Local Class Field Theory

Zachary Gardner

zacharygardner137@utexas.edu

These notes cover the first and third lecture in a class field theory graduate summer mini-course co-taught at UT Austin in Summer 2019 by Rok Gregoric and Zachary Gardner. The first lecture is a review of necessary number theory background and the third lecture is an introduction to local class field theory. The third lecture is dependent on the second lecture covering cohomological preliminaries and assumes the reader is familiar with the basics of Tate cohomology. Some familiarity with profinite groups would also be helpful. For the reader who is not so familiar, we highly recommend Andrew Sutherland's expository papers on Tate cohomology and Tate's theorem. As a final note, all rings are taken to be commutative and unital unless otherwise stated.

Lecture 1 - Number Theory Background

Introduction

Definition. *A **number field** is a field which is a finite dimensional $\mathbb{Q}$-vector space. A **global function field** is a field which is a finite dimensional $\mathbb{F}_p(t)$-vector space, for p a prime and t an indeterminant. A **global field** is either a number field or global function field.*

Global fields will, unsurprisingly, be the main item of focus for global class field theory. A general rule of thumb is that if a result holds for one type of global field then an analogous result holds for the other type. This is why number fields and global function fields are placed under the same umbrella term. Note that things are often easier to prove for global function fields than for number fields. Before we get into the number theory proper, we will give a lightning tour of the algebraic results we need.

Some Field and Galois Theory

Definition. *Let L/K be an extension of fields. Then, L/K is:*

- ***algebraic** if every $\alpha \in L$ is **algebraic over** K – i.e., α is a root of some nonzero polynomial with coefficients in K;*
- ***separable** if every $\alpha \in L$ is **separable over** K – i.e., the minimal polynomial of α over K has no repeated roots;*
- ***normal** if every irreducible polynomial with coefficients in K either has no roots in L or splits completely in L;*
- ***Galois** if it is algebraic, separable, and normal;*

- ***abelian*** *if it is Galois and* $\mathrm{Gal}(L/K)$ *is abelian;*
- ***cyclic*** *if it is Galois and* $\mathrm{Gal}(L/K)$ *is cyclic.*

*For L/K Galois, we let $\mathrm{Gal}(L/K)$ denote the group of K-linear automorphisms of L fixing K pointwise. This group has order $[L : K]$. We say L/K is **G-Galois** if L/K is Galois with $\mathrm{Gal}(L/K) \cong G$.*

We record the following useful results for future (though possibly not explicit) reference. Know that these results are lurking in the proofs of various results that will go unproved in these notes.

Theorem (Primitive Element Theorem)**.** *Let L/K be a finite separable extension. Then, there exists $\alpha \in L$ such that $L = K(\alpha)$.*

Theorem (Normal Basis Theorem)**.** *Let L/K be a finite G-Galois extension. Then, there exists $\alpha \in L$ such that $\{\sigma\alpha : \sigma \in G\}$ is a K-basis for L. Equivalently, $L \cong K[G]$ as G-modules.*[1]

Theorem (Fundamental Theorem of Galois Theory)**.** *Let L/K be a (possibly infinite) G-Galois extension of fields and endow G with the profinite topology arising from the natural isomorphism*

$$G \cong \varprojlim \mathrm{Gal}(E/K),$$

where the inverse limit is taken over $K \subseteq E \subseteq L$ with E/K finite Galois. Then, the maps $H \mapsto L^H$ and $E \mapsto \mathrm{Gal}(L/E)$ induce an inclusion-reversing bijection between the set of closed subgroups of G and fields intermediate between K and L. Moreover,

(i) $H \leq G \implies L/L^H$ *is Galois with* $\mathrm{Gal}(L/L^H) \cong \overline{H}$*, the closure of H in G;*

(ii) *open subgroups of G correspond to finite extensions of K (and, more generally, cosets correspond to embeddings);*

(iii) *normal subgroups of G correspond to Galois extensions of K (and, more generally, conjugates correspond to conjugates).*

Given a field K, let $\overline{K}$ denote a choice of algebraic closure and K^{sep} a choice of separable closure. For L/K a separable extension contained in K^{sep}, the **Galois closure** of L/K is the minimal field M contained in K^{sep} such that $L \subseteq M$ and M/K is Galois. Such an M exists and is a finite extension of L. Unless otherwise stated, separable extensions of K will be taken to be sub-extensions of some K^{sep} (this helps clarify any matters of uniqueness).

Proposition. *Let K be a field and L_1, L_2 Galois over K. Then, the compositum L_1L_2 is Galois over K satisfying*

$$\mathrm{Gal}(L_1L_2/K) \hookrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$$

with image $\{(\sigma, \tau) : \sigma|_{L_1 \cap L_2} = \tau|_{L_1 \cap L_2}\}$. Hence, if L_1, L_2 are abelian over K then L_1L_2 is as well.

[1] Given a ring R and group G, we use the notation $R[G]$ to denote the group ring of R-linear formal sums of elements of G.

This allows us to define a **maximal abelian extension** K^{ab} of K relative to some separable closure K^{sep} as a suitable compositum. We define

$$\begin{aligned}\mathrm{Gal}(K) &:= \mathrm{Gal}(K^{\mathrm{sep}}/K),\\ \mathrm{Gal}^{\mathrm{ab}}(K) &:= \mathrm{Gal}(K^{\mathrm{ab}}/K).\end{aligned}$$

The former is the **absolute Galois group of** K and is in some sense the prime object of study for modern number theory.

Remark. $\mathrm{Gal}^{\mathrm{ab}}(K)$ *is sometimes referred to as the abelianized absolute Galois group of* K *even though* $\mathrm{Gal}^{\mathrm{ab}}(K)$ *and* $\mathrm{Gal}(K)^{\mathrm{ab}}$ *are not literally isomorphic. They are, however, isomorphic in the "profinite" sense of having the same finite quotients. If* K *is nonarchimedean local then this relationship can be strengthened somewhat by a result of local class field theory known as the Norm Limitation Theorem.*

We say K is **perfect** if every finite extension of K is separable. If K is finite or $\operatorname{char} K = 0$ then K is perfect. For $\operatorname{char} K = p > 0$, K is perfect if and only if every element of K is a pth power. Recall that if ℓ/k is an extension of finite fields then ℓ/k is cyclic with $\mathrm{Gal}(\ell/k)$ generated by the **Frobenius map** $\sigma : \alpha \mapsto \alpha^{|k|}$. This will be important later when we discuss unramified extensions.

Definition. *Let* L/K *be a finite field extension (and so* L *is a* K*-vector space of finite dimension). Define* $N_{L/K} : L \to L$ *by* $a \mapsto \det \mu_\alpha$*, where* $\mu_\alpha : L \to L$ *is the* K*-linear map given by multiplication by* α*.*

Proposition. *Let* L/K *be a finite field extension. Then,*

(i) *the image of* $N_{L/K}$ *is contained in* K*;*

(ii) *if* $\alpha \in K$ *then* $N_{L/K}(\alpha) = \alpha^{[L:K]}$*;*

(iii) $N_{L/K}$ *defines a group homomorphism* $L^\times \to K^\times$ *and hence* $N_{L/K}(L^\times) \leq K^\times$*;*

(iv) *given* $K \subseteq E \subseteq L$, $N_{L/K} = N_{E/K} \circ N_{L/E}$*;*

(v) *if* L/K *is Galois and* $\alpha \in L$ *then* $N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma\alpha$*;*[2]

(vi) *if* L/K *is separable and* M *is the Galois closure of* L/K *then* $N_{L/K} = N_{M/K}|_L$.

Some Commutative Algebra

Let $A \subseteq B$ be an extension of rings. The **integral closure** of A in B is

$$\{b \in B : p(b) = 0 \text{ for some monic } p(x) \in A[x]\},$$

whose elements are said to be **integral (over** A**)**. The integral closure of A in B is a ring, a somewhat nontrivial statement which follows from the fact that $b \in B$ is integral over A if and only if the subring $A[b] \subseteq B$ generated by b is a finitely generated A-module.

[2] There are similar product expressions for the norm in the case that L/K is not separable but we will not need them.

If A is an integral domain and no extension ring is specified then the **integral closure** of A is taken to be the integral closure of A in the quotient field $\mathrm{Frac}(A)$. A is **integrally closed** if it is equal to its own integral closure. A is a **Dedekind domain** if it is a Noetherian (i.e., every ascending chain of ideals terminates), integrally closed integral domain of Krull dimension ≤ 1 (i.e., if A is not a field then every nonzero prime ideal is maximal). A is a **discrete valuation ring** (**DVR** for short) if it is a local Dedekind domain which is not a field – i.e., a local PID of Krull dimension 1. It follows that a Dedekind domain which is not a field is precisely a ring all of whose localizations at prime ideals are DVRs.

