An Invitation to Local Fields

Groups, Rings and Group Rings
Ubatuba-São Paulo, 2008

Eduardo Tengan
(ICMC-USP)

"To get a book from these texts, only scissors and glue were needed."

J.-P. Serre, in response to receiving the 1995 Steele
Prize for his book "Cours d'Arithmétique"

The author was supported by FAPESP grant 06/59613-8.

Preface

1 What is a Local Field?

Historically, the first local field, the field of p-adic numbers $\mathbb{Q}_p$, was introduced in 1897 by Kurt Hensel, in an attempt to borrow ideas and techniques of power series in order to solve problems in Number Theory. Since its inception, local fields have attracted the attention of several mathematicians, and have found innumerable applications not only to Number Theory but also to Representation Theory, Division Algebras, Quadratic Forms and Algebraic Geometry. As a result, local fields are now consolidated as part of the standard repertoire of contemporary Mathematics.

But what exactly is a local field? **Local field** is the name given to any finite field extension of either the field of p-adic numbers $\mathbb{Q}_p$ or the field of Laurent power series $\mathbb{F}_p((t))$. Local fields are complete topological fields, and as such are not too distant relatives of $\mathbb{R}$ and $\mathbb{C}$. Unlike $\mathbb{Q}$ or $\mathbb{F}_p(t)$ (which are **global fields**), local fields admit a single valuation, hence the tag 'local'. Local fields usually pop up as completions of a global field (with respect to one of the valuations of the latter).

2 What are Local Fields good for?

Local fields help us better understand the arithmetic of global fields, much in the same way $\mathbb{R}$ helps us better understand inequalities in $\mathbb{Q}$. In this context local fields are like playing drums: they are not too hard to play with, yet all the major phenomena of global fields already appear in some way or other in local fields.

In some fortuitous instances, this interaction between global and local fields assumes a particularly strong form, the so-called **local-global** or **Haße principle**, which *completely* reduces a global problem to its local counterparts. The classical example is the famous Haße-Minkowski theorem: a quadratic form over $\mathbb{Q}$ is isotropic (i.e. represents zero non-trivially) if and only if it is isotropic over $\mathbb{R}$ and over $\mathbb{Q}_p$ for each prime p. Here is another example: a (finite dimensional) central simple algebra D over $\mathbb{Q}$ is trivial (i.e. isomorphic to a matrix ring over $\mathbb{Q}$) if and only if $D \otimes_{\mathbb{Q}} \mathbb{R}$ and $D \otimes_{\mathbb{Q}} \mathbb{Q}_p$ are trivial for all primes p.

3 Should I read these Notes?

Well, the answer to this question is of course up to you. But here are some of the "lollipops" that you may miss if you decide not to. In the first chapter, after covering the basic theorems of the subject, we show that every quadratic form over $\mathbb{Q}_p$ in at least 5 variables is isotropic. Combined with the Haße-Minkowski theorem above, this proves that a quadratic form over $\mathbb{Q}$ in at least 5 variables is isotropic if and only if it is isotropic over $\mathbb{R}$! Still in the first chapter we show that every Galois extension of $\mathbb{Q}_p$ is solvable! In the second chapter, we give a description of *all* abelian extensions of $\mathbb{Q}_p$. In particular we prove that every abelian extension of $\mathbb{Q}_p$ is contained in some cyclotomic extension. This is a local version of the celebrated Kronecker-Weber theorem, which states that any abelian extension of $\mathbb{Q}$ is contained in some cyclotomic extension.

Unfortunately, due to restrictions of time and space (= laziness of the author), it was not possible to cover the interactions between global and local fields systematically. But we do include an important example: the proof of the *global* Kronecker-Weber theorem from the local one, assuming just a few basic facts about global fields, which can easily be found in standard texts on Algebraic Number Theory.

All in all, this text is more or less self-contained in that we do not require much beyond what is usually covered in regular Algebra courses. For convenience of the reader, the "less standard" topics are briefly reviewed (or viewed, depending on the reader) in the Appendix.

4 Where to go next?

There are plenty of good books about local fields, varying in difficulty and scope. The first part of Serre's "A course in Arithmetic" is particularly recommended, with many important applications that are not covered in this text. Several books on Number Theory contain good introductions to local fields, such as the those by Borevich-Shafarevich, Neukirch and Milne. And everyone should eventually look at the two books "Local Fields," the one by Cassels and the one by Serre.

Since local fields are a prelude to global ones, one should also start learning about global fields. Besides the Number Theory books quoted above, Cassels-Fröhlich's book is a must, specially the articles by Serre and by Tate. Milne's "Class Field Theory" is also extremely helpful. Finally the authoritative book (= if it's not there it's wrong) "Cohomology of Number Fields" by Neukirch-Schimdt-Wingberg cannot be forgotten.

5 Some Commonly Used Terms

- CLEARLY: I don't want to write down all the "in-between" steps.
- RECALL: I shouldn't have to tell you this, but...
- WLOG (Without Loss Of Generality): I'm not about to do all the possible cases, so I'll do one and let you figure out the rest.
- CHECK or CHECK FOR YOURSELF: This is the boring part of the proof, so you can do it on your own time.
- SKETCH OF A PROOF: I couldn't verify all the details, so I'll break it down into the parts I couldn't prove.
- HINT: The hardest of several possible ways to do a proof.
- SIMILARLY: At least one line of the proof of this case is the same as before.
- BY A PREVIOUS THEOREM: I don't remember how it goes (come to think of it I'm not really sure we did this at all), but if I stated it right (or at all), then the rest of this follows.
- PROOF OMITTED: Trust me, it's true.

Contents

Local Fields: Basics

1 Two basic examples: $\mathbb{F}_p((t))$ and $\mathbb{Q}_p$

Let p be a prime and let $\mathbb{F}_p$ be the finite field with p elements. Consider the ring $\mathbb{F}_p[[t]]$ of formal power series with coefficients in $\mathbb{F}_p$:

$$a_0 + a_1 t + a_2 t^2 + \cdots, \qquad a_i \in \mathbb{F}_p$$

Addition and multiplication are performed in the usual way as with polynomials. For instance, one has

$$(1-t)\cdot(1+t+t^2+t^3+\cdots) = 1$$

The principal ideal (t) is a maximal ideal of $\mathbb{F}_p[[t]]$ with residue field $\mathbb{F}_p[[t]]/(t) \cong \mathbb{F}_p$. Also the group of units of $\mathbb{F}_p[[t]]$ is given by

$$\boxed{\mathbb{F}_p[[t]]^\times = \big\{a_0 + a_1 t + a_2 t^2 + \cdots \in F_p[[t]] \;\big|\; a_0 \neq 0\big\}}$$

In fact, if

$$(a_0 + a_1 t + a_2 t^2 + \cdots)(b_0 + b_1 t + b_2 t^2 + \cdots) = 1$$

has a solution in the b_i's, one must have $a_0 b_0 = 1$ and hence $a_0 \neq 0$, and conversely if $a_0 \neq 0$ then one can recursively set $b_0 = a_0^{-1}$ and $b_n = -a_0^{-1}(a_n b_0 + a_{n-1} b_1 + \cdots + a_1 b_{n-1})$ for $n \geq 1$.

In other words, the complement of the maximal ideal (t), namely the set of power series $a_0 + a_1 t + a_2 t^2 + \cdots$ with nonzero constant term $a_0 \neq 0$, consists solely of units, and therefore (t) is the unique maximal ideal of $\mathbb{F}_p[[t]]$, which is thus a **local ring**. The ring $\mathbb{F}_p[[t]]$ is also a UFD and, even better, a **discrete valuation ring** (dvr for short; see appendix for the definition), as every nonzero element $f \in \mathbb{F}_p[[t]]$ admits a rather simple prime factorisation

$$\boxed{f = \underbrace{t^n}_{\substack{\text{power of}\\ \text{uniformiser } t}} \times \underbrace{(a_n + a_{n+1} t + a_{n+2} t^2 + \cdots)}_{\text{unit in } \mathbb{F}_p[[t]]}, \quad a_n \neq 0}$$

for some $n \geq 0$. As a consequence, the nonzero elements of the fraction field $\mathbb{F}_p((t)) \overset{\text{df}}{=} \operatorname{Frac} \mathbb{F}_p[[t]]$ also admit a similar factorisation with $n \in \mathbb{Z}$, and thus elements of $\mathbb{F}_p((t))$ can be identified with "Laurent power series" $f = \sum_{i \geq i_0} a_i t^i$, $i_0 \in \mathbb{Z}$. The **discrete valuation** v on $\mathbb{F}_p((t))$ associated to the dvr $\mathbb{F}_p[[t]]$ is given by

$$\boxed{\begin{aligned} v(f) &= n \in \mathbb{Z} \text{ such that } f \text{ has prime factorisation } f = t^n \cdot u,\ u \in \mathbb{F}_p[[t]]^\times \\ &= \min\{n \in \mathbb{Z} \mid a_n \neq 0\} \end{aligned}}$$

for $f = \sum_{i \geq i_0} a_i t^i \in \mathbb{F}_p((t))^\times$, and $v(0) = \infty$ if $f = 0$. The discretely valued field $\mathbb{F}_p((t))$ is our first example of a **local field**.

Being a discretely valued field, $\mathbb{F}_p((t))$ is also a normed field with norm given by (see appendix)

$$|f|_v = 2^{-v(f)} \qquad \text{for} \quad f \in \mathbb{F}_p((t))$$

(Here 2 denotes your favourite real number greater than 1) One has the following rule of the thumb for the topology defined by $|-|_v$: the power series $a_0 + a_1 t + a_2 t^2 + \cdots$ converges (to itself) and thus its general term should approach zero. Hence

$$\boxed{\lim_{n\to\infty} t^n = 0}$$

For example, for any $f \in \mathbb{F}_p((t))$ one has the following "derivative rule"

$$\lim_{n\to\infty} \frac{(f+t^n)^5 - f^5}{t^n} = 5f^4$$

Observe that $\mathbb{F}_p((t))$ contains $\mathbb{F}_p(t) = \operatorname{Frac}\mathbb{F}_p[t]$ as a dense subfield since any power series $f = \sum_{i\geq i_0} a_i t^i$ can be written as a limit of rational functions (for instance, of the "truncations" $\sum_{i_0\leq i\leq n} a_i t^i$ of f), much in the same way as $\mathbb{R}$ contains $\mathbb{Q}$ as a dense subfield since any real number is a limit of rational ones. As you can see, much of the intuition from Analysis can be borrowed for the study of $\mathbb{F}_p((t))$ (and other local fields). The good news is that, thanks to the **strong triangle inequality** (see appendix)

$$|f+g|_v \leq \max\{|f|_v, |g|_v\},$$

Analysis on $\mathbb{F}_p((t))$ turns out to be *much easier* than on $\mathbb{R}$ or $\mathbb{C}$! For instance, one has the following amazing

Lemma 1.1 (Calculus Student's Psychedelic Dream) *Let $f_n \in \mathbb{F}_p((t))$, $n \geq 0$. Then the series*

$$f_0 + f_1 + f_2 + f_3 + \cdots$$

converges in $\mathbb{F}_p((t))$ if and only if $\lim_{n\to\infty} f_n = 0$.

Proof The "only if" is clear (it works for any metric space). Now assume that $\lim_{n\to\infty} f_n = 0$, i.e., that $v(f_n) \to \infty$ as $n \to \infty$. This means that for a fixed n there are only finitely many terms in the infinite sum $f_0 + f_1 + f_2 + \cdots$ that actually contribute to the coefficient of t^n, and hence $f_0 + f_1 + f_2 + \cdots$ is a well-defined element of $\mathbb{F}_p((t))$. Now a routine check (using the definitions) shows that this element is indeed the limit of the partial sums $f_0 + \cdots + f_m$. □

The above lemma turns out to be quite useful in explicit computations. For instance, one can find the multiplicative inverse of $1 + t + t^2$, say, by applying the usual formula for the sum of a geometric progression:

$$\frac{1}{1+t+t^2} = 1 - (t+t^2) + (t+t^2)^2 - (t+t^2)^3 + \cdots$$

This series converges since the general term has valuation $v\big((t+t^2)^n\big) = n \to \infty$.

Now we show that $\mathbb{F}_p((t))$ is actually a **complete discretely valued field**. In other words, we show that every Cauchy sequence in $\mathbb{F}_p((t))$ converges. In fact, if $\{f_n\}_{n\geq 0}$ is Cauchy then $\lim_{n\to\infty}(f_{n+1} - f_n) = 0$ and therefore

$$\lim_{n\to\infty} f_n = f_0 + \sum_{n\geq 0}(f_{n+1} - f_n)$$

converges by the Calculus Student's Psychedelic Dream, proving that $\mathbb{F}_p((t))$ is indeed complete.

Remark 1.2 Conversely, any complete discretely valued field K with valuation v satisfies the Calculus Student's Psychedelic Dream: if $\lim_{n\to\infty} f_n = 0$ then $\big|\sum_{M\leq n\leq N} f_n\big|_v \leq \max\big\{|f_n|_v \;\big|\; M \leq n \leq N\big\}$ can be made arbitrarily small by choosing M sufficiently large, hence the partial sums $\sum_{0\leq n\leq N} f_n$ form a Cauchy sequence and therefore $\sum_{n\geq 0} f_n$ converges.

Before leaving the realm of $\mathbb{F}_p((t))$, we wish to give an alternative but rather useful description of $\mathbb{F}_p[[t]]$ as a **projective limit** of the discrete rings $\mathbb{F}_p[t]/(t^n)$ (check the appendix if you are unfamiliar with limits). Namely, we have an algebraic and topological isomorphism

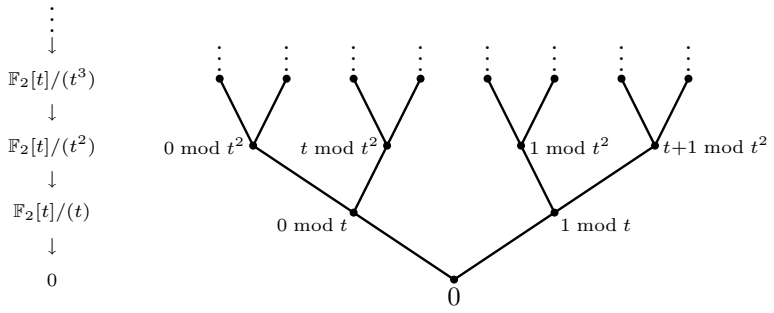
$$\boxed{\mathbb{F}_p[[t]] \approx \varprojlim_{n\in\mathbb{N}} \frac{\mathbb{F}_p[t]}{(t^n)} \stackrel{\text{df}}{=} \Big\{(f_n) \in \prod_{n\in\mathbb{N}} \frac{\mathbb{F}_p[t]}{(t^n)} \;\Big|\; f_m = f_n \bmod t^m \text{ for all } n \geq m\Big\}}$$

given by

$$a_0 + a_1 t + a_2 t^2 + \cdots \mapsto (a_0 \bmod t,\ a_0 + a_1 t \bmod t^2,\ a_0 + a_1 t + a_2 t^2 \bmod t^3, \ldots)$$

Under this isomorphism the projection maps $\phi_n \colon \mathbb{F}_p[[t]] \to \mathbb{F}_p[t]/(t^n)$ become just the "truncation maps" given by $a_0 + a_1 t + \cdots \mapsto a_0 + \cdots + a_{n-1} t^{n-1} \bmod t^n$.

A good way to picture this projective limit (or any other for the matter) is as the set of infinite paths in an infinite rooted tree. For instance, for $p = 2$, one has the tree in the illustration, whose vertices in the n-th level are labelled by elements of $\mathbb{F}_2[t]/(t^n)$ and an element of the n-th level is connected by an edge to its image in the $(n-1)$-th level. Then an element $a_0 + a_1 t + a_2 t^2 + \cdots \in \mathbb{F}_2[[t]]$ corresponds to the path given by $(a_0 \bmod t,\ a_0 + a_1 t \bmod t^2,\ a_0 + a_1 t + a_2 t^2 \bmod t^3, \ldots) \in \varprojlim_{n \in \mathbb{N}} \mathbb{F}_2[t]/(t^n)$.



$\mathbb{F}_2[[t]]$ as a projective limit

Observe that $\prod_{n \in \mathbb{N}} \mathbb{F}_p[t]/(t^n)$ is compact by Tychonoff's theorem and hence that $\mathbb{F}_p[[t]]$, as a closed subspace of this product, is also compact (this can also be proven by the original description of $\mathbb{F}_p[[t]]$, try!). Therefore any element $f \in \mathbb{F}_p((t))$ has a compact neighbourhood $f + \mathbb{F}_p[[t]] = \{g \in \mathbb{F}_p((t)) \mid |g - f|_v < 2\}$, i.e., we have that $\mathbb{F}_p((t))$ is a **locally compact complete discretely valued field with finite residue field** $\mathbb{F}_p$ (image how this would look if written in German!).

Enough about $\mathbb{F}_p((t))$ for now. Next we introduce the second main example of a local field. By analogy with the above, we define the **ring of p-adic integers** $\mathbb{Z}_p$ as the projective limit of the discrete rings $\mathbb{Z}/(p^n)$:

$$\mathbb{Z}_p \stackrel{\text{df}}{=} \varprojlim_{n \in \mathbb{N}} \frac{\mathbb{Z}}{(p^n)} = \left\{ (f_n) \in \prod_{n \in \mathbb{N}} \frac{\mathbb{Z}}{(p^n)} \;\middle|\; f_m = f_n \bmod p^m \text{ for all } n \geq m \right\}$$

We may choose unique integers F_n with $0 \leq F_n < p^n$ representing $f_n \in \mathbb{Z}/(p^n)$. Writing F_n in base p

$$F_n = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}, \qquad 0 \leq a_i < p$$

we find that for $m \leq n$ we must have $F_m = a_0 + a_1 p + \cdots + a_{m-1} p^{m-1}$, i.e., one obtains F_m by "truncating" F_n. Hence a p-adic integer corresponds **uniquely** to a sequence of integers of the form

$$(a_0,\ a_0 + a_1 p,\ a_0 + a_1 p + a_2 p^2, \ldots) \qquad 0 \leq a_i < p$$

which is usually written as an "infinite base p representation"

$$a_0 + a_1 p + a_2 p^2 + \cdots \qquad \text{with} \quad 0 \leq a_i < p$$

Computations with this "infinite series" can be done as with $\mathbb{F}_p[[t]]$, except that one has to pay attention to the "carry 1". For instance in $\mathbb{Z}_2$ one has that

$$1 + 2 + 2^2 + 2^3 + \cdots = \frac{1}{1 - 2} = -1$$

by the usual formula for the sum of a geometric series! From a different perspective, adding 1 to $1+2+2^2+2^3+\cdots$ we obtain

$$\begin{aligned} 1+(1+2+2^2+2^3+\cdots) &= 2+2+2^2+2^3+\cdots \\ &= 2^2+2^2+2^3+\cdots \\ &= 2^3+2^3+\cdots \\ &= \cdots = 0 \end{aligned}$$

We obtain an "infinite" sequence of "carry 1's" and the end result is zero! But wait, is that licit or sheer nonsense? If we go back to the original definition, there is no doubt that the above computations are indeed correct: 1 corresponds to the constant tuple $(1 \bmod 2, 1 \bmod 2^2, 1 \bmod 2^3, \ldots)$ while $1+2+2^2+2^3+\cdots$ corresponds to the tuple $(1 \bmod 2, 1+2 \bmod 2^2, 1+2+2^2 \bmod 2^3, \ldots)$, hence their sum is indeed zero. The punchline is: *if a computation with the "infinite base p representation" works modulo p^n for all n then it works.* For obvious reasons, we shall mostly work with the more intuitive infinite base p representation, and leave it to the sceptical reader the chore of translating the statements back into the projective limit definition of $\mathbb{Z}_p$.

Observe that in the same way that $\mathbb{F}_p[t]$ is contained in $\mathbb{F}_p[[t]]$ we have that $\mathbb{Z}$ is contained in $\mathbb{Z}_p$ via the "diagonal embedding" $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ given by $a \mapsto (a \bmod p^n)_{n\in\mathbb{N}}$ (or a finite base p representation is a special case of an infinite one). Also, as with $\mathbb{F}_p[[t]]$, there is a very simple description of the units of $\mathbb{Z}_p$ as those p-adic integers with "non-zero constant term":

$$\boxed{\mathbb{Z}_p^\times = \left\{a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p \;\middle|\; a_0 \neq 0, \quad 0 \leq a_i < p\right\}}$$

This is clear since $a_0 + a_1 p + \cdots + a_{n-1}p^{n-1} \bmod p^n$, $0 \leq a_i < p$, is invertible in $\mathbb{Z}/(p^n)$ if and only if $a_0 \neq 0$. Therefore $\mathbb{Z}_p^\times$ consists exactly of those elements in the complement of the principal ideal (p), which is maximal since $\mathbb{Z}_p/(p) = \mathbb{F}_p$. Hence, as with $\mathbb{F}_p[[t]]$, $\mathbb{Z}_p$ is also a local ring with finite residue field $\mathbb{F}_p$. And it is also a discrete valuation ring, since any element $f \in \mathbb{Z}_p$ has a prime factorisation

$$\boxed{f = \underbrace{p^n}_{\substack{\text{power of}\\ \text{uniformiser } p}} \times \underbrace{(a_n + a_{n+1}p^{n+1} + a_{n+2}p^{n+2} + \cdots)}_{\text{unit in } \mathbb{Z}_p} \qquad a_n \neq 0}$$

for some $n \geq 0$, with $0 \leq a_i < p$. Hence elements of the field of fractions $\mathbb{Q}_p \stackrel{\text{df}}{=} \operatorname{Frac}\mathbb{Z}_p$ can be written as "Laurent power series" $\sum_{i\geq i_0} a_i p^i$, $0 \leq a_i < p$, and the valuation on $\mathbb{Q}_p$ associated to the dvr $\mathbb{Z}_p$ is given by

$$\boxed{\begin{aligned} v(f) &= n \in \mathbb{Z} \text{ such that } f \text{ has prime factorisation } f = p^n \cdot u,\ u \in \mathbb{Z}_p^\times \\ &= \min\{n \in \mathbb{Z} \mid a_n \neq 0\} \end{aligned}}$$

for a nonzero element $f = \sum_{i\geq i_0} a_i p^i$, $0 \leq a_i < p$.

The topology on $\mathbb{Q}_p$ is now expressed by the rule of the thumb

$$\boxed{\lim_{n\to\infty} p^n = 0}$$

It is easy to check that this topology on $\mathbb{Z}_p$, given by the valuation v, coincides with the one induced from the compact product $\prod_{n\in\mathbb{N}} \mathbb{Z}/(p^n)$, hence $\mathbb{Z}_p$ is compact and thus $\mathbb{Q}_p$ is a locally compact. And since any element of $\mathbb{Q}_p$ is a limit of rational numbers (for instance of the truncations of its base p expansion), we have that $\mathbb{Q}$ is contained as a dense subfield of $\mathbb{Q}_p$. Finally, Calculus Student's Psychedelic Dream holds in $\mathbb{Q}_p$ and $\mathbb{Q}_p$ is a complete, virtually by the very same proofs for $\mathbb{F}_p((t))$. To sum up, $\mathbb{Q}_p$ is a **locally compact complete discretely valued field with finite residue field** $\mathbb{F}_p$, and it is our second main example of a local field. Note that while $\operatorname{char}\mathbb{F}_p((t)) = p$ we have that $\operatorname{char}\mathbb{Q}_p = 0$.

2 Hensel's lemma and applications

An amazing feature of local fields such as $\mathbb{F}_p((t))$ or $\mathbb{Q}_p$ is that, arithmetically speaking, they lie in between finite fields such as $\mathbb{F}_p$ and global fields such as $\mathbb{F}_p(t)$ or $\mathbb{Q}$. That is exactly what makes the study of local fields so attractive: it allows us to obtain information about global fields at a cheaper price. For instance, we may often reduce finding the solution to a system of polynomial equations over $\mathbb{F}_p((t))$ or $\mathbb{Q}_p$ to the much simpler similar task over $\mathbb{F}_p$. The main tool for that is the very important **Hensel's lemma**, whose punchline is

Hensel: "Smooth points in the residue field lift"

Precisely, we have

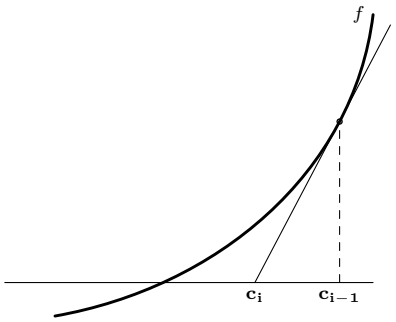
Lemma 2.1 (Hensel) *Let K be a complete valued field with valuation ring A. Let $\mathfrak{m}$ be the maximal ideal of A and $k = A/\mathfrak{m}$ be its residue field. Let $m \leq n$ and consider polynomials $f_1, \ldots, f_m \in A[x_1, \ldots, x_n]$. Write $\bar{f}_i$ for the image of f_i in $A[x_1, \ldots, x_n]/\mathfrak{m}A[x_1, \ldots, x_n] = k[x_1, \ldots, x_n]$.*

Suppose that we are given a **smooth point** $\mathbf{c} = (c_1, \ldots, c_n) \in k^n$ *in the variety cut out by the system of equations $\bar{f}_i(\mathbf{x}) = 0$, i.e.,*

1. *$\bar{f}_i(\mathbf{c}) = 0$ for all i and*
2. *$m = \mathrm{rk}\Big(\frac{\partial \bar{f}_i}{\partial x_j}(\mathbf{c})\Big)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ (in other words the codimension of the variety equals the rank of the Jacobian matrix)*

Then $\mathbf{c}$ lifts to a point $\mathbf{a} = (a_1, \ldots, a_n) \in A^n$ of the the variety cut out by the system of equations $f_i(\mathbf{x}) = 0$, i.e., $f_i(\mathbf{a}) = 0$ for all $1 \leq i \leq m$ and $c_j = a_j \bmod \mathfrak{m}$ for all $1 \leq j \leq n$.

Proof The proof is based on the classical **Newton's method** for numerically finding the roots of a polynomial equation (see picture).



Newton's method: $\mathbf{c_i} = \mathbf{c_{i-1}} - \frac{f(\mathbf{c_{i-1}})}{f'(\mathbf{c_{i-1}})}$

As with Newton's method, we inductively construct a sequence of "approximate" roots $\mathbf{c}_i = (c_{i1}, \ldots, c_{in}) \in (A/\mathfrak{m}^i)^n$, $i = 1, 2, \ldots$, such that

(a) the point $\mathbf{c}_i \in (A/\mathfrak{m}^i)^n$ belongs to the variety cut out by the f_r, that is, $f_r(\mathbf{c}_i) = 0$ for all r (here and in the following we will indistinctively write f_r for its image in $A[x_1, \ldots, x_n]/\mathfrak{m}^i A[x_1, \ldots, x_n]$ as it will be clear from the context in which ring we are working);

(b) for all $i \leq j$, we have that $\mathbf{c}_i = \mathbf{c}_j \bmod \mathfrak{m}^i$ (which of course means that $c_{it} = c_{jt} \bmod \mathfrak{m}^i$ holds for each coordinate, $1 \leq t \leq n$)

The sequence $\mathbf{c}_i$ will then define a point $\mathbf{a} \in A^n = \varprojlim (A/\mathfrak{m}^i)^n$ in the variety cut out by the f_r. We begin by setting $\mathbf{c}_1 = \mathbf{c}$. For $i \geq 2$, let $\tilde{\mathbf{c}}_{i-1} \in (A/\mathfrak{m}^i)^n$ be any lift of $\mathbf{c}_{i-1} \in (A/\mathfrak{m}^{i-1})^n$ and consider the system in $\mathbf{y}_i = (y_1, \ldots, y_n)$

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1}(\tilde{\mathbf{c}}_{i-1}) & \ldots & \frac{\partial f_1}{\partial x_n}(\tilde{\mathbf{c}}_{i-1}) \\ \vdots & & \vdots \\ \frac{\partial f_m}{\partial x_1}(\tilde{\mathbf{c}}_{i-1}) & \ldots & \frac{\partial f_m}{\partial x_n}(\tilde{\mathbf{c}}_{i-1}) \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} f_1(\tilde{\mathbf{c}}_{i-1}) \\ \vdots \\ f_m(\tilde{\mathbf{c}}_{i-1}) \end{pmatrix} \qquad (*)$$

Modulo $\mathfrak{m}$ the Jacobian matrix has full rank m and thus by relabelling the x_j we may assume that the first m columns are, modulo $\mathfrak{m}$, linearly independent over k. Hence the determinant of the $m \times m$ minor given by the first m columns is a unit in $A/\mathfrak{m}^i$, and therefore we may set $y_{m+1} = \cdots = y_n = 0$ and solve for the first m variables. Now define

$$\mathbf{c}_i = \tilde{\mathbf{c}}_{i-1} - \mathbf{y}_i$$

Notice that when $m = n = 1$ this reduces to the formula of Newton's method.

Now we need to show that the $\mathbf{c}_i$'s satisfy our requirements (a) and (b). Assume by induction that $f_r(\mathbf{c}_{i-1}) = 0$ for all r. Since $\tilde{\mathbf{c}}_{i-1}$ lifts $\mathbf{c}_{i-1}$, to show (b) we have to show that $\mathbf{y}_i \bmod \mathfrak{m}^{i-1} = (0, \ldots, 0)$. But this is clear since $y_{m+1} = \cdots = y_n = 0$ and modulo $\mathfrak{m}^{i-1}$ the system $(*)$ is homogeneous and non-singular in the first m variables. This proves that $\mathbf{c}_{i-1} = \mathbf{c}_i \pmod{\mathfrak{m}^{i-1}}$. Finally, to show (a), from Taylor's formula we have that

$$\begin{aligned}
\begin{pmatrix} f_1(\mathbf{c}_i) \\ \vdots \\ f_m(\mathbf{c}_i) \end{pmatrix} &= \begin{pmatrix} f_1(\tilde{\mathbf{c}}_i - \mathbf{y}_i) \\ \vdots \\ f_m(\tilde{\mathbf{c}}_i - \mathbf{y}_i) \end{pmatrix} \\
&= \begin{pmatrix} f_1(\tilde{\mathbf{c}}_i) \\ \vdots \\ f_m(\tilde{\mathbf{c}}_i) \end{pmatrix} - \begin{pmatrix} \frac{\partial f_1}{\partial x_1}(\tilde{\mathbf{c}}_{i-1}) & \cdots & \frac{\partial f_1}{\partial x_n}(\tilde{\mathbf{c}}_{i-1}) \\ \vdots & & \vdots \\ \frac{\partial f_m}{\partial x_1}(\tilde{\mathbf{c}}_{i-1}) & \cdots & \frac{\partial f_m}{\partial x_n}(\tilde{\mathbf{c}}_{i-1}) \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} + q(\mathbf{y}) \\
&= q(\mathbf{y}) \qquad \text{by } (*)
\end{aligned}$$

where $q(\mathbf{y})$ is a vector whose components are sums of forms in $y_1, \ldots, y_n$ of degree at least 2. But $\mathbf{y}_i \bmod \mathfrak{m}^{i-1} = (0, \ldots, 0)$ and since $i \geq 2$ this implies that $q(\mathbf{y})$ vanishes in $(A/\mathfrak{m}^i)^n$. □

Remark 2.2 Given some extra hypotheses, we can also lift some "singular points". We have the following stronger version of Hensel's lemma, due to Tougeron, and whose proof is a variant of the above (left as an exercise for the reader, of course!)
With the above notation, suppose that there is a point $\mathbf{a}_0 \in A^n$ such that

$$f_r(\mathbf{a}_0) \equiv 0 \pmod{\mathfrak{m} \cdot \delta^2}$$

for all $r = 1, \ldots, m$, where $\delta \in A$ denotes the determinant of the $m \times m$ minor $\left(\frac{\partial f_i}{\partial x_j}(\mathbf{a}_0)\right)_{1 \leq i,j \leq m}$ of the Jacobian. Then there exists a point $\mathbf{a} \in A^n$ in the variety cut out by the f_r with $\mathbf{a}_0 \equiv \mathbf{a} \pmod{\mathfrak{m} \cdot \delta^2}$.

Example 2.3 (Squares in Local Fields) Let K be either $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$ with p an odd prime. Denote by A its valuation ring and let π be a uniformiser. Let $a \in A$ be a nonzero element and write it $a = \pi^n u$ with $u \in A^\times$. Then a is a square in A if and only if n is even and $u \bmod \pi$ is a square in $\mathbb{F}_p$. This condition is clearly necessary: any square has even valuation, therefore if a is a square n must be even and u be a square, and thus so must $u \bmod \pi$. Conversely, considering the polynomial $f(x) = x^2 - u$, if there exists $v_0 \in \mathbb{F}_p$ such that $u \bmod \pi = v_0^2$ then $f(v_0) = 0$ and $f'(v_0) = 2v_0 \neq 0$ in $\mathbb{F}_p$ (remember that $p \neq 2$) and hence by Hensel's lemma we may lift v_0 to a root of $f(x)$ in A, showing that u is a square. Therefore a is a square too since n is even.
From the above characterisation of squares in A one immediately obtains that $K^\times/(K^\times)^2$ is a finite group isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$; representatives of elements in $K^\times/(K^\times)^2$ are given for instance by $1, u, \pi, u\pi$ where $u \in A^\times$ is such that $u \bmod \pi$ is not a quadratic residue in $\mathbb{F}_p$. In particular, we conclude that there are exactly 3 quadratic extensions of K (in some fixed algebraic closure of K). This is in stark contrast with a global field, such as $\mathbb{Q}$ or $\mathbb{F}_p[t]$, which have infinitely many non-isomorphic quadratic extensions (obtained, for instance, by adjoining the square roots of different prime elements).
A more careful analysis (exercise!) shows that the group $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$, with generators given by the images of $-1, 2, 3$.

