eman ta zabal zazu

Universidad del País Vasco
Euskal Herriko Unibertsitatea

ZTF-FCT
Zientzia eta Teknologia Fakultatea
Facultad de Ciencia y Tecnología

Local Fields and their Abelian Extensions

Final Degree Dissertation
Degree in Mathematics

Jorge Fariña Asategui

Supervisor:
Gustavo A. Fernández Alcober

Leioa, 2019-2020

Contents

Preface

"In most sciences one generation tears down what another has built and what one has established another undoes. In mathematics alone each generation adds a new story to the old structure."

—Hermann Hankel.

April 8th, 1796. A young Carl Frieldrich Gauss (1777-1855) woke up and wrote the entry, "Numerorum primorum non omnes numeros infra ipsos residua quadratica esse posse demonstratione munitum." [1] to his diary [Kle03]. He had just devised the first correct proof of the quadratic reciprocity law. Previous efforts from Fermat, Euler and Legendre among others, had helped to establish this law and partial results on its veracity. Gauss was amazed by the beauty of this law, which he called *Theorema Aureum* (Golden Theorem), and he managed to provide seven more different proofs in his lifetime (three of them were published along the first one in his Disquisitiones Arithmeticae in 1801 [Gau01]). Today, more than two hundred different proofs of this law have been published.

Quadratic reciprocity shows an impressive simmetry that allows to determine if a prime p is a square modulo a prime q, by looking whether q is a square modulo p. A natural generalization is to find higher reciprocity laws, i.e. cubic, cuartic, quintic, etc. This leads directly to extending the field of rationals to more elaborated number fields. Ernst Kummer's (1810-1893) ideal numbers, a precursor for ideals later developed by Richard Dedekind (1831-1916), came to existence in search of these higher reciprocity laws.

In 1900, David Hilbert (1862-1943) made up a list of twenty three problems concerning some of the most relevant unsolved questions of his time. Among those problems, Problem 9th deals with general reciprocity laws [Hil00]:

[1] Prime numbers below (modulo) all numbers may not be quadratic residues, possesses a tough proof.

“Für einen beliebigen Zahlkörper soll das Reciprocitätsgesetz der l ten Potenzreste bewiesen werden, wenn l eine ungerade Primzahl bedeutet und ferner, wenn l eine Potenz von 2 oder eine Potenz einer ungeraden Primzahl ist. Die Aufstellung des Gesetzes, sowie die wesentlichen Hülfsmittel zum Beweise desselben werden sich, wie ich glaube, ergeben, wenn man die von mir entwickelte Theorie des Körpers der l ten Einheitswurzeln 1) und meine Theorie 2) des relativ-quadratischen Körpers in gehöriger Weise verallgemeinert.”[2]

Theory of ideals was further developed and Emil Artin (1898-1962) provided the first proof for his general reciprocity law in a series of papers around 1927, which implies all known reciprocity laws. This was deduced proving the main theorem of global class field theory, which describes abelian extensions of a global field in terms of its arithmetic intrinsic properties. A good account of this procedure is given in [Lan94] for example.

Later, the approach turned about to the local-global principle. The local version of class field theory, i.e. for local fields, was first proved by determining the Brauer group of a local field (see Chapter 3), and the global version was obtained by considering all primes at once via ideles and adeles. This procedure turned out to be better understood in the language of group cohomology, and this is the way it is currently presented [AT09].

Nowadays, generalisations to non abelian extensions are being developed extending the theory for abelian extensions. In this work we shall seek to study local class field theory.

Let us show the reader an intuitive motivation for class field theory. Given a field K and a finite Galois extension L/K, the main theorem of Galois theory describes the intermediate field extensions in terms of the subgroups of the Galois group. However, this procedure needs the finite extension field L to be fixed first. We may wonder if we can give a description of all the finite extensions of a given field. This is not an easy feat to accomplish with all generality[3], but it is easier if we restrict our attention to finite abelian extensions. In the case where the base field is either the field of complex numbers or the reals, this description is trivial since $\mathbb{C}$ is algebraically closed and $\mathbb{R}$ has a unique abelian extension, namely $\mathbb{C}$.

[2] For any number field the reciprocity law for lth residues should be proved, when l is an odd prime and when l is a power of 2 or of an odd prime. The list of laws, as well as complementaries for the proof itself should be obtained, in my opinion, from my well-developed lth cyclotomic field theory 1) and an appropiate generalization of my theory 2) of relative-quadratic fields.

[3] There are still open problems concerning the Galois group $\mathrm{Gal}(\mathbb{Q}^{al}/\mathbb{Q})$, such as whether each finite group occurs as a quotient of it [Mil20].

Let E and F be two finite abelian extensions of K. Then, the composite EF is also Galois. What is more, $\mathrm{Gal}(EF/K)$ is isomorphic to a subgroup of the cartesian product $\mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$, which is abelian; thus, EF/K is abelian too.

But, what can be said about the composite of a countable number of abelian extensions? Let us see a motivating example. Let the base field be the field of rationals. Then, it is known from the course in Algebraic Equations that for each natural number n, the nth cyclotomic extension is abelian. Since the degree of the nth cyclotomic extension is precisely $\varphi(n)$, these degrees are not bounded and the composite of them all is an infinite extension. We leave to the reader the details on why this composite is an abelian Galois extension of $\mathbb{Q}$, as a preparation for the following explanations which shall generalize this example to a general field extension L/K.

Let L/K be a general Galois infinite field extension and define the set

$$\mathcal{L} := \{E : E \text{ finite Galois intermediate extension of } L/K\}.$$

Note that for any pair $E, F \in \mathcal{L}$ their composite $EF \in \mathcal{L}$. This makes $\mathcal{L}$ into a directed poset with respect to the inclusion. Also, note that for any pair $E, F \in \mathcal{L}$ the natural inclusions $\varphi_{EF} : E \to F$ lift the elements in E to F, whenever $E \subseteq F$. This makes $\mathcal{L}$ into a direct system over itself. Note that the same natural liftings $\varphi_E : E \to L$ exist for each $E \in \mathcal{L}$. What is more, these liftings are compatible with the ones in the direct system, i.e. , $\varphi_E = \varphi_{EF}\varphi_F$ whenever $E \subseteq F$. Then, by the universal property of the direct limit (see Chapter 1), L can be regarded as the direct limit $\varinjlim E = \bigcup E$. Then, any element in L lies in a finite Galois extension of K, E, and there is a very natural way to describe the K-automorphisms of L: as coherent tuples $(\sigma_E)_E$.

An expected, but which the reader should prove, property of an infinite Galois extension L/K is that its Galois group is infinite (hint: show the degrees of intermediate fields are not bounded).