Let A be an integral domain and $K := \mathrm{Frac}(A)$ its quotient field. A **fractional ideal** of A is a nonzero A-submodule I of K such that $\alpha I \subseteq A$ for some nonzero $\alpha \in K$ (we may take α to lie in A). If A is Noetherian then an A-submodule of K is a fractional ideal of A if and only if it is finitely generated. Intersections, products, and sums of fractional ideals are defined as for ordinary ideals of A. Given I a fractional ideal of A, define

$$I^{-1} := \{\alpha \in K : \alpha I \subseteq A\}.$$

This acts as an inverse for fractional ideal multiplication and makes the set of fractional ideals of A into an abelian group. This group has a subgroup consisting of **principal fractional ideals** – i.e., fractional ideals of the form αA for some nonzero $\alpha \in K$. The quotient by this subgroup yields the **class group** $\mathrm{Cl}(A)$ of A, which is another important object of study in number theory.

Proposition. *Let A be a Dedekind domain. Then, every nonzero proper fractional ideal of A factors uniquely (up to reordering) as a finite product of prime ideals of A.*

Note that the statement is vacuously true if A is a field. Given $\mathfrak{p} \in \mathrm{Spec}(A)$ and I a nonzero proper fractional ideal of A, define $v_{\mathfrak{p}}(I)$ to be the multiplicity of $\mathfrak{p}$ in a prime ideal factorization of I (this is well-defined by the above proposition). Letting $K := \mathrm{Frac}(A)$, this defines a map $v_{\mathfrak{p}} : K \to \mathbb{Z}$ via $v_{\mathfrak{p}}(\alpha) := v_{\mathfrak{p}}(\alpha A)$.

Given a number field K, define the **ring of integers** $\mathcal{O}_K$ to be the integral closure of $\mathbb{Z}$ in K. This is a Dedekind domain with quotient field K that is a finitely generated $\mathbb{Z}$-module. Dirichlet's Unit Theorem tells us that $\mathcal{O}_K^\times$ is a finitely generated abelian group. We define the **class group** of K to be $\mathrm{Cl}(K) := \mathrm{Cl}(\mathcal{O}_K)$. An important theorem of algebraic number theory asserts that this is also a finitely generated abelian group.

Valuation Theory and Local Fields

Let K be a field. A **discrete valuation** on K is a map $v : K \to \mathbb{Z} \cup \{\infty\}$ such that, for every $x, y \in K$,

(i) $v(x) = \infty \iff x = 0$;

(ii) $v(xy) = v(x) + v(y)$;

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$.

An **absolute value** on K is a map $|\cdot| : K \to \mathbb{R}^{\geq 0}$ such that, for every $x, y \in K$,

(i) $|x| = 0 \iff x = 0$;

(ii) $|xy| = |x||y|$;

(iii) $|x+y| \leq |x| + |y|$.

$|\cdot|$ is **nonarchimedean** if $|x+y| \leq \max\{|x|,|y|\}$ for every $x, y \in K$; it is **archimedean** otherwise. $|\cdot|$ is **trivial** if $|x| = 1$ for every nonzero $x \in K$. For the sake of convenience we do not consider the trivial absolute value to be nonarchimedean (though there are reasons in the global case to think otherwise). Two absolute values $|\cdot|_1, |\cdot|_2$ are said to be **equivalent** if there exists $c > 0$ such that $|\cdot|_2 = |\cdot|_1^c$. This defines an equivalence relation $\sim$ whose equivalence classes are called **places** of K. If $|\cdot|_1, |\cdot|_2$ are equivalent absolute values and $|\cdot|_1$ is nonarchimedean then $|\cdot|_2$ is also nonarchimedean. A place represented by an archimedean absolute value is called an **infinite place**, while a place represented by a nonarchimedean absolute value is called a **finite place**

A discrete valuation v induces a nonarchimedean absolute value $|\cdot|_v := \exp(-v(\cdot))$. Similarly, a nonarchimedean absolute value $|\cdot|$ induces a discrete valuation $w(\cdot) := -\log|\cdot|$. It follows that nonarchimedean absolute values on K and discrete valuations on K are in bijection (this technically may require excluding the trivial discrete valuation).

Remark. *Discrete valuations are sometimes called additive valuations, while absolute values are sometimes called multiplicative valuations. Condition (iii) for an absolute value is sometimes replaced with the condition that there exists a constant $d > 0$ such that $|1+x| \leq d$ for every $x \in K$ such that $|x| \leq 1$. This results in the same notion of absolute value for $d = 2$, and in the notion of a nonarchimedean absolute value for $d = 1$. The difference is immaterial at the end of the day since every absolute value of the second type is equivalent to an absolute value of the first type.*

Note also that places are sometimes called primes. Given a Dedekind domain A with quotient field K and $\mathfrak{p} \in \operatorname{Spec}(A)$, the map $v_{\mathfrak{p}}$ defined previously extends to a discrete valuation on K. By the above comment, this induces a nonarchimedean absolute value $|\cdot|_{\mathfrak{p}}$ and hence a place of K. So, the prime $\mathfrak{p}$ is essentially determining a place of K. The discrete valuation $v_{\mathfrak{p}}$ is **normalized** in the sense that $v_{\mathfrak{p}}(\pi) = 1$ for every $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Some of the justification for classifying places as finite or infinite comes from:

Theorem (Ostrowski)**.** *Let ω be a place of a number field K. If ω is finite then it is represented by $|\cdot|_{\mathfrak{p}}$ for some $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_K)$. If ω is infinite then it is represented by $|\cdot|'$ defined via $|\alpha|' := |\sigma\alpha|$ for $|\cdot|$ the standard absolute value on $\mathbb{C}$ and σ an embedding of K into $\mathbb{C}$ fixing $\mathbb{Q}$ pointwise (note that there are $[K : \mathbb{Q}]$ such embeddings).*

Proposition. *Let K be a field and v a valuation on K. Define,*

$$\mathcal{O}_K := \{x \in K : v(x) \geq 0\},$$
$$\mathfrak{p}_K := \{x \in K : v(x) > 0\}.$$

Then, $\mathcal{O}_K$ is a local PID with (nonzero) maximal ideal $\mathfrak{p}_K$. Moreover,

$$\mathcal{O}_K = \{x \in K : |x| \leq 1\},$$
$$\mathfrak{p}_K = \{x \in K : |x| < 1\}$$

for every $|\cdot| \sim |\cdot|_v$.

The field $k := \mathcal{O}_K/\mathfrak{p}_K$ is called the **residue field** of K, while $\mathcal{O}_K$ is called the **valuation ring** of K and is a prime example of a DVR. A generator π of $\mathfrak{p}_K$ is called a **uniformizer** of K.

Note that $v = v_{\mathfrak{p}_K}$ with regard to our prior notation. Given π a uniformizer of K, every $\alpha \in K^\times$ can be written uniquely as $u\pi^n$ for $u \in \mathcal{O}_K^\times$ and $n \in \mathbb{Z}$. For such an α, $v(\alpha) = n$. This yields a non-canonical isomorphism $K^\times \cong \mathcal{O}_K^\times \times \mathbb{Z}$ arising from the short exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \mathcal{O}_K^\times \arrow[r] & K^\times \arrow[r, "v"] & \mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

Remark. *Even though they share the same notation, don't confuse the ring of integers of a field K with the valuation ring of K since the two notions may not agree even if they both make sense. For example, the integral closure of $\mathbb{Z}$ in $\mathbb{Q}_p$ is not the same as $\mathbb{Z}_p$. To make matters even more confusing, people sometimes refer to valuation rings as rings of integers.*

Definition. *A **local field** is a field K with an absolute value $|\cdot|$ such that the induced metric topology makes K into a (non-discrete) locally compact topological field (in particular, K is a Hausdorff space such that every point has a compact neighborhood).*

Lemma. *K is nonarchimedean local if and only if it is complete with respect to a discrete valuation and has a ring of integers with finite residue field.*

Let A be a Dedekind domain with $\mathfrak{p} \in \operatorname{Spec}(A)$ and quotient field K. Define $K_\mathfrak{p}$ to be the metric completion of K with respect to the metric induced by $|\cdot|_\mathfrak{p}$. Define $A_\mathfrak{p}$ similarly. Then, $K_\mathfrak{p}$ is a local field with valuation ring $A_\mathfrak{p}$. $A_\mathfrak{p}$ is a DVR with maximal ideal $\hat{\mathfrak{p}} := \mathfrak{p}A_\mathfrak{p}$ that is complete with respect to the extension metric induced by $|\cdot|_{\hat{\mathfrak{p}}}$. For a slightly more algebraic perspective, the filtration

$$A \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \cdots$$

gives rise to an inverse limit which we imbue with the ($\mathfrak{p}$-adic) Krull topology in which $\{\mathfrak{p}^n\}_{n\geq 0}$ is a basis of 0. Then, there is a natural isomorphism $A_\mathfrak{p} \cong \varprojlim A/\mathfrak{p}^n$ of topological rings.