Next we give an application of Hensel's lemma to quadratic forms. First we need some background in quadratic forms over finite fields.

Example 2.4 (Quadratic Forms over Finite Fields) Let q be a power of an odd prime. Then any quadratic form with at least 3 variables over $\mathbb{F}_q$ is **isotropic**, i.e., it represents zero non-trivially. In fact,

we may assume that the quadratic form is of the form $ax^2 + by^2 + z^2$ with $a, b \neq 0$. Since $\mathbb{F}_q^\times$ is cyclic, there are exactly $(q-1)/2$ squares in $\mathbb{F}_q^\times$ and therefore the sets

$$\{ax^2 \mid x \in \mathbb{F}_q\} \qquad \text{and} \qquad \{-by^2 - 1 \mid y \in \mathbb{F}_q\}$$

have both cardinality $(q+1)/2$. Hence they must intersect non-trivially, yielding a nontrivial solution of $ax^2 + by^2 + z^2 = 0$. On the other hand, there exist **anisotropic** quadratic forms in 2 variables: just take any non-square $u \in \mathbb{F}_q$, and consider the quadratic form $x^2 - uy^2$.

Now we use Hensel's lemma to derive a similar result over a local field.

Example 2.5 (Quadratic Forms over Local Fields) Let K be either $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$ with p an odd prime. Let A be its valuation ring and π be a uniformiser. Let u be a non-square unit so that $\{1, u, \pi, u\pi\}$ are representatives of the elements in $K^\times/(K^\times)^2$. We claim that the quadratic form

$$\phi(w, x, y, z) = w^2 - u \cdot x^2 - \pi \cdot y^2 + u\pi \cdot z^2$$

is anisotropic. In fact, suppose that $\phi(w, x, y, z) = 0$ has a nontrivial solution (w_0, x_0, y_0, z_0). Multiplying this solution by a convenient power of π we may assume that $w_0, x_0, y_0, z_0 \in A$ and at least one of them is a unit. Now we have two cases. If either w_0 or x_0 is a unit, then reducing $\bmod \pi$, we obtain that the quadratic form $w^2 - \bar{u}x^2$ over $\mathbb{F}_p$ is isotropic, a contradiction. On the other hand, if both w_0 and x_0 are multiples of π, say $w_0 = \pi w_0'$ and $x_0 = \pi x_0'$ with $w_0', x_0' \in A$, then $\pi({w_0'}^2 - u{x_0'}^2) - (y_0^2 - uz_0^2) = 0$. But now either y_0 or z_0 is a unit, and we get a contradiction as in the previous case.
Now we show that every quadratic form $\phi(x_1, \ldots, x_n) = a_1x_1^2 + \cdots + a_nx_n^2$ over K in $n \geq 5$ variables is isotropic. Since $\{1, u, \pi, u\pi\}$ represent the elements in $K^\times/(K^\times)^2$, in order to show that ϕ is isotropic we may assume that each $a_i \in \{1, u, \pi, u\pi\}$. Hence we may write $\phi = \psi_1 + \pi \cdot \psi_2$ where ψ_1 and ψ_2 are quadratic forms whose coefficients are units in A. Hence it is enough to show that any quadratic form in 3 variables whose coefficients are units is isotropic.
Wlog let $\psi(x, y, z) = ux^2 + vy^2 + z^2$ be such a quadratic form where $u, v \in A^\times$ are arbitrary units. By the previous example, we have that the congruence $\psi(x, y, z) \equiv 0 \pmod{\pi}$ has a nontrivial solution $(x_0, y_0, z_0) \not\equiv (0, 0, 0) \pmod{\pi}$. But then

$$\Big(\frac{\partial\psi}{\partial x}(x_0), \frac{\partial\psi}{\partial y}(y_0), \frac{\partial\psi}{\partial z}(z_0)\Big) = (2x_0, 2y_0, 2z_0) \not\equiv (0, 0, 0) \pmod{\pi}$$

and therefore Hensel's lemma implies that $\psi(x, y, z) = 0$ has a nontrivial solution, as required.
A more careful analysis (left to the reader, of course!) shows that for $K = \mathbb{Q}_2$ the result still holds: every quadratic form over $\mathbb{Q}_2$ in 5 or more variables is isotropic.

Example 2.6 (Quaternion Algebras) In the preceding example, the fact that $\phi(w, x, y, z) = w^2 - u \cdot x^2 - \pi \cdot y^2 + u\pi \cdot z^2$ is anisotropic allows us to construct a nontrivial quaternion algebra over the local field K: just take

$$\Big(\frac{u, \pi}{K}\Big) \stackrel{\text{df}}{=} \{a + bi + cj + dij \mid a, b, c, d \in K, \quad i^2 = u, \quad j^2 = \pi, \quad ij = -ji\}$$

This is a division algebra since the reduced norm of $a + bi + cj + dij$ is

$$\phi(a, b, c, d) = (a + bi + cj + dij)(a - bi - cj - dij) = a^2 - ub^2 - \pi c^2 + u\pi d^2$$

which is never zero for $a+bi+cj+dij \neq 0$ as we have seen. Therefore we have that any $a+bi+cj+dij \neq 0$ is invertible:

$$(a + bi + cj + dij)^{-1} = \frac{a - bi - cj - dij}{\phi(a, b, c, d)}$$

Later we will see that this the only nontrivial quaternion algebra over K up to isomorphism. Again, this is in stark contrast with the global field case, for which there are always infinitely many non-isomorphic quaternion algebras (but is close to the real case: there is just one nontrivial quaternion algebra over $\mathbb{R}$).

Example 2.7 (Roots of Unity) Here we show that the group of roots of unity of $\mathbb{Q}_p$ has order $p-1$ for p odd. Consider $f(x) = x^{p-1} - 1 \in \mathbb{Z}_p[x]$. Since the image $\bar{f}(x) \in \mathbb{F}_p[x]$ of $f(x)$ splits completely and $\bar{f}'(r_0) = -r_0^{p-2} \neq 0$ for any root $r_0 \in \mathbb{F}_p$ of $\bar{f}(x) = 0$ (namely any $r_0 \in \mathbb{F}_p^\times$), by Hensel's lemma each element of $\mathbb{F}_p^\times$ lifts to a root of $f(x)$ (these are called **Teichmüller lifts**), and hence $f(x)$ splits completely in $\mathbb{Z}_p[x]$. Hence $\mathbb{Q}_p$ contains all the $(p-1)$-th roots of unity.
Next we show that $\mathbb{Q}_p$ does not contain any primitive n-th root of unity with $p \mid n$. It is enough to show that the cyclotomic polynomial $g(x) = x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible over $\mathbb{Q}_p[x]$, but this follows from the usual combination of Gauß' lemma and Eisenstein's criterion applied to $g(x+1)$.
Finally, assume that $p \nmid n$ and that there exists a primitive n-th root of unity $\zeta \in \mathbb{Q}_p$. We show that $n \mid (p-1)$. First, observe that ζ has valuation 0 and hence $\zeta \in \mathbb{Z}_p^\times$. Second, we claim that reduction modulo p is injective when restricted to the subgroup of $\mathbb{Z}_p^\times$ generated by ζ. In fact, if $\zeta^i \equiv 1 \pmod{p}$ but $\zeta^i \neq 1$ then we would get a contradiction $0 = \zeta^{i(n-1)} + \zeta^{i(n-2)} + \cdots + \zeta^i + 1 \equiv n \pmod{p}$. Therefore $\zeta \bmod p$ has order n in $\mathbb{F}_p^\times$. But by "Fermat's little theorem" we also have $\zeta^{p-1} \equiv 1 \pmod{p}$, and it follows that $n \mid (p-1)$.
A variation of the above argument (again left to the reader) shows that ± 1 are the only roots of unity in $\mathbb{Q}_2$.

Example 2.8 (Automorphisms of $\mathbb{Q}_p$) It is easy to show that any *continuous* field automorphism ϕ of $\mathbb{Q}_p$ has to be the identity: since ϕ restricts to the identity on $\mathbb{Q}$, if $(a_n)_{n\geq 1}$ is a sequence of rational numbers converging to any given $a \in \mathbb{Q}_p$ we have that $\phi(a) = \lim_{n\to\infty} \phi(a_n) = \lim_{n\to\infty} a_n = a$. However it is not so easy to show that *any* field automorphism of $\mathbb{Q}_p$ is in fact trivial. To prove that, we first show that $a \in \mathbb{Z}_p^\times$ if and only if the equation $x^n = a^{p-1}$ can be solved in $\mathbb{Q}_p$ for infinitely many $n \geq 1$. In fact, if a is a unit then $a^{p-1} \equiv 1 \pmod{p}$ and Hensel's lemma shows that $x_0 = 1 \bmod p$ lifts to a solution of $x^n = a^{p-1}$ for all n not divisible by p. Conversely, denote by v the p-adic valuation. Since $x^n = a^{p-1}$ implies that $n \mid (p-1)\cdot v(a)$, if this equation can be solved for infinitely many n then necessarily $v(a) = 0$. Hence if ϕ is a field automorphism of $\mathbb{Q}_p$ it must take units to units. Writing an element $a \in \mathbb{Q}_p^\times$ as $a = p^n u$ with $u \in \mathbb{Z}_p^\times$ and using the fact that ϕ restricts to the identity on $\mathbb{Q}$, we have that $\phi(a) = p^n u'$ for some unit u'. Hence ϕ preserves the valuation and is therefore continuous, and so it has to be the identity.

Finally we show how one may refine Hensel's lemma in order not only to lift roots but also factorisations. The punchline is:

Hensel: "Separable factorisations in the residue field lift"

Lemma 2.9 (Hensel, revisited) *Let K be a complete valued field with valuation ring A. Let $\mathfrak{m}$ be the maximal ideal and $k = A/\mathfrak{m}$ be the residue field of A. Denote the image of a polynomial $p \in A[x]$ in $A[x]/\mathfrak{m}A[x] = k[x]$ by $\bar{p}$. Let $f(x) \in A[x]$ with $\bar{f} \neq 0$ and suppose that $\bar{f}$ factors as*

$$\bar{f}(x) = g_0(x)h_0(x) \qquad \textit{with} \qquad \gcd\big(g_0(x), h_0(x)\big) = 1$$

Then there exist polynomials $g(x), h(x) \in A[x]$ with $\deg g(x) = \deg g_0(x)$ lifting the above factorisation: $f(x) = g(x)h(x)$ with $\bar{g}(x) = g_0(x)$ and $\bar{h}(x) = h_0(x)$.

Proof Write $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $g(x) = b_r x^r + b_{r-1}x^{r-1} + \cdots + b_0$ and $h(x) = c_s x^s + c_{s-1}x^{s-1} + \cdots + c_0$ where the b_i, c_i are indeterminates and $r = \deg g_0(x)$ and $s = n - r$. Expanding $f(x) = g(x)h(x)$ we obtain $n+1$ equations $\sum_{i+j=d} b_i c_j = a_d$, $0 \leq d \leq n$, in the $(r+1)+(s+1) = n+2$ variables b_i, c_j. The Jacobian matrix of this system is the $(n+1) \times (n+2)$ matrix

$$\begin{pmatrix}
b_0 & 0 & 0 & \cdots & 0 & c_0 & 0 & 0 & \cdots & 0 \\
b_1 & b_0 & 0 & \cdots & 0 & c_1 & c_0 & 0 & \cdots & 0 \\
b_2 & b_1 & b_0 & \cdots & 0 & c_2 & c_1 & c_0 & \cdots & 0 \\
\vdots & & & & & \vdots & & & & \\
0 & 0 & 0 & \cdots & b_0 & 0 & 0 & 0 & \cdots & \vdots \\
 & & & & \vdots & & & & & \\
0 & 0 & 0 & \cdots & b_r & 0 & 0 & 0 & \cdots & c_s
\end{pmatrix}$$

Now the coefficients of $g_0(x)$ and $h_0(x)$ give a solution to this system modulo $\mathfrak{m}$, which is a smooth point since the rank of Jacobian matrix evaluated at this point is $n+1$: the determinant of the first $n+1$ columns is non-zero since b_r assumes a non-zero value (recall that $r = \deg g_0(x)$) and the $n \times n$ matrix obtained by suppressing the r-th column and the last line is the resultant of the relatively prime polynomials $g_0(x)$ and $h_0(x)$. □

Corollary 2.10 *Keep the above notation and let v be the valuation of K. If*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

is an irreducible polynomial in $K[x]$ then

$$\min_{0\le i\le n} v(a_i) = \min\{v(a_0), v(a_n)\}$$

In particular, if $a_n = 1$ and $a_0 \in A$ then $a_i \in A$ for all i.

Proof Choose the smallest integer i for which $v(a_i)$ is minimal and let us show that $0 < i < n$ yields a contradiction. We have that $p(x) \stackrel{\text{df}}{=} a_i^{-1} \cdot f(x) \in A[x]$ is such that $\bar{p} \neq 0$ in $k[x]$. But then we have a factorisation $\bar{p}(x) = x^i g_0(x)$ with $g_0(0) = 1$ and hence x^i and $g_0(x)$ are relatively prime. By Hensel's lemma $p(x)$ factors in $A[x]$ non-trivially (since $0 < i < n$), which is impossible since $f(x) = a_i \cdot p(x)$ is irreducible in $K[x]$. □

3 Local fields in general

By now you may be wondering: what is a local field after all?

Definition 3.1 A finite field extension L of either $\mathbb{F}_p((t))$ or $\mathbb{Q}_p$ is called a **local field**.

Example 3.2 Let q be a power of a prime p. Then $\mathbb{F}_q((t))$ is a local field. By example 2.3 there are exactly 3 local fields of degree 2 over $\mathbb{Q}_p$ when p is odd, and 7 for $p = 2$.

Example 3.3 Although we won't cover global fields in these notes, it is instructive to show how local fields arise from them. For instance, take the ring of Gaußian integers $\mathbb{Z}[i]$ and the maximal ideal (3), with residue field $\mathbb{Z}[i]/(3) \cong \mathbb{F}_9$. Then

$$A = \varprojlim_{n\in\mathbb{N}} \frac{\mathbb{Z}[i]}{(3^n)} = \Big\{(a_n) \in \prod_{n\in\mathbb{N}} \frac{\mathbb{Z}[i]}{(3^n)} \;\Big|\; a_m = a_n \bmod 3^m \text{ for all } n \ge m\Big\}$$

is a local domain with a principal maximal ideal (3). Moreover $\mathbb{Z}[i] \subset A$ by "diagonal embedding" $a \mapsto (a, a, \ldots)$. The unit group of A is $A^\times = A - (3)$, i.e. the subset of A consisting of tuples $(a_1, a_2, \ldots)$ with $a_1 \neq 0 \bmod 3$, and for $f \in A$ one has a prime factorisation $f = 3^n u$ with $u \in A^\times$ so that setting $w(f) = n$ defines a valuation w on the fraction field $K = \operatorname{Frac} A$. As with $\mathbb{Q}_p$, this makes K into a complete valued field. Moreover, choosing a set of representatives S of $\mathbb{Z}[i]/(3) \cong \mathbb{F}_9$, for instance $S = \{a + bi \mid 0 \le a, b < 3\}$, we may uniquely write each element of K as a convergent power series $\sum_{n\ge n_0} s_n 3^n$ with $s_n \in S$.
We now show that K is a local field, actually a quadratic extension of $\mathbb{Q}_3$. First observe that A contains a copy of $\mathbb{Z}_3$ since $\mathbb{Z}/3^n$ is a subring of $\mathbb{Z}[i]/(3^n)$ for all n. Hence $K \supset \mathbb{Q}_3$. Besides $A = \mathbb{Z}_3[i]$ (recall that $\mathbb{Z}[i] \subset A$). But $i^2 = -1$ and $i \notin \mathbb{Q}_3$ since the image of $x^2 + 1$ is irreducible in $\mathbb{F}_3[x]$, so $x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$ and hence in $\mathbb{Q}_3[x]$ by Gauß' lemma. Therefore $K = \mathbb{Q}_3(i)$ is the quadratic extension of $\mathbb{Q}_3$ generated by a root of $x^2 + 1$.

The reason why we spent so much time looking at the two basic examples of the previous section is that virtually all the difficulty in the study of a general local field is already present in those two particular instances. This is no accident: we now show that a general local field L is structurally similar to $K = \mathbb{F}_p((t))$ or $K = \mathbb{Q}_p$ in that it is a complete discretely valued field. The first step is to show how to extend the valuation v of K to a valuation w of L. In fact, there is no wiggle room: the extension is *unique* (Valuative Highlander's Philosophy: "there can be only one [valuation]"). Granting this result, we can easily "guess" a formula for w. For simplicity, assume that L is Galois over K (the general case can be reduced to this one by considering the Galois closure of L). Then for any $\sigma \in \operatorname{Gal}(L/K)$ we have that $w \circ \sigma = w$ since both are valuations extending v. But then for $x \in L$ we have that

$$w\big(N_{L/K}(x)\big) = w\Big(\prod_\sigma \sigma x\Big) = [L:K] \cdot w(x) \Rightarrow w(x) = \frac{1}{[L:K]} \cdot v\big(N_{L/K}(x)\big)$$

Our approach in proving the theorem below will be the opposite one: we will use the "guessed" formula to show the existence of an extension.

Theorem 3.4 (Valuative Highlander's Philosophy) *Let K be a complete discretely valued field with valuation v, and L be a finite extension of K. Then there is a unique valuation w on L extending v. It is given by*

$$\boxed{w(x) = \frac{1}{[L:K]} \cdot v\big(N_{L/K}(x)\big) \qquad \text{for } x \in L}$$

Moreover L is complete with respect to w.

PROOF Let A be the valuation ring of K and let B be the integral closure of A in L (check the appendix for a list of basic results about integral extensions). We first show that

$$B = \{x \in L \mid N_{L/K}(x) \in A\} = \{x \in L \mid v\big(N_{L/K}(x)\big) \geq 0\}$$

Since A is a UFD, it is normal, and hence $N_{L/K}(b) \in A$ for $b \in B$, i.e., $B \subset \{x \in L \mid N_{L/K}(x) \in A\}$. To prove the opposite inclusion, take $x \in L$ with $N_{L/K}(x) \in A$ and let $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in K[t]$ be its minimal polynomial. Since $N_{L/K}(x) = \pm a_0^m$ for some $m > 0$ we must have $v(a_0) \geq 0 \iff a_0 \in A$. By corollary 2.10 we conclude that $f(t) \in A[t]$, i.e., that $x \in B$, as required.

Next we show that the above formula for w defines a valuation on L (with valuation ring equal to B). Clearly $w(xy) = w(x) + w(y)$ and $w(x) = \infty \iff x = 0$, so we just have to show that $w(x+y) \geq \min\{w(x), w(y)\}$ for $x, y \in L$. First observe that we already know the special case $w(x) \geq 0 \Rightarrow w(1+x) \geq 0$. In fact:

$$w(x) = \frac{v\big(N_{L/K}(x)\big)}{[L:K]} \geq 0 \Rightarrow x \in B \Rightarrow 1 + x \in B \Rightarrow w(1+x) = \frac{v\big(N_{L/K}(1+x)\big)}{[L:K]} \geq 0$$

The general case now follows easily: wlog $w(x) \geq w(y)$ and hence $w(x/y) \geq 0 \Rightarrow w(1 + x/y) \geq 0$, i.e., $w(x+y) \geq w(y) = \min\{w(x), w(y)\}$.

Now we show that w is unique. Suppose that w' is another valuation of L extending v. Since w and w' are distinct but agree on K, they must be inequivalent and hence there exists an element $b \in L$ such that $w(b) \geq 0$ but $w'(b) < 0$ (see appendix). Then $b \in B$. Let $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ be its minimal polynomial over K. Since A is normal, $f(t) \in A[t]$. But since $w'(b) < 0$ we obtain a contradiction:

$$0 \leq v(a_0) = w'(a_0) = w'(-b^n - a_{n-1}b^{n-1} \cdots - a_1 b) = w'(b^n) < 0$$

Finally we show that L is complete with respect to w. Let $\omega_1, \ldots, \omega_n$ be a basis of L over K. Let $(x_i)_{i \geq 1}$ be a Cauchy sequence in L and write x_i in terms of the chosen basis: $x_i = y_{i1}\omega_1 + \cdots + y_{in}\omega_n$, $y_{ij} \in K$. Since K is complete and L is finite dimensional over K, we have that all norms on L are equivalent (exercise!) and hence using for instance the sup norm we conclude that, for each j, $(y_{ij})_{i \geq 1}$ is a Cauchy sequence in K. Hence this sequence converges to an element $y_j \in K$ and $(x_i)_{i \geq 1}$ converges to $y_1\omega_1 + \cdots + y_n\omega_n$ in L, completing the proof that L is complete! □

Thanks to the Valuative Highlander's Philosophy, the results of the previous section hold mutatis mutandis for any local field, for their proofs were based solely on properties of general complete valued fields. In particular we still have at our disposal Calculus Student's Psychedelic Dream and Hensel's lemma and all their wonderful consequences in our more general setting.

Definition 3.5 Let K be a local field with valuation v. Let L be a finite field extension of K and w be the unique extension of v to L. Let π and Π be uniformisers of K and L, and denote by k and l the residue fields of K and L respectively. We define the **ramification degree** $e_{L/K}$ of the extension $L \supset K$ to be the index of the value group of v in the value group of w:

$$\boxed{e_{L/K} = [w(L^\times) : v(K^\times)]}$$

In other words, we have the factorisation $\pi = u\Pi^{e_{L/K}}$ for $u \in L$ with $w(u) = 0$.
Observe that since w restricts to v in K we may view k as a subfield of l. We define the **inertia degree** $f_{L/K}$ of the extension $L \supset K$ to be the degree of the corresponding extension of residue fields:

$$\boxed{f_{L/K} = [l : k]}$$

Since index of groups and degree of extensions are multiplicative, the same holds for the ramification and the inertia degrees: given finite extensions $M \supset L \supset K$ of local fields we have that

$$\boxed{e_{M/K} = e_{M/L} \cdot e_{L/K} \qquad \text{and} \qquad f_{M/K} = f_{M/L} \cdot f_{L/K}}$$

Definition 3.6 A finite extension of local fields $L \supset K$ is **unramified** if its ramification degree is $e_{L/K} = 1$. In other words, $L \supset K$ is unramified if a uniformiser of K is still a uniformiser of L. On the other hand, if the ramification degree is as large as possible, i.e., $e_{L/K} = [L : K]$, then the extension is said to be **totally ramified**.

Example 3.7 Let e and f be positive integers and write $K = \mathbb{F}_p((t))$ and $L = \mathbb{F}_{p^f}((t))(t^{1/e})$ where $t^{1/e}$ denotes an e-th root of t (in some algebraic closure of K). Let w be the unique valuation on L extending the valuation v on K. Then $w(t^{1/e}) = 1/e$ and using the fact that L is basically a "power series ring" in $t^{1/e}$ it is easy to show that the valuation ring of w is $\mathbb{F}_{p^f}[[t]][t^{1/e}]$ with residue field $\mathbb{F}_{p^f}$. Therefore $L \supset K$ has inertia degree f and ramification degree e. Observe that $L \supset K$ breaks into two parts: an *unramified extension* $M \supset K$ where $M = \mathbb{F}_{p^f}((t))$ and a *totally ramified extension* $L \supset M$.

$$\begin{array}{rl} & L = \mathbb{F}_{p^f}((t^{1/e})) \\ \text{totally ramified} & \Big| \, e \\ & M = \mathbb{F}_{p^f}((t)) \\ \text{unramified} & \Big| \, f \\ & K = \mathbb{F}_p((t)) \end{array}$$

Later we will show that any extension of local fields admits such a decomposition.

Example 3.8 Let p be an odd prime and $u \in \mathbb{F}_p$ be a non-square. By example 2.3, there are 3 quadratic extensions of $K = \mathbb{F}_p((t))$, namely $L_1 = K(\sqrt{u})$, $L_2 = K(\sqrt{t})$ and $L_3 = K(\sqrt{ut})$. Since $\mathbb{F}_p(\sqrt{u}) = \mathbb{F}_{p^2}$ we have that $L_1 = \mathbb{F}_{p^2}((t))$ and t is a uniformiser for both K and L_1, that is, $L_1 \supset K$ is unramified with inertia degree $f_{L_1/K} = [\mathbb{F}_{p^2} : \mathbb{F}_p] = 2$. On the other hand, if w_2 and w_3 are the extensions of the valuation v of K to L_2 and L_3 respectively we must have that $w_2(\sqrt{t}) = w_3(\sqrt{ut}) = 1/2$ since $w_2(t) = w_3(ut) = 1$, showing that both $L_2 \supset K$ and $L_3 \supset K$ are totally ramified. By the proof of the Valuative Highlander's Philosophy, the valuation rings of w_2 and w_3 are the integral closures of $\mathbb{F}_p[[t]]$ in L_2 and L_3, which can easily be shown to be $\mathbb{F}_p[[t]](\sqrt{t})$ and $\mathbb{F}_p[[t]](\sqrt{ut})$ respectively and thus can be viewed as the rings of "power series" in the uniformisers $\sqrt{t}$ and $\sqrt{ut}$ with residue field $\mathbb{F}_p$. Therefore the inertia degrees of $L_2 \supset K$ and $L_3 \supset K$ are both 1.
A similar computation shows that $\mathbb{Q}_p$ has exactly 1 unramified quadratic extension and 2 totally ramified quadratic extensions. For $\mathbb{Q}_2$, of its 7 quadratic extensions, exactly 1 is unramified and the other 6 are totally ramified.

Observe that for each extension in the last example the product of the ramification and inertia degrees was always 2, the degree of the extension. Magic? Coincidence? Or would it be

Theorem 3.9 *Let $L \supset K$ be a degree n extension of complete discretely valued fields. Let v be the valuation of K and w be its unique extension to L. Denote by A and B the valuation rings of v and w, π and Π be uniformisers of A and B, and $k = A/(\pi)$ and $l = B/(\Pi)$ be their residue fields respectively.*

Then the ramification and inertia degrees e and f of $L \supset K$ are finite. Moreover B is the integral closure of A in L and, as an A-module, it is free of rank n. A basis is given by $\{\omega_i \Pi^j \mid 1 \leq i \leq f, 0 \leq j < e\}$, where $\omega_1, \ldots, \omega_f \in B$ are representatives of a basis of l over k. In particular we have the relation

$$\boxed{ef = n}$$

Proof We normalise $v(\pi) = w(\pi) = 1$ and $w(\Pi) = 1/e$. We have already seen in the proof of the Valuative Highlander's Philosophy that B is the integral closure of A in L. Also it is clear from the explicit formula for w that $e \leq n$. Now we show that f is also finite and that $ef \leq n$. Let $\omega_1, \ldots, \omega_r \in B$ be elements whose images in l are linearly independent over k. Then it is enough to show that the set $\{\omega_i \Pi^j \mid 1 \leq i \leq r, 0 \leq j < e\}$ is linearly independent over K. Given any dependency relation

$\sum_{ij} a_{ij}\omega_i\Pi^j = 0$ with $a_{ij} \in K$, by clearing out the denominators we may assume that all $a_{ij} \in A$ and that at least one of them is a unit. Let j_0 be the smallest integer such that $a_{ij_0} \in A^\times$ for at least one i, and thus $\sum_i a_{ij_0}\omega_i \not\equiv 0 \pmod{\Pi}$ by the linear independence of the $\omega_i \bmod \Pi$. Then

$$w\Big(\sum_i a_{ij}\omega_i\Pi^j\Big) > w\Big(\sum_i a_{ij_0}\omega_i\Pi^{j_0}\Big) = \frac{j_0}{e} \qquad \text{for all } j \neq j_0$$

This is clear for $j > j_0$ and for $j < j_0$ one has that $\sum_i a_{ij}\omega_i \in \pi B$ and therefore $w(\sum_i a_{ij}\omega_i\Pi^j) \geq 1 > j_0/e$. From the strong triangle inequality, $w(\sum_{ij} a_{ij}\omega_i\Pi^j) = j_0/e$ and hence $\sum_{ij} a_{ij}\omega_i\Pi^j$ cannot be zero, a contradiction.

Next we show that any element $b \in B$ can be written (uniquely by the above) as an A-linear combination of $\{\omega_i\Pi^j \mid 1 \leq i \leq f, 0 \leq j < e\}$. For that we show that given any $b \in B$ we can find an A-linear combination c_0 of the $\omega_i\Pi^j$ such that $b = c_0 + b_1\pi$ for some $b_1 \in B$. Granting this fact, the proof then follows: by the same token $b_1 = c_1 + b_2\pi$ with c_1 in the A-span of the $\omega_i\Pi^j$ and so $b = c_0 + c_1\pi + b_2\pi^2$, and inductively we can write $b = c_0 + c_1\pi + c_2\pi^2 + \cdots + c_n\pi^n + b_{n+1}\pi^{n+1}$ where the "error term" $b_{n+1}\pi^{n+1}$ approaches zero. By the Calculus Student's Psychedelic Dream, we have that $b = c_0 + c_1\pi + c_2\pi^2 + \cdots$, which is in the A-span of the $\omega_i\Pi^j$ again by the Psychedelic Dream, this time applied to K.

We have thus to show that $B/\pi B$ is generated over $k = A/(\pi)$ by the images of the $\omega_i\Pi^j$. Wlog we may assume that $b \in B - \pi B$ so that $0 \leq w(b) < 1$. Hence we may write $b = \Pi^j u$ for $j = e \cdot w(b)$ and some unit $u \in B^\times$. Now we can find $a_{ij} \in A$ such that $u \equiv \sum_i a_{ij}\omega_i \pmod{\Pi}$ and therefore $b = \sum_i a_{ij}\omega_i\Pi^j + b'$ with $w(b') > w(b)$. If $w(b') \geq 1 \iff b' \in \pi B$ then we are done. Otherwise we repeat the procedure with b'. Since the valuations of the "tails" are increasing, we must eventually stop.

So far we have shown that B is a free A-module of rank ef with basis $\{\omega_i\Pi^j \mid 1 \leq i \leq f, 0 \leq j < e\}$, which is also linearly independent over K. To finish the proof, we have to show that any $c \in L$ is in the K-span of this set. But $c\pi^m \in B$ for m sufficiently large, and we are done. □

Remark 3.10 When L is separable over K, the above is a particular case of the well-known formula $n = \sum_i e_i f_i$ for extensions of Dedekind domains (see any Number Theory book in the bibliography), except that our situation is much simpler since there is just one prime to deal with.

Now we introduce some important notation that will be used throughout.

Definition 3.11 Let K be a local field with valuation v. For $i \geq 1$ write

$$\begin{aligned}
O_K &\stackrel{\text{df}}{=} \text{valuation ring of } v = \{x \in K \mid v(x) \geq 0\} \\
U_K &\stackrel{\text{df}}{=} \text{group of units of } O_K = \{x \in O_K \mid v(x) = 0\} \\
\mathfrak{m}_K &\stackrel{\text{df}}{=} \text{maximal ideal of } O_K = \{x \in O_K \mid v(x) > 0\} \\
U_K^{(i)} &\stackrel{\text{df}}{=} 1 + \mathfrak{m}_K^i = \text{closed ball } \{x \in K \mid |x-1|_v \leq 2^{-i}\} \text{ centred at } 1 \\
&\quad = \text{open ball } \{x \in K \mid |x-1|_v < 2^{-i+1}\} \text{ centred at } 1
\end{aligned}$$

We also extend the last definition to $i = 0$ by setting $U_K^{(0)} = U_K$. Observe that the $U_K^{(i)}$ are subgroups of U_K and that their translates form a topological basis of U_K.

Fix a uniformiser π and let $k = O_K/\mathfrak{m}_K$ be the (finite) residue field of K. Denote by k^+ (respectively $k^\times$) the additive (respectively multiplicative) group of k. For U_K we have a filtration

$$U_K = U_K^{(0)} \supset U_K^{(1)} \supset U_K^{(2)} \supset U_K^{(3)} \supset \cdots$$

with quotients

$$\boxed{\frac{U_K}{U_K^{(1)}} = k^\times \qquad (u \bmod U_K^{(1)} \mapsto u \bmod \mathfrak{m}_K)}$$

and

$$\boxed{\frac{U_K^{(i)}}{U_K^{(i+1)}} \cong k^+ \qquad (u = 1 + a\pi^{i+1} \bmod U_K^{(i+1)} \mapsto a \bmod \mathfrak{m}_K)}$$

The first isomorphism is canonical, but the second is not since it depends on the choice of the uniformiser π. In any case, it can be made canonical if we consider instead the isomorphism $U_K^{(i)}/U_K^{(i+1)} = \mathfrak{m}_K^i/\mathfrak{m}_K^{i+1}$ given by $u \bmod U_K^{(i+1)} \mapsto u - 1 \bmod \mathfrak{m}_K^{i+1}$.

Just to make sure we understand the notation above, take for instance $K = \mathbb{Q}_p$ with uniformiser $\pi = p$. Then $O_K = \mathbb{Z}_p$, $\mathfrak{m}_K = (p)$, $U_K = \mathbb{Z}_p^\times = \mathbb{Z}_p - (p)$, and $U_K^{(i)}$ is the set of p-adic integers of the form $1 + a_i p^i + a_{i+1}p^{i+1} + \cdots$ with $0 \le a_j < p$. The isomorphism $U_K/U_K^{(1)} = k^\times$ takes the class of $a_0 + a_1 p + a_2 p^2 + \cdots$, $0 \le a_j < p$, to $a_0 \bmod p$, and the isomorphism $U_K^{(i)}/U_K^{(i+1)} \cong k^+$ takes the class of $1 + a_i p^i + a_{i+1}p^{i+1} + \cdots$, $0 \le a_j < p$, to $a_i \bmod p$.

It is easy to check that we have an isomorphism, both algebraic and topological,

$$U_K = \varprojlim_{i \ge 1} \frac{U_K}{U_K^{(i)}}$$

and hence U_K is a **profinite group** (that is, a projective limit of finite groups). In particular, we have that U_K is compact.

