Notes on Galois Cohomology, and Related Pairings

Jonathan Komada Eriksen

Contents

The first four sections, and Section 7, of this note closely follows the book "A Gentle Course in Local Class Field Theory", by Guillot [2] (often referred to as "the book" in the text). However, our main goal will not really be local class field theory (even if we include a bit in the last section), but rather to cover the definition of many different pairings, useful in cryptography, which we do in Section 5. For this chapter, the main source for this section is the article by Silverman [5] for all the pairings on abelian varieties, and the book by Voight [7] for the hilbert pairing and relation to quaternion algebras. Personally, I could never remember the definition of all these different pairings; clearly a sign that I did not understand them. Although this is probably subjective, I think galois cohomology is greatly clarifying for understanding how these pairings appear, and hopefully I'll be able to remember them now!

Additionally, I have included Section 6, a chapter with notes on the Selmer groups of an abelian variety. This is a very cool group, whose definition is not hard to give, assuming galois cohomology. The main references here are [6, Chapter X], and a note by Poonen [3].

These notes are mainly written for myself. Proofs will often be incomplete, or outright missing, containing what I think is just enough information to remind me how its done when I look back at these notes in the future (or, other times, I was just too lazy to write them down). But definition and theorem statements might be useful for others too, as a quick reminder/collection of various useful results.

1 Infinite Galois theory

The first goal is to define the absolute galois group $\mathrm{Gal}(\overline{F}/F)$, and subsequently to extend the fundamental theorem of galois theory to these extensions.

1.1 Profinite groups

Definition 1.1: Topological groups and isomorphisms

A **topological group** G is a group equipped with a topology such that the inverse map is continuous, and the group operation is continuous (wrt. the product topology).
Similarily, a **topological isomorphism** is an isomorphism φ of topological groups, which is also a homeomorphism (i.e. both φ and φ^{-1} is continuous).

Example 1.1.1. *Some simple, but important examples of topological groups will be finite groups with the discrete topology (which will be used to construct profinite groups), and both the additive and multiplicative group of K, where K can be $\mathbb{R}, \mathbb{C}$, or any local field $\mathbb{Q}_p$ (in this case, the topology will of course be the one induced by the absolute value).*

For a slightly more involved example, one can check that $\mathbf{GL}_n(K)$ is also a toplogical group for any n (using the product topology on K^{n^2}), and any subgroup of a topological group is a topological group. As an aside, the closed *subgroups of $\mathbf{GL}_n(\mathbb{R})$ is called a **linear Lie group**, and a* closed *subgroup of $\mathbf{GL}_n(\mathbb{Q}_p)$ is called a **linear p-adic Lie group**.*

The following is really an important lemma describing the relationships between open, closed and finite index subgroups.

Lemma 1.1.2. *Let G be a topological group, and $H < G$ a subgroup.*

- *H open $\Rightarrow$ H closed.*

- *H closed and finite index $\Rightarrow$ H open.*
- *if G is additionally assumed to be compact, then H open $\Leftrightarrow$ H closed and finite index.*

Proof. The key is that the cosets of H are all homeomorphic to H. Thus, if H is open, the compliment of H is open (being the union of all the cosets except H), thus H is closed. The same works to argue that H closed and finite index implies open (finite index being necessary to argue that the finite union is closed of course). Finally, G being compact, we see that the cosets of H form an open cover when H is open, and thus gives that H must have finite index. □

The big intuition to remember from the above lemma is that for compact topological groups (which will be essentially all we look at), open sets are really big.

The main topological groups that we will care about are the following:

Definition 1.2: Profinite groups

A **profinite group** is a compact and Haussdorf topological group G for which every open set containing the identity, also contain an open, normal subgroup $U < G$.

The more classical definitions are given by the following

Proposition 1.1.3. *Let G be a topological group. TFAE:*

- *G is profinite.*
- *G is topologically isomorphic to an inverse limit $\lim_{i\in I} G_i$ of finite groups, for a directed set I.*
- *G is a closed subgroup of a product of finite groups.*

Proof. We first discuss (3) implies (1). First, we show that a product of finite groups is profinite. The fact such a product is Haussdorf is immidiate, while compactness is a consequence of the famous "Tychonoff's theorem" (asside: which is equivalent to AoC). Finally, the fact that every open subset containing the identity also contains an open, normal subgroup of the form

$$U = \{(g_i)_{i\in I} \mid g_{i_k} = 1, 1 \leq k \leq n\},$$

where $\{i_k\}_k \subset I$ denote a finite set of indeces, is clear by examining the definition of the product topology. Then, finally it is easy to see that a closed subgroup of a profinite group is again profinite; Compactness and Haussdorf is immidiate, while the open subgroup condition follows from taking the group $U \cap H$ for the subgroup $U < G$ that one gets from G being profinite. Note that the last point, closed subgroups of profinite groups are again profinite also shows (2) implies (3), as $\lim_{i\in I} G_i$ is indeed a closed subgroup of $\prod_{i\in I} G_i$.

Finally, (1) implies (2) is a bit more technical, and you can look in the book if you need to. The key part is to show that any profinite G is isomorphic to

$$\varprojlim_{U_i<G} G/U_i$$

where the U_i run over the open, normal subgroups of G, and where the subgroups indeed form a directed set by inclusion. □

1.2 Infinite galois extensions

Let K/F be a (not necessarily finite!) galois extension, i.e. seperable and normal. The galois group has a natural description

Proposition 1.2.1. *There is an isomorphism of groups*

$$\mathrm{Gal}(K/F) = \varprojlim_{L} \mathrm{Gal}(L/F)$$

where the inverse limit is taken over all finite *galois extensions L/F.*

Proof. This is surprisingly obvious. The map

$$\iota : \mathrm{Gal}(K/F) \to \prod_{L} \mathrm{Gal}(L/F)$$

is clearly injective (if $\rho \in \mathrm{Gal}(K/F)$ is not the identity, then we must have $\rho(x) \neq x$ for some $x \in K$, but x is then contained in a finite extension L, so $\iota(\rho)$ is also not the identity). Now the image of ι is precicely the inverse limit (maybe slightly harder to prove surjectivity, but both are really directly from definitions). □

Now in the usual (finite) galois correspondence, the subgroups of the galois group is in bijection with intermidiate fields. When extending this to infinite galois extensions this unfortunately fails, however it is easily fixed by considering topological groups instead! By the proposition above, $Gal(K/F)$ has a natural topology in light of Proposition 1.1.3, making it into a profinite group. This topology is appearently called the **Krull topology**.

We start by a lemma which says that nothing new happens in one direction of the Galois correspondence. We use the usual notation: Given a subgroup $H < \mathrm{Gal}(K/F)$, let L_H denote the fixed-field of H.

Lemma 1.2.2. *Let K/F be an algebraic Galois extension. Then*

$$L = L_{\mathrm{Gal}(K/L)}$$

for any (not necessarily finite!) field extension L/F, with $K \subseteq L \subseteq F$.

Proof. The proof is the same as in the finite case. □

However, the Galois correspondence does not hold for all subgroups of $\mathrm{Gal}(K/F)$.

Lemma 1.2.3. *Let $F \subset L \subset K$. Then* $\mathrm{Gal}(K/L)$ *is a closed subgroup of* $\mathrm{Gal}(K/F)$ *(in the Krull topology).*

Proof. We show that every element in the complement of $H = \mathrm{Gal}(K/L)$ is contained in an open set contained in the complement of H. Let $\rho \in \mathrm{Gal}(K/F)$ be an element such that $\rho \notin \mathrm{Gal}(K/L)$. Take any element $x \in L$ such that $\rho(x) \neq x$, and consider the finite extension $E = F[x]$. Replacing E by its galois closure, we assume E/F is galois.

Then the set

$$U = \{\tau \in \mathrm{Gal}(K/F) \mid \tau_E = \rho_E\}$$

i.e. the fiber $\pi^{-1}(\rho_E)$ of the surjection $\pi : \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F)$ is open (for instance, it is homeomorphic to $\mathrm{Gal}(K/E)$). Clearly $U \cap H = \varnothing$, so we are done. □

We can now prove

Theorem 1.2.4 (The Fundamental Theorem of (infinite) Galois Theory)**.** *Let K/F be an algebraic Galois extension. There is a one-to-one, order-reversing correspondence between the intermidiate subfields of K/F and the closed (eq. open of finite index) subgroups of* $\mathrm{Gal}(K/F)$*, mapping L to* $\mathrm{Gal}(K/L)$ *and $H < \mathrm{Gal}(K/F)$ to L_H.*

Proof. By the results above, all that remains to prove is that given a closed subgroup $H < \mathrm{Gal}(K/F)$, we have that

$$\mathrm{Gal}(K/L_H) = H.$$

Now let $H < \mathrm{Gal}(K/F)$ be any subgroup (not necessarily normal), and let Let $H_0 = \mathrm{Gal}(K/L_H)$. We obviously have $H \subseteq H_0$. If we can prove that $H_0 \subseteq \overline{H}$, we are done, because of the previous Lemma which stated that H_0 is closed. This part is a little technical, but follows from a result we skipped, which says the following: Let $X = \lim_i X_i$ is an inverse limit of discrete topological spaces over a directed set, let $p_i : X \to X_i$ be the projection maps. Then, given $A, B \subset X$, such that $p_i(A) \subset p_i(B)$ for all i, we have that $A \subset \overline{B}$. □

Example 1.2.5. *The two nicest examples of infinite galois extensions to remember are*

$$\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) = \widehat{\mathbb{Z}}$$

and

$$\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) = \widehat{\mathbb{Z}}^{\times}.$$

Both of these are trivial to derive from the definitions, but illustrative to think about.

2 Group and Galois cohomology

Recall (or see note on) the basic results and constructions in homological algebra.

One thing to state, which went over my head in homological algebra, is the fact that a projective resultion of a module is a quasi-isomorphism to the module as a chain complex.

2.1 Group cohomology

For an group G, let $\mathbb{Z}[G]$ denote the group ring of G, i.e. the ring whose underlying abelian group is the free group generated by elements of G, and whose multiplication is given by extending the group operation linearly. A G-module is then simply a $\mathbb{Z}[G]$-module, i.e. an abelian group with an action of G given by linear maps.

In this subsection, we will **assume that G is finite**, before extending to the profinite case later.

Definition 2.1: Group (co)homology

The ***n*-th cohomology group** of G with coefficients in M is given by

$$H^n(G, M) := \mathrm{Ext}^{\mathbb{Z}[G]}_n(\mathbb{Z}, M).$$

where $\mathbb{Z}$ is the trivial $\mathbb{Z}[G]$-module (i.e. all of the group elements act trivially).
Similarily, the ***n*-th homology group** of G with coefficients in M is given by

$$H_n(G, M) := \mathrm{Tor}^n_{\mathbb{Z}[G]}(\mathbb{Z}, M).$$

These cohomology groups are infact highly computable, and the main "challenge" is to find a projective resultion of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module. From now on we assume that G is finite; in which case there is a "standard-resultion" we will define in a bit. But of course, any projective resultion will do, which can sometimes give easier examples, as for instance shown in the following

Example 2.1.1. *Let $G = \langle T \rangle$ be a cyclic group of order r. We construction a resultion of $\mathbb{Z}$ (coming from the projection $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$ given by $\epsilon(T) = 1$) as*

$$P_* := \cdots \to \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{T-1} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{T-1} \mathbb{Z}[G] \to 0$$

where $N = T^{r-1} + T^{r-2} + \cdots + 1$ is the "norm map" (which will be essential in class field theory). This is straight forward to verify that is a projective resultion.

The cochain complex $\mathrm{Hom}_{\mathbb{Z}[G]}(P_*, M)$ is now very simple. Since all the $P_n = \mathbb{Z}[G]$, we have that $\mathrm{Hom}_{\mathbb{Z}[G]}(P_n, M) = M$ (as for any ring), and thus the cochain complex looks like

$$0 \to M \xrightarrow{T-1} M \xrightarrow{N} M \xrightarrow{T-1} M \xrightarrow{N} M \to \dots$$

Thus, for $n = 0$, we find that

$$H^0(G, M) = M^G := \{m \in M \mid g \cdot m = m, \forall g \in G\}.$$

For $n > 0$, we find that

$$H^{2n}(G, M) = M^G / N(M),$$

while for $n \geq 0$, we find that

$$H^{2n+1}(G, M) = {}_N M / M'$$

where ${}_N M := \{m \in M \mid N \cdot m = 0\}$, and $M' := (T-1)(M)$.

