$. Note that $\mathrm{Hom}(X, Y)$ is naturally a G-module, with the G-action defined by $(gf)(x) = g(f(g^{-1}x)), \forall g \in G, f \in \mathrm{Hom}(X, Y), x \in X$. We have $\mathrm{Hom}_G(X, Y) = \mathrm{Hom}(X, Y)^G$.

Similarly, if X, Y are G-modules, then $X \otimes_{\mathbb{Z}} Y$ is naturally a G-module, where the G-action is defined by $g(x \otimes y) = gx \otimes gy$.

17.1.2. *Induction and coinduction.* Let H be a subgroup of G. We have two functors from H-modules to G-modules, called *induction* and *coinduction*, defined by

$$\mathrm{Ind}_H^G(X) = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} X, \quad \mathrm{coInd}_H^G(X) = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], X).$$

In the first definition, $\mathbb{Z}[G]$ is viewed as a right $\mathbb{Z}[H]$-module by right multiplication of H on G, and the G-action on $\mathrm{Ind}_H^G(X)$ is induced by the left multiplication of G on $\mathbb{Z}[G]$. In the second definition, $\mathbb{Z}[G]$ is viewed as a left $\mathbb{Z}[H]$-module by left multiplication of H on G, and the G-action on $\mathrm{coInd}_H^G(X)$ is induced by right multiplication of G on $\mathbb{Z}[G]$. In other words, for $g_0 \in G$ and $f \in \mathrm{coInd}_H^G(X)$, we define

$$(g_0 f)(\sum_g a_g[g]) := f(\sum_g a_g[gg_0]), \quad \forall \sum_g a_g[g] \in \mathbb{Z}[G].$$

When H is trivial, we write Ind^G and coInd^G for the two functors. If a G-module Y is isomorphic to $\mathrm{Ind}^G(X)$ (resp. $\mathrm{coInd}^G(X)$) for some abelian group X, we call Y *induced* (resp. *coinduced*).

Exercise 17.1.3. If G is a finite group, then the functors Ind^G and coInd^G are naturally isomorphic. In fact, $\mathbb{Z}[G]$ has a canonical finite $\mathbb{Z}$-basis $\{[g] \mid g \in G\}$. Therefore $\mathrm{Ind}^G(X) = \bigoplus_{g\in G}[g] \cdot X$, and the G-action is given by permuting the summands $[g] \cdot X$. Given an element $x = \sum_g [g] \cdot x_g$ of $\mathrm{Ind}^G(X)$, we define a function $f_x : G \to X, g \mapsto x_{g^{-1}}$, viewed as an element of $\mathrm{coInd}^G(X)$. Show that the map $x \mapsto f_x$ is a G-module isomorphism $\mathrm{Ind}^G(X) \xrightarrow{\sim} \mathrm{coInd}^G(X)$, and that this isomorphism is functorial in X. (If we defined f_x to be $g \mapsto x_g$ then the map $x \mapsto f_x$ would not be G-equivariant.)

The following exercise generalizes the previous one.

Exercise 17.1.4. Let G be an arbitrary group, and let H be a finite index subgroup. Then the functors Ind_H^G and coInd_H^G are naturally isomorphic. (Hint: Use $g \mapsto g^{-1}$ to relate G/H and $H\backslash G$.)

Remark 17.1.5. In [Mil20], our functor coInd_H^G is denoted by Ind_H^G, and what we call coinduced modules are called induced modules. Our convention agrees with that in [Ser79].

Lemma 17.1.6. *The functors* Ind_H^G *and* coInd_H^G *are exact.*

Proof. This follows from the fact that $\mathbb{Z}[G]$, when viewed as a left (resp. right) $\mathbb{Z}[H]$-module, is free. In fact, if $(g_i)_{i\in I}$ is a set of representatives of the cosets in G/H, then $([g_i])_{i\in I}$ is a basis of $\mathbb{Z}[G]$ as a right $\mathbb{Z}[H]$-module. Similarly, there exists a basis of $\mathbb{Z}[G]$ as a left $\mathbb{Z}[H]$-module. □

18. Lecture 18, 4/6/2021

18.1. **Group (co)homology, continued.** Let X be a G-module. Write X_0 for the underlying abelian group. Then we have an injective G-homomorphism

$$X \longrightarrow \mathrm{coInd}^G(X_0), \quad x \longmapsto (\sum_g a_g[g] \mapsto \sum_g a_g g(x)),$$

and a surjective G-homomorphism

$$\mathrm{Ind}^G(X_0) \longrightarrow X, \quad (\sum_g a_g[g]) \otimes x \longmapsto \sum_g a_g g(x).$$

Recall that in an abelian category $\mathcal{A}$, an object I is called *injective* (resp. *projective*) if the functor $\operatorname{Hom}_{\mathcal{A}}(\cdot, I)$ (resp. $\operatorname{Hom}_{\mathcal{A}}(I, \cdot)$) from $\mathcal{A}$ to the category of abelian groups is exact.

Exercise 18.1.1. Check the following two versions of Frobenius reciprocity: Let H be a subgroup of G. For any G-module X and H-module A, we have natural isomorphisms

$$\operatorname{Hom}_{\mathbb{Z}[G]}(X, \operatorname{coInd}_H^G A) \cong \operatorname{Hom}_{\mathbb{Z}[H]}(X, A)$$

and

$$\operatorname{Hom}_{\mathbb{Z}[G]}(\operatorname{Ind}_H^G A, X) \cong \operatorname{Hom}_{\mathbb{Z}[H]}(A, X).$$

Lemma 18.1.2. *If A is an injective abelian group, then* $\operatorname{coInd}^G A$ *is an injective G-module. If A is a projective abelian group, then* $\operatorname{Ind}^G A$ *is a projective G-module.*

Proof. This follows easily from Frobenius reciprocity. □

Corollary 18.1.3. *The category of G-modules has enough injective objects and enough projective objects, i.e., for each G-module X there exists an injective G-homomorphism $X \to I$ and a surjective G-homomorphism $P \to X$, where I is an injective G-module and P is a projective G-module.*

Proof. Let X_0 be the underlying abelian group of X. The category of abelian groups have enough injective objects, so we can find an injective homomorphism $X_0 \to I_0$ where I_0 is an injective abelian group. Since coInd^G is exact, we have injective G-homomorphisms $X \to \operatorname{coInd}^G X_0 \to \operatorname{coInd}^G I_0$. By Lemma 18.1.2, $\operatorname{coInd}^G I_0$ is an injective G-module.

The proof of enough projective objects is similar, using that the category of abelian groups has enough projectives and using the surjection $\operatorname{Ind}^G X_0 \to X$. □

By the above corollary, for any left exact additive functor $\mathcal{F}$ from G-modules to an abelian category, we have the right derived functors $R^i\mathcal{F}, i \geq 0$. Similarly, for any right exact additive functor $\mathcal{G}$ from G-modules to an abelian category, we have the left derived functors $L_i\mathcal{G}, i \geq 0$.

18.1.4. *Recall of derived functors.* (See [Wei95, §2] for details.) Let $\mathcal{F} : \mathcal{A} \to \mathcal{B}$ be a left exact additive functor between abelian categories.[7] Assume that $\mathcal{A}$ has enough injectives. Then the right derived functors $R^i\mathcal{F}$ (for $i \geq 0$) are defined as follows. For $X \in \mathcal{A}$, we find an injective resolution

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

(i.e., an exact sequence in $\mathcal{A}$ with each I^i an injective object), which exists since $\mathcal{A}$ has enough injectives. We then define $R^i\mathcal{F}(X) \in \mathcal{B}$ to be the i-th cohomology object of the complex

$$\mathcal{F}(I^0) \to \mathcal{F}(I^1) \to \cdots$$

in $\mathcal{B}$. (We shall write the resolution as $0 \to X \to I^\bullet$, and write the above complex as $\mathcal{F}(I^\bullet)$.) The definition of $R^i\mathcal{F}(X)$ is independent of the choice of the injective resolution up to canonical isomorphism. Hence we can think of the functor $R^i\mathcal{F}$ as being canonically defined.

[7] An additive functor $\mathcal{F} : \mathcal{A} \to \mathcal{B}$ between abelian categories is called *left (resp. right) exact*, if for any short exact sequence $0 \to A \to B \to C \to 0$ in $\mathcal{A}$, the sequence $0 \to \mathcal{F}(A) \to \mathcal{F}(B) \to \mathcal{F}(C)$ (resp. $\mathcal{F}(A) \to \mathcal{F}(B) \to \mathcal{F}(C) \to 0$) is exact.

Note that $R^0\mathcal{F} = \mathcal{F}$, and $R^i\mathcal{F}(I) = 0$ for all injective objects I and all $i \geq 1$. Moreover, the family of functors $(R^i\mathcal{F})_{i\geq 0}$ has the additional structure of a *δ-functor*. Namely, for any short exact sequence $0 \to A \to B \to C \to 0$ in $\mathcal{A}$, we have a long exact sequence

$$0 \to \mathcal{F}(A) \to \mathcal{F}(B) \to \mathcal{F}(C) \xrightarrow{\delta^0} R^1\mathcal{F}(A) \to R^1\mathcal{F}(B) \to R^1\mathcal{F}(C) \xrightarrow{\delta^1} R^2\mathcal{F}(A) \to \cdots$$

Moreover this long exact depends functorially on the short exact sequence. This means that if we have a commutative diagram with exact rows in $\mathcal{A}$:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

then for each $i \geq 0$ the following diagram commutes:

$$\begin{tikzcd}
R^i\mathcal{F}(C) \arrow[r, "\delta^i"] \arrow[d] & R^{i+1}\mathcal{F}(A) \arrow[d] \\
R^i\mathcal{F}(C') \arrow[r, "\delta^i"] & R^{i+1}\mathcal{F}(A')
\end{tikzcd}$$

Now suppose that $\mathcal{F} : A \to B$ is a right exact additive functor between abelian categories, and that $\mathcal{A}$ has enough projectives. Then the left derived functors $L_i\mathcal{F}$ ($i \geq 0$) are defined. For each X in $\mathcal{A}$, take a projective resolution

$$\cdots \to P_1 \to P_0 \to X \to 0.$$

By definition $L_i\mathcal{F}(X)$ is the i-th homology of the complex $\mathcal{F}(P_\bullet)$. We have $L_0\mathcal{F} = \mathcal{F}$, and $L_i\mathcal{F}(P) = 0$ for all projective P and all $i \geq 1$. For any short exact sequence $0 \to A \to B \to C \to 0$ in $\mathcal{A}$, we have a long exact sequence

$$\cdots L_2\mathcal{F}(C) \xrightarrow{\delta} L_1\mathcal{F}(A) \to L_1\mathcal{F}(B) \to L_1\mathcal{F}(C) \xrightarrow{\delta} \mathcal{F}(A) \to \mathcal{F}(B) \to \mathcal{F}(C) \to 0.$$

18.1.5. *Definition of group (co)homology.* Given any G-module X, we define the G-invariants

$$X^G = \{x \in X \mid gx = x, \forall g \in G\}$$

and the G-coinvariants

$$X_G = X/\langle gx - x \mid g \in G, x \in X\rangle.$$

Then $X \mapsto X^G$ and $X \mapsto X_G$ are functors from G-modules to abelian groups. Note that they are left exact and right exact respectively.

Definition 18.1.6. For $i \geq 0$, we define $\mathbf{H}^i(G, \cdot)$ to be the i-th right derived functor of the left exact functor $X \mapsto X^G$ from G-modules to abelian groups. We define $\mathbf{H}_i(G, \cdot)$ to be the i-th left derived functor of the right exact functor $X \mapsto X_G$ from G-modules to abelian groups.

Example 18.1.7. By definition we have $\mathbf{H}^0(G, X) = X^G$ and $\mathbf{H}_0(G, X) = X_G$.

Example 18.1.8. Let G be the trivial group. Then $\mathbf{H}^i(G, X) = \mathbf{H}_i(G, X) = 0$ for $i > 0$.

Exercise 18.1.9. Let $(M_j)_{j\in J}$ be a family of G-modules. Then $\mathbf{H}^i(G, \prod_j M_j) \cong \prod_j \mathbf{H}^i(G, M_j)$.

18.2. **Free resolution of $\mathbb{Z}$.** Note that the functor $X \mapsto X^G$ from G-modules to abelian groups can be alternatively regarded as the functor $X \mapsto \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, X)$, where $\mathbb{Z}$ is equipped with the trivial G-action. Therefore, $\mathbf{H}^i(G, X) = \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, X)$. If we take a projective resolution

$$\cdots \to P_1 \to P_0 \to \mathbb{Z} \to 0$$

of $\mathbb{Z}$ in the category of G-modules, then $\mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, X)$ can be computed as the i-th cohomology of

$$\mathrm{Hom}_{\mathbb{Z}[G]}(P_0, X) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, X) \to \cdots .$$

This gives an alternative, and in fact more practical, way of computing $\mathbf{H}^i(G, X)$. Note that we can fix the resolution $P_\bullet$ once and for all, independent of X.

We will soon exhibit a *free resolution* $P_\bullet \to \mathbb{Z} \to 0$, i.e., each P_i is a direct sum of copies of $\mathbb{Z}[G]$. With such a resolution we can also compute $\mathbf{H}_i(G, \cdot)$. Note that the functor $X \mapsto X_G$ is really the same as $X \mapsto \mathbb{Z} \otimes_{\mathbb{Z}[G]} X$, where $\mathbb{Z}$ is viewed as a right $\mathbb{Z}[G]$-module with the trivial G-action. Hence $\mathbf{H}_i(G, X) = \mathrm{Tor}_{i,\mathbb{Z}[G]}(\mathbb{Z}, X)$. Now we view the left G-module P_i also as a right G-module by defining $p \cdot g$ to be $g^{-1} \cdot p$, for $p \in P_i, g \in G$. Then $P_\bullet \to \mathbb{Z} \to 0$ is also a free resolution in the category of right $\mathbb{Z}[G]$-modules. Thus $\mathbf{H}_i(G, X)$ is the i-th homology of

$$\cdots \to P_1 \otimes_{\mathbb{Z}[G]} X \to P_0 \otimes_{\mathbb{Z}[G]} X.$$

Definition 18.2.1. A G-module X is called *relatively injective* (resp. *relatively projective*), if it is a direct summand of a coinduced (resp. induced) G-module.

Proposition 18.2.2. *Let X be a relatively injective G-module. Then $\mathbf{H}^i(G, X) = 0$ for $i \geq 1$. Let Y be a relatively projective G-module, then $\mathbf{H}_i(G, Y) = 0$ for $i \geq 1$.*

Proof. Fix a free resolution $P_\bullet \to \mathbb{Z} \to 0$ in the category of G-modules. Since $\mathbf{H}^i(G, \cdot)$ is compatible with finite direct sums, we may assume that $X = \mathrm{coInd}\, A$. Then $\mathbf{H}^i(G, X)$ is the i-th cohomology of $\mathrm{Hom}_{\mathbb{Z}[G]}(P_\bullet, \mathrm{coInd}^G A)$, which is the same as $\mathrm{Hom}_{\mathbb{Z}}(P_\bullet, A)$ by Frobenius reciprocity. Note that $P_\bullet \to \mathbb{Z} \to 0$ is also a free resolution in the category of $\mathbb{Z}$-modules. (Everything free over $\mathbb{Z}[G]$ is also free over $\mathbb{Z}$.) Thus $\mathbf{H}^i(G, X) \cong \mathrm{Ext}^i_{\mathbb{Z}}(\mathbb{Z}, A)$, and this vanishes for $i \geq 1$ since $\mathbb{Z}$ is a free $\mathbb{Z}$-module.

The statement about $\mathbf{H}_i(G, Y)$ is proved similarly. We may assume that $Y = \mathrm{Ind}^G A$. Then $\mathbf{H}_i(G, Y)$ is the i-th homology of $P_\bullet \otimes_{\mathbb{Z}[G]} \mathrm{Ind}^G A$, which is obviously isomorphic to $P_\bullet \otimes_{\mathbb{Z}} A$. Hence $\mathbf{H}_i(G, Y) \cong \mathrm{Tor}_{i,\mathbb{Z}}(\mathbb{Z}, Y)$, and this vanishes for $i \geq 1$. □

The following result is a generalization of Proposition 18.2.2, and its proof is essentially the same.

Proposition 18.2.3 (Shapiro's Lemma)**.** *Let H be a subgroup of G. For each H-module X, there are natural isomorphisms*

$$\mathbf{H}^i(G, \mathrm{coInd}^G_H X) \cong \mathbf{H}^i(H, X)$$

and

$$\mathbf{H}_i(G, \mathrm{Ind}^G_H X) \cong \mathbf{H}_i(H, X)$$

for $i \geq 0$.

Exercise 18.2.4. Prove Proposition 18.2.3.

19. Lecture 19, 4/8/2021

19.1. **Explicit free resolution of $\mathbb{Z}$.** We now describe an explicit choice of a free resolution $P_\bullet \to \mathbb{Z} \to 0$ in the category of G-modules. Let $P_i = \mathbb{Z}[G^{i+1}]$, with G-action given by

$$g \cdot [g_0, g_1, \cdots, g_i] = [gg_0, \cdots, gg_i], \quad \forall g \in G, (g_0, \cdots, g_i) \in G^{i+1}.$$

Note that P_i is indeed a free $\mathbb{Z}[G]$-module, with a $\mathbb{Z}[G]$-basis

$$\{[1, g_1, \cdots, g_i] \mid g_1, \cdots, g_i \in G\}.$$

Define the differential $d_i : P_i \to P_{i-1}$ by

$$d_i[g_0, \cdots, g_i] := \sum_{0 \le j \le i} (-1)^j [g_0, \cdots, \widehat{g_j}, \cdots, g_i], \quad \forall (g_0, \cdots, g_i) \in G^{i+1}.$$

Here hat means ommision. Define $\epsilon : P_0 \to \mathbb{Z}$ by $\epsilon[g_0] = 1, \forall g_0 \in G$.