We could expect the finite Galois correspondence to generalize immediately to the infinite case. Sadly, this is not the case. In particular, not all finite index subgroups of $\mathrm{Gal}(L/K)$ need correspond to finite intermediate extensions, i.e. they may not be of the form $\mathrm{Gal}(L/E)$ (see Problem A.1). However, this may be fixed by endowing the Galois group with a special topology where these subgroups are precisely open, turning $\mathrm{Gal}(L/K)$ into a topological group. Let G denote the Galois group of the extension L/K. Given an intermediate field E Galois over K, there is a natural projection from G to $\mathrm{Gal}(E/K)$ by restriction of automorphisms. Also, for intermediate Galois field extensions $K \subseteq E \subseteq F \subseteq L$, there is a natural composition of restrictions $G \to \mathrm{Gal}(F/K) \to \mathrm{Gal}(E/K)$ which is no more than the usual restriction $G \to \mathrm{Gal}(E/K)$. What is more, for any pair of intermediate Galois field extensions $K \subseteq E, F \subseteq L$, there exists another intermediate Galois extensions field, namely the composite EF, containing both E and F and whose corresponding subgroup $\mathrm{Gal}(L/EF)$ is precisely the intersection of both subgroups $\mathrm{Gal}(L/E)$ and $\mathrm{Gal}(L/F)$. Then, these subgroups form a filter of normal subgroups. This filter can be used to give a topology to G, which is called the *Krull* topology. Also, it gives us as the data of an inverse system, where the objects are the finite Galois groups $\mathrm{Gal}(E/K)$ endowed with the discrete topology and the connection homomorphisms are the above restrictions. Thus, we may identify G with the inverse limit $\varprojlim \mathrm{Gal}(E/K)$ via the aforementioned projections and the universal property of the inverse limit (see Chapter 1). We shall see in Chapter 1 that both constructions coincide up to isomorphism and endow G with the same topology.

Now, we restrict our attention to abelian extensions of a field K. Applying previous reasoning with the added condition the extensions are abelian, i.e. letting $\mathcal{L} := \{E : E/K \text{ is finite abelian}\}$, the direct limit exists and it contains all the abelian extensions of K. This direct limit is called the *maximal abelian extension* of K and denoted by K^{ab}. Then, by the infinite Galois correspondence (see Chapter 1), studying the finite abelian extensions of K is equivalent to studying open subgroups of $\mathrm{Gal}(K^{ab}/K)$. The drawback is we have defined these open subgroups as the ones coming from finite intermediate extensions and *a priori* we have no way to distinguish among them. The special case where K is a finite field is very well known and we shall study it first to come up with a motivation for other fields. And this is precisely the objective of class field theory: studying these open subgroups via an easier-to-study group. What is more, we shall show this easier-to-study group is related to the arithmetic of the base group K, making the data of abelian finite extensions of K intrinsic to K, which, in my humble opinion, is a result of an astonishing beauty.

We aim to provide a complete proof of local class field theory. To fulfill this goal, we take a more algebraic approach, rather than the modern cohomological perspective. We follow the outline in [KKS11] and fill in the details from other sources and ourselves, trying to make the proof as short and as easy as possible since most texts take a lot longer to provide a full proof of this theorem. Inevitably we will be missing many interesting concepts and theories that arise in our discussion, which could take a whole book by themselves. We have no space either to deduce the global version of class field theory, which is a beautiful application of the local-global principle.

In the first chapter we introduce some preliminary concepts such as topological groups, profinite groups, character groups and Pontrjagin's duality, which shall appear in the rest of the work. We follow mostly [RZ10].

In the second chapter, we present basic facts about local and global fields and describe ramification of prime ideals in their abelian extensions. Due to lack of space, concepts such as differents or discriminants are not even mentioned. We provide a short introduction to topological groups and fields, in order to state Pontrjagin's duality, which is fundamental for the proof of local class field theory. We follow mostly [FV02] and [SG80] to state and prove results on completions. For the rest of the chapter we follow [KKS11].

The third chapter is devoted to determining the Brauer group of local fields. For that, we introduce the theory of division algebras, simple central algebras, crossed products and cyclic algebras, as well as a little introduction to classic group cohomology. We follow mostly [Jac85] for the theory of simple central algebras and [KKS11] for the determination of the Brauer group of a local field. The cohomological introduction is taken from [Mor96].

The last chapter is where a proof for local class field theory is given. We first show the finite field case as a precursor for local fields.Then, we prove local class field theory with all the tools from previous chapters. We follow and complete the proofs in [KKS11].

We have summarized some minor results that had no place on the main flow of the text in an appendix as solved exercises, just for completeness. Most problems are taken from the same sources as the main text, but some are taken from other sources. For example, Dedekind's Independence Theorem has been taken from [Jac09], which is not used for the main text. A second appendix contains the essentials of the theory of inverse limits, direct limits and profinite groups, just in case the reader is unfamiliar with these notions, allowing the reader to follow the explanations in this work flawlessly.

The reader is not assumed to have any prior knowledge apart from what is taught in this degree.

Lastly, a little notation issue. Map composition will be written multiplicatively from left to right, i.e. for maps f and g, their composition (also called product) will be written fg where first we apply f and then g.

Commutative rings will be assumed to have an identity, see [Poo14] for a short nice discussion on this.

List of Symbols

$\mathrm{Ann}_R(M)$	Annihilator of M
$\mathrm{Br}(k)$	Brauer group of a field k
$Z(G)$	Center of G.
$C_G(S)$	Centralizer of the set S in G.
G^*	Character group of G.
$X(K)$	Character group of $\mathrm{Gal}(K^{ab}/K)$.
$\mathbb{C}$	Complex numbers
$\hom_{\mathrm{cont}}(A, B)$	Continuous homomorphisms from A to B
H_G	Core of the subgroup H in the group G.
$[L : K]$	Degree of a field extension L/K
$\varinjlim_n G_n$	Direct limit.
A^e	Enveloping algebra of the k-algebra A
$\mathrm{N}_{L/K}$	Field norm of L/K
$\mathbb{F}_q$	Finite field of q elements
L/K	Field extension $K \subseteq L$
M^G	G-invariant part of M
$\mathrm{Gal}(L/K)$	Galois Group of the extension L/K
$R^\times$	Multiplicative group of units of a ring R
$\mathbb{Z}[G]$	Group ring
$\mathrm{Im}\ \varphi$	Image of φ
$\mathbb{Z}$	Integers
$\mathbb{Z}/n\mathbb{Z}$	Integers modulo n
$\varprojlim_n G_n$	Inverse limit.
$\ker \varphi$	Kernel of φ
$M_n(R)$	n-dimensional matrix ring with coefficients in R
K^{ab}	Maximal abelian extension of K.
$\min_{(}S)$	Minimum of the ordered set S
$B^n(G, M)$	n-coboundaries
$Z^n(G, M)$	n-cocycles
$H^n(G, M)$	nth cohomology group
ζ_n	nth primitive root of unity
A^{op}	Opposite algebra of the k-algebra A
$\mathrm{ord}_{\mathfrak{p}}$	$\mathfrak{p}$-adic valuation

$\mathbb{Z}_p$	p-adic Integers
$\mathbb{Q}_p$	p-adic numbers
$\widehat{G}$	Profinite completion of G
$\mathbb{H}$	Quaternions
$\mathbb{Q}$	Rational numbers
$\mathbb{R}$	Real numbers
End M	Ring of endomorphisms of M
$\mathcal{O}_K$	Ring of integers of a number field K
$A \otimes_k B$	Tensor product of k-algebras A and B
$\mathcal{O}_\nu$	Valuation ring of a valuation field K

Chapter 1

Preliminaries

In this work we will be working thoroughly with topological groups, profinite groups and character groups. Thus, we present briefly the basics, mostly without proofs, just for the reader to be more familiar with these notions and to ease the understanding of the proof of local class field theory. We follow mostly [RZ10].