Turning to homology, we get a very similar result, as $P_* \otimes_{\mathbb{Z}[G]} M$ is simply

$$\cdots \to M \xrightarrow{T-1} M \xrightarrow{N} M \xrightarrow{T-1} M \to 0.$$

Thus, we have

$$H_n(G, M) = \begin{cases} M/M' & \text{if } n = 0 \\ {}_N M/M' & \text{if } n = 2k, k > 0 \\ M^G/N(M) & \text{if } n = 2k+1, n \geq 0 \end{cases}$$

Of course the 0-th (co)homology groups are especially important (they are functorial, and indeed the other groups are the derived functors). Its easy to see that they are the same as in the example above in general:

$$H^0(G, M) = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) = M^G$$

because you can send 1 to any element $m \in M$, on which G acts trivially. Correspondingly,

$$H_0(G, M) = \mathbb{Z} \otimes_{\mathbb{Z}[G]} M = M_G,$$

where $M_G := M/M'$, and as in the example $M' = \{m - g \cdot m \mid \forall m \in M, g \in G\}$; indeed, verify that M' is precicely the kernel of the map $M \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} M$ given by $m \to 1 \otimes m$.

Another thing is that in the above example, the homology and cohomoly groups were very similar. This motivated the following

Definition 2.2: Tate cohomology

Let M be a G-module. The ***n*-th Tate cohomology group** is given by

$$\widehat{H}^n(G,M) := \begin{cases} H^n(G,M) & \text{if } n > 0 \\ M^G/N(M) & \text{if } n = 0 \\ {}_N M/M' & \text{if } n = -1 \\ H_{-n-1}(G,M) & \text{if } n < -1 \end{cases}$$

where $N = \sum_{\sigma \in G} \sigma$.

The fairly long previous example is thus completely summarized in the following:

Example 2.1.2. *Let G be a finite cyclic group, and M a G-module. We have that*

$$\widehat{H}^n(G,M) = \begin{cases} M^G/N(M) & \text{if } n = 2k, k \in \mathbb{Z} \\ {}_N M/M' & \text{if } n = 2k+1, k \in \mathbb{Z} \end{cases}$$

If M is a trivial G-module (i.e. the action by G on M is trivial), we have even simpler that

$$\widehat{H}^n(G,M) = \begin{cases} M/rM & \text{if } n = 2k, k \in \mathbb{Z} \\ M[r] & \text{if } n = 2k+1, k \in \mathbb{Z} \end{cases}$$

where r is the order of G, and $M[r]$ denotes the r-torsion of M.

2.2 The standard resolution.

The following is a projective resolution of $\mathbb{Z}$ as a $R = \mathbb{Z}[G]$-module for any G. This will give us the direct description of (co)homology groups, most usefull in low degrees (or theoretically).

In the following, we will consider repeated tensors $R^{\otimes n} = R \otimes \cdots \otimes R$, where the tensor product is over $\mathbb{Z}$ (not over R!). However, $R^{\otimes n}$ will still be considered as an R-module, where the action is given as

$$\sigma \cdot (\sigma_1 \otimes \cdots \otimes \sigma_n) = \sigma\sigma_1 \otimes \cdots \otimes \sigma\sigma_n$$

Let $\partial_n^{(i)} : R^{\otimes n+1} \to R^{\otimes n}$ be the map defined by $\partial_n^{(i)}(\sigma_0 \otimes \dot{\sigma}_n) = \sigma_0 \otimes \widehat{\sigma}_i \otimes \sigma_n$, i.e. dropping the i-th factor. We then give the

Definition 2.3: Standard resolution

Let $R = \mathbb{Z}[G]$. The **standard resolution** of $\mathbb{Z}$ (as an R-module) is

$$\ldots \xrightarrow{\partial_2} R \otimes R \xrightarrow{\partial_1} R \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

where the maps are defined as

$$\partial_n := \sum_{i=0}^{n} (-1)^i \partial_n^{(i)}$$

and ϵ is as before (i.e. $\epsilon(\sigma) = 1$ for all $\sigma \in G$).

From now, we often drop the subscript n, as it is obvious from context. The fact that $(R^{\otimes \star+1}, \partial_\star)$ is a cochain complex needs proof, but is completely standard, i.e. the same as in the case of simplical homology (as usual, it follows from noting that $\partial^{(i)}\partial^{(j)} = \partial^{(j-1)}\partial^{(i)}$ whenever $i < j$).

The standard resolution will give as a general, explicit description of the cohomology groups.

Definition 2.4: Homogenous cochains

Let M be a $\mathbb{Z}[G]$-module. The **homogenous cochains** for G, of degree n, with values in M, denoted $C^n(G, M)$, is the group of set maps

$$f : G^{n+1} \to M$$

satisfying $f(\sigma\sigma_0, \dots, \sigma\sigma_n) = \sigma f(\sigma_0, \dots, \sigma_n)$. The maps

$$d^n : C^n(G, M) \to C^{n+1}(G, M)$$
$$d^n(f) \to g : g(\sigma_0, \dots \sigma_{n+1}) = \sum_{i=0}^{n+1} (-1)^i f(\sigma_0, \dots, \widehat{\sigma}_i, \dots, \sigma_{n+1})$$

define the group of **cocycles** $Z^n(G, M) := \ker d^n$ and the group of **coboundries** $B^n(G, M) := \operatorname{Im} d^{n-1}$.

Lemma 2.2.1. *We have that $H^n(G, M) \simeq Z^n(G, M)/B^n(G, M)$.*

Proof. This is just explicitly computing the cohomology groups using the standard resolution. Let $R = \mathbb{Z}[G]$. An element of $\operatorname{Hom}_R(R^{\otimes n+1}, M)$ is uniquely determined by how it acts on a basis, i.e. the values $f(\sigma_0 \otimes \cdots \otimes \sigma_n), \sigma_i \in G$. Thus, we clearly have $\operatorname{Hom}_R(R^{\otimes n+1}, M) \simeq C^n(G, M)$ (note that the "homogenous" condition comes from the fact that the maps should be R-linear). The induces maps is of course given by precomposing with ∂_n, which in turn coincides with the defintion of d^n, which gives the statement of the lemma. □

There is also an alternate description, that also comes from the standard resultion, but using a change of coordinates. The book does not stick to one choice, but rather uses whatever is most useful, so it seems sensible to define both.

The key difference is that the homogenous cochains uses the basis of $R^{\otimes n+1}$ as a $\mathbb{Z}$-module (given by all the tensors), while the inhomogenous cochains, which we are just about to define, uses the basis as an R-module, given by the following

Lemma 2.2.2. *Let $[\sigma_1 \mid \cdots \mid \sigma_n]$ denote the element $1 \otimes \sigma_1 \otimes \sigma_1\sigma_2 \otimes \cdots \otimes \sigma_1\sigma_2 \dots \sigma_n \in R^{\otimes n+1}$. These elements form a basis of $R^{\otimes n+1}$ as an R-module*

Proof. Trivial. □

This gives the alternate

Definition 2.5: Inhomogenous cochains

Let M be a $\mathbb{Z}[G]$-module. The **inhomogenous cochains** for G, of degree n, with values in M, denoted $\mathcal{C}^n(G, M)$ is simply the group of set maps

$$f : G^n \to M$$

subject to no other restriction. Further, we set $\mathcal{C}^0(G, M) = M$. The boundary maps

$$\begin{aligned} d^0 : \mathcal{C}^0(G, M) &\to \mathcal{C}^n(G, M) \\ d^0(f) \to g : g(\sigma) &= \sigma \cdot m - m \end{aligned}$$

and

$$\begin{aligned} d^n : \mathcal{C}^n(G, M) &\to \mathcal{C}^{n+1}(G, M) \\ d^n(f) \to g : g(\sigma_1, \dots \sigma_{n+1}) =& \sigma_1 \cdot f(\sigma_2, \dots, \sigma_{n+1}) \\ &+ \sum_{i=1}^{i=n} (-1)^i f(\sigma_1, \dots, \sigma_{i-1}, \sigma_i \sigma_{i+1}, \sigma_{i+2}, \dots \sigma_{n+1}) \\ &+ (-1)^{n+1} f(\sigma_1, \dots, \sigma_n) \end{aligned}$$

define the group of **cocycles** $\mathcal{Z}^n(G, M) = \ker(d^n)$ and the group of **coboundries** $\mathcal{B}^n(G, M) = \mathrm{Im}(d^{n-1})$.

Lemma 2.2.3. *We have that* $H^n(G, M) \simeq \mathcal{Z}^n(G, M)/\mathcal{B}^n(G, M)$.

Proof. It is the same as before, except we identify the functions by $f(\sigma_1, \dots, \sigma_n) = f([\sigma_1 \mid \dots \sigma_n])$. The tricky thing is to describe the boundary maps, but it can also be done by direct computation, which follows from the isomorphism

$$\begin{aligned} C^n(G, M) &\to \mathcal{C}^n(G, M) \\ f &\to g : g(\sigma_1, \dots, \sigma_n) = f(1, \sigma_1, \sigma_1\sigma_2, \dots, \sigma_1\sigma_2 \dots \sigma_n) \end{aligned}$$

(which for $n = 0$, becomes $f \to f(1)$), whose inverse is defined by sending g to $f : f(\sigma_0, \dots, \sigma_n) = \sigma_0 \cdot g(\sigma_0^{-1}\sigma_1, \sigma_1^{-1}\sigma_2, \dots, \sigma_{n-1}^{-1}\sigma_n)$. □

The isomorphism given in the "proof" above, is useful for changing between homogenous and inhomogenous cochains.

2.3 Galois cohomology

We defined group cohomology for finite groups. This is easily extended to profinite groups, except we need to be a bit careful. We will only consider the following

Definition 2.6: Discrete G-module

Let G be a profinite group, and let M be a G module. Then, M is a **Discrete G-module** if it satisfies any (and hence all) of the following:

- The map $G \times M \to M$ given by $(\sigma, m) \to \sigma m$ is continuous, when M is given the discrete topology.
- The stabilizer of any $m \in M$ is open in G.
- $M = \cup_{U \subseteq G} M^U$, where U runs over the open subgroups of G.

At this point, we could repeat the definition of (in)homogenous cochains when G is profinite and M is discrete, which only has the additional requirement of being continuous. This gives us the following

Lemma 2.3.1. *Let G be profinite, and M a discrete G-module. Then*

$$H^n(G, M) \simeq \varinjlim_{U \subseteq G} H^n(G/U, M^U)$$

Proof. Consider the map

$$\iota : \varinjlim_{U \subseteq G} C^n(G/U, M^U) \to C^n(G, M)$$

given by combining the obvious maps $C^n(G/U, M^U) \to C^n(G, M^U) \to C^n(G, M)$. It is not too hard to show that ι is an isomorphism, and since the isomorphism is compatible with the boundary operators, the lemma follows. □

This allows us to give the following

Definition 2.7: Galois cohomology

Let F be a field, and let M be a discrete $\mathrm{Gal}(\overline{F}/F)$-module. For any n, the ***n*-th galois cohomology group** of F with coefficients in M is given by

$$H^n(F, M) := H^n(\mathrm{Gal}(\overline{F}/F), M).$$

The main modules we will consider for galois cohomology will be the units $\mathbb{G}_m(\overline{F})$, n-th roots of unity $\mu_n(\overline{F})$, and points on abelian varieties $A(\overline{F})$. By the lemma above, we have

$$H^n(F, A(\overline{F})) = \varinjlim_{E/F} H^n(\mathrm{Gal}(E/F), A(E))$$

and it is typical to just write $H^n(F, A)$ (even though we really mean the points on whatever variety we want).

3 Low degrees

We now study some cohomology groups in low degrees. The first two are examples of how Galois cohomology tells us something about the relevant galois-module, while the last is an example of how group homology in general says something about the group itself.

3.1 Brauer groups

We now define Brauer groups, before quickly seeing that they are really the second cohomology group of the absolute galois group.

Recall the Artin-Wedderburn theorem, which implies that a central, simple F-algebra is isomorphic to $\mathbf{M}_n(K)$ for some n, and some skewfield K, which is finite dimensional over F.

Definition 3.1: Brauer Group

Let F be a field. Two central, simple F-algebras A, B are said to be **brauer equivalent**, when there is a skewfield K, with $Z(K) = F$, such that $A \simeq \mathbf{M}_n(K)$ and $B \simeq \mathbf{M}_m(K)$. The **brauer group** of F, denoted $B(F)$ is the set of all brauer equivalence classes over F, together with the group operation given by the tensor product.

It is not obvious that the above definition makes sense, but I will not bother showing it here. One important point is that inverses are given by the opposite rings, i.e. $[K][K^{\text{op}}] = [K \otimes K^{\text{op}}] = [F]$.