4 Structure of group of units

In this section we describe the structure of the multiplicative group of a local field K. First of all the valuation v on K gives rise to an exact sequence

$$1 \longrightarrow U_K \longrightarrow K^\times \xrightarrow{v} \mathbb{Z} \to 0$$

which admits a splitting $s\colon \mathbb{Z} \to K^\times$ given by a choice of a uniformiser π. Hence we have a non-canonical isomorphism $K^\times \cong U_K \times \mathbb{Z}$ and we are left to describe the structure of U_K.

Let $\mathbb{F}_q$ be the residue field of K, where q is a power of a prime p. We have an exact sequence

$$1 \longrightarrow U_K^{(1)} \longrightarrow U_K \longrightarrow \mathbb{F}_q^\times \longrightarrow 1$$

Here the last map is just the reduction modulo $\mathfrak{m}_K$. This sequence splits *canonically*: in fact, by Hensel's lemma each element in $\mathbb{F}_q^\times$ lifts to a *uniquely* determined $(q-1)$-th root of unity in K (the so-called **Teichmüller lifts**, see example 2.7). Hence we may write $U_K = \mu_{q-1} \times U_K^{(1)}$, where μ_{q-1} denotes the subgroup of $(q-1)$-th roots of unity in $K^\times$. We have thus reduced the problem to finding the structure of $U_K^{(1)}$.

First observe that $U_K^{(1)}$ is a continuous $\mathbb{Z}_p$-module, with $\mathbb{Z}_p$ acting by exponentiation. In fact, given $u \in U_K^{(1)}$ and $a \in \mathbb{Z}_p$ we may define

$$u^a \stackrel{\text{df}}{=} \lim_{n \to \infty} u^{a_n}$$

where $(a_n)_{n \ge 1}$ is any sequence of integers converging to a. This makes sense because

$$U_K = \varprojlim_{i \ge 1} \frac{U_K^{(1)}}{U_K^{(i+1)}} \qquad \text{and} \qquad \mathbb{Z}_p = \varprojlim_{i \ge 1} \frac{\mathbb{Z}}{(q^i)}$$

and from the isomorphism $U_K^{(i)}/U_K^{(i+1)} \cong \mathbb{F}_q^+$ we conclude that $U_K^{(1)}/U_K^{(i+1)}$ is a finite group of cardinality q^i, i.e., a $\mathbb{Z}/(q^i)$-module. Hence writing $u = (u_1, u_2, \ldots)$, $u_i \in U_K^{(1)}/U_K^{(i+1)}$, and $a = (a_1, a_2, \ldots)$, $a_i \in \mathbb{Z}/(q^i)$, we have that $u^a = (u_1^{a_1}, u_2^{a_2}, \ldots)$ under the above isomorphisms.

From now on we will concentrate on the case $\operatorname{char} K = 0$ and leave the positive characteristic case as an exercise. We show using "p-adic Lie Theory" that $U_K^{(1)}$ is in fact finitely generated as a $\mathbb{Z}_p$-module. Since $\mathbb{Z}_p$ is a PID, $U_K^{(1)}$ will break into a torsion part (roots of unity) and a free part, and then we will be left to compute the rank of this free part. In order to "Lie-nearise" $U_K^{(1)}$, we make use of the p-adic logarithmic and exponential functions:

Lemma 4.1 *Let K be a local field of char 0 with valuation v and residue field of char p. Consider the power series*

$$\log(1+x) \stackrel{\text{df}}{=} x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots$$
$$\exp x \stackrel{\text{df}}{=} 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots$$

Then $\log(1+x)$ converges for all x with $v(x) > 0$ while $\exp x$ converges for all x with $v(x) > v(p)/(p-1)$. Hence for i sufficiently large we have a continuous isomorphism of $\mathbb{Z}_p$-modules

$$\boxed{U_K^{(i)} \underset{\exp}{\overset{\log}{\rightleftarrows}} \mathfrak{m}_K^i}$$

Notice that while $U_K^{(i)}$ is a multiplicative $\mathbb{Z}_p$-module with action given by exponentiation, $\mathfrak{m}_K^i$ is an additive $\mathbb{Z}_p$-module with action given by multiplication.

PROOF Let $n \geq 1$ and write $n = p^k m$ with $p \nmid m$. We have that

$$v(n) = v(p) \cdot k \leq v(p) \cdot \log_p n$$

while

$$v(n!) = v(p) \cdot \left(\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \right) \leq v(p) \cdot \frac{n/p}{1 - 1/p} = \frac{v(p) \cdot n}{p-1}$$

Therefore if $v(x) > 0$ then

$$v\Big(\frac{x^n}{n}\Big) = n \cdot v(x) - v(n) \geq n - v(p) \cdot \log_p n \to \infty$$

as $n \to \infty$, while if $v(x) > v(p)/(p-1)$ then

$$v\Big(\frac{x^n}{n!}\Big) = n \cdot v(x) - v(n!) \geq n \cdot \Big(v(x) - \frac{v(p)}{p-1}\Big) \to \infty$$

as $n \to \infty$. The convergence of $\log(1+x)$ and $\exp x$ now follows from Calculus Student's Psychedelic Dream.

Finally it is easy to show that for i sufficiently large the two functions $\log\colon U_K^{(i)} \to \mathfrak{m}_K^i$ and $\exp\colon \mathfrak{m}_K^i \to U_K^{(i)}$ are inverse of each other and are compatible with the $\mathbb{Z}_p$-action, so we are done. □

The lemma shows that $U_K^{(i)} \cong \mathfrak{m}_K^i$ for i sufficiently large. But we have an isomorphism $O_K \cong \mathfrak{m}_K^i$ of $\mathbb{Z}_p$-modules given by multiplication by π^i. On the other hand we know that O_K is free over $\mathbb{Z}_p$ of rank $[K : \mathbb{Q}_p]$ by theorem 3.9, and hence so is $U_K^{(i)}$.

Now since $U_K^{(i)}/U_K^{(i+1)} = k^+$ for $i \geq 1$, we have that $[U_K^{(1)} : U_K^{(i)}]$ is finite for all $i \geq 1$. Therefore $U_K^{(1)}$ contains a finite index $\mathbb{Z}_p$-submodule which is free of rank $[K : \mathbb{Q}_p]$. This proves that $U_K^{(1)}$ is finitely generated as a $\mathbb{Z}_p$-module. The free part of $U_K^{(1)}$ has rank $[K : \mathbb{Q}_p]$ and its torsion part is a cyclic p-group $\mathbb{Z}_p/p^r = \mathbb{Z}/p^r$ for some r (it is cyclic because it is isomorphic to a torsion subgroup of $K^\times$). Putting everything together, we have just shown

Theorem 4.2 (Structure of group of units) *Let K be a local field with residue field $\mathbb{F}_q$ where q is a power of a prime p. If $\operatorname{char} K = 0$ then there is a non-canonical isomorphism, both algebraic and topological,*

$$\boxed{K^\times \cong \mathbb{Z} \times \mu_K \times \mathbb{Z}_p^{[K:\mathbb{Q}_p]}}$$

where μ_K is the finite cyclic group of roots of units in $K^\times$ with $|\mu_K| = (q-1)p^r$ for some r.

If $\operatorname{char} K = p$ then there is a non-canonical isomorphism, both algebraic and topological,

$$\boxed{K^\times \cong \mathbb{Z} \times \mu_K \times \mathbb{Z}_p^{\mathbb{N}}}$$

where μ_K is the finite cyclic group of roots of units in $K^\times$ with $|\mu_K| = (q-1)$.

We (meaning of course I) won't do the positive characteristic case, since it is a bit more involved. But we indicate how to construct the isomorphism $U_K^{(1)} \cong \mathbb{Z}_p^{\mathbb{N}}$. Let $\omega_1, \dots, \omega_f$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. For any n not divisible by p define a continuous morphism $g_n \colon \mathbb{Z}_p^f \to U_K^{(n)}$ by

$$g_n(a_1, \dots, a_f) = \prod_{1 \le i \le f} (1 + \omega_i t^n)^{a_i}$$

The required isomorphism $g \colon \mathbb{Z}_p^{\mathbb{N}} \to U_K^{(1)}$ is then given by the convergent product

$$g = \prod_{p \nmid n} g_n \colon \prod_{p \nmid n} \mathbb{Z}_p^f \to U_K^{(1)}$$

The necessary verifications are left as an exercise to the reader (for the lazy one, the answer can be found in the excellent book by Neukirch, page 140).

5 Extensions of Local Fields

We conclude this chapter with a study of extension of local fields. We begin with a result showing that "unramified extensions are stable under base change".

Theorem 5.1 *Let K be a local field, $L \supset K$ be a finite unramified extension and let K' be an arbitrary finite extension of K. If $L' = LK'$ is the compositum of L and K' (in some algebraic closure of K) then $L' \supset K'$ is also unramified.*

Proof Denote by k, k', l and l' the residue fields of K, K', L and L' respectively. By theorem 3.9, we know that $O_L = O_K[\theta]$ where $\theta \in O_L$ is such that its image $\bar{\theta} \in l$ is a primitive element over k. Since O_L is integral over O_K, we have that θ is integral over the normal rings O_K and $O_{K'}$ and hence the minimal polynomials $p(x)$ and $q(x)$ of θ over K and K' belong to $O_K[x]$ and $O_{K'}[x]$ respectively. Also the image $\bar{p}(x) \in k[x]$ is the minimal polynomial of $\bar{\theta}$ since $l = k(\bar{\theta})$ and $\deg \bar{p}(x) = \deg p(x) = [L : K] = [l : k]$. Since $q(x) \mid p(x)$ in $O_{K'}[x]$, the image $\bar{q}(x) \in k'[x]$ of $q(x)$ is such that $\bar{q}(x) \mid \bar{p}(x)$ in $k'[x]$. But $\bar{p}(x)$ is separable since k is perfect, hence $\bar{q}(x)$ is separable as well. Since $q(x)$ is irreducible in $K'[x]$, we conclude by Hensel's lemma that $\bar{q}(x)$ is irreducible in $k'[x]$ and hence it is the minimal polynomial of $\bar{\theta} \in l'$ over k'. Therefore, since $L' = K'(\theta)$, we have that

$$f_{L'/K'} \ge [k'(\bar{\theta}) : k'] = \deg \bar{q}(x) = \deg q(x) = [L' : K']$$

On the other hand, $f_{L'/K'} \le [L' : K']$ in general, so we must have equality, proving that $L' \supset K'$ is indeed unramified. □

In particular, the last proposition shows that the compositum of unramified extensions is unramified. Hence every extension $L \supset K$ of local fields can be split into two extensions $L \supset M \supset K$ where M is the **maximal unramified extension** of K in L. We have that $M \supset K$ is unramified while $L \supset M$ is totally ramified, hence $[L : M] \mid e_{L/K}$ and $[M : K] \mid f_{L/K}$. On the other hand, $e_{L/K} \cdot f_{L/K} = [L : K] = [L : M] \cdot [M : K]$, therefore we conclude that $[L : M] = e_{L/K}$ and $[M : K] = f_{L/K}$. This shows that the picture in example 3.7 holds in general.

Remark 5.2 The compositum of two totally ramified extensions need not be totally ramified. Hence there is not such a thing as a "maximal totally ramified extension."

Next we concentrate on Galois extensions. We begin with a

Definition 5.3 Let $L \supset K$ be a Galois extension of local fields with $G = \mathrm{Gal}(L/K)$. Note that since any $\sigma \in G$ preserves the valuation of L, $\sigma(O_L) \subset O_L$ and $\sigma(\mathfrak{m}_L^{i+1}) \subset \mathfrak{m}_L^{i+1}$, hence σ acts on $O_L/\mathfrak{m}_L^{i+1}$ for $i \ge 0$. We define the i-th **higher ramification group** to be the subgroup G_i of G consisting of those automorphims $\sigma \in G$ having trivial action on $O_L/\mathfrak{m}_L^{i+1}$. The group G_0 is called **inertia group**.

The higher ramification groups give a filtration

$$G_{-1} \overset{\mathrm{df}}{=} G \supset G_0 \supset G_1 \supset G_2 \supset G_3 \supset \cdots$$

of the Galois group G. Observe that this filtration is **exhaustive** (i.e. G_i is trivial for i sufficiently large): if $\omega_1, \dots, \omega_n \in O_L$ is a basis of L over K, if $\sigma \ne 1$ then $\sigma(\omega_j) \ne \omega_j$ for some j and hence $\sigma(\omega_j) \not\equiv \omega_j \pmod{\mathfrak{m}_L^{i+1}} \iff \sigma \notin G_i$ for i sufficiently large. Also observe that $G_{i+1} \trianglelefteq G_i$ for all i: for $\tau \in G_i$, $\sigma \in G_{i+1}$ and $b \in O_L$, we have that $\sigma\big(\tau^{-1}(b)\big) \equiv \tau^{-1}(b) \pmod{\mathfrak{m}_L^{i+2}}$ and hence $\tau\sigma\tau^{-1}(b) \equiv b \pmod{\mathfrak{m}_L^{i+2}}$, i.e., $\tau\sigma\tau^{-1} \in G_{i+1}$.

We study the beginning of this filtration a bit closer.

Theorem 5.4 (Galois Group and Maximal Unramified Extension) *Let $L \supset K$ be a Galois extension of local fields with $G = \mathrm{Gal}(L/K)$ and let $l \supset k$ be the corresponding extension of residue fields. Let G_0 be the inertia group of this extension. Denote by $\bar{\sigma} \in \mathrm{Gal}(l/k)$ the automorphism induced by $\sigma \in G$ on $l = O_L/\mathfrak{m}_L$. Then*

1. *the map $\sigma \mapsto \bar{\sigma}$ induces an isomorphism between G/G_0 and $\mathrm{Gal}(l/k)$. In particular we have that $|G_0| = e_{L/K}$.*
2. *the field $M \stackrel{\mathrm{df}}{=} L^{G_0}$ is the maximal unramified extension of K contained in L. In particular, M is Galois over K with cyclic Galois group $G/G_0 = \mathrm{Gal}(l/k)$.*

We have thus the following picture:

$$\begin{array}{ccccc} L & & & & l \\ \Big| & \text{totally ramified} & e & G_0 & \Big\| \\ M & & & & l \\ \Big| & \text{unramified} & f & G/G_0 = \mathrm{Gal}(l/k) & \Big| \\ K & & & & k \end{array}$$

Proof To prove 1, it is enough to show that the map $G \to \mathrm{Gal}(l/k)$ given by $\sigma \mapsto \bar{\sigma}$ is surjective, since G_0 is the kernel of this map by definition. Let $\theta \in O_L$ be an element whose image $\theta \in l$ is a primitive element of l over k. As in proof of the theorem 5.1, the minimal polynomial $p(x)$ of θ belongs to $O_K[x]$. The minimal polynomial $q_0(x) \in k[x]$ of $\bar{\theta}$ then divides the image $\bar{p}(x) \in k[x]$ of $p(x)$. Since G acts transitively on the roots of $p(x)$ and any automorphism $\sigma_0 \in \mathrm{Gal}(l/k)$ is determined by its value $\sigma_0(\bar{\theta})$, which is a root of $q_0(x)$ and hence of $\bar{p}(x)$, we have that $\sigma_0 = \bar{\sigma}$ where $\sigma \in G$ is any automorphism that takes θ to a root of $p(x)$ lifting $\sigma_0(\bar{\theta})$. Finally, to prove 2, let $M = L^{G_0}$ and just apply 1 to the Galois extension $L \supset M$. We then conclude that M has residue field l and hence that $f_{M/K} = f_{L/K}$, proving that M is the maximal unramified extension of K contained in L. □

Corollary 5.5 (Unramified Highlander's Philosophy) *Let K be a local field and let $\mathbb{F}_q$ be its residue field. Then there is a bijection between finite unramified extensions of K (in some algebraic closure of K) and finite extensions of $\mathbb{F}_q$, which associates to each finite extension of K its residue field. In particular, there is exactly one unramified extension of each degree, and they are all cyclic extensions (i.e. Galois extensions with cyclic Galois group).*

Proof Keep the notation of the last theorem. The natural isomorphism of Galois groups $\mathrm{Gal}(M/K) \approx \mathrm{Gal}(l/k)$ induced by $\sigma \mapsto \bar{\sigma}$ translates into a bijection between the subextensions of $M \supset K$ and those of $l \supset k$: it takes N with $H = \mathrm{Gal}(M/N)$ to the subfield $l^{\bar{H}}$ of l fixed by the image $\bar{H} \subset \mathrm{Gal}(l/k)$ of H. But $M \supset N$ is unramified, so $\sigma \mapsto \bar{\sigma}$ also induces an isomorphism $\mathrm{Gal}(M/N) \approx \mathrm{Gal}(l/n)$ where n denotes the residue field of N. In other words, $\bar{H} = \mathrm{Gal}(l/n)$ and hence $n = l^{\bar{H}}$. To sum up there is a bijection between the unramified subextensions of $L \supset K$ and the subextensions of $l \supset k$, taking N to its residue field n.

Therefore to finish the proof we just need to show that: (1) any unramified extension of K is contained in some Galois extension of K; and (2) given a finite extension $l \supset \mathbb{F}_q$ it is possible to find a Galois extension L of K whose residue field contains l. (1) follows from the proof of theorem 5.1, which shows that any unramified extension of K is separable. To prove (2), given any finite extension l of $\mathbb{F}_q$, we have that l is splitting field of $x^{q^n} - x \in \mathbb{F}_q[x]$ for some n. It suffices then to consider the splitting field L of $x^{q^n} - x \in K[x]$ over K. □

Definition 5.6 Let $L \supset K$ be an unramified extension. The unique automorphism in $\mathrm{Gal}(L/K)$ lifting the Frobenius automorphism of the residue field extension is also called **Frobenius automorphism** of $L \supset K$.

Example 5.7 The unramified extension of degree n over $\mathbb{F}_p((t))$ is just $\mathbb{F}_{p^n}((t))$. For p odd, the unramified extension over $\mathbb{Q}_p$ of degree 2 is $\mathbb{Q}_p(\sqrt{u})$, where u is a non-square in $\mathbb{Z}_p^\times$ (see example 3.8). The Frobenius map is $\sqrt{u} \mapsto -\sqrt{u}$ (there is no other choice).

The degree 3 unramified extension L of $\mathbb{Q}_5$ is given by $\mathbb{Q}_5(\theta)$ where θ is a root of $f(x) = x^3+3x^2-1$. This follows from the fact that the image $\bar{f}(x) \in \mathbb{F}_5[x]$ of $f(x)$ is irreducible, hence $f(x)$ is also irreducible; on the other hand, the residue field l of L contains the image $\bar{\theta} \in l$ of $\theta \in O_L$ (θ is integral over $\mathbb{Z}_5$), hence $[l : \mathbb{F}_5] \geq [L : \mathbb{Q}_5] = 3$, and we thus must have equality, showing that L is unramified over $\mathbb{Q}_3$. The Frobenius automorphism ϕ is characterised by $\phi(\theta) \equiv \theta^5 \pmod 5$. A straightforward computation shows that $-\theta^2 - 3\theta - 1$ is another root of $f(x)$ and that ϕ is explicitly given by $\theta \mapsto -\theta^2 - 3\theta - 1$.

We close this section showing that, in a local field, you will never have trouble solving equations by radicals!

Theorem 5.8 *Every Galois extension $L \supset K$ of local fields is solvable.*

Proof Although quite impressive, this theorem has a simple proof. Write $G = \mathrm{Gal}(L/K)$, let G_i denote the i-th higher ramification group, and l and k be the residue fields of L and K respectively. Since $G/G_0 = \mathrm{Gal}(l/k)$ is cyclic, in order to show that G is solvable it is enough to show that G_0 is solvable. The key idea is then to construct, for $i \geq 0$, injective morphisms $f_i \colon G_i/G_{i+1} \hookrightarrow U_L^{(i)}/U_L^{(i+1)}$.

Let Π be a uniformiser of L. Define $f_i \colon G_i/G_{i+1} \to U_L^{(i)}/U_L^{(i+1)}$ by

$$\boxed{f(\sigma G_{i+1}) = \frac{\sigma(\Pi)}{\Pi} \bmod U_L^{(i+1)} \qquad \text{for } \sigma \in G_i}$$

First we show that this map is well-defined: since $\sigma \in G_i$ preserves the valuation, $\sigma(\Pi) = u\Pi$ for some unit $u \in O_L^\times$; but we also have $\sigma(\Pi) \equiv \Pi \pmod{\Pi^{i+1}}$ and therefore $u \equiv 1 \pmod{\Pi^i}$, i.e., $u = \sigma(\Pi)/\Pi \in U_L^{(i)}$. Replacing i by $i+1$ shows that $\sigma(\Pi)/\Pi \in U_L^{(i+1)}$ whenever $\sigma \in G_{i+1}$.

Next we show that the definition of f_i does not depend on the choice of Π: replacing Π by another uniformiser $u\Pi$, $u \in O_L^\times$, alters f_i by $\sigma(u)/u \bmod U_L^{(i+1)}$. But $\sigma \in G_i$ and thus $\sigma(u) \equiv u \pmod{\mathfrak{m}_L^{i+1}}$ showing that $\sigma(u)/u \in U_L^{(i+1)}$.

We now check that f_i is group morphism. Let $\sigma, \tau \in G_i$. Since $\tau(\Pi)$ is also a uniformiser, we have that

$$\begin{aligned} f_i(\sigma\tau G_{i+1}) &= \frac{\sigma\tau(\Pi)}{\Pi} \bmod U_L^{(i+1)} = \frac{\sigma\big(\tau(\Pi)\big)}{\big(\tau(\Pi)\big)} \cdot \frac{\tau(\Pi)}{\Pi} \bmod U_L^{(i+1)} \\ &= f_i(\sigma G_{i+1}) f_i(\tau G_{i+1}) \end{aligned}$$

Finally, we show that f_i is injective. Let $\sigma \in G_i$ and suppose that $u \stackrel{\mathrm{df}}{=} \sigma(\Pi)/\Pi$ satisfies $u \in U_L^{(i+1)} \iff u \equiv 1 \pmod{\Pi^{i+1}}$. Then $\sigma(\Pi) \equiv \Pi \pmod{\Pi^{i+2}}$, which implies that $\sigma \in G_{i+1}$. In fact, we have that $\sigma \in G_0$ and that L is totally ramified over $M \stackrel{\mathrm{df}}{=} L^{G_0}$ by theorem 5.4. Hence we may choose Π to be a $|G_0|$-th root of a uniformiser of M and by theorem 3.9 we have that O_L is generated over O_M by the powers of Π. Therefore $\sigma(\Pi) \equiv \Pi \pmod{\Pi^{i+2}}$ implies that $\sigma(b) \equiv b \pmod{\Pi^{i+2}}$ for all $b \in O_L$, as claimed. □

6 Exercises

1. Show that $\mathbb{F}_p((t))$ and $\mathbb{Q}_p$ are uncountable.

2. Show that the p-adic number $f = \sum_i a_i p^i \in \mathbb{Q}_p$ belongs to $\mathbb{Q}$ if and only if its p-base expansion is periodic. Find the 5-base expansion for $2/3$ and $1/10$ in $\mathbb{Q}_5$.

3. (Multiplicative Calculus Student's Psychedelic Dream) Let K be a local field and consider elements $f_n \in K^\times$, $n \geq 0$. Show that the infinite product $\prod_{n\geq 0} f_n$ converges to an element of $K^\times$ if and only if $\lim_{n\to\infty} f_n = 1$.

4. Show that $\mathbb{F}_p((t))$ is the completion of $\mathbb{F}_p(t)$ with respect to the valuation given by the prime t of $\mathbb{F}_p[t]$. Similarly show that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the valuation given by the prime p of $\mathbb{Z}$.

5. Over which $\mathbb{Q}_p$ is the quadratic form $3x^2 + 7y^2 - 15z^2$ anisotropic?

6. Give an example of two totally ramified extensions of some local field K whose compositum is not totally ramified over K.

7. Show that the splitting field of $x^{p^n} - x$ is the unramified extension of $\mathbb{Q}_p$ of degree n.

8. Find the Galois groups of $x^5 + x + 1$ over $\mathbb{Q}$, $\mathbb{Q}_3$ and $\mathbb{Q}_5$.

9. Let n be a positive integer and p be an odd prime. Is D_n the Galois group of some Galois extension of $\mathbb{Q}_p$? (I write D_n for the dihedral group with $2n$ elements with the sole purpose of confusing my audience!)

Local Class Field Theory

1 Introduction

Local Class Field Theory is the study of **abelian extensions** of a local field K, that is, Galois extensions of K with abelian Galois group. The celebrated **local Artin reciprocity theorem** shows that all information about such extensions is already contained, in an unexpectedly simple form, in the multiplicative group $K^\times$. The local reciprocity theorem is beyond doubt one of the greatest achievements of contemporary Mathematics. Its (ravishingly beautiful!) proof will occupy us for most of this chapter.

1.1 Notation and General Remarks

Throughout this chapter, we adopt the following notations and conventions. For any field K we denote by

$$K_{sp} \stackrel{\text{df}}{=} \text{separable closure of } K$$

$$G_K \stackrel{\text{df}}{=} \text{Gal}(K_{sp}/K) = \text{absolute Galois group of } K$$

Recall that G_K is a topological group: a topological basis consists of the left translates of the subgroups G_L where L runs over all finite extensions of K. Galois theory establishes a 1-1 correspondence between *closed* subgroups of G_K and fields between K and K_{sp}.

The group G_K is an example of a **profinite group** (i.e. a projective limit of finite groups): we have, both algebraically and topologically,

$$G_K \approx \varprojlim_{L \supset K} \text{Gal}(L/K)$$

where L runs over all finite Galois extensions of K and each $\text{Gal}(L/K)$ is given the discrete topology.

Given any profinite group G, we denote by

$$[G:G] \stackrel{\text{df}}{=} \text{closure (in the profinite topology) of the commutator subgroup of } G$$

$$G^{ab} \stackrel{\text{df}}{=} \frac{G}{[G:G]} = \text{maximal abelian quotient of } G$$

By the Galois correspondence we then have

$$K^{ab} \stackrel{\text{df}}{=} K_{sp}^{[G_K:G_K]} = \text{maximal abelian extension of } K$$

$$= \text{compositum of all finite abelian extensions of } K \text{ inside } K_{sp}$$

$$G_K^{ab} = \text{Gal}(K^{ab}/K)$$

Finally, if K is a local field with residue field k we write (see section I.5)

$$K_{nr} \stackrel{\text{df}}{=} \text{maximal unramified extension of } K \text{ in } K_{sp}$$

$$= \text{compositum of all finite unramified extensions of } K \text{ inside } K_{sp}$$

$$G_K^{nr} \stackrel{\text{df}}{=} \text{Gal}(K_{nr}/K) \approx G_k = \hat{\mathbb{Z}}$$

$$\Phi_K \stackrel{\text{df}}{=} \text{Frobenius automorphism of } K_{nr} \supset K$$

where

$$\hat{\mathbb{Z}} \stackrel{\text{df}}{=} \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/(n) = \prod_p \mathbb{Z}_p$$

and p runs over all prime integers. The last isomorphism follows from the Chinese Remainder Theorem (check!). The Frobenius map Φ_K is a topological generator of G_K^{nr}, corresponding to the element $1 \in \hat{\mathbb{Z}}$ under the above isomorphism.

2 Statements of the main theorems

Theorem 2.1 (Local Artin Reciprocity) *Let K be a local field. There exists a unique group morphism, called* **local Artin map**,

$$\theta_K \colon K^\times \to G_K^{ab}$$

such that the following holds: for any finite abelian extension $L \supset K$, the map $\theta_{L/K} \colon K^\times \to \mathrm{Gal}(L/K)$ (also referred to as local Artin map) given by the composition

$$K^\times \xrightarrow{\theta_K} G_K^{ab} \xrightarrow{\text{canonical}} \mathrm{Gal}(L/K)$$

satisfies:

1. *$\theta_{L/K}$ is surjective with kernel given by the* **norm group** *$N_{L/K}L^\times$. Thus we have an induced isomorphism (which we still denote by $\theta_{L/K}$)*

$$\boxed{\theta_{L/K} \colon \frac{K^\times}{N_{L/K}(L^\times)} \approx \mathrm{Gal}(L/K)}$$

2. *if $L \supset K$ is unramified, $\Phi_{L/K} \in \mathrm{Gal}(L/K)$ denotes the corresponding Frobenius map, and $v \colon K^\times \to \mathbb{Z}$ denotes the normalised valuation of K, then for all $a \in K^\times$*

$$\boxed{\theta_{L/K}(a) = \Phi_{L/K}^{v(a)}}$$

The first property is a "compatibility" one in that it says that the "big" Artin map θ_K is compatible with its "finite layers" in the sense that the diagram

$$\begin{array}{ccc} K^\times & \xrightarrow{\theta_K} & G_K^{ab} \\ \Big\downarrow{\scriptstyle \text{can.}} & & \Big\downarrow{\scriptstyle \text{can.}} \\ \dfrac{K^\times}{N_{L/K}(L^\times)} & \xrightarrow[\approx]{\theta_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

commutes. This implies that for all finite extensions $M \supset L \supset K$ with $M \supset K$ (and thus $L \supset K$) abelian we have a commutative diagram

$$\begin{array}{ccc} \dfrac{K^\times}{N_{M/K}(M^\times)} & \xrightarrow[\approx]{\theta_{M/K}} & \mathrm{Gal}(M/K) \\ \Big\downarrow{\scriptstyle \text{can.}} & & \Big\downarrow{\scriptstyle \text{can.}} \\ \dfrac{K^\times}{N_{L/K}(L^\times)} & \xrightarrow[\approx]{\theta_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

Conversely, to give θ_K is equivalent to give maps $\theta_{L/K}$, one for each finite abelian extension $L \supset K$, compatible in the above sense.

The second property is a "normalisation" property in that it fixes the value of the local Artin map for unramified extensions. Let $L \supset K$ be an unramified extension of degree n and let π be a uniformiser of K. From 1 and 2 we conclude that $\pi^{n\mathbb{Z}} \cdot U_K = \ker \theta_{L/K} = N_{L/K}L^\times$ and therefore (see the explicit formula for the valuation of L in theorem I.3.4) that the norm map $N_{L/K} \colon U_L \twoheadrightarrow U_K$ is surjective on units for unramified extensions.

The "functorial" properties of the reciprocity map immediately imply:

Theorem 2.2 *Let K be a local field and let L and L' be finite abelian extensions of K. Then*

1. $L' \supset L \iff N_{L'/K}L'^{\times} \subset N_{L/K}L^{\times}$;
2. $N_{(L'\cap L)/K}(L' \cap L)^{\times} = N_{L'/K}L'^{\times} \cdot N_{L/K}L^{\times}$;
3. $N_{(L'\cdot L)/K}(L' \cdot L)^{\times} = N_{L'/K}L'^{\times} \cap N_{L/K}L^{\times}$.

PROOF We prove 3 as an example and leave the other two as exercises. We have a commutative diagram

$$\begin{array}{ccc} K^{\times} & \xrightarrow{\theta_{(L'\cdot L)/K}} & \mathrm{Gal}\big((L'\cdot L)/K\big) \\ \| & & \big\downarrow \text{can.} \\ K^{\times} & \xrightarrow{\theta_{L'/K}\times\theta_{L/K}} & \mathrm{Gal}(L'/K)\times\mathrm{Gal}(L/K) \end{array}$$

where the right vertical arrow is injective. Hence

$$N_{(L'\cdot L)/K}(L'\cdot L)^{\times} = \ker\theta_{(L'\cdot L)/K} = \ker(\theta_{L'/K}\times\theta_{L/K}) = \ker\theta_{L'/K}\cap\ker\theta_{L/K} = N_{L'/K}L'^{\times}\cap N_{L/K}L^{\times}$$

□

Observe that 1 of the last theorem shows that there is a 1-1 containment reversing correspondence between finite abelian extensions of K and **norm groups** of $K^{\times}$, that is, subgroups of $K^{\times}$ which are of the form $N_{L/K}L^{\times}$ for some finite abelian extension $L \supset K$. The **local existence theorem** tells us which subgroups of $K^{\times}$ are norm groups.

Theorem 2.3 (Local Existence) *Let K be a local field. A subgroup of finite index of $K^{\times}$ is a norm group if and only if it is open. Hence there is a 1-1 containment reversing correspondence*

$$\{\,\textit{finite abelian extensions of } K\,\} \leftrightarrow \{\,\textit{open subgroups of } K^{\times} \textit{ of finite index}\,\}$$
$$L \mapsto N_{L/K}L^{\times}$$

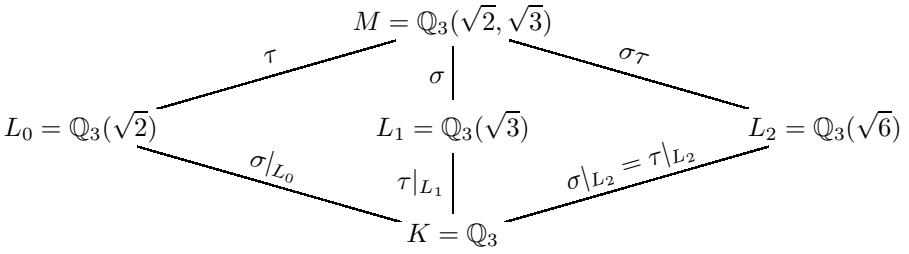
Remark 2.4 When $\mathrm{char}\,K = 0$, a subgroup $T \subset K^{\times}$ of finite index is automatically open: since T has finite index, $T \supset (K^{\times})^n$ for some n, and $(K^{\times})^n \supset U_K^{(m)}$ for m sufficiently large (exercise!). Hence if $\mathrm{char}\,K = 0$ there is a perfect 1-1 correspondence between subgroups of $K^{\times}$ of finite index and finite abelian extensions of K!