Exercise 19.1.1. Check that $P_\bullet \xrightarrow{\epsilon} \mathbb{Z} \to 0$ is a resolution in the category of G-modules. (Do not forget to check that the compositions of consecutive differentials are zero.)

19.2. **Computing cohomology.** Let X is a G-module. Recall that $\mathbf{H}^i(G, X)$ is the i-th cohomology of $\mathrm{Hom}_{\mathbb{Z}[G]}(P_\bullet, X)$. Now $\mathrm{Hom}_{\mathbb{Z}[G]}(P_i, X)$ is identified with abelian group $\widetilde{C}^i(G, X)$ consisting of functions $f : G^{i+1} \to X$ satisfying the *homogeneous condition*

$$f(gg_0, \cdots, gg_i) = g \cdot f(g_0, \cdots, g_i).$$

Such functions are called *homogeneous i-cochains.* The differential $\widetilde{d} : \widetilde{C}^i(G, X) \to \widetilde{C}^{i+1}(G, X)$ induced by $d : P_{i+1} \to P_i$ is given by

$$(\widetilde{d}f)(g_0, \cdots g_{i+1}) = \sum_{j=0}^{i} (-1)^j f(g_0, \cdots, \widehat{g_j}, \cdots, g_i)$$

We would like to dehomogenize $\widetilde{C}^i(G, X)$. Let $C^i(G, X)$ be the abelian group of all maps $G^i \to X$. We have an isomorphism

$$\widetilde{C}^i(G, X) \xrightarrow{\sim} C^i(G, X), \quad f \mapsto \underline{f},$$

where

$$\underline{f}(g_1, \cdots, g_i) = f(1, g_1, g_1 g_2, \cdots g_1 \cdots g_i).$$

The induced differential $d : C^i(G, X) \to C^{i+1}(G, X)$ is given by

$$(df)(g_1, \cdots, g_{i+1}) = g_1 f(g_2, \cdots, g_{i+1}) + \sum_{j=1}^{i} (-1)^j f(g_1, \cdots, g_j g_{j+1}, \cdots, g_{i+1}) + (-1)^{i+1} f(g_1, \cdots, g_i).$$

The kernel and image of $d : C^i(G, X) \to C^{i+1}(G, X)$ are denoted by $Z^i(G, X)$ and $B^{i+1}(G, X)$, and their elements are called i-cocycles and $i+1$-coboundaries. We have

$$\mathbf{H}^i(G, X) = Z^i(G, X)/B^i(G, X).$$

Example 19.2.1. The differential $d^0 : C^0(G, X) = X \to C^1(G, X)$ sends $x \in X$ to the function $G \to X, g \mapsto gx - x$. Its kernel is indeed $\mathbf{H}^0(G, X) = X^G$.

Example 19.2.2. The differential $d^1 : C^1(G,X) \to C^2(G,X)$ sends f to the function $G^2 \to X, (g_1,g_2) \mapsto g_1 \cdot f(g_2) - f(g_1g_2) + f(g_1)$. Its kernel $Z^1(G,X)$ consists of functions $f : G \to X$ satisfying $f(g_1g_2) = f(g_1) + g_1 \cdot f(g_2)$, called *crossed homomorphisms*. Thus $\mathbf{H}^1(G,X)$ is the quotient of the group of crossed homomorphisms by the group of functions of the form $g \mapsto gx - x$ for some $x \in X$ (which are called *principal crossed homomorphisms*). Note that if G acts trivially on X, then $\mathbf{H}^1(G,X) = \mathrm{Hom}(G,X)$.

Example 19.2.3. Suppose we have a short exact sequence of groups $1 \to X \to E \to G \to 1$, where X is abelian (written multiplicatively). We say that E is an extension of G by X. Fix a set-theoretic section $s : G \to E$ of the map $E \to G$. For each $g \in G$, let g act on X by $x \mapsto s(g)xs(g)^{-1}$. This defines a G-module structure on X, which is independent of the choice of s. The function $G^2 \to X, (g,h) \mapsto s(g)s(h)s(gh)^{-1}$ is an element of $Z^2(G,X)$, and its image in $\mathbf{H}^2(G,X)$ is independent of the choice of s. In this way, $\mathbf{H}^2(G,X)$ classifies all the isomorphism classes of extensions of G by X with the prescribed G-action on X.

19.2.4. *Functoriality.* Suppose that $X \to Y$ is a map of G-modules. Then sice $\mathbf{H}^i(G,\cdot)$ is a functor we have a homomorphism $\mathbf{H}^i(G,X) \to \mathbf{H}^i(G,Y)$. This can be described in terms of cochains as follows. We have an obvious map $C^i(G,X) \to C^i(G,Y)$ for each i, induced by the map $X \to Y$. These maps commute with the differentials, and hence induce maps $\mathbf{H}^i(G,X) \to \mathbf{H}^i(G,Y)$. The last maps are the correct ones.

19.2.5. *The connecting homomorphism in terms of cochains.* Given a short exact sequence $0 \to A \to B \to C \to 0$ of G-modules, the connecting map $\delta : \mathbf{H}^i(G,C) \to \mathbf{H}^{i+1}(G,A)$ can be described in terms of cochains as follows. Given $\zeta \in \mathbf{H}^i(G,C)$, first find an i-cocycle $z : G^i \to C$ representing z. Since $B \to C$ is surjective, we can lift z to an i-cochain $\widetilde{z} : G^i \to B$. Now $d\widetilde{z}$ need no longer be 0, but we at least have $d\widetilde{z} \in C^i(G,A)$ since $dz = 0$. Since $d(d\widetilde{z}) = 0$, we have $d\widetilde{z} \in Z^i(G,A)$. The class in $\mathbf{H}^i(G,A)$ represented by $d\widetilde{z}$ is $\delta(\zeta)$.

Remark 19.2.6. As we discussed before, we can use the free resolution $P_\bullet \to \mathbb{Z} \to 0$ to compute $\mathbf{H}_i(G,X)$ as well. See [Ser79, §VII.4] for explicit formulas in terms of finitely supported functions $G^i \to X$ and differentials.

19.3. **Computing $\mathbf{H}_1(G,\mathbb{Z})$.** Let $\mathbb{Z}$ be the $\mathbb{Z}[G]$-module with trivial G-action. We compute $\mathbf{H}_1(G,\mathbb{Z})$. Consider the *augmentation map*

$$\pi : \mathbb{Z}[G] \longrightarrow \mathbb{Z}, \quad \sum_g a_g[g] \longmapsto \sum_g a_g.$$

(This is the same as the map $\epsilon : P_0 \to \mathbb{Z}$ before.) Let I_G be the kernel of π. Note that I_G is a free $\mathbb{Z}$-module with basis $\{1 - [g] \mid g \in G - \{e\}\}$. For any G-module X, we have

$$X_G \cong X/I_GX.$$

From the short exact sequence $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$, we obtain the long exact sequence

$$\mathbf{H}_1(G,\mathbb{Z}[G]) \to \mathbf{H}_1(G,\mathbb{Z}) \to \mathbf{H}_0(G,I_G) \to \mathbf{H}_0(G,\mathbb{Z}[G]).$$

The first term is zero since $\mathbb{Z}[G]$ is induced (Proposition 18.2.2), and the last map is zero since it is the map $I_G/I_G^2 \to \mathbb{Z}[G]/I_G$ induced by the inclusion $I_G \to \mathbb{Z}[G]$.

Thus we have a canonical isomorphism

$$\mathbf{H}_1(G,\mathbb{Z}) \cong I_G/I_G^2.$$

Now it is elementary to check that

$$G \longrightarrow I_G/I_G^2, \quad g \mapsto 1-[g]$$

induces an isomorphism $G^{\mathrm{ab}} \xrightarrow{\sim} I_G/I_G^2$. (Here G^{ab} is the abelianization of G as an abstract group.) Thus we have a canonical isomorphsm between $\mathbf{H}_1(G,\mathbb{Z})$ and G^{ab}.

20. Lecture 20, 4/13/2021

20.1. **Change of group.** Let X be a G-module and X' be a G'-module. Suppose we have homomorphisms $\alpha : G' \to G$ and $\beta : X \to X'$. We say that (α,β) is *compatible*, if

$$\beta(\alpha(g')\cdot x) = g' \cdot \beta(x)$$

for all $g' \in G', x \in X$. In this case, for each $i \geq 0$ we have a homomorphism

$$\begin{aligned} C^i(G,X) &\longrightarrow C^i(G',X') \\ f &\longmapsto ((g_1',\cdots,g_i') \mapsto \beta(f(\alpha(g_1'),\cdots,\alpha(g_i')))). \end{aligned}$$

These homomorphisms commute with the differentials $C^i(G,X) \to C^{i+1}(G,X)$ and $C^i(G',X') \to C^{i+1}(G',X')$, and so they induce homomorphisms

$$\mathbf{H}^i(G,X) \longrightarrow \mathbf{H}^i(G',X').$$

Example 20.1.1. We have $X = X'$, $\beta = \mathrm{id}$, and $\alpha : H \to G$ is the inclusion of a subgroup. In this case the homomorphism $\mathbf{H}^i(G,X) \to \mathbf{H}^i(H,X)$ is called *restriction*, denoted by Res.

Example 20.1.2. Let H be a normal subgroup of G, and let X be a G-module. Let α be the quotient map $G \to G/H$, and let β be the inclusion $X^H \to X$. Note that X^H is indeed a G/H-module, and that (α,β) is compatible. The homomorphism

$$\mathbf{H}^i(G/H, X^H) \longrightarrow \mathbf{H}^i(G,X)$$

is called *inflation*, denoted by Inf.

Remark 20.1.3. For homology, we have natural *corestriction maps.* When H is a subgroup of G, for each G-module we have a natural map

$$\mathrm{Cor} : \mathbf{H}_i(H,X) \to \mathbf{H}_i(G,X).$$

When $i = 0$ this is the map $X_H \to X_G$ induced by the identity on X. The corestriction maps can be defined using the presentation of homology in terms of chains and differentials. (The group of i-chains $C_i(H,X)$ is the group of finitely supported functions $H^i \to X$. We have $C_i(H,X) \to C_i(G,X)$ by extension by zero.)

20.2. **The inflation-restriction sequence.** Let X be a G-module, and let H be a normal subgroup of G.

Proposition 20.2.1. *The sequence*

$$0 \to \mathbf{H}^1(G/H, X^H) \xrightarrow{\text{Inf}} \mathbf{H}^1(G, X) \xrightarrow{\text{Res}} \mathbf{H}^1(H, X)$$

is exact.

Proof. Elementary computation with 1-cocycles. □

We have the following generalization.

Proposition 20.2.2. *Let q be a positive integer. Suppose that $\mathbf{H}^i(H, X) = 0$ for $1 \le i \le q - 1$. (If $q = 1$, this hypothesis is void.) Then the sequence*

$$0 \to \mathbf{H}^q(G/H, X^H) \xrightarrow{\text{Inf}} \mathbf{H}^q(G, X) \xrightarrow{\text{Res}} \mathbf{H}^q(H, X)$$

is exact.

Lemma 20.2.3. *Let Y be a G-module. If Y is coinduced, then it is also coinduced when viewed as an H-module. Similarly for induced.*

Proof. Since $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module, we can write $\mathbb{Z}[G] \cong \mathbb{Z}[H] \otimes_{\mathbb{Z}} M$ for some abelian group M. If $Y = \operatorname{coInd}^G X$ for some abelian group X, then

$$Y = \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X) \cong \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}[H], \operatorname{Hom}_{\mathbb{Z}}(M, X)) = \operatorname{coInd}^H(\operatorname{Hom}_{\mathbb{Z}}(M, X)),$$

and the isomorphism is H-equivariant. If $Y = \operatorname{Ind}^G X$, then

$$Y = \mathbb{Z}[G] \otimes_{\mathbb{Z}} X \cong \mathbb{Z}[H] \otimes_{\mathbb{Z}} (M \otimes_{\mathbb{Z}} X) = \operatorname{Ind}^H(M \otimes_{\mathbb{Z}} X),$$

and the isomorphism is H-equivariant. □

Proof of Proposition 20.2.2. We induct on q. For $q = 1$ this is Proposition 20.2.1. Assume $q \ge 2$. Recall that we have an injective G-homommorphism $X \hookrightarrow Y := \operatorname{coInd}^G X_0$, where X_0 is the underlying abelian group of X. Let $Z = Y/X$. Since $\mathbf{H}^i(G, Y) = 0$ for all $i \ge 1$ (see Proposition 18.2.2), by the long exact sequence associated with $0 \to X \to Y \to Z$ we have

$$\mathbf{H}^i(G, Z) \cong \mathbf{H}^{i+1}(G, X) \tag{20.2.3.1}$$

for $i \ge 1$.

Now since $\mathbf{H}^1(H, X) = 0$ by hypothesis (as $q \ge 2$), the sequence

$$0 \to X^H \to Y^H \to Z^H \to 0$$

is exact. It is easy to see that $Y^H = \operatorname{coInd}^{G/H} X_0$, i.e., it is coinduced as a G/H-module. Thus by the same argument as above we have

$$\mathbf{H}^i(G/H, Z^H) \cong \mathbf{H}^{i+1}(G/H, X^H) \tag{20.2.3.2}$$

for $i \ge 1/$

Now if we view the G-module Y as an H-module, then it is also coinduced by Lemma 20.2.3. Then from the short exact sequence $0 \to X \to Y \to Z \to 0$ of H-modules we obtain

$$\mathbf{H}^i(H, Z) \cong \mathbf{H}^{i+1}(H, X) \tag{20.2.3.3}$$

for $i \ge 1$.

One checks that the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathbf{H}^{q-1}(G/H, Z^H) \arrow[r, "\mathrm{Inf}"] \arrow[d] & \mathbf{H}^{q-1}(G, Z) \arrow[r, "\mathrm{Res}"] \arrow[d] & \mathbf{H}^{q-1}(H, Z) \arrow[d] \\
0 \arrow[r] & \mathbf{H}^{q}(G/H, X^H) \arrow[r, "\mathrm{Inf}"] & \mathbf{H}^{q}(G, X) \arrow[r, "\mathrm{Res}"] & \mathbf{H}^{q}(H, X)
\end{tikzcd}$$

commutes, where the vertical maps are the isomorphisms (20.2.3.1) (20.2.3.2) (20.2.3.3), which are connecting homomorphisms. To finish the proof, it suffices to check that the first row is exact. Note that Z indeed satisfies the condition that $\mathbf{H}^i(H, Z) = 0$ for $1 \le i \le q-2$, since we have (20.2.3.3). Thus the first row of the above diagram is exact by the induction hypothesis. □

Remark 20.2.4. Proposition 20.2.2 also follows from the general machinary of Hochschild–Serre spectral sequence, arising from the fact that the functor $(\cdot)^G : G\text{-mods} \to \mathrm{Ab}$ is the composition of the functors $(\cdot)^H : G\text{-mods} \to G/H\text{-mods}$ and $(\cdot)^{G/H} : G/H\text{-mods} \to \mathrm{Ab}$.

20.3. **Finite index subgroups.** Assume that $H \le G$ is a finite index subgroup. We then have *corestriction maps* $\mathbf{H}^i(H, X) \to \mathbf{H}^i(G, X)$ and *restriction maps* $\mathbf{H}_i(G, X) \to \mathbf{H}_i(H, X)$ for any G-module X. The most natural way to define them is via Grothendieck's general formalism of universal δ-functors, which will be reviewed in the appendix. Alternatively, one can define them using Shapiro's Lemma (Proposition 18.2.3), see [Mil20, §II, Example 1.29]. Below we define them using "dimension shifting", which is essentially equivalent to the approach of universal δ-functors.

20.3.1. *Corestriction for cohomology.* For each $i \ge 0$, we need to define a natural transformation $\mathrm{Cor}^i : \mathbf{H}^i(H, \cdot) \to \mathbf{H}^i(G, \cdot)$, between functors from G-mods to Ab. When $i = 0$, for each G-module X we have the norm map

$$\mathrm{N}_{G/H} : X^H \longrightarrow X^G, \quad x \longmapsto \sum_{gH \in G/H} g \cdot x,$$

which is well defined and functorial in X. We define Cor^0 to be $\mathrm{N}_{G/H}$.

We now define Cor^i inductively on i. Assume that Cor^i has been constructed, and we construct Cor^{i+1}. Let X be a G-module. Choose an injective G-homomorphism $X \hookrightarrow Y$ such that Y is coinduced (e.g., $Y = \mathrm{coInd}^G X_0$). Let $Z = Y/X$. By Lemma 20.2.3, Y is also coinduced as an H-module. Hence $\mathbf{H}^{i+1}(G, Y) = \mathbf{H}^{i+1}(H, Y) = 0$. Thus the following diagram has exact rows[8]:

$$\begin{tikzcd}
\mathbf{H}^i(H, Y) \arrow[r] \arrow[d, "\mathrm{Cor}^i"] & \mathbf{H}^i(H, Z) \arrow[r, "\delta"] \arrow[d, "\mathrm{Cor}^i"] & \mathbf{H}^{i+1}(H, X) \arrow[r] & 0 \\
\mathbf{H}^i(G, Y) \arrow[r] & \mathbf{H}^i(G, Z) \arrow[r, "\delta"] & \mathbf{H}^{i+1}(G, X) \arrow[r] & 0
\end{tikzcd}$$

Since Cor^i is a natural transformation $\mathbf{H}^i(H, \cdot) \to \mathbf{H}^i(G, \cdot)$, the above diagram commutes. Therefore there is a unique homomorphism $\mathrm{Cor}^{i+1}_X : \mathbf{H}^{i+1}(H, X) \to$

[8] As i can be 0, we don't know if $\mathbf{H}^i(H, Y)$ and $\mathbf{H}^i(G, Y)$ vanish.