More generally, given a field K with absolute value $|\cdot|$, we can consider the metric completion $\hat{K}$. This is a complete field with metric induced by the absolute value that is the unique extension of $|\cdot|$ to $\hat{K}$. Of course, $\hat{K}$ also satisfies a universal property regarding embeddings of K into complete valued fields (i.e., fields equipped with an absolute value). It follows that $\hat{K} = K$ if K is already complete and that completion is defined up to unique isomorphism at a place and not just an absolute value.

Let A be a complete DVR with quotient field K and maximal ideal $\mathfrak{p}$. As above, $A \cong \varprojlim A/\mathfrak{p}^n$. $A^\times$ admits a similar filtration

$$A^\times \supseteq 1 + \mathfrak{p} \supseteq 1 + \mathfrak{p}^2 \supseteq \cdots$$

and Krull-type topology, giving a natural isomorphism $A^\times \cong \varprojlim A^\times/(1+\mathfrak{p}^n)$. For future reference, $A^\times$ is naturally a profinite group satisfying the no small subgroups condition – i.e., there is an open neighborhood of 1 in $A^\times$ that contains no nontrivial subgroups of G.[3]

Theorem. *Let K be a local field. Then, K is isomorphic as a topological ring to one of the following:*

- $\operatorname{char} K = 0$, *$|\cdot|$ archimedean: $\mathbb{R}$ or $\mathbb{C}$;*

[3] Complete topological groups satisfying the no small subgroups condition are the natural object of study for a result called Chevalley's Theorem important in global class field theory.

- $\operatorname{char} K = 0$, $|\cdot|$ *nonarchimedean: finite extension of* $\mathbb{Q}_p$ *(for* $p > 0$ *prime);*
- $\operatorname{char} K = p > 0$, $|\cdot|$ *nonarchimedean:* $\mathbb{F}_q((t))$ *for* q *a power of* p.

Corollary. *Let* A *be a Dedekind domain such that* $K := \operatorname{Frac}(A)$ *is a global field. Then, given* $\mathfrak{p} \in \operatorname{Spec}(A)$, $K_{\mathfrak{p}}$ *is a local field. Conversely, every local field arises as the completion of a global field.*

Ramification Theory

The "$AKLB$ setup" is the following: A is a Dedekind domain which is not a field, $K = \operatorname{Frac}(A)$, L is a finite separable extension of K, and B is the integral closure of A in L. The $AKLBG$ setup is similar except that we additionally require that L/K is G-Galois.

Example. *Take* L/K *a separable extension of either nonarchimedean local or number fields and* $A = \mathcal{O}_K, B = \mathcal{O}_L$. *Note that such a field extension must necessarily be finite. That this is an example of the* $AKLB$ *setup follows from work done below.*

Assume the $AKLB$ setup. Then, B is a Dedekind domain with quotient field L. Let $\mathfrak{p} \in \operatorname{Spec}(A)$. $\mathfrak{q} \in \operatorname{Spec}(B)$ is said to **lie above** $\mathfrak{p}$ if $\mathfrak{q} \cap K = \mathfrak{p}$. There are only finitely many such primes, given precisely by $\mathfrak{q} \in \operatorname{Spec}(B)$ such that $\mathfrak{q} | \mathfrak{p}B$.[4] Let $g_{\mathfrak{p}}$ denote the number of such primes lying above $\mathfrak{p}$. Fix now $\mathfrak{q} \in \operatorname{Spec}(B)$ lying above $\mathfrak{p}$. The **ramification index** $e_{\mathfrak{q}}$ of $\mathfrak{q}$ is the multiplicity of $\mathfrak{q}$ in a prime ideal factorization of $\mathfrak{p}B$, while the **inertia degree** $f_{\mathfrak{q}}$ of $\mathfrak{q}$ is $[B/\mathfrak{q} : A/\mathfrak{p}]$. We sometimes use the notation $e_{\mathfrak{q}/\mathfrak{p}}$ and $f_{\mathfrak{q}/\mathfrak{p}}$ if we want to emphasize the role of $\mathfrak{p}$. Ramification index and inertia degree behave well with respect to extensions. We obtain the following "combinatorial" result.

Proposition. *Assume the* $AKLB$ *setup and let* $\mathfrak{p} \in \operatorname{Spec}(A)$. *Then,* $[L : K] = \sum_{\mathfrak{q} | \mathfrak{p}B} e_{\mathfrak{q}} f_{\mathfrak{q}}$.

Definition. *Assume the* $AKLB$ *setup. Let* $\mathfrak{q} \in \operatorname{Spec}(B)$ *lying above* $\mathfrak{p} \in \operatorname{Spec}(A)$. *Then,* L/K *is:*

- ***ramified at*** $\mathfrak{q}$ *if* $e_{\mathfrak{q}} > 1$;
- ***totally ramified at*** $\mathfrak{q}$ *if* $e_{\mathfrak{q}} = [L : K]$ *(i.e., the ramification index is maximal);*
- ***unramified at*** $\mathfrak{q}$ *if* $e_{\mathfrak{q}} = 1$ and $B/\mathfrak{q}$ *is a separable extension of* $A/\mathfrak{p}$.

We say L/K *is* ***unramified above*** $\mathfrak{p} \in \operatorname{Spec}(A)$ *when it is unramified at every prime of* B *lying above* $\mathfrak{p}$. *In such case,* $\mathfrak{p}$ *is* ***inert*** *if* $\mathfrak{p}B$ *is prime and* ***splits completely*** *or is* ***split*** *if* $g_{\mathfrak{p}} = [L : K]$ *(i.e., it is maximal).* L/K *is* ***unramified*** *if it is unramified above every* $\mathfrak{p} \in \operatorname{Spec}(A)$.

Proposition. *Assume the* $AKLBG$ *setup.* G *acts on the set of fractional ideals of* B *via* $\sigma(I) := \{\sigma(x) : x \in I\}$. *This restricts to an action of* G *on* $\operatorname{Spec}(B)$, *the fibers of which are precisely the primes lying above some prime of* A. *In particular,* G *acts transitively on the set of primes lying above a prime of* A.

[4] People often use the notation $\mathfrak{q}|\mathfrak{p}$.

Proposition. *Assume the AKLBG setup and let $\mathfrak{p} \in \operatorname{Spec}(A)$. Then, the ramification index and inertia degree are the same for every prime of B lying above $\mathfrak{p}$. We denote the common values by $e_\mathfrak{p}$ and $f_\mathfrak{p}$, respectively.*

Corollary. *Assume the AKLBG setup and let $\mathfrak{p} \in \operatorname{Spec}(A)$. Then, $[L : K] = e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p}$.*

Corollary. *Assume the AKLBG setup and let $\mathfrak{q} \in \operatorname{Spec}(B)$. Then, $v_\mathfrak{q}$ is G-invariant in the sense that $v_\mathfrak{q}(\sigma\alpha) = v_\mathfrak{q}(\alpha)$ for every $\sigma \in G$ and $\alpha \in L$.*

One application of this result is the following.

Lemma. *Let L/K be a finite separable extension of either nonarchimedean local or number fields. Then, $N_{L/K}(\mathcal{O}_L) \subseteq \mathcal{O}_K$.*

Proof. In either case we have $\mathcal{O}_K = \mathcal{O}_L \cap K$. We already know $N_{L/K}(\mathcal{O}_L) \subseteq N_{L/K}(L) \subseteq K$, so it suffices to show $N_{L/K}(\mathcal{O}_L) \subseteq \mathcal{O}_L$. By passing to the Galois closure we may assume without loss of generality that L/K is Galois. Suppose first that L, K are local fields. Let $|\cdot|$ be the relevant absolute value on L. Then, $\mathcal{O}_L = \{\alpha \in L : |\alpha| \leq 1\}$. Given $\alpha \in \mathcal{O}_L$,

$$N_{L/K}(\alpha) = \prod_{\sigma \in \operatorname{Gal}(L/K)} \sigma\alpha \implies |N_{L/K}(\alpha)| = \prod_{\sigma \in \operatorname{Gal}(L/K)} |\sigma\alpha| = |\alpha|^{|\operatorname{Gal}(L/K)|} \leq 1,$$

using that $|\cdot|$ is $\operatorname{Gal}(L/K)$-invariant (this follows since $|\cdot|$ arises from a $\operatorname{Gal}(L/K)$-invariant discrete valuation). Suppose now that L, K are number fields. Given $\alpha \in \mathcal{O}_L$, there exists a monic $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. Given $\sigma \in \operatorname{Gal}(L/K)$,

$$f(\sigma\alpha) = \sigma(f(\alpha)) = \sigma(0) = 0 \implies \sigma\alpha \in \mathcal{O}_L.$$

Since $N_{L/K}(\alpha) = \prod_{\sigma \in \operatorname{Gal}(L/K)} \sigma\alpha$ and $\mathcal{O}_L$ is a ring, $N_{L/K}(\alpha) \in \mathcal{O}_L$. □

One consequence of the above is that $N_{L/K}(\mathcal{O}_L^\times) \subseteq \mathcal{O}_K^\times$. We will see later using group cohomology that $N_{L/K}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$ for L/K a finite unramified extension of local fields.