In the first chapter, we gave a complete description of the unit group $K^{\times}$. Hence with the reciprocity and existence theorems we obtain a complete classification of *all* abelian extensions of a local field K! The proofs of these two deep theorems will be given later. In this section we give some applications to impress you with the power of these results.

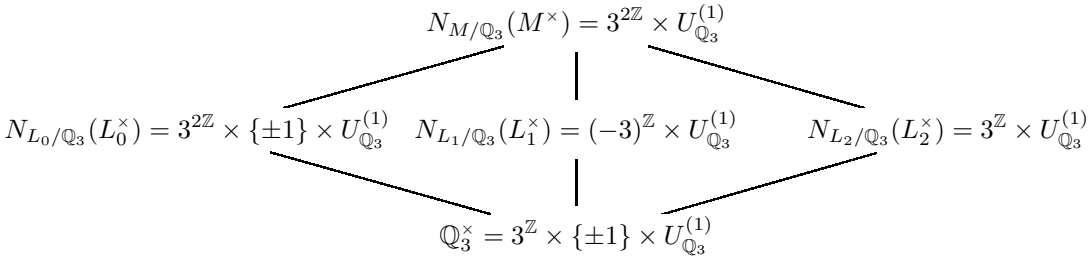
Example 2.5 Consider the Galois extension $M = \mathbb{Q}_3(\sqrt{2},\sqrt{3})$ of $\mathbb{Q}_3$ with Galois group $\mathrm{Gal}(M/\mathbb{Q}_3) \cong \mathbb{Z}/2\times\mathbb{Z}/2$, generated by automorphisms σ and τ given by

$$\begin{cases} \sigma(\sqrt{2}) = -\sqrt{2} \\ \sigma(\sqrt{3}) = \sqrt{3} \end{cases} \qquad \begin{cases} \tau(\sqrt{2}) = \sqrt{2} \\ \tau(\sqrt{3}) = -\sqrt{3} \end{cases}$$

The lattice of subfields is



Now we now identify the corresponding norm subgroups in $\mathbb{Q}_3^\times = 3^{\mathbb{Z}} \times \{\pm 1\} \times U_{\mathbb{Q}_3}^{(1)}$ (see section 2 of chapter I). Observe that since the indices of these subgroups divide 4 and $U_{\mathbb{Q}_3}^{(1)} \cong \mathbb{Z}_3$ is 2-divisible (see lemma I.4.1), all of them contain $U_{\mathbb{Q}_3}^{(1)}$. Since $L_0 \supset \mathbb{Q}_3$ is unramified we know that $N_{L_0/\mathbb{Q}_3}(L_0^\times) = 3^{2\mathbb{Z}} \times U_{\mathbb{Q}_3}$. Moreover $-3 \in N_{L_1/\mathbb{Q}_3}(L_1^\times)$ and $-6 \in N_{L_2/\mathbb{Q}_3}(L_2^\times)$, thus $3 \in N_{L_2/\mathbb{Q}_3}(L_2^\times)$ since $-2 \in U_{\mathbb{Q}_3}^{(1)}$. Also since M is the compositum of L_0 and L_2 we have that $N_{M/\mathbb{Q}_3}(M^\times) = N_{L_0/\mathbb{Q}_3}(L_0^\times) \cap N_{L_2/\mathbb{Q}_3}(L_2^\times)$. Putting everything together, we obtain the following lattice of subgroups of $\mathbb{Q}_3^\times$, drawn upside down:



Finally, we have that

$$\begin{cases} \theta_{L_0/\mathbb{Q}_3}\big(-1 \cdot N_{L_0/\mathbb{Q}_3}(L_0^\times)\big) = 1 \\ \theta_{L_1/\mathbb{Q}_3}\big(-3 \cdot N_{L_1/\mathbb{Q}_3}(L_1^\times)\big) = 1 \\ \theta_{L_2/\mathbb{Q}_3}\big(3 \cdot N_{L_2/\mathbb{Q}_3}(L_0^\times)\big) = 1 \end{cases} \Rightarrow \begin{cases} \theta_{M/\mathbb{Q}_3}\big(-1 \cdot N_{M/\mathbb{Q}_3}(M^\times)\big) = \tau \\ \theta_{M/\mathbb{Q}_3}\big(-3 \cdot N_{M/\mathbb{Q}_3}(M^\times)\big) = \sigma \\ \theta_{M/\mathbb{Q}_3}\big(3 \cdot N_{M/\mathbb{Q}_3}(M^\times)\big) = \sigma\tau \end{cases}$$

which completely determines $\theta_{M/\mathbb{Q}_3}$.

For the next, we need the following explicit computation of norm groups of cyclotomic extensions.

Lemma 2.6 *Let n be a positive integer and consider the cyclotomic extension $L = \mathbb{Q}_p(\zeta_{p^n})$ of $\mathbb{Q}_p$ where ζ_{p^n} denotes a primitive p^n-th root of unity. Then the extension $L \supset \mathbb{Q}_p$ is totally ramified of degree $[L : \mathbb{Q}_p] = \phi(p^n) = (p-1) \cdot p^{n-1}$ (ϕ denotes the Euler function) and $1 - \zeta_{p^n}$ is a uniformiser of L. The corresponding norm group is*

$$N_{L/\mathbb{Q}_p}(L^\times) = p^{\mathbb{Z}} \cdot U_{\mathbb{Q}_p}^{(n)}$$

Hence the local Artin map gives a canonical isomorphism $U_{\mathbb{Q}_p}/U_{\mathbb{Q}_p}^{(n)} \approx \mathrm{Gal}(L/\mathbb{Q}_p)$ (which are canonically isomorphic to $(\mathbb{Z}/p^n)^\times$).

Proof The polynomial in $\mathbb{Q}_p[x]$

$$f(x) \stackrel{\mathrm{df}}{=} \frac{x^{p^n} - 1}{x^{p^{n-1}} - 1} = x^{(p-1)p^{n-1}} + x^{(p-2)p^{n-1}} + \cdots + x^{p^{n-1}} + 1$$

is irreducible by the usual argument combining Gauß' lemma and Eisenstein's criterion applied to $f(x+1)$. Hence $f(x)$ is the minimal polynomial of ζ_{p^n} over $\mathbb{Q}_p$ and thus $[L : \mathbb{Q}_p] = \phi(p^n) = (p-1) \cdot p^{n-1}$. Also

$$N_{L/K}(1 - \zeta_{p^n}) = \prod_{\substack{0<i<p^n \\ p \nmid i}} (1 - \zeta_{p^n}^i) = f(1) = p$$

and from the explicit formula of theorem I.3.4 we conclude that L is totally ramified over $\mathbb{Q}_p$ with uniformiser $1 - \zeta_{p^n}$ and residue field $\mathbb{F}_p$.

The last expression also shows that all powers of p belong to $N_{L/\mathbb{Q}_p}(L^\times)$. By computations of section I.4, we have that $\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mu_{p-1} \times U_{\mathbb{Q}_p}^{(1)}$ and $L^\times \cong (\zeta_{p^n} - 1)^{\mathbb{Z}} \times \mu_{p-1} \times U_L^{(1)}$, where $\mu_{p-1} \subset \mathbb{Q}_p^\times$ is the group of $(p-1)$-th roots of unity. Thus to show that $N_{L/\mathbb{Q}_p}(L^\times) = p^{\mathbb{Z}} \cdot U_{\mathbb{Q}_p}^{(n)}$ it suffices to show that $N_{L/\mathbb{Q}_p} U_L^{(1)} \supset U_{\mathbb{Q}_p}^{(n)}$. In fact, in that case $N_{L/\mathbb{Q}_p}(L^\times)$ will have index at most $|\mu_{p-1}| \cdot [U_{\mathbb{Q}_p}^{(1)} : U_{\mathbb{Q}_p}^{(n)}] = (p-1) \cdot p^{n-1}$ in $\mathbb{Q}_p^\times$, but from the local Artin reciprocity theorem we know that this index is precisely $(p-1) \cdot p^{n-1} = [L : \mathbb{Q}_p]$.

By lemma I.4.1, the exp and log functions give an isomorphism $U_{\mathbb{Q}_p}^{(i)} \cong (p^i)$ for $i \geq 1$ (respectively $i \geq 2$) when $p \neq 2$ (respectively $p = 2$). Hence, when $p \neq 2$ the map $x \mapsto x^{(p-1) \cdot p^{n-1}}$ gives an

isomorphism $U_{\mathbb{Q}_p}^{(1)} \cong U_{\mathbb{Q}_p}^{(n)}$ since $x \mapsto (p-1)\cdot p^{n-1}\cdot x$ gives an isomorphism $(p) \cong (p^n)$, proving that $N_{L/\mathbb{Q}_p}U_L^{(1)} \supset \left(U_{\mathbb{Q}_p}^{(1)}\right)^{[L:\mathbb{Q}_p]} = U_{\mathbb{Q}_p}^{(n)}$ in this case. When $p=2$ and $n \geq 2$ (for $n=1$, $L=\mathbb{Q}_2$), we have that $x \mapsto x^{2^{n-1}}$ gives an isomorphism $U_{\mathbb{Q}_2}^{(2)} \cong U_{\mathbb{Q}_p}^{(n+1)}$ and only get that $N_{L/\mathbb{Q}_2}U_L^{(1)} \supset U_{\mathbb{Q}_2}^{(n+1)}$. However an explicit computation shows that $5^{2^{n-2}} = N_{L/\mathbb{Q}_p}(2+i)$, where $i = (\zeta_{2^n})^{2^{n-2}}$ is a primitive 4-th root of 1, and since $U_{\mathbb{Q}_2}^{(2)} = U_{\mathbb{Q}_2}^{(3)} \cup 5\cdot U_{\mathbb{Q}_2}^{(3)}$ applying $x \mapsto x^{2^{n-2}}$ gives $U_{\mathbb{Q}_2}^{(n)} = U_{\mathbb{Q}_2}^{(n+1)} \cup 5^{2^{n-2}}\cdot U_{\mathbb{Q}_2}^{(n+1)}$, proving that $N_{L/\mathbb{Q}_2}U_L^{(1)} \supset U_{\mathbb{Q}_2}^{(n)}$ in this case as well. □

Remark 2.7 It can be shown (using formal groups à la Lubin-Tate, see for instance Neukirch's book or Serre's article in Cassels-Fröhlich) that the isomorphism $U_{\mathbb{Q}_p}/U_{\mathbb{Q}_p}^{(n)} \approx \mathrm{Gal}(L/\mathbb{Q}_p)$ takes $u \bmod U_{\mathbb{Q}_p}^{(n)}$ to the automorphism given by $\zeta_{p^n} \mapsto \zeta_{p^n}^{u^{-1}}$.

We are now ready to show the celebrated

Theorem 2.8 (Local Kronecker-Weber) *Every finite abelian extension of $\mathbb{Q}_p$ is contained in a cyclotomic extension.*

Proof Let $L \supset \mathbb{Q}_p$ be a finite abelian extension. Since $N_{L/\mathbb{Q}_p}L^\times$ has finite index in $\mathbb{Q}_p^\times$, there exists m such that $p^m \in N_{L/\mathbb{Q}_p}L^\times$, and since $N_{L/\mathbb{Q}_p}L^\times$ is open, there exists n such that $N_{L/\mathbb{Q}_p}L^\times \supset U_{\mathbb{Q}_p}^{(n)}$. Let $N = p^n\cdot(p^m-1)$. We claim that $N_{\mathbb{Q}_p(\zeta_N)/\mathbb{Q}_p}\mathbb{Q}_p(\zeta_N)^\times = p^{m\mathbb{Z}} \times U_{\mathbb{Q}_p}^{(n)} \subset N_{L/\mathbb{Q}_p}L^\times$, which in turn implies that $\mathbb{Q}_p(\zeta_N) \supset L$, finishing the proof of the theorem.

To prove the claim, observe that $\mathbb{Q}_p(\zeta_N)$ is the compositum of $M_0 = \mathbb{Q}_p(\zeta_{p^m-1})$ and $M_1 = \mathbb{Q}_p(\zeta_{p^n})$, hence the norm group of $\mathbb{Q}_p(\zeta_N)$ is the intersection of the norm groups of M_0 and M_1. By the lemma, we already know that $N_{M_1/\mathbb{Q}_p}M_1^\times = p^{\mathbb{Z}} \times U_{\mathbb{Q}_p}^{(n)}$. On the other hand, we show below that M_0 is unramified over $\mathbb{Q}_p$ of degree m and hence has norm group $p^{m\mathbb{Z}} \times U_{\mathbb{Q}_p}$. Putting everything together, we conclude that $\mathbb{Q}_p(\zeta_N)$ has norm group $p^{m\mathbb{Z}} \times U_{\mathbb{Q}_p}^{(n)}$ as claimed.

Finally, to show that M_0 is the degree m unramified extension of $\mathbb{Q}_p$, let $f(x) \in \mathbb{Z}_p[x]$ be the minimal polynomial of ζ_{p^n-1} over $\mathbb{Q}_p$ and let $\bar{f}(x) \in \mathbb{F}_p[x]$ denote the image of $f(x)$ in $\mathbb{F}_p[x]$. Since $x^{p^m-1}-1$ is separable over $\mathbb{F}_p[x]$, by Hensel's lemma the irreducible factors of $x^{p^m-1}-1$ over $\mathbb{Q}_p$ and over $\mathbb{F}_p$ are in 1-1 correspondence, thus $\bar{f}(x)$ is irreducible over $\mathbb{F}_p[x]$. Hence $[M_0:\mathbb{Q}_p] = \deg f(x) = \deg \bar{f}(x) \leq f_{M_0/\mathbb{Q}_p}$, but since we always have $[M_0:\mathbb{Q}_p] \geq f_{M_0/\mathbb{Q}_p}$, equality holds (compare with example I.5.7). On the other hand M_0 and $\mathbb{F}_{p^m}$ are the splitting fields of $x^{p^m-1}-1$ over $\mathbb{Q}_p$ and $\mathbb{F}_p$, respectively. Hence m is the largest of the degrees of the irreducible factors of $x^{p^m-1}-1$ over $\mathbb{Q}_p$ and $\mathbb{F}_p$. This shows that $\deg \bar{f}(x) \leq m$ and also $[M_0:\mathbb{Q}_p] \geq m$, hence both are equal to m. □

Example 2.9 We have that $\mathbb{Q}_3(\sqrt{2},\sqrt{3})$ has norm group $3^{2\mathbb{Z}} \times U_{\mathbb{Q}_3}^{(1)}$, so by the above proof we have that $\mathbb{Q}_3(\sqrt{2},\sqrt{3}) \subset \mathbb{Q}_3(\zeta_{24})$. Explicitly, writing $i = \zeta_{24}^6$, a primitive 4-th root of 1, we have that

$$\zeta_8 = \frac{\sqrt{2}+i\sqrt{2}}{2} \qquad \text{and} \qquad \zeta_3 = \frac{-1+i\sqrt{3}}{2}$$

Hence $\sqrt{2} = 2\zeta_{24}^3\cdot(1+\zeta_{24}^6)^{-1}$ and $\sqrt{3} = (2\zeta_{24}^8+1)\cdot\zeta_{24}^{-6}$.

Before we end this section, we give a general overview of the proof of the local reciprocity. The first part of the proof, the Tate-Nakayama theorem, is a purely group theoretical result that describes the maximal abelian quotient G^{ab} of a finite group G in terms of a $\mathbb{Z}[G]$-module C satisfying some conditions. The second part of the proof is to show that for a finite Galois extension of local fields $L \supset K$ with $G = \mathrm{Gal}(L/K)$ we may take $C = L^\times$, and for that we will make use of our knowledge of the structure of $L^\times$. Once the reciprocity theorem is proved, the proof of the existence theorem is then not too difficult.

3 Tate-Nakayama theorem

Let G be a finite group. In this section, we prove a purely group theoretic result giving an isomorphism

$$G^{ab} \approx \frac{C^G}{N_G(C)}$$

where C is a G-module satisfying some conditions and $N_G\colon C \to C^G$ denotes the **norm map** of C (see appendix). The methods of this section are inspired in computations of Algebraic Topology, with the starting point being the well-known relation $H_1(X,\mathbb{Z}) = \pi_1(X)^{ab}$ between the first singular homology group of a topological space X and the maximal abelian quotient $\pi_1(X)^{ab}$ of the fundamental group of X. Since Galois extensions are algebraic analogs of covering spaces in Topology, this turns out to be a quite natural point of view (if, of course, you've studied Algebraic Topology before, but don't worry if you haven't, the proofs below are purely algebraic, but it's a good idea to eventually look at the source of inspiration for them).

All the results that we will need from group cohomology are summarised in the appendix for the convenience of the reader. We begin with a criterion for cohomological triviality for a G-module.

Theorem 3.1 (Twin number vanishing criterion) *Let G be a finite group and M be a G-module. If there are two consecutive numbers i and $i+1$ for which*

$$H_T^i(H,M) = H_T^{i+1}(H,M) = 0 \qquad \text{for all subgroups } H \leq G$$

then $H_T^r(G,M) = 0$ for all $r \in \mathbb{Z}$.

Proof First observe that by dimension shifting (see appendix) it is enough to show the "weaker" conclusion $H_T^r(G,M) = 0$ for all $r \geq 1$. In fact, writing an exact sequence of G-modules

$$0 \to N \to P \to M \to 0$$

for some induced G-module P (which is thus also induced as an H-module for all $H \leq G$) we obtain an isomorphism $H_T^{j+1}(H,N) = H_T^j(H,M)$ for all $H \leq G$ and $j \in \mathbb{Z}$. Hence if we know that $H_T^r(H,M) = 0$ for all $r \geq 1$ then we know that $H_T^r(H,N) = 0$ for all $r \geq 2$, and applying the "weak twin number criterion" to N in place of M we conclude that $H_T^1(H,N) = 0$ as well, that is $H_T^0(H,M) = 0$, so that the conclusion of the weak criterion holds also for $r \geq 0$. Proceeding inductively in this manner, we extend the result to all $r \in \mathbb{Z}$.

A similar proof using dimension shifting (check!) also allows us to assume that $i = 1$ (or any other fixed number we deem convenient). Hence from now on we assume that $H^1(H,M) = H^2(H,M) = 0$ for all $H \leq G$ and prove that these conditions imply that $H^r(G,M) = 0$ for all $r \geq 1$.

Since $H^r(G,M)$ is a torsion abelian group, it is enough to show that its p-primary component vanishes for all prime numbers p. Let G_p be a p-Sylow subgroup of G. A restriction-corestriction argument shows that $\mathrm{res}\colon H^r(G,M) \to H^r(G_p,M)$ is injective on p-primary components (see appendix), thus it is enough to show that $H^r(G_p,M) = 0$.

Hence we may assume that G is solvable and proceed by induction on the order of G. If G is cyclic, the theorem follows from the periodicity of cohomology. Now let $H \lhd G$ be a proper normal subgroup such that G/H is cyclic. By induction $H^r(H,M) = 0$ for all $r \geq 1$ and hence we have an exact inflation-restriction sequence

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

for all $r \geq 1$. Therefore $H^r(G/H,M^H) = H^r(G,M)$ for all $r \geq 1$ and in particular $H^1(G,M) = H^2(G,M) = 0$ implies that $H^1(G/H,M^H) = H^2(G/H,M^H) = 0$. But G/H is cyclic, so periodicity yields $H^r(G/H,M^H) = 0$ for all $r \geq 1$, and hence $H^r(G,M) = 0$ for all $r \geq 1$ too. □

Now we can prove the main result of this section.

Theorem 3.2 (Tate-Nakayama) *Let G be a finite group and let C be a G-module such that for all subgroups $H \leq G$*

1. *$H^1(H,C) = 0$*
2. *$H^2(H,C)$ is cyclic of order $|H|$*

Let γ be a generator of $H^2(G,C)$. Then for all $r \in \mathbb{Z}$ the cup product with γ gives an isomorphism

$$\boxed{H_T^r(G,\mathbb{Z}) \xrightarrow[\approx]{\cup\gamma} H_T^{r+2}(G,C)}$$

Observe that if $\gamma \in H^2(G,C)$ is a generator then $\mathrm{res}(\gamma) \in H^2(H,C)$ is also a generator since $\mathrm{cor} \circ \mathrm{res}(\gamma) = [G:H] \cdot \gamma$ has order $|H|$, hence $\mathrm{res}(\gamma)$ must have order $|H|$ as well in view of 2.

PROOF The key idea of the proof is to apply a "double dimension shifting" (wow!) and for that we construct a cohomologically trivial G-module $C(\gamma)$ fitting into an exact sequence

$$0 \to C \to C(\gamma) \to I_G \to 0 \tag{$*$}$$

Here $I_G = \langle \sigma - 1 \mid \sigma \in G \rangle$ is the kernel of the augmentation map $\mathbb{Z}[G] \to \mathbb{Z}$ (see appendix), so that we have an exact sequence of G-modules

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

Once $C(\gamma)$ is constructed, the proof of the theorem follows easily: from $(**)$, using the fact that $\mathbb{Z}[G]$ has trivial cohomology, we conclude that the connecting map $\delta_a \colon H_T^r(G,\mathbb{Z}) \approx H_T^{r+1}(G, I_G)$ is an isomorphism; similarly, from $(*)$, we have that the connecting map $\delta_c \colon H_T^{r+1}(G, I_G) \approx H_T^{r+2}(G, C)$ is also an isomorphism. The composition $\delta_c \circ \delta_a$ gives the desired isomorphism $H_T^r(G,\mathbb{Z}) \approx H_T^{r+2}(G, C)$, which equals to the cup product with γ, as we later show.

Let c be a 2-cocycle representing γ. Since we wish $H^2(G, C(\gamma))$ to vanish, the idea is to construct $C(\gamma)$ so that c becomes a coboundary in $C(\gamma)$. Take $C(\gamma)$ to be the direct sum of C with the free abelian group with basis x_σ, $\sigma \in G$, $\sigma \neq 1$:

$$C(\gamma) \stackrel{\text{df}}{=} C \oplus \bigoplus_{\substack{\sigma \in G \\ \sigma \neq 1}} \mathbb{Z} x_\sigma$$

We extend the G-action from C to $C(\gamma)$ in such a way that c becomes the coboundary of $\sigma \mapsto x_\sigma$:

$$\sigma \cdot x_\tau = x_{\sigma\tau} - x_\sigma + c(\sigma, \tau)$$

where we interpret "x_1" to be $c(1,1)$. The 2-cocycle relation then guarantees that $1 \cdot x_\tau = x_\tau$ and $(\rho\sigma) \cdot x_\tau = \rho \cdot (\sigma \cdot x_\tau)$ hold for all $\rho, \sigma, \tau \in G$ (check!), turning $C(\gamma)$ into a G-module containing C as a G-submodule. Finally the map $C(\gamma) \to I_G$ in $(*)$ is given by $x_\sigma \mapsto \sigma - 1$ for $\sigma \neq 1$, and is identically zero on C. Another easy check shows that the latter map preserves the G-action.

In order to show that $C(\gamma)$ is cohomologically trivial we apply the twin number vanishing criterion: we need to verify that $H^1(H, C(\gamma)) = H^2(H, C(\gamma)) = 0$ for all subgroups $H \leq G$. Here the hypotheses 1 and 2 of the theorem come into play. First observe that from $(**)$ and the explicit description of the connecting map in terms of the standard resolution (see appendix) we obtain

(i) $H^1(H, I_G) = H_T^0(H, \mathbb{Z})$ is cyclic of order $|H|$ with generator given by the class $[f]$ of the 1-cocycle $f(\sigma) = \sigma - 1$, $\sigma \in H$.

(ii) $H^2(H, I_G) = H^1(H, \mathbb{Z}) = \operatorname{Hom}(H, \mathbb{Z}) = 0$

From $(*)$ we have an exact sequence

$$\begin{aligned} 0 = H^1(H, C) &\longrightarrow H^1(H, C(\gamma)) \longrightarrow H^1(H, I_G) \\ &\xrightarrow{\delta} H^2(H, C) \longrightarrow H^2(H, C(\gamma)) \longrightarrow H^2(H, I_G) = 0 \end{aligned}$$

Hence everything falls through if we can show that the connecting map δ is an isomorphism. At least we know that both $H^1(H, I_G)$ and $H^2(H, C)$ are cyclic groups of order $|H|$, so it is enough to show that δ is surjective. We show by explicit computation that $\delta([f]) = \operatorname{res}(\gamma)$ where $[f] \in H^1(H, I_G)$ is as in (i). First we lift f to the function $\tilde{f} \colon H \to C(\gamma)$ given by $\tilde{f}(\sigma) = x_\sigma$. Now $(d\tilde{f})(\sigma, \tau) = \sigma \cdot x_\tau - x_{\sigma\tau} + x_\sigma = c(\sigma, \tau)$ for all $\sigma, \tau \in G$, where d denotes the coboundary map, hence $\delta([f]) = [d\tilde{f}] = [c] = \operatorname{res}(\gamma)$, as required.

Finally, we verify that the composition $\delta_c \circ \delta_a$ of the two connecting maps $\delta_a \colon H_T^r(G,\mathbb{Z}) \xrightarrow{\approx} H_T^{r+1}(G, I_G)$ and $\delta_c \colon H_T^{r+1}(G, I_G) \xrightarrow{\approx} H_T^{r+2}(G, C)$ is indeed the cup product with γ. Denote by $\mu \in H_T^0(G,\mathbb{Z}) = \mathbb{Z}/|G|$ the generator $1 \bmod |G|$ and by $\phi = [f] = \delta_a(\mu) \in H^1(G, I_G)$ where f is as in (i). By the compatibility of cup products with the connecting maps (see appendix) we obtain, for all $\alpha \in H_T^r(G,\mathbb{Z})$,

$$\begin{aligned} \alpha \cup \gamma = \alpha \cup \delta_c(\phi) &= (-1)^r \cdot \delta_c(\alpha \cup \phi) = (-1)^r \cdot \delta_c\big(\alpha \cup \delta_a(\mu)\big) \\ &= (-1)^r \cdot \delta_c\big((-1)^r \cdot \delta_a(\alpha \cup \mu)\big) = (-1)^r \cdot \delta_c\big((-1)^r \cdot \delta_a(\alpha)\big) = \delta_c \circ \delta_a(\alpha) \end{aligned}$$

since $- \cup \mu$ is the identity on $H_T^r(G,\mathbb{Z})$. □

Recall that (see appendix) $H_T^{-2}(G,\mathbb{Z}) = H_T^{-1}(G,I_G) = I_G/I_G^2$ and that $G^{ab} = I_G/I_G^2$ via the isomorphism $\sigma\cdot[G:G] \mapsto (\sigma-1)\cdot I_G^2$. As a consequence we obtain

Corollary 3.3 ("Abstract" Reciprocity) *With the notation and hypotheses of the Tate-Nakayama theorem, we have an isomorphism*

$$\boxed{\frac{C^G}{N_G(C)} = H_T^0(G,C) \approx H_T^{-2}(G,\mathbb{Z}) = G^{ab}}$$

We wish to apply the Tate-Nakayama's theorem to $G=\mathrm{Gal}(L/K)$ and $C=L^\times$ where $L\supset K$ is a finite Galois extension of local fields. Hence we need to verify that, for all subgroups $H\leq G$,

1. $H^1(H,L^\times)=0$;
2. $H^2(H,L^\times)$ is cyclic of order $|H|$.

The first condition is just Hilbert Satz 90 (see appendix), so we are left to compute $H^2(G,L^\times)$. This is not too difficult since we know the structure of $L^\times$ and since G is solvable so we will be able to reduce everything to the cyclic case. We begin by looking at the cyclic factor G/G_0 corresponding to the maximal unramified extension of K in L.

4 Unramified Cohomology

In this section, $L\supset K$ will be a finite unramified extension with $G=\mathrm{Gal}(L/K)$, and $l\supset k$ will be the corresponding extension of residue fields. Recall that we have a canonical isomorphism $G=\mathrm{Gal}(L/K)\approx \mathrm{Gal}(l/k)$, and so G is cyclic.

We now compute $H^2(G,L^\times)$. The starting point is the exact sequence of G-modules

$$0 \longrightarrow U_L \longrightarrow L^\times \xrightarrow{v} \mathbb{Z} \longrightarrow 0 \qquad (\dagger)$$

where v denotes the normalised valuation of L. We need to compute the cohomology of U_L and $\mathbb{Z}$.

To compute the cohomology of $\mathbb{Z}$, we use the exact sequence of G-modules (with trivial G-action)

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

Since $H_T^r(G,\mathbb{Q})$ is torsion and multiplication by any non-zero integer is an automorphism of $\mathbb{Q}$, we conclude that $H_T^r(G,\mathbb{Q})=0$ for all r. Hence we have that $H_T^r(G,\mathbb{Z}) = H_T^{r-1}(G,\mathbb{Q}/\mathbb{Z})$ for all r.

Next we compute the cohomology of U_L.

Theorem 4.1 *For all r we have that*

$$H_T^r(G,U_L)=0$$

Proof We have exact sequences of G-modules (via the isomorphism $G\approx\mathrm{Gal}(l/k)$)

$$0\to U_L^{(1)}\to U_L\to l^\times\to 0$$

$$0\to U_L^{(r+1)}\to U_L^{(r)}\to l^+\to 0$$

The group $H_T^r(G,l^+)$ is trivial for all r since l^+ is an induced module by the normal basis theorem (see appendix). We now show that the group $H_T^r(G,l^\times)$ is also trivial for all r. By the periodicity of cohomology of cyclic groups, it is enough to prove that for $r=0$ and $r=1$. The case $r=1$ is just Hilbert 90, while the case $r=0$ follows from the surjectivity of the norm map $N_{l/k}: l^\times\to k^\times$: if $k=\mathbb{F}_q$ and b is a generator of the group $l^\times$ then $N_{l/k}(b)=b^{1+q+\cdots+q^{n-1}}$ has order $q-1$ and hence is a generator of $k^\times$.

Hence, from the long exact sequences associated to the two short ones above, we conclude that $H_T^r(G,U_L^{(i+1)}) = H_T^r(G,U_L^{(i)})$ for all r and all $i\geq 0$. Now to show that $H_T^r(G,U_L)$ is trivial, again by periodicity we may assume $r>0$. Let $f\colon G^r\to U_L$ be an r-cocycle and denote by d the $(r-1)$-th coboundary map. Since $H^r(G,U_L^{(1)}) = H^r(G,U_L)$, f differs by a coboundary from an r-cocycle $f_1\colon G^r\to U_L^{(1)}$, i.e., there exists $g_0\colon G^{r-1}\to U_L$ such that $f_1 = f\cdot d(g_0)^{-1}$. Proceeding in this manner, we inductively construct functions $g_i\colon G^{r-1}\to U_L^{(i)}$ such that $f\cdot d(g_0g_1\ldots g_i)^{-1}$ is an r-cocycle with values in $U_L^{(i+1)}$. Then the product $g_0g_1\ldots g_i$ converges to a function $g\colon G^{r-1}\to U_L$ (multiplicative Calculus Student Psychedelic Dream!) and we have that $dg=f$, that is, the class $[f]$ is trivial in $H^r(G,U_L)$. □

The case $r = 0$ is of special interest, since it gives an unconditional proof of

Corollary 4.2 (Norm groups of unramified extensions) *Let $L \supset K$ be the unramified extension of degree n and let $\pi \in K$ be a common uniformiser. Then the norm map $N_{L/K}: U_L \to U_K$ is surjective and hence*

$$N_{L/K} L^\times = \pi^{n\mathbb{Z}} \cdot U_K$$

Back to the computation of $H^2(G, L^\times)$. From (†) and the fact that U_L has trivial cohomology, we conclude that the valuation v induces an isomorphism $H^2(G, L^\times) = H^2(G, \mathbb{Z})$. On the other hand, we have another isomorphism given by connecting map $\delta: H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\approx} H^2(G, \mathbb{Z})$. Putting everything together, we obtain a canonical isomorphism, called **invariant map**,

$$\mathrm{inv}_{L/K}: H^2(G, L^\times) \xrightarrow{\approx} \frac{\frac{1}{|G|}\mathbb{Z}}{\mathbb{Z}}$$

given by the composition

$$H^2(G, L^\times) \underset{\approx}{\xrightarrow{v}} H^2(G, \mathbb{Z}) \underset{\approx}{\xleftarrow{\delta}} H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{f \mapsto f(\Phi)} \frac{\frac{1}{|G|}\mathbb{Z}}{\mathbb{Z}}$$

where we write $\Phi \in G$ for the Frobenius automorphism.

If $M \supset L$ is another unramified extension with $H = \mathrm{Gal}(M/K)$ then following the isomorphisms above we obtain a commutative diagram

$$\begin{array}{ccc} H^2(H, M^\times) & \xrightarrow[\approx]{\mathrm{inv}_{M/K}} & \frac{\frac{1}{|H|}\mathbb{Z}}{\mathbb{Z}} \\ \inf \uparrow & & \uparrow \cup \\ H^2(G, L^\times) & \xrightarrow[\approx]{\mathrm{inv}_{L/K}} & \frac{\frac{1}{|G|}\mathbb{Z}}{\mathbb{Z}} \end{array}$$

where the left vertical arrow is given by inflation and the right vertical one is the inclusion map. Hence the invariant maps for the various unramified extensions of K fit together into a single invariant map

$$\boxed{\mathrm{inv}_K: H^2(G_K^{nr}, K_{nr}^\times) \xrightarrow{\approx} \mathbb{Q}/\mathbb{Z}}$$

(see the notation at the end of section 1).

Theorem 4.3 (Functorial property of the invariant map) *Let $K' \supset K$ be an arbitrary (possibly ramified) finite extension of local fields. We have a commutative diagram*

$$\begin{array}{ccc} H^2(G_{K'}^{nr}, K'^\times_{nr}) & \xrightarrow[\approx]{\mathrm{inv}_{K'}} & \mathbb{Q}/\mathbb{Z} \\ \mathrm{res} \uparrow & & \uparrow [K' : K] \\ H^2(G_K^{nr}, K_{nr}^\times) & \xrightarrow[\approx]{\mathrm{inv}_K} & \mathbb{Q}/\mathbb{Z} \end{array}$$

where the left vertical map is restriction and the right vertical one is multiplication by $[K' : K]$. Hence if $K' \supset K$ is an arbitrary finite Galois extension with $G = \mathrm{Gal}(K'/K)$ then $H^2(G, K'^\times)$ contains a cyclic group of order $|G|$.