$\mathbf{H}^{i+1}(G, X)$ making the diagram

$$\begin{tikzcd}
\mathbf{H}^i(H, Z) \arrow[r, "\delta"] \arrow[d, "\mathrm{Cor}^i"] & \mathbf{H}^{i+1}(H, X) \arrow[d, "\mathrm{Cor}_X^{i+1}"] \\
\mathbf{H}^i(G, Z) \arrow[r, "\delta"] & \mathbf{H}^{i+1}(G, X)
\end{tikzcd}$$

commute.

We need to check that the definition of Cor_X^{i+1} is independent of the choice of $X \hookrightarrow Y$. Suppose $X \hookrightarrow Y'$ is another choice and $Z' = Y'/X'$. Up to replacing Y' by $Y' \oplus Y$ (equipped with the diagonal embedding $X \hookrightarrow Y' \oplus Y$), we may assume that there is a G-homomorphism $Y' \to Y$ commuting with $X \hookrightarrow Y$ and $X \hookrightarrow Y'$. Let $f : Z' \to Z$ be the induced map. From the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & X \arrow[r] \arrow[d, "\mathrm{id}"] & Y' \arrow[r] \arrow[d] & Z' \arrow[r] \arrow[d, "f"] & 0 \\
0 \arrow[r] & X \arrow[r] & Y \arrow[r] & Z \arrow[r] & 0
\end{tikzcd}$$

we obtain commutative diagrams

$$\begin{tikzcd}
\mathbf{H}^i(G, Z') \arrow[r, "\delta"] \arrow[d, "f"] & \mathbf{H}^{i+1}(G, X) \arrow[d, "\mathrm{id}"] \\
\mathbf{H}^i(G, Z) \arrow[r, "\delta"] & \mathbf{H}^{i+1}(G, X)
\end{tikzcd}$$

and

$$\begin{tikzcd}
\mathbf{H}^i(H, Z') \arrow[r, "\delta"] \arrow[d, "f"] & \mathbf{H}^{i+1}(H, X) \arrow[d, "\mathrm{id}"] \\
\mathbf{H}^i(H, Z) \arrow[r, "\delta"] & \mathbf{H}^{i+1}(H, X)
\end{tikzcd}$$

The well definedness of Cor_X^{i+1} reduces to the commutativity of the following diagram

$$\begin{tikzcd}
\mathbf{H}^i(H, Z') \arrow[r, "\mathrm{Cor}^i"] \arrow[d, "f"] & \mathbf{H}^i(G, Z') \arrow[d, "f"] \\
\mathbf{H}^i(H, Z) \arrow[r, "\mathrm{Cor}^i"] & \mathbf{H}^i(G, Z)
\end{tikzcd}$$

The commutativity of the above diagram follows from the fact that Cor^i is a natural transformation.

We have proved the well definedness of Cor_X^{i+1}. It still remains to check that it is functorial in X. For this, suppose $f : X_1 \to X_2$ is a G-homomorphism between G-modules. Choose $X_i \hookrightarrow Y_i$, with Y_i coinduced. We can replace Y_1 by $Y_1 \oplus Y_2$, and define the map $X_1 \hookrightarrow Y_1 \oplus Y_2$ by summing the maps $X_1 \to Y_1$ and $X_1 \to X_2 \to Y_2$. Thus we may assume that there is a G-homorphism $\widetilde{f} : Y_1 \to Y_2$ extending $f : X_1 \to X_2$. The naturality of Cor^{i+1} with respect to f follows from the naturality of Cor^i with respect to the map $Y_1/X_1 \to Y_2/X_2$ induced by $\widetilde{f}$. This finishes the definition of Cor^{i+1} as a natural transformation $\mathbf{H}^{i+1}(H, \cdot) \to \mathbf{H}^{i+1}(G, \cdot)$.

Proposition 20.3.2. *The family of natural transformations* $\mathrm{Cor}^i : \mathbf{H}^i(H,\cdot) \to \mathbf{H}^i(G,\cdot)$ *($i \geq 0$) between functors from G*-mods *to* Ab *is uniquely characterized by the following properties:*

(i) $\mathrm{Cor}^0 = \mathrm{N}_{G/H}$.

(ii) If $0 \to A \to B \to C \to 0$ is a short exact sequence of G-modules, then for each $i \geq 0$ we have a commutative diagram

$$\begin{tikzcd}
\mathbf{H}^i(G,C) \arrow[r] \arrow[d, "\mathrm{Cor}^i"] & \mathbf{H}^{i+1}(G,A) \arrow[d, "\mathrm{Cor}^{i+1}"] \\
\mathbf{H}^i(G,C) \arrow[r] & \mathbf{H}^{i+1}(G,A)
\end{tikzcd}$$

where the horizontal maps are the connecting homomorphisms.

Exercise 20.3.3. Prove Proposition 20.3.2. (Note that by our construction, property (ii) is satisfied if B is coinduced. One still needs to check (ii) in general. Hint for this: Find an embedding $B \hookrightarrow B'$ with B' coinduced. Conclude that there is a morphism from the short exact sequence $0 \to A \to B \to C \to 0$ to a short exact sequence of the form $0 \to A \to B' \to C' \to 0$. Then relate the connecting homomorphism $\mathbf{H}^i(G,C) \to \mathbf{H}^{i+1}(G,A)$ to the functorial map $\mathbf{H}^i(G,C) \to \mathbf{H}^i(G,C')$, and similarly for G replaced by H.)

20.3.4. *Restriction for homology.* For each $i \geq 0$, we need to define a natural transformation $\mathrm{Res}_i : \mathbf{H}_i(G,\cdot) \to \mathbf{H}_i(H,\cdot)$, between functors from G-mods to Ab. For each G-module X we have

$$\mathrm{N}'_{G/H} : X_G \longrightarrow X_H, \quad x \mod I_G X \longmapsto \sum_{Hg \in H\backslash G} g \cdot x \mod I_H X,$$

which is functorial in X. We define Res_0 to be $\mathrm{N}'_{G/H}$. We then inductively define Res_i similarly as before using dimension shifting. Here the key fact is that for any G-module X there is a surjection of G-modules $Y \to X$ with Y induced, and the fact that Y is also induced as an H-module (Lemma 20.2.3). The family of natural transformations Res_i is characterized similarly as in Proposition 20.3.2.

Appendix. Universal δ-functors

The following definitions are taken from Grothendieck's Tohoku paper [Gro57], with some simplifications. Fix abelian categories $\mathcal{A}$ and $\mathcal{B}$.

Definition 20.3.5. A *δ-functor* from $\mathcal{A}$ to $\mathcal{B}$ (ranging over $\mathbb{Z}_{\geq 0}$) is the following datum:

- For each integer $i \geq 0$, an additive functor $\mathcal{H}^i : \mathcal{A} \to \mathcal{B}$.
- For each short exact sequence $0 \to A \to B \to C \to 0$ in $\mathcal{A}$ and for each $i \geq 0$, a connecting homomorphism $\delta : \mathcal{H}^i(C) \to \mathcal{H}^{i+1}(A)$.

These should satisfy the following conditions:

(i) For each short exact sequence $0 \to A \to B \to C \to 0$ in $\mathcal{A}$, the connecting homomorphisms δ as above give rise to a long complex

$$\mathcal{H}^0(A) \to \mathcal{H}^0(B) \to \mathcal{H}^0(C) \xrightarrow{\delta} \mathcal{H}^1(A) \to \cdots,$$

i.e., the composition of two consecutive maps is 0.

(ii) If we have a commutative diagram with exact rows in $\mathcal{A}$:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

then for each $i \geq 0$ the following diagram commutes:

$$\begin{tikzcd}
\mathcal{H}^i(C) \arrow[r, "\delta^i"] \arrow[d] & \mathcal{H}^{i+1}(A) \arrow[d] \\
\mathcal{H}^i(C') \arrow[r, "\delta^i"] & \mathcal{H}^{i+1}(A')
\end{tikzcd}$$

We often denote a δ-functor by $(\mathcal{H}^i)_{i\geq 0}$, omitting δ from the notation. We say that a δ-functor is *exact*, if the long complex associated with any short exact sequence is always exact. A *morphism* between two δ-functors $(\mathcal{H}^i)$ and $(\mathcal{E}^i)$ is a collection of natural transformations $\mathcal{H}^i \to \mathcal{E}^i$ which are compatible with the connecting homomorphisms.

Definition 20.3.6. A δ-functor $(\mathcal{H}^i)$ from $\mathcal{A}$ to $\mathcal{B}$ is called *universal*, if for any other δ-functor $(\mathcal{E}^i)$ from $\mathcal{A}$ to $\mathcal{B}$, any natural transformation $\mathcal{H}^0 \to \mathcal{E}^0$ extends uniquely to a morphism of δ-functors $(\mathcal{H}^i) \to (\mathcal{E}^i)$.

Remark 20.3.7. If $(\mathcal{H}^i)$ is a universal δ-functor, then it is uniquely determined by $\mathcal{H}^0$ (up to unique isomorphism between δ-functors).

Definition 20.3.8. An additive functor $\mathcal{F} : \mathcal{A} \to \mathcal{B}$ is called *effacable (or effaçable)*, if for any $A \in \mathcal{A}$ there exists a monomorphism $u : A \to B$ in $\mathcal{A}$ such that $\mathcal{F}(u) = 0$.

Theorem 20.3.9 (Grothendieck, [Gro57, Proposition 2.2.1])**.** *Let $(\mathcal{H}^i)_{i\geq 0}$ be an exact δ-functor. If $\mathcal{H}^i$ is effacable for all $i \geq 1$, then $(\mathcal{H}^i)_{i\geq 0}$ is universal.*

Sketch of proof. Let $(\mathcal{H}^i)$ be such a δ-functor. Suppose $(\mathcal{E}^i)$ is another δ-functor and we have a natural transformation $f^0 : \mathcal{H}^0 \to \mathcal{E}^0$. We inductively define $f^i : \mathcal{H}^i \to \mathcal{E}^i$ as follows. Fix $i \geq 1$, and assume that f^j has been constructed for $0 \leq j \leq i-1$. Let $A \in \mathcal{A}$. By assumption we can find a short exact sequence $0 \to A \to B \to C \to 0$ such that $\mathcal{H}^i(A) \to \mathcal{H}^i(B)$ is the zero map. This means that $\mathcal{H}^i(A) \cong \mathcal{H}^{i-1}(C)/\mathcal{H}^{i-1}(B)$. The desired map $f^i : \mathcal{H}^i(A) \to \mathcal{E}^i(A)$ must, and can, be induced by the composition

$$\mathcal{H}^{i-1}(C) \xrightarrow{f^{i-1}} \mathcal{E}^{i-1}(C) \xrightarrow{\delta} \mathcal{E}^i(A).$$

One still needs to check well definedness of f^i for fixed A, functoriality of f^i in A, and compatibility with the connecting homomorphisms.[9] The first two points can be checked in a similar way as when we constructed Cor^i in §20.3.1. The third point is checked in a similar way as Exercise 20.3.3. □

Remark 20.3.10. The converse is not always true. It is true if $\mathcal{A}$ has enough injective objects. In this case, $\mathcal{H}^i$ is in fact $R^i\mathcal{H}^0$.

[9] The checking of these three poins are described as "raisonnements standarts" in [Gro57, Proposition 2.2.1].

20.3.11. *Corestriction for cohomology.* Now consider an arbitrary subgroup H of G. We view $(\mathbf{H}^i(H,\cdot))$ as a family of functors from G-mods to Ab. Then it has the canonical structure of an exact δ-functor, since each short exact sequence of G-modules is also a short exact sequence of H-modules.

Lemma 20.3.12. *The exact δ-functor $(\mathbf{H}^i(H,\cdot))$ on G-mods is universal.*

Proof. For each G-module X, we have the injection $X \hookrightarrow Y := \operatorname{coInd}^G X_0$. By Lemma 20.2.3, Y is also coinduced as an H-module. Thus $\mathbf{H}^i(H,Y) = 0$ for $i \geq 1$ by Proposition 18.2.3. This shows that $\mathbf{H}^i(H,\cdot)$ is effacable on G-mods for each $i \geq 1$. The lemma follows from Theorem 20.3.9. □

Now assume that H is a finite index subgroup of G. By the above lemma, we can extend the natural transformation $\mathrm{N}_{G/H} : \mathbf{H}^0(H,\cdot) \to \mathbf{H}^0(G,\cdot)$ to a unique momorphism of δ-functors $(\mathbf{H}^i(H,\cdot)) \to (\mathbf{H}^i(G,\cdot))$. This defines corestriction for cohomology.

20.3.13. *Restriction for homology.* Similarly, when H is of finite index in G, we define restriction for homology extending $\mathrm{N}'_{G/H} : \mathbf{H}_0(G,\cdot) \to \mathbf{H}_0(H,\cdot)$. Here we can view $(\mathbf{H}_i(H,\cdot))$ and $(\mathbf{H}_i(G,\cdot))$ as δ-functors from the opposite category of G-mods to the opposite category of Ab. The key point is then to check that $\mathbf{H}_i(H,\cdot)$ is effacable on the opposite category of G-mods, for $i \geq 1$. In other words, for each G-module X and each $i \geq 1$, we need to find an epimorphism $u : Y \to X$ such that $\mathbf{H}_i(H,Y) \to \mathbf{H}_i(H,X)$ is zero. For this we can take Y to be an induced G-module (e.g., $Y = \operatorname{Ind}^G X_0$), and note that it is also induced as an H-module by Lemma 20.2.3.

21. Lecture 21, 4/15/2021

21.1. **Restriction and corestriction.** Let G be a group, and let H be a finite index subgroup of G.

Proposition 21.1.1. *Let X be a G-module. Then the compositions*

$$\mathbf{H}^i(G,X) \xrightarrow{\mathrm{Res}} \mathbf{H}^i(H,X) \xrightarrow{\mathrm{Cor}} \mathbf{H}^i(G,X)$$

and

$$\mathbf{H}_i(G,X) \xrightarrow{\mathrm{Res}} \mathbf{H}_i(H,X) \xrightarrow{\mathrm{Cor}} \mathbf{H}_i(G,X)$$

are both equal to multiplication by $[G:H]$.

Proof. We only prove the statement about the first composition, as the other one is proved similarly. When $i = 0$ this follows immediately from the definition of $\mathrm{N}_{G/H}$. In general we can take a short exact sequence $0 \to X \to Y \to Z$ with $Y = \operatorname{coInd}^G X_0$. As in the proof of Proposition 20.2.2 we have $\mathbf{H}^i(G,Z) \cong \mathbf{H}^{i+1}(G,X)$ and $\mathbf{H}^i(H,Z) \cong \mathbf{H}^{i+1}(G,X)$. These isomorphisms commute with Res and Cor. Up to replacing X by Z the proof reduces to the induction hypothesis. □

Corollary 21.1.2. *If G is finite, then $\mathbf{H}^i(G,X)$ and $\mathbf{H}_i(G,X)$ are killed by $|G|$ for $i \geq 1$.*

Proof. The composition $\mathbf{H}^i(G,X) \xrightarrow{\mathrm{Res}} \mathbf{H}^i(\{1\},X) \xrightarrow{\mathrm{Cor}} \mathbf{H}^i(G,X)$ is equal to $|G|$, but it is zero since the middle group is zero. Hence $\mathbf{H}^i(G,X)$ is killed by $|G|$. The other statement is proved similarly. □

Corollary 21.1.3. *If G is finite and X is a G-module which is finitely generated as an abelian group, then $\mathbf{H}^i(G,X)$ and $\mathbf{H}_i(G,X)$ are finite abelian group killed by $|G|$ for $i \geq 1$.*

Proof. Using the description in terms of cochains and chains, it is easy to see that $\mathbf{H}^i(G,X)$ and $\mathbf{H}_i(G,X)$ are finitely generated abelian group. □

21.1.4. *Transfer.* An important special case is the homomorphism

$$\mathrm{Res}: \mathbf{H}_1(G,\mathbb{Z}) \longrightarrow \mathbf{H}_1(H,\mathbb{Z})$$

when $H \leq G$ is of finite index. Recall that the two sides are canonically identified with G^{ab} and H^{ab}. The resulting homomorphism $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is called *transfer*, and it can be described by an explicit formula as follows.

Proposition 21.1.5. *Fix a section $\theta : H\backslash G \to G$ of the projection $G \to H\backslash G$. For each $s \in G$ and $t \in H\backslash G$, define $x_{t,s} \in H$ by*

$$\theta(t)s = x_{t,s}\theta(ts).$$

Then the transfer map $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is induced by

$$G \longrightarrow H, \quad s \longmapsto \prod_{t \in H\backslash G} x_{t,s}.$$

Exercise 21.1.6. Prove Proposition 21.1.5.

21.2. **Tate cohomology.** From now on, G is a fintie group. For any G-module X, we have the *norm map*

$$\mathrm{N}_G : X \longrightarrow X, \quad x \longmapsto \sum_{g \in G} g \cdot x.$$

We write $X[\mathrm{N}_G]$ for $\ker(\mathrm{N}_G : X \to X)$. Recall that $\mathbf{H}^0(G,X) = X^G$ and $\mathbf{H}_0(G,X) = X_G = X/I_G X$. It is easy to see that

$$\mathrm{N}_G(X) \subset X^G, \quad I_G X \subset X[\mathrm{N}_G].$$

Define

$$\widehat{\mathbf{H}}^0(G,X) := X^G/\,\mathrm{N}_G(X)$$

and

$$\widehat{\mathbf{H}}^{-1}(G,X) := X[\mathrm{N}_G]/I_G X.$$

Thus $\widehat{\mathbf{H}}^0(G,X)$ is a quotient group of $\mathbf{H}^0(G,X)$, and $\widehat{\mathbf{H}}^{-1}(G,X)$ is a subgroup of $\mathbf{H}_0(G,X)$.