In addition to the basic definition above, we also look at two specific subgroups: For any n, we denote by $B_n(F)$ the n-torsion of $B(F)$. Also, for any field-extension E/F, we can define a map $B(F) \to B(E)$ by $[A] \to [A \otimes_F E]$. The kernel of this map is called the **relative Brauer group**, and is denoted by $B(E/F)$.

We will now build the bridge between Galois cohomology and the Brauer group. In what follows, we will work with **normalized** (inhomogenous) 2-cocycles, which additionally satisfies

$$c(\sigma, 1) = c(1, \tau) = 0, \forall \sigma, \tau \in G$$

and **normalized** 2-coboundries, which are of the form $d^1(f)$, for f satisfying $f(1) = 0$. These normalized cocycles modulo the normalized boundries are also isomorphic to $H^2(G, M)$ (needs proof...).

The bridge is then really provided by the following

Definition 3.2: Crossed product algebra

Let E/F be a finite galois extension, and pick a normalized 2-cocycle $c \in \mathcal{Z}^2(\text{Gal}(E/F), E^\times)$. The **crossed product algebra** A_c is defined as follows.

- As an E-vector space, $A_c \simeq E[G]$, i.e. the basis elements are in bijection with the elements of G. Let a_σ be the basis element associated to $\sigma \in G$.
- The multiplcation is given by c. Namely, define

$$\left(\sum_{\sigma \in G} e_\sigma a_\sigma\right) \cdot \left(\sum_{\tau \in G} e'_\tau a_\tau\right) = \sum_{\sigma, \tau \in G} e_\sigma \sigma(e'_\tau) c(\sigma, \tau) a_{\sigma\tau}$$

This makes A_c into a central, simple F-algebra.

Of course, the above definition requires a lot of argument, as does the following Theorem, but I'm not gonna bother.

Theorem 3.1.1. *There is an isomorphism*

$$H^2(G(E/F), E^\times) \simeq B(E/F)$$

obtained by sending a normalized 2*-cocycle* c *to* $[A_c]$.

Proof. See book (Chapter 7). □

With the functoriality of the cohomology groups, it comes as no surprise that we have

$$B(F) = H^2(\mathrm{Gal}(\overline{F}/F), \overline{F}^\times) = \varinjlim_{E/F} H^2(\mathrm{Gal}(E/F), E^\times) = \varinjlim_{E/F} B(E/F)$$

But various subgroups of the brauer group are also worth studying themselves

Example 3.1.2. *Recall that a quaternion algebra* B *over* F *comes equipped with an involution which satisfies* $\overline{q_1 q_2} = \overline{q}_2 \overline{q}_1$*. Thus, the involution induces an isomorphism* $B \simeq B^{\mathrm{op}}$*. Thus, for any quaternion algebra, we have* $[B]^2 = [B][B^{\mathrm{op}}] = [F]$*, and hence every quaternion algebra defines an element of* $B_2(F)$*.*

Incredibly, a converse of this theorem is also true; Appearently the Merkurjev-Suslin theorem states that $B_2(F)$ *is generated by quaternion algebras over* F*.*

We give the first example of a Brauer group as a famous

Theorem 3.1.3 (Wedderburn)**.** *Let* $\mathbb{F}_q$ *be a finite field. Then* $B(\mathbb{F}_q)$ *is trivial.*

Proof. To prove this, it is clearly enough to prove that $H^2(\mathrm{Gal}(E/\mathbb{F}_q), E^\times)$ is trivial for any finite galois extension $E/\mathbb{F}_q$. Of course, $\mathrm{Gal}(E/\mathbb{F}_q)$ is cyclic, so we are again in the situation of Example 2.1.2, and thus

$$H^2(\mathrm{Gal}(E/\mathbb{F}_q), E^\times) = \mathbb{F}_q / N(E^\times).$$

Let $|E| = q^n$. The norm map is of course given by $N(x) = x^q x^{q^2} \dots x^{q^{n-1}} = x^{\frac{q^n-1}{q-1}}$, and thus (since $E^\times$ is cyclic of order $q^n - 1$), we have $|N(E^\times)| = q - 1$, and thus $N(E^\times) = \mathbb{F}_q^\times$. □

Of course, the above implies the more classical formulation, namely that a finite division-ring is commutative.

So Brauer groups of finite fields are trivial. How about local number fields? In fact, they also have a nice, unified formulation

Theorem 3.1.4. *Let* F *be a local number field. Then* $B(F) = \mathbb{Q}/\mathbb{Z}$*.*

Proof. See book (Chapter 8), though we give a quick recount of the proof here. The first step is to show that for local number fields, the formula

$$B(F) = \varinjlim_{E/F \text{unramified}} H^2(\mathrm{Gal}(E/F), E^\times)$$

holds, i.e. its enough to consider unramified extensions. Basics of local fields (which we cover in Section 7), tells us that unramified extensions are basically as easy as finite field extensions, i.e. one unique extension (once we fix an algebraic closure) of degree n for each positive integer n (see Theorem 7.1.2), denoted E_n. Further, $\mathrm{Gal}(E_n, F) = \mathbb{Z}/n\mathbb{Z}$. Thus we may use our favorite Example 2.1.2. It can be shown that $N(E_n^\times) = \{f \in F \mid n | v(f)\}$, and thus

$$B(E_n/F) = \mathbb{Z}/n\mathbb{Z}.$$

This gives all we need, as famously the colimit of these groups gives $\mathbb{Q}/\mathbb{Z}$. □

These groups are often written as $B(E_n/F) = \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ to emphasize that they are subgroups of $\mathbb{Q}/\mathbb{Z}$. Using the theorem above, we get an easy proof of a fairly fundamental result about quaternion algebras.

Example 3.1.5. *By Example 3.1.2, we know that every quaternion algebra over a local number field F corresponds to an element of $B_2(F)$. But, by the theorem above,*

$$B_2(F) = \frac{1}{2}\mathbb{Z}/\mathbb{Z}.$$

Thus, there are only two quaternion algebras over F. The trivial element we know corresponds to $M_2(F)$, and for dimension reasons, the second must in fact be division (and unique!).

3.2 Hilbert 90

One of the "fundamental" theorems of Galois cohomology, is Hilbert 90. Appearently, the general result is due to Noether so the name is a bit of a misnomer.

In this subsection, be careful that we have largely swapped from additive to multiplicative notation, since our modules will be $E^\times$ for some field E.

Theorem 3.2.1 (Hilbert 90)**.** *Let F be a field. For any finite Galois extension E/F, we have*

$$H^1(\mathrm{Gal}(E/F), E^\times) = 0.$$

Thus, we also have $H^1(F, \mathbb{G}_m) = 0$.

Proof. We work with inhomogenous cochains. Let $G = \mathrm{Gal}(E/F)$. Pick up a 1-cocycle $\varphi : G \to E^\times$. We need to show that this is in fact a coboundry, i.e. $\varphi(\tau) = \tau(a)/a$ for some $a \in E^\times$. Set

$$0 \neq b := \sum_\sigma \varphi(\sigma)\sigma(c)$$

for some $c \in E^\times$ (the fact that such a c exists is a basic lemma on characters by Dedekind). Thus,

$$\begin{aligned}\varphi(\tau)\tau(b) &= \sum_{\sigma\in G} \varphi(\tau)\tau(\varphi(\sigma))\tau(\sigma(c)) \\ &= \sum_{\sigma\in G} \varphi(\tau\sigma)\tau(\sigma(c)) = b,\end{aligned}$$

and we have $\varphi(\tau) = \tau(b^{-1})/b^{-1}$.

□

The actual result proved by Hilbert is interestingly

Corollary 3.2.2. *Let E/F be a finite, cyclic field-extension, whose galois group is generated by σ. Given an element $x \in E$ with $N_{E/F}(x) = 1$, there exists another element $a \in E^\times$, such that $x = \sigma(a)/a$.*

Proof. This is direct from the theorem, since by Example 2.1.2, we have

$$0 = H^1(\mathrm{Gal}(E/F), E^\times) = {}_N E^\times / M',$$

where the last group written out is ${}_N M = \{x \in E^\times \mid N_{E/F}(x) = 1\}$, and $M' = \{\sigma(a)/a \mid \sigma \in \mathrm{Gal}(E/F), a \in E^\times\}$. □

We can thus explicitly describe

Theorem 3.2.3. *Let F be a field and n a natural number, and assume either that F is perfect, or n is prime to the characteristic of F. Then*

$$H^1(F, \mu_n) \simeq F^\times/(F^\times)^n,$$

and

$$H^2(F, \mu_n) \simeq B_n(F).$$

Proof. Start with the exact sequence of discrete $\mathrm{Gal}(\overline{F}, F)$-modules

$$0 \to \mu_n(\overline{F}) \to \overline{F} \xrightarrow{x \to x^n} \overline{F} \to 0$$

From the long exact sequence in Galois cohomology, we get

$$\cdots \to H^0(F, \mathbb{G}_m) \to H^0(F, \mathbb{G}_m) \to H^1(F, \mu_n) \to H^1(F, \mathbb{G}_m) \to \ldots$$

By Hilbert 90, $H^1(F, \mathbb{G}_m) = 0$, while $H^0(F, \mathbb{G}_m) = F^\times$. Thus, the first result follows immidiately. The second follows similarily, from studying the long exact sequence just a bit further ahead:

$$\cdots \to H^1(F, \mathbb{G}_m) \to H^2(F, \mu_n) \to H^2(F, \mathbb{G}_m) \xrightarrow{\tau(x) \to \tau(x)^n} H^2(F, \mathbb{G}_m) \to \ldots$$

Here, the first entry is again 0 by Hilbert 90, and thus we see that $H^2(F, \mu_n)$ is indeed isomorphic to the n-torsion in $H^2(F, \mathbb{G}_m) = B(F)$. □

3.3 The first homology group

Finally, we give a very different flavored example. We have said very little about group homology beyond the definition, and it won't come up much in this note at all, but we will need one simple result in Section 7. This result is either way interesting on its own.

Recall that that the **abelianization** of a group G is defined as $G^{\mathrm{ab}} := G/[G, G]$, where $[G, G]$ denotes the **commutator subgroup**, defined as

$$[G, G] := \langle \{\sigma\tau\sigma^{-1}\tau^{-1} \mid \sigma, \tau \in G\} \rangle.$$

Alternatively, the abelianization (together with the quotient map $g : G \to G^{\mathrm{ab}}$) is the group satisfying the universal property that for any group homomorphism $f : G \to H$, to an abelian group H, there exists a unique homomorphism h such that $f = h \circ g$.

Proposition 3.3.1. *For any finite group G, there is an isomorphism*

$$H_1(G, \mathbb{Z}) \simeq G^{\mathrm{ab}}.$$

Proof. Use the standard resolution. □

4 More cohomological tools

In this section, we will develop more cohomological tools, which will have various uses in the final three sections.

4.1 The inflation-restriction sequence

We begin with what is essentially a warm-up for the next subsection; however, this subsection is really all we will need (in Section 7 and Section 6), and the next is more because it is interesting in its own right.

In the next two subsections, we will be working with a finite group G, and a normal subgroup $H < G$, and as usual M is a G (and hence also an H) module. Note that in this setting, we can also form the natural G/H-module M^H.

Definition 4.1: Inflation and Restriction

The **restriction** is the map in cohomology

$$\mathrm{Res}_{G,H} : H^*(G, M) \to H^*(H, M)$$

induced by the inclusion $H \hookrightarrow G$ (this does not require H to be normal in G).
The **inflation** is the map in cohomology

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

induced by the projection $G \to G/H$, and the inclusion $M^H \hookrightarrow M$.

We will typically drop the subscripts if it is clear from context.

Remark 4.1.1. *One can think of the above definitions in both our definitions of the homology-groups; in terms of (in)homogenous cochains, they are very immidiate as just compositions of functions. But, the other point of view gives some more insight in my opinion, as the restriction and inflation maps are in fact extremely general: any ring homomorphism $\varphi : A \to B$ induces an exact functor Res_φ from B-modules to A-modules (by restricting the scalars to $\varphi(A)$), and this gives corresponding map of ext groups. For the inflation map, I didn't check the details, but I believe it comes from the functor from A-modules to B-modules given by $G(M) = \mathrm{Hom}_A(B, M)$ (with the B-module structure given by $b \cdot f(b') = f(b'b)$. This functor should be right-adjoint to Res_φ, i.e.*

$$\mathrm{Hom}_A(U, G(M)) \simeq \mathrm{Hom}_B(\mathrm{Res}_\varphi(U), M),$$

where the isomorphism is given by sending $f : U \to \mathrm{Hom}_A(B, M)$ to $g(u) := f(u)(1_B)$.