Definition. *Let L/K be a finite separable extension, v a discrete valuation on K, and w a discrete valuation on L. Then, w* ***extends*** *v* ***with index*** *$e > 0$ if $w|_K = ev$. The relevant shorthand is $w|v$.*

Proposition. *Assume the AKLB setup and let $\mathfrak{p} \in \operatorname{Spec}(A)$. Then, given $\mathfrak{q} \in \operatorname{Spec}(B)$ lying above $\mathfrak{p}$, $v_\mathfrak{q}$ extends $v_\mathfrak{p}$ with index $e_\mathfrak{q}$. Moreover, $\mathfrak{q} \mapsto v_\mathfrak{q}$ induces a bijection between primes lying above $\mathfrak{p}$ and discrete valuations on L extending $v_\mathfrak{p}$.*

It is often the case that, given A a complete DVR with residue field k, we wish to understand A in terms of information about k. Hensel's Lemma is a tool that lets us do just that. Note that Hensel's Lemma has many equivalent statements as well as a number of generalizations that all bear the same name.

Lemma (Hensel)**.** *Let A be a complete DVR with maximal ideal $\mathfrak{p}$ and residue field k. Let $F \in A[x]$ and $f \in k[x]$ its reduction mod $\mathfrak{p}$.*

(a) *Every simple root of f in k lifts to a simple root of F in A.*

(b) *Suppose that F is primitive (i.e., its coefficients generate A as an ideal) and $g, h \in k[x]$ are coprime such that $f = gh$. Then, there exist $G, H \in A[x]$ such that $F = GH$, $\deg G = \deg g$, $\deg H = \deg h$, and G, H reduce to g, h mod $\mathfrak{p}$.*

Remark. *The theory of filtered modules, filtered homomorphisms, and the associated graded provides tools that function analogously to Hensel's Lemma. Some results can be proven in different ways using both techniques, while other results only allow one technique. It is therefore useful to understand how to apply both filtered stuff and Hensel's Lemma.*

Corollary. *Assume the AKLB setup and that A is a complete DVR with maximal ideal $\mathfrak{p}$. Then, there exists a unique prime $\mathfrak{q}$ of B lying above $\mathfrak{p}$.*

Theorem. *Let A be a complete DVR with maximal ideal $\mathfrak{p}$ and L/K a finite extension. Then, $|\cdot| := |N_{L/K}(\cdot)|_{\mathfrak{p}}^{1/[L:K]}$ is the unique absolute value on L extending $|\cdot|_{\mathfrak{p}}$ and is complete. If in addition L/K is separable then we have the AKLB setup with B the valuation ring of L with respect to $|\cdot|$ and, moreover, $|\cdot| = |\cdot|_{\mathfrak{q}}^{1/e_{\mathfrak{q}}}$ for $\mathfrak{q}$ the unique prime of B lying above $\mathfrak{p}$.*

Remark. *Similar extension results hold for global fields. Moreover, the extension results for local and global fields are compatible under completion at the appropriate places.*

Theorem. *Let A be a complete DVR with quotient field K and residue field k. Let $\mathcal{C}_K$ denote the category whose objects are finite unramified extensions of K and morphisms are K-algebra homomorphisms. Let $\mathcal{C}_k$ denote the category whose objects are finite separable extensions of k and morphisms are k-algebra homomorphisms. Let $\mathscr{F} : \mathcal{C}_K \to \mathcal{C}_k$ be the functor which sends a finite unramified extension L/K to its residue field ℓ and a morphism $\varphi \in \mathrm{Hom}_{K-\mathrm{alg}}(L_1, L_2)$ to $\overline{\varphi} \in \mathrm{Hom}_{k-\mathrm{alg}}(\ell_1, \ell_2)$ defined by $\overline{\alpha} \mapsto \overline{\varphi(\alpha)}$, where α is a lift of $\overline{\alpha}$ to L_1 and $\overline{\varphi(\alpha)}$ is the projection of $\varphi(\alpha)$ to ℓ_2. Then, $\mathscr{F}$ is a well-defined equivalence of categories.*

The proof of the theorem yields an important characterization of unramified extensions.

Corollary. *Assume the AKLB setup and let A be a complete DVR with quotient field K and residue field k. Then, L/K is unramified if and only if $B = A[\alpha]$ for some $\alpha \in L$ whose minimal polynomial in $A[x]$ has separable image in $k[x]$.*

Corollary. *Let A be a complete DVR with quotient field K and finite residue field k of size q. Then, a finite extension L/K of degree n is unramified if and only if $L \cong K(\zeta_{q^n-1})$ for ζ_{q^n-1} a primitive $(q^n - 1)$-root of unity.*

Corollary. *Let A be a complete DVR with quotient field K and finite residue field k of size q. Then, K has a unique (up to isomorphism) unramified extension of each finite degree. Moreover, the compositum of unramified extensions of K is an unramified extension of K.*

It follows that K has a maximal unramified extension K^{unr} obtained by adjoining suitable roots of unity. Hence, $L^{\text{unr}} = LK^{\text{unr}}$ for L/K a finite separable extension.

Let L/K be a finite unramified extension of nonarchimedean local fields with finite residue fields ℓ/k. The theorem gives that both extensions are Galois and there is a natural isomorphism $\varphi : \text{Gal}(L/K) \xrightarrow{\sim} \text{Gal}(\ell/k)$. It follows that $\text{Gal}(L/K)$ is cyclic with generator $\text{Frob}_{L/K} := \varphi^{-1}(\sigma)$, for σ the Frobenius element of $\text{Gal}(\ell/k)$. More generally, let L/K be an extension contained inside of K^{unr}. Then, $\text{Frob}_{L/K}$ is the unique element of $\text{Gal}(L/K)$ such that

$$\text{Frob}_{L/K}|_E = \text{Frob}_{E/K}$$

for every $K \subseteq E \subseteq L$ with E/K finite (note that we have implicitly used that subgroups of cyclic groups are cyclic with "compatible" generators). It follows that

$$\text{Gal}(K^{\text{unr}}/K) \cong \text{Gal}(\overline{k}/k) \cong \hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$$

and that there is a sequence of containments

$$K \subseteq K^{\text{unr}} \subseteq K^{\text{ab}} \subseteq K^{\text{sep}} \subseteq \overline{K}.$$

Lecture 3 - Local Class Field Theory

Introduction

For future reference, we define Galois cohomology to be $H^\bullet(L/K) := H^\bullet(G, L^\times)$ for L/K a G-Galois extension of fields. Under the same hypotheses, Hilbert's Theorem 90 gives $H^1(L/K) = 0$. Our focus will be on proving the following theorem.

Theorem (Local Artin Reciprocity)**.** *Let K be a local field. Then, there exists a unique continuous homomorphism*

$$\theta_K : K^\times \to \text{Gal}(K^{\text{ab}}/K)$$

such that, for every finite extension L/K in K^{ab}, the homomorphism $\theta_{L/K} : K^\times \to \text{Gal}(L/K)$ given by composing θ_K with the restriction map $\text{Gal}(K^{\text{ab}}/K) \twoheadrightarrow \text{Gal}(L/K)$ is surjective with kernel $N_{L/K}(L^\times)$ and, for K nonarchimedean and L/K unramified, $\theta_{L/K}(\pi) = \text{Frob}_{L/K}$ for every uniformizer π of $\mathcal{O}_K$. Equivalently, $\theta_K^{-1}(\text{Frob}_K)$ generates the maximal ideal of $\mathcal{O}_{K^{\text{unr}}}$. Moreover, θ_K induces an isomorphism

$$\hat{\theta}_K : \widehat{K^\times} \to \text{Gal}(K^{\text{ab}}/K)$$

for $\widehat{K^\times}$ the profinite completion of $K^\times$.

As an abuse of notation, we often identify $\theta_{L/K}$ with the isomorphism it induces by the First Isomorphism Theorem. The case of K archimedean is easy to dispense with, so we assume K is nonarchimedean. Our strategy will be to use Tate cohomology theory to explicitly construct the isomorphism $K^\times/N_{L/K}(L^\times) \xrightarrow{\sim} \text{Gal}(L/K)$ induced by $\theta_{L/K}$ for L/K a finite extension contained in K^{ab}. This isomorphism will be functorial in L, allowing us to construct θ_K by using the fact that

$$\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \varprojlim \mathrm{Gal}(L/K),$$

where L/K ranges over the inverse system of finite extensions contained in K^{ab} (with maps given by restriction).