Also define

$$\widehat{\mathbf{H}}^i(G,X) := \begin{cases} \mathbf{H}^i(G,X), & i \geq 1, \\ \mathbf{H}_{-i-1}(G,X), & i \leq -2. \end{cases}$$

Recall that since G is finite, coinduced G-modules are the same as induced G-modules. Thus relatively injective G-modules are the same as relatively projective G-modules, i.e., they are direct summands of (co)induced G-modules.

Lemma 21.2.1. *Let X be a relatively injective G-module. Then $\widehat{\mathbf{H}}^i(G,X) = 0$ for all $i \in \mathbb{Z}$.*

Proof. If $i \neq 0, -1$, then this is just Proposition 18.2.2. For $i = 0$ or -1, we may assume that $X = \mathrm{Ind}^G A$. Then $X \cong \bigoplus_{g \in G} A$, and G acts on X by permuting the coordiates. We have

$$X^G = \{(a_g)_{g \in G} \mid a_g = a_h, \forall g, h \in G\}.$$

Any element $(a_g)_{g \in G}$ of it can be written as $\mathrm{N}_G((a_1, 0, \cdots, 0))$. Hence $X^G = \mathrm{N}_G(X)$. Also

$$X[\mathrm{N}_G] = \left\{(a_g)_{g \in G} \mid \sum a_g = 0\right\}.$$

Any element $(a_g)_{g \in G}$ of it is equal to

$$\sum_{g \in G} (-a_g, 0, \cdots, 0, a_g, 0, \cdots, 0),$$

where $-a_g$ appears at the coordiate corresponding to $1 \in G$, and a_g appears at the g-th coordiate. Now each summand clearly lies in $I_G X$, so $X[\mathrm{N}_G] = I_G X$. □

Let $0 \to X \to Y \to Z \to 0$ be a short exact sequence of G-modules. There is a connecting homomorphism $\widehat{\mathbf{H}}^{-1}(G, Z) \to \widehat{\mathbf{H}}^{0}(G, X)$ defined as follows. Let $\alpha \in \widehat{\mathbf{H}}^{-1}(G, Z) = Z[\mathrm{N}_G]/I_G Z$. Find a lift $z \in Z[\mathrm{N}_G]$ of α, and find a lift $y \in Y$ of z. Since $\mathrm{N}_G(z) = 0$, we have $\mathrm{N}_G(y) \in X$. It is easy to see that $\mathrm{N}_G(y) \in X^G$. Its image in $\widehat{\mathbf{H}}^{0}(G, X) = X^G / \mathrm{N}_G(X)$ is independent of all choices.

One checks that the connecting homomorphism defined as above, together with the usual connecting homomorphisms for usual homology and cohomology, give rise to a doubly infinite long exact sequence

$$\cdots \to \widehat{\mathbf{H}}^{i}(G, X) \to \widehat{\mathbf{H}}^{i}(G, Y) \to \widehat{\mathbf{H}}^{i}(G, Z) \to \widehat{\mathbf{H}}^{i+1}(G, X) \to \cdots,$$

where i ranges over $\mathbb{Z}$. Moreover, this long exact sequence depends functorially on the short exact sequence $0 \to X \to Y \to Z \to 0$.

Remark 21.2.2. Given any G-module X, we know that there is a G-equivariant injection $X \to I$ and a G-equivariant surjection $P \to X$, where I and P are induced G-modules. In view of Lemma 21.2.1, the connecting homomorphisms induce isomorphisms $\widehat{\mathbf{H}}^{i}(G, X) \cong \widehat{\mathbf{H}}^{i-1}(G, I/X)$ and $\widehat{\mathbf{H}}^{i}(G, X) \cong \widehat{\mathbf{H}}^{i+1}(G, \ker(P \to X))$. This "dimension shifting" allows us to reduce the proofs of many properties of $\widehat{\mathbf{H}}^{i}(G, \dot{)}$ to the case $i = 0$. It also follows from the dimension shifting that the family of functors $\widehat{\mathbf{H}}^{i}(G, \cdot)$ together with the connecting homomorphisms is characterized by $\widehat{\mathbf{H}}^{0}(G, \cdot)$. (In other words, one can start with the definition of $\widehat{\mathbf{H}}^{0}(G, \cdot)$ and inductively define $\widehat{\mathbf{H}}^{i}(G, \cdot)$ for all $i \in \mathbb{Z}$ by dimension shifting.)

21.3. **Restriction and corestriction for Tate cohomology.** Let G be a finite group, and $H \leq G$ a subgroup. We have defined $\mathrm{Res} : \mathbf{H}^i(G, \cdot) \to \mathbf{H}^i(H, \cdot)$ and $\mathrm{Res} : \mathbf{H}_i(G, \cdot) \to \mathbf{H}_i(H, \cdot)$ for all $i \geq 0$. One checks that $\mathrm{Res} : \mathbf{H}^0(G, \cdot) \to \mathbf{H}^0(H, \cdot)$ factors through $\widehat{\mathbf{H}}^{0}(G, \cdot) \to \widehat{\mathbf{H}}^{0}(H, \cdot)$, and that $\mathrm{Res} : \mathbf{H}_0(G, \cdot) \to \mathbf{H}_0(H, \cdot)$ induces $\widehat{\mathbf{H}}^{-1}(G, \cdot) \to \widehat{\mathbf{H}}^{-1}(H, \cdot)$. Thus we have

$$\mathrm{Res} : \widehat{\mathbf{H}}^{i}(G, \cdot) \longrightarrow \widehat{\mathbf{H}}^{i}(H, \cdot)$$

for all $i \in \mathbb{Z}$. Moreover, we have the following characterization.

Proposition 21.3.1. *We have a family of natural transformations* $\mathrm{Res} : \widehat{\mathbf{H}}^i(G, \cdot) \to \widehat{\mathbf{H}}^i(H, \cdot)$*, for all* $i \in \mathbb{Z}$*, and this family is uniquely characterized by the following properties:*

(i) For each G*-module* X*, the map* $\mathrm{Res} : \widehat{\mathbf{H}}^0(G, X) \to \widehat{\mathbf{H}}^0(H, X)$ *is induced by the inclusion* $X^G \to X^H$*.*

(ii) These natural transformations are compatible with the connecting homomorphisms.

Proof. The uniqueness follows from dimension shifting. To prove that Res indeed satisfies condition (ii), we need to check that for a short exact sequence $0 \to A \to B \to C \to 0$, we have a commutative diagram

$$\begin{tikzcd}
\widehat{\mathbf{H}}^i(G, C) \arrow[r, "\delta"] \arrow[d, "\mathrm{Res}"] & \widehat{\mathbf{H}}^{i+1}(G, A) \arrow[d, "\mathrm{Res}"] \\
\widehat{\mathbf{H}}^i(H, C) \arrow[r, "\delta"] & \widehat{\mathbf{H}}^{i+1}(H, A)
\end{tikzcd}$$

Only the case $i = -1$ is essentially new. But in this case the compatibility can be checked using the explicit description of δ. □

Similarly, we have corestriction, characterized as follows.

Proposition 21.3.2. *We have a family of natural transformations* $\mathrm{Cor} : \widehat{\mathbf{H}}^i(G, \cdot) \to \widehat{\mathbf{H}}^i(H, \cdot)$*, for all* $i \in \mathbb{Z}$*, and this family is uniquely characterized by the following properties:*

(i) For each G*-module* X*, the map* $\mathrm{Cor} : \widehat{\mathbf{H}}^0(H, X) \to \widehat{\mathbf{H}}^0(G, X)$ *is induced by the norm map* $\mathrm{N}_{G/H} : X^H \to X^G$*.*

(ii) These natural transformations are compatible with the connecting homomorphisms.

Corollary 21.3.3. *For each* $i \in \mathbb{Z}$*, the composition*

$$\widehat{\mathbf{H}}^i(G, \cdot) \xrightarrow{\mathrm{Res}} \widehat{\mathbf{H}}^i(H, \cdot) \xrightarrow{\mathrm{Cor}} \widehat{\mathbf{H}}^i(G, \cdot)$$

is equal to multiplication by $[G : H]$*.*

Proof. Check this for $i = 0$ explicitly, and prove the general case by dimension shifting. □

Corollary 21.3.4. *For each* $i \in \mathbb{Z}$*, the abelian group* $\widehat{\mathbf{H}}^i(G, X)$ *is killed by* $|G|$*. It is finite if* X *is finitely generated as an abelian group.*

Proof. This is proved in the same way as Corollary 21.1.2 (but note that now the statement holds for all $i \in \mathbb{Z}$, since we have $\widehat{\mathbf{H}}^i(\{1\}, \cdot) = 0$ for all i). □

Remark 21.3.5. When X is finitely generated, the groups $\mathbf{H}^0(G, X) = X^G$ and $\mathbf{H}_0(G, X) = X_G$ need not be finite (e.g., they can both be X if G acts trivially on X).

Remark 21.3.6. For Tate cohomology, there is no natural way to define inflation $\mathrm{Inf} : \widehat{\mathbf{H}}^i(G/H, X^H) \to \widehat{\mathbf{H}}^i(G, X)$ for all i. (We do not have inflation for homology in general, so we run into trouble when $i \leq -2$.)

21.4. **Cup product.** We continue letting G be a finite group. For G-modules A and B, we define a G-module structure on $A \otimes B = A \otimes_{\mathbb{Z}} B$ by $g \cdot (a \otimes b) = ga \otimes gb$.

Proposition 21.4.1. *There is a unique family of $\mathbb{Z}$-bilinear pairings:*

$$\cup : \widehat{\mathbf{H}}^p(G, A) \otimes \widehat{\mathbf{H}}^q(G, B) \longrightarrow \widehat{\mathbf{H}}^{p+q}(G, A \otimes B), \quad p, q \in \mathbb{Z}$$

satisfying the following conditions:

(i) Functoriality in A and B.

(ii) For $p = q = 0$, this is induced by the natural map $A^G \otimes B^G \to (A \otimes B)^G$ by passing to quotients.

(iii) Suppose $0 \to A \to A' \to A'' \to 0$ is a short exact sequence of G-modules, and B is a G-module such that $0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0$ is still exact. Then for each $\beta \in \widehat{\mathbf{H}}^q(G, B)$ the following diagram commutes:

$$\begin{tikzcd}
\widehat{\mathbf{H}}^p(G, A'') \arrow[r, "\delta"] \arrow[d, "\cdot\cup\beta"] & \widehat{\mathbf{H}}^{p+1}(G, A) \arrow[d, "\cdot\cup\beta"] \\
\widehat{\mathbf{H}}^{p+q}(G, A'' \otimes B) \arrow[r, "\delta"] & \widehat{\mathbf{H}}^{p+q+1}(G, A \otimes B)
\end{tikzcd}$$

(iv) Suppose $0 \to B \to B' \to B'' \to 0$ and $0 \to A \otimes B \to A \otimes B' \to A \otimes B'' \to 0$ are exact. Then for each $\alpha \in \widehat{\mathbf{H}}^p(G, A)$ the following diagram commutes

$$\begin{tikzcd}
\widehat{\mathbf{H}}^q(G, B'') \arrow[r, "\delta"] \arrow[d, "(-1)^p\alpha\cup\cdot"] & \widehat{\mathbf{H}}^{q+1}(G, B) \arrow[d, "\alpha\cup\cdot"] \\
\widehat{\mathbf{H}}^{p+q}(G, A \otimes B'') \arrow[r, "\delta"] & \widehat{\mathbf{H}}^{p+q+1}(G, A \otimes B)
\end{tikzcd}$$

Proof. The uniqueness follows from dimension shifting. See [CF10, §IV.7] or [Bro82, §VI.5] for the proof of existence. □

22. Lecture 22, 4/20/2021

22.1. **Properties of cup product.**

Proposition 22.1.1. *The cup product satisfies the following properties. Let A, B, C be G-modules. Let $a \in \widehat{\mathbf{H}}^p(G, A), b \in \widehat{\mathbf{H}}^q(G, b), c \in \widehat{\mathbf{H}}^r(G, c)$.*

(i) We have

$$(a \cup b) \cup c = a \cup (b \cup c)$$

under the identification $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$.

(ii) We have $a \cup b = (-1)^{pq} b \cup a$ under the identification $A \otimes B \cong B \otimes A$.

(iii) Let $H \leq G$. Then $\mathrm{Res}(a \cup b) = \mathrm{Res}(a) \cup \mathrm{Res}(b)$, and $\mathrm{Cor}(a' \cup \mathrm{Res}(b)) = \mathrm{Cor}(a') \cup b$ for $a' \in \widehat{\mathbf{H}}^p(H, A)$.

Proof. All the properties can be checked directly for the cup product between $\widehat{\mathbf{H}}^0$. The general case is then proved by dimension shifting. For instance, let us check $\mathrm{Cor}(a' \cup \mathrm{Res}(b)) = \mathrm{Cor}(a') \cup b$ for $a' \in \widehat{\mathbf{H}}^0(H, A)$ and $b \in \widehat{\mathbf{H}}^0(G, B)$. We lift a' to an element $a' \in A^H$, and lift b to an element $b \in B^G$. Then $\mathrm{Cor}(a' \cup \mathrm{Res}(b))$ is represented by

$$\mathrm{N}_{G/H}(a' \otimes b) = \sum_{g \in G/H} ga' \otimes gb = \sum_{g \in G/H} ga' \otimes b = (\sum_{g \in G/H} ga') \otimes b.$$

But $\sum_{g/H} ga' \in A^G$ represents $\mathrm{Cor}(a')$. The desired identify follows. □

22.2. **The use of group cohomology in local CFT.** We shall use group cohomology to construct the local Artin map as follows. Let L/K be a finite abelian extension of local fields. Let $G = \mathrm{Gal}(L/K)$, and let $C = L^\times$ viewed as a G-module. We shall show that there is a distinguished element $\alpha \in \widehat{\mathbf{H}}^2(G, C)$ called the *fundamental class*, with the property that

$$\alpha \cup \cdot : \widehat{\mathbf{H}}^i(G, \mathbb{Z}) \longrightarrow \widehat{\mathbf{H}}^{i+2}(G, C \otimes \mathbb{Z}) = \widehat{\mathbf{H}}^{i+2}(G, C)$$

is an isomorphism for each $i \in \mathbb{Z}$. Applying this to $i = -2$, we obtain an isomorphism from $\mathbf{H}_1(G, \mathbb{Z}) = G^{\mathrm{ab}} = G$ to $\widehat{\mathbf{H}}^0(G, C) = K^\times / \mathrm{N}_{L/K}(L^\times)$. The inverse of this isomorphism can be thought of as a surjective homomorphism

$$K^\times \longrightarrow \mathrm{Gal}(L/K)$$

whose kernel is exactly $\mathrm{N}_{L/K}(L^\times)$. This will be our definition of the local Artin map.

Let G be an arbitrary finite group and C a G-module. We shall first investigate abstractly when a class $\alpha \in \widehat{\mathbf{H}}^2(G, C)$ has the property that $\alpha \cup \cdot : \widehat{\mathbf{H}}^i(G, \mathbb{Z}) \to \widehat{\mathbf{H}}^{i+2}(G, C)$ is an isomorphism for all $i \in \mathbb{Z}$. This is the content of Tate's theorem, which we will state and prove in the next lecture. Before that we need some preparations.

22.3. **Cohomology of finite cyclic groups.** Let G be a finite cyclic group of order n. The main result about cohomology of G is Theorem 22.3.3. Our approach follows [CF10, §IV.8]. See [Ser79, §VIII.4] for a different point of view.

Lemma 22.3.1. *The group $\widehat{\mathbf{H}}^2(G, \mathbb{Z})$ is cyclic of order n.*

Proof. We have a short exact sequence

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

where the last map is the augmentation map $\sum_g a_g[g] \mapsto \sum_g a_g$. Let s be a generator of G. We then have a short exact sequence

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

where the two maps are multiplication by $\sum_{g \in G}[g]$ and by $1 - [s]$ respectively. (To see that the map $\mathbb{Z}[G] \to I_G$ given yb multiplication is surjective, use that $1 - [s^k] = (1 - [s])(1 + [s] + \cdots + [s^{k-1}])$.) From these two short exact sequences, we obtain connecting homomorphisms

$$\widehat{\mathbf{H}}^0(G, \mathbb{Z}) \xrightarrow{\sim} \widehat{\mathbf{H}}^1(G, I_G)$$

and

$$\widehat{\mathbf{H}}^1(G, I_G) \xrightarrow{\sim} \widehat{\mathbf{H}}^2(G, \mathbb{Z})$$

both of which are isomorphisms since $\mathbb{Z}[G]$ is induced. Now note that $\widehat{\mathbf{H}}^0(G,\mathbb{Z}) = \mathbb{Z}/\operatorname{N}_G(\mathbb{Z}) = \mathbb{Z}/n$ (which holds for any finite group G of order n). Hence $\widehat{\mathbf{H}}^2(G,\mathbb{Z})$ is cyclic of order n. □

Lemma 22.3.2. *Let $x \in \widehat{\mathbf{H}}^0(G,\mathbb{Z}) = \mathbb{Z}/n$ be a generator. Then $x \cup \cdot$ defines an automorphism of $\widehat{\mathbf{H}}^i(G,A)$ for each $i \in \mathbb{Z}$ and each G-module A. (Here we identified $\mathbb{Z} \otimes A$ with A.)*

Proof. By dimension shifting, we reduce to the case $i = 0$. (To give more details, suppose $i > 0$. Find a short exact sequence $0 \to A \to P \to A' \to 0$ with P induced. Then the connecting homomorphism $\widehat{\mathbf{H}}^{i-1}(G,A') \to \widehat{\mathbf{H}}^i(G,A)$ is an isomorphism. This isomorphism is compatible with the endomorphisms on the two groups provided by $x \cup \cdot$, since the short exact sequence remains exact (in fact, unchanged) after tensoring with $\mathbb{Z}$. Thus we can lower i and reduce to the case $i = 0$. If $i < 0$, we find a short exact sequence $0 \to A' \to P \to A \to 0$ with P induced and argue similarly.)