Proof First we note that $K'_{nr} = K_{nr} \cdot K'$ by theorem I.5.1 and the unramified Highlander's Philosophy (corollary I.5.5) so that the restriction map on H^2 is well-defined. Let e and f be the ramification and inertia degrees of $K' \supset K$ and denote by v and v' the normalised valuations of K and K' respectively

so that $v'|_K = e \cdot v$. Observe that $\Phi_{K'}|_{K_{nr}} = \Phi_K^f$. Hence, from the definition of the invariant map, we obtain a commutative diagram

$$\begin{array}{ccccccc}
H^2(G_{K'}^{nr}, K'^{\times}_{nr}) & \xrightarrow{v'} & H^2(G_{K'}^{nr}, \mathbb{Z}) & \longrightarrow & \mathrm{Hom}_{ct}(G_{K'}^{nr}, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\
\uparrow{\scriptstyle \mathrm{res}} & & \uparrow{\scriptstyle e\cdot \mathrm{res}} & & \uparrow{\scriptstyle e\cdot \mathrm{res}} & & \uparrow{\scriptstyle ef} \\
H^2(G_K^{nr}, K_{nr}^{\times}) & \xrightarrow{v} & H^2(G_K^{nr}, \mathbb{Z}) & \longrightarrow & \mathrm{Hom}_{ct}(G_K^{nr}, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z}
\end{array}$$

Since $ef = [K' : K]$, the first result follows.

To show the second result, assume that $K' \supset K$ is finite Galois with $G = \mathrm{Gal}(K'/K)$. Using the inflation-restriction sequence and Hilbert 90, we conclude that the inflation maps

$$\inf\colon H^2(G_K^{nr}, K_{nr}^{\times}) \hookrightarrow H^2(G_K, K_{sp}^{\times}) \quad \text{and} \quad \inf\colon H^2(G_{K'}^{nr}, K'^{\times}_{nr}) \hookrightarrow H^2(G_{K'}, K_{sp}^{\times})$$

are injective. Identifying $H^2(G_K^{nr}, K_{nr}^{\times})$ and $H^2(G_{K'}^{nr}, K'^{\times}_{nr})$ with $\mathbb{Q}/\mathbb{Z}$ via inv_K and $\mathrm{inv}_{K'}$ and using the result just proven, we obtain a commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^2(G, K'^{\times}) & \xrightarrow{\inf} & H^2(G_K, K_{sp}^{\times}) & \xrightarrow{\mathrm{res}} & H^2(G_{K'}, K_{sp}^{\times}) \\
 & & & & \uparrow{\scriptstyle \inf} & & \uparrow{\scriptstyle \inf} \\
 & & & & H^2(G_K^{nr}, K_{nr}^{\times}) & \xrightarrow{\mathrm{res}} & H^2(G_{K'}^{nr}, K'^{\times}_{nr}) \\
 & & & & \| {\scriptstyle \mathrm{inv}_K} & & \| {\scriptstyle \mathrm{inv}_{K'}} \\
 & & & & \mathbb{Q}/\mathbb{Z} & \xrightarrow{[K' : K]} & \mathbb{Q}/\mathbb{Z}
\end{array}$$

We conclude that $H^2(G, K'^{\times})$ contains a subgroup isomorphic to $\frac{\frac{1}{[K':K]}\mathbb{Z}}{\mathbb{Z}}$, that is, a cyclic group of order $|G| = [K' : K]$. □

In order to show that $H^2(G, K'^{\times})$ actually equals $\frac{\frac{1}{[K':K]}\mathbb{Z}}{\mathbb{Z}}$, we shall bound the order of $H^2(G, K'^{\times})$ from above using a counting argument. Since G is solvable, it will be enough to do that assuming G cyclic. This is done in the next section.

5 Proof of the Local Reciprocity: conclusion

We begin by introducing a very useful tool in the cohomology of cyclic groups that will help simplify our counting argument.

Definition 5.1 Let G be a cyclic group and M be a G-module whose Tate cohomology groups are all finite. We define its **Herbrand quotient** as

$$\boxed{h(G, M) = \frac{|H_T^0(G, M)|}{|H_T^1(G, M)|}}$$

The Herbrand quotient plays the same role as the Euler characteristic in Topology. We have two main computational lemmas:

Lemma 5.2 (Multiplicativity) *Let G be a cyclic group and consider an exact sequence of G-modules*

$$0 \to M' \to M \to M'' \to 0$$

If two of the Herbrand quotients $h(G, M)$, $h(G, M')$, $h(G, M'')$ are defined (i.e. have finite Tate cohomology groups) then so is the third and

$$\boxed{h(G, M) = h(G, M') \cdot h(G, M'')}$$

PROOF From the periodicity of cohomology of cyclic groups, the long exact sequence associated to the above short one becomes an "exact hexagon"

$$\begin{array}{ccccc} H^0_T(G,M') & \xrightarrow{f^0} & H^0_T(G,M) & \xrightarrow{g^0} & H^0_T(G,M'') \\ & & & & \downarrow{\scriptstyle \delta^0} \\ \uparrow{\scriptstyle \delta^1} & & & & \\ & & & & \\ H^1_T(G,M'') & \xleftarrow{g^1} & H^1_T(G,M) & \xleftarrow{f^1} & H^1_T(G,M') \end{array}$$

The first result follows directly from from this hexagon. The second result also follows from this hexagon by elementary counting, as one has

$$\begin{array}{ll} |H^0_T(G,M')| = |\ker f^0| \cdot |\ker g^0| & |H^1_T(G,M')| = |\ker f^1| \cdot |\ker g^1| \\ |H^0_T(G,M)| = |\ker g^0| \cdot |\ker \delta^0| & |H^1_T(G,M)| = |\ker g^1| \cdot |\ker \delta^1| \\ |H^0_T(G,M'')| = |\ker \delta^0| \cdot |\ker f^1| & |H^1_T(G,M'')| = |\ker \delta^1| \cdot |\ker f^0| \end{array}$$

□

Lemma 5.3 (Finite Index Invariance) *Let G be a cyclic group, M be a G-module and M' be a G-submodule of finite index. Then $h(G,M')$ is defined if and only if $h(G,M)$ is defined, in which case $h(G,M') = h(G,M)$.*

PROOF By the last lemma, it suffices to show that if M is a finite group then $h(G,M) = 1$. Let σ be a generator of G. Since M is a finite group one has that $|H^0_T(G,M)| = |M^G|/|N_G(M)|$ and $|H^1_T(G,M)| = |\ker N_G|/|(\sigma-1)\cdot M|$. But $|M| = |\ker N_G| \cdot |N_G(M)|$ and similarly (since M^G is the kernel of multiplication by $\sigma - 1$) one has that $|M| = |M^G| \cdot |(\sigma-1)\cdot M|$, and the result follows. □

Let $L \supset K$ be a cyclic extension of local fields with Galois group G of order n. We apply the above to the exact sequence of G-modules

$$0 \to U_L \to L^\times \to \mathbb{Z} \to 0$$

induced by the valuation of L. It is easy to compute $h(G,\mathbb{Z}) = n$ and we have

Theorem 5.4 *With the above notation and hypotheses, $h(G,U_L) = 1$.*

PROOF By the previous lemma, it is enough to show that U_L contains an induced G-submodule of finite index. First assume that $\operatorname{char} K = 0$ and let π be a uniformiser of K. By lemma I.4.1 we have an isomorphism of G-modules $U_L^{(i)} \cong \mathfrak{m}_L^i$ for i sufficiently large. On the other hand, for j sufficiently large $\mathfrak{m}_L^i \supset \pi^j O_L \cong O_L$. Since $U_L/U_L^{(i)}$ and $\mathfrak{m}_L^i/\pi^j O_L$ are finite, it is enough to show that O_L contains an induced module of finite index. Now let $\omega_1,\ldots,\omega_n$ be a normal basis of $L \supset K$; multiplying by a convenient power of π we may assume that $\omega_1,\ldots,\omega_n \in O_L$. Since O_L is a finite O_K-module (theorem I.3.9), we have that the induced module $M = O_K\omega_1 + \cdots + O_K\omega_n$ has finite index in O_L.

Now we sketch a proof that works even if $\operatorname{char} K \neq 0$. Let M be as above. Multiplying the ω_i by a sufficiently large power of π we may assume that $M \cdot M \subset \pi M$. Then we may consider the submodule of finite index $V = 1 + M$ of U_L and the filtration given by $V^{(i)} = 1 + \pi^i M$ for $i \geq 0$. It is easy to show that we have an isomorphism of G-modules $V^{(i)}/V^{(i+1)} \cong M/\pi M$, which has trivial cohomology since the latter is induced. As in the proof of theorem 4.1, this implies that V itself has trivial cohomology. □

Hence we get $h(G,L^\times) = h(G,U_L)\cdot h(G,\mathbb{Z}) = n$. Since $H^1(G,L^\times)$ is trivial by Hilbert 90, we conclude that $|H^2(G,L^\times)| = n$ when G is cyclic. In general, for an arbitrary Galois extension we have

Theorem 5.5 *Let $L \supset K$ be an arbitrary finite Galois extension of local fields with $G = \operatorname{Gal}(L/K)$. Then the group $H^2(G,L^\times)$ is cyclic of order $|G|$.*

PROOF Since $H^2(G, L^\times)$ contains a cyclic group of order $|G|$ by theorem 4.3, it is enough to show that the order of $H^2(G, L^\times)$ divides $|G|$. For that, we use the special cyclic case above together with the fact that G is solvable (see theorem I.5.8). Alternatively, without resorting to theorem I.5.8, one may use the fact that $\text{res}\colon H^2(G, L^\times) \to H^2(G_p, L^\times)$ defines an injection on the p-primary components, where G_p is any p-Sylow subgroup of G (see appendix), and we may work with the solvable group G_p instead of G.

The proof is by induction on $|G|$. We already know the result for G cyclic. In general, let $H \lhd G$ be a normal subgroup such that H is cyclic and non-trivial. By Hilbert 90, we have an exact inflation-restriction sequence

$$0 \to H^2(G/H, (L^H)^\times) \to H^2(G, L^\times) \to H^2(H, L^\times)$$

Hence the order of $H^2(G, L^\times)$ divides the product of the orders of $H^2(H, L^\times)$ and $H^2(G/H, (L^H)^\times)$, which in turn divides $|H| \cdot |G/H| = |G|$ by induction hypothesis, and we are done. □

As a corollary, we obtain the following result that allows us to extend the invariant map of last section to the whole group $H^2(G_K, K_{sp}^\times)$. This map plays an important role in the study of division algebras over a local field.

Corollary 5.6 *Let K be a local field. We have an isomorphism*

$$\boxed{\text{inv}_K\colon H^2(G_K, K_{sp}^\times) \xrightarrow{\approx} \mathbb{Q}/\mathbb{Z}}$$

obtained by composing the inflation map $\text{inf}\colon H^2(G_K^{nr}, K_{nr}^\times) \xrightarrow{\approx} H^2(G_K, K_{sp}^\times)$ *and the invariant map* $\text{inv}_K\colon H^2(G_K^{nr}, K_{nr}^\times) \xrightarrow{\approx} \mathbb{Q}/\mathbb{Z}$ *of last section.*

PROOF By Hilbert 90 and the inflation-restriction sequence, we have an inclusion $\text{inf}\colon H^2(G_K^{nr}, K_{nr}^\times) \hookrightarrow H^2(G_K, K_{sp}^\times)$, which we now show to be also surjective. Since

$$H^2(G_K, K_{sp}^\times) = \varinjlim_{\substack{K' \text{ finite} \\ \text{Galois over } K}} H^2\big(\text{Gal}(K'/K), K'^\times\big),$$

given any $\gamma \in H^2(G_K, K_{sp}^\times)$ we can find a finite Galois extension K' such that

$$\gamma \in H^2\big(\text{Gal}(K'/K), K'^\times\big) = \ker\big(H^2(G_K, K_{sp}^\times) \xrightarrow{\text{res}} H^2(G_{K'}, K_{sp}^\times)\big)$$

(by Hilbert 90 and the inflation-restriction sequence the inflation maps in the above limit are injective, so we may view $H^2\big(\text{Gal}(K'/K), K'^\times\big)$ as a subgroup of $H^2(G_K, K_{sp}^\times)$ and we write γ also for the corresponding element in this subgroup). Now by theorem 4.3 and the above theorem, we have that $\text{inf}\colon H^2(G_K^{nr}, K_{nr}^\times) \hookrightarrow H^2(G_K, K_{sp}^\times)$ allows us to make the identification

$$\ker\big(H^2(G_K^{nr}, K_{nr}^\times) \xrightarrow{\text{res}} H^2(G_{K'}^{nr}, K'^\times{}_{nr})\big) = \ker\big(H^2(G_K, K_{sp}^\times) \xrightarrow{\text{res}} H^2(G_{K'}, K_{sp}^\times)\big)$$

(see the second diagram of the proof of theorem 4.3). Hence γ belongs to this kernel and a fortiori to (the inflation of) $H^2(G_K^{nr}, K_{nr}^\times)$. □

Finally, we are ready to make

Definition 5.7 For any finite abelian extension $L \supset K$ of local fields, we define the local reciprocity map $\theta_{L/K}\colon K^\times \to \text{Gal}(L/K)$ as the composition of the natural projection map $K^\times \twoheadrightarrow K^\times/N_{L/K}L^\times$ with the inverse of the Tate-Nakayama isomorphism

$$\text{Gal}(L/K) \xrightarrow{\approx} \frac{K^\times}{N_{L/K}L^\times}$$

given by the cup product with the unique element $\gamma \in H^2(\text{Gal}(L/K), L^\times)$ such that $\text{inv}_{L/K}(\gamma) = \frac{1}{[L:K]} \bmod \mathbb{Z}$. Such element γ is called a **fundamental class**.

To prove that the above isomorphism satisfies the two properties of theorem 2.1, we describe $\theta_{L/K}$ in terms of characters. Let $L \supset K$ be as above with $G = \mathrm{Gal}(L/K)$. Recall that we have two exact sequences of G-modules

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0 \qquad (*)$$

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0 \qquad (**)$$

where $\mathbb{Q}$ and $\mathbb{Z}[G]$ have trivial cohomology, hence the connecting maps

$$\delta\colon H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\approx} H^2(G, \mathbb{Z})$$
$$\delta_a\colon H_T^{-2}(G, \mathbb{Z}) \xrightarrow{\approx} H_T^{-1}(G, I_G)$$

are isomorphisms. Besides we have a natural isomorphism $G^{ab} = H_T^{-1}(G, I_G)$ given by

$$G^{ab} \xrightarrow{\approx} H_T^{-1}(G, I_G) = \frac{I_G}{I_G^2}$$
$$\sigma \cdot [G : G] \mapsto (\sigma - 1) \cdot I_G^2$$

Theorem 5.8 (Local Reciprocity Revisited) *With the above notation, for any $a \in K^\times$ and any character $\chi \in H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ one has*

$$\boxed{\chi\big(\theta_{L/K}(a)\big) = \mathrm{inv}_K(\bar{a} \cup \delta\chi)}$$

where $\bar{a}$ is the image of a in $H_T^0(G, L^\times) = K^\times / N_{L/K} L^\times$. In other words, the cup product gives a perfect pairing

$$\begin{array}{ccccc}
H_T^0(G, L^\times) \otimes H_T^2(G, \mathbb{Z}) & \xrightarrow{\cup} & H_T^2(G, L^\times) & \xrightarrow{\inf} & H_T^2(G_K, K_{sp}^\times) \\
\Big\uparrow{\scriptstyle \mathrm{id}\otimes\delta}\ \Big|{\scriptstyle \approx} & & \Big\downarrow{\scriptstyle \approx} & & \Big\downarrow{\scriptstyle \approx}\ {\scriptstyle \mathrm{inv}_K} \\
\dfrac{K^\times}{N_{L/K}L^\times} \otimes \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \dfrac{\frac{1}{|G|}\mathbb{Z}}{\mathbb{Z}} & \hookrightarrow & \mathbb{Q}/\mathbb{Z}
\end{array}$$

Proof Let $\gamma \in H^2(G, L^\times)$ be the fundamental class and $n = |G|$. Given $a \in K^\times$ and $\chi \in H^1(G, \mathbb{Q}/\mathbb{Z})$, write $\sigma \overset{\mathrm{df}}{=} \theta_{L/K}(a) \in G$ and $\chi(\sigma) = \frac{i}{n} \bmod \mathbb{Z}$ with $0 \le i < n$. Since $\mathrm{inv}_K(\gamma) = \frac{1}{n} \bmod \mathbb{Z}$, in order to show that $\chi(\sigma) = \mathrm{inv}_K(\bar{a} \cup \delta\chi)$ we have to show that $\bar{a} \cup \delta\chi = i \cdot \gamma$ in $H^2(G, L^\times)$. However by the very definition of $\theta_{L/K}$ we have that $\bar{\sigma} \cup \gamma = \bar{a}$, where $\bar{\sigma} \in H_T^{-2}(G, \mathbb{Z})$ denotes the image of σ under the isomorphism $H_T^{-2}(G, \mathbb{Z}) = G^{ab} = G$. Hence

$$\bar{a} \cup \delta\chi = \bar{\sigma} \cup \gamma \cup \delta\chi = \bar{\sigma} \cup \delta\chi \cup \gamma$$

and we are left to show that $\bar{\sigma} \cup \delta\chi = i \bmod n$ in $H_T^0(G, \mathbb{Z})$. Note that $\bar{\sigma} \cup \delta\chi = \delta(\bar{\sigma} \cup \chi)$ and by the lemma below $\bar{\sigma} \cup \chi \in H_T^{-1}(G, \mathbb{Q}/\mathbb{Z})$ is represented by $\chi(\sigma) = \frac{i}{n} \bmod \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. On the other hand, the connecting map $\delta\colon H_T^{-1}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\approx} H_T^0(G, \mathbb{Z})$ is induced by the norm map (see appendix), which in our case is just multiplication by n. Hence $\delta(\bar{\sigma} \cup \chi) = i \bmod n$, as required.

Finally, the above identity implies that the pairing

$$H_T^0(G, L^\times) \otimes H_T^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow[\approx]{\mathrm{id}\otimes\delta} H_T^0(G, L^\times) \otimes H_T^2(G, \mathbb{Z}) \xrightarrow{\cup} H_T^2(G, L^\times)$$

is perfect. In fact, if $\chi \in H_T^1(G, \mathbb{Q}/\mathbb{Z})$ is such that $\bar{a} \cup \delta\chi = 0 \iff \chi(\theta_{L/K}(a)) = 0$ for all $a \in K^\times$ then $\chi = 0$ since $\theta_{L/K}\colon K^\times \twoheadrightarrow \mathrm{Gal}(L/K)$ is surjective. On the other hand, if $a \in K^\times$ is such that $\bar{a} \cup \delta\chi = 0 \iff \chi(\theta_{L/K}(a)) = 0$ for all $\chi \in H_T^1(G, \mathbb{Q}/\mathbb{Z})$ then clearly $\theta_{L/K}(a) = 0 \iff a \in \ker\theta_{L/K} = N_{L/K}L^\times$ and thus $\bar{a} = 0$, showing that the left kernel of this pairing is also trivial. □

Lemma 5.9 *Let G be a finite group and A and B be G-modules. Let $f: G \to B$ be a 1-cocycle.*

1. *for $a \in \ker(A \xrightarrow{N_G} A)$, the cup product of $[a] \in H_T^{-1}(G, A)$ and $[f] \in H_T^1(G, B)$ is given by*
$$[a] \cup [f] = -\Big[\sum_{\sigma \in G} \sigma(a) \otimes f(\sigma)\Big] \in H_T^0(G, A \otimes B)$$
Here brackets denote the corresponding cohomology classes.
2. *for $\sigma \in G$ denote by $\bar{\sigma} \in H_T^{-2}(G, \mathbb{Z})$ the image of σ under the isomorphism $G^{ab} \approx H_T^{-2}(G, \mathbb{Z})$. Then*
$$\bar{\sigma} \cup [f] = [f(\sigma)] \in H_T^{-1}(G, B)$$

Proof We use dimension shifting. Write an exact sequence of G-modules
$$0 \to B \to B' \to B'' \to 0$$
with B' induced, and such that it is *split* as a sequence of abelian groups, so that
$$0 \to A \otimes B \to A \otimes B' \to A \otimes B'' \to 0$$
is still exact (check the appendix for more details). Then the connecting map $\delta: H_T^0(G, B'') \xrightarrow{\approx} H_T^1(G, B)$ is an isomorphism and thus we may write $[f] = \delta[b'']$ for some $b'' \in B''^G$ and
$$[a] \cup [f] = [a] \cup \delta[b''] = -\delta[a \otimes b'']$$
On the other hand, the connecting map $\delta: H_T^{-1}(G, A \otimes B'') \to H_T^0(G, A \otimes B)$ is induced by the norm. There exists a pre-image $b' \in B'$ of b'' such that $f(\sigma) = \sigma(b') - b' \in B$ for all $\sigma \in G$. Since $a \otimes b'$ is a pre-image of $a \otimes b''$ under $A \otimes B' \to A \otimes B''$, we conclude that $\delta[a \otimes b'']$ is represented by
$$\begin{aligned} N_G(a \otimes b') &= \sum_{\sigma \in G} \sigma a \otimes \sigma(b') = \sum_{\sigma \in G} \sigma a \otimes f(\sigma) + \sum_{\sigma \in G} \sigma a \otimes b' \\ &= \sum_{\sigma \in G} \sigma a \otimes f(\sigma) + N_G(a) \otimes b' = \sum_{\sigma \in G} \sigma a \otimes f(\sigma) \end{aligned}$$

To show 2, observe that tensoring the augmentation sequence $(**)$ with B we obtain an exact sequence
$$0 \to I_G \otimes B \to \mathbb{Z}[G] \otimes B \to \mathbb{Z} \otimes B = B \to 0$$
since $\mathbb{Z}$ is a free $\mathbb{Z}$-module and hence $\operatorname{Tor}_1^{\mathbb{Z}}(B, \mathbb{Z}) = 0$. Since $\mathbb{Z}[G] \otimes B$ is induced (see appendix), we have that the connecting map $\delta_a: H_T^{-1}(G, B) \xrightarrow{\approx} H_T^0(G, I_G \otimes B)$ is an isomorphism, hence it suffices to show that $\delta_a(\bar{\sigma} \cup [f]) = \delta_a[f(\sigma)]$. Since $\delta_a(\bar{\sigma} \cup [f]) = \delta_a(\bar{\sigma}) \cup [f]$ and $\delta_a(\bar{\sigma}) = [\sigma - 1] \in H_T^{-1}(G, I_G)$, applying 1 we obtain
$$\begin{aligned} \delta_a(\bar{\sigma} \cup [f]) = [\sigma - 1] \cup [f] &= -\Big[\sum_{\tau \in G} \tau(\sigma - 1) \otimes f(\tau)\Big] \\ &= \Big[\sum_{\tau \in G} \tau \otimes f(\tau) - \sum_{\tau \in G} \tau\sigma \otimes f(\tau)\Big] = \Big[\sum_{\tau \in G} \tau\sigma \otimes f(\tau\sigma) - \sum_{\tau \in G} \tau\sigma \otimes f(\tau)\Big] \\ &= \Big[\sum_{\tau \in G} \tau\sigma \otimes \tau f(\sigma)\Big] \in H_T^0(G, I_G \otimes B) \end{aligned}$$

On the other hand, since $\delta_a: H_T^{-1}(G, B) \xrightarrow{\approx} H_T^0(G, I_G \otimes B)$ is induced by the norm and $1 \otimes f(\sigma) \in \mathbb{Z}[G] \otimes B$ is a pre-image of $f(\sigma) \in B = \mathbb{Z} \otimes B$ we have that
$$\delta_a[f(\sigma)] = \big[N_G\big(1 \otimes f(\sigma)\big)\big] = \Big[\sum_{\tau \in G} \tau \otimes \tau f(\sigma)\Big] \in H_T^0(G, I_G \otimes B)$$
Hence the two classes $\delta_a(\bar{\sigma} \cup [f])$ and $\delta_a[f(\sigma)]$ are equal in $H_T^0(G, I_G \otimes B)$ since
$$\sum_{\tau \in G} \tau\sigma \otimes \tau f(\sigma) - \sum_{\tau \in G} \tau \otimes \tau f(\sigma) = \sum_{\tau \in G} \tau(\sigma - 1) \otimes \tau f(\sigma) = N_G\big((\sigma - 1) \otimes f(\sigma)\big) \in N_G(I_G \otimes B)$$

□

Using the description of the reciprocity map given in theorem 5.8, it is easy to show that for an unramified extension of local fields $L \supset K$ one has $\theta_{L/K}(a) = \Phi_{L/K}^{v(a)}$, where v denotes the normalised valuation of K and $\Phi_{L/K}$ is the Frobenius automorphism of $L \supset K$. In fact, let $n = [L : K]$ and $G = \mathrm{Gal}(L/K)$ and consider the character $\chi\colon G \to \mathbb{Q}/\mathbb{Z}$ given by $\chi(\Phi_{L/K}) = \frac{1}{n} \bmod \mathbb{Z}$. Then $\bar{a} \cup \delta\chi$ is represented by the 2-cocycle $c\colon G \times G \to L^\times$ given by

$$c(\Phi_{L/K}^i, \Phi_{L/K}^j) = \begin{cases} a & \text{if } i + j \geq 0 \\ 0 & \text{otherwise} \end{cases} \qquad 0 \leq i, j < n$$

Now since the invariant map is given by the composition

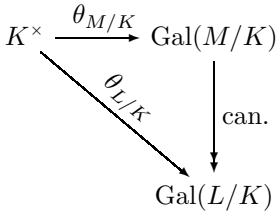
$$H^2(G, L^\times) \xrightarrow[\approx]{v} H^2(G, \mathbb{Z}) \xleftarrow[\approx]{\delta} H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \approx \mathbb{Q}/\mathbb{Z}$$

and $v([c]) = \delta[f]$ where $f\colon G \to \mathbb{Q}/\mathbb{Z}$ is the 1-cocycle given by $f(\Phi_{L/K}) = \frac{v(a)}{n} \bmod \mathbb{Z}$, we conclude that

$$\chi\big(\theta_{L/K}(a)\big) = \mathrm{inv}_K(\bar{a} \cup \delta\chi) = \mathrm{inv}_K([c]) = \frac{v(a)}{n} \bmod \mathbb{Z} = \chi(\Phi_{L/K}^{v(a)})$$

showing that $\theta_{L/K}(a) = \Phi_{L/K}^{v(a)}$ since χ is injective.

We can also show the compatibility of the various maps $\theta_{L/K}$ in the sense that given finite extensions $M \supset L \supset K$ with M and L abelian over K we have a commutative diagram



This will prove that the maps $\theta_{L/K}$ fit together into a single map $\theta_K\colon K^\times \to G_K^{ab}$, which will then satisfy all the properties required in theorem 2.1.

Let $a \in K^\times$, let $\chi \in \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$ and denote by $\chi' = \inf(\chi) \in \mathrm{Hom}(\mathrm{Gal}(M/K), \mathbb{Q}/\mathbb{Z})$. Then $\inf(\bar{a} \cup \delta\chi) = \bar{a} \cup \delta\chi'$ and thus

$$\chi(\theta_{L/K}(a)) = \mathrm{inv}_K(\bar{a} \cup \delta\chi) = \mathrm{inv}_K(\bar{a} \cup \delta\chi') = \chi'(\theta_{M/K}(a)) = \chi(\theta_{M/K}(a)|_L)$$

Since this holds for all $\chi \in \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$, we conclude that $\theta_{L/K}(a) = \theta_{M/K}(a)|_L$, as was to be shown.

With the above, we finish the proof of the local reciprocity theorem. Hurray!

6 Hilbert Symbol and Proof of Existence Theorem

In this section, we prove the existence theorem, and for that we shall need a few results from Kummer theory and its relation with local reciprocity. This is accomplished in the first subsection.

6.1 Hilbert symbol

For any field K and any positive integer n prime to $\mathrm{char}\, K$, denote by $\mu_n \subset K_{sp}^\times$ the group of n-th roots of 1 of K.

Definition 6.1.1 Let K be a local field such that $K \supset \mu_n$. For $a, b \in K^\times$ we define the **Hilbert symbol** (a, b) as

$$(a, b) \stackrel{\mathrm{df}}{=} \frac{\theta_K(b)(\alpha)}{\alpha} \in \mu_n \qquad \text{where} \quad \alpha^n = a, \quad \alpha \in K_{sp}^\times$$

Observe that since $K \supset \mu_n$ this definition is independent of the choice of α.

Lemma 6.1.2 *Let K be a local field such that $K \supset \mu_n$. The Hilbert symbol $(-,-)\colon K^\times \times K^\times \to \mu_n$ has the following properties:*

1. *Bilinearity: for all $a, a_1, a_2, b, b_1, b_2 \in K^\times$,*
$$(a_1 \cdot a_2, b) = (a_1, b) \cdot (a_2, b) \quad \text{and} \quad (a, b_1 \cdot b_2) = (a, b_1) \cdot (a, b_2)$$
2. *Steinberg relations: $(a, 1-a) = 1$ for all $a \neq 0, 1$ and $(a, -a) = 1$ for all $a \in K^\times$*
3. *Skew-symmetry: $(a, b) = (b, a)^{-1}$ for all $a, b \in K^\times$*
4. *$(a, b) = 1$ if and only if $b \in N_{L/K} L^\times$ where $L = K(\sqrt[n]{a})$*
5. *The Hilbert symbol gives a perfect pairing $K^\times/(K^\times)^n \times K^\times/(K^\times)^n \to \mu_n$: if $a \in K^\times$ is such that $(a, b) = 1$ for all $b \in K^\times$ then $a \in (K^\times)^n$, and similarly for the other entry.*

Proof Write $\alpha = \sqrt[n]{a}$. The Hilbert symbol is clearly linear in the first entry, and also in the second since $\theta_K(b_2)(\alpha)$ is an n-th root of a and thus

$$(a, b_1 \cdot b_2) = \frac{\theta_K(b_1 b_2)(\alpha)}{\alpha} = \frac{\theta_K(b_1)\big(\theta_K(b_2)(\alpha)\big)}{\theta_K(b_2)(\alpha)} \cdot \frac{\theta_K(b_2)(\alpha)}{\alpha} = (a, b_1) \cdot (a, b_2)$$

Also, 4 is a direct consequence of the definition of the Hilbert symbol and the reciprocity theorem 2.1. Now we show that $4 \Rightarrow 2$. Since (a, b) is a $[L : K]$-th root of 1 (by Kummer theory for instance), we may wlog assume that $[L : K] = n$. Let ζ be a primitive n-th root of 1. Then

$$x^n - a = \prod_{0 \le i \le n} (x - \zeta^i \alpha) \Rightarrow \begin{cases} 1 - a = N_{L/K}(1 - \alpha) \\ -a = N_{L/K}(-\alpha) \end{cases}$$

and hence $(a, 1-a) = 1$ and $(a, -a) = 1$ by 4 (actually, $(a, -a) = 1$ can be shown to be a formal consequence of bilinearity and the identity $(a, 1-a) = 1$, as the reader may verify).

Now we show that 3 follows formally from 1 and 2. In fact:

$$(ab, -ab) = 1 \iff (a, -a) \cdot (a, b) \cdot (b, a) \cdot (b, -b) = 1 \iff (a, b) \cdot (b, a) = 1$$

Finally, suppose that $(a, b) = 1$ for all $b \in K^\times$, and let $L = K(\alpha)$ as above. Since $\theta_{L/K}\colon K^\times \twoheadrightarrow \mathrm{Gal}(L/K)$ is surjective (see theorem 2.1) we conclude that $\alpha \in K$, i.e., $a \in (K^\times)^n$, as was to be shown. By the skew-symmetry 3, the same holds for the other entry, and we are done. □

Properties 3–5 immediately yield the following interesting corollary, which will be used below in the proof of the Existence Theorem.

Corollary 6.1.3 *Let n be a positive integer and let K be a local field containing a primitive n-th root of 1. If an element $a \in K^\times$ belongs to $N_{L/K} L^\times$ for every cyclic extension $L \supset K$ of degree n then $a \in (K^\times)^n$.*

The Hilbert symbol can be defined more intrinsically in terms of the so-called **Galois symbol**. Recall that for any field K and any positive integer n prime to $\mathrm{char}\, K$ (we do not assume $K \supset \mu_n$), we have an exact sequence of G_K-modules (the **Kummer sequence**)

$$1 \longrightarrow \mu_n \longrightarrow K_{sp}^\times \xrightarrow{\ n\ } K_{sp}^\times \longrightarrow 1$$

where the last map is given by $x \mapsto x^n$. By Hilbert 90 the connecting map $\partial\colon K^\times \to H^1(G_K, \mu_n)$ induces an isomorphism $K^\times/(K^\times)^n = H^1(G_K, \mu_n)$, and we also have that $H^2(G_K, \mu_n)$ is the n-torsion of $H^2(G_K, K_{sp}^\times)$. Explicitly, ∂a is given by the 1-cocycle $\sigma \mapsto \sigma(\alpha)/\alpha \in \mu_n$ where $\alpha = \sqrt[n]{a}$ is any n-th root of a in K_{sp}.