The Invariant Map

We will construct $\theta_{L/K}$ by building its inverse, a task which requires some machinery. Let L/K be an unramified G-Galois extension of a nonarchimedean local field K (we will consider general separable extensions later). Let v be the valuation on L extending the (normalized) valuation on K and take $\mathbb{Z}$ to be a trivial hence discrete G-module. Then, we have an exact sequence

$$1 \longrightarrow \mathcal{O}_L^\times \longrightarrow L^\times \xrightarrow{v} \mathbb{Z} \longrightarrow 0$$

of abelian groups which is in fact an exact sequence of G-modules since v is constant on Galois orbits. Let π be a uniformizer for K. Since L/K is unramified, we may also take π to be a uniformizer for L. The map $1 \mapsto \pi$ extends to a $\mathbb{Z}$-linear map $f : \mathbb{Z} \to L^\times$ which is G-linear since, given $\sigma \in G$, σ fixes K pointwise and so

$$\sigma \cdot f(1) = \sigma(\pi) = \pi = f(1) = f(\sigma(1)) = f(\sigma \cdot 1).$$

The map f is then by construction a G-linear right section of the above short exact sequence and so the above short exact sequence splits, yielding a non-canonical G-module isomorphism $L^\times \cong \mathcal{O}_L^\times \oplus \mathbb{Z}$. This is great for a very important reason:

Lemma. *Let L/K be an unramified G-Galois extension of nonarchimedean local fields. Then, $H^n(G, \mathcal{O}_L^\times) = 0$ for every $n > 0$. Moreover, if L/K is finite, then $\mathcal{O}_L^\times$ is **(Tate) cohomologically trivial** – i.e., $\hat{H}^n(H, \mathcal{O}_L^\times) = 0$ for every $H \leq G$ and $n \in \mathbb{Z}$.*

Proof. Suppose that we have shown the result for L/K finite and let L/K be arbitrary. Given $N \leq G$ open, L^N/K is a finite unramified extension with $\mathrm{Gal}(L^N/K) \cong G/N$.[5] Since Tate cohomology agrees with group cohomology for a finite group in positive degree,

$$H^\bullet(G, \mathcal{O}_L^\times) = \varinjlim\nolimits_{\mathrm{colim}} H^\bullet(G/N, (\mathcal{O}_L^\times)^N) \cong \varinjlim\nolimits_{\mathrm{colim}} H^\bullet(\mathrm{Gal}(L^N/K), \mathcal{O}_{L^N}^\times) = 0,$$

where the colimits are taken over $N \trianglelefteq G$ open. We now show the result for L/K finite. We have $\hat{H}^\bullet(G, L^\times) \cong \hat{H}^\bullet(G, \mathcal{O}_L^\times) \oplus \hat{H}^\bullet(G, \mathbb{Z})$.[6] Since G is cyclic, the corresponding Tate cohomology is 2-periodic and so it suffices to look at degree 0 and degree 1. Hilbert's Theorem 90 gives $\hat{H}^1(G, L^\times) = 0$ and hence $\hat{H}^1(G, \mathcal{O}_L^\times) = 0$. At the same time, $\hat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/[L : K]\mathbb{Z}$ and so $\hat{H}^0(G, L^\times) = K^\times/N_{L/K}(L^\times)$ contains a cyclic subgroup of order $[L : K]$. This subgroup is everything since

$$|\hat{H}^0(G, L^\times)| = |K^\times : N_{L/K}(L^\times)| \leq |K^\times : N_{L/K}(K^\times)| = |K^\times : (K^\times)^{[L:K]}| = [L : K]$$

and so $\hat{H}^0(G, \mathcal{O}_L^\times) = 0$. Hence, $\hat{H}^\bullet(G, \mathcal{O}_L^\times) = 0$. Given $H \leq G$, the Fundamental Theorem of Galois Theory gives $H = \mathrm{Gal}(L/L^H)$ and we obtain $\hat{H}^\bullet(H, \mathcal{O}_L^\times) = 0$ by applying the above argument to the finite unramified extension L/L^H. □

[5] Note that a subgroup of a profinite group is open if and only if it is closed with finite index. This is perhaps not so surprising if you are familiar with infinite Galois theory.

[6] This property of Tate cohomology is basically a consequence of the fact that Ext and Tor are additive functors. In fact, Tate cohomology may be viewed as an Ext functor for the appropriate module.

Remark. *We showed on Monday that, for L/K a finite separable extension of nonarchimedean local fields, $N_{L/K}(\mathcal{O}_L^\times) \subseteq \mathcal{O}_K^\times$. An immediate consequence of the above is that $N_{L/K}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$ in the case of L/K unramified. The above proof also provides a sanity check for local Artin reciprocity since, for L/K a finite unramified extension of local fields,* $\mathrm{Gal}(L/K)$ *and*

$$\hat{H}^0(\mathrm{Gal}(L/K), L^\times) = K^\times / N_{L/K}(L^\times)$$

are both cyclic of order $[L : K]$ and so are (non-canonically) isomorphic.

By the lemma, looking at the long exact sequence induced by the above short exact sequence yields an exact sequence

$$0 = H^2(G, \mathcal{O}_L^\times) \longrightarrow H^2(G, L^\times) \xrightarrow{v} H^2(G, \mathbb{Z}) \longrightarrow H^3(G, \mathcal{O}_L^\times) = 0$$

and so $v : H^2(G, L^\times) \xrightarrow{\sim} H^2(G, \mathbb{Z})$ is an isomorphism. Now, consider the following short exact sequence of trivial hence discrete G-modules:

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

Once again, a lemma illustrates the importance of a given short exact sequence.

Lemma. *Let G be a profinite group acting trivially on $\mathbb{Q}$. Then, $H^n(G, \mathbb{Q}) = 0$ for every $n > 0$.*

Proof. Fix $n > 0$. We have

$$H^n(G, \mathbb{Q}) = \varinjlim H^n(G/N, \mathbb{Q})$$

with the colimit taken over $N \trianglelefteq G$ open and so it suffices to prove the result for G finite. Multiplication by $|G|$ is an automorphism of $\mathbb{Q}$ and so induces an automorphism of $\hat{H}^n(G, \mathbb{Q})$ which is also multiplication by $|G|$. We therefore have $\hat{H}^n(G, \mathbb{Q}) = 0$ since $\hat{H}^n(G, \mathbb{Q})$ is $|G|$-torsion. The result follows since Tate and group cohomology agree for a finite group in positive degree. □

By the lemma, looking at the long exact sequence induced by the above short exact sequence yields an exact sequence

$$0 = H^1(G, \mathbb{Q}) \longrightarrow H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2(G, \mathbb{Z}) \longrightarrow H^2(G, \mathbb{Q}) = 0$$

where δ is the connecting homomorphism induced by the snake lemma. This prompts the following definition:

Definition. *Let L/K be an unramified G-Galois extension of a nonarchimedean local field K. The* ***invariant map*** $\mathrm{inv}_{L/K} : H^2(L/K) \to \mathbb{Q}/\mathbb{Z}$ *is defined to be the composition*

$$H^2(L/K) \xrightarrow{v} H^2(G, \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{f \mapsto f(\mathrm{Frob}_{L/K})} \mathbb{Q}/\mathbb{Z}$$

where we interpret $H^1(G, \mathbb{Q}/\mathbb{Z})$ as the Pontryagin dual $G^\vee :=$ $\mathrm{Hom}_{\mathrm{cont}}(G, \mathbb{Q}/\mathbb{Z})$ of continuous group homomorphisms $G \to \mathbb{Q}/\mathbb{Z}$.[7]

[7] This follows since crossed homomorphisms are the same as homomorphisms in this case. The topology on $\mathbb{Q}/\mathbb{Z}$ is the quotient topology induced by the standard topology on $\mathbb{Q}$.

Lemma. *Under the same hypotheses as in the above definition,* $\mathrm{inv}_{L/K}$ *is an injective homomorphism, with image* $\dfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ *for* L/K *finite.*

Proof. We begin by showing that $f \mapsto f(\mathrm{Frob}_{L/K})$ and hence $\mathrm{inv}_{L/K}$ is injective. Suppose first that L/K is finite. Then, G is cyclic of order $[L:K]$ with generator $\mathrm{Frob}_{L/K}$ and so $f \mapsto f(\mathrm{Frob}_{L/K})$ is injective since $f \in G^\vee$ is then uniquely determined by its value at $\mathrm{Frob}_{L/K}$. Suppose now that L/K is infinite. Then, $\mathrm{Frob}_{L/K}$ is defined by

$$\mathrm{Frob}_{L/K}|_E = \mathrm{Frob}_{E/K}$$

for every E/K finite contained in L. Let $f, g \in G^\vee$ such that f, g agree on $\mathrm{Frob}_{L/K}$. Then, the above argument gives that

$$f|_{\mathrm{Gal}(E/K)} = g|_{\mathrm{Gal}(E/K)}$$

for every E/K finite contained in L. Continuity of f, g and the fact that

$$\mathrm{Gal}(L/K) \cong \varprojlim \mathrm{Gal}(E/K)$$

then give $f = g$. Hence, $f \mapsto f(\mathrm{Frob}_{L/K})$ is injective.