When $i = 0$, the map in question is scalar multiplication by $x \in \mathbb{Z}/n$ on the $\mathbb{Z}/n$-module $\widehat{\mathbf{H}}^0(G,A) = A^G/N_G(A)$. Since $x \in (\mathbb{Z}/n)^\times$, this map is an automorphism. □

Theorem 22.3.3. *Let $x \in \widehat{\mathbf{H}}^2(G,\mathbb{Z})$ be a generator. Then $x \cup \cdot$ defines an isomorphism $\widehat{\mathbf{H}}^i(G,A) \to \widehat{\mathbf{H}}^{i+2}(G,A)$ for each $i \in \mathbb{Z}$ and each G-module A. (Here we identified $A \otimes \mathbb{Z}$ with A.) In particular, the isomorphism class of $\widehat{\mathbf{H}}^i(G,A)$ is periodic in i with period 2.*

Proof. Note that the two short exact sequences in Lemma 22.3.1 remain exact after $\otimes A$, since they are split in the category Ab. (All the three abelian groups $I_G, \mathbb{Z}[G], \mathbb{Z}$ are free.) Therefore the theorem reduces to Lemma 22.3.2 by the compatibility of cup product with connecting homomorphisms. □

Definition 22.3.4. For every G-module A, we write $h^q(A)$ for $\left|\widehat{\mathbf{H}}^q(G,A)\right|$ whenever it is finite. Define the *Herbrand quotient* to be $h(A) = h^0(A)/h^1(A)$ (whenever the two numbers are finite).

Proposition 22.3.5. *Let $0 \to A \to B \to C \to 0$ be a short exact sequence of G-modules. If two of $h(A), h(B), h(C)$ are defined, then so is the third, and we have $h(B) = h(A)h(C)$.*

Proof. In view of the periodicity of $\widehat{\mathbf{H}}^i(G,\cdot)$, we have an exact hexagon

$$\begin{tikzcd}
& \widehat{\mathbf{H}}^0(G,A) \arrow[r] & \widehat{\mathbf{H}}^0(G,B) \arrow[dr] & \\
\widehat{\mathbf{H}}^1(G,C) \arrow[ur] & & & \widehat{\mathbf{H}}^0(G,C) \arrow[dl] \\
& \widehat{\mathbf{H}}^1(G,B) \arrow[ul] & \widehat{\mathbf{H}}^1(G,A) \arrow[l] &
\end{tikzcd}$$

The statement easily follows. □

Proposition 22.3.6. *If A is a finite G-module, then $h(A) = 1$.*

Proof. First note that $h(A)$ is defined since all $\widehat{\mathbf{H}}^i(G, A)$ are finite. Let $s \in G$ be a generator. We have exact sequences

$$0 \to A^G \to A \xrightarrow{1-[s]} A \to A_G \to 0$$

and

$$0 \to \widehat{\mathbf{H}}^{-1}(G, A) \to A_G \xrightarrow{\mathrm{N}_G} A^G \to \widehat{\mathbf{H}}^0(G, A) \to 0.$$

The first shows that $\left|A^G\right| = |A_G|$, and the second shows that $h^0(A) = h^1(A)$. □

23. Lecture 23, 4/22/2021

23.1. **Tate's theorem.**

Let G be a finite group. Our approach to Tate's theorem (Theorem 23.1.5 below) follows [Neu13, §I.7]. See [Mil20, §II.3] for a different approach using splitting modules (which is Tate's original idea in his 1952 paper [Tat52]). See [CF10, Chap.IV, §§9 - 10] or [Ser79, §IX] for more refined versions of the theorem, whose proofs are more complicated.

Definition 23.1.1. A G-module A is called *cohomologically trivial*, if $\widehat{\mathbf{H}}^i(H, A) = 0$ for all subgroups $H \leq G$ and all $i \in \mathbb{Z}$.

Example 23.1.2. Recall that an induced G-module is also induced as an H-module, for any $H \leq G$. Hence induced G-modules, and more generally relatively projective G-modules, are cohomologically trivial.

Theorem 23.1.3. *A G-module A is cohomologically trivial if there exists $q \in \mathbb{Z}$ such that for all subgroups $H \leq G$ we have $\widehat{\mathbf{H}}^q(H, A) = \widehat{\mathbf{H}}^{q+1}(H, A) = 0$.*

Proof. Firstly, observe that we only need to show that

$$\widehat{\mathbf{H}}^{q-1}(G, A) = \widehat{\mathbf{H}}^{q+2}(G, A) = 0,$$

since we can recursively apply this result to conclude that $\widehat{\mathbf{H}}^i(G, A) = 0$ for all i, and then we can also replace G by its subgroups, to conclude the proof.

By dimension shifting we may assume that $q = 1$. (Since an induced G-module is cohomologically trivial, by dimension shifting we can find a G-module $A_\pm$ such that $\widehat{\mathbf{H}}^i(H, A_\pm) \cong \widehat{\mathbf{H}}^{i\pm 1}(H, A)$ for all subgroups $H \leq G$ and all $i \in \mathbb{Z}$.)

First assume that G is solvable. Then G admits a proper normal subgroup N such that G/N is cyclic. By induction we may assume that the theorem holds for N. Since A satisfies the same assumptions with G replaced by N, we know that A is cohomologically trivial as an N-module. It follows that for all $i \geq 1$, we have the inflation-restriction exact sequence

$$0 \to \mathbf{H}^i(G/N, A^N) \xrightarrow{\mathrm{Inf}} \mathbf{H}^i(G, A) \xrightarrow{\mathrm{Res}} \mathbf{H}^i(N, A) = 0.$$

Since $\mathbf{H}^i(G, A) = 0$ for $i \in \{1, 2\}$, we have $\mathbf{H}^i(G/N, A^N) = 0$ for $i \in \{1, 2\}$. But G/N is cyclic, so by periodicity-2 we know that $\widehat{\mathbf{H}}^i(G/N, A^N) = 0$ for all $i \in \mathbb{Z}$. By the above exact sequence for $i = 3$, we conclude that $\mathbf{H}^3(G, A) = 0$.

Since $\widehat{\mathbf{H}}^0(G/N, A^N) = \widehat{\mathbf{H}}^0(N, A) = 0$, we have

$$A^G = (A^N)^{G/N} = \mathrm{N}_{G/N}(A^N) = \mathrm{N}_{G/N}(\mathrm{N}_N A) = \mathrm{N}_G(A).$$

Hence $\widehat{\mathbf{H}}^0(G, A) = 0$. The proof of the theorem is complete for G solvable.

For general G, we fix a Sylow p-subgroup G_p for each prime p dividing $|G|$. Since G_p is solvable, we have $\widehat{\mathbf{H}}^i(G_p, A) = 0$ for all $i \in \mathbb{Z}$ by the above. Since $\mathrm{Cor}_{G/G_p} \circ \mathrm{Res}_{G/G_p} = [G : G_p]$ is coprime to p, we know that $\mathrm{Res}_{G/G_p} : \widehat{\mathbf{H}}^i(G, A) \to \widehat{\mathbf{H}}^i(G_p, A)$ is injective on the p-primary part. Thus the p-primary part of $\widehat{\mathbf{H}}^i(G, A)$ is zero for all i. Since $\widehat{\mathbf{H}}^i(G, A)$ is $|G|$-torsion, we conclude that $\widehat{\mathbf{H}}^i(G, A) = 0$. □

Lemma 23.1.4. *Let A, B be G-modules, and let $\alpha \in \widehat{\mathbf{H}}^0(G, A)$. Let $a \in A^G$ be a lift of α. Then for each $i \in \mathbb{Z}$, the map $\alpha \cup \cdot : \widehat{\mathbf{H}}^i(G, B) \to \widehat{\mathbf{H}}^i(G, A \otimes B)$ is the same as the functorial map induced by the G-homomorphism $B \to A \otimes B, b \mapsto a \otimes b$. (Note that the last map is indeed a G-homomorphism since a is G-invariant.)*

Proof. By dimension shifting (cf. the proof of Lemma 22.3.2) we easily reduce to the case $i = 0$, when the lemma is clear. □

Theorem 23.1.5 (Tate)**.** *Let A be a G-module. Let $p \in \mathbb{Z}$ be such that for each subgroup $H \leq G$, we have $\widehat{\mathbf{H}}^{p-1}(H, A) = 0$ and $\widehat{\mathbf{H}}^p(H, A) \cong \mathbb{Z}/|H|$. Then any generator α of $\widehat{\mathbf{H}}^p(G, A) \cong \mathbb{Z}/|G|$ has the property that the map*

$$\mathrm{Res}_{G/H}(\alpha) \cup \cdot : \widehat{\mathbf{H}}^i(H, \mathbb{Z}) \longrightarrow \widehat{\mathbf{H}}^{i+p}(H, A)$$

is an isomorphism for each $H \leq G$ and each $i \in \mathbb{Z}$.

Proof. We first observe that for any subgroup $H \leq G$, the element $\mathrm{Res}(\alpha) \in \widehat{\mathbf{H}}^p(H, A) \cong \mathbb{Z}/|H|$ is a generator. In fact, suppose its order is less than $|H|$. Then $\mathrm{Cor}\,\mathrm{Res}(\alpha) = [G : H]\alpha$ has order less than $|H|$, contradicting with the fact that α generates $\widehat{\mathbf{H}}^p(G, A) \cong \mathbb{Z}/|G|$. Thus we reduce to proving that

$$\alpha \cup \cdot : \widehat{\mathbf{H}}^i(G, \mathbb{Z}) \longrightarrow \widehat{\mathbf{H}}^{i+p}(G, A)$$

is an isomorphism for each $i \in \mathbb{Z}$.

Now to prove this statement, by dimension shifting we reduce to the case $p = 0$. Let $a \in A^G$ be a lift of α. By Lemma 23.1.4, we only need to show that the G-homomorphism

$$f : \mathbb{Z} \longrightarrow A, \quad n \longmapsto na$$

induces isomorphisms $\widehat{\mathbf{H}}^i(G, \mathbb{Z}) \xrightarrow{\sim} \widehat{\mathbf{H}}^i(G, A)$ for all $i \in \mathbb{Z}$. Up to replacing A by $A \oplus \mathbb{Z}[G]$ and replacing a by $a \oplus \sum_{g \in G}[g]$, we may assume that f is injective. (This is the key trick!) Let $A' = \mathrm{coker}(f)$. Then we have a short exact sequence

$$0 \to \mathbb{Z} \xrightarrow{f} A \to A' \to 0.$$

We only need to show that A' is cohomologically trivial as a G-module. Let $H \leq G$. Since $\widehat{\mathbf{H}}^{-1}(H, A) = 0$ by assumption and $\widehat{\mathbf{H}}^1(H, \mathbb{Z}) = \mathrm{Hom}_{\mathrm{gp}}(H, \mathbb{Z}) = 0$, we have an exact sequence

$$0 \to \widehat{\mathbf{H}}^{-1}(H, A') \to \widehat{\mathbf{H}}^0(H, \mathbb{Z}) \xrightarrow{(*)} \widehat{\mathbf{H}}^0(H, A) \to \widehat{\mathbf{H}}^0(H, A') \to 0,$$

where $(*)$ is the functorial map induced by f. If we can show that (*) is an isomorphism, then $\widehat{\mathbf{H}}^{-1}(H, A') = \widehat{\mathbf{H}}^0(H, A') = 0$, and so A' is cohomologically trivial by Theorem 23.1.3 since H is arbitrary. But (*) is an isomorphism since it sends $1 \in \widehat{\mathbf{H}}^0(H, \mathbb{Z}) = \mathbb{Z}/|H|$ to the image of a in $\widehat{\mathbf{H}}^0(H, A) = A^H/\mathrm{N}_H(A)$, which is a generator of $\widehat{\mathbf{H}}^0(H, A) \cong \mathbb{Z}/|H|$ by our first observation. □

24. Lecture 24, 4/27/2021

We shall apply Theorem 23.1.5 to the following situation. The integer p is 2. The group G is $\mathrm{Gal}(E/K)$, where E/K is a finite Galois extension of local fields. The G-module A is $E^\times$. Using Galois theory, the hypotheses of the theorem are translated to the following statement:

Theorem 24.0.1. *For every subextension L/K inside E, we have $\mathbf{H}^1(\mathrm{Gal}(E/L), E^\times) = 0$ and $\mathbf{H}^2(\mathrm{Gal}(E/L), E^\times)$ is cyclic of order $[E : L]$.*

We now study $\mathbf{H}^1$ and $\mathbf{H}^2$ in the above theorem. Note that it suffices to prove the theorem only for $L = K$ since the desired statements depend only on the extension E/L and are insensitive to K.

24.1. Hilbert 90 and consequences.

Let E/K be a finite Galois extension of fields, and let $G = \mathrm{Gal}(E/K)$. The groups $(E, +)$ and $E^\times$ are G-modules.

Proposition 24.1.1. *We have $\widehat{\mathbf{H}}^i(G, E) = 0$ for all $i \in \mathbb{Z}$.*

Proof. By the normal basis theorem, $E \cong \mathrm{Ind}^G K$ is an induced G-module. □

Theorem 24.1.2 (Hilbert 90). *We have $\mathbf{H}^1(G, E^\times) = 0$.*

Proof. Let ϕ be a 1-cocycle in $C^1(G, E^\times)$. Recall that this means ϕ is a function $G \to E^\times, s \mapsto \phi_s$ satisfying $\phi_{st} = \phi_s \cdot s(\phi_t)$. We need to show that ϕ is a coboundary, i.e., $\phi_s = b/s(b)$ for some fixed $b \in E^\times$.

Let $a \in E^\times$, and let

$$b := \sum_{t \in G} \phi_t \cdot t(a) \in E.$$

By the linear independence of the characters $t : E^\times \to E^\times$ (where t runs through G), we can find a such that $b \neq 0$. For $s \in G$, we compute

$$s(b) = \sum_{t \in G} s(\phi_t) \cdot (st)(a) = \sum_{t \in G} \frac{\phi_{st}}{\phi_s} \cdot (st)(a) = \phi_s^{-1} b.$$

Thus $\phi_s = b/s(b)$ as desired. □

Corollary 24.1.3 (Classical Hilber 90). *Assume that E/K is a cyclic extension. Let $s \in G$ be a generator. Then any element of E whose norm to K is 1 is of the form $s(a)/a$ for some $a \in E^\times$.*

Proof. Since G is cyclic, we have $\widehat{\mathbf{H}}^{-1}(G, E^\times) \cong \widehat{\mathbf{H}}^1(G, E^\times) = 0$. But $\widehat{\mathbf{H}}^{-1}(G, E^\times)$ is the quotient of $\ker(\mathrm{N}_{E/K} : E^\times \to K^\times)$ by $I_G \cdot E^\times = \{s(a)/a \mid a \in E^\times\}$. □

Corollary 24.1.4. *If K is a finite field , then $\widehat{\mathbf{H}}^i(G, E^\times) = 0$ for all $i \in \mathbb{Z}$. In particular, $\mathrm{N}_{E/K} : E^\times \to K^\times$ is surjective.*

Proof. In this case G is cyclic, and the Herbrand quotients $h(E^\times) = 1$ since $E^\times$ is finite. Thus the vanishing of $\widehat{\mathbf{H}}^1(G, E^\times)$ implies the vanishing of all $\widehat{\mathbf{H}}^i(G, E^\times)$. The "in particular" part follows from the vanishing of $\widehat{\mathbf{H}}^0(G, E^\times)$. □

Exercise 24.1.5. Let E/K be a finite extension of finite fields. Use elementary methods to show that $\mathrm{N}_{E/K} : E^\times \to K^\times$ is surjective.

24.2. **Brauer groups.** Let L/K and E/K be finite Galois extensions, with $E \subset L$. Write $G_{L/K}$ for $\mathrm{Gal}(L/K)$, etc. We have $G_{E/K} = G_{L/K}/G_{L/E}$, and $E^\times = (L^\times)^{G_{L/E}}$. Thus we have the inflation-restriction sequence

$$0 \to \mathbf{H}^q(G_{E/K}, E^\times) \xrightarrow{\mathrm{Inf}} \mathbf{H}^q(G_{L/K}, L^\times) \xrightarrow{\mathrm{Res}} \mathbf{H}^q(G_{L/E}, L^\times).$$

Recall that this sequence is exact if we know the vanishing of $\mathbf{H}^i(G_{L/E}, L^\times)$ for all $1 \leq i \leq q-1$ (see Proposition 20.2.2). Since $\mathbf{H}^1(G_{L/E}, L^\times) = 0$, the above sequence is exact for $q = 2$. We write $\mathrm{Br}(L/K)$ for $\mathbf{H}^2(G_{L/K}, L^\times)$, etc. Thus we have an exact sequence

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

We think of the first map as the inclusion. Define $\mathrm{Br}(K)$ to be the union of $\mathrm{Br}(L/K)$, where L runs thourgh all finite Galois extensions of K inside K^s. In other words, $\mathrm{Br}(K)$ is the direct limit of $\mathrm{Br}(L/K)$, where the transition maps are the injections $\mathrm{Inf} : \mathrm{Br}(L/K) \to \mathrm{Br}(L'/K)$ when $L \subset L'$. Note that when $L \subset L'$, the following diagram commutes:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Br}(E/K) \arrow[r, "\mathrm{Inf}"] \arrow[d, equal] & \mathrm{Br}(L/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{Inf}"] & \mathrm{Br}(L/E) \arrow[d, "\mathrm{Res}"] \\
0 \arrow[r] & \mathrm{Br}(E/K) \arrow[r, "\mathrm{Inf}"] & \mathrm{Br}(L'/K) \arrow[r, "\mathrm{Res}"] & \mathrm{Br}(L'/E)
\end{tikzcd}$$

(The commutativity follows easily from the fact that Inf and Res are induced by natural maps between the sets of cochains.) Thus we have an exact sequnece

$$0 \to \mathrm{Br}(E/K) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(E)$$

We have denoted the two maps still by Inf and Res respectively.