The Galois symbol is defined to be the pairing $\{-,-\}\colon K^\times \times K^\times \to H^2(G_K, \mu_n \otimes \mu_n)$ given by

$$K^\times \otimes K^\times \xrightarrow{\partial \otimes \partial} H^1(G_K, \mu_n) \otimes H^1(G_K, \mu_n) \xrightarrow{\ \cup\ } H^2(G_K, \mu_n \otimes \mu_n) \qquad (\dagger)$$

It has the following properties:

1. Bilinearity: $\{a_1 \cdot a_2, b\} = \{a_1, b\} \cdot \{a_2, b\}$ and $\{a, b_1 \cdot b_2\} = \{a, b_1\} \cdot \{a, b_2\}$
2. Steinberg relations: $\{a, 1-a\} = 1$ for all $a \neq 0, 1$ and $\{a, -a\} = 1$ for all $a \in K^\times$
3. Skew-symmetry: $\{a, b\} = \{b, a\}^{-1}$ for all $a, b \in K^\times$
4. If $\mu_n \subset K$ then $\{a, b\} = 1 \iff a \in N_{L/K} L^\times$ where $L = K(\sqrt[n]{b})$.

Property 1 is clear, and 2–3 are formal consequences of $\{a, 1-a\} = 1$ (one can also prove 3 using the skew-symmetry of the cup product). To prove the last Steinberg relation, one factors $x^n - a = \prod_i f_i(x)$ into irreducible polynomials $f_i(x) \in K[x]$ and set $K_i = K(\alpha_i)$ where $\alpha_i \in K_{sp}$ is any root of $f_i(x)$. Then

$$\{1-a, a\} = \prod_i \{N_{K_i/K}(1-\alpha_i), a\} = \prod_i \mathrm{cor}_{K_i/K}\{1-\alpha_i, a\} = \prod_i \mathrm{cor}_{K_i/K}\{1-\alpha_i, \alpha_i\}^n = 1$$

where $\mathrm{cor}_{K_i/K}\colon H^2(G_{K_i}, \mu_n \otimes \mu_n) \to H^2(G_K, \mu_n \otimes \mu_n)$ is the corestriction map.

Finally, to show 4 let $\zeta \in K$ be a primitive n-th root of unity. The choice of ζ defines a *non-canonical* isomorphism of G_K-modules $\phi_\zeta\colon \mu_n \to \mathbb{Z}/n$ given by $\phi_\zeta(\zeta) = 1 \bmod n$ and hence we obtain a commutative diagram

$$\begin{array}{ccc} H^1(G_K, \mu_n) \otimes H^1(G_K, \mu_n) & \xrightarrow{\cup} & H^2(G_K, \mu_n \otimes \mu_n) \\ \Big\downarrow{\scriptstyle \mathrm{id}\otimes\phi_\zeta} & \cong & \Big\downarrow{\scriptstyle \cong\ \mathrm{id}\otimes\phi_\zeta} \\ H^1(G_K, \mu_n) \otimes H^1(G_K, \mathbb{Z}/n) & \xrightarrow{\cup} & H^2(G_K, \mu_n) \end{array}$$

where the vertical arrows are isomorphisms. Then the symbol $\{a, b\}$ corresponds to the element $\partial a \cup \chi_b \in H^2(G_K, \mu_n)$ where $\chi_b \in H^1(G_K, \mathbb{Z}/n)$ is the character given by $\chi_b(\sigma) = \phi_\zeta\big(\partial b(\sigma)\big) = \phi_\zeta\big(\sigma(\sqrt[n]{b})/\sqrt[n]{b}\big)$. Hence we have to show that $\partial a \cup \chi_b = 0 \iff a \in N_{L/K} L$ where $L = K_{sp}^{\ker \chi_b} = K(\sqrt[n]{b})$ denotes the cyclic extension of K defined by χ_b.

We make the identifications $H^1(G_K, \mathbb{Z}/n) = {}_nH^1(G_K, \mathbb{Q}/\mathbb{Z})$ and ${}_nH^2(G_K, K_{sp}^\times) = H^2(G_K, \mu_n)$ where the subscript denotes the n-torsion part of the corresponding groups. Now an explicit computation shows that, for all $a \in K^\times$ and $\chi \in H^1(G_K, \mathbb{Z}/n) = {}_nH^1(G_K, \mathbb{Q}/\mathbb{Z})$,

$$a \cup \delta\chi = -\partial a \cup \chi \in {}_nH^2(G_K, K_{sp}^\times) = H^2(G_K, \mu_n)$$

where δ is as in theorem 5.8. In fact, let $G = G_K/\ker\chi$ and σ be a generator of the cyclic group G. Let $n = |G|$ and $0 \leq t < n$ be such that $\chi(\sigma) = t \bmod n$. We have that $a \cup \delta\chi$ and $-\partial a \cup \chi$ are represented by the inflations of the 2-cocycles $f\colon G \times G \to L^\times$ and $g\colon G \times G \to \mu_n$ given by

$$f(\sigma^i, \sigma^j) = \begin{cases} a^t & \text{if } i+j \geq n \\ 1 & \text{otherwise} \end{cases} \qquad \text{and} \qquad g(\sigma^i, \sigma^j) = \Big(\frac{\sigma^i \sqrt[n]{a}}{\sqrt[n]{a}}\Big)^{-j \cdot t} \qquad \text{for } 0 \leq i, j < n$$

and it is easy to check that they differ by the coboundary of the function $h\colon G \to L^\times$ given by

$$h(\sigma^i) = (\sqrt[n]{a})^{i \cdot t} \qquad \text{for } 0 \leq i < n$$

We apply the above to $\chi = \chi_b$ and $G = \mathrm{Gal}(L/K)$. Since the cup product $- \cup \delta\chi_b$ gives an isomorphism $H_T^0(G, L^\times) \cong H_T^2(G, L^\times) \subset H^2(G_K, K_{sp}^\times)$ (see appendix) we have that

$$\partial a \cup \chi_b = 0 \iff a \cup \delta\chi_b = 0 \iff a \in N_{L/K} L^\times$$

as was to be shown.

What all this has to do with the Hilbert symbol? We now specialise the above discussion to the case when K is a local field containing μ_n. Since $H^2(G_K, \mu_n)$ is the n-torsion of $H^2(G_K, K_{sp}^\times) \overset{\mathrm{inv}_K}{=} \mathbb{Q}/\mathbb{Z}$, we have that $H^2(G_K, \mu_n) = \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ and thus we obtain a *canonical* isomorphism

$$H^2(G_K, \mu_n \otimes \mu_n) \xleftarrow[\approx]{\cup} H^2(G_K, \mu_n) \otimes H^0(G_K, \mu_n) \xrightarrow[\approx]{\mathrm{inv}_K \otimes \mathrm{id}} \frac{\frac{1}{n}\mathbb{Z}}{\mathbb{Z}} \otimes \mu_n = \mu_n$$

which allows us to write the Galois symbol pairing (†) simply as a pairing $K^\times \otimes K^\times \to \mu_n$. We claim that this pairing is precisely the Hilbert symbol. In fact, let $\zeta \in K$ be a primitive n-th root of 1; given $a, b \in K^\times$, the pairing we have just defined takes $a \otimes b$ to

$$\zeta^{n\cdot \mathrm{inv}_K(\partial a \cup \chi_b)} = \zeta^{-n\cdot \mathrm{inv}_K(a \cup \delta\chi_b)} = \zeta^{-\chi_b(\theta_K(a))}$$

by the reciprocity theorem 5.8. Here χ_b is defined via ϕ_ζ using the *same* chosen root of unity ζ, so that the dependency on this choice "cancels." Now if $\beta = \sqrt[n]{b}$ by definition of χ_b we have that

$$\zeta^{-\chi_b(\theta_K(a))} = \left(\frac{\theta_K(a)(\beta)}{\beta}\right)^{-1} = (b,a)^{-1} = (a,b)$$

proving the claim. This shows that properties 1–4 of the lemma are consequences of the corresponding properties of the Galois symbol. The reciprocity is only needed to show the perfectness of the pairing.

Remark 6.1.4 When K has positive characteristic p, one has an exact sequence of G_K-modules (the **Artin-Schreier** sequence)

$$0 \longrightarrow \mathbb{Z}/p \longrightarrow K_{sp}^+ \xrightarrow{\wp} K_{sp}^+ \longrightarrow 0$$

where $\wp(x) = x^p - x$. Then it is possible to define a pairing

$$K^+ \times K^\times \to \mathbb{Z}/p$$

taking $a \in K^+$ and $b \in K^\times$ to $[a,b) \stackrel{\mathrm{df}}{=} \delta\psi_a \cup b \in H^2(G_K, K_{sp}^\times)$ where the character $\psi_a \in H^1(G_K, \mathbb{Z}/p)$ is defined to be the image of a with respect to the connecting map of the Artin-Schreier sequence.
One shows that for a local field K

$$[a,b) = \theta_K(b)(\alpha) - \alpha \in \mathbb{Z}/p \qquad \text{where} \qquad \wp(\alpha) = a$$

and that this pairing satisfies

1. Bilinearity: $[a_1 + a_2, b) = [a_1, b) + [a_2, b)$ and $[a, b_1 b_2) = [a, b_1) + [a, b_2)$
2. Steinberg relation: $[a, -a) = 0$ for all $a \neq 0$
3. $[a,b) = 0 \iff b \in N_{L/K}L^\times$ where $L = K(\alpha)$ with $\wp(\alpha) = a$
4. If $[a,b) = 0$ for all $b \in K^\times$ then $a \in \wp(K^+)$.

The proofs are mutatis mutandis the same as for the Hilbert symbol; we refer the reader to Serre's "Local Fields" for further details.

Lemma 6.1.5 *Let p be a prime, q be a power of p and $K = \mathbb{F}_q((t))$. If an element $b \in K^\times$ belongs to $N_{L/K}L^\times$ for every cyclic extension $L \supset K$ of degree p then $b \in (K^\times)^p$.*

Proof We sketch the proof and refer the reader to Serre's book for details. For any $a \in K^+$ and $b \in K^\times$ one has **Schmid's formula**

$$[a,b) = T_{\mathbb{F}_q/\mathbb{F}_p} \operatorname{res}\Big(a \cdot \frac{db}{b}\Big)$$

where $db/b = (\sum_{n\geq n_0} n c_n t^{n-1}) \cdot (\sum_{n\geq n_0} c_n t^n)^{-1}$ is the *logarithmic derivative* of $b = \sum_{n\geq n_0} c_n t^n$, and res denotes the *residue*, that is, the coefficient of t^{-1}. Schmid's formula can be proved by an explicit computation using the above properties of the pairing $[-,-)$.

Now if $b \in N_{L/K}L^\times$ for every cyclic extension $L \supset K$ of degree p then $[a,b) = 0$ for all $a \in K^+$. If b were not a p-th power then $db/b \neq 0$, and we would be able to find a such that $\operatorname{res}\big(a \cdot \frac{db}{b}\big) = c$ for any given $c \in \mathbb{F}_q$. But then by Schmid's formula $[a,b) = T_{\mathbb{F}_q/\mathbb{F}_p}(c) = 0$ for all $c \in \mathbb{F}_q$, contradicting the fact that the trace is surjective. □

6.2 Proof of the Existence Theorem

Now we are ready to prove the existence theorem. First we remark that in the definition of a norm group $N_{L/K}L^\times$ it is indifferent whether we require $L \supset K$ to be an abelian Galois extension or not:

Theorem 6.2.1 (Norm Limitation) *Let $L \supset K$ be a finite separable extension of local fields and let E be the maximal abelian extension of K contained in L. Then $N_{E/K}E^\times = N_{L/K}L^\times$.*

PROOF Let M be a finite Galois extension of K that contains L, let $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$ so that E is the fixed field of $H \cdot [G : G]$. Since the cup product commutes with corestriction, we have a commutative diagram (check!)

$$\begin{array}{ccc} \dfrac{L^\times}{N_{M/L}M^\times} & \xrightarrow[\approx]{\theta_{M/L}} & \dfrac{H}{[H:H]} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \text{can.}} \\ \dfrac{K^\times}{N_{M/K}M^\times} & \xrightarrow[\approx]{\theta_{M/K}} & \dfrac{G}{[G:G]} \end{array}$$

where the horizontal arrows are isomorphisms by the reciprocity theorem. Therefore $\theta_{M/K}$ gives an isomorphism between the cokernels of two vertical arrows and thus $[K^\times : N_{L/K}L^\times] = \big[G : H \cdot [G : G]\big] = |\operatorname{Gal}(E/K)|$. But we also have an isomorphism $\theta_{E/K}\colon K^\times/N_{E/K}E^\times \approx \mathrm{Gal}(E/K)$ and hence both $N_{E/K}E^\times$ and $N_{L/K}L^\times$ have the same index in $K^\times$. However $N_{E/K}E^\times \supset N_{L/K}L^\times$ since $E \subset L$ and therefore we must have $N_{E/K}E^\times = N_{L/K}L^\times$. □

Before plunging into the proof of the existence theorem let us make a couple of the preliminary observations. Let G be any topological group and $H \leq G$ be a subgroup. If H is open then it is also closed, since H is the complement of the union of its (open) left cosets different from H. The very same argument shows that if H is closed and of finite index then H is also open so that for subgroups of finite index "open" and "closed" are equivalent notions. Moreover in order to show that H is open it is enough to show that it contains an open subgroup T, for then H will be the union of the left translates of T. Finally observe that the norm map $N_{L/K}\colon L \to K$ is continuous for all finite extensions $L \supset K$ of local fields since it is given by a product of automorphisms of some finite Galois extension M of K, and these automorphisms are continuous since they preserve the valuation of M (Highlander's Philosophy!).

We first show the easy direction of the existence theorem:

Lemma 6.2.2 *Let $L \supset K$ be a finite extension of local fields. Then $N_{L/K}L^\times$ is an open (and closed) subgroup of finite index of $K^\times$. Moreover the kernel of $N_{L/K}\colon L^\times \to K^\times$ is compact.*

PROOF We already know that $N_{L/K}L^\times$ has finite index in $K^\times$ by the reciprocity theorem 2.1. Also, $U_K \cap N_{L/K}L^\times = N_{L/K}U_L$ (see the formula for the valuation of L in theorem I.3.4), so that we have an injection $U_K/N_{L/K}U_L \hookrightarrow K^\times/N_{L/K}L^\times$ showing that $N_{L/K}U_L$ also has finite index in U_K. Since U_L is compact, $N_{L/K}U_L$ is compact and hence closed and open in U_K (since the latter group is Hausdorff). Since U_K is open in $K^\times$ we have that $N_{L/K}U_L$ is open in $K^\times$ as well. Therefore $N_{L/K}L^\times$ is open too as it contains the open subgroup $N_{L/K}U_L$. Moreover since $N_{L/K}$ is continuous we have that $\ker N_{L/K}$ is closed. And since it is contained in the compact subgroup U_L we conclude that $\ker N_{L/K}$ is compact as well. □

We now prove the converse. Let K is a local field and $T \subset K^\times$ be an open subgroup of finite index. First observe that if T contains a norm group $N_{L/K}L^\times$ for some finite abelian extension $L \supset K$ then T itself is a norm group: by the functorial properties of the reciprocity map we have that $T = N_{M/K}M^\times$ where $M = L^{\theta_K T}$. Also the intersection of two norm groups $N_{L_1/K}L_1^\times$ and $N_{L_2/K}L_2^\times$ is a norm group, namely the norm group of the compositum $L_1 \cdot L_2$. Hence the family of norm groups is *directed* (i.e. the intersection of any two members of this family contains a third member).

Definition 6.2.3 Let K be a field. Then the **universal norm group** D_K of K is defined to be the intersection of all norm groups:

$$D_K \stackrel{\mathrm{df}}{=} \bigcap_{[K':K]<\infty} N_{K'/K}(K'^\times) \subset K^\times$$

The existence theorem is essentially the statement that for a local field K its universal norm group D_K is trivial. In fact, considering the images of the norm groups in the finite group $K^\times/T$ and using the fact that this family is directed, $D_K = 1$ implies that some member of this family must have trivial image, therefore T contains a norm group as was to be shown.

Hence all that is left to prove is

Lemma 6.2.4 *Let K be a local field. Then $D_K = 1$.*

PROOF First observe that if L is a finite extension of K then $D_K \subset N_{L/K} D_L$. To show this let $a \in D_K$. For each finite extension $L' \supset L$ we have that

$$F(L') \stackrel{\text{df}}{=} N_{L/K}^{-1}(a) \cap N_{L'/L}(L'^{\times}) \subset L^{\times}$$

is a non-empty compact set: by hypothesis there exists $c \in N_{L'/K} L'^{\times}$ such that $a = N_{L'/K}(c)$, hence $N_{L'/L}(c) \in F(L')$; moreover $N_{L'/L}(L'^{\times})$ is closed and $N_{L/K}^{-1}(a)$ is compact by the previous lemma. Clearly $F(L' \cdot L'') \subset F(L') \cap F(L'')$, hence by compactness (finite intersection property) we have that $\bigcap_{L'} F(L') \neq \emptyset$, and any element in this intersection belongs to D_L and has norm a.

Now we prove that D_K is trivial. It is enough to show that D_K is divisible since this implies $D_K = \bigcap_{n \geq 1} (K^{\times})^n = 1$. Let p be a prime number. Given $a \in D_K$ we have to show that $x^p = a$ has a solution with $x \in D_K$. Assume first that $p \neq \operatorname{char} K$ and let ζ be a primitive p-th root of 1. For each finite extension $L \supset K(\zeta)$ consider the finite set

$$E(L) \stackrel{\text{df}}{=} \{b \in K^{\times} \mid b^p = a \text{ with } b \in N_{L/K} L^{\times}\}$$

Clearly $E(L \cdot L') \subset E(L) \cap E(L')$. Moreover each $E(L)$ is non-empty: writing $a = N_{L/K}(c)$ with $c \in D_L$ (which is possible by the above) then corollary 6.1.3 implies that $c = d^p$ for some $d \in L^{\times}$ and hence $N_{L/K}(d) \in E(L)$. By compactness, $\bigcap_L E(L) \neq \emptyset$ and any element x in this intersection is in D_K and satisfies $x^p = a$, as required. If $p = \operatorname{char} K$, the proof is similar, but using lemma 6.1.5 instead. □

Remark 6.2.5 The lemma together with theorem 2.1 shows that $\theta_K : K^{\times} \to G_K^{ab}$ is injective and has dense image. Therefore we have a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & U_K & \longrightarrow & K^{\times} & \xrightarrow{v} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \theta_K}\,\approx & & \downarrow{\scriptstyle \theta_K} & & \downarrow{\scriptstyle \text{inclusion}} & & \\
0 & \longrightarrow & I_K^{ab} & \longrightarrow & G_K^{ab} & \xrightarrow{\text{can.}} & G_K^{nr} = \hat{\mathbb{Z}} & \longrightarrow & 0
\end{array}$$

where I_K^{ab} is the **inertia group** of $K^{ab} \supset K$.

7 Further applications

We end this chapter with a couple of important applications of the local reciprocity theorem. Here we assume a few more prerequisites than before.

7.1 The global Kronecker-Weber theorem

As an illustration of how the study of local fields is relevant in addressing global questions, we show how to derive the global Kronecker-Weber from the local one.

Theorem 7.1.1 (Kronecker-Weber) *Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.*

PROOF Let L be a finite abelian extension of $\mathbb{Q}$. The idea is to find n such that $M \stackrel{\text{df}}{=} L(\zeta_n)$ has exactly the same ramification data as $\mathbb{Q}(\zeta_n)$, that is, for each prime $p \in \mathbb{Z}$ the ramification degrees of the prime ideals of M and $\mathbb{Q}(\zeta_n)$ lying above p are the equal. We claim that this forces $M = \mathbb{Q}(\zeta_n)$ and therefore $L \subset \mathbb{Q}(\zeta_n)$.

In fact, denote by $I_p \subset \operatorname{Gal}(M/\mathbb{Q})$ the inertia group of a prime ideal of M lying above p (they are all equal since M is abelian over $\mathbb{Q}$). Consider the subgroup I of $\operatorname{Gal}(M/\mathbb{Q})$ generated by all the I_p. The fixed field M^I is unramified over $\mathbb{Q}$, hence by Minkowski's theorem (see for instance Neukirch's book) we have that $M^I = \mathbb{Q}$ and hence $I = \operatorname{Gal}(M/\mathbb{Q})$. On the other hand, the ramification degree of a prime ideal of $\mathbb{Q}(\zeta_n)$ lying above p is the same as the ramification degree of $\mathbb{Q}_p(\zeta_n)$ over $\mathbb{Q}_p$. Factoring $n = \prod_p p^{e_p}$, we have that $\mathbb{Q}_p(\zeta_n)$ is the compositum of the totally ramified extension $\mathbb{Q}_p(\zeta_{p^{e_p}}) \supset \mathbb{Q}_p$ and the unramified extension $\mathbb{Q}_p(\zeta_{n/p^{e_p}}) \supset \mathbb{Q}_p$ (see the proof of the local Kronecker-Weber), hence this

ramification degree is $\phi(p^{e_p})$ (see lemma 2.6). Therefore if M and $\mathbb{Q}(\zeta_n)$ have the same ramification data then $|I_p| = \phi(p^{e_p})$ for all p and

$$[M:\mathbb{Q}] = |I| \leq \prod_p |I_p| = \prod_p \phi(p^{e_p}) = \phi(n) = [\mathbb{Q}(\zeta_n):\mathbb{Q}]$$

But since $M \supset \mathbb{Q}(\zeta_n)$, the two fields must be equal, as claimed.

Now we construct n with the above property. For each prime $p \in \mathbb{Z}$, choose a prime ideal $\mathfrak{m}_p$ of L lying above p and denote by L_p the completion of L with respect to this prime (all completions are isomorphic since L is Galois over $\mathbb{Q}$). By the local Kronecker-Weber, there exists an integer $n_p = p^{e_p} \cdot m_p$ with $p \nmid m_p$ such that $L_p \subset \mathbb{Q}_p(\zeta_{n_p})$. Set $n = \prod_{p \in S} p^{e_p}$ where S denotes the (finite) set of primes that ramify in L. Denoting by M_p the completion of M with respect to a prime lying above $\mathfrak{m}_p$, we have to check that the ramification degree of $M_p \supset \mathbb{Q}_p$ equals $\phi(p^{e_p})$, the ramification degree of $\mathbb{Q}_p(\zeta_n) \supset \mathbb{Q}_p$. But since $M_p = L_p(\zeta_n)$ and since $L_p \subset \mathbb{Q}_p(\zeta_{n_p})$ we have that $M_p(\zeta_{m_p}) = \mathbb{Q}_p(\zeta_n)(\zeta_{m_p})$, which has ramification degree $\phi(p^{e_p})$ over $\mathbb{Q}_p$. Since $\mathbb{Q}_p(\zeta_{m_p}) \supset \mathbb{Q}_p$ is unramified we have that $M_p(\zeta_{m_p}) \supset M$ is also unramified by theorem I.5.1 and thus $M \supset \mathbb{Q}_p$ also has ramification degree $\phi(p^{e_p})$, as was to be shown. □

7.2 Central simple algebras and Brauer group

The final application is to central simple algebras. We recall without proof some basic facts about central simple algebras, referring the reader to Gille-Szamuely's book for proofs.

Let K be any field. A **central simple algebra** A over K is a finite dimensional associative K-algebra which satisfies the following equivalent conditions:

1. A has no trivial two sided ideals and the centre of A is K;
2. $A \cong M_n(D)$ for some n and some division algebra D with centre K (here $M_n(D)$ denotes the ring of $n \times n$ matrices with entries in D, and D is uniquely determined by A up to isomorphism);
3. there exists a finite Galois extension $L \supset K$ that "splits" A, i.e., $A \otimes_K L \cong M_n(L)$ for some n.

We say that two central simple algebras A and B over K are **Brauer equivalent** if there is an isomorphism $A \otimes_K M_m(K) \cong B \otimes_K M_n(K)$ for some m and n. The **Brauer group** $\mathrm{Br}(K)$ of K is the group consisting of all the (Brauer) equivalence classes $[A]$ of central simple algebras A over K. The product in $\mathrm{Br}(K)$ is induced by the tensor product: $[A] \cdot [B] = [A \otimes_K B]$. One verifies that this is well-defined, and turns $\mathrm{Br}(K)$ into a torsion abelian group. The identity element of $\mathrm{Br}(K)$ is $[K]$ and $[A]^{-1} = [A^{op}]$, where A^{op} is the opposite algebra of A, defined by inverting the order of the multiplication in A.

By 2 of the above definition, we have that the elements of the Brauer group of K are in 1-1 correspondence with the isomorphism classes of division algebras over K. In other words, $\mathrm{Br}(K)$ is a "directory" of all division algebras over K. One can also view $\mathrm{Br}(K)$ as a measure of the arithmetic complexity of K (i.e., of its absolute Galois group) due to the following important

Theorem 7.2.1 *For any field K, one has an isomorphism*

$$\mathrm{Br}(K) = H^2(G_K, K_{sp}^\times)$$

Furthermore, if $L \supset K$ is an arbitrary field extension, restriction $\mathrm{res}: H^2(G_K, K_{sp}^\times) \to H^2(G_L, L_{sp}^\times)$ *in cohomology corresponds to restriction* $\mathrm{Br}(K) \to \mathrm{Br}(L)$ *of Brauer groups, defined by* $[A] \mapsto [A \otimes_K L]$.

The above isomorphism can be described as follows. Let L be a finite Galois extension of K and set $G = \mathrm{Gal}(L/K)$. Given a 2-cocycle $f: G \times G \to L^\times$ representing an element of $H^2(G, L^\times)$ we can build a central simple algebra A_f (the so-called **crossed product**) which, as a vector space over L, is given by

$$A_f = \bigoplus_{\sigma \in G} L \cdot e_\sigma$$

Multiplication on A_f is defined by

$$(a_\sigma e_\sigma) \cdot (b_\tau e_\tau) = a_\sigma \sigma(b_\tau) f(\sigma,\tau) \cdot e_{\sigma\tau} \qquad \text{for} \quad a_\sigma, b_\tau \in L^\times, \quad \sigma, \tau \in G$$

One obtains a map $H^2(G, L^\times) \to \mathrm{Br}(K)$ given by $[f] \mapsto [A_f]$. Taking the direct limit over all L we obtain the desired isomorphism.

The "simplest" central simple algebras are the cyclic ones:

Definition 7.2.2 A central simple algebra A over K is **cyclic** if there exists a cyclic extension $L \supset K$ that splits A (as in definition 3).

Now we are ready to show the main result about central simple algebras over local fields:

Theorem 7.2.3 *Every central simple algebra A over a local field K is cyclic.*

PROOF Recall that we have a commutative diagram (see theorem 4.3 and corollary 5.6)

$$\begin{array}{ccc} \mathrm{Br}(L) & \xrightarrow[\approx]{\mathrm{inv}_L} & \mathbb{Q}/\mathbb{Z} \\ \mathrm{res}\uparrow & & \uparrow[L:K] \\ \mathrm{Br}(K) & \xrightarrow[\approx]{\mathrm{inv}_K} & \mathbb{Q}/\mathbb{Z} \end{array}$$

Hence if $[A]$ has order n in $\mathrm{Br}(K)$ then *any* cyclic extension of degree n will split A, for instance the unramified extension of degree n. □

As we saw, the Brauer group of a local field played a prominent role in the proof of the local reciprocity theorem. It also plays a central role in the proof of the *global* reciprocity theorem. We just state the important

Theorem 7.2.4 (Brauer group of global fields) *Let K be a global field. One has an exact sequence*

$$0 \longrightarrow \mathrm{Br}(K) \xrightarrow{\sum_v \mathrm{res}_v} \bigoplus_v \mathrm{Br}(K_v) \xrightarrow{\sum_v \mathrm{inv}_{K_v}} \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

Here K_v denotes the completion of K with respect to the valuation v, $\mathrm{res}_v\colon \mathrm{Br}(K) \to \mathrm{Br}(K_v)$ and $\mathrm{inv}_{K_v}\colon \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$ are the usual restriction and invariant maps, and the direct sum runs over all valuations of K, including the archimedean ones.

The proof of the above theorem is the main step of the proof of the global reciprocity law. In terms of central simple algebras, it describes the **local-global** or **Haße principle** for division algebras: a division algebra D over a global field K is completely determined by its restrictions $D \otimes_K K_v$ to the local fields K_v. In particular, D is trivial if and only if $D \otimes_K K_v$ is trivial for all v.

8 Exercises

1. Show that $\theta_{\mathbb{Q}_5(\zeta_5)/\mathbb{Q}_5}(2)(\zeta_5) = \zeta_5^3$.

2. Let $M \supset L \supset K$ be finite extensions of local fields with $M \supset K$ abelian. Show that the following diagrams commute:

$$\begin{array}{ccc} \dfrac{L^\times}{N_{M/L}(M^\times)} & \xrightarrow[\approx]{\theta_{M/L}} & \mathrm{Gal}(M/L) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow \\ \dfrac{K^\times}{N_{M/K}(M^\times)} & \xrightarrow[\approx]{\theta_{M/K}} & \mathrm{Gal}(M/K) \end{array} \qquad \begin{array}{ccc} \dfrac{L^\times}{N_{M/L}(M^\times)} & \xrightarrow[\approx]{\theta_{M/L}} & \mathrm{Gal}(M/L) \\ \uparrow & & \uparrow{\scriptstyle \mathrm{Ver}} \\ \dfrac{K^\times}{N_{M/K}(M^\times)} & \xrightarrow[\approx]{\theta_{M/K}} & \mathrm{Gal}(M/K) \end{array}$$

Here the unlabelled maps are the canonical ones and Ver denotes the *transfer map* (Verlagerung in German): given finite groups $H \leq G$, $\mathrm{Ver}\colon G^{ab} \to H^{ab}$ is defined via the restriction map $\mathrm{res}\colon G^{ab} = H_T^{-2}(G,\mathbb{Z}) \to H^{ab} = H_T^{-2}(H,\mathbb{Z})$.

3. Compute the reciprocity map for the cyclotomic extension $\mathbb{Q}_3(\zeta_{18}) \supset \mathbb{Q}_3$ and draw the lattices of subfields and corresponding norm groups.

4. Show that every finite abelian group is the Galois group of some extension of $\mathbb{Q}$.

Appendix

1 Integral Extensions

Definition 1.1 Let $S \supset R$ be an extension of commutative rings. An element $s \in S$ is **integral** over R if it satisfies a monic polynomial with coefficients in R:

$$s^n + r_{n-1}s^{n-1} + \cdots + r_0 = 0, \qquad r_i \in R$$

The extension $S \supset R$ is **integral** if every element of S is integral over R.

Integral extensions are to rings what algebraic extensions are to fields. The next lemma explicits this relation, showing how to "clear out" the denominators.

Lemma 1.2 *Let R be a domain. Then for any element α in the algebraic closure of the field* $\operatorname{Frac} R$ *there is $r \in R$ such that $r\alpha$ is integral over R.*

Proof Suppose that $c_n\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0$ with $c_i \in R$, $c_n \neq 0$. Multiplying by c_n^{n-1} we have $(c_n\alpha)^n + c_{n-1}(c_n\alpha)^{n-1} + \cdots + c_n^{n-1}c_0 = 0$, hence we may take $r = c_n$. □

Definition 1.3 A domain R is called **normal** or **integrally closed** if every element of $\operatorname{Frac} R$ which is integral over R lies in R.

For instance, $\mathbb{Z}$ is a normal domain. This follows from the more general fact

Theorem 1.4 *Every UFD is normal.*

Proof Let A be a UFD and $K = \operatorname{Frac} A$. Suppose that an element $x/y \in K$, with $x, y \in A$ relatively prime, is integral over A, and let

$$\left(\frac{x}{y}\right)^n + a_{n-1}\left(\frac{x}{y}\right)^{n-1} + a_{n-2}\left(\frac{x}{y}\right)^{n-2} + \cdots + a_0 = 0, \qquad a_i \in A$$

be a monic equation for x/y. Multiplying by y^n we obtain

$$x^n = -a_{n-1}x^{n-1}y - a_{n-2}x^{n-2}y^2 - \cdots - a_0y^n$$

and hence x is a multiple of y. But since x and y are relatively prime, we must have that y is a unit in A and hence $x/y \in A$, as required. □

Integral elements have a very useful intrinsic "polynomial-free" characterisation:

Theorem 1.5 (Characterisation of integral elements) *Let $S \supset R$ be an extension of rings and $\alpha \in S$. The following are equivalent:*

1. *α is integral over R.*
2. *α is an element of an R-algebra $A \subset S$ which is finitely generated as an R-module.*

Proof Suppose that α is integral over R, root of a monic polynomial in $R[x]$ of degree n. Then $A = R[\alpha]$ is a finite R-module, generated by $1, \alpha, \ldots, \alpha^{n-1}$ over R, and $\alpha \in A$. Conversely, suppose that α belongs to a ring A which is finitely generated as an R-module, say by ω_i, $1 \leq i \leq n$. We use the so-called **determinant trick**: for $i = 1, \ldots, n$, we can write

$$\alpha\omega_i = \sum_{1 \leq j \leq n} m_{ij}\omega_j, \qquad m_{ij} \in R$$

In matrix notation, we can rewrite the previous system as $(\alpha I - M) \cdot \omega = 0$, where $M = (m_{ij})$, $\omega = (\omega_1, \ldots, \omega_n)^T$ and I denotes the $n \times n$ identity matrix. Since this homogeneous linear system in ω has a non-trivial solution, $\det(\alpha I - M) = 0$. Therefore α is a root of the monic polynomial $p(x) = \det(xI - M)$ in $R[x]$, i.e., α is integral over R. □

Using the above characterisation we easily obtain

Theorem 1.6 *Let $S \supset R$ be an extension of rings. The elements of S integral over R form a subring of S containing R.*

PROOF Let $\alpha, \beta \in S$ be roots of monic polynomials in $R[X]$ of degrees m and n, respectively. Then $R[\alpha, \beta]$ is a finite R-module generated by $\alpha^i \beta^j$, $0 \leq i \leq m-1$, $0 \leq j \leq n-1$. Therefore $\alpha+\beta, \alpha\beta \in R[\alpha, \beta]$ are integral over R. □

The subring of S consisting of all elements which are integral over R is called **integral closure** or **normalisation** of R in S. The name integral closure stems from

Theorem 1.7 (Transitivity of integrality) *Let $T \supset S \supset R$ be extensions of rings. If T is integral over S and S is integral over R, then T is integral over R. In particular, if R is a domain and K is a field containing R then the integral closure of R in K is an integrally closed ring.*

PROOF Let $t \in T$ be integral over S with $t^n + s_{n-1}t^{n-1} + \cdots + s_0 = 0$, $s_i \in S$. Since each s_i is integral over R, $R[s_0, \ldots, s_{n-1}]$ is a finite R-module, hence so is $A = R[t, s_0, \ldots, s_{n-1}]$, and $t \in A$. Thus t is integral over R. □

Theorem 1.8 (Norms and Traces of integral elements) *Let R be a domain and L be a finite separable field extension of $K = \operatorname{Frac} R$. Let S be the integral closure of R in L. If R is normal, then $T_{L/K}(s)$ and $N_{L/K}(s)$ are elements of R for all $s \in S$.*

PROOF Let $n = [L : K]$ and $\sigma_1, \ldots, \sigma_n \colon L \to K_{sp}$ be the K-embeddings of L into K_{sp}. Since s is the root of a monic polynomial in $R[X]$, so are $\sigma_i(s)$ for all i. Hence $\sigma_i(s)$ are integral over R, and thus so are the elements $N_{L/K}(s) = \prod \sigma_i(s)$ and $T_{L/K}(s) = \sum \sigma_i(s)$ of $K = \operatorname{Frac} R$. Since R is normal, they must lie in R. □

Example 1.9 The sequence of **Fibonacci numbers** is defined by $F_0 = 0$, $F_1 = 1$, and $F_{k+2} = F_{k+1} + F_k$ for $k \geq 0$. The first terms are thus $0, 1, 1, 2, 3, 5, 8, 13, \ldots$ It is easy to show by induction that

$$F_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}, \qquad \text{where} \quad \alpha = \frac{1+\sqrt{5}}{2} \quad \text{and} \quad \beta = \frac{1-\sqrt{5}}{2}$$

Notice that α and β are integral over $\mathbb{Z}$.
We now prove that if $m \mid n$ then $F_m \mid F_n$. Write $n = dm$ with $d \in \mathbb{Z}$. We just perform the division:

$$\frac{F_n}{F_m} = \alpha^{(d-1)m} + \alpha^{(d-2)m}\beta^m + \cdots + \alpha^m \beta^{(d-2)m} + \beta^{(d-1)m}$$

This shows that $F_n/F_m \in \mathbb{Q}$ is integral over the normal domain $\mathbb{Z}$, hence $F_n/F_m \in \mathbb{Z}$ and we are done.