Now by general abstract nonsense, since G is right-exact, this should thus induces canonical isomorphisms

$$\mathrm{Inf}_\varphi : \mathrm{Ext}^*_A(U, G(M)) \to \mathrm{Ext}^*_A(\mathrm{Res}_\varphi(U), M)$$

This stuff at least seems to correctly generalize Definition 4.1, using A and B as the relevant group rings, and $U = \mathbb{Z}$ with a trivial module structure.

Proposition 4.1.2. *There is an exact sequence*

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

Proof. The composition $H \hookrightarrow G \to G/H$ is obviously the trivial map, thus so is $\mathrm{Res} \circ \mathrm{inf}$. Thus, if we first first prove injectivity of Inf, and then exactness in $H^1(G, M)$, we are done.

Working with inhomogenous cochains, assume that $g(\sigma) = \sigma(m) - m$ for some $m \in M$ (i.e. g is trivial), and that g is the image of some f in $H^1(G/H, M^H)$. Since $f(1) = 0$ (this is obvious, since

f is a cocycle), we must have $g(h) = 0$ for all $h \in H$. But this shows that $m \in M^H$, and thus f was already a coboundary.

Next, we must prove exactness in $H^1(G, M)$. Assume now that f restricts to a trivial class, i.e. $f(h) = h(m) - m$ for all $m \in M$ and $h \in H$. We are free to replace f with $g := f - f'$, where f' is the coboundary defined by $f'(\sigma) = \sigma(m) - m$ (since they differ by a coboundary, they represent the same class in $H^1(G, M)$). We can show that g is really the inflation of an element in $H^1(G/H, M^H)$. First, $g(h) = 0$ for all $h \in H$; this is clear since f and f' agree on H by definition. Thus, g is really a G/H-cochain. Second, we must show that $g(\sigma) \in M^H \subset M$ for all $\sigma \in G$. To see this, recall that g is a crossed homomorphism, i.e. satisfying

$$g(\tau\sigma) = g(\tau) + \tau g(\sigma).$$

Thus, $h \cdot g(\sigma) = g(h\sigma) - g(h) = g(h\sigma) = g(\sigma)$, where the last equality comes from the fact that g is constant on cosets of H (i.e. well defined as a function with domain G/H), which we already proved. □

Remark 4.1.3. *Again, I didn't bother checking, but I believe the same sequence should hold for any ring-homomorphism φ, using the generalities discussed in Remark 4.1.1.*

4.2 Five term exact sequence

In this section, we state how to develop a few more terms, continuing the sequence from Proposition 4.1.2. This will not be used further in the note, but its really cool.

Definition 4.2: Transgression

The **transgression** is defined as the morphism

$$\begin{aligned} \mathrm{tr} : H^1(H, M)^{G/H} &\to H^2(G/H, M^H) \\ [c] &\to d^1(f) \end{aligned}$$

where d^1 is the usual boundary map, and f is defined as follows: Let T be a transversal set for the right cosets of H, i.e. $G = \sqcup_{t \in T} tH$ (so every element of G can be written as th for $t \in T$ and $h \in H$ in a unique way). Then f is defined as

$$f(th) = m_t + t \cdot c(h),$$

where $m_t \in M$ is defined as follows: as an inhomogenous cochain, c is simply a function $c : H \to M$. The fact that it is fixed by G/H means that for any $\sigma \in G$, we have $\sigma_*([c]) = [c]$, where $\sigma_*([c])$ is represented by the cochain $h \to \sigma \cdot c(\sigma^{-1}h\sigma)$. Thus, for all $\sigma \in G$, there exists an element $m_\sigma \in M$ such that

$$\sigma \cdot c(\sigma^{-1}h\sigma) - c(h) = \sigma(m_\sigma) - m_\sigma$$

(since they differ by a coboundary); this is the definition of m_t.

The definition of the transgression is certainly remarkably convoluted! Of course, proving that the transgression is even well defined, and independent of all the choices would probably take up another couple of pages, so I'm not gonna bother doing that.

Now the previous subsection was could have been called the "inflation-restriction" sequence, since it used all we want from it, but that name is usually meant to refer to the following, longer sequence

Proposition 4.2.1 (The inflation-restriction sequence)**.** *There is an exact sequence*

$$0 \to H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(H, M)^{G/H} \xrightarrow{\text{tr}} H^2(G/H, M^H) \xrightarrow{\text{Inf}} H^2(G, M)$$

Proof. No thank you. I don't really want to touch this transgression thing, but we can at least prove that the image of Res naturally lies in $H^1(H, M)^{G/H}$ (we did not include this in Proposition 4.1.2):

Assume f is in the image of Res, i.e. f is really a crossed homomorphism for all of G, i.e.

$$f(\tau\sigma) = f(\tau) + \tau f(\sigma)$$

We need to show that for all $h \in H$, there exists an $m \in M$ such that $\sigma \cdot f(\sigma^{-1}h\sigma) - f(h) = h(m) - m$. Using that f is a crossed homomorphism for all of G, we expand the first term as

$$\sigma \cdot (f(\sigma^{-1}) + \sigma^{-1}f(h\sigma)) = \sigma f(\sigma^{-1}) + f(h\sigma) = \sigma f(\sigma^{-1}) + f(h) + hf(\sigma)$$

But $\sigma f(\sigma^{-1}) = f(1) - f(\sigma)$, and thus we get

$$\sigma \cdot f(\sigma^{-1}h\sigma) - f(h) = f(1) - f(\sigma) + f(h) + h(f(\sigma)) - f(h) = h(f(\sigma)) - f(\sigma),$$

which is what we wanted for $m = f(\sigma)$. □

Remark 4.2.2. *To what extent does the above stuff generalize, for instance in light of Remark 4.1.1? It turns out, incredibly well appearently! According to wikipedia, the inflation-restriction sequence is a special case of the five-term exact sequence, which in term is comes from spectral sequences! Now, I know absolutely nothing about spectral sequences, but maybe this is sufficient motivation to finally learn about them. I want to comment though, that I guess the extremely wicked definition of the transgression probably has a much more natural definition in the five-term exact sequence, similar to how the usual connecting homomorphism is quite natural, even if it seems very convoluted/ad-hoc when you actually unravel the definition in special cases.*

4.3 The cup product

We now define what is going to give us all our pairings:

Definition 4.3: Cup product

Let G be a (pro)finite group, and let M_1, M_2 be (discrete) G-modules. The **cup product** is the operation

$$H^n(G, M_1) \times H^m(G, M_2) \to H^{n+m}(G, M_1 \otimes M_2)$$
$$(x_1, x_2) = x_1 \smile x_2$$

defined (on homogenous cochains) by

$$f_1 \smile f_2(\sigma_1, \dots \sigma_{n+m}) = f_1(\sigma_0, \dots, \sigma_n) \otimes f_2(\sigma_n, \dots \sigma_{n+m})$$

It is not obvious, but straight forward to prove that the above definition makes sense: It follows from the formula, when $f_1 \in C^n(G, M_1), f_2 \in C^m(G, M_2)$

$$d(f_1 \smile f_2) = d(f_1) \smile f_2 + (-1)^n f_1 \smile d(f_2)$$

which can lead to showing that cocycles are sent to cocycles, and that the choice is irrelevant up to coboundries. Note that, what is obvious is that the cup product distributes over the group law, so the cup product is bilinear, thus $x_1 \smile -$ and $- \smile x_2$ are both group homomorphisms.

The cup product operation turns out to be a very "nice" operation, that satisfies many of properties you want. Before we state these properties, note that the definition above is a bit rigid, and that we often use a looser definition, combining the modules with a suitable pairing: Assume that we have a pairing $M_1 \times M_2 \to M_3$. This of course defines a homomorphism $M_1 \otimes M_2 \to M_3$ which, if this is a homomorphism of $\mathbb{Z}[G]$-modules, also defines a homomorphism $H^\star(G, M_1 \otimes M_2) \to H^\star(G, M_3)$. It is usual to call the full composition

$$H^n(G, M_1) \times H^m(G, M_2) \to H^{n+m}(G, M_1 \otimes M_2) \to H^{n+m}(G, M_3)$$

a cup product.

Theorem 4.3.1. *The cup product satisfies:*

Compatibility with connecting homomorphisms *Assume we are given two exact sequences*

$$0 \to M_1' \to M_1 \to M_1'' \to 0$$

and

$$0 \to M_3' \to M_3 \to M_3'' \to 0$$

and a module M_2 such that there exists a pairing $M_1 \otimes M_2 \to M_3$ which also induces pairings $M_1' \otimes M_2 \to M_3'$ and $M_1'' \otimes M_2 \to M_3$. Then, for any $x_1 \in H^n(G, M'')$ and $x_2 \in H^m(G, M_2)$, we have that

$$\delta(x_1 \smile x_2) = \delta(x_1) \smile x_2$$

where the δ refer to the connecting homomorphisms of the second and first exact sequence. If instead the pairings are induced by $M_2 \otimes M_1 \to M_3$, then we instead have

$$(-1)^m \delta(x_2 \smile x_1) = x_2 \smile \delta(x_1)$$

Compatibility with homomorphisms of groups and modules *Given maps $h_1 : M_1 \to M_1'$ and $h_2 : M_2 \to M_2$, then for any $x_1 \in H^n(G, M_1), x_2 \in H^m(G, M_2)$, we have*

$$(h_1 \otimes h_2)_*(x_1 \cup x_2) = (h_1)_*(x_1) \cup (h_2)_*(x_2) \in H^{n+m}(G, M_1' \otimes M_2').$$

Similarily, given a map $\varphi : H \to G$, then for any $x_1 \in H^n(G, M_1), x_2 \in H^m(G, M_2)$, we have

$$(\varphi^*)(x_1 \smile x_2) = (\varphi^*)(x_1) \smile (\varphi^*)(x_2) \in H^{n+m}(H, M_1 \otimes M_2).$$

Associativity *For any tuple that makes sense, we have*

$$(x_1 \smile x_2) \smile x_3 = x_1 \smile (x_2 \smile x_3)$$

Graded commutativity *For any $x_1 \in H^n(G, M_1), x_2 \in H^m(G, M_2)$, we have*

$$x_1 \smile x_2 = (-1)^{nm}(\mathrm{sw}_*)(x_1 \smile x_2)$$

where $\mathrm{sw} : M_1 \otimes M_2 \to M_2 \otimes M_1$ *is the map given by swapping the coordinates.*

Proof. I can't be bothered, maybe in the future. □

Example 4.3.2. *Let $G = C_2$ be the group with 2 elements. Again by Example 2.1.2, we have that*

$$H^n(G, \mathbb{F}_2) = \mathbb{F}_2$$

(as groups) for all n. Using the cup product, we can turn $H^\star(G, \mathbb{F}_2) := \bigoplus_{n\geq 0} H^n(G, \mathbb{F}_2)$ into a graded commutative ring. Indeed, let $t \in H^1(G, \mathbb{F}_2)$ (as an inhomogenous cochain) be the identity map. Then, one can in fact show (using something called the "Arason exact sequence" that

$$H^*(G, \mathbb{F}_2) \simeq \mathbb{F}_2[t]$$

the polynomial ring in one variable.

A seriously wild generalization of this example is the conjectures by Milnor, generalized by Bloch and Kato. The proof now asserts the structure of $H^*(F, \mathbb{F}_p)$ exactly, as follows: Assume F is a field containing a p-th root of unity. Let A be the ring of (noncommutative, if $p > 2$) polynomials in the variables $\ell(a)$, where a spans over the elements of F. Let I be the ideal generated by the elements of the form $\ell(ab) - \ell(a) - \ell(b)$ for $a, b \in F^\times$, and $\ell(a)\ell(a-1)$ for $a \in F^\times \setminus \{1\}$. Then

$$H^*(F, \mathbb{F}_p) = A/I.$$

There also exists a (more complicated to state) version using μ_p when $\mu_p(F) \neq \mu_p(\overline{F})$.

4.4 Results for local class field theory

The "proof" we give in this subsection are very rough sketches, as we have not covered most of the theory needed. Maybe in the future. They are only gathered here for the application in Section 7.

One of the most important results, which together with "dimension shifting", gives the result we are after, is the following

Theorem 4.4.1 (Nakayama-Tate)**.** *Let G be a (pro)finite group, and M a G-module. If there exists an integer $r \in \mathbb{Z}$ such that*

$$\widehat{H}^r(S, M) = \widehat{S}^{r+1}(S, M) = 0$$

for all subgroups $S < G$, then we also have $\widehat{H}^n(S, M) = 0$ for any $n \in \mathbb{Z}$.