Example 24.2.1. If K is a finite field, then $\mathrm{Br}(K) = 0$ by Corollary 24.1.4.

Remark 24.2.2. It turns out that $\mathrm{Br}(K)$ can be identified with the *classical Brauer group* of K. Recall that this is the set of equivalence classes of central simple algebras over K. Two central simple algebras A and B over K are equivalent if and only if $A \cong M_n(D)$ and $B \cong M_m(D)$ for some integers n, m and a central division algebra D over K. (Here n and D are uniquely determined by A.) The group operation is given by $\otimes_K$. The subgroup $\mathrm{Br}(E/K) \subset \mathrm{Br}(K)$ is identified with the subgroup of the equivalence classes of central simple algebras over K which split over E (i.e., those A such that $A \otimes_K E \cong M_n(E)$). The map $\mathrm{Res} : \mathrm{Br}(K) \to \mathrm{Br}(E)$ is given by base changing the central simple algebras from K to E. The identification is given by an explicit construction, which starts with a 2-cocycle in $Z^2(G_{E/K}, E^\times)$ and gives a central simple algebra over K which splits over E. For details see [Ser79, §X.5] and [Mil20, §IV]. We will not need this relationship in our course.

Remark 24.2.3. By Wedderburn's Little Theorem, every finite division ring is a field. This shows that the classical Brauer group of a finite field vanishes. Compare with Example 24.2.1.

In order to finish the proof of Theorem 24.0.1, we need to show that when E/K is a finite Galois extension of local fields we have $\mathrm{Br}(E/K) \cong \mathbb{Z}/[E : K]$.

24.3. **The Brauer group of an unramified extension.** Let E/K be an unramified extension of local fields of degree n. We shall compute $\mathrm{Br}(E/K)$. Let $G = \mathrm{Gal}(E/K)$, and let $U = \mathcal{O}_E^\times$. We have a short exact sequence of G-modules

$$1 \to U \to E^\times \xrightarrow{v} \mathbb{Z} \to 0,$$

where v is the valuation.

Proposition 24.3.1. *The valuation $v : E^\times \to \mathbb{Z}$ induces an isomorphism $\widehat{\mathbf{H}}^i(G, E) \xrightarrow{\sim} \widehat{\mathbf{H}}^i(G, \mathbb{Z})$ for each $i \in \mathbb{Z}$.*

Proof. It suffices to show that $\widehat{\mathbf{H}}^i(G, U) = 0$ for all i. Let $U_0 = U$ and $U_j = 1 + \pi^j \mathcal{O}_E \subset U$ for $j \geq 1$. Recall that U is profinite and naturally isomorphic to $\varprojlim_j (U/U_j)$. Note that each U_j is G-stable. Using the perspective that Tate cohomology is given by cocycles modulo coboundaries, it is easy to see that the vanishing of $\widehat{\mathbf{H}}^i(G, U)$ follows from the vanishing of $\widehat{\mathbf{H}}^i(G, U_j/U_{j+1})$ for all $j \geq 0$. (For details, see [CF10, §VI.1.2, Lemma 3].)

When $j = 0$, we have $U_j/U_{j+1} \cong k_E^\times$, and the isomorphism is G-equivariant. We have $\widehat{\mathbf{H}}^i(G, k_E^\times) = \widehat{\mathbf{H}}^i(\mathrm{Gal}(k_E/k_K), k_E^\times)$ (here $G \cong \mathrm{Gal}(k_E/k_K)$), and we have seen the vanishing of this in Corollary 24.1.4.

When $j \geq 1$, we have a G-equivariant isomorphism $U_j/U_{j+1} \cong (k_E, +)$, and we have seen the vanishing of its cohomology in Proposition 24.1.1. □

Theorem 24.3.2. *We have a canonical isomorphism* $\mathrm{inv} : \mathrm{Br}(E/K) \xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

Proof. By Proposition 24.3.1, we have a canonical isomorphism $\mathrm{Br}(E/K) \cong \mathbf{H}^2(G, \mathbb{Z})$. Now G acts trivially on $\mathbb{Z}$, and we have a short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. We have $\widehat{\mathbf{H}}^i(G, \mathbb{Q}) = 0$ since on the one hand this is killed by $|G|$ and on the other hand multiplication by $|G|$ must be an automorphism since it is an automorphism on $\mathbb{Q}$.[10] Therefore the connecting homomorphism gives an isomorphism

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

The left hand side is just $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$, and this is canonically isomorphic to $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ by looking at where the Frobenius generator $\sigma \in G \cong \mathbb{Z}/n\mathbb{Z}$ goes to. In other words, we have $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z}, f \mapsto f(\sigma)$. □

25. Lecture 25, 4/29/2021

Remark 25.0.1. Let E/K be a finite unramified extension of local fields. We have seen in the proof of Proposition 24.3.1 that $\widehat{\mathbf{H}}^i(G_{E/K}, \mathcal{O}_E^\times) = 0$ for all $i \in \mathbb{Z}$. Applying this to $i = 0$ and using that $(\mathcal{O}_E^\times)^{G_{E/K}} = \mathcal{O}_K^\times$, we get the useful result that the norm map

$$\mathrm{N}_{E/K} : \mathcal{O}_E^\times \longrightarrow \mathcal{O}_K^\times$$

is surjective. It easily follows that the image of $\mathrm{N}_{E/K} : E^\times \to K^\times$ has index $[E : K]$ in $K^\times$. (Use that the norm of a uniformizer in E has valuation $[E : K]$.)

[10] We are using the following simple fact: For a G-module A and an integer n, the functorial endomorphism of $\widehat{\mathbf{H}}^i(G, A)$ induced by $A \to A, a \mapsto na$ is multiplicaiton by n. This can be seen using dimension shifting.

25.1. **Functoriality of** inv**.** Let K be a local field. For each $n \geq 1$, let K_n be the unique degree n unramified extension of K inside a fixed algebraic closure $\bar{K}$. We have constructed a canonical isomorphism

$$\mathrm{inv} : \mathrm{Br}(K_n/K) \xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

If $n|m$, then $K_n \subset K_m$. In this case we have a diagram

$$\begin{tikzcd}
\mathrm{Br}(K_n/K) \arrow[r, "\mathrm{inv}"] \arrow[d, "\mathrm{Inf}"] & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \arrow[d, "\mathrm{id}"] \\
\mathrm{Br}(K_m/K) \arrow[r, "\mathrm{inv}"] & \frac{1}{m}\mathbb{Z}/\mathbb{Z}
\end{tikzcd}$$

Chasing the constructions (especially using the compatibility of Inf with connecting homomorphisms), we see that the above diagram commutes.

We define $\mathrm{Br}(K^{\mathrm{ur}}/K) := \bigcup_n \mathrm{Br}(K_n/K)$. (This is a subgroup of $\mathrm{Br}(K)$, and we will later see that it is in fact equal to $\mathrm{Br}(K)$.) Then we have a canonical isomorphism

$$\mathrm{inv} : \mathrm{Br}(K^{\mathrm{ur}}/K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}.$$

We now let L/K be a possibly ramified (and possibly inseparable) finite extension inside $\bar{K}$. For each $n \geq 1$, we form the compositum LK_n inside $\bar{K}$. Then the extension LK_n/L is finite unramified (but its degree may be less than n). Thus we have

$$\mathrm{inv} : \mathrm{Br}(LK_n/L) \hookrightarrow \mathbb{Q}/\mathbb{Z}.$$

We have a pair of maps $\mathrm{Gal}(LK_n/L) \hookrightarrow \mathrm{Gal}(K_n/K), \tau \mapsto \tau|_{K_n}$ and $K_n^\times \hookrightarrow (LK_n)^\times$. They form a compatible pair, and therefore give rise to a change-of-group map

$$\mathrm{Res} : \mathrm{Br}(K_n/K) = \mathbf{H}^2(\mathrm{Gal}(K_n/K), K_n^\times) \longrightarrow \mathrm{Br}(LK_n/L) = \mathbf{H}^2(\mathrm{Gal}(LK_n/L), (LK_n)^\times).$$

Lemma 25.1.1. *The diagram*

$$\begin{tikzcd}
\mathrm{Br}(K_n/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}"] & \mathrm{Br}(LK_n/L) \arrow[d, "\mathrm{inv}"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "{[L:K]}"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

commutes.

Proof. Let $e = e(L/K)$ and $f = f(L/K)$. We have a commutative diagram

$$\begin{tikzcd}
\mathrm{Br}(K_n/K) \arrow[r, "v_K", "\cong"'] \arrow[d, "\mathrm{Res}"] & \mathbf{H}^2(G_{K_n/K}, \mathbb{Z}) \arrow[d, "e\cdot\mathrm{Res}"] & \mathbf{H}^1(G_{K_n/K}, \mathbb{Q}/\mathbb{Z}) \arrow[l, "\delta"', "\cong"] \arrow[r, hook] \arrow[d, "e\cdot\mathrm{Res}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "ef"] \\
\mathrm{Br}(LK_n/L) \arrow[r, "v_L", "\cong"'] & \mathbf{H}^2(G_{LK_n/L}, \mathbb{Z}) & \mathbf{H}^1(G_{LK_n/L}, \mathbb{Q}/\mathbb{Z}) \arrow[l, "\delta"', "\cong"] \arrow[r, hook] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

and the two rows define inv in the two cases. The first square commutes becasue $v_K = e \cdot v_L|_{K^\times}$. The second square commutes because Res is compatible with the connecting homomorphisms attached to $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. The third diagram commutes because the Frobenius generator in $\mathrm{Gal}(K_n/K)$ is the f-th power of the image of the Frobenius in $\mathrm{Gal}(LK_n/L)$ under the map $\mathrm{Gal}(LK_n/L) \to$

$\mathrm{Gal}(K_n/K)$. (To see this, note that the images of the two Frebenius elements in $\mathrm{Aut}(K_{k_n})$ are the automorphisms $x \mapsto x^{|k_K|}$ and $x \mapsto x^{|k_L|}$ respectively, and $|k_L| = |k_K|^f$.) □

Taking inductive limit over n, we obtain a commutative diagram

$$\begin{tikzcd}
\mathrm{Br}(K^{\mathrm{ur}}/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\cong"', "\mathrm{inv}"] & \mathrm{Br}(L^{\mathrm{ur}}/L) \arrow[d, "\cong"', "\mathrm{inv}"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "{[L:K]}"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

Thus the kernel of the first row is cyclic of order $[L : K]$. Note that if L/K is finite Galois, then this kernel is a subgroup of $\mathrm{Br}(L/K)$, since $\mathrm{Br}(L/K) \subset \mathrm{Br}(K)$ is the kernel of $\mathrm{Res} : \mathrm{Br}(K) \to \mathrm{Br}(L)$. Thus we have proved:

Lemma 25.1.2. *Let L/K be a degree n finite Galois extension (inside $\bar{K}$.) The group* $\mathrm{Br}(L/K)$ *contains the subgroup of* $\mathrm{Br}(K^{\mathrm{ur}}/K)$ *which is isomorphic to* $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ *under* $\mathrm{inv} : \mathrm{Br}(K^{\mathrm{ur}}/K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$. □

Our next goal is to show that the containment in the above lemma is in fact an equality. For this, it suffices to show the following result.

Theorem 25.1.3 (Second Fundamental Inequality)**.** *The order of* $\mathrm{Br}(L/K)$ *divides* $[L : K]$.

Corollary 25.1.4. *For every degree n Galois extension L/K,* $\mathrm{Br}(L/K)$ *is equal to* $\mathrm{Br}(K_n/K)$ *as subgroups of* $\mathrm{Br}(K)$. *In particular, there is a canonical isomorphism* $\mathrm{inv} : \mathrm{Br}(L/K) \xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. *We also have* $\mathrm{Br}(K) = \mathrm{Br}(K^{\mathrm{ur}}/K)$, *and there is a canonical isomorphism* $\mathrm{inv} : \mathrm{Br}(K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$. □

Remark 25.1.5. In the classical language, the above result says that every central simple algebra over K splits over a finite *unramified* extension of K. Moreover, the equivalence classes of central simple algebras are classified by an associated invariant in $\mathbb{Q}/\mathbb{Z}$.

At this point, we have proved Theorem 24.0.1, modulo proving the Second Fundamental Inequality.

25.2. **Proof of the Second Fundamental Inequality.** Our approach follows [CF10, §VI.1.4-VI.1.6] with slight simplifications.

Let L/K be a degree n Galois extension of local fields. Let $G = \mathrm{Gal}(L/K)$, and let $U = \mathcal{O}_L^\times$. Let $\pi = \pi_K$ be a uniformizer in K.

Lemma 25.2.1. *There exists a G-stable open subgroup V of U such that* $\widehat{\mathbf{H}}^i(G, V) = 0$ *for all $i \in \mathbb{Z}$.*

Proof. Let $\{e_1, \cdots, e_n\}$ be a normal basis for L/K, that is, it is a K-basis of L, and G permutes the e_i's simply transitively. Let $A = \mathcal{O}_L e_1 \oplus \cdots \oplus \mathcal{O}_L e_n \subset L$. Up to replacing e_i by $\pi^r e_i$ for a large integer r (common for all i), we may assume that each e_i lies in $\mathcal{O}_L$, and in particular $A \subset \mathcal{O}_L$. Note that A is open, since the topology on $L \cong K^n$ is just the product topology of the topology on K. Therefore there exists $N \geq 1$ such that $A \supset \pi^N \mathcal{O}_L$.

Let $M = \pi^{N+1}A$. We claim that $M \cdot M \subset \pi M$. In fact,

$$M \cdot M = \pi^{2N+2}A \cdot A \subset \pi^{2N+2}\mathcal{O}_L = \pi^{N+2}\pi^N\mathcal{O}_L \subset \pi^{N+2}A = \pi M.$$

Let $V = 1 + M$. We claim that V is an open, G-stable subgroup of U. To see that V is closed under multiplication, use that $M + M \subset M$ and $M \cdot M \subset \pi M \subset M$. To see that V is closed under inversion, use that $(1-m)^{-1} = 1 + \sum_{k\geq 1} m^k$ for all $m \in \mathfrak{m}_L$ (and in particular for all $m \in M$). For $m \in M$, the converging series $\sum_{k\geq 1} m^k$ lies in M since M is an open and hence closed subgroup of $\mathcal{O}_L$. Thus V is a subgroup of U. To see that V is open, note that $V = 1 + \pi^{N+1}A \supset 1 + \pi^{2N+1}A$, and the latter is an open subgroup of U. Finally, V is stable under G since G fixes π and stabilizes A.

It remains to show that $\widehat{\mathbf{H}}^i(G, V) = 0$ for all $i \in \mathbb{Z}$. We have a decreasing filtration

$$V = V_0 \supset V_1 \supset V_2 \supset \cdots$$

where $V_j = 1 + \pi_K^j M \subset V$. Since V is profinite (being an open subgroup of U), we have $V \cong \varprojlim_j V/V_j$. Moreover each V_j is G-stable. Thus as in the proof of Proposition 24.3.1, the vanishing of $\widehat{\mathbf{H}}^i(G, V)$ follows from the vanishing of $\widehat{\mathbf{H}}^i(G, V_j/V_{j+1})$ for all $j \geq 0$. We have a G-equivariant isomorphism $M/\pi_K M \xrightarrow{\sim} V_j/V_{j+1}, m \mapsto 1 + \pi_K^j m$. (To see that this is indeed a homomorphism, we need to use that $M \cdot M \subset \pi_K M$.) But $M/\pi_K M \cong A/\pi_K A \cong k_K e_1 \oplus \cdots k_K e_n \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} k_K$ is induced as a G-module. Hence V_j/V_{j+1} has trivial cohomology. □

26. Lecture 26, 5/4/2021

26.1. Proof of the Second Fundamental Inequality, continued.

Corollary 26.1.1. *Assume that L/K is a degree n cyclic extension of local fields. Let $U = \mathcal{O}_L^\times$. Then $|\mathrm{Br}(L/K)| = n$.*

Proof. Let $G = \mathrm{Gal}(L/K)$. Let $U = \mathcal{O}_L^\times$, and let $V \subset U$ be as in Lemma 25.2.1. Then the Herbrand quotient $h(V) = 1$, and $h(U/V) = 1$ because U/V is finite (since V is an open subgroup of the compact U). Thus we have $h(U) = h(V)h(U/V) = 1$. Since $L^\times/U \cong \mathbb{Z}$, we have $h(L^\times) = h(U)h(\mathbb{Z}) = h(\mathbb{Z})$. We compute that $\widehat{\mathbf{H}}^0(G, \mathbb{Z}) = \mathbb{Z}/n$ and $\widehat{\mathbf{H}}^{-1}(G, \mathbb{Z}) = 0$. Hence $h(\mathbb{Z}) = n$. This shows that $h(L^\times) = n$. But $\mathbf{H}^1(G, L^\times) = 0$ by Hilbert 90. Hence $\mathrm{Br}(L/K)$ has order n. □

Proof of Theorem 25.1.3. Let $G = \mathrm{Gal}(L/K)$. It suffices to show that for each prime p, the p-part of $|G|$ divides the p-part of $|\mathrm{Br}(L/K)|$. Let G_p be a Sylow-p subgroup of G, and let $K' = L^{G_p}$. We saw in the proof of Theorem 23.1.3 that $\mathrm{Res} : \widehat{\mathbf{H}}^i(G, \cdot) \to \widehat{\mathbf{H}}^i(G_p, \cdot)$ is injective on the p-primary part. If we know the theorem for the extension L/K' instead of L/K, then $\mathbf{H}^2(G_p, L^\times)$ has order dividing $|G_p|$, and it follows that the p-part of $\left|\mathbf{H}^2(G, L^\times)\right|$ divides $|G_p|$, which is the p-part of $|G|$.