To see that $\mathrm{inv}_{L/K}$ has the claimed image in the case of L/K finite, first note that the map $\mathrm{Frob}_{L/K} \mapsto 1/[L:K]$ defines an element of $G^\vee$ and so $\mathrm{inv}_{L/K}$ contains $\dfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ in its image. This must be the entire image of $\mathrm{inv}_{L/K}$ since both $\dfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ and

$$H^2(\mathrm{Gal}(L/K), L^\times) \cong \hat{H}^0(\mathrm{Gal}(L/K), L^\times)$$

have order $[L:K]$. □

Moreover, the functoriality of inflation and the maps used to define the invariant map gives a commutative diagram

$$\begin{tikzcd} H^2(E/K) \arrow[r, "\mathrm{inv}_{E/K}"] \arrow[d, "\mathrm{Inf}"'] & \mathbb{Q}/\mathbb{Z} \arrow[d, equal] \\ H^2(L/K) \arrow[r, "\mathrm{inv}_{L/K}"'] & \mathbb{Q}/\mathbb{Z} \end{tikzcd}$$

for K a nonarchimedean local field and $K \subseteq E \subseteq L$ such that L/K is unramified (which automatically gives that E/K is unramified).

Theorem. *Let* K *be a nonarchimedean local field. Then, there exists a unique isomorphism*

$$\mathrm{inv}_K : H^2(K^{\mathrm{unr}}/K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

such that, for every finite extension L/K *contained in* K^{unr}*, composition with inflation*

$$\mathrm{Inf} : H^2(L/K) \to H^2(K^{\mathrm{unr}}/K)$$

induces $\mathrm{inv}_{L/K}$.

Proof. Take $\mathrm{inv}_K := \mathrm{inv}_{K^{\mathrm{unr}}/K}$. The above comments show this map behaves as desired. Uniqueness follows from a little bit of Galois theory. □

Definition. *As the above theorem suggests, we have reason to study*

$$\mathrm{Br}(K) := H^2(K^{\mathrm{sep}}/K),$$
$$\mathrm{Br}^{\mathrm{unr}}(K) := H^2(K^{\mathrm{unr}}/K)$$

for a field K. The former is called the ***(cohomological) Brauer group of*** K *and appears in many different applications outside of class field theory.*

Remark. *The notation $\mathrm{Br}^{\mathrm{unr}}(K)$ is our own. Though this may seem like a separate notion, we will see shortly that $\mathrm{Br}^{\mathrm{unr}}(K) \cong \mathrm{Br}(K)$ canonically for K a local field.*

Theorem. *Let L/K be a finite separable extension of nonarchimedean local fields. Then, there exists a canonical homomorphism $\psi : \mathrm{Br}^{\mathrm{unr}}(K) \to \mathrm{Br}^{\mathrm{unr}}(L)$ such that we have a commutative diagram*

$$\begin{tikzcd}
\mathrm{Br}^{\mathrm{unr}}(K) \arrow[r, "\psi"] \arrow[d, "\mathrm{inv}_K"'] & \mathrm{Br}^{\mathrm{unr}}(L) \arrow[d, "\mathrm{inv}_L"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "{[L:K]}"'] & \mathbb{Q}/Z
\end{tikzcd}$$

where the bottom map is multiplication by $[L : K]$. Moreover, if L/K is Galois then $\ker\psi$ can be canonically identified as a cyclic subgroup of $H^2(L/K)$ of order $[L : K]$.

Proof. Note first of all that $L^{\mathrm{unr}} = LK^{\mathrm{unr}}$ since maximal unramified extensions of local fields are obtained by adjoining suitable roots of unity that depend only on the characteristic of the residue field. One consequence of this is that L^{unr}/K is Galois provided that L/K is Galois. Let $\mathfrak{p}$ be the unique maximal ideal of $\mathcal{O}_K$ with associated normalized discrete valuation v_K. Let $\mathfrak{q}$ be the unique maximal ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}$ with associated normalized discrete valuation v_L. Let e and f be the ramification degree and inertia degree of $\mathfrak{q}$, respectively. Then, v_L extends v_K with index e, $[L : K] = ef$, and

$$\mathrm{Frob}_L |_{K^{\mathrm{unr}}} = \mathrm{Frob}_K^f .$$

Hence, $\mathrm{Gal}(K^{\mathrm{unr}}/K)$ has index e in $\mathrm{Gal}(L^{\mathrm{unr}}/L)$. Moreover, v_K and v_L extend (by lifting uniformizers) to give a commutative diagram

$$\begin{tikzcd}
K^{\mathrm{unr},\times} \arrow[r, "v_K"] \arrow[d] & \mathbb{Z} \arrow[d, "{[e]}"] \\
L^{\mathrm{unr},\times} \arrow[r, "v_L"'] & \mathbb{Z}
\end{tikzcd}$$

where the righthand vertical map is multiplication by e. Let $\mathrm{Res} : H^2(L^{\mathrm{unr}}/K) \to \mathrm{Br}^{\mathrm{unr}}(L)$ and $\mathrm{Inf}' : \mathrm{Br}^{\mathrm{unr}}(K) \to H^2(L^{\mathrm{unr}}/K)$ be the appropriate restriction and inflation maps. Define

$\psi := \mathrm{Res} \circ \mathrm{Inf}'$. Given $g \in \mathrm{Gal}(K^{\mathrm{unr}}/K)^\vee$, we have

$$\begin{aligned}([e] \circ \psi)(g)(\mathrm{Frob}_L) &= e\psi(g)(\mathrm{Frob}_L)\\ &= eg(\mathrm{Frob}_K^f)\\ &= efg(\mathrm{Frob}_K)\\ &= [L:K]g(\mathrm{Frob}_K).\end{aligned}$$

Putting everything together therefore gives a commutative diagram

$$\begin{tikzcd}
\mathrm{Br}^{\mathrm{unr}}(K) \arrow[r, "v_K"] \arrow[d, "\psi"] & H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K), \mathbb{Z}) \arrow[r, "\delta^{-1}"] \arrow[d, "{[e]\circ\psi}"] & H^1(\mathrm{Gal}(K^{\mathrm{unr}}/K), \mathbb{Q}/\mathbb{Z}) \arrow[r, "g\mapsto g(\mathrm{Frob}_K)"] \arrow[d, "{[e]\circ\psi}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "{[L:K]}"] \\
\mathrm{Br}^{\mathrm{unr}}(L) \arrow[r, "v_L"'] & H^2(\mathrm{Gal}(L^{\mathrm{unr}}/L), \mathbb{Z}) \arrow[r, "\delta^{-1}"'] & H^1(\mathrm{Gal}(L^{\mathrm{unr}}/L), \mathbb{Q}/\mathbb{Z}) \arrow[r, "g\mapsto g(\mathrm{Frob}_L)"'] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

and hence a commutative diagram

$$\begin{tikzcd}
\mathrm{Br}^{\mathrm{unr}}(K) \arrow[r, "\psi"] \arrow[d, "\mathrm{inv}_K"'] & \mathrm{Br}^{\mathrm{unr}}(L) \arrow[d, "\mathrm{inv}_L"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "{[L:K]}"'] & \mathbb{Q}/Z
\end{tikzcd}$$

Thus, $\ker\psi \cong \dfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ is cyclic of order $[L:K]$. Suppose now that L/K is Galois. Then, applying Hilbert's Theorem 90 gives us short exact inflation-restriction sequences

$$0 \longrightarrow H^2(L/K) \xrightarrow{\mathrm{Inf}} H^2(L^{\mathrm{unr}}/K) \xrightarrow{\mathrm{Res}} \mathrm{Br}^{\mathrm{unr}}(L) \longrightarrow 0$$

and

$$0 \longrightarrow \mathrm{Br}^{\mathrm{unr}}(K) \xrightarrow{\mathrm{Inf}'} H^2(L^{\mathrm{unr}}/K) \xrightarrow{\mathrm{Res}'} H^2(L^{\mathrm{unr}}/K^{\mathrm{unr}}) \longrightarrow 0$$

and hence a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \ker\psi \arrow[r] \arrow[d, "\varphi"] & \mathrm{Br}^{\mathrm{unr}}(K) \arrow[r, "\psi"] \arrow[d, "\mathrm{Inf}'"] & \mathrm{Br}^{\mathrm{unr}}(L) \arrow[d, equal] \\
0 \arrow[r] & H^2(L/K) \arrow[r, "\mathrm{Inf}"'] & H^2(L^{\mathrm{unr}}/K) \arrow[r, "\mathrm{Res}"'] & \mathrm{Br}^{\mathrm{unr}}(L)
\end{tikzcd}$$

defining φ as an injective homomorphism. It follows that $H^2(L/K)$ contains a cyclic subgroup of order $[L:K]$. □

Corollary. *Let L/K be a finite G-Galois extension of nonarchimedean local fields. Then, $H^2(L/K)$ is cyclic of order $[L:K]$.*