1.1 Topological groups and fields

We can endow a group with a topology to have at the same time an algebraic structure and a structure of a topological space. However, this topology must satisfy some compatibility conditions with the algebraic structure. Namely, both the product and the inversion map in the group must be continuous. If these conditions are satisfied, then the group is called a *topological group.*

In topological groups there are two important homeomorphisms, $l_a(x) := ax$ called the *left translation map* and $r_a(x) := xa$ the *right translation map.* Thus, cosets of an open (closed) subgroup, are again open (closed).

This shows how a topology on a group should work like, but it does not give a way to define such a topology on a general group. Luckily, given a group G there is a natural way to make it into a topological group. Let $\mathcal{N}$ be a filter of normal subgroups, i.e. a set of normal subgroups such that for each pair in $\mathcal{N}$ the intersection is an overgroup of a normal subgroup in $\mathcal{N}$. Since in topological groups a fundamental system of open neighborhoods of the identity gives us a fundamental system of open neighborhoods for any other element in the group via these translation homeomorphisms, $\mathcal{N}$ defines a fundamental system of open neighborhoods and thus a topology. Since subgroups contain the identity by definition, open subgroups are precisely overgroups of the normal subgroups in $\mathcal{N}$. The special case when the elements in $\mathcal{N}$ are all those normal of finite index is called the *profinite topology.* Here, open subgroups are precisely all those subgroups of finite index, since the core of any subgroup is normal and of finite index if the subgroup itself is of finite index. For that, note that if a subgroup H is of finite index, its core H_G is of finite index too since it is precisely the kernel of the action of the left multiplication map over the set of left cosets of H in G.

The following proposition takes account of elemental properties of topological groups.

Proposition 1.1. *Let G be a topological group and H a subgroup of G. Then,*

1. *If H is open, it is closed too.*
2. *If H is closed and of finite index, it is open too.*
3. *If G is compact, H is open if and only if it is closed and of finite index.*

Proof. For the first assertion, note G is a union of cosets of H, then, $G \setminus H$ is a union of cosets which are all open since they are left translations of H. Then, the complementary of H is open too; hence, H is closed. The same argument proves the second assertion where we need finite index since an arbitrary union of closed sets need not be again closed, we need finiteness of the union. Now, the third assertion follows from the definition of compactness and the first two assertions. □

Now, we shall see a little useful lemma to check a group homomorphism is continuous.

Lemma 1.2. *Let $f : G \to H$ be a group homomorphism of topological groups. If $\ker f$ is open in G, then f is continuous.*

Proof. Let U be an open subset of H, and let $V := f^{-1}(U)$. Then, $V = \bigcup f^{-1}(h)$ where h runs over all the elements in U. Thus, it is enough to show each $f^{-1}(h)$ is open. We claim $f^{-1}(h) = \bigcup g \ker f$ where g runs over elements in $f^{-1}(h)$. Then, since the kernel is open, all its cosets are open too and the union of cosets is open too proving the lemma. To prove our claim note for any $g \in f^{-1}(h)$ we have $g \cdot 1 \in g \ker f$. For the reverse inclusion, just note $f(g \ker f) = f(g)f(\ker f) = f(g) = h$. □

If we have now a topological group with respect to the addition, R, which is also a ring for the product and the product is continuous, we say R is a *topological ring.* If R is also a field and the inverse map for the product is continuous over the subspace of units, R is called a *topological field.*

A Hausdorff topological space such that each element possesses a compact neighborhood is called a *locally compact space.* A topological group (field) that is a locally compact space with respect to a nondiscrete topology is called a *locally compact group (field).*

1.2 Profinite groups

Profinite groups arise naturally as Galois groups. In fact, it can be proved all profinite groups can be realized as Galois groups [RZ10]. We showed in the introduction how Galois groups are actually profinite. We define here the notions of inverse and direct limits and profinite groups.

Let $\mathcal{I} = (\mathcal{I}, \preceq)$ be a directed partially ordered set or directed poset, i.e. a partially ordered set such that for each pair $i, j \in \mathcal{I}$, there exists some $k \in \mathcal{I}$ such that $i, j \preceq k$. Let $\{X_i\}_{i\in\mathcal{I}}$ be a collection of objects in a category $\mathcal{C}$ and a collection of morphisms in this category $\varphi_{ij} : X_i \to X_j$ defined whenever $j \preceq i$ making the diagrams

$$\begin{tikzcd}
X_i \arrow[rr, "\varphi_{ik}"] \arrow[dr, "\varphi_{ij}"'] & & X_k \\
& X_j \arrow[ur, "\varphi_{jk}"'] &
\end{tikzcd}$$

commute whenever $k \preceq j \preceq i$ and φ_{ii} is the identity map. Then, $\{X_i, \varphi_{ij}\}_{i,j\in\mathcal{I}}$ is named an *inverse system* over $\mathcal{I}$. Later, we shall restrict out attention to the category of topological groups whose morphisms are continuous group homomorphisms. A *directed* system is the dual notion of the inverse system, so it is obtained by simple reversing of arrows in the definition of an inverse system, i.e. a collection $\{X_i\}_{i\in\mathcal{I}}$ and morphisms $\varphi_{ij} : X_j \to X_i$ whenever $j \preceq i$ making the diagrams

$$\begin{tikzcd}
X_i & & X_k \arrow[ll, "\varphi_{ik}"'] \arrow[dl, "\varphi_{jk}"] \\
& X_j \arrow[ul, "\varphi_{ij}"] &
\end{tikzcd}$$

commute whenever $k \preceq j \preceq i$.