Hence we can replace K by K' and replace G by G_p. Thus we may assume that G is a p-group, and in particular solvable. Let $H \leq G$ be a proper normal subgroup such that G/H is cyclic. Let $E = L^H$. By induction we may assume that the theorem holds for E/K. Also the theorem holds for L/E by Corollary 26.1.1, since L/E is cyclic. Now we have the exact sequence

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

Thus $|\mathrm{Br}(L/K)|$ divides $|\mathrm{Br}(E/K)| \cdot |\mathrm{Br}(L/E)| = \left|G_{E/K}\right| \left|\cdot G_{L/E}\right| = |G|$. □

26.2. **The local Artin map.** At this point, we have verified the axioms in Tate's theorem in the setting of a finite Galois extension of local fields, i.e., we have proved Theorem 24.0.1. We summarize the results as follows:

Theorem 26.2.1. *Let L/K be a degree n Galois extension of local fields. Then $\mathrm{Br}(L/K) = \mathrm{Br}(K_n/K)$ as subgroups of $\mathrm{Br}(K)$, and we have a canonical isomorphism*

$$\mathrm{inv} : \mathrm{Br}(L/K) = \mathrm{Br}(K_n/K) \xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

Define

$$u_{L/K} := \mathrm{inv}^{-1}(\frac{1}{n}) \in \mathrm{Br}(L/K),$$

called the fundamental class. *By Tate's theorem, the map*

$$u_{L/K} \cup \cdot : \widehat{\mathbf{H}}^q(G_{L/K}, \mathbb{Z}) \longrightarrow \widehat{\mathbf{H}}^{q+2}(G_{L/K}, L^\times)$$

is an isomorphism for each $q \in \mathbb{Z}$. □

Definition 26.2.2. In the setting of Theorem 26.2.1, taking $q = -2$ we have the isomorphism

$$G_{L/K}^{\mathrm{ab}} \cong \widehat{\mathbf{H}}^{-2}(G_{L/K}, \mathbb{Z}) \xrightarrow{\sim} \widehat{\mathbf{H}}^{0}(G_{L/K}, L^\times) = K^\times / \mathrm{N}_{L/K}(L^\times).$$

We denote the inverse isomorphism by $\phi_{L/K}$. Sometimes we also think of $\phi_{L/K}$ as a surjective homomorphism $K^\times \to G_{L/K}^{\mathrm{ab}}$ whose kernel is exactly $\mathrm{N}_{L/K}(L^\times)$.

Lemma 26.2.3. *Let G be a finite group, and let B be a G-module. Let $g \in G$ and $\beta \in Z^1(G, B)$ (a 1-cocycle $G \to B$). Let $\bar{g}$ be the image of g in $G^{\mathrm{ab}} = \widehat{\mathbf{H}}^{-2}(G, \mathbb{Z})$, and let $\bar{\beta}$ be the image of β in $\widehat{\mathbf{H}}^{1}(G, B)$. Then the element $\bar{g} \cup \bar{\beta} \in \widehat{\mathbf{H}}^{-1}(G, B) = B[\mathrm{N}_G]/I_G B$ is represented by $\beta(g) \in B$.*[11]

Proof. See [Ser79, App. to Chap. XI, Lem. 3] or [Neu13, I.5.7]. □

Lemma 26.2.4. *Keep the setting of Theorem 26.2.1. Let $G = G_{L/K}$. Let $f \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = \widehat{\mathbf{H}}^{1}(G, \mathbb{Q}/\mathbb{Z})$, and let $a \in K^\times$. Note that f factors through G^{ab}, so $f(\phi_{L/K}(a)) \in \mathbb{Q}/\mathbb{Z}$ is well defined. We have*

$$f(\phi_{L/K}(a)) = \mathrm{inv}(\bar{a} \cup \delta f),$$

where δf is the image of f in $\widehat{\mathbf{H}}^{2}(G, \mathbb{Z})$ under the connecting homomorphism associated with $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$, and $\bar{a} \in \widehat{\mathbf{H}}^{0}(G, L^\times) = K^\times / \mathrm{N}(L^\times)$ is the image of a.

Remark 26.2.5. Clearly the element $\phi_{L/K}(a) \in G^{\mathrm{ab}}$ is characterized by the values $f(\phi_{L/K}(a))$ for all f.

Proof of Lemma 26.2.4. Write g for $\phi_{L/K}(a) \in \widehat{\mathbf{H}}^{-2}(G, \mathbb{Z})$. Write u for the fundamental class $u_{L/K}$. By the definition of $\phi_{L/K}$, we have

$$\bar{a} = u \cup g \in \widehat{\mathbf{H}}^{0}(G, L^\times).$$

[11] Note that $\mathrm{N}_G(\beta(g)) = \sum_{h \in G} h(\beta(g)) = \sum_h \beta(hg) - \beta(h) = 0$, so indeed $\beta(g) \in B[\mathrm{N}_G]$.

Thus

$$\bar{a} \cup \delta f = (u \cup g) \cup \delta f = u \cup (g \cup \delta f) = u \cup \delta(g \cup f).$$

Here $g \cup f$ lies in $\widehat{\mathbf{H}}^{-1}(G, \mathbb{Q}/\mathbb{Z})$, and δ of it lies in $\widehat{\mathbf{H}}^{0}(G, \mathbb{Z})$. Note that $\widehat{\mathbf{H}}^{-1}(G, \mathbb{Q}/\mathbb{Z})$ is the n-torsion of $\mathbb{Q}/\mathbb{Z}$, namely $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. By Lemma 26.2.3, the element $g \cup f \in \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ is equal to $f(g)$. Write $f(g) = r/n \mod \mathbb{Z}$. Then $\delta(g \cup f) = \delta(r/n) \in \widehat{\mathbf{H}}^{0}(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ is represented by $\mathrm{N}_G(r/n) = n \cdot r/n = r \in \mathbb{Z}$. Thus from the above computation we have

$$\bar{a} \cup \delta f = u \cup \bar{r} = r \cdot u.$$

The inv of this element is $r \cdot \mathrm{inv}(u) = r/n \mod \mathbb{Z}$ (since $\mathrm{inv}(u) = 1/n \mod \mathbb{Z}$), which is equal to $f(g)$ as desired. □

Let L/K be a finite abelian extension. We shall take $\phi_{L/K} : K^\times \to G_{L/K} = G_{L/K}^{\mathrm{ab}}$ as above as the definition of the local Artin map. We need to check the following compatibility:

Lemma 26.2.6. *Let $L' \supset L$ be two finite Galois extensions of K. The following diagram commutes:*

$$\begin{tikzcd} K^\times \arrow[r, "\phi_{L'/K}"] \arrow[d, equal] & G_{L'/K}^{\mathrm{ab}} \arrow[d, "\pi"] \\ K^\times \arrow[r, "\phi_{L/K}"] & G_{L/K}^{\mathrm{ab}} \end{tikzcd}$$

Here π is induced by the canonical projection $G_{L'/K} \to G_{L/K}$.

Proof. Write G and G' for $G_{L/K}$ and $G_{L'/K}$ respectively. Let $a \in K^\times$. Let $g = \phi_{L/K}(a) \in G^{\mathrm{ab}}$, and let $g' = \phi_{L'/K}(a) \in G'^{\mathrm{ab}}$. We need to show that $\pi(g') = g$.

Let $f \in \widehat{\mathbf{H}}^{1}(G, \mathbb{Q}/\mathbb{Z})$ be an arbitrary element, and let $f' = \mathrm{Inf}(f) \in \widehat{\mathbf{H}}^{1}(G', \mathbb{Q}/\mathbb{Z})$. If we think of f and f' as characters $G^{\mathrm{ab}} \to \mathbb{Q}/\mathbb{Z}$ and $G'^{\mathrm{ab}} \to \mathbb{Q}/\mathbb{Z}$, then $f' = f \circ \pi$. By duality, in order to show that $\pi(g') = g$, we only need to show that $f'(g') = f(g)$.

By Lemma 26.2.4 we have

$$f'(g') = \mathrm{inv}(\bar{a} \cup \delta f')$$

Since the operations $\delta(\cdot)$, $\bar{a} \cup \cdot$, and $\mathrm{inv}(\cdot)$ are all compatible with inflation, the right hand side is equal to $\mathrm{inv}(\bar{a} \cup \delta f)$, which is equal to $f(g)$. □

By Lemma 26.2.6, we can define the local Artin map

$$\phi_K : K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

by taking the inverse limit of $\phi_{L/K}$ over all finite abelian extensions L/K. Comparing with Theorem 8.2.3, we see that condition (ii) in that theorem is satisfied by construction. We still need to check condition (i):

Lemma 26.2.7. *Let $\pi \in K$ be a uniformizer. Then $\phi_K(\pi)$ acts as the Frobenius σ on K^{ur}.*

Proof. Let n be an arbitrary positive integer. Write G for $G_{K_n/K}$. Let $\sigma' = \phi_{K_n/K}(\pi)$. It suffices to show that σ' is equal to the Frobenius $\sigma \in G$. Let $f \in \widehat{\mathbf{H}}^{1}(G, \mathbb{Q}/\mathbb{Z})$. We have

$$f(\sigma') = \mathrm{inv}(\bar{\pi} \cup \delta f).$$

Recall that inv : $\mathrm{Br}(K_n/K) \xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ is the composition

$$\mathrm{Br}(K_n/K) \xrightarrow{v} \widehat{\mathbf{H}}^2(G,\mathbb{Z}) \xrightarrow{\delta^{-1}} \widehat{\mathbf{H}}^1(G,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{ev}_\sigma} \mathbb{Q}/\mathbb{Z},$$

where ev_σ is the evaluation of elements of $\mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$ at σ. We have $v(\bar{\pi} \cup \delta f) = v(\pi) \cdot \delta f = \delta f$. Hence

$$f(\sigma') = \mathrm{ev}_\sigma \circ \delta^{-1}(\delta(f)) = \mathrm{ev}_\sigma(f) = f(\sigma).$$

Since f is arbitrary, this shows that $\sigma = \sigma'$. □

We have finished the proof of Theorem 8.2.3.

27. Lecture 27, 5/6,2021

27.1. **Functoriality properties of the local Artin map.** As a bonus of the cohomological method, we have the following functorial properties of the local Artin map. When $H \le G$ are finite groups, we define the *transfer map* $V : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ to be the composition

$$G^{\mathrm{ab}} = \widehat{\mathbf{H}}^{-2}(G,\mathbb{Z}) \xrightarrow{\mathrm{Res}} \widehat{\mathbf{H}}^{-2}(H,\mathbb{Z}) = H^{\mathrm{ab}}.$$

(Here V stands for *verlagerung*.) It has an explicit description, see Proposition 21.1.5.

Theorem 27.1.1. *Let K be a local field. Let K'/K be a finite separable extension inside K^s. (In particular, ${K'}^{\mathrm{ab}} \supset K^{\mathrm{ab}}$.) The following diagrams commute*

$$\begin{tikzcd}
K'^{\times} \arrow[r, "\phi_{K'}"] \arrow[d, "\mathrm{N}_{K'/K}"'] & \mathrm{Gal}({K'}^{\mathrm{ab}}/K') \arrow[d, "i"] \\
K^{\times} \arrow[r, "\phi_K"] & \mathrm{Gal}(K^{\mathrm{ab}}/K)
\end{tikzcd}$$

$$\begin{tikzcd}
K'^{\times} \arrow[r, "\phi_{K'}"] & \mathrm{Gal}({K'}^{\mathrm{ab}}/K') \\
K^{\times} \arrow[r, "\phi_K"] \arrow[u, "incl"] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[u, "V"']
\end{tikzcd}$$

Here $i(\tau) = \tau|_{K^{\mathrm{ab}}}$, and V is the topological transfer map *defined as follows. Let L be a common Galois extension of K' and K. Then $G_{L/K'} \subset G_{L/K}$, and we have the transfer map $G^{\mathrm{ab}}_{L/K} \to G^{\mathrm{ab}}_{L/K'}$. We define V to be the inverse limit of these maps over all L.*

Sketch of proof. Let L be a common finite Galois extension of K' and K. Let $G = G_{L/K}$ and $H = G_{L/K'} \le G$. It suffices to prove the commutativity of the following diagrams:

$$\begin{tikzcd}
\widehat{\mathbf{H}}^{0}(H, L^{\times}) \arrow[d, "\mathrm{Cor}"'] & \widehat{\mathbf{H}}^{-2}(H,\mathbb{Z}) \arrow[l, "u_{L/K'} \cup \cdot"'] \arrow[d, "\mathrm{Cor}"] \\
\widehat{\mathbf{H}}^{0}(G, L^{\times}) & \widehat{\mathbf{H}}^{-2}(G,\mathbb{Z}) \arrow[l, "u_{L/K} \cup \cdot"']
\end{tikzcd}$$

$$\begin{tikzcd}
\widehat{\mathbf{H}}^0(H, L^\times) & \widehat{\mathbf{H}}^{-2}(H, \mathbb{Z}) \arrow[l, "u_{L/K'} \cup \cdot"'] \\
\widehat{\mathbf{H}}^0(G, L^\times) \arrow[u, "\mathrm{Res}"] & \widehat{\mathbf{H}}^{-2}(G, \mathbb{Z}) \arrow[l, "u_{L/K} \cup \cdot"'] \arrow[u, "\mathrm{Res}"']
\end{tikzcd}$$

For the second diagram, we use $\mathrm{Res}(u_{L/K}) = u_{L/K'}$, which follows from Lemma 25.1.1, and we use the formula $\mathrm{Res}(a \cup b) = \mathrm{Res}(a) \cup \mathrm{Res}(b)$. For the first diagram, we must show $u_{L/K} \cup \mathrm{Cor}(\beta) = \mathrm{Cor}(u_{L/K'} \cup \beta)$. Now the right hand side is

$$\mathrm{Cor}(\mathrm{Res}(u_{L/K}) \cup \beta) = u_{L/K} \cup \mathrm{Cor}(\beta).$$

□

27.2. **Connection with Lubin–Tate theory.** Let K be a local field. Recall that for each uniformizer π in K, we have constructed a tower of fields $K_\pi = \bigcup_n K_{\pi,n}$. The compositum $K^{\mathrm{LT}} := K^{\mathrm{ur}} \cdot K_\pi$ is a subfield of K^{ab}, and we have shown that it is independent of π (Theorem 16.2.1). Also, we have constructed a homomorphism

$$\phi_\pi : K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{LT}}/K),$$

and shown that it is independent of π. We denote ϕ_π by ϕ', and denote the local Artin map $\phi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ by ϕ. We have

$$\phi'(\pi)|_{K^{\mathrm{ur}}} = \sigma, \quad \phi'(\pi)|_{K_\pi} = \mathrm{id}\,.$$

For $a \in \mathcal{O}_K^\times$, the element $\phi'(a)$ acts trivially on K^{ur}, and its action on $K_{\pi,n} = K(\Lambda_{f,n})$ (where $f \in \mathcal{F}_\pi$) is induced by the action of a^{-1} on the $\mathcal{O}_K/\pi^n$-module $\Lambda_{f,n}$. Let

$$U_{r,n} = \pi^{r\mathbb{Z}} \times (1 + \pi^n \mathcal{O}_K) \subset K^\times$$

for $r, n \geq 1$. In particular, elements of $\phi'(U_{r,n})$ act trivially on $K_{\pi,n}$.

Theorem 27.2.1. *We have $K^{\mathrm{LT}} = K^{\mathrm{ab}}$, and $\phi' = \phi$.*

Lemma 27.2.2. *For $a \in K^\times$, we have $\phi(a)|_{K^{\mathrm{LT}}} = \phi'(a)$.*

Proof. Since $K^\times$ is generated by uniformizers, we may assume that a is a uniformizer π. Then $\phi(\pi)$ and $\phi'(\pi)$ both act as σ on K^{ur}. It remains to check that $\phi(\pi)$ acts trivially on $K_{\pi,n}$ for each n. Recall that the kernel of $K^\times \xrightarrow{\phi} \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(K_{\pi,n}/K)$ is $\mathrm{N}_{K_{\pi,n}/K}(K_{\pi,n}^\times)$. Hence it suffices to check that π is a norm from $K_{\pi,n}^\times$. But this was proved in Theorem 15.1.3. □

For $r, n \geq 1$, let $K_{r,n} = K_r K_{\pi,n}$ (where K_r/K is the degree r unramified extension), and let $N_{r,n} := \mathrm{N}_{K_{r,n}/K}(K_{r,n}^\times)$.

Lemma 27.2.3. *We have $U_{r,n} = N_{r,n}$.*

Proof. We know that $N_{r,n}$ consists of those $a \in K^\times$ such that $\phi(a)$ acts trivially on $K_{r,n}$. Since $\phi(a) = \phi'(a)$ on K^{LT} and since $\phi'(U_{r,n})$ acts trivially on $K_{\pi,n}$ and on K_r, we know that

$$N_{r,n} \supset U_{r,n}$$

. On the other hand, the index of $N_{r,n}$ in $K^\times$ equals $[K_{r,n} : K]$, and we have computed in Theorem 15.1.3 that this number is equal to $r[K_{\pi,n} : K] = r(q-1)q^{n-1}$. We observe that this number is equal to the index of $U_{r,n}$ in $K^\times$. Hence $N_{r,n} = U_{r,n}$.

□

Proof of Theorem 27.2.1. We only need to show that an arbitrary finite abelian extension L/K is contained inside K^{LT}. The norm subgroup $\mathrm{N}_{L/K}(L^\times)$ is open and finite index in $K^\times$ (by Corollary 9.1.6, which is valid here since we already have the existence of ϕ_K). Therefore $\mathrm{N}_{L/K}(L^\times)$ contains $U_{r,n}$ for sufficiently large r, n. For $a \in K^\times$, using $U_{r,n} = N_{r,n}$ we have

$$\phi(a)|_{K_{r,n}} = \mathrm{id} \Leftrightarrow a \in N_{r,n} \Leftrightarrow a \in U_{r,n} \Rightarrow a \in \mathrm{N}_{L/K}(L^\times) \Leftrightarrow \phi(a)|_L = \mathrm{id}\,.$$

Let M be an abelian extension of K containing L and $K_{r,n}$. Since the map $\phi_{M/K} : K^\times \to G_{M/K}$ is surjective, the above shows that any element $\tau \in G_{M/K}$ fixing $K_{r,n}$ also fixes L. This implies that $L \subset K_{r,n}$ by Galois theory. Thus $L \subset K^{\mathrm{LT}}$ as desired. □

We can now also prove the Local Existence Theorem.