Proof. One starts by proving that if $\widehat{H}^0(S, M) = \widehat{H}^1(S, M) = 0$ for all $S < G$, then we also have $\widehat{H}^2(S, M) = 0$, and similarily, that triviality in the first and second Tate cohomology groups implies triviality in the zero-eth cohomology group. Then, one shows that for Tate-cohomology, there is a possible "dimension-shifting" procedure: Namely for any $r \in \mathbb{Z}$, there exists a G-module $M(-r)$, such that

$$\widehat{H}^n(S, M(-r)) = \widehat{H}^{n+r}(S, M)$$

for all $n \in \mathbb{Z}$ and $S < G$. The result now follows by induction. □

A G-module M with the property in the theorem above is called **cohomologically trivial**.

The following definition seems like a very strong group-cohomolical version of a quasi-isomorphism. Note that, unlike quasi-isomorphisms, it is of course specific to group cohomology.

Definition 4.4: Cohomological equivalence

A **cohomological equivalence** is a morphism $f : M \to N$ of G-modules, such that

$$f_{*,S} : \widehat{H}^*(S, M) \to \widehat{H}^*(S, N)$$

is an isomorphism for all $S < G$.

We will for the main theorem use the following cohomological equivalence:

Lemma 4.4.2. *Let G be a finite group, and M a G-module, such that for any subgroup $S < G$ of order n, we have*

$$\widehat{H}^0(S, M) = \mathbb{Z}/n\mathbb{Z}$$

and

$$\widehat{H}^{-1}(S, M) = 0.$$

Then, for any $m \in M^G$ mapping to a generator of $\widehat{H}^0(S, M) := M^G/N(M)$, the homomorphism of G-modules defined by

$$f : \mathbb{Z} \to M$$
$$f(1) = m$$

is a cohomological equivalence.

Proof. Can't be bothered. □

Finally, the results in this section piece together to

Theorem 4.4.3 (Tate (again!))**.** *Let G be a finite group, and M a G-module, such that for any subgroup $S < G$ of order n, we have*

$$H^2(S, M) = \mathbb{Z}/n\mathbb{Z}$$

and

$$H^1(S, M) = 0.$$

Then, for any $r \in \mathbb{Z}$, we have that $H^{r-2}(S, \mathbb{Z}) \simeq H^r(S, M)$.

Proof. Dimension shifting gives a module $M(-2)$ such the previous Proposition applies, and gives

$$\widehat{H}^{r-2}(S, \mathbb{Z}) \simeq \widehat{H}^{r-2}(S, M(-2)) = \widehat{H}^r(S, M).$$

□

5 Cohomological pairings

There is in fact a pletora of pairings on abelian varieties that arises from cohomology theories that are worth studying.

5.1 The Hilbert symbol

We start with a pairing, not on abelian varieties, but which is certainly also worth studying (and probably the by far oldest/most classical example?)

Definition 5.1: Hilbert symbol

Let F be a field containing an n-th rooth of unity. The ***n*-th Hilbert symbol** is the bilinear map

$$\begin{aligned} F^\times/(F^\times)^n \times F^\times/(F^\times)^n &\to H^2(F,\mu_n) \\ (a,b) &\to [a] \smile [b] \end{aligned}$$

where $[a] \in H^1(F,\mu_n)$ is the element under a fixed isomorphism

$$F^\times/(F^\times)^n \simeq H^1(F,\mu_n).$$

Of course, the isomorphism mentioned above comes from Theorem 3.2.3. The target group $H^2(F,\mu_n)$ is also one we recognize as the n-torsion of the Brauer group!

The original formulation of the Hilbert symbol was only for $n = 2$, and is as follows:

$$\begin{aligned} F^\times \times F^\times &\to \{\pm 1\} \\ (a,b) &= \begin{cases} 1 & \text{if } b \text{ is a norm from } F(\sqrt{a}) \\ -1 & \text{otherwise} \end{cases} \end{aligned}$$

The norm thing can be reformulated as saying the equation $ax^2 + by^2 = 1$ has a solution with $x, y \in F$. The fact that the cohomological interpretation actually coincides with this definition is not entirely obvious. Still, I am gonna assume that this is equivalent from now on.

Our favorite example of applications of the Hilbert symbol is computing the ramification of different quaternion algebras. The following example assumes some knowledge of quaternion algebras.

Example 5.1.1. *Let $B = \mathbb{Q} + \mathbb{Q}\mathbf{i} + \mathbb{Q}\mathbf{j} + \mathbb{Q}\mathbf{k}$ be the quaternion algebra defined by*

$$\mathbf{i}^2 = a, \mathbf{j}^2 = b.$$

As covered in Example 3.1.5, there are only two quaternion algebras over $\mathbb{Q}_p$ for various places p (we only showed it for finite primes, but the case of $B(\mathbb{R})$ is even easier).

We say that B is ramified at p if $B \otimes_{\mathbb{Q}} \mathbb{Q}_p \neq \mathbf{M}_2(\mathbb{Q}_p)$, i.e. $B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ does not correspond to the trivial element of $B(\mathbb{Q}_p)$. The claim now is that this ramification can simply be reformulated as B is ramified at p if $(a,b)_2 \in H^2(\mathbb{Q}_p,\mathbb{Z})$ is not trivial. I am going to do neither, but there are (at least) two ways to prove this: For a direct proof, prove that the condition $ax^2 + by^2 = 1$ has a solution if and only if $B \simeq M_2(\mathbb{Q}_p)$ (see Voight, Theorem 5.4.4). But more in the spirit of this note, is to prove that the crossed product algebra of the cocycle $(a,b)_2$ is actually isomorphic to $B \otimes_{\mathbb{Q}} \mathbb{Q}_p$.

5.2 The Weil pairing

Now we get to some famous pairings on Abelian varieties. Naturally this, and the next section rely on basic knowledge of these objects (though we really only need the basics!). We start with the Weil pairing, even though it does NOT rely on Galois cohomology! However, the Weil pairing

is probably the simplest example, and more importantly, it will be necessary to define the other pairings (in terms of cup-products this is actually not so surprising, as recall that can use a pairing $M_1 \otimes M_2 \to M_3$ to land in a nicer target group!).

To construct this, we start with the Kummer sequence (used in the proof of Theorem 3.2.3), but this time for an abelian variety A/F, where F is any field. From

$$0 \to A[m] \to A \xrightarrow{[m]\cdot -} A \to 0$$

we apply the hom functor $\mathrm{Hom}(-, \mathbb{G}_m)$, to get a long exact sequence in cohomology

$$\cdots \to \mathrm{Hom}(A, \mathbb{G}_m) \to \mathrm{Hom}(A[m], \mathbb{G}_m) \to \mathrm{Ext}^1(A, \mathbb{G}_m) \to \mathrm{Ext}^1(A, \mathbb{G}_m) \to \dots$$

Now, A is complete, while $\mathbb{G}_m$ is affine, so $\mathrm{Hom}(A, \mathbb{G}_m) = 0$. Further we have that map $A[m] \to \mathbb{G}_m$ must clearly have image in μ_m. Finally, for the last group we simply define the dual abelian variety as $\widehat{A} = \mathrm{Ext}^1(A, \mathbb{G}_m)$. This is not the typical definition, but showing the equivalence with the usual definition, we save for a later note.

Thus we get

$$0 \to \mathrm{Hom}(A, \mu_m) \to \widehat{A} \xrightarrow{[m]\cdot -} \widehat{A}$$

which means we get an immidiate isomorphism $\widehat{A}[m] \simeq \mathrm{Hom}(A, \mu_m)$. Thus we can make the

Definition 5.2: Weil pairing

Let A be an abelian variety. The ***m*-Weil pairing** is defined as the pairing

$$\begin{aligned} e_{W,m} : A[m] \times \widehat{A}[m] &\to \mu_m \\ e_{W,m}(P, Q) &= \varphi_Q(P) \end{aligned}$$

where φ_Q is the element of $\mathrm{Hom}(A, \mu_m)$ under the isomorphism $\widehat{A}[m] \simeq \mathrm{Hom}(A, \mu_m)$.

In what follows, we will interchangably consider the weil pairing as a map

$$A[m] \otimes \widehat{A}[m] \to \mu_m$$

which of course exists by the universal property of the tensor product.

5.3 The (local) Tate pairing

Next, we define the Tate pairing (on local fields!). Note that this is not what is typically called the "Tate pairing" in cryptography, which is really the "Lichtenbaum-Tate pairing" we cover in the next section.

The Tate pairing is actually extremely similar to the Hilbert symbol (in fact, I think formulated in sufficient generality, the Hilbert symbol can actually be seen as a special case of the Tate pairing), but we need to be a bit careful. Starting again from the kummer sequence for the abelian variety A/F

$$0 \to A[m] \to A \xrightarrow{m\cdot -} A \to 0$$

we apply Galois cohomology, and we get the sequence

$$\dots H^0(F,A) \to H^0(F,A) \to H^1(F,A[m]) \to H^1(F,A) \to H^1(F,A) \to \dots$$

Now, recall that $H^0(F,A)$ are the fixed points of A under the action of galois, i.e. $A(F)$. Thus we get at an exact sequence

$$0 \to A(F)/mA(F) \to H^1(F,A[m]) \to H^1(F,A)[m] \to 0 \tag{1}$$

by the usual short-exact from long-exact sequence concept.

Now, mimicing the construction of the Hilbert symbol, we can associate an element of $A(F)/mA(F)$ with $H^1(F,A[m])$. Note that this map was an isomorphism before, but that is no longer true. Now, trying to make the same definition as before with the cup product would land us in $H^2(F,A[m]\otimes A[m])$, which might not be so useful. However, if we now assume that F is a local field, we can use the Weil pairing to land us in a Brauer group we actually know, if we repeat the above process with the dual of A too!

Doing this, the cup product together with the Weil pairing defines a new pairing

$$\begin{aligned} H^1(F,A[m]) \times H^1(F,\widehat{A}[m]) \to H^2(F,\mu_m) &= \frac{1}{m}\mathbb{Z}/\mathbb{Z} \\ (\sigma,\eta) &\to e_{W,m}(\sigma \smile \eta) \end{aligned}$$

Similarily for the Hilbert symbol, we use the injection $A(F)/mA(F) \hookrightarrow H^1(F,A[m])$ in place of the first coordinate. However, this is no longer an isomorphism, and doing this for the dual as well is a bad idea, because it turns out that the image is always trivial! Although we omit the proof, of this one can even show that $\widehat{A}(F)/m\widehat{A}(F)$ is precicely the annihilator of the image of $A(F)/mA(F)$, thus it makes sense to use a lift of $H^1(F,A)[m]$ to get a non-degenerate pairing, as in the following

Definition 5.3: Tate pairing (for local fields)

Let F be a local field, and let A be an abelian variety. The ***m*-Tate pairing** is defined as the pairing

$$\begin{aligned} e_{T,m} : A(F)/mA(F) \times H^1(F,\widehat{A})[m] &\to \frac{1}{m}\mathbb{Z}/\mathbb{Z} \\ e_{T,m}(P,\sigma) &= e_{W,m}(\varphi_P \smile \sigma') \end{aligned}$$

where again φ_P is the image of P under $A(F)/mA(F) \hookrightarrow H^1(F,A[m])$, and σ' is a lift of σ in the exact sequence 1.

5.4 The Lichtenbaum-Tate pairing

Of course, copying the construction of the Tate pairing to a finite field would be mute; Wedderburn's little theorem (see Theorem 3.1.3) shows that this would be trivial, as the target group is trivial! However, just a little bit of adaption will be enough. The construction works over any field; over finite fields it is extremely useful in cryptography, and over number fields, it is very useful for computing the weak Mordell-Weil group (see Section 6).

The idea will be simple: We want to land in the target group $H^1(F,\mu_m)$ instead, as then we have $H^1(F,\mu_m) \simeq F^\times/(F^m)^\times$ by theorem 3.2.3. To do this, simply replace $H^1(F,\widehat{A}[m])$ by $H^0(F,\widehat{A}[m])$. This gives us a perfectly valid pairing

$$H^1(F, A[m]) \times H^0(F, \widehat{A}[m]) \to H^1(F, \mu_m) = F^\times/(F^m)^\times$$
$$(\sigma, P) \to e_{W,m}(\sigma \smile P)$$

Thats pretty much it! As before, we use the injection $A(F)/mA(F) \hookrightarrow H^1(F, A[m])$ to give the following

Definition 5.4: Lichtenbaum-Tate Pairing

Let A/F be an abelian variety. The ***m*-Lichtembaum-Tate pairing** is defined as the pairing

$$e_{LT,m} : A(F)/mA(F) \times \widehat{A}[m](F) \to F^\times/(F^m)^\times$$
$$e_{T,m}(P, Q) = e_{W,m}(\varphi_P \smile Q)$$

where again φ_P is the image of P under $A(F)/mA(F) \hookrightarrow H^1(F, A[m])$, and we recognize $\widehat{A}[m](F) = H^0(F, \widehat{A}[m])$.