Given an inverse system $\{X_i, \varphi_{ij}\}_{i,j\in\mathcal{I}}$, we define the *inverse limit* $\varprojlim_{i\in\mathcal{I}} X_i = \varprojlim X_i$ as an object X in $\mathcal{C}$ together with morphisms $\varphi_i : X \to X_i$ which are compatible, i.e. $\varphi_j = \varphi_i\varphi_{ij}$, satisfying the universal property:

$$\begin{tikzcd}
Y \arrow[r, dashed, "\psi"] \arrow[dr, "\psi_i"'] & X \arrow[d, "\varphi_i"] \\
& X_i
\end{tikzcd}$$

whenever Y is an object in $\mathcal{C}$ and $\psi_i : Y \to X_i$ is a set of compatible morphisms, then there is a unique morphism $\psi : Y \to X$ such that $\psi_i = \psi\varphi_i$. Intuitively, ψ is determined by looking at each ψ_i and building ψ upon them since they form a *coherent* tuple (at the level of morphisms) $(\psi_i)_{i\in\mathcal{I}}$, i.e. a tuple whose components satisfy the compatibility condition. What is more, we may construct the inverse limit as the closed subset of the cartesian product $\prod_{i\in\mathcal{I}} X_i$ formed by all coherent tuples (at the level of elements), i.e. the tuples $(x_i)_{i\in\mathcal{I}}$ such that $\varphi_{ij}(x_i) = x_j$ whenever $j \preceq i$. It is left to the reader to prove this construction satisfies the universal property of the inverse limit [RZ10]. This reduces many times properties of inverse limits of objects in $\mathcal{C}$ to properties of the objects in $\mathcal{C}$. In particular, if the objects are finite groups, then the resulting inverse limit will behave similarly to a finite group and many properties will be deduced by reducing it to the finite case.

Again, the definition of the direct limit is the dual notion of the inverse limit and it is left to the reader the details of its definition (hint: reverse all arrows in the definition of the inverse limit). Intuitively, the direct limit is a union. In the category of abelian topological groups $X = \varinjlim X_i = \bigcup_i \varphi_i(X)$ and $X = \bigcup_i X_i$ if the projections are onto [RZ10]. In the introduction, we have seen how a field extension may be seen as a direct limit, and we shall see how taking its group of automorphisms dualizes it turning into an inverse limit and finally applying the hom functor gives us a direct limit again. This scheme applies in other situations too and it will be vital for us.

We will be working with finite groups, which can be endowed with the discrete topology to turn them into topological groups. In this context, the inverse limit is compact, Hausdorff and totally disconnected [RZ10] and it is called a *profinite group.*

Given a group G we may define the directed set of normal subgroups $\mathcal{N} := \{N \leq_f G : G/N \text{ finite}\}$. Then, we define the *profinite completion* of G, denoted by $\widehat{G}$ as the inverse limit $\varprojlim G/N$ where N runs over $\mathcal{N}$. Then, G is naturally embedded into its profinite completion by the obvious map $g \mapsto (gN)_N$.

The topological closure of a subgroup of a profinite group can be obtained as follows.

Lemma 1.3. *Let G be a profinite group and H a subgroup of G. Then, the topological closure of H in G can be obtained as*

$$\overline{H} = \bigcap_N HN \cong \varprojlim HN/N,$$

where N runs over all open normal subgroups in G.

We shall see in the next section that we are interested in the open subgroups of the Galois group $\mathrm{Gal}(K^{ab}/K)$. Class field theory will be based upon an easier-to-study group whose profinite completion is precisely this Galois group (up to isomorphism). Then, the following proposition [RZ10] is vital for us to translate the Galois correspondence to this easier-to-study group.

Proposition 1.4. *Let G be a residually finite group, i.e. the intersection of all its normal subgroups of finite index is trivial. Then, there is a 1-to-1 correspondence between the open subgroups in G and the open subgroups in its profinite completion $\widehat{G}$ given by $H \mapsto \overline{H}$ and $K \mapsto K \cap G$ respectively.*

1.3 Infinite Galois correspondence

We state without proof the infinite version of the main theorem of Galois theory [Mor96] even if we just need the assertion on finite extensions.

Theorem 1.5. *Let L/K be an infinite Galois extension and G its Galois group endowed with the Krull topology. Then, there is a one-to-one inclusion reversing correspondence betweeen the closed subgroups of G and the intermediate extensions of L/K. What is more, the intermediate extension E is normal if and only if its corresponding closed subgroup $N := \mathrm{Gal}(L/E)$ is normal in G, in which case $G/N \cong \mathrm{Gal}(E/K)$ as topological groups. Also, if we restrict to finite extensions, this correspondence is one-to-one between finite intermediate extensions and open subgroups of G.*

We shall see the inverse limit $\varprojlim \mathrm{Gal}(E/K)$ is isomorphic to G with the Krull topology as topological groups. Since the natural projections $G \to \mathrm{Gal}(E/K)$ are compatible with the connection homomorphisms for being the usual restrictions as above, by the universal property of the inverse limit, there exists a unique group homomorphism $\Phi : G \to \varprojlim \mathrm{Gal}(E/K)$ compatible with the corresponding projections. By construction, this homomorphism is precisely the one given by $\sigma \mapsto (\sigma_{|E})_E$. We shall see it is an isomorphism. The kernel is trivial since the only automorphism that restricts to the identity in all finite intermediate fields is the identity. For that, recall $L = \varinjlim E = \bigcup_E E$ where E runs through all the finite intermediate extensions in L/K. Then, for each $s \in L$, $s \in E$ for some E and since $\sigma_E(s) = s$ for all E and all $s \in L$, σ is the identity as wanted.

To show it is onto we shall see that each infinite coherent tuple $(\sigma_E)_E$ lifts to an automorphism in $\mathrm{Gal}(L/K)$ where coherence means that for intermediate fields $E \subseteq F$ and a tuple $(\sigma_E)_E$, the component σ_F restricts to σ_E in E. Then, since each $s \in L$ is contained in some finite Galois extension of K, E, we may define the automorphism $\sigma \in G$ as $s \mapsto \sigma(s) := \sigma_E(s)$. It is well defined since if s is in another intermediate Galois extension field F, $\sigma_E(s) = \sigma_F(s)$. To see that[1], note that $K(s) \subseteq E, F$, and for being coherent, the restrictions of σ_E and σ_F to $K(s)$ coincide; thus, their image on s too. Note this automorphism is actually an automorphism and fixes K; thus, $\sigma \in G$. Clearly, all automorphisms in G can be obtained in this fashion, since their restriction to

[1] We could have used EF instead of $K(s)$ too and apply coherence there.

each intermediate finite extension form coherent tuples $(\sigma_E)_E$.

Then, we obtain an isomorphism of groups between G and the inverse limit $\varprojlim \mathrm{Gal}(E/K)$. We need to make it into a homeomorphism. We shall copy the topology in the inverse limit to G through the above isomorphism. We know that a fundamental system of open neighborhoods in $\varprojlim \mathrm{Gal}(E/K)$ is given by the kernels of the projection homomorphisms (Lemma 2.1.1 in [RZ10]). Thus, since these are usual restrictions/projections of G into $\mathrm{Gal}(E/K) \cong G/\mathrm{Gal}(L/E)$ for intermediate finite Galois extension fields E the kernels are precisely the normal subgroups $\mathrm{Gal}(L/E)$. Then, $\{\mathrm{Gal}(L/E)\}_E$ forms a fundamental system of open neighborhoods in G, which is precisely the way we defined the Krull topology.