Proof. $H^2(L/K)$ contains a cyclic subgroup of order $[L:K]$ by the previous theorem and so it suffices to show that $|H^2(L/K)| \leq [L:K]$. Suppose first that G is cyclic. We take as given that $\mathcal{O}_L^\times$ contains a cohomologically trivial G-submodule A of finite index.[8] Letting h denote the Herbrand quotient, the short exact sequence

[8] This follows from the Normal Basis Theorem and a fairly straightforward bootstrapping argument.

$$1 \longrightarrow A \longrightarrow \mathcal{O}_L^\times \longrightarrow \mathcal{O}_L^\times/A \longrightarrow 1$$

gives $h(\mathcal{O}_L^\times) = h(A)h(\mathcal{O}_L^\times/A) = 1$ since A is cohomologically trivial and $\mathcal{O}_L^\times/A$ is finite. The short exact sequence

$$1 \longrightarrow \mathcal{O}_L^\times \longrightarrow L^\times \xrightarrow{v} \mathbb{Z} \longrightarrow 0$$

then gives

$$|H^2(L/K)| = |\hat{H}^0(G, L^\times)| = \frac{|\hat{H}^0(G, L^\times)|}{|\hat{H}^1(G, L^\times)|} = h(L^\times) = h(\mathcal{O}_L^\times)h(\mathbb{Z}) = [L:K]$$

where we have implicitly invoked Hilbert's Theorem 90 and the 2-periodicity of Tate cohomology for cyclic groups.

Now, drop the assumption that G is cyclic. G is a p-group hence solvable, where p is the characteristic of the residue field of K.[9] Hence, G admits a composition series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

all of whose successive quotients are cyclic p-groups. The goal now is to induct on both the length n and the order of G. The base case is handled above. For the inductive step, it suffices by the Fundamental Theorem of Galois Theory to consider $K \subsetneq E \subsetneq L$ with E/K Galois. Then, by Hilbert's Theorem 90 we have a short exact sequence

$$0 \longrightarrow H^2(E/K) \xrightarrow{\text{Inf}} H^2(L/K) \xrightarrow{\text{Res}} H^2(L/E)$$

$[E:K], [L:E]$ are both strictly smaller than $[L:K]$ and so the inductive hypothesis gives that $|H^2(E/K)| \leq [E:K]$ and $|H^2(L/E)| \leq [L:E]$. Hence,

$$|H^2(L/K)| \leq |H^2(E/K)||H^2(L/E)| \leq [E:K][L:E] = [L:K]$$

and so we have our result. □

Remark. *The above proof along with the proof of the previous theorem actually shows something stronger than the statement of the corollary, namely that there exists a generator $\gamma \in H^2(L/K)$ with order $[L:K]$ such that, for every $H \leq G$, $H^2(H, L^\times)$ is generated by* $\mathrm{Res}(\gamma)$*.*

Corollary. *Let K be a nonarchimedean local field. Then, the canonical map*

$$\mathrm{Inf} : \mathrm{Br}^{\mathrm{unr}}(K) \to \mathrm{Br}(K)$$

is an isomorphism. There exists a unique isomorphism

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

such that, for every finite extension L/K contained in K^{sep}, composition with inflation

$$\mathrm{Inf} : H^2(L/K) \to \mathrm{Br}(K)$$

induces $\mathrm{inv}_{L/K} : H^2(L/K) \xrightarrow{\sim} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ *extending the invariant map in the unramified case. Moreover, we have a commutative diagram*

[9] If G is a finite p-group then it has a nontrivial center. This allows us to do an inductive argument to build a suitable composition series for G. That $G = \mathrm{Gal}(L/K)$ is a p-group for L/K a finite separable extension of nonarchimedean local fields and suitable p follows from looking at the ramification filtration of G.

$$\begin{tikzcd}
\mathrm{Br}^{\mathrm{unr}}(K) \arrow[r, "\psi"] \arrow[d, "\mathrm{inv}_K"'] & \mathrm{Br}^{\mathrm{unr}}(L) \arrow[d, "\mathrm{inv}_L"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "{[L:K]}"'] & \mathbb{Q}/Z
\end{tikzcd}$$

and if L/K is also Galois then

$$\begin{tikzcd}
0 \arrow[r] & H^2(L/K) \arrow[r, "\mathrm{Inf}"] \arrow[d, "\mathrm{inv}_{L/K}"] & \mathrm{Br}(K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_K"] & \mathrm{Br}(L) \arrow[r] \arrow[d, "\mathrm{inv}_L"] & 0 \\
0 \arrow[r] & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r, "{[L:K]}"'] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

is an isomorphism of exact sequences.

Proof. Most of the results follow from work we have done already. Given L/K finite Galois, we have $\varphi : \ker\psi \xrightarrow{\sim} H^2(L/K)$ canonically and so $H^2(L/K)$ is identified as a subgroup of $\mathrm{Br}^{\mathrm{unr}}(K)$ in a functorial manner. We already know that the inflation maps $H^2(L/K) \to \mathrm{Br}(K)$ are injective and so, since $\mathrm{Br}(K)$ and $\mathrm{Br}^{\mathrm{unr}}(K)$ are both expressible as colimits over directed systems with morphisms given by inflation, it follows that $\mathrm{Inf} : \mathrm{Br}^{\mathrm{unr}}(K) \to \mathrm{Br}(K)$ is an isomorphism. Thus, given L/K finite separable, we may replace K^{unr} and L^{unr} in the previous theorem with K^{sep} and $L^{\mathrm{sep}} = K^{\mathrm{sep}}$, respectively. Then, $\psi = \mathrm{Res}$ as defined in the proof of the previous theorem and we obtain the desired commutative diagrams. □

Proof of Main Part of Local Artin Reciprocity

Definition. *Let L/K be a finite G-Galois extension of nonarchimedean local fields. Then, the **fundamental class** of L/K is $u_{L/K} := \mathrm{inv}_{L/K}^{-1}(1/[L:K])$.*

Fundamental classes will soon play a very important role. First, though, recall the basics of cup products and the statement of Tate's Theorem.

Definition. *Let G be a finite group. A **cup product** on G is a family of $\mathbb{Z}$-linear homomorphisms*

$$\hat{H}^p(G,A) \otimes \hat{H}^q(G,B) \to \hat{H}^{p+q}(G, A \otimes B)$$
$$a \otimes b \mapsto a \smile b$$

for $p, q \in \mathbb{Z}$ and G-modules A, B[10] that is

(i) *functorial in A, B;*

(ii) *induced by the natural product $A^G \otimes B^G \to (A \otimes B)^G$ for $p = 0 = q$;*

(iii) *"well-behaved" with respect to short exact sequences.*

Moreover, for all $p, q, r \in \mathbb{Z}$, G-modules A, B, C, $a \in \hat{H}^p(G,A), b \in \hat{H}^q(G,B), c \in \hat{H}^r(G,C)$, and $H \leq G$,

[10] Note that $A \otimes B$ is the G-module whose underlying abelian group is $A \otimes_{\mathbb{Z}} B$ equipped with a diagonal action of G – i.e., $g \cdot (a \otimes b) = ga \otimes gb$ for $g \in G, a \in A, b \in B$.

(i) $(a \smile b) \smile c = a \smile (b \smile c)$ *via the natural isomorphism* $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$;

(ii) $a \smile b = (-1)^{pq} b \smile a$ *via the natural isomorphism* $A \otimes B \cong B \otimes A$;

(iii) $\operatorname{Res}(a \smile b) = \operatorname{Res}(a) \smile \operatorname{Res}(b)$;

(iv) $\operatorname{CoRes}(a \smile \operatorname{Res}(b)) = \operatorname{CoRes}(a) \smile b$,

where $\operatorname{Res} = \operatorname{Res}^G_H$ *and* $\operatorname{CoRes} = \operatorname{CoRes}^G_H$.