In cryptography, we are often in certain special cases. Since $F = \mathbb{F}_q$ will be a finite field, and assuming $\mu_m(\overline{\mathbb{F}}_q) \subseteq \mathbb{F}_q$, we have $\mathbb{F}_q^\times/(\mathbb{F}_q^m)^\times \simeq \mu_m$, where the isomorphism is given by raising to $\frac{q-1}{m}$ (since $\mathbb{F}_q$ is cyclic). Usually A will be an elliptic curve, or we will be working with a principal polarization, and both these cases give access to an isomorphism $\widehat{A} \simeq A$, thus the Lichtenbaum-Tate pairing is often stated as

$$A(F)/[m]A(F) \times A[m](F) \to \mu_m$$

which we get by composing with the relevant isomorphisms.

6 Bonus 1: Selmer groups

Talking about galois-cohomological groups related to abelian varieties, it would be a shame not to mention the famous Selmer groups, named after Norwegian cryptographer and number theorist Ernst Selmer. By a (long) stretch of the imagination, this guy could probably be called the first elliptic curve cryptographer, as he worked on both elliptic curves and cryptography long before ECC was a thing (though he never combined them of course, as public-key crypto was not invented yet when he worked on cryptography...).

6.1 The Selmer curve

Famously, by the Hasse Minkowski theorem, any quadratic equation has a solution over $\mathbb{Q}$ if and only if it has so at all places (equivalently, a quadratic form over $\mathbb{Q}$ represents 0 if and only if it does so over at all places).

The Selmer curve is a famous example[1], showing that this result *cannot* be extended to cubic curves.

[1] In fact, Selmer studied a whole family of these examples in [4] building on work by Cassels, with the one given being the simplest example violating the Hasse principle.

Theorem 6.1.1 (Selmer's curve)**.** *Consider the projective curve*

$$C/\mathbb{Q} : 3X^3 + 4Y^3 + 5Z^3 = 0.$$

We have that $\#C(\mathbb{Q}) = 0$*, but* $\#C(\mathbb{R}) > 0$*, and* $\#C(\mathbb{Q}_p) > 0$ *for all primes* p*.*

Proof. A nice and "elementary" proof (i.e. only using basic algebraic number theory) is given by Conrad in an online note [1]. □

We now turn to the goal of computing the weak mordell-Weil group $A(K)/[m]A(K)$ for an abelian variety A defined over a number field K. We shall see that the main difficulty in computing this group is precicely the general phenomenon underlying Theorem 6.1.1.

6.2 Principal homogenoous spaces (torsors)

We now make a small pit-stop, defining principal homogenous spaces, and seeing that they give a geometric interpretation of the first cohomology group $H^1(\mathrm{Gal}(\overline{K}/K), A)$ (we will denote our general fields by K in this section, as we will soon focus entirely on (global) number fields which are almost always denoted by K for some reason...), which will be used in the motivation of the definition of the Selmer group and the Tate-Shafarevich group.

Definition 6.1: Principal homogenous space

Let A/K be an abelian variety. A **homogenous space** of A over K is a variety X/K, together with a transitive action

$$X \times A \to X$$

defined over K. A homogenous space is **principal** if the action is also free. Another name for principal homogenous spaces of A over K is K-torsors.

In a later note, I hope to study torsors in much greater detail.

Proposition 6.2.1. *Let* A/K *be an abelian variety, and let* X/K *be a principal homogenous space of* A *over* K*. For any point* $p_0 \in X$*, the map*

$$\begin{aligned} \theta : A &\to X \\ \theta(P) &= p_0 + P \end{aligned}$$

(where the $+$ *denotes the action of* A *on* X*) is an isomorphism defined over* $K(p_0)$*.*

Proof. The action is free, transitive, and defined over K. □

Two notes before we can give the final theorem: First, given two principal homogenous spaces X, X' of A over K, they are said to be equivalent if there exists an isomorphism $X \to X'$ that is defined over K, and compatible with the action of A. Second, for points $x, y \in X$, we can use the notation $y - x$ to refer to the point $P \in A$ such that $y = x + P$, since the action is free and transitive.

Finally, the promised connection with the first cohomology group:

Theorem 6.2.2. *Let* A/K *be an abelian variety. The is a bijection between principal homogenous spaces of* A *over* K*, and* $H^1(\mathrm{Gal}(\overline{K}/K), A)$*, sending a space* X *to the cocycle* $\sigma \to \sigma(p_0) - p_0$ *for any point* $p_0 \in X$*.*

Further, X *represents the trivial class if and only if it has a rational point* $p_0 \in X(K)$*.*

Proof. Checking that the map is well defined consists of checking that the image is a cocycle (this is almost immidiate), and that it is independent of choice of principal homogenous space, and point. Proving injectivity is also routine, but proving surjectivity uses the connection with twists that we haven't covered. See [6, Theorem X.3.6] for details (at least when A is an elliptic curve).

For the second statement, note that it is clear that X represents the trivial class if it has a rational point (the cocycle is then the trivial map). Conversely, if X is trivial, then there is an isomorphism $\psi : A \to X$ (as principal homogenous spaces of A over K), and X has the rational point $\psi(0_A)$. □

6.3 Selmer and Tate-Shafarevich.

The motivation here lies in computing the weak Mordell-Weil group $A(K)/[m]A(K)$ for a global field K. It turns out that the Selmer group is the best current way of achieving this (though, the algorithm is not proven to terminate, as it relies on Conjecture 6.3.5). This subsection is a short summary of the main definitions and results from [6, Chapter X] (we use general abelian varieties, but nothing really changes, see the notes by Poonen [3], which were also very helpful).

Our starting point is again the Kummer sequence of an abelian variety A/K, where K is a global field. In general, one starts with any isogeny, but for notational simplicity, we start with $[m]$, and look at

$$0 \to A[m] \to A \xrightarrow{[m]} A \to 0$$

Applying group cohomology, and zooming in on the first connecting homomorphism, we (as before) get the exact sequence

$$0 \to A(K)/[m]A(K) \to H^1(G_K, A[m]) \to H^1(G_K, A)[m] \to 0$$

where $G_K = \mathrm{Gal}(\overline{K}/K)$. The connection between the previous subsection becomes clear: The last term can be identified with the m-torsion in a group where the elements can be represented by principal homogenous spaces (in Silverman, there is an exercise to show how to compute the group operation in terms of the torsors C/K directly, but I'm not sure this generalizes to higher dimension). This also provides the motivation: by the exactness, computing $A(K)/[m]A(K)$ is the same as computing the kernel of the second map. The group $H^1(G_K, A[m])$ is definitely computable, and thus, by Theorem 6.2.2, the problem of determining its kernel becomes the problem of deciding if some variety (the corresponding torsor $X/K \in H^1(G_K, A)$) has a rational point. This is of course an impossible question to answer in full generality, and even typically the problem in practice, thus we need something more.

We now consider a place ν of K. Letting $G_\nu = \mathrm{Gal}(\overline{K}_\nu/K_\nu)$, we have a natural inclusion $G_\nu \subset G_K$ given by $\sigma \to \sigma\,|_{\overline{K}}$ (the image here is exactly the absolute decomposition group), as well as maps $A(\overline{K}) \subset A(\overline{K}_\nu)$, thus we get restriction maps as in Definition 4.1

$$\mathrm{Res}_\nu : H^*(G_K, A) \to H^*(G_\nu, A).$$

These are compatible with cohomology. Taking the product of these maps for *all* places of K, we get the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A(K)/[m]A(K) & \longrightarrow & H^1(G_K, A[m]) & \xrightarrow{\gamma} & H^1(G_K, A)[m] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \\
0 & \longrightarrow & \prod_\nu A(K_\nu)/[m]A(K_\nu) & \longrightarrow & \prod_\nu H^1(G_\nu, A[m]) & \xrightarrow{\overline{\gamma}} & \prod_\nu H^1(G_\nu, A)[m] & \longrightarrow & 0
\end{array}$$

As said, we are after $\ker \gamma$, where

$$\gamma : H^1(G_K, A[m]) \to H^1(G_K, A)[m].$$

Composing with the right-most restriction, and using the commutativity of the diagram, we can at least get some information on this kernel by considering $\rho := \text{Res} \circ \gamma = \overline{\gamma} \circ \text{Res}$, and looking at $\ker \rho$ instead, which is significantly easer (in the Principal homogenous space view, we are now asked whether a torsor X has a K_ν-rational point for a local field K_ν!). Of course, this kernel might be bigger (see Example 6.3.4), which motivates the following

Definition 6.2: Selmer and Sha

Let $m \in \mathbb{Z}$, and let A/K be an abelian variety defined over a number field K. The ***m*-Selmer group** of A/K is

$$\text{Sel}^m(A/K) := \ker\left(H^1(G_K, A[m]) \xrightarrow{\rho} \prod_\nu H^1(G_\nu, A)[m] \right).$$

The **Tate-Shafarevich** group is

$$Ш(K, A) := \ker\left(H^1(G_K, A) \xrightarrow{\text{Res}} \prod_\nu H^1(G_\nu, A) \right)$$

Remark 6.3.1. *The fact that $Ш(K, A)$ is the kernel of the product restriction maps, makes me wonder about the connection to the five-term exact sequence in Proposition 4.2.1. Seems like $Ш(K, A)$ can be interpreted as the intersection of all the corresponding inflation maps, but what do the other things (like the transgression) tell us? Hmmm, anyway...*

From these definitions, one immidiately gets

Proposition 6.3.2. *There is an exact sequence*

$$0 \to A(K)/[m]A(K) \to \text{Sel}^m(A/K) \to Ш(A/K)[m] \to 0$$

Proof. Immidiate from the definition, or if you prefer massive sledge-hammers, it is the top row of the Snake lemma applied to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)/[m]A(K) & \longrightarrow & H^1(G_K, A[m]) & \xrightarrow{\gamma} & H^1(G_K, A)[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \text{Res}} & & \\ 0 & \longrightarrow & 0 & \longrightarrow & \prod_\nu H^1(G_\nu, A)[m] & \xrightarrow{\text{id}} & \prod_\nu H^1(G_\nu, A)[m] & \longrightarrow & 0 \end{array}$$

□

Now a big result about the Selmer group, and why it is so nice is

Theorem 6.3.3. *For any $m \in \mathbb{Z}$, $\text{Sel}^m(A/K)$ is finite.*

Proof. See [6, Theorem 4.2] for elliptic curves. □

Notice that the above result implies the weak Mordell-Weil theorem. Further, whenever $Ш(K,A)[m]$ is trivial, we get a very nice way of computing the weak Mordell-Weil group, since as the Selmer group is very computable. Unfortunately, $Ш(K,A)$ is not always trivial:

Example 6.3.4. *Let $C/\mathbb{Q}$ be the curve defined in Theorem 6.1.1. It is a curve of genus 1, and thus its jacobian is an elliptic curve $E/\mathbb{Q}$, making C into a principal homogenous space of E over $\mathbb{Q}$ (in fact, for any principal homogenous space C' of an elliptic curve E' over K, we have an isomorphism $\mathrm{Pic}^0(C) \simeq E$, see [6, Theorem 3.8]). Again by Theorem 6.1.1, we have that $Ш(K,E)$ is non-trivial, since C represents a non-trivial element.*

Now, the story very roughly goes like this (again, see [6, Chapter X] for details, at least when A is an elliptic curve): $\mathrm{Sel}^m(A/K)$ is a nice, finite, and actually quite computable group. Thus, by Proposition 6.3.2, computing either $A(K)/[m]A(K)$, or $Ш(K,A)[m]$, reduces to computing the other. Of course, our goal was to compute $A(K)/[m]A(K)$, and thus the current problem seems to be that there is no known way of computing $Ш(K,A)$, even when A is an elliptic curve.

To compute $A(K)/[m]A(K)$, there is a strategy to circumvent the computation of the full $Ш(K,A)$; however, this strategy uses the following

Conjecture 6.3.5. *For any abelian variety A/K, $Ш(K,A)$ is finite.*

This section might have been a bit short, and overly handwavy (not really touching many details), but the take away is the definition of the Selmer group, the Tate-Shafarevich group, and the importance of Conjecture 6.3.5!

Example 6.3.6. *This example is from the note by Poonen [3]; I don't really understand it, but I'll put it here in the hope that I will understand it some day.*

Appearently, there are strong analogies between abelian varieties, and unit groups. So let $\mathcal{O}_{\overline{K}}$ denote the ring of algebraic integers over K, and $\mathcal{O}_{\overline{K}}^\times$ the units. One can show that

$$\ker H^1(G_K, \mathcal{O}_{\overline{K}}^\times) \to \prod_\nu H^1(G_\nu, \mathcal{O}_{\overline{K}_\nu}^\times)$$

is isomorphic to $\mathcal{C}\ell(K)$ (is this the adelic definition of the class group maybe?). This shows that the "Sha" in this analogie is finite.