1.4 Character groups and Pontrjagin's duality

The *character group* or *dual* of a topological group, G^*, is the group of continuous group homomorphisms from G to $\mathbb{T}$, i.e. $G^* = \hom_{\text{cont}}(G, \mathbb{T})$, where $\mathbb{T}$ is the multiplicative subgroup of complex numbers of unit norm.

We will be dealing with character groups throughout the proof of local class field theory. Then, we shall fix some special notation and show a couple of results. For a field K we denote the character group of $\mathrm{Gal}(K^{ab}/K)$ by $X(K)$. Since we restrict to continuous homomorphisms, we see that the preimage of any atom in $\mathbb{T}$ is open, since $\mathbb{T}$ is given the discrete topology. But open in compact topological groups implies finite index. In particular, the kernel is of finite index, i.e. the image of the given homomorphism is of finite order. Thus, the image groups of these homomorphisms are mapped to $\mathbb{Q}/\mathbb{Z}$ via the usual isomorphism $e^{2\pi ix} \mapsto x + \mathbb{Z}$. Then, for a profinite group $G^* = \hom_{\text{cont}}(G, \mathbb{Q}/\mathbb{Z})$. Also, if we define addition of homomorphisms via addition of their images, $X(K)$ can be seen as an additive group and since for a homomorphism φ, $o(\varphi) = \mathrm{lcm}(o(\varphi(g)))_{g\in G}$, the additive order of any homomorphism is finite and $X(K)$ is torsion.

All characters of an abelian profinite group arise as charactes of a finite abelian group. Note that for any $\chi \in G^*$, $\ker \chi$ is normal in G and open too for being the preimage of 0 and $\mathbb{Q}/\mathbb{Z}$ being discrete. Then, we can regard χ as the natural composition $G \to G/\ker \chi \to \mathbb{Q}/\mathbb{Z}$.

A useful property of characters is that given a group homomorphism $\varphi : G \to H$ where H is abelian and finite, it will be onto if and only if the only character annihilating the image of φ is the trivial character, i.e. if $\mathrm{Ann}_{H^*}(\varphi(G)) = 0$. Note the only if part is trivial. For the if part assume by contradiction that there exists an element $h \in H$ such that $h \notin \mathrm{Im}\ \chi$. We shall find a nontrivial character $\chi \in H^*$ such that $\chi(\varphi(G))$=0. For that consider the non-trivial but finite quotient $H/\varphi(G)$. Since the quotient is finite and abelian, $\bigcap_{\chi\in(H/\varphi(G))^*} \ker \chi = 0$, there is at least one character χ in $(H/\varphi(G))^*$ which is non-trivial and we may lift it to a character in of H by $\chi' := \pi\chi$, getting a non trivial character of H annhilating the image of G by φ, arriving to a contradiction and proving the desired property.

Putting everything together, let L/K be an infinite Galois extension. Let us recall the definition of the set $\mathcal{L}$ and how natural it is to construct the direct limit of this direct system, $\varinjlim E = \bigcup E = L$, which is no more than the infinite Galois extension L. Now, we shall consider the Galois groups of each finite Galois extension of K in $\mathcal{L}$. These groups $\mathrm{Gal}(E/K)$ together with the usual restrictions $\varphi_{EF} : \mathrm{Gal}(F/K) \to \mathrm{Gal}(E/K)$ give us the data of an inverse system over the same directed poset $\mathcal{L}$. Now, it is natural again to consider the inverse limit $\varprojlim \mathrm{Gal}(E/K) \cong \mathrm{Gal}(L/K)$. Note that Galois correspondence being inclusion reversing turns inclusions into restrictions, dualizing the construction, turning a direct limit into an inverse limit. This had been shown so far in our discussion.

Now, consider the dual of each finite Galois group, i.e. the homomorphisms from $\mathrm{Gal}(E/K)$ to $\mathbb{Q}/\mathbb{Z}$. Note that a character $\chi_E : \mathrm{Gal}(E/K) \to \mathbb{Q}/\mathbb{Z}$ lifts to a character $\chi_F : \mathrm{Gal}(F/K) \to \mathbb{Q}/\mathbb{Z}$ whenever $E \subseteq F$ and $\chi_F(\sigma) := \chi_E(\sigma_{|E})$ for each $\sigma \in \mathrm{Gal}(F/K)$. Intuitively, we are plugging the bigger group $\mathrm{Gal}(F/K)$ in the left via a restriction. This allows us to lift the characters of the smaller group $\mathrm{Gal}(E/K)$ to the bigger group $\mathrm{Gal}(F/K)$. This gives us the data for a direct system over the same directed poset $\mathcal{L}$. Naturally, we build the direct limit $\varinjlim \mathrm{Gal}(E/K)^* \cong \mathrm{Gal}(L/K)^*$. To obtain that isomorphism, recall the image of each character is finite. Hence, any character can be obtained in this lifting fashion. To see that, note this kernel is a subgroup of the form $\mathrm{Gal}(L/E)$ where E is a finite Galois extension of K for the kernel being open. Then, this character can be obtained from a character of the finite Galois group $\mathrm{Gal}(E/K)$ by plugging in the left $\mathrm{Gal}(L/K)$ through the usual restriction. Then the isomorphism follows from the universal property of the direct limit, since the liftings are compatible with the connection homomorphisms as they are also usual inclusions.

Lastly, we want to build the bidual $\mathrm{Gal}(L/K)^{**}$. For that, consider the bidual of each finite Galois group, $\mathrm{Gal}(E/K)^{**}$. These form an inverse system over the same directed poset $\mathcal{L}$. Just note a character $\chi_E : \mathrm{Gal}(E/K)^* \to \mathbb{Q}/\mathbb{Z}$ restricts to a character $\chi_F : \mathrm{Gal}(F/K)^* \to \mathbb{Q}/\mathbb{Z}$ since the bidual of a finite group is known to be isomorphic to the original finite group through the evaluation homomorphism and we may define this restriction through these isomorphisms and the usual restriction in the Galois groups. Then, we consider the inverse limit $\varprojlim \operatorname{Gal}(E/K)^{**} \cong \operatorname{Gal}(L/K)^{**}$. Note these evaluation isomorphisms are compatible with the restrictions by definition; thus, we obtain the evaluation isomorphism of inverse limits $\operatorname{Gal}(L/K)^{**} \cong \varprojlim \operatorname{Gal}(E/K)^{**} \cong \varprojlim \operatorname{Gal}(E/K) \cong \operatorname{Gal}(L/K)$. This is known with more generality for profinite groups as Pontrjagin's duality and even in more generality for locally compact abelian groups.