Proposition. *Let G be a finite group. Then, there exists a unique cup product on G.*[11]

Theorem (Tate-Nakayama)**.** *Let G be a finite group and A a G-module such that $H^2(G, A)$ is cyclic with generator γ and, for every $H \leq G$, $H^1(H, A) = 0$ and $H^2(H, A)$ is cyclic of order $|H|$ generated by $\operatorname{Res}(\gamma)$.*[12] *Then, for every $n \in \mathbb{Z}$, the map*

$$\Phi_\gamma : \hat{H}^n(G, \mathbb{Z}) \to \hat{H}^{n+2}(G, A)$$

given by taking the cup product with γ is an isomorphism compatible with restriction and corestriction in the sense that, given any $H \leq G$ and $n \in \mathbb{Z}$, we have commutative diagrams

$$\begin{tikzcd}
\hat{H}^n(G,\mathbb{Z}) \arrow[r, "\Phi_\gamma"] \arrow[d, "\operatorname{Res}"'] & \hat{H}^{n+2}(G,A) \arrow[d, "\operatorname{Res}"] \\
\hat{H}^n(H,\mathbb{Z}) \arrow[r, "\Phi_{\operatorname{Res}(\gamma)}"'] & \hat{H}^{n+2}(H,A)
\end{tikzcd}
\quad \textit{and} \quad
\begin{tikzcd}
\hat{H}^n(G,\mathbb{Z}) \arrow[r, "\Phi_\gamma"] & \hat{H}^{n+2}(G,A) \\
\hat{H}^n(H,\mathbb{Z}) \arrow[r, "\Phi_{\operatorname{Res}(\gamma)}"'] \arrow[u, "\operatorname{CoRes}"] & \hat{H}^{n+2}(H,A) \arrow[u, "\operatorname{CoRes}"']
\end{tikzcd}$$

Corollary. *Let L/K be a finite G-Galois extension of nonarchimedean local fields. Then, for every $n \in \mathbb{Z}$, the map*

$$\Phi_{L/K} : \hat{H}^n(G, \mathbb{Z}) \to \hat{H}^{n+2}(G, L^\times)$$

given by taking the cup product with $u_{L/K}$ is an isomorphism compatible with restriction and corestriction.

Let L/K be a finite G-Galois extension of nonarchimedean local fields. $\theta_{L/K}$ is defined as the inverse of the composition

$$G^{\mathrm{ab}} \xrightarrow{\sim} H_1(G, \mathbb{Z}) = \hat{H}^{-2}(G, \mathbb{Z}) \xrightarrow{\Phi_{L/K}} \hat{H}^0(G, L^\times) = K^\times / N_{L/K}(L^\times)$$

where $\Phi_{L/K}$ is the isomorphism provided by the above corollary.

Lemma. *Let $K \subseteq E \subseteq L$ be a tower of finite Galois extensions of nonarchimedean local fields. Then, we have commutative diagrams*

[11] Uniqueness here means up to natural equivalence.

[12] It in fact suffices that these results hold for at least one p-Sylow subgroup of G for every prime p dividing $|G|$.

$$\begin{tikzcd}
E^\times \arrow[r, "\theta_{L/E}"] \arrow[d, "N_{E/K}"'] & \mathrm{Gal}(L/E)^{\mathrm{ab}} \arrow[d] \\
K^\times \arrow[r, "\theta_{L/K}"'] & \mathrm{Gal}(L/K)^{\mathrm{ab}}
\end{tikzcd} \quad \textit{and} \quad \begin{tikzcd}
K^\times \arrow[r, "\theta_{L/K}"] \arrow[d, equal] & \mathrm{Gal}(L/K)^{\mathrm{ab}} \arrow[d] \\
K^\times \arrow[r, "\theta_{E/K}"'] & \mathrm{Gal}(E/K)^{\mathrm{ab}}
\end{tikzcd}$$

where the unmarked vertical lefthand and righthand maps are inclusion and restriction maps, respectively.

Proof. Let Res : $H^2(L/K) \to H^2(L/E)$ and CoRes : $H^2(L/E) \to H^2(L/K)$ be the appropriate restriction and co-restriction maps. One can show that

(i) $u_{E/K} = [L : E]u_{L/K}$;

(ii) $\mathrm{Res}(u_{L/K}) = u_{L/E}$;

(iii) $\mathrm{CoRes}(u_{L/E}) = [E : K]u_{L/K}$.

The result then follows from the explicit forumlas for restriction and co-restriction and the compatibility of the Tate isomorphism with restriction and co-restriction. □

Thus, $\{\theta_{L/K}\}$ for L/K finite abelian forms a compatible system giving rise to the desired continuous local Artin map $\theta_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ via $\theta_K|_L = \theta_{L/K}$.[13] That θ_K sends uniformizers to Frobenius elements follows from a very careful bookkeeping argument. In fact, careful accounting shows that the standard filtration of $\mathcal{O}_K^\times$ maps isomorphically onto the ramification filtration of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$.[14]

The Existence Theorem

We know from above that the local Artin map $\theta_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ "plays nice" with respect to finite extensions L/K contained in K^{ab} in the sense that the local Artin homomorphism

$$\theta_{L/K} : K^\times/N_{L/K}(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K)$$

is functorial in L. It follows that the local Artin homomorphisms induce an isomorphism

$$\varprojlim K^\times/N_{L/K}(L^\times) \cong \varprojlim \mathrm{Gal}(L/K) \cong \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

where the inverse limits are taken over finite extensions L/K contained in K^{ab}.

Definition. *Let K be a field. Then, $\Gamma \leq K^\times$ is a* ***norm subgroup*** *if there exists a finite Galois extension L/K such that $\Gamma = N_{L/K}(L^\times)$.*

To prove the statement about profinite completion, it suffices to prove the following.

Theorem (Existence Theorem)**.** *Let K be a nonarchimedean local field and $\Gamma \leq K^\times$. Then, Γ is a norm group if and only if it is open with finite index (equivalently, closed with finite index).*

[13] Continuity of θ_K follows from the continuity of each $\theta_{L/K}$ and the profinite nature of the topology on $\mathrm{Gal}(K^{\mathrm{ab}}/K)$.

[14] We have not explained ramification filtrations and so we do not give a precise formulation of this statement.

For the sake of convenience, we assume char $K = 0$ with unique maximal ideal $\mathfrak{p}$. This assumption allows us to take an approach along the lines of Kummer theory.

Lemma. *Let $\Gamma \le \Gamma' \le K^\times$ with Γ finite index open. Then, Γ' is finite index open.*

Proof. The result follows from $|K^\times : \Gamma'| \le |K^\times : \Gamma| < \infty$ and the fact that $U \subseteq K^\times$ is an open neighborhood of 1 if and only if it contains $1 + \mathfrak{p}^m$ for $m \gg 0$. □

Lemma. *Let $n > 0$. Then, $(K^\times)^n$ is a finite index open subgroup of $K^\times$.*

This proves the forward direction of the Existence Theorem since, given L/K a finite abelian extension of nonarchimedean local fields, $N_{L/K}(L^\times) \supseteq N_{L/K}(K^\times) = (K^\times)^{[L:K]}$.

Lemma. *Let $\Gamma \le \Gamma' \le K^\times$ with Γ a norm subgroup. Then, Γ' is a norm subgroup.*

Proof. By assumption, there exists L/K finite abelian such that $\Gamma = N_{L/K}(L^\times)$. We have

$$\Gamma'/\Gamma \hookrightarrow K^\times/N_{L/K}(L^\times) \xrightarrow{\theta_{L/K}} \mathrm{Gal}(L/K)$$

where the first map is induced by the inclusion $\Gamma' \subseteq K^\times$ and so there exists $K \subseteq E \subseteq L$ such that $\Gamma'/\Gamma \cong \mathrm{Gal}(L/E)$. It then follows from the commutativity of the diagram

$$\begin{tikzcd} E^\times \arrow[r, "\theta_{L/E}"] \arrow[d, "N_{E/K}"'] & \mathrm{Gal}(L/E) \arrow[d] \\ K^\times \arrow[r, "\theta_{L/K}"] & \mathrm{Gal}(L/K) \end{tikzcd}$$

that $\Gamma' = N_{E/K}(E^\times)$. □

Lemma. *Let $n > 0$. Then, $(K^\times)^n$ is a norm subgroup of $K^\times$.*

Proof. First reduce to the case that K contains the set of nth roots of unity. Second use Kummer theory to get the result. □

TO DO: Elaborate on the first reduction and the Kummer theory details.

Lemma. *Let $\Gamma \le K^\times$ be a finite index open subgroup. Then, Γ contains $(K^\times)^n$ for some $n > 0$.*

This proves the backward direction of the Existence Theorem.
TO DO: Work out some explicit cases of the local Artin map.

References and Further Reading

The main text for these notes is *Algebraic Number Theory* by Cassels and Fröhlich, with special emphasis placed on the section on local class field theory written by Serre. Serre's *Local Fields* goes into far more detail on the same material and is recommended by Rok. Andrew Sutherland's lecture notes on 18.785 Number Theory I and 18.786 Number Theory II are quite good for learning algebraic number theory and local class field theory, respectively.[15] Oron Propp's notes on 18.786

[15] Sutherland's 18.785 notes from Fall 2017 are more extensive, but the ones from Fall 2015 are better written in my opinion.

Number Theory II present a more homotopy theoretic viewpoint of local class field theory. Bjorn Poonen has some concise and wonderful notes summarizing the statements of local and global class field theory, while Keith Conrad has some great notes on the history of class field theory. We have in our treatment neglected to talk about many important things, among them Lubin-Tate formal groups and class formations. A good reference for the former is Emily Riehl's undergraduate thesis, while a good reference for the latter is *Local Fields* or *Class Field Theory* by Artin and Tate. Finally, Romyar Sharifi's notes on group and Galois cohomology contain a wonderful treatment of Kummer theory.