7 Bonus 2: local class field theory

The focus on the book is to be something of an introduction to local CFT I guess. It was not my main motivation for reading, but it turned out to be quite interesting, so I will include some notes relevant to that here.

7.1 Basic structure of local field extensions

In this section, we assume basic knowledge on the definition of valuations, and completions. For a local field F, we denote by v_F the valuation, $\mathcal{O}_F$ the valuation ring, $\mathfrak{p}$ the maximal ideal, and $\mathbb{F}$ the residue field $\mathcal{O}_F/\mathfrak{p}$. Given an extension K/F, the maximal ideal of K will instead be denoted by $\mathfrak{P}$.

Recall also that v_F extends uniquely to a valuation v_K on K.

Definition 7.1: Ramification index and Inertia Degree

Let K/F be an extension of local number fields. The **ramification index** of K/F is denoted $e = e(K/F) = [v_K(K^\times) : v_F(F^\times)]$.
The **inertia degree** of K/F is denoted $f = f(K/F) := [\mathbb{K} : \mathbb{F}]$.

In terms of ideals, the ramification index also matches what we are used to, that is $e(K/F) = \mathfrak{p}\mathcal{O}_K = \mathfrak{P}^e$. But this point of view seems less common/usefull for local fields?

The fundamental identity we are used to for number fields holds also for local number fields. Keep in mind that there is a unique prime ideal in a number field, so the below really matches with $g = 1$.

Theorem 7.1.1. *Let K/F be an extension of local number fields of degree n. Then*

$$n = ef$$

Proof. Pick a uniformizer $\pi \in \mathcal{O}_K$, as well as elements $a_1, \dots a_f \in \mathcal{O}_K$ which lifts a basis of $\mathbb{K}$ as an $\mathbb{F}$-vector space. One starts by proving that $(\pi^i a_j)$ are linearly independent over F for $i \in \{0, \dots, e-1\}$ and $j \in \{1, \dots, f\}$.

Once that is proven, consider the $\mathcal{O}_F$ module N spanned by (π^i, a_j). Writing N_0 for the submodule spanned by just the $a_j's$, we have that

$$N = N_0 + \mathfrak{P}N_0 + \dots \mathfrak{P}^{e-1}N_0.$$

We also have $\mathcal{O}_K = N_0 + \mathfrak{P}$, because the a_j form a basis of $\mathbb{K} = \mathcal{O}_K/\mathfrak{P}$. The trick now is to use this iteratively to show that

$$\mathcal{O}_K = N_0 + \mathfrak{P}\mathcal{O}_K = N_0 + \mathfrak{P}N_0 + \mathfrak{P}^2\mathcal{O}_K = \dots = N + \mathfrak{P}^e\mathcal{O}_K$$

Since $\mathfrak{P}^e = \mathfrak{p}$, Nakayama's lemma shows that $N = \mathcal{O}_K$. □

Given an extension of local number fields, we have a simple, but important map

$$\mathrm{Gal}(K/F) \to \mathrm{Gal}(\mathbb{K}/\mathbb{F})$$

since $\sigma(\mathfrak{P}) = \mathfrak{P}$ for all $\sigma \in \mathrm{Gal}(K/F)$. This map is surjective, which we now prove. An extension of local number fields should be understood in terms of its unramified part and its ramified part separately. The easiest is probably the unramified part, as shown in the following

Theorem 7.1.2. *Let F be a local number field. For any natural number n, there exists an unramified extension L/F of degree n, unique up to isomorphism. For such an extension, the natural map $\mathrm{Gal}(L/F) \to \mathrm{Gal}(\mathbb{L}/\mathbb{F})$ is an isomorphism.*

Proof. The proof of this is actually not very hard. Choose an extension of $\mathbb{F}$ of degree n (which is of course unique up to isomorphism), written as $\mathbb{F}/\langle \bar{P}(X) \rangle$ and lift $\bar{P}(X)$ to $P(X) \in F[X]$ using Hensel's lemma, and use this to construct L. The statements follow quickly from there. □

An easy corollary of the above proof is that unramified extensions of local number fields are automatically Galois, and that $\mathrm{Gal}(L/F)$ is cyclic, and generated by a canonical element. This element is also called the Frobenius, and denoted $\mathrm{Frob}_{L/F}$.

Fixing an algebraic closure $\overline{F}$ and $\overline{\mathbb{F}}$, the above really gives an inclusion (and dimension!) preserving bijections between the intermidiate unramified fields $F \subset L \subset \overline{F}$, and $\mathbb{F} \subset \mathbb{L} \subset \overline{\mathbb{F}}$. This allows us to make the following

Definition 7.2: Inertia subfield

Let K/F be an extension of local number fields. The **inertia subfield** $K_0 \subset K$ is the field characterised by the property that L/F is unramified if and only if $L \subseteq K_0$.

Note that for the inertia subfield, we always have $[K_0 : K] = e(K/F)$, implying that $K_0 = K$ if and only if K is unramified.

The following is innocent, but will be important.

Proposition 7.1.3. *Let $L_1/F, L_2/F$ be field extensions, both contained in a common field extension K/F. If L_1/F and L_2/F are both unramified, then so is the compositum L_1L_2/F.*

Proof. Follows immidiately from the fact that L_1, L_2 are both contained in K_0. □

We can state

Lemma 7.1.4. *The natural map* $\mathrm{Gal}(K/F) \to \mathrm{Gal}(\mathbb{K}, \mathbb{F})$ *is surjective.*

Proof. We already know that $\mathrm{Gal}(K_0/F) \simeq \mathrm{Gal}(\mathbb{K}, \mathbb{F})$, thus we need only prove that the natural map factors via the usual restriction $\mathrm{Gal}(K/F) \to \mathrm{Gal}(K_0/F)$. But this simply follows from $\mathcal{O}_K = \mathcal{O}_{K_0} + \mathfrak{P}$. □

This gives the natural definition of the **Inertia subgroup** $I(K/F)$ as the kernel of the above surjection. We immidiately give the more general

Definition 7.3: Higher ramification groups

Let K/F be an extension of local fields. For any $s \geq -1$, we define the group $G_s(K/F)$ as

$$G_s(K/F) := \{\sigma \in \mathrm{Gal}(K/F) \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}^{s+1}}, \forall \alpha \in \mathcal{O}_K\},$$

generalizing $I(K/F) = G_0(K/F)$.

For a p-adic field F, unramified extensions can be constructed as $F(\mu_N)$ for any N coprime to p. These extensions satisfy $[F(\mu_N) : F] = \lambda$, where λ is the order of q in $(\mathbb{Z}/N\mathbb{Z})^\times$ (this needs proof of course, but it follows pretty quickly from results in this section + general stuff about finite fields).

In the other end, totally ramified extensions are not unique, but we have a similar easy source of them. For instance, $\mathbb{Q}_p(\mu_{p^m})$ is totally ramified of degree $p^{m-1}(p-1)$. In fact, we can even put these two together to give an easy description of the local cyclotomic fields: Namely, the extension $K = \mathbb{Q}_p(\mu_N)$ for $N = p^m n$, where n is prime to p, satisfies $K_0 = \mathbb{Q}_p(\mu_n)$.

The higher ramification groups are the main weapon to study the totally ramified extension K/K_0 of any galois extension K/F, as the $G_s(K/F)$ are all normal in $G(K/F)$ (not too hard to show), the inclusion of subgroups

$$\mathrm{Gal}(K/F) \supset G_0(K/F) \supset G_1(K/F) \supset \dots$$

gives an inclusion of fields

$$F \subset K_0 \subset K_1 \subset \dots$$

Another very related group (as we shall almost immidiately see) is

Definition 7.4: Principal units

We define the group of ***s*-principal units** $U_K^{(s)}$ as

$$U_K^{(0)} := \mathcal{O}_K^\times$$

and for $s \geq 1$,

$$U_K^{(s)} := \{\alpha \in \mathcal{O}_K^\times \mid \alpha \equiv 1 \pmod{\mathfrak{P}}\}.$$

Lemma 7.1.5. *There are isomorphisms*

$$U_K^{(0)}/U_K^{(1)} = \mathbb{K}^\times$$

and for $s \geq 1$,

$$U_K^{(s)}/U_K^{(s+1)} = \mathbb{K}.$$

Proof. The first map obvious from the surjection $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{P})^\times$. The second isomorphism comes from the map formed by chosing a uniformizer Π (i.e. $(\Pi) = \mathfrak{P}$), and forming $U^{(s)} \to \mathcal{O}_K/\mathfrak{P}$ by sending α to the residue class of $(\alpha - 1)/\Pi^s$. □

Proposition 7.1.6. *For any* $s \geq 0$*, we have*

$$G_s(K/F)/G_{s+1}(K/F) \simeq U_K^{(s)}/U_K^{(s+1)}.$$

Proof. I won't bother proving this, but the isomorphism comes from the map defined by sending $\tau \in G_s(K/F)$ to $\tau(\Pi)/\Pi$, where Π is a uniformizer. □

We have now reached a sort of mini-goal, in a cool theorem:

Theorem 7.1.7. *Let* K/F *be a galois extension of local number fields. Then* $\mathrm{Gal}(K/F)$ *is solvable.*

Proof. By the previous proposition, the theorem is proven once it is shown that $G_s(K/F)$ eventually vanishes, as this gives the series

$$1 = G_s(K/F) < G_{s-1}(K/F) < \cdots < G_0(K/F) < \mathrm{Gal}(K/F).$$

The fact that $G_s(K/F)$ eventually vanishes is not too hard to prove (morally at least, its not very surprising that any $\sigma \in \mathrm{Gal}(K/F)$ that acts as the identity mod $\mathfrak{P}^s$ for all $s \in \mathbb{N}$, must be the identity itself). □

We now turn to the multiplicative structure of a local number field. The easiest (or at least, most familiar) example is $\mathbb{R}$, where we have

$$\mathbb{R}^\times = \{\pm 1\} \times \mathbb{R}_{\geq 0} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{R}$$

where the isomorphism $\mathbb{R}_{\geq 0} \simeq \mathbb{R}$ is given by the logarithm.

Proposition 7.1.8. *The three groups $\mathcal{O}_F, \mathcal{O}_F^\times$ and $U_F^{(1)}$ are all profinite. Specifically, we have*

$$\mathcal{O}_F = \varprojlim_s \mathcal{O}_F/\mathfrak{p}^s$$
$$\mathcal{O}_F^\times = \varprojlim_s \mathcal{O}_F^\times/U_F^{(s)}$$
$$U_F^{(1)} = \varprojlim_s U_F^{(1)}/U_F^{(s)}$$

Proof. The first one follows from combining the fact that $\mathfrak{p}^n$ is open, so all the $\mathcal{O}_F \to \mathcal{O}_F/\mathfrak{p}^n$ are continuous, and that $\mathcal{O}_F$ is dense. The next two follow from the fact that the first is even an isomorphism of rings. □

Proposition 7.1.9. *There is an isomorphism of topological groups*

$$F^\times \simeq \mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times U_F^{(1)}.$$

Hence $F^\times$ is locally compact (but not compact!).

Proof. One first shows the isomorphism $\mathcal{O}_F^\times \simeq \mu_{q-1} \times U_F^{(1)}$, given by reduction mod $\mathfrak{p}$ (where the first component maps isomorphically onto $\mathbb{F}^\times$, while the second is of course the kernel), from which it follows that the map sending $(n, \omega, u) \in \mathbb{Z} \times \mu_{q-1} \times U_F^{(1)}$ to $\pi^n \omega u \in F^\times$ is an isomorphism.

Now, since $U_F^{(1)}$ is profinite, any open set of $F^\times$ containing the identity $(0, 0, 1)$ must also contain an open, compact subgroup $(0, 0, H)$. Since we can always translate by x, this shows $F^\times$ is locally compact. □

As promised, the logarithm will essentially give the structure of $U_F^{(1)}$. By logarithm, we use the typical power-series meaning, i.e.

$$\log(1+X) = \sum_{n \geq 1} (-1)^{n-1} \frac{X^n}{n}$$

and similarily, the exponential

$$\exp(X) = \sum_{n \geq 0} \frac{X^n}{n!}.$$

Proposition 7.1.10. *For any $x \in \mathfrak{p}$, $\log(1+X)$ converges at $X = x$. Thus, there is a continuous homomorphism*

$$\log : U^{(1)} \to F$$

such that $\log(U^{(s)}) \subseteq \mathfrak{p}^s$.