Example 1.10 Let d be a square-free integer. Let $K = \mathbb{Q}(\sqrt{d})$ and denote by A the integral closure of $\mathbb{Z}$ in K. We have the following explicit description of A:

$$A = \mathbb{Z} + \mathbb{Z}\omega, \qquad \text{where} \quad \omega = \begin{cases} \sqrt{d} & \text{if } d \equiv 2 \text{ or } d \equiv 3 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

Let us prove the case $d \equiv 3 \pmod 4$; the other ones are similar and are left to the reader. First, it is clear that $\mathbb{Z} + \mathbb{Z}\sqrt{d} \subset A$. Now let $\alpha \in A$ and write $\alpha = r + s\sqrt{d}$, $r, s \in \mathbb{Q}$; we need to show that $r, s \in \mathbb{Z}$. Observe that $T_{K/\mathbb{Q}}(\alpha) = 2r$ and $T_{K/\mathbb{Q}}(\alpha\sqrt{d}) = 2ds$ are integers, hence we may write $r = m/2$ and $s = n/2d$ for some $m, n \in \mathbb{Z}$. But $N_{K/\mathbb{Q}}(\alpha) = r^2 - ds^2 = (m^2 d - n^2)/4d$ is also an integer. Since $d \equiv 3 \pmod 4$, both m and n must be even, hence $r \in \mathbb{Z}$ and $ds^2 \in \mathbb{Z}$. Using the fact that d is square-free, we conclude that $s \in \mathbb{Z}$ as well.

2 Valuations

Definition 2.1 An **abelian ordered group** $(G, +, \leq)$ is an abelian group $(G, +)$ together with a partial order $\leq$ such that $a \leq b \Rightarrow a + g \leq b + g$ for all $a, b, g \in G$. Examples of such groups are the additive groups $\mathbb{Z}$ and $\mathbb{R}$ with the usual order.

Definition 2.2 Let $(G, +, \leq)$ be an ordered group and ∞ be a formal symbol satisfying $g + \infty = \infty$ and $g \leq \infty$ for all $g \in G \cup \{\infty\}$. A **valuation** v on a field K with values in G is a map $v\colon K \to G \cup \{\infty\}$ such that

1. $v(xy) = v(x) + v(y)$;
2. $v(x + y) \geq \min\{v(x), v(y)\}$;
3. $v(x) = \infty \iff x = 0$.

If v is identically zero on $K^\times$, we say that v is **trivial**. If G is a discrete subgroup of $\mathbb{R}$ (for example $\mathbb{Z}$), we say that v is a **discrete valuation**. We say that a discrete valuation v is **normalised** if $G = \mathbb{Z}$ and v is surjective.

Valuations are intimately connected with prime factorisations in UFDs, as in the following

Example 2.3 Let p be a prime number. Given any nonzero rational number r, we may write it as $r = p^n \cdot \frac{a}{b}$ with $a, b \in \mathbb{Z}$ both not divisible by p. Setting $v_p(r) = n$, we obtain a normalised discrete valuation on $\mathbb{Q}$.
Similarly let k be any field and let $p(x) \in k[x]$ be an irreducible polynomial. Then we may write any nonzero $r(x) \in k(x)$ as $r(x) = p(x)^n \cdot \frac{f(x)}{g(x)}$ with $f(x), g(x) \in k[x]$ not divisible by $p(x)$. Setting $v_{p(x)}\big(r(x)\big) = n$ also gives a normalised discrete valuation on $k(x)$.

Let v be a valuation on a field K. Setting

$$|x|_v \stackrel{\text{df}}{=} 2^{-v(x)}$$

(where 2 denotes your favourite real number bigger than 1 and $2^{-\infty} = 0$ by definition) we obtain analogous "multiplicative" properties

1. $|xy|_v = |x|_v \cdot |y|_v$;
2. $|x + y|_v \leq \max\{|x|_v, |y|_v\}$;
3. $|x|_v = 0 \iff x = 0$.

turning K into a **normed metric space**. The presence of a valuation thus allows us to employ techniques and ideas from Analysis and Topology. A word of caution: as a consequence of the "strong triangle inequality" $|x + y|_v \leq \max\{|x|_v, |y|_v\}$, some things behave a little differently from the real or complex world. For instance, one has the **super strong triangle inequality**

$$|x|_v \neq |y|_v \Rightarrow |x + y|_v = \max\{|x|_v, |y|_v\}$$

In fact, using 1 one can easily show that $|-y|_v = |y|_v$ for all y. Thus if $|x|_v > |y|_v$, say, then by 2 one has $|x|_v \leq \max\{|x + y|_v, |-y|_v\} \Rightarrow |x|_v \leq |x + y|_v$ while $|x + y|_v \leq |x|_v$, again by 2, proving the super strong triangle inequality. In particular amongst $|x|_v$, $|y|_v$ and $|x - y|_v$ there are always two equal values, showing that in a discretely valued field all triangles are isosceles!

A concept from Topology that will be quite useful to us is that of a complete metric space. We say that K is **complete** with respect to $|-|_v$ (or v) if every **Cauchy sequence** converges: given a sequence $\{x_n\}_{n \geq 0}$ in K such that

$$\forall \epsilon > 0 \quad \exists n_0 = n_0(\epsilon) \quad \text{such that} \quad n, m \geq n_0 \Rightarrow |x_n - x_m|_v < \epsilon$$

then $\lim_{n \to \infty} x_n$ exists in K, namely there is an element $x_\infty \in K$ such that

$$\forall \epsilon > 0 \quad \exists n_0 = n_0(\epsilon) \quad \text{such that} \quad n \geq n_0 \Rightarrow |x_n - x_\infty|_v < \epsilon$$

Definition 2.4 Two valuations v and w on a field K are **equivalent** if they define the same topology on K.

More explicitly, we have the following

Theorem 2.5 (Equivalence of valuations) *Two valuations v and w on a field K are equivalent if and only if there exists $c > 0$ such that $v(x) = c \cdot w(x)$ for all $x \in K$.*

PROOF Clearly if v is a multiple of w then they define the same topology on K. Conversely, if v and w define the same topology then $w(x) > 0 \Rightarrow v(x) > 0$ since both conditions express the fact that $x^n \to 0$ when $n \to \infty$. We may assume that both valuations are nontrivial and therefore there exists $\pi \in K^\times$ such that $w(\pi) > 0$. Set $c = \frac{v(\pi)}{w(\pi)}$. Then $v(x) = c \cdot w(x)$ whenever x is a power of π. In general, for an arbitrary element $x \in K^\times$, we "approximate" x by a power of π, taking a rational approximation $\frac{n}{m}$ of $\frac{w(x)}{w(\pi)}$ such that $\frac{n}{m} < \frac{w(x)}{w(\pi)} \leq \frac{n+1}{m}$ where m, n are integers and $m > 0$. Then $m \cdot w(x) > n \cdot w(\pi) \iff w(\frac{x^m}{\pi^n}) > 0$ and therefore

$$v\Big(\frac{x^m}{\pi^n}\Big) > 0 \Rightarrow v(x) > \frac{n}{m} \cdot v(\pi) = \frac{n}{m} \cdot \big(c \cdot w(\pi)\big) \geq \frac{n}{n+1} \cdot \big(c \cdot w(x)\big)$$

Since we may take n arbitrarily large, we have that $v(x) \geq c \cdot w(x)$. Replacing x by x^{-1} we obtain the opposite inequality $v(x) \leq c \cdot w(x)$, finishing the proof. □

The above proof shows that if $w(x) > 0 \Rightarrow v(x) > 0$ holds for all $x \in K$ then the two valuations are actually equivalent. In other words we have

Lemma 2.6 (Independency of Inequivalent Valuations) *Let v and w be inequivalent valuations on a field K. Then there exists $x \in K$ such that $v(x) > 0$ and $w(x) \leq 0$.*

Every valuation v on a field K defines a subring

$$O_v \stackrel{\text{df}}{=} \{x \in K \mid v(x) \geq 0\} = \{x \in K \mid |x|_v \leq 1\}$$

called **valuation ring** of v. It is a local ring with maximal ideal

$$\mathfrak{m}_v \stackrel{\text{df}}{=} \{x \in O_K \mid v(x) > 0\} = \{x \in O_K \mid |x|_v < 1\}$$

and unit group

$$O_v^\times = \{x \in O_K \mid v(x) = 0\} = \{x \in O_K \mid |x|_v = 1\}$$

Observe that in O_v we have that $a \mid b \iff v(a) \leq v(b)$.

Theorem 2.7 (Discrete valuation rings) *Let R be a domain with field of fractions $K = \operatorname{Frac} R$. Then the following conditions are equivalent*

1. *R is the valuation ring of a discrete valuation on K.*
2. *R is a local PID different from K;*
3. *R is a noetherian normal local ring with Krull dimension 1 (that is, the prime ideals of R are just (0) and its maximal ideal);*
4. *R is a UFD with a single irreducible element π up to units.*

Any R satisfying the above conditions is called a **discrete valuation ring** *or* **dvr** *for short. Any generator of the maximal ideal of R is called a* **uniformiser**.

PROOF To show that $1 \Rightarrow 2$, observe that if v is a normalised valuation on K such that $R = O_v$ then given any ideal I of R with $n = \min\{v(r) \mid r \in I\}$ then I can be generated by any $r \in R$ such that $v(r) = n$.

Clearly $2 \Rightarrow 4 \Rightarrow 3$. We also have $4 \Rightarrow 1$ since we may define a valuation v on K by setting $v(a) = n$ where $a = u \cdot \pi^n$, $u \in R^\times$.

Finally, we show that $3 \Rightarrow 2$. Let $\mathfrak{m}$ be the maximal ideal of R. First observe that any nonzero ideal of R contains some power of $\mathfrak{m}$. This follows by noetherian induction: if there is a non-zero ideal I that does not contain any power of $\mathfrak{m}$, then we may choose I maximal with this property. Since R has Krull dimension 1 and $I \neq \mathfrak{m}$ and $I \neq (0)$, we have that I is not prime and hence there exist $a, b \notin I$ such that $ab \in I$. Then both $I + (a)$ and $I + (b)$ properly contain I, hence $I + (a) \supset \mathfrak{m}^i$ and $I + (a) \supset \mathfrak{m}^j$ for some i and j and therefore $I \supset \big(I + (a)\big) \cdot \big(I + (b)\big) \supset \mathfrak{m}^{i+j}$, a contradiction.

Next consider the R-module

$$\mathfrak{m}^{-1} \stackrel{\text{df}}{=} \{a \in K \mid a \cdot m \in R \text{ for all } m \in \mathfrak{m}\}$$

Let $a \in \mathfrak{m}$ be any nonzero element and let i be the smallest positive integer such that $(a) \supset \mathfrak{m}^i$. If $b \in \mathfrak{m}^{i-1} - (a)$ then $b \cdot \mathfrak{m} \subset (a)$ but $b \notin (a)$, i.e., $\frac{b}{a} \in \mathfrak{m}^{-1}$ but $\frac{b}{a} \notin R$, showing that $\mathfrak{m}^{-1} \not\subset R$. This implies that $\mathfrak{m} \cdot \mathfrak{m}^{-1} = R$. In fact, suppose not. Then $\mathfrak{m} \cdot \mathfrak{m}^{-1} \subset \mathfrak{m}$ and if $a \in \mathfrak{m}^{-1} - R$ then a is integral over R by the determinant trick, hence $a \in R$ since R is normal, a contradiction.

Now we show that for any nonzero ideal I we have that $I = \mathfrak{m}^n$ for a uniquely determined n. Uniqueness follows immediately from $\mathfrak{m} \cdot \mathfrak{m}^{-1} = R$ by multiplying two distinct representations by some power of $\mathfrak{m}^{-1}$. To prove existence, we use noetherian induction: let I be a nonzero ideal which is maximal among those that cannot be written as a power of $\mathfrak{m}$. Then $I \subset \mathfrak{m}$ and hence $\mathfrak{m}^{-1} \cdot I$ is an ideal of R which properly contains I since multiplying $I = \mathfrak{m}^{-1} \cdot I$ by $\mathfrak{m}$ and using $\mathfrak{m} \cdot \mathfrak{m}^{-1} = R$ we conclude that $I \cdot \mathfrak{m} = I$ and hence $I = (0)$ by Nakayama's lemma. Therefore $\mathfrak{m}^{-1} \cdot I = \mathfrak{m}^n$ for some n and hence $I = \mathfrak{m}^{n+1}$.

By Nakayama's lemma $\mathfrak{m} \neq \mathfrak{m}^2$. Let $\pi \in \mathfrak{m} - \mathfrak{m}^2$. Since (π) is a power of $\mathfrak{m}$, the only possibility is $\mathfrak{m} = (\pi)$. Hence $\mathfrak{m}$ is principal, and therefore so are all ideals of R. Therefore $R \neq K$ is a local PID. □

3 Limits

3.1 Direct Limits

Definition 3.1.1 A partially ordered set $(I, \geq)$ is said to be **directed** if given any pair $i, j \in I$ there exists $k \in I$ such that $k \geq i$ and $k \geq j$.

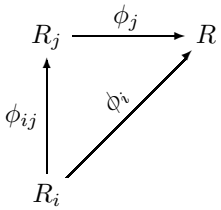
Definition 3.1.2 Let $(I, \geq)$ be a directed set. A **direct system** of rings (or groups, topological spaces, and so on) is a family of rings $(R_i)_{i \in I}$ (or groups, topological spaces, and so on), together with a family of morphisms of rings (or of groups, topological spaces, and so on) $\phi_{ij} \colon R_i \to R_j$, $i \leq j$, such that

1. $\phi_{ii} = \mathrm{id}_{R_i}$ for all $i \in I$;
2. $\phi_{ik} = \phi_{jk} \circ \phi_{ij}$ for any triple $i \leq j \leq k$ in I.

Given a direct system (R_i, ϕ_{ij}), we may consider its **direct limit**, which consists of a ring (or group...)

$$R = \varinjlim_{i \in I} R_i$$

together with morphisms $\phi_i \colon R_i \to R$ which are compatible with the ϕ_{ij} in the sense that for all $i \leq j$ the diagram



commutes. Intuitively R can be viewed as a "generalised union" of the R_i, with "generalised inclusion maps" $\phi_i \colon R_i \to R$ (which are not necessarily injective). The direct limit is characterised by the following universal property, which distinguishes it as the "smallest" ring "containing" all the R_i: given a test ring T and maps $f_i \colon R_i \to T$ which are compatible with the ϕ_{ij}, namely $f_j \circ \phi_{ij} = f_i$ for all $i \leq j$, then there exists a unique $f \colon R \to T$ such that $f_i = f \circ \phi_i$ for all i.

We may construct the direct limit by setting

$$R = \frac{\coprod_{i \in I} R_i}{\sim}$$

the disjoint union of the R_i modulo the equivalence relation $\sim$ which identifies $r_i \in R_i$ and $r_j \in R_j$ if there exists $k \in I$ with $k \geq i$ and $k \geq i$ such that $\phi_{ik}(r_i) = \phi_{jk}(r_j) \in R_k$. One may perform addition and multiplication of the classes of $r_i \in R_i$ and $r_j \in R_j$ by replacing them by representatives in a common

ring R_k where $k \geq i$ and $k \geq j$ (such k exists since the index set I is directed). It is easy to check that everything is well-defined. The maps $\phi_i \colon R_i \to R$ are the natural ones.

As a concrete example, let k be a field and R be a k-algebra. Consider the directed set given by the finite subsets of R, ordered by inclusion. Given a finite set S in this system, let R_S be the k-subalgebra of R generated by the elements of S. If $S \subset S'$, let $\phi_{SS'} \colon R_S \hookrightarrow R_{S'}$ be inclusion map. Then one has

$$R = \varinjlim_S R_S$$

3.2 Projective Limits

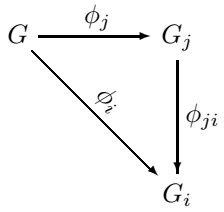
Let $(I, \leq)$ be a directed set. A **projective system** of groups (or rings, topological spaces, and so on) is a family of groups $(G_i)_{i \in I}$ and maps $\phi_{ji} \colon G_j \to G_i$, $i \leq j$, such that

1. $\phi_{ii} = \mathrm{id}_{G_i}$ for all $i \in I$;
2. $\phi_{ki} = \phi_{ji} \circ \phi_{kj}$ for any triple $i \leq j \leq k$ in I.

The **projective limit** of the above projective system is a group (ring, topological space, ...)

$$G = \varprojlim_{i \in I} G_i$$

together with "projection" maps $\phi_i \colon G \to G_i$ such that



commutes for all $i \leq j$. The projective limit is characterised by the following universal property: given a test group T and morphisms $g_i \colon T \to G_i$ such that $g_i = \phi_{ji} \circ g_j$ for all $i \leq j$, then there is a unique $g \colon T \to G$ such that $g_i = \phi_i \circ g$ for all $i \in I$.

We can construct G as the subgroup of the product $\prod_{i \in I} G_i$ consisting of "coherent tuples", namely

$$G = \left\{ (\sigma_i) \in \prod_{i \in I} G_i \;\middle|\; \phi_{ji}(\sigma_j) = \sigma_i \text{ for all } i \leq j \right\}$$

with $\phi_i \colon G \to G_i$ given the i-th projection map.

Projective limits usually arise by "stacking" quotient maps. As a concrete example, consider the directed set of finite Galois extensions l of a field k in some separable closure k_{sp}, ordered by inclusion. Set $G_l = \mathrm{Gal}(l/k)$ and let $\phi_{ml} \colon G_m \twoheadrightarrow G_l$ be the natural quotient (or projection) maps for all $m \supset l \supset k$ in this directed set. Then

$$G = \varprojlim_l G_l$$

is just the absolute Galois group $\mathrm{Gal}(k_{sp}/k)$ of k, since to give an automorphism $\sigma \in \mathrm{Gal}(k_{sp}/k)$ is the same as to give a family $\sigma_l \in \mathrm{Gal}(l/k)$ of compatible automorphisms for all finite Galois extensions l of k.

4 Group homology and cohomology

4.1 Definitions

In this subsection, G will denote a finite group.

Definition 4.1.1 A **G-module** M is just a left $\mathbb{Z}[G]$-module, where $\mathbb{Z}[G]$ is the group ring of G with integer coefficients. In other words, M is an abelian group together with a G-action, that is, a map $G \times M \to M$ sending (σ, m) to an element $\sigma \cdot m \in M$ such that, for all $m, m' \in M$, and $\sigma, \sigma' \in G$,

1. $1 \cdot m = m$
2. $\sigma \cdot (m + m') = \sigma \cdot m + \sigma \cdot m'$
3. $(\sigma\sigma') \cdot m = \sigma \cdot (\sigma' \cdot m)$

A **morphism of G-modules** $f: M \to N$ is a map of left $\mathbb{Z}[G]$-modules, i.e., a group morphism such that $f(\sigma m) = \sigma f(m)$ for all $\sigma \in G$ and $m \in M$.
If M is a G-module, we write M^G for the subgroup of G-fixed points:

$$M^G \stackrel{\text{df}}{=} \{m \in M \mid \sigma \cdot m = m \text{ for all } \sigma \in G\}$$

Example 4.1.2 Examples of G-modules arising in nature are

1. $M = \mathbb{Z}$, $M = \mathbb{Q}$, or $M = \mathbb{Q}/\mathbb{Z}$ where G operates trivially: $\sigma m = m$ for all $\sigma \in G$ and $m \in M$;
2. $M = \mathbb{Z}[G]$ or $M = I_G$, where G operates by left multiplication. Here I_G is the so-called **augmentation ideal** of $\mathbb{Z}[G]$, defined as the kernel of the **augmentation map** $\epsilon: \mathbb{Z}[G] \to \mathbb{Z}$ given by
$$\sum_{\sigma \in G} n_\sigma \sigma \mapsto \sum_{\sigma \in G} n_\sigma$$
Observe that I_G is a free $\mathbb{Z}$-module with basis $\sigma - 1$, $\sigma \in G$, $\sigma \neq 1$. If $\mathbb{Z}$ is given the trivial action as above, then the augmentation map is a morphism of G-modules;
3. if $L \supset K$ is a finite Galois extension with $G = \mathrm{Gal}(L/K)$, then $M = L^+$, $M = L^\times$ and $M = \mu_L$ are all examples of G-modules where G operates via the Galois action. Here L^+ and $L^\times$ are the additive and multiplicative groups of L and $\mu_L \subset L^\times$ is the subgroup of roots of 1 contained in L.
4. for any G-module M we have a morphism of G-modules $N_G: M \to M^G$ given by
$$N_G(m) \stackrel{\text{df}}{=} \sum_{\sigma \in G} \sigma m, \qquad m \in M$$
called **norm map**. In the previous example, when $M = L^\times$ the norm map N_G coincides with the usual norm of fields $N_{L/K}: L \to K$. When $M = L^+$ then it becomes the trace $T_{L/K}: L \to K$.

From now on, unless otherwise stated the abelian groups M of the example will always be given the G-actions above. With this convention, for any G-module M we have an isomorphisms of abelian groups

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

and

$$\mathbb{Z} \otimes_{\mathbb{Z}[G]} M = \frac{M}{I_G \cdot M}$$

since $\mathbb{Z}[G]/I_G = \mathbb{Z}$ (induced by augmentation).

Now we show how to build new modules from old ones. Let M and N be two G-modules. Then the set

$$\mathrm{Hom}_G(M, N)$$

of all morphisms of G-modules between M and N can be made into a G-module by "conjugation" $(\sigma f)(m) \stackrel{\text{df}}{=} \sigma f(\sigma^{-1} m)$ for $f \in \mathrm{Hom}_G(M, N)$ and $m \in M$. Similarly, the tensor product of M and N over $\mathbb{Z}$

$$M \otimes N$$

can be made into a G-module by "diagonal action" $\sigma(m \otimes n) \stackrel{\text{df}}{=} \sigma(m) \otimes \sigma(n)$ for $m \in M$ and $n \in N$. The next definition shows how to "lift" modules from subgroups:

Definition 4.1.3 Let $H \leq G$ be a subgroup and N be an H-module. The **induced module** from N is the G-module

$$\mathrm{Ind}_H^G(N) \stackrel{\text{df}}{=} \mathrm{Hom}_H(G, N)$$

of all H-linear functions $f: G \to N$ (i.e. $f(h \cdot g) = h \cdot f(g)$ for all $h \in H$ and $g \in G$) and where the G-action is given by $(\sigma f)(g) = f(g\sigma)$ for all $\sigma, g \in G$. When $H = 1$ we simply write $\mathrm{Ind}^G(N)$. A G-module M is called **induced** if $M = \mathrm{Ind}^G(N)$ for some abelian group N.

Another way to "lift" an H-module is via the "base change" $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N$, where the G-action is given by multiplication on the left component (in the tensor product, the left component is viewed as a right $\mathbb{Z}[H]$-module via $m \cdot \sigma \stackrel{\text{df}}{=} \sigma^{-1} \cdot m$ for all $\sigma \in H$ and $m \in \mathbb{Z}[G]$). Base change is related to induced modules via the isomorphism of G-modules

$$\mathrm{Ind}^G(N) \cong \mathbb{Z}[G] \otimes N$$

given by $\phi \mapsto \sum_{g \in G} g \otimes \phi(g^{-1})$. Here N is any abelian group with trivial G-action. Observe that an induced G-module $M = \mathbb{Z}[G] \otimes N$ is also induced as an H-module: if $H\sigma_1, \ldots, H\sigma_n$ are right cosets of H then $M = \mathbb{Z}[H] \otimes N'$ where $N' = \bigoplus_{1 \le i \le n} \sigma_i N$.

Example 4.1.4 Let $L \supset K$ be a finite Galois extension with $G = \mathrm{Gal}(L/K)$. Then L^+ is an induced G-module. In fact, by the normal basis theorem there exists $\omega \in L$ such that $\{\sigma(\omega) \mid \sigma \in G\}$ is a basis of L over K. Then we have a G-isomorphism $K[G] \cong L^+$ given by $\sum_{\sigma \in G} a_\sigma \sigma \mapsto \sum_{\sigma \in G} a_\sigma \sigma(\omega)$. Since $K[G] = \mathbb{Z}[G] \otimes K$ is induced by the above, so is L^+.

The following lemma will be useful in arguments involving dimension shifting (which we will see later).

Lemma 4.1.5 *Let M be an arbitrary G-module and denote by M_0 the underlying abelian group. Then there is an injective map of G-modules*

$$M \hookrightarrow \mathrm{Ind}^G(M_0)$$

sending m to the function $\phi_m : G \to M_0$ given by $\phi_m(\sigma) = \sigma \cdot m$. There is also a surjective map of G-modules

$$\mathrm{Ind}^G(M_0) \twoheadrightarrow M$$

given by $\phi \mapsto \sum_{\sigma \in G} \sigma\phi(\sigma^{-1})$.

Definition 4.1.6 Let M be a G-module and $i \ge 0$. The i-th **cohomology group** of M is defined as

$$H^i(G, M) \stackrel{\text{df}}{=} \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, M)$$

while the i-th **homology group** of M is defined as

$$H_i(G, M) \stackrel{\text{df}}{=} \mathrm{Tor}_i^{\mathbb{Z}[G]}(\mathbb{Z}, M)$$

We briefly recall the definitions of Ext and Tor below, but we warn you that except for low degrees $i = 0, 1$ the computations of these groups are not done directly from their definitions but rather via their functorial properties and some "vanishing theorems" that tell you sufficient conditions under which these groups are trivial.

A G-module I is called **injective** if the functor $\mathrm{Hom}_G(-, I)$ is exact. A G-module P is called **projective** if the functor $\mathrm{Hom}_G(P, -)$. For instance, free $\mathbb{Z}[G]$-modules are projective. It can be shown that any G-module M can be embedded into an injective module and it can also be written as a quotient of a projective module. Hence we can inductively construct an **injective resolution** of M, namely an exact sequence

$$0 \to M \to I^0 \to I^1 \to I^2 \to \cdots$$

where the G-modules I^i are all injective, and similarly one may construct a **projective resolution**

$$\cdots \to P^2 \to P^1 \to P^0 \to M \to 0$$

Now we can define $\mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, M)$ as follows. Choose an injective resolution of M as above and apply the G-fixed point functor $\mathrm{Hom}_G(\mathbb{Z}, -) = (-)^G$ to it. We obtain a complex

$$0 \to M^G \to (I^0)^G \to (I^1)^G \to (I^2)^G \to \cdots$$

Then

$$\mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, M) \stackrel{\text{df}}{=} \frac{\ker\Big((I^i)^G \to (I^{i+1})^G\Big)}{\mathrm{im}\Big((I^{i-1})^G \to (I^i)^G\Big)}$$

(Here we interpret $I^{-1} = 0$). Now an easy but rather tedious computation shows that the groups thus obtained are independent of the choice of the injective resolution of M. Alternatively, one can choose a projective resolution of $\mathbb{Z}$

$$\cdots \to P^2 \to P^1 \to P^0 \to \mathbb{Z} \to 0$$

and apply the functor $\mathrm{Hom}_G(-, M)$ to it, defining

$$\mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, M) \stackrel{\mathrm{df}}{=} \frac{\ker\Big(\mathrm{Hom}_G(P^i, M) \to \mathrm{Hom}_G(P^{i+1}, M)\Big)}{\mathrm{im}\Big(\mathrm{Hom}_G(P^{i-1}, M) \to \mathrm{Hom}_G(P^i, M)\Big)}$$

(Here we interpret $P^{-1} = 0$) Again, this is independent of the chosen projective resolution of $\mathbb{Z}$, and it can be shown that either procedure, via projective resolutions of $\mathbb{Z}$ or injective resolutions of M, yield isomorphic groups.

For $\mathrm{Tor}_i^{\mathbb{Z}[G]}(\mathbb{Z}, M)$, the procedure is similar, except that Hom is replaced by the tensor product and the we use projective resolutions for both entries (in the tensor product $M \otimes_{\mathbb{Z}[G]} N$ we view M as a right $\mathbb{Z}[G]$-module via $m \cdot \sigma \stackrel{\mathrm{df}}{=} \sigma^{-1} \cdot m$ for $\sigma \in G$ and $m \in M$). For instance, if $P_\bullet \to M \to 0$ is a projective resolution of M, applying the functor $\mathbb{Z} \otimes_{\mathbb{Z}[G]} - = -/I_G \cdot -$ we obtain

$$\mathrm{Tor}_i^{\mathbb{Z}[G]}(\mathbb{Z}, M) = \frac{\ker\Big(P_i/I_G \cdot P_i \to P_{i-1}/I_G \cdot P_{i-1}\Big)}{\mathrm{im}\Big(P_{i+1}/I_G \cdot P_{i+1} \to P_i/I_G \cdot P_i\Big)}$$

Example 4.1.7 (Cyclic groups) Let G be a cyclic group of order n and let σ be a generator of G. Then we have a projective resolution of $\mathbb{Z}$

$$\cdots \xrightarrow{I} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{I} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{I} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

where ϵ is the augmentation map, and I and N denote multiplication by $\sigma - 1$ and $1 + \sigma + \cdots + \sigma^{n-1}$, respectively. Hence we obtain

$$H^i(G, M) = \begin{cases} M^G & \text{if } i = 0 \\ \dfrac{\ker N_G}{I_G \cdot M} & \text{if } i \text{ is odd} \\ \dfrac{M^G}{N_G(M)} & \text{if } i > 0 \text{ is even} \end{cases}$$

where $N_G \colon M \to M^G$ is the **norm map** and I_G is the augmentation ideal of $\mathbb{Z}[G]$. Using the same projective resolution of $\mathbb{Z}$, for homology we obtain

$$H_i(G, M) = \begin{cases} \dfrac{M}{I_G \cdot M} & \text{if } i = 0 \\ \dfrac{M^G}{N_G(M)} & \text{if } i \text{ is odd} \\ \dfrac{\ker N_G}{I_G \cdot M} & \text{if } i > 0 \text{ is even} \end{cases}$$

The main functorial property of Tor and Ext, and thus of the homology and cohomology groups, are their **long exact sequences**. For any short exact sequence of G-modules

$$0 \to A \to B \to C \to 0$$

one has long exact sequences

$$\begin{aligned} 0 &\longrightarrow H^0(G, A) = A^G \longrightarrow H^0(G, B) = B^G \longrightarrow H^0(G, C) = C^G \\ &\xrightarrow{\delta^0} H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C) \\ &\xrightarrow{\delta^1} H^2(G, A) \longrightarrow H^2(G, B) \longrightarrow H^2(G, C) \xrightarrow{\delta^2} \cdots \end{aligned}$$

and

$$\begin{aligned}\cdots \xrightarrow{\delta_3} & H_2(G,A) \longrightarrow H_2(G,B) \longrightarrow H_2(G,C)\\ \xrightarrow{\delta_2} & H_1(G,A) \longrightarrow H_1(G,B) \longrightarrow H_1(G,C)\\ \xrightarrow{\delta_1} & H_0(G,A) = \frac{A}{I_G \cdot A} \longrightarrow H_0(G,B) = \frac{B}{I_G \cdot B} \longrightarrow H_0(G,C) = \frac{C}{I_G \cdot C} \longrightarrow 0\end{aligned}$$

for cohomology and homology respectively. The maps δ^i and δ_i are called **connecting morphisms**. The other maps are the natural ones induced by the maps $A \to B$ and $B \to C$.