Proof of Theorem 9.2.1. If U is an open finite index subgroup of $K^\times$, then U contains $U_{r,n}$ for sufficienty large r, n. Since $U_{r,n} = N_{r,n}$ is a norm subgroup, so is U, see Corollary 8.3.4. □

We have finished the proof of the two main theorems of local CFT, with the additional knowledge Theorem 27.2.1, which gives an explicit description of K^{ab} and the local Artin map.

27.3. **The group of ideles.** Let K be a global field. We define the group of ideles $\mathbb{A}_K^\times = \mathbb{I}_K$ to be the *restricted product*

$$\prod_v{}' K_v^\times ,$$

where v runs through all the places of K. This means that elements of $\mathbb{I}_K$ are tuples $(a_v)_v \in \prod_v K_v^\times$ such that $a_v \in \mathcal{O}_{K_v}$ for almost all v. We define the topology on $\mathbb{I}_K$ by declaring a basis of open sets to be sets of the form $\prod_v V_v$, where each V_v is an open subset of $K_v^\times$, and $V_v = \mathcal{O}_{K_v}^\times$ for almost all v. Under this topology, $\mathbb{I}_K$ is a topological group, and it is locally compact and Hausdorff.

The diagonal embedding $K^\times \to \prod_v K_v^\times$ factors through $\mathbb{I}_K$. We shall henceforth think of $K^\times$ as a subgroup of $\mathbb{I}_K$. It is a discrete subgroup, with respect to the topology on $\mathbb{I}_K$.

Definition 27.3.1. For a finite extension L/K, we define the norm map

$$\mathrm{N}_{L/K} : \mathbb{I}_L \longrightarrow \mathbb{I}_K$$

as follows. For $b = (b_w)_w \in \mathbb{I}_L$, the v-th component of $\mathrm{N}_{L/K}(b)$ is $\prod_{w|v} \mathrm{N}_{L_w/K_v}(b_w)$. Note that the norm map restricts to the usual norm map $L^\times \to K^\times$.

28. Lecture 28, 5/11/2021

28.1. **The global Artin map.** Let L/K be a finite abelian extension. Let v be a place of K and let w be a place of L over v. The decomposition subgroup $D(w/v) \subset G_{L/K}$ is canonically identified with $\mathrm{Gal}(L_w/K_v)$. If we choose a K_v-algebra embedding $L_w \to \bar{K}_v$, then we have a surjective map $\mathrm{Gal}(\bar{K}_v/K_v) \to D(w/v)$ (which factors uniquely through $\mathrm{Gal}(K_v^{\mathrm{ab}}/K_v)$). This map is independent of the embedding $L_w \to \bar{K}_v$, since the maps resulting from different choices will differ by conjugation on the target, and the target is abelian. We thus have a map

$$i_v^L : \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \longrightarrow D(w/v) \subset G_{L/K}.$$

Since $G_{L/K}$ is abelian, the subgroup $D(w/v)$ depends only on v and is independent of w. Moreover, the map i_v^L is depends only on v and is independent of w.

Exercise 28.1.1. Verify the last statement.

Remark 28.1.2. The CFT for a local archimedian field is almost trivial. For $K = \mathbb{C}$, the local Artin map ϕ_K is the trivial map $\mathbb{C}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{C}) = 1$. For $K = \mathbb{R}$, the local Artin map ϕ_K is the map $\mathrm{sgn} : \mathbb{R}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \{\pm 1\}$. In this case, we have $\mathrm{Br}(\mathbb{R}) = \mathrm{Br}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$ (by explicit computation using cocycles; the non-trivial element corresponds to the Hamilton quaternion algebra), and the local Artin map has the same cohomological description, i.e., it is inverse to the map $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to \mathbb{R}^\times / \mathrm{N}_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times)$ given by cupping with a generator of $\mathrm{Br}(\mathbb{R})$.

Definition 28.1.3. Let L/K be a finite abelian extension. We define the *global Artin map* by the formula

$$\begin{aligned} \phi_{L/K} : \mathbb{I}_K &\longrightarrow G_{L/K} \\ (a_v)_v &\longmapsto \prod_v i_v^L(\phi_{K_v}(a_v)), \end{aligned} \tag{28.1.3.1}$$

where ϕ_{K_v} is the local Artin map. Note that the product is finite, since for almost all v we have $a_v \in \mathcal{O}_{K_v}^\times$ and L is unramified over v, and we know that $\phi_{K_v}(a_v)$ acts trivially on K_v^{ur}.

If L and L' are two finite abelian extensions of K with $L \subset L'$, then the maps $\phi_{L/K}$ and $\phi_{L'/K}$ are compatible with the projection $G_{L/K} \to G_{L'/K}$, which follows from the analogous property of the local Artin maps. Hence by taking the inverse limit over L we obtain the global Artin map

$$\phi_K : \mathbb{I}_K \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

(However, the number of nontrivial terms in the product (28.1.3.1) can increase as L gets larger and larger.)

28.2. **Statements of global CFT.**

Theorem 28.2.1 (Global Reciprocity Law)**.** *The map ϕ_K factors through the quotient $\mathbb{I}_K/K^\times$. For each finite abelian extension L/K, the map $\phi_{L/K} : \mathbb{I}_K \to G_{L/K}$ is surjective, and its kernel is $K^\times \cdot \mathrm{N}_{L/K}(\mathbb{I}_L)$.*

We write C_K for $\mathbb{I}_K/K^\times$, called the *idele class group*. We equip it with the quotient topology. For any finite extension L/K, the map $\mathrm{N}_{L/K} : \mathbb{I}_L \to \mathbb{I}_K$ descends to a map $\mathrm{N}_{L/K} : C_L \to C_K$. The Global Reciprocity Law is equivalent to the statement that for L/K finite abelian, $\phi_{L/K}$ induces an isomorphism

$$C_K / \mathrm{N}_{L/K}(C_L) \xrightarrow{\sim} G_{L/K}.$$

Theorem 28.2.2 (Global Existence Theorem)**.** *The open finite index subgroups of C_K are precisely those of the form $\mathrm{N}_{L/K}(C_L)$ for finite abelian extensions L/K.*

As in the local case, from the above two theorems we deduce that the map $L \mapsto \mathrm{N}_{L/K}(C_L)$ is a bijection from the set of finite abelian extensions of K (inside a fixed $\bar{K}$) to the set of open finite index subgroups of C_K.

Theorem 28.2.3 (Functoriality of the global Artin map)**.** *Let K be a global field. Let K'/K be a finite separable extension inside K^s. The following diagrams commute*

$$\begin{tikzcd}
C_{K'} \arrow[r, "\phi_{K'}"] \arrow[d, "\mathrm{N}_{K'/K}"'] & \mathrm{Gal}(K'^{\mathrm{ab}}/K') \arrow[d, "i"] \\
C_K \arrow[r, "\phi_K"] & \mathrm{Gal}(K^{\mathrm{ab}}/K)
\end{tikzcd}$$

$$\begin{tikzcd}
C_{K'} \arrow[r, "\phi_{K'}"] & \mathrm{Gal}(K'^{\mathrm{ab}}/K') \\
C_K \arrow[r, "\phi_K"] \arrow[u, "j"] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[u, "V"']
\end{tikzcd}$$

Here $i(\tau) = \tau|_{K^{\mathrm{ab}}}$, j is induced by the inclusion $K \hookrightarrow K'$, and V is the topological transfer map defined in the same way as in Theorem 27.1.1.

28.3. **Passing to the ideal theoretic formulation.** For simplicity, we only work with number fields K. For each non-archimedean place v of K, we write $\mathfrak{p}_v$ for the corresponding prime ideal of $\mathcal{O}_K$.

Recall that a *modulus for K* is a formal product

$$\mathfrak{m} = \prod_v v^{e(v)}$$

where v runs through all the places of K, satisfying that

(i) $e(v) \in \mathbb{Z}_{\geq 0}$, and $e(v) = 0$ for almost all v.
(ii) If v is a complex place, then $e(v) = 0$.
(iii) If v is a real place, then $e(v) \in \{0, 1\}$.

Given a modulus $\mathfrak{m}$ as above, we define the following objects:

(i) Let $V_{\mathfrak{m}}$ be the (open) subgroup of $\mathbb{I}_K$ consisting of $(a_v)_v \in \mathbb{I}_K$ satisfying:
  - If v is archimedean and $e(v) > 0$, then $a_v \in K_v \cong \mathbb{R}$ is positive.
  - If v is non-archimedean and $e(v) > 0$, then $a_v \in \mathcal{O}_{K_v}^\times \subset K_v^\times$ and $v(1 - a_v) \geq e(v)$.

(ii) Let $U_{\mathfrak{m}}$ be the (open) subgroup of $V_{\mathfrak{m}}$ consisting of those $(a_v)_v \in V_{\mathfrak{m}}$ such that $a_v \in \mathcal{O}_{K_v}^\times$ for all non-archimedean v.
(iii) Let $I_{\mathfrak{m}}$ be the group of fractional ideals of K whose prime factors are those $\mathfrak{p}_v$ with $e(v) = 0$. (This is a free abelian group generated by the set of $\mathfrak{p}_v$ with $e(v) = 0$.)
(iv) Let $\widetilde{P}_{\mathfrak{m}} = K^\times \cap V_{\mathfrak{m}}$.
(v) Let $P_{\mathfrak{m}}$ be the group of principal fractional ideals generated by elements of $\widetilde{P}_{\mathfrak{m}}$. We have $P_{\mathfrak{m}} \subset I_{\mathfrak{m}}$. We define the *ray class group*

$$\mathrm{Cl}_{\mathfrak{m}} := I_{\mathfrak{m}}/P_{\mathfrak{m}}.$$

Since $\widetilde{P}_{\mathfrak{m}} = V_{\mathfrak{m}} \cap K^\times$, we have an injective homomorphism

$$V_{\mathfrak{m}}/\widetilde{P}_{\mathfrak{m}}U_{\mathfrak{m}} \hookrightarrow \mathbb{I}_K/K^\times U_{\mathfrak{m}}$$

induced by the inclusion $V_{\mathfrak{m}} \hookrightarrow \mathbb{I}_K$. The weak approximation theorem for adeles implies that $\mathbb{I}_K = V_{\mathfrak{m}}K^\times$. Thus the above injection is an isomorphism. On the other hand, we have a well-defined homomorphism

$$V_{\mathfrak{m}} \longrightarrow I_{\mathfrak{m}}, \quad (a_v)_v \longmapsto \prod_{v<\infty} \mathfrak{p}_v^{v(a_v)},$$

which is surjective and has kernel $U_{\mathfrak{m}}$. The induced isomorphism $V_{\mathfrak{m}}/U_{\mathfrak{m}} \xrightarrow{\sim} I_{\mathfrak{m}}$ descends to an isomorphism

$$V_{\mathfrak{m}}/\widetilde{P}_{\mathfrak{m}} U_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Cl}_{\mathfrak{m}} .$$

We thus obtain a canonical isomorphism

$$\mathbb{I}_K/K^\times U_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Cl}_{\mathfrak{m}} . \tag{28.3.0.1}$$

Remark 28.3.1. The group $\mathrm{Cl}_{\mathfrak{m}}$ is finite.

Let L/K be a finite extension, and let $\mathfrak{m}$ be a modulus for K. Let $I_{\mathfrak{m},L}$ be the group of fractional ideals of L whose prime factors are over those non-archimedean places v of K with $e(v) = 0$. We have the ideal norm map

$$I_{\mathfrak{m},L} \longrightarrow I_{\mathfrak{m}}, \quad \mathfrak{P} \mapsto \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})},$$

where $\mathfrak{P}$ is any prime ideal of $\mathcal{O}_L$ belonging to $I_{\mathfrak{m},L}$ and $\mathfrak{p}$ is the prime ideal of $\mathcal{O}_K$ below $\mathfrak{P}$. We denote the image of this map by $\mathrm{N}_{L/K}(\mathfrak{m})$. Note that under (28.3.0.1), the image of $\mathrm{N}_{L/K}(\mathbb{I}_L)$ in the left hand side corresponds to the image of $\mathrm{N}_{L/K}(\mathfrak{m})$ in the right hand side.

Theorem 28.3.2 (Reciprocity Law)**.** *Let L/K be a finite abelian extension. Then there exists a modulus $\mathfrak{m}$ for K satisfying the following conditions:*

(i) Every place of K (including the archimedean ones) is unramified in L if and only if it does not appear $\mathfrak{m}$.[12]

(ii) By (i), for every finite place v of K not appearing in $\mathfrak{m}$, we have the Frobenius element $\mathrm{Frob}_v \in G_{L/K}$. The homomorphism

$$I_{\mathfrak{m}} \longrightarrow G_{L/K}, \quad \mathfrak{p}_v \longmapsto \mathrm{Frob}_v, \quad v \textit{ finite and not appearing in } \mathfrak{m}$$

induces an isomorphism

$$\mathrm{Cl}_{\mathfrak{m}} / \mathrm{im}(\mathrm{N}_{L/K}(\mathfrak{m})) \xrightarrow{\sim} G_{L/K}.$$

A modulus $\mathfrak{m}$ as above is called admissible *for L/K.*

Sketch of proof. Recall from Remark 25.0.1 that if E/F is a finite unramified extension of non-archimedean local fields, then $\mathrm{N}_{E/F}(\mathcal{O}_E^\times) = \mathcal{O}_F^\times$. Using this fact and the fact that $\mathrm{N}_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times) = \mathbb{R}_{>0}$, we can find $\mathfrak{m}$ satisfying (i) such that $\mathrm{N}_{L/K}(\mathbb{I}_L) \supset U_{\mathfrak{m}}$. Let $A := \mathbb{I}_K/K^\times \mathrm{N}_{L/K}(\mathbb{I}_L)$. Then A is a quotient of the group $\mathbb{I}_K/K^\times U_{\mathfrak{m}} \cong \mathrm{Cl}_{\mathfrak{m}}$, and $A \cong \mathrm{Cl}_{\mathfrak{m}} / \mathrm{im}(\mathrm{N}_{L/K}(\mathfrak{m}))$. By the idelic Reciprocity Law, we have the global Artin isomorphism $A \xrightarrow{\sim} G_{L/K}$. One checks that the resulting isomorphism $\mathrm{Cl}_{\mathfrak{m}} / \mathrm{im}(\mathrm{N}_{L/K}(\mathfrak{m})) \xrightarrow{\sim} G_{L/K}$ has the description as in (ii). □

Theorem 28.3.3 (Existence Theorem)**.** *For any modulus $\mathfrak{m}$ for K, there exists a unique finite abelian extension $K_{\mathfrak{m}}/K$ for which $\mathfrak{m}$ is admissible and such that $\mathrm{N}_{L/K}(\mathfrak{m}) \subset P_{\mathfrak{m}} \subset I_{\mathfrak{m}}$. In particular, $\mathrm{Cl}_{\mathfrak{m}} \cong G_{K_{\mathfrak{m}}/K}$. The field $K_{\mathfrak{m}}$ is called the ray class field of $\mathfrak{m}$.*

[12] Here we say that an archimedean place v of K is unramified in L, if for every place w of L over v we have $[L_w : K_v] = 1$.

Remark 28.3.4. Given a finite abelian extension L/K, a modulus $\mathfrak{m}$ is admissible for L/K if and only if $L \subset K_{\mathfrak{m}}$. Since such $\mathfrak{m}$ always exists, we can classify all finite abelian extensions of K by classifying intermediate extensions of $K_{\mathfrak{m}}/K$ for all moduli $\mathfrak{m}$. (This classification of course has repetitions, but the repetitions can be figured out precisely.) For a given $\mathfrak{m}$, the intermediate extensions of $K_{\mathfrak{m}}/K$ correspond to subgroups of $\mathrm{Cl}_{\mathfrak{m}}$ by the isomorphism $\mathrm{Cl}_{\mathfrak{m}} \cong G_{K_{\mathfrak{m}}/K}$.

References

[AT09] Emil Artin and John Tate. *Class field theory*. AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original.

[Bro82] Kenneth S. Brown. *Cohomology of groups*, volume 87 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1982.

[CF10] John William Scott Cassels and Albrecht Fröhlich. *Algebraic number theory*. London Mathematical Society London, 2010.

[Cox13] David A. Cox. *Primes of the form $x^2 + ny^2$*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[Gre63] Marvin J. Greenberg. Schemata over local rings. II. *Ann. of Math. (2)*, 78:256–266, 1963.

[Gro57] Alexandre Grothendieck. Sur quelques points d'algèbre homologique. *Tohoku Mathematical Journal, Second Series*, 9(2):119–183, 1957.

[LT65] Jonathan Lubin and John Tate. Formal complex multiplication in local fields. *Annals of Mathematics*, pages 380–387, 1965.

[Mil20] J.S. Milne. Class field theory (v4.03), 2020. Available at www.jmilne.org/math/.

[Mor96] Patrick Morandi. *Field and Galois theory*, volume 167 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Neu13] Jürgen Neukirch. *Class Field Theory:-The Bonn Lectures-Edited by Alexander Schmidt*. Springer Science & Business Media, 2013.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[Tat52] John Tate. The higher dimensional cohomology groups of class field theory. *Annals of Mathematics*, pages 294–297, 1952.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[Wei95] Charles A Weibel. *An introduction to homological algebra*. Number 38. Cambridge university press, 1995.