Similarily, for all $n \geq e/(p-1)$, $\exp(X)$ converges at $X = x$ for all $x \in \mathfrak{p}^n$. This gives a continuous homomorphism

$$\exp : \mathfrak{p}^n \to U^{(n)}$$

Thus, for $n \geq e/(p-1)$, we have $U^{(n)} \simeq \mathfrak{p}^n$, where the isomorphism is given by mutually inverse log/exp maps.

Proof. Maybe later, probably never. □

Of course $\mathcal{O}_K \simeq \mathfrak{p}^n$ as groups for all n, thus we can finish with

Proposition 7.1.11. *Let $d = [F : \mathbb{Q}_p]$. The group $U_F^{(1)}$ is topologically isomorphic to*

$$\mathbb{Z}/p^\alpha\mathbb{Z} \times \mathbb{Z}_p^d$$

for some $\alpha \geq 0$.

Proof. We have the exact sequence of $\mathbb{Z}_p$ modules

$$0 \to U_F^{(n)} \to U_F^{(1)} \to U_F^{(1)}/U_F^{(n)} \to 0$$

and by choosing n large enough, we have $U_F^{(n)} \simeq \mathfrak{p}^n \simeq \mathcal{O}_F \simeq \mathbb{Z}_p^d$, while $U_F^{(1)}/U_F^{(n)}$ is finite of order q^{n-1} by Lemma 7.1.5. Thus $U^{(1)}$ is a finitely generated $\mathbb{Z}_p$-module, and thus

$$U^{(1)} \simeq \mathbb{Z}_p^d \times T$$

where T denotes the torsion part (by the fundamental theorem of finitely generated modules over a PID), which will also then by of order p^α for some $\alpha \geq 0$ (where q is a power of p). Finally, it is of course cyclic, as it is a finite subgroup of $F^\times$. □

We can summarize in the following

Theorem 7.1.12. *Let F be a local number field, with $d = [F : \mathbb{Q}_p]$, and $|\mathbb{F}| = q = p^n$. We have an isomorphism of topological groups*

$$F^\times \simeq \mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^\alpha\mathbb{Z} \times \mathbb{Z}_p^d.$$

Under this identification, we have

- *The projection onto the first factor $v_F : F^\times \to \mathbb{Z}$ is the normalized valuation.*
- *The subgroup $0 \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^\alpha\mathbb{Z} \times \mathbb{Z}_p^d$ correspnods to $\mathcal{O}_F^\times$.*
- *The subgroup $0 \times 0 \times \mathbb{Z}/p^\alpha\mathbb{Z} \times \mathbb{Z}_p^d$ correspnods to $U_F^{(1)}$.*
- *The subgroup $0 \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^\alpha\mathbb{Z} \times 0$ correspnods to the roots of unity in $F^\times$.*

Proof. This is just summarizing what we have covered in the latter half of this subsection. □

The following will also be useful:

Lemma 7.1.13. *For a local number field F, we have*

- *Any finite index subgroup of $F^\times$ is closed (or equivalently, open).*
- *Each open subgroup of $F^\times$ contains $U^{(s)}$ for some s, and convercely, any subgroup $U_F^{(s)}$ is open in $F^\times$.*
- *Each subgroup of finite index in $F^\times$ contains a subgroup of the form $\langle \pi^n \rangle \times U_F^{(s)}$ for π a uniformizer, and $n, s \in \mathbb{N}$.*

Proof. For the first point, the isomorphism Theorem 7.1.12 shows that this reduces to proving that any finite index subgroup of $\mathbb{Z}_p$ is closed. For the two others, see book (Lemma 4.11). □

7.2 Artin reciprocity

Local class field theory will give us a perfect description of the abelian extensions of F, in terms of norm subgroups of finite index in $F^\times$. We begin with the following proposition, which works both great as an example, but also will be needed for the final piece of the puzzle later:

Proposition 7.2.1. *Let E_n/F be a unramified extension of local number-fields of degree n. Then*

$$N_{E_n/F}(E_n^\times) = \{f \in F^\times \mid v(f) \equiv 0 \pmod{n}\}.$$

Proof. Let v denote the valuation on F, and w on E_n. For any $a \in E_n$, we have $v(N_{E_n/F}(a)) = nw(a)$, and since E_n is unramified, we have $w(E_n) = \mathbb{Z}$, and thus $v(N_{E_n/F}(E_n^\times)) = n\mathbb{Z}$. Thus, we need to prove that any $f \in \mathcal{O}_F^\times$ (i.e. any f with $v(f) = 0$) is in the image of the norm map. In the book, this is shown using kind of a lengthy but simple argument (essentially lifting an element from the residue fields), however this can also AGAIN be shown by Example 2.1.2: Let $G = \mathrm{Gal}(E_n/F) \simeq \mathbb{Z}/n\mathbb{Z}$. The exact sequence

$$0 \to \mathcal{O}_{E_n}^\times \to E^\times \xrightarrow{w} \mathbb{Z} \to 0$$

gives in G-cohomology

$$\cdots \to H^1(G, \mathbb{Z}) \to H^2(G, \mathcal{O}_{E_n}^\times) \to H^2(G, E^\times) \to H^2(G, \mathbb{Z}) \to H^3(G, \mathcal{O}_{E_n}^\times) \to \dots$$

Applying Example 2.1.2 everywhere (and Theorem 3.1.4 for $H^2(G, E^\times)$), we get

$$\dots 0 \to \mathcal{O}_F^\times / N_{E_n/F}(\mathcal{O}_{E_n}^\times) \to \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0 \to \dots$$

This shows that $\mathcal{O}_F^\times / N_{E_n/F}(\mathcal{O}_{E_n}^\times) = 0$, which is what we wanted. □

Thus, for unramified extensions, we have $\mathrm{Gal}(E_n/F) \simeq F^\times / N_{E_n/F}(E_n^\times)$. Amazingly, by the work done in Section 4.4, we get the result saying that this generalises completely.

Theorem 7.2.2 (Reciprocity isomorphism)**.** *Let L/F be a Galois extension of local number fields. Then*

$$\mathrm{Gal}(L/F)^{\mathrm{ab}} \simeq F^\times / N_{L/F}(L^\times).$$

Proof. For any subgroup $\mathrm{Gal}(L/K)$, we have $H^1(\mathrm{Gal}(L/K), \mathbb{G}_m) = 0$ by Hilbert 90 (Theorem 3.2.3, and $H^2(\mathrm{Gal}(L/K), \mathbb{G}_m) = \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ by the structure of the Brauer group of a local number field (Theorem 3.1.4), and thus Tate's theorem (Theorem 4.4.3) applies.

We apply it to $r = 0, S = G$ and get

$$F^\times / N_{L/F}(L^\times) \simeq \widehat{H}^0(\mathrm{Gal}(L/F), \mathbb{G}_m) \simeq \widehat{H}^{-2}(\mathrm{Gal}(L/F), \mathbb{Z}) = H_1(\mathrm{Gal}(L/F), \mathbb{Z}) \simeq \mathrm{Gal}(L/F)^{\mathrm{ab}}$$

where the first isomorphism is by definition (Definition 2.2), and the last isomorphism is Proposition 3.3.1. □

By the Galois correspondence, it is now clear that there is a bijection between abelian extensions of F, and norm subgroups $N_L := N_{L/F}(L^\times)$. What remains to prove the fundamental theorem of local class field theory is thus to prove that *any* finite index subgroup of $F^\times$ is a norm-subgroup. This is known as the "existance theorem".

Before we prove this, we give an important definition.

Definition 7.5: (Local) Artin Symbol

Let F be a local number field. By the above discussion, we have a homomorphism composed as

$$F^\times \to F^\times/N_L \xrightarrow{\sim} \mathrm{Gal}(L/F)^{\mathrm{ab}}.$$

For $x \in F^\times$, the **(local) Artin symbol** $(x, L/F)$ is defined as the image of x under this composition.

This is all a bit handwavy, but one needs to take care when defining the Artin symbol like this, as the last isomorphism in the definition above seems to depend on many choices. But it turns out that there is a way to make consistent choices, so that the isomorphism really is "canonical" in a certain sense.

7.3 The main theorem

We now go on to prove the existence theorem. First we need two results on norm subgroups.

Lemma 7.3.1. *Let L_1, L_2 be finite abelian extensions of F. Then*

$$N_{L_1L_2} = N_{L_1} \cap N_{L_2}.$$

Proof. Assume $x \in N_{L_1L_2}$. Then the elements $N_{L_1L_2/Li}(x)$ show that $x \in N_{L_i}$ for both i.

Showing the reverse direction is conciderably harder: Assuming $x \in N_{L_1} \cap N_{L_2}$, one considers the artin symbol $(x, L_1L_2/F) \in \mathrm{Gal}(L_1L_2/F)$, and argues that it is a trivial element, since $(x, L_1/F)$ and $(x, L_2/F)$ are both trivial. Of course, this uses a form of functoriality of the Artin symbol we have not covered (but it is maybe not so surprising that it works); see book (Lemma 13.13 and 13.14). □

Proposition 7.3.2. *Let $A < F^\times$ be a subgoup containing a norm subgroup $N_L < A$. Then A is itself a norm subgroup.*

Proof. We have that $F^\times/N_L \simeq \mathrm{Gal}(L/F)$ for some abelian extension L. The subgroups of $F^\times$ containing N_L are thus in bijection with the subgroups of $\mathrm{Gal}(L/F)$, which in turn are in bijection with abelian extensions $F \subset K \subset L$. Since $N_K = N_L$ if and only if $K = L$, the result follows since the groups in question are finite. □

Theorem 7.3.3 (Existence theorem)**.** *For any subgroup $A < F^\times$ of finite index, there exists a field L/F such that $A = N_L$.*

Proof. We will first prove the result for A containing $\mathcal{O}_F^\times$, and then reduce to this case.

Assume that A contains $\mathcal{O}_F^\times$. This already implies that $A = v_F^{-1}(n\mathbb{Z})$ for some $n \geq 1$, as $\mathcal{O}_F^\times$ is precicely the kernel of $v_F : F^\times \to \mathbb{Z}$. Thus, $A = E_n$, the unique unramified extension of degree n, by Proposition 7.2.1.

Now, for any norm-subgroup N, consider the group $A_N = (A \cap N)\mathcal{O}_F^\times$. This still has finite index, thus A_N is a norm-subgroup, since it obviously contains $\mathcal{O}_F^\times$. We must show that we can choose N, such that $N \cap A_N \subseteq A$, as the result then follows by Lemma 7.3.1 and Proposition 7.3.2.

We will show the even stronger fact that we can always find N so that $N \cap \mathcal{O}_F^\times \subseteq A$. The hardest step is in fact the following first step: the intersection $\cap_N N \cap \mathcal{O}_F^\times = \{1\}$, where the intersection is taken over all possible norm subgroups. Anyway, assume that this is true, then since the norm subgoups N are all closed and open by Lemma 7.1.13, the complement of them together with A

(which is also open, since of finite index) form an open cover of $\mathcal{O}_F^\times$. But $\mathcal{O}_F^\times$ is profinite, hence compact, by Proposition 7.1.8, thus there in fact exists a finite subcover $A \cup N_1^c \cup \cdots \cup N_d^c$. Again taking compliments, we see that there exists a norm group $N := N_1 \cap \cdots \cap N_d$ such that $A^c \cap N$ intersects trivially with $\mathcal{O}_F^\times$, in other words $N \cap \mathcal{O}_F^\times$ is contained in A. □

This finishes the the fundamental theorem of local class field theory, which we now summarize:

Theorem 7.3.4 (The fundamental theorem of local class field theory)**.** *Let F be a local number field. There is a bijective and order-reversing (wrt. inclusion) correspondence between the subgroups of $F^\times$ of finite index and the finite abelian extensions of F.*

Proof. Combine Theorem 7.2.2 and Theorem 7.3.3. □

References

[1] Keith Conrad. "Selmer's example". In: *Expository Papers* (2017).

[2] Pierre Guillot. *A gentle course in local class field theory: local number fields, Brauer groups, Galois cohomology*. Cambridge University Press, 2018.

[3] Bjorn Poonen. "The Selmer group, the Shafarevich-Tate group, and the weak Mordell-Weil Ttheorem". In: *Preprint* (1999).

[4] Ernst S Selmer. "The diophantine equation ax 3+ by 3+ cz 3= 0." In: (1951).

[5] Joseph H Silverman. "A survey of local and global pairings on elliptic curves and abelian varieties". In: *International Conference on Pairing-Based Cryptography*. Springer. 2010, pp. 377–396.

[6] Joseph H Silverman. *The arithmetic of elliptic curves*. Vol. 106. Springer, 2009.

[7] John Voight. *Quaternion algebras*. Springer Nature, 2021.