Theorem 1.6 (Pontrjagin's duality). *Given a locally compact abelian group G and its character group G^*, the character group of G^* and the group G are naturally isomorphic, where this isomorphism is given by the evaluation map.*

The interested reader is advised to check [Pon46] for a full proof of Pontrjagin's duality for locally compact abelian groups and [RZ10] for profinite groups.

Remark. The reader may be wondering why we are using restrictions instead of liftings when considering the Galois groups. In the case of characters we are able to do these liftings because we are considering just homomorphisms, not automorphisms. If we try to lift an automorphism in this fashion it will have a non-trivial kernel and thus it will not be injective, it will not be even a homomorphism since field homomorphisms are injective. This shows why in this case it is natural to consider restrictions and therefore the inverse limit whilst with characters it is more natural to lift them and consider the direct limit.

Let us analyze the case $K = \mathbb{F}_q$. Then, all finite intermediate fields are known to us to be cyclic and we have a more precise description of $\mathcal{L} = \{\mathbb{F}_{q^n} : n \in \mathbb{N}\}$. Then, $\mathbb{F}_q^{ab} = \mathbb{F}_q^{sep} = \varinjlim \mathbb{F}_{q^n} = \bigcup \mathbb{F}_{q^n}$ and the Galois group $\operatorname{Gal}(\mathbb{F}_q^{ab}/\mathbb{F}_q) \cong \varprojlim \operatorname{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$. Finally, since $\mathbb{Q}/\mathbb{Z}$ is discrete and each finite group in $\mathcal{L}$ is discrete, to know all continuous homomorphisms $\operatorname{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \to \mathbb{Q}/\mathbb{Z}$ is just to know all such group homomorphisms. For being the base group finite and cyclic, it is enough to provide the image of the Frobenius automorphism, and choose it to be an element in $\mathbb{Q}/\mathbb{Z}$ of order divisor the order of the group, i.e. any element in $\langle 1/n + \mathbb{Z}\rangle$ where n is this order. Then, $X(\mathbb{F}_q) \cong \varinjlim \operatorname{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)^* \cong \varinjlim \langle 1/n + \mathbb{Z}\rangle = \bigcup \langle 1/n + \mathbb{Z}\rangle = \mathbb{Q}/\mathbb{Z}$. Thus, $X(\mathbb{F}_q) \cong \mathbb{Q}/\mathbb{Z}$ where this isomorphism is given by $\chi = \chi_n \mapsto k/n + \mathbb{Z}$, where k/n is the image of the nth Frobenius automorphism under $\chi_n = \pi_n \chi$. In other words, this isomorphism is obtained mapping each character χ to its image in the Frobenius automorphism of $\operatorname{Gal}(\mathbb{F}_q^{ab}/\mathbb{F}_q)$. Note this argument is valid for any finite field, in particular for $\mathbb{F}_{q^f}$. Then, $X(\mathbb{F}_q) \cong X(\mathbb{F}_{q^f})$. But we know explicitly a very natural homomorphism between these two character groups (which is not an isomorphism, caution!). Since the Galois groups $\operatorname{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ are cyclic, whenever f divides n there is a unique subgroup of index f, namely $\operatorname{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_{q^f})$. What is more, an fth power of a Frobenius automorphism in $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is a Frobenius automorphism in $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_{q^f})$. Thus, given a homomorphism $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \to \mathbb{Q}/\mathbb{Z}$, $\sigma \mapsto k/n + \mathbb{Z}$ we obtain a homomorphism $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_{q^f})$ by the multiplication-by-f map in $\mathbb{Q}/\mathbb{Z}$ and the usual power-by-f map in the Galois groups, $\sigma \mapsto fk/n + \mathbb{Z}$

$$\begin{tikzcd}
\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \arrow[r] \arrow[d, "\text{restriction}"'] & \mathbb{Q}/\mathbb{Z} \arrow[d, "\text{multiplication by } f"] \\
\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_{q^f}) \arrow[r] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

whenever n divides f. Multiplication-by-f is an epimorphism in each term of the directed set, and if we consider the character groups and the natural isomorphisms mapping a character to its image in the corresponding Frobenius automorphisms, we get the following commutative diagram which we shall use in the proof of local class field theory.

Lemma 1.7. *The diagram*

$$\begin{tikzcd}
X(\mathbb{F}_q) \arrow[r] \arrow[d, "\text{restriction}"'] & \mathbb{Q}/\mathbb{Z} \arrow[d, "\text{multiplication by } f"] \\
X(\mathbb{F}_{q^f}) \arrow[r] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

is commutative.

Chapter 2

Global and Local Fields

The first example of a field seen in an elementary algebra course is usually the field of rational numbers, $\mathbb{Q}$. Finite extensions of $\mathbb{Q}$ are called *number fields*, and they are the main object of study in algebraic number theory. Along with number fields (and finite fields), function fields are the best known examples of fields. Of special interest in algebraic geometry are finite extensions of $\mathbb{F}_q(T)$, where $\mathbb{F}_q(T)$ is the field of rational functions in one variable with coefficients in $\mathbb{F}_q$. We call the latter fields *global function fields.* These two types of fields may look rather different at first glance, but they share many properties. This analogy between both of them motivates the definition of a *global field* as either a number field or a global function field. Pursuing these analogies has been shown fruitful for both algebraic geometry and number theory. In this chapter we develop the basic theory of both global and local fields that is used in subsequent chapters.

We will use the following equivalent [Mil17] definitions of a Dedekind domain throughout the chapter.

Definition 2.1 (Dedekind domain). An integral domain A is said to be a Dedekind domain if it is a field or any of the following equivalent conditions is satisfied.

1. Any proper ideal $\mathfrak{a}$ in A factors uniquely into a product of prime ideals.
2. A is noetherian, integrally closed and every nonzero prime ideal is maximal.

2.1 Discrete valuations

Definition 2.2 (Discrete valuation). Let K be a field. Let $\nu : K^\times \to \mathbb{Z}$ be a non-trivial surjective group homomorphism satisfying the additional condition

$$\text{(i)}\ \ \nu(a+b) \geq \min(\nu(a), \nu(b)), \quad \forall a, b \in K^\times,$$

and set $\nu(0) = \infty$ to extend ν to the entire field K. Then, ν is said to be a *discrete valuation* of K. A field with a discrete valuation is called a *discrete valuation field.*

The first example of a discrete valuation of a field is the map $\mathrm{ord}_p : \mathbb{Q}^\times \to \mathbb{Z}$ defined as follows for a rational prime p. For any rational number a, let us write it as an irreducible fraction in the form

$$a = p^n \frac{a_0}{a_1}, \quad n \in \mathbb{Z} \text{ and } p \nmid a_0, a_1.$$

We define $\mathrm{ord}_p(a) = n$ and set $\mathrm{ord}_p(0) = \infty$. It is easy to check that ord_p is a discrete valuation of $\mathbb{Q}$. This map is called the *p-adic valuation.*

Similarly, for a Dedekind domain A and its field of fractions K, we define the $\mathfrak{p}$*-adic valuation*, $\mathrm{ord}_{\mathfrak{p}} : K^\times \to \mathbb{Z}$ for a nonzero prime ideal $\mathfrak{p}$ of A, by writing the fractional ideal (a) for any $a \in K^\times$ as the unique product of prime ideals $(a) = \mathfrak{p}^n \prod \mathfrak{q}_i^{n_i}$ with $n, n_i \in \mathbb{Z}$ and $\mathfrak{q}_i \neq \mathfrak{p}$ for all i, and defining $\mathrm{ord}_{\mathfrak{p}}(a) = n$. Note that we set $\mathrm{ord}_{\mathfrak{p}}(0) = \infty$ as before.

Let K be a discrete valuation field for ν. Then, it is immediate from the definition of a discrete valuation that the set $\mathcal{O}_\nu = \{a \in K : \nu(a) \geq 0\}$ forms a subring of K and it is called the *valuation ring* of K.

Proposition 2.3. *Let K be a field and ν a valuation of K.*

(i) Let $\mathcal{O}_\nu$ be the valuation ring of K with respect to ν. Then, $\mathcal{O}_\nu$ is a principal ideal domain and thus a Dedekind domain. The only nonzero prime (and maximal) ideal of $\mathcal{O}_\nu$ is

$$\mathfrak{p} = \{a \in K : \nu(a) \geq 1\},$$

and ν coincides with $\mathrm{ord}_{\mathfrak{p}}$. Any element a in K such that $\nu(a) = 1$ generates $\mathfrak{p}$; any ideal of $\mathcal{O}_\nu$ is of the form $(a^n) = \{b \in K : \nu(b) \geq n\}$ for such an element a and $n \in \mathbb{N}$, and any fractional ideal of $\mathcal{O}_\nu$ of the form $(a^n) = \{b \in K : \nu(b) \geq n\}$ for same a and $n \in \mathbb{Z}$. The group of units of $\mathcal{O}_\nu$ is exactly the set of the elements with null valuation, i.e. $\mathcal{O}_\nu^\times = \{a \in K : \nu(a) = 0\}$.

(ii) Conversely, let A be a Dedekind domain with a unique non-zero prime ideal $\mathfrak{p}$. Then, A coincides with the valuation ring for the discrete valuation $\mathrm{ord}_{\mathfrak{p}}$.

(iii) Given an integral domain A, the following conditions are all equivalent.

(a) A is the valuation ring of a discrete valuation of its field of fractions.

(b) A is a principal ideal domain with a unique nonzero prime ideal.

(c) A is a Dedekind domain with a unique nonzero prime ideal.

An integral domain A satisfying any of the last three equivalent conditions is called a discrete valuation ring*.*

Proof. First note that an element $c \in \mathcal{O}_\nu$ of null valuation is a unit in the valuation ring since $1 = cc^{-1}$ in K implies taking valuations, $0 = \nu(c) + \nu(c^{-1})$; thus, $\nu(c^{-1}) = 0$ and $c \in \mathcal{O}_\nu^\times$. Similarly, if $c \in \mathcal{O}_\nu^\times$, then $\nu(c) = 0$. Let a be an element of K such that $\nu(a) = 1$. Now fix a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_\nu$. Let $n = \min\{\nu(b) : b \in \mathfrak{a}\}$. Then, by the definition of an ideal, $\mathfrak{a} \subseteq \mathfrak{b} := \{b \in K : \nu(b) \geq n\} \supseteq (a^n)$. To prove these inclusions are actually equalities, let first $b \in \mathfrak{b}$. Then, $b = a^n c$ where $c = a^{-n} b \in K$. Taking valuations, $\nu(c) = \nu(a^{-n}) + \nu(b) \geq 0$. Thus, $c \in \mathcal{O}_\nu$ proving $b \in (a^n)$. Let now $b \in \mathfrak{a}$ such that $\nu(b) = n$. Then, $b = a^n c$ for some $c \in K$ and taking valuations, $\nu(b) = \nu(c) + \nu(a^n)$. Thus, $\nu(c) = 0$ and $c \in \mathcal{O}_\nu^\times$, so $a^n = c^{-1} b \in \mathfrak{a}$ getting both equalities. The other asssertions in (i) are straightforward to check now.

For (ii) just note A is trivially contained in the valuation ring. For the reverse inclusion note that for an element $a \in \mathcal{O}_{\mathrm{ord}_\mathfrak{p}}$, $(a) = \mathfrak{p}^n$ with $n \geq 0$; thus, $a \in A$.

Now, (iii) follows from (i) and (ii). □

A generator π of the unique maximal ideal $\mathfrak{p}$ of a discrete valuation ring is called a *uniformizer* or a *prime element* of $\mathcal{O}_\nu$ or K. The natural quotient field $\mathcal{O}_\nu/\mathfrak{p}$ is called the *residue field of* $\mathcal{O}_\nu$.

We shall see how prime ideals origin embeddings of global fields into what we call *local fields*. For that, we need to attach a special topology to these fields.

2.2 Completion and local fields

From a discrete valuation ν, we can obtain a metric. Let c be a real number such that $1 < c < \infty$. Then, it is easily checked that the map $d_\nu : K \times K \to \mathbb{R}$ defined as $d_\nu(x, y) := c^{-\nu(x-y)}$ for $x \neq y$ and $d_\nu(x, y) := 0$ for $x = y$, defines a metric in K. This metric induces a Hausdorff topology where $V_{n,a} = \{b \in K : \nu(b - a) \geq n\}$ can be taken as a fundamental system of open (and closed) neighborhoods for each point a in K.

As with respect to the usual metric in $\mathbb{Q}$, a Cauchy sequence in K with respect to d_ν may not converge in K. Thus, we may complete K with respect to this metric to make all Cauchy sequences converge.

LEMMA 2.4. *Let A be the set of all Cauchy sequences in K. Then, A is a ring with respect to componentwise addition and multiplication. The set of all Cauchy sequences convergent to 0 form a maximal ideal of A, $\mathfrak{m}$. The field $A/\mathfrak{m}$ is a discrete valuation field with discrete valuation $\hat{\nu}$ defined as $\hat{\nu}((a_n) + \mathfrak{m}) = \lim \nu(a_n)$.*

PROOF. Proving A is a ring is straightforward; thus, it is left to the reader. To prove $\mathfrak{m}$ is maximal, let $\mathfrak{m}'$ be an ideal strictly containing $\mathfrak{m}$. We shall prove $\mathfrak{m}' = A$. Take a Cauchy sequence (a_n) in $\mathfrak{m}' \setminus \mathfrak{m}$. Then, there exists a positive integer n_0 such that $a_n \neq 0$ for $n \geq n_0$. Let (b_n) be a sequence such that for $n \geq n_0$, $b_n = a_n^{-1}$. Then, (b_n) is clearly Cauchy and $(a_n)(b_n) + \mathfrak{m} = (1) + \mathfrak{m}$. Thus, since $\mathfrak{m}'$ is an ideal, (1) is in $\mathfrak{m}'$ and $\mathfrak{m}' = A$ as wanted. The fact $\hat{\nu}$ is a discrete valuation for $A/\mathfrak{m}$ follows now from the properties of the usual limit. □

A discrete valuation field K is called a *complete discrete valuation field* if every Cauchy sequence in K converges in K. A discrete valuation field $\hat{K}$ with valuation $\hat{\nu}$ is called a *completion* of K if it is complete, $\hat{\nu}_{|K} = \nu$ and K is a dense subfield of $\hat{K}$ with respect to d_ν. This completion is unique up to isomorphism.

PROPOSITION 2.5. *Every discrete valuation field K has a unique completion up to K-isomorphism.*

PROOF. We shall prove that the field $A/\mathfrak{m}$ in previous lemma is the unique completion of K. For that, first note that K is embedded in $A/\mathfrak{m}$ by the natural map $a \to (a) + \mathfrak{m}$. Now, for a Cauchy sequence (a_n) in K and any real number M, there exists a positive integer n_0 such that for $m, n \geq n_0$, $\nu(a_m - a_n) \geq M$. Thus, if we take (a_{n_0}) which clearly converges in K, we get $\hat{\nu}((a_{n_0}) - (a_n)) \geq M$, proving that K is dense in $A/\mathfrak{m}$. To prove completeness, let $((a_n^{(m)})_n)_m$ be a Cauchy sequence in $A/\mathfrak{m}$ (with respect to $d_{\hat{\nu}}$). Let $n_1, n_2, \ldots$ be an increasing sequence of positive integers such that for $i, j \geq n_m$, $\hat{\nu}(a_i^{(m)} - a_j^{(m)}) \geq M$. Then, $(a_{n_m}^{(m)})_m$ is a Cauchy sequence in K and the limit of $((a_n^{(m)})_n)_m$ in $A/\mathfrak{m}$ (with respect to $d_{\hat{\nu}}$). This proves $A/\mathfrak{m}$ is a completion of K.

For uniqueness, assume $(\hat{K}_1, \hat{\nu}_1)$ and $(\hat{K}_2, \hat{\nu}_2)$ to be two completions of K. Let 1_K be the identity map in K. Then, we extend this isomorphism by continuity from K, as a dense subfield of $\hat{K}_1$, to $\hat{K}_1$. This means, for an element $a \in \hat{K}_1$, we take a Cauchy sequence (a_n) in K such as $\lim_1 a_n = a$ and we map it to $b = \lim_2 a_n \in \hat{K}_2$. This map is well defined. For that note that if we consider two distinct Cauchy sequences converging to a, (a_n) and (a'_n), by completeness of $\hat{K}_2$, they must converge and since $(a_n - a'_n)$ converges to 0, its image too and this limit is unique. What is more; thus, $b = \lim_2 a_n = \lim_2 a'_n$. It is straightforward to check now that the extension $\hat{1}_K : \hat{K}_1 \to \hat{K}_2$ is a field isomorphism and $\hat{\nu}_1 = \hat{\nu}_2 \circ \hat{1}_K$. □

From this proposition and the construction of $A/\mathfrak{m}$ it follows immediately.

Corollary 2.6. *Let K be a discrete valuation field and $\hat{K}$ its completion. Then, $\mathcal{O}_\nu$ is dense in $\mathcal{O}_{\hat{\nu}}$, the unique prime ideal $\mathfrak{p}$ is dense in $\hat{\mathfrak{p}}$ and residue fields $\mathcal{O}_\nu/\mathfrak{p}$ and $\mathcal{O}_{\hat{\nu}}/\hat{\mathfrak{p}}$ are equal up to isomorphism.*

Given a global field K and a discrete valuation $\nu := \mathrm{ord}_\mathfrak{p}$ for a non-zero prime $\mathfrak{p}$ in the ring of integers of K we define the *local field K_ν* as the completion of K with respect to ν ($\mathbb{R}$ and $\mathbb{C}$ are also considered as local fields, but they can be dealt with separately).

Lemma 2.7. *Let K be a global field and ν a discrete valuation. Then, $\mathcal{O}_{\hat{\nu}}$ is compact and the residue field $\mathcal{O}_{\hat{\nu}}/\hat{\mathfrak{p}}$ is finite. Thus, the local field K_ν is a complete valuation field whose residue field is finite.*

Proof. By Problem A.2 it is known $\mathcal{O}_{\hat{\nu}} \cong \varprojlim_n \mathcal{O}_{\hat{\nu}}/\hat{\mathfrak{p}}^n$ as topological rings; thus, compactness follows. From Problem A.3, $\hat{\mathfrak{p}}^n/\hat{\mathfrak{p}}^{n+1} \cong \mathcal{O}_{\hat{\nu}}/\hat{\mathfrak{p}}$; thus, since K is a global field, its residue field is finite (see Problem A.4) and it follows from the third isomorphism theorem and Corollary 2.6 that all the rings $\mathcal{O}_{\hat{\nu}}/\hat{\mathfrak{p}}^n$ are finite, just note $(\mathcal{O}_{\hat{\nu}}/\hat{\mathfrak{p}}^{n+1})/(\hat{\mathfrak{p}}^n/\hat{\mathfrak{p}}^{n+1}) \cong \mathcal{O}_{\hat{\nu}}/\hat{\mathfrak{p}}^n$ and take orders. □

In the literature, some authors prefer to define local fields as complete valuation rings with finite residue field which by previous lemma and its converse [Neu99] is an equivalent definition. Local fields are locally compact.

Proposition 2.8. *Let K be a global field and ν a discrete valuation of K. The local field K_ν is locally compact.*

Proof. We shall see $a + \mathcal{O}_{\hat{\nu}}$ is a compact neighborhood of a for each $a \in K_\nu$. Recall that the left translation map $l_b(x) = b + x$ is an homeomorphism of the topological group $(K_\nu, +)$; thus, it is enough to prove $\mathcal{O}_\nu$ is an open neighborhood of 0 since compactness is known. For that, note that by definition $\mathcal{O}_\nu$ is the open ball of radius c centered at 0; hence open by definition. □

2.3 Prime ideals in finite extensions of global and local fields

For this section, let A be a Dedekind domain, K its field of fractions, L a separable extension of K and B the integral closure of A in L. A basic result on Dedekind domains shows B is a Dedekind domain too[1]. What is more, B

[1] This is true for a general finite extension, separability need not be assumed.

is a finitely generated torsion-free A-module.

Now, let $\mathfrak{q}$ be a prime ideal of B. Let $\mathfrak{p} = \mathfrak{q} \cap A$. Then, $\mathfrak{p}$ can be shown to be a prime ideal of A (checking this is straightforward and it is left to the reader). In this situation we say $\mathfrak