Think of the short exact sequence as a way to "decompose" B into simpler modules, a submodule A and a quotient module C. If we know the homology/cohomology of A and C then the long exact sequence allows us to find out the homology/cohomology of B.

Example 4.1.8 Let ϵ be the augmentation map. From the exact sequence of G-modules

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

and the fact that $\mathbb{Z}[G]$ is free (and thus has trivial homology), we conclude that the connecting morphisms give isomorphisms $H_p(G,\mathbb{Z}) = H_{p-1}(G, I_G)$ for all $p \geq 1$. In particular, for $p = 1$ we have that

$$H_1(G,\mathbb{Z}) = H_0(G, I_G) = \frac{I_G}{I_G^2} = G^{ab}$$

where $G^{ab} \stackrel{\text{df}}{=} G/[G:G]$ is the maximal abelian quotient of G. The isomorphism $G^{ab} \approx I_G/I_G^2$ is given by $\sigma \cdot [G:G] \mapsto (\sigma - 1) \cdot I_G^2$.

The main vanishing theorem is **Shapiro's lemma**.

Lemma 4.1.9 (Shapiro) *Let $H \subset G$ be a subgroup and N be an H-module. Then for all $i \geq 0$ we have isomorphisms*

$$H^i(H,N) = H^i(G, \mathrm{Ind}_H^G(N)) \qquad \textit{and} \qquad H_i(H,N) = H_i(G, \mathrm{Ind}_H^G(N))$$

In particular, any induced G-module has trivial cohomology and homology.

Proof (Sketch) For any any G-module M and any H-module N we have a canonical isomorphism $\mathrm{Hom}_G(M, \mathrm{Ind}_H^G N) = \mathrm{Hom}_H(M,N)$ and the functor $\mathrm{Ind}_H^G(-)$ is exact. From these two properties it follows that $\mathrm{Ind}_H^G(-)$ preserves injectives, hence given an injective resolution $0 \to N \to I^\bullet$ of N, we obtain an injective resolution $0 \to \mathrm{Ind}_H^G(N) \to \mathrm{Ind}_H^G(I^\bullet)$ of $\mathrm{Ind}_H^G(N)$. The result follows by applying $\mathrm{Hom}_G(\mathbb{Z}, -)$ and using the fact that $\mathrm{Hom}_G(\mathbb{Z}, \mathrm{Ind}_H^G N) = \mathrm{Hom}_H(\mathbb{Z}, N)$. The proof for homology is similar. □

Corollary 4.1.10 *If $L \supset K$ is a finite Galois extension with $G = \mathrm{Gal}(L/K)$ then $H^0(G, L^+) = K^+$ and $H^p(G, L^+) = 0$ for $p \geq 1$.*

Definition 4.1.11 The p-th **Tate cohomology group** is defined by

$$H_T^p(G,M) = \begin{cases} H^p(G,M) & \text{if } p \geq 1\\ \dfrac{M^G}{N_G M} & \text{if } p = 0\\ \dfrac{\ker N_G}{I_G \cdot M} & \text{if } p = -1\\ H_{-p-1}(G,M) & \text{if } p \leq -2 \end{cases}$$

The importance of the Tate cohomology groups is that it allows us to splice the long exact sequences of homology and cohomology into a single very long one. Given a short exact sequence of G-modules

$$0 \to A \to B \to C \to 0$$

we have a commutative diagram with exact rows

$$\begin{array}{ccccccccc} H_1(G,C) & \longrightarrow & H_0(G,A) & \longrightarrow & H_0(G,B) & \longrightarrow & H_0(G,C) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N_G} & & \downarrow{\scriptstyle N_G} & & \downarrow{\scriptstyle N_G} & & \\ 0 & \longrightarrow & H^0(G,A) & \longrightarrow & H^0(G,B) & \longrightarrow & H^0(G,C) & \longrightarrow & H^1(G,A) \end{array}$$

where the vertical arrows are induce by the norm maps. Hence we obtain an exact sequence

$$\begin{aligned} \cdots \to H_T^{-1}(G,A) \to H_T^{-1}(G,B) \to H_T^{-1}(G,C) \\ \to H_T^0(G,A) \to H_T^0(G,B) \to H_T^0(G,C) \\ \to H_T^1(G,A) \to H_T^1(G,B) \to H_T^1(G,C) \to \cdots \end{aligned}$$

Example 4.1.12 (Periodicity of Tate cohomology for cyclic groups) If G is cyclic we have that

$$H_T^p(G,M) = \begin{cases} \dfrac{M^G}{N_G M} & \text{if } p \text{ is even} \\ \dfrac{\ker N_G}{I_G \cdot M} & \text{if } p \text{ is odd} \end{cases}$$

4.2 Explicit Resolutions

Here we show how to define homology and cohomology via an explicit projective resolution of $\mathbb{Z}$:

Definition 4.2.1 The **standard resolution** of $\mathbb{Z}$ is the projective resolution

$$\cdots \xrightarrow{d_3} \tilde{C}_2 \xrightarrow{d_2} \tilde{C}_1 \xrightarrow{d_1} \tilde{C}_0 \xrightarrow{d_0} \mathbb{Z} \longrightarrow 0$$

where $\tilde{C}_p = \mathbb{Z}[G^{p+1}]$ is the free $\mathbb{Z}$-module with basis $(\sigma_0, \sigma_1, \ldots, \sigma_p) \in G^{p+1} = G \times \cdots \times G$ ($p+1$ times) with "diagonal" G-action $s \cdot (\sigma_0, \ldots, \sigma_p) = (s \cdot \sigma_0, \ldots, s \cdot \sigma_p)$, and where $d_{p+1} \colon \tilde{C}_{p+1} \to \tilde{C}_p$ is given by

$$d(\sigma_0, \sigma_1, \ldots, \sigma_{p+1}) = \sum_{0 \le k \le p+1} (-1)^k (\sigma_0, \sigma_1, \ldots, \sigma_{k-1}, \sigma_{k+1}, \ldots, \sigma_{p+1})$$

Applying $\mathrm{Hom}_G(-, M)$ to the standard resolution, we obtain a complex of abelian groups

$$0 \longrightarrow \tilde{C}^0(G,M) \xrightarrow{\tilde{d}^0} \tilde{C}^1(G,M) \xrightarrow{\tilde{d}^1} \tilde{C}^2(G,M) \xrightarrow{\tilde{d}^2} \cdots$$

where

$$\tilde{C}^p(G,M) \stackrel{\text{df}}{=} \left\{ \text{functions } \tilde{f} \colon G^{p+1} \to M \;\middle|\; \begin{array}{l} \tilde{f}(s \cdot \sigma_0, \ldots, s \cdot \sigma_p) = s \cdot \tilde{f}(\sigma_0, \ldots, \sigma_p) \text{ for all} \\ s \in G \text{ and } (\sigma_0, \ldots, \sigma_p) \in G^{p+1} \end{array} \right\}$$

and $\tilde{d}^p \colon \tilde{C}^p(G,M) \to \tilde{C}^{p+1}(G,M)$ is given by

$$(\tilde{d}^p \tilde{f})(\sigma_0, \ldots, \sigma_{p+1}) = \sum_{0 \le k \le p+1} (-1)^k \tilde{f}(\sigma_0, \ldots, \sigma_{k-1}, \sigma_{k+1}, \ldots, \sigma_{p+1})$$

We have an isomorphism between $\tilde{C}^p(G,M)$ and the abelian group $C^p(G,M)$ of all functions from G^p to M: it takes $f \in \tilde{C}^p(M)$ to the function

$$(\sigma_1, \sigma_2, \ldots, \sigma_p) \mapsto \tilde{f}(1, \sigma_1, \sigma_1\sigma_2, \sigma_1\sigma_2\sigma_3, \ldots, \sigma_1\sigma_2 \cdots \sigma_p)$$

The above complex is therefore isomorphic to the following "inhomogeneous" one

$$0 \longrightarrow C^0(G,M) \xrightarrow{d^0} C^1(G,M) \xrightarrow{d^1} C^2(G,M) \xrightarrow{d^2} \cdots$$

where $d^p\colon C^p(G,M) \to C^{p+1}(G,M)$ is given by

$$\begin{aligned}(d^p f)(\sigma_1,\ldots,\sigma_{p+1}) = {}& \sigma_1 \cdot f(\sigma_2,\ldots,\sigma_{p+1}) \\ & + \sum_{1\le k\le p} (-1)^k f(\sigma_1,\ldots,\sigma_{k-1},\sigma_k\cdot\sigma_{k+1},\sigma_{k+2},\ldots,\sigma_{p+1}) \\ & + (-1)^{p+1} f(\sigma_1,\ldots,\sigma_p)\end{aligned}$$

Hence we obtain an explicit formula

$$H^p(G,M) = \frac{\ker d^p}{\operatorname{im} d^{p+1}}$$

An element of $\ker d^p$ is called a p**-cocycle** while an element of $\operatorname{im} d^{p-1}$ is called a p**-coboundary**. Let

$$0 \to A \to B \to C \to 0$$

be a short exact sequence of G-modules. In terms of cocycles and coboundaries, one has a very explicit description of the **connecting morphism**

$$\delta\colon H^p(G,C) \to H^{p+1}(G,A)$$

as follows: given a p-cocycle $f\colon G^p \to C$ representing an element $\varphi = [f] \in H^p(G,C)$, we may lift it to a function $\hat{f}\colon G^p \to B$. Then $d^p\hat{f}$ is in the image of the map $C^{p+1}(G,A) \to C^{p+1}(G,B)$ induced by $A \to B$, so we may view it as a p-cocycle $d^p\hat{f}\colon G^{p+1} \to A$, and $\delta(\varphi) = [d^p\hat{f}] \in H^{p+1}(G,A)$.

Similarly, for homology one obtains an inhomogeneous complex

$$\cdots \xrightarrow{d_3} C_2(G,M) \xrightarrow{d_2} C_1(G,M) \xrightarrow{d_1} C_0(G,M) \longrightarrow 0$$

where $C_p(G,M) = C^p(G,M)$ and $d_p\colon C_p(G,M) \to C_p(G,M)$ is given now by

$$\begin{aligned}(d_p f)(\sigma_1,\ldots,\sigma_{p-1}) = {}& \sum_{\sigma\in G} \sigma^{-1}\cdot f(\sigma,\sigma_1,\ldots,\sigma_{p-1}) \\ & + \sum_{1\le k\le p-1} (-1)^k \sum_{\sigma\in G} f(\sigma_1,\ldots,\sigma_{k-1},\sigma_k\cdot\sigma,\sigma^{-1},\sigma_{k+1},\ldots,\sigma_{p-1}) \\ & + (-1)^{p+1} \sum_{\sigma\in G} f(\sigma_1,\ldots,\sigma_{p-1},\sigma)\end{aligned}$$

Example 4.2.2 We have that a 1-cocycle is a function $f\colon G \to M$ such that $f(\sigma\tau) = \sigma f(\tau) + f(\sigma)$. It is a coboundary if and only if it has the form $f(\sigma) = \sigma m - m$ for some $m \in M$. In particular, if the G-action on M is trivial, then all 1-coboundaries are trivial and a 1-cocycle is just a group morphism: $H^1(G,M) = \operatorname{Hom}(G,M)$ in this case.

Example 4.2.3 Let G be a cyclic group of order n generated by σ. Then one has an exact sequence of G-modules

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

As we shall see later, $H^i(G,\mathbb{Q}) = 0$ for all $i \ge 1$ and hence the connecting maps induce isomorphisms $\delta\colon H^i(G,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\approx} H^{i+1}(G,\mathbb{Z})$ for all $i \ge 0$. Then $H^1(G,\mathbb{Q}/\mathbb{Z}) = \operatorname{Hom}(G,\mathbb{Q}/\mathbb{Z})$ is a group of order n, generated by a morphism $f\colon G \to \mathbb{Q}/\mathbb{Z}$ given by $f(\sigma) = \frac{1}{n} \bmod \mathbb{Z}$, and hence $H^2(G,\mathbb{Z})$ is also cyclic of order n, generated by the class of the 2-cocycle

$$\delta f(\sigma^i,\sigma^j) = \begin{cases} 1 & \text{if } i+j \ge n \\ 0 & \text{otherwise} \end{cases} \qquad \text{for} \quad 0 \le i,j < n$$

which can be computed as described above using the lift $\hat{f}\colon G \to \mathbb{Q}$ of f given by $\hat{f}(\sigma^i) = \frac{i}{n}$ for $0 \le i < n$.

Now we use the explicit characterisation of cohomology in terms of cocycles to prove a very important vanishing theorem in Galois cohomology:

Theorem 4.2.4 (Hilbert's Satz 90) *Let $L \supset K$ be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Then*

$$H^1(G, L^\times) = 0$$

PROOF Let $f\colon G \to L^\times$ be a 1-cocycle, and consider the element

$$m \stackrel{\mathrm{df}}{=} \sum_{\sigma \in G} f(\sigma) \cdot \sigma(a)$$

where $a \in L^\times$ is chosen so that $m \neq 0$, which is possible by Dedekind's independency of characters. Then for every $\tau \in G$ we have that

$$m = \sum_{\sigma \in G} f(\tau\sigma) \cdot \tau\sigma(a) = \sum_{\sigma \in G} \tau\big(f(\sigma)\big) \cdot f(\tau) \cdot \tau\sigma(a) = \tau(m) \cdot f(\tau)$$

That is, $f(\tau)^{-1} = \tau(m)/m$, showing that f is a coboundary. □

4.3 Dimension shifting; Inflation, Restriction, Corestriction

We have seen how changing modules alters the cohomology groups via the long exact sequence. Now we show how changing the group alters the cohomology. Let $f\colon G' \to G$ be a group morphism and A be a G-module. We may view A as a G'-module as well via

$$\sigma' \cdot a \stackrel{\mathrm{df}}{=} f(\sigma') \cdot a \qquad \text{for} \quad a \in A, \quad \sigma' \in G'$$

We denote this G'-module by f^*A. Clearly A^G is a subgroup of $(f^*A)^{G'}$, hence the inclusion map defines a functorial map $H^0(G, A) \to H^0(G', f^*A)$. By general properties of derived functors, this map in degree 0 extends uniquely for all $p \geq 0$ to a functorial map $H^p(G, A) \to H^p(G', f^*A)$, compatible with the connecting maps. We recall the proof of this fact since it relies on a recurrent technique in group homology/cohomology known as **dimension shifting**.

First write an exact sequence of G-modules

$$0 \to A \to I \to B \to 0$$

with I injective (cohomologically trivial would do, for instance an induced module). Since $H^p(G, I) = 0$ for all $p > 0$ we have that the connecting maps give isomorphisms $\delta\colon H^{p-1}(G, B) \xrightarrow{\approx} H^p(G, A)$ for all $p > 1$. Now, for $p > 1$, if we already know the map $H^{p-1}(G, -) \to H^{p-1}(G', f^*-)$ in dimension $p-1$ we may define it in dimension p via the composition

$$H^p(G, A) \xrightarrow[\approx]{\delta^{-1}} H^{p-1}(G, B) \longrightarrow H^{p-1}(G', f^*B) \xrightarrow{\partial} H^p(G', f^*A)$$

where ∂ denotes the connecting map with respect to the exact sequence of G'-modules

$$0 \to f^*A \to f^*I \to f^*B \to 0$$

For the "base case" $p = 1$ the procedure is similar but we need to use the commutative diagram instead

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A^G & \longrightarrow & I^G & \longrightarrow & B^G & \longrightarrow & H^1(G, A) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \vdots & & \\
0 & \longrightarrow & (f^*A)^{G'} & \longrightarrow & (f^*I)^{G'} & \longrightarrow & (f^*B)^{G'} & \longrightarrow & H^1(G', f^*A) & \longrightarrow & \cdots
\end{array}$$

Similar procedures work for homology and also for Tate cohomology groups. One may consider the more general case where A' is a G'-module and $g\colon A \to A'$ is a group morphism which is compatible with f in the sense that $g(f(\sigma') \cdot a) = \sigma' \cdot g(a)$ for all $a \in A$ and $\sigma' \in G'$. Then the degree 0 map induced by g extends to a map $H^p_T(G, A) \to H^p_T(G', A')$ for all p.

Definition 4.3.1 Let $H \leq G$ be a subgroup and M be a G-module. We define the **restriction** map

$$\mathrm{res}\colon H^p_T(G,M) \to H^p_T(H,M)$$

to be the map induced by the inclusion map $M^G \hookrightarrow M^H$ in degree 0 (take $f\colon H \hookrightarrow G$ to be the inclusion map).
Now suppose that $H \lhd G$ is normal. We define the **inflation**

$$\mathrm{inf}\colon H^p_T(G/H, M^H) \to H^p_T(G,M)$$

to be the map induced by the identity $(M^H)^{G/H} = M^G$ in degree 0 (take $f\colon G \twoheadrightarrow G/H$ to be the quotient map and $g\colon M^H \hookrightarrow M$ to be the inclusion).

For $p \geq 0$, the restriction and inflation maps have a very simple description in terms of the standard resolution. Given a p-cocycle $f\colon G^p \to M$, $\mathrm{res}([f])$ is represented by the restriction $f\colon H^p \to M$ of f to H^p. On the other hand, for a p-cocycle $f\colon (G/H)^p \to M^H$ we have that $\mathrm{inf}([f])$ is given by the p-cocycle $\tilde{f}\colon G^p \to M$ given by the composition

$$G^p \twoheadrightarrow (G/H)^p \xrightarrow{f} M^H \hookrightarrow M$$

where the unlabelled maps are the natural ones.

Theorem 4.3.2 (Inflation-restriction sequence) *Let M be a G-module, and H be a normal subgroup of G. Suppose that $H^p(H,M) = 0$ for $p = 1, \ldots, q-1$. Then*

$$0 \longrightarrow H^q(G/H, M^H) \xrightarrow{\mathrm{inf}} H^q(G,M) \xrightarrow{\mathrm{res}} H^q(H,M)$$

is exact.

Proof The result follows easily for $p = 1$ by direct computation with cocycles. The general case follows by dimension shifting. Suppose that $q \geq 2$ and consider an exact sequence of G-modules (see lemma 4.1.5)

$$0 \to M \to \mathrm{Ind}^G(M_0) \to N \to 0 \qquad (*)$$

Note that the middle term is induced also as an H-module. Since $H^1(H,M) = 0$ by hypothesis we have that the sequence of G/H-modules

$$0 \to M^H \to \left(\mathrm{Ind}^G(M_0)\right)^H \to N^H \to 0 \qquad (**)$$

is still exact. The middle term $\left(\mathrm{Ind}^G(M_0)\right)^H = \mathrm{Ind}^{G/H}(M_0)$ is induced as a G/H-module, and we have a commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^q(G/H, M^H) & \xrightarrow{\mathrm{inf}} & H^q(G,M) & \xrightarrow{\mathrm{res}} & H^q(H,M) \\
 & & \uparrow \approx & & \uparrow \approx & & \uparrow \approx \\
0 & \longrightarrow & H^{q-1}(G/H, N^H) & \xrightarrow{\mathrm{inf}} & H^{q-1}(G,N) & \xrightarrow{\mathrm{res}} & H^{q-1}(H,N)
\end{array}$$

where the vertical arrows are the connecting maps associated to $(*)$ and $(**)$, which are isomorphisms since the middle terms of $(*)$ and $(**)$ are cohomologically trivial. Since $H^p(H,N) = H^{p+1}(H,M) = 0$ for $p = 1, 2, \ldots, q-2$ we have that the bottom row is exact by induction on q. Hence the top row is also exact. □

Remark 4.3.3 For the expert (but then you shouldn't be reading this appendix!): the previous result follows directly from the Hochschild-Serre spectral sequence

$$H^p(G/H, H^q(H, M)) \Rightarrow H^{p+q}(G, M)$$

Remark 4.3.4 Using the inflation map one can define cohomology for profinite groups as well. A group is **profinite** if it is the projective limit of finite groups. For instance, for any field k, its **absolute Galois group** $G_k \stackrel{\text{df}}{=} \text{Gal}(k_{sp}/k)$ is profinite. If $G = \varprojlim_{i \in I} G_i$, giving the discrete topology to the finite groups G_i, G is made into a topological space as well, namely the projective limit of the topological spaces G_i. Since the product of discrete groups is compact by Tychonoff's theorem and G is a closed subgroup of $\prod_{i \in I} G_i$ we have that G is compact. Now let M a continuous G-module, namely a G-module for which the action $G \times M \to M$ is continuous. This means that for every $m \in M$ the orbit $G \cdot m$ is finite. Then we can define the p-th cohomology group as

$$H^p(G, M) \stackrel{\text{df}}{=} \varprojlim_{H} H^p(G/H, M^H)$$

where H runs over all open normal subgroups of G and the transition maps are given by inflation.

Let us go back to the finite case. Let $H \leq G$ be a subgroup and M be a G-module. We define the **norm map** $N_{G/H} \colon M^H \to M^G$ via

$$N_{G/H}(m) \stackrel{\text{df}}{=} \sum_{\sigma \in S} \sigma(m)$$

where S is a set of left cosets representatives of G/H. Clearly this does not depend on the choice of S and the above sum is G-invariant. Now dimension shifting allows us to extend this map to all other dimensions using an exact sequence of G-modules (see lemma 4.1.5)

$$0 \to M \to \text{Ind}^G(M_0) \to N \to 0$$

and the fact that the middle term is also induced as an H-module.

Definition 4.3.5 The map

$$\text{cor} \colon H^p_T(H, M) \to H^p_T(G, M)$$

induced by the norm map $N_{G/H} \colon M^H \to M^G$ in degree 0 is called **corestriction**.

Theorem 4.3.6 (Restriction-Corestriction) *Let $H \leq G$ be a subgroup and M be a G-module. Then the composition*

$$H^p_T(G, M) \xrightarrow{\text{res}} H^p_T(H, M) \xrightarrow{\text{cor}} H^p_T(G, M)$$

equals multiplication by $[G : H]$. In particular, $H^p_T(G, M)$ is killed by $|G|$.

Proof For $p = 0$ we have that the above composition is

$$\frac{M^G}{N_G M} \longrightarrow \frac{M^H}{N_H M} \xrightarrow{N_{G/H}} \frac{M^G}{N_G M}$$

where the first map is the natural one. This composition is clearly multiplication by $[G : H]$. The general case now follows easily by dimension shifting. □

Example 4.3.7 Let G_p be any p-Sylow subgroup of G. Then res: $H^p(G, M) \to H^p(G_p, M)$ is injective on the p-primary components of these groups. In fact, cor $\circ$ res is multiplication by $[G : G_p]$, which is prime to p, and thus is an automorphism on these p-primary components.

Example 4.3.8 We have that $H^p_T(G, \mathbb{Q}) = 0$ for all p. In fact, multiplication by $|G|$ is an automorphism of $\mathbb{Q}$. Since $H^p(G, -)$ is a functor, this implies that multiplication by $|G|$ is also an automorphism of $H^p_T(G, \mathbb{Q})$ which must then be zero by the theorem.

4.4 Cup product

Definition 4.4.1 There exists a unique family of maps

$$H_T^p(G,A)\otimes H_T^q(G,B)\xrightarrow{\cup} H_T^{p+q}(G,A\otimes B)$$

(tensor products over $\mathbb{Z}$) called **cup products**, which are characterised by the following properties:

1. the cup product is a morphism of bifunctors (a.k.a natural transformations) in the pair (A,B);
2. for $p=q=0$ the cup product is induced by the natural map $A^G\otimes B^G\to(A\otimes B)^G$;
3. the cup product is compatible with connection morphisms: if

$$0\to A'\to A\to A''\to 0$$

is an exact sequence of G-modules and B is a G-module such that

$$0\to A'\otimes B\to A\otimes B\to A''\otimes B\to 0$$

is exact then the diagram

$$\begin{array}{ccc} H_T^p(G,A'')\otimes H_T^q(G,B) & \xrightarrow{\cup} & H_T^{p+q}(G,A''\otimes B) \\ \Big\downarrow{\scriptstyle \delta^p\otimes \mathrm{id}} & & \Big\downarrow{\scriptstyle \delta^{p+q}} \\ H_T^{p+1}(G,A')\otimes H_T^q(G,B) & \xrightarrow{\cup} & H_T^{p+q+1}(G,A'\otimes B) \end{array}$$

commutes. On the other hand, if

$$0\to B'\to B\to B''\to 0$$

is an exact sequence of G-modules and A is a G-module such that

$$0\to A\otimes B'\to A\otimes B\to A\otimes B''\to 0$$

is exact then the diagram

$$\begin{array}{ccc} H_T^p(G,A)\otimes H_T^q(G,B'') & \xrightarrow{\cup} & H_T^{p+q}(G,A\otimes B'') \\ \Big\downarrow{\scriptstyle \mathrm{id}\otimes\delta^q} & & \Big\downarrow{\scriptstyle (-1)^p\cdot\delta^{p+q}} \\ H_T^p(G,A)\otimes H_T^{q+1}(G,B') & \xrightarrow{\cup} & H_T^{p+q+1}(G,A\otimes B') \end{array}$$

commutes.

Uniqueness of this family is easily proven by dimension shifting, while existence is given by the explicit formulas in cocycles. First we extend the standard resolution by setting $\tilde{C}_{-p}=\tilde{C}^*_{p-1}$ for $p\geq 1$, where $\tilde{C}^*_{p-1}$ is the dual of $\tilde{C}_{p-1}=\mathbb{Z}[G^p]$, namely the free $\mathbb{Z}$-module with basis given by functions $(\sigma_1^*,\dots,\sigma_p^*)$, which send $(\sigma_1,\dots,\sigma_p)$ to $1\in\mathbb{Z}$ and every other basis element of $\tilde{C}_{p-1}$ to $0\in\mathbb{Z}$. The boundary map $d_{-p}\colon\tilde{C}_{-p}\to\tilde{C}_{-p-1}$ is given by

$$d_{-p}(\sigma_1^*,\dots,\sigma_p^*)=\sum_{s\in G}\sum_{0\leq i\leq q}(-1)^i(\sigma_1^*,\dots,\sigma_i^*,s^*,\sigma_{i+1}^*,\dots,\sigma_p^*)$$

and $d_0\colon\tilde{C}_0\to\tilde{C}_{-1}$ is given by $d_0(\sigma_0)=\sum_{s\in G}(s^*)$. One may then compute the Tate cohomology groups by applying $\mathrm{Hom}_G(-,M)$ to this sequence and computing the cohomology of the resulting complex.

Now define $\phi_{p,q}\colon\tilde{C}_{p+q}\to\tilde{C}_p\otimes\tilde{C}_q$ as follows:

- For $p, q \geq 0$
$$\phi_{p,q}(\sigma_0, \ldots, \sigma_{p+q}) = (\sigma_0, \ldots, \sigma_p) \otimes (\sigma_p, \ldots, \sigma_{p+q})$$
- For $p, q \geq 1$
$$\phi_{-p,-q}(\sigma_1^*, \ldots, \sigma_{p+q}^*) = (\sigma_1^*, \ldots, \sigma_p^*) \otimes (\sigma_{p+1}^*, \ldots, \sigma_{p+q}^*)$$
- For $p \geq 0$, $q \geq 1$
$$\phi_{p,-p-q}(\sigma_1^*, \ldots, \sigma_q^*) = \sum (\sigma_1, s_1, \ldots, s_p) \otimes (s_p^*, \ldots, s_1^*, \sigma_1^*, \ldots, \sigma_q^*)$$
$$\phi_{-p-q,p}(\sigma_1^*, \ldots, \sigma_q^*) = \sum (\sigma_1^*, \ldots, \sigma_q^*, s_1^*, \ldots, s_p^*) \otimes (s_p, \ldots, s_1, \sigma_q)$$
$$\phi_{p+q,-q}(\sigma_0, \ldots, \sigma_p) = \sum (\sigma_0, \ldots, \sigma_p, s_1, \ldots, s_q) \otimes (s_q^*, \ldots, s_1^*)$$
$$\phi_{-q,p+q}(\sigma_0, \ldots, \sigma_p) = \sum (s_1^*, \ldots, s_q^*) \otimes (s_q, \ldots, s_1, \sigma_0, \ldots, \sigma_p)$$

  where the sum runs over all $(s_1, \ldots, s_p) \in G^p$.

Then a straightforward but long check shows that $(\epsilon \otimes \epsilon) \circ \phi_{0,0} = \epsilon$ (here $\epsilon \colon \tilde{C}_0 \to \mathbb{Z}$ denotes the augmentation map) and that

$$\phi_{p,q} \circ d = (d \otimes 1) \circ \phi_{p+1,q} + (-1)^p (1 \otimes d) \circ \phi_{p,q+1}$$

for all $p, q \in \mathbb{Z}$ (we omitted the indices of the coboundary maps d for notational clarity). Now given $f \in \mathrm{Hom}_G(\tilde{C}_p, A)$ and $g \in \mathrm{Hom}_G(\tilde{C}_q, B)$ we define $f \cup g \in \mathrm{Hom}_G(\tilde{C}_{p+q}, A \otimes B)$ by

$$f \cup g = (f \otimes g) \circ \phi_{p,q}$$

and now it is easy to check that if f and g are cocycles, so is $f \cup g$, and that its class depends only on the classes of f and g. A lengthy but easy check shows that the pairing $\cup$ so defined has the desired properties of the cup product.

The following lemma can be easily proved by dimension shifting, and is left as an exercise for the reader since I'm running out of time and energy:

Lemma 4.4.2 *Let $H \leq G$ be a subgroup. We have*

1. *$(a \cup b) \cup c = a \cup (b \cup c)$ in $H_T^{p+q+r}(G, A \otimes B \otimes C)$ for $a \in H_T^p(G, A)$, $b \in H_T^q(G, B)$, $c \in H_T^r(G, C)$;*
2. *$a \cup b = (-1)^{pq} \cdot b \cup a$ under the isomorphism $A \otimes B = B \otimes A$ for $a \in H_T^p(G, A)$, $b \in H_T^q(G, B)$;*
3. *$\mathrm{res}(a \cup b) = \mathrm{res}\, a \cup \mathrm{res}\, b \in H_T^{p+q}(H, A \otimes B)$ for $a \in H_T^p(G, A)$ and $b \in H_T^q(G, B)$;*
4. *$\mathrm{cor}\big(a \cup \mathrm{res}\, b\big) = \mathrm{cor}\, a \cup b$ for $a \in H^p(H, A)$ and $b \in H^q(G, B)$.*

Our last theorem shows that how the cup product enters in the periodicity of the cohomology of cyclic groups:

Theorem 4.4.3 *Let G be a cyclic group of order n and σ be a generator. Consider the 2-cocycle $f \colon G \times G \to \mathbb{Z}$ given by*

$$f(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } i + j \geq n \\ 0 & \text{otherwise} \end{cases} \qquad \text{for} \quad 0 \leq i, j < n$$

Then for any G-module M the cup product $- \cup [f]$ gives an isomorphism

$$H_T^p(G, M) \xrightarrow[\approx]{\cup [f]} H_T^{p+2}(G, M)$$

Proof We have exact sequences of G-modules

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$
$$0 \longrightarrow \mathbb{Z} \xrightarrow{\mu} \mathbb{Z}[G] \xrightarrow{\sigma - 1} I_G \longrightarrow 0$$

where ϵ is the augmentation map, μ denotes multiplication by $1 + \sigma + \cdots + \sigma^{n-1}$ and $\mathbb{Z}[G] \to I_G$ is given by multiplication by $\sigma - 1$. The connecting maps $\partial \colon H_T^p(G, \mathbb{Z}) \xrightarrow{\approx} H_T^{p+1}(G, I_G)$ and $\delta \colon H_T^{p+1}(G, I_G) \xrightarrow{\approx} H_T^{p+2}(G, \mathbb{Z})$ are isomorphisms and by explicit computations with cocycles we have that $[f] = \delta \circ \partial(\phi)$ where $\phi = 1 \bmod n \in H_T^0(G, \mathbb{Z}) = \mathbb{Z}/n$.

Since all terms of the above sequences are free $\mathbb{Z}$-modules they stay exact after tensoring with M. Therefore for any $\alpha \in H_T^p(G, M)$ we have that

$$\alpha \cup [f] = \alpha \cup \delta \circ \partial(\phi) = \delta \circ \partial(\alpha \cup \phi) = \delta \circ \partial(\alpha)$$

since $- \cup \phi$ is the identity, as can be easily checked by dimension shifting for example. Now since $\mathbb{Z}[G] \otimes M$ is induced the connecting maps $\partial \colon H_T^p(G, M) \xrightarrow{\approx} H_T^{p+1}(G, M \otimes I_G)$ and $\delta \colon H_T^{p+1}(G, M \otimes I_G) \xrightarrow{\approx} H_T^{p+2}(G, M)$ are isomorphisms, hence so is $\delta \circ \partial$ and we are done. □

Bibliography

1. E. Artin and J. Tate, *Class field Theory*, Addison-Wesley.
2. Z. I. Borevich, I. R. Shafarevich, *Number Theory*, Academic Press.
3. J. W. S. Cassels, *Local Fields*, London Mathematical Society Student Text 3, Cambridge University Press.
4. J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press.
5. P. Gille and T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge University Press.
6. J. S. Milne, *Algebraic Number Theory*, course notes, available at `http://www.jmilne.org/math/`
7. J. S. Milne, *Class Field Theory*, course notes, available at `http://www.jmilne.org/math/`
8. J. Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften 322, Springer-Verlag.
9. J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields*, Grundlehren der Mathematischen Wissenschaften 323, Springer-Verlag
10. J-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics 7, Springer-Verlag
11. J-P. Serre, *Local Fields*, Graduate Texts in Mathematics 67, Springer-Verlag
12. S. S. Shatz, *Profinite groups, Arithmetic, and Geometry*, Annals of Mathematical Studies 67, Princeton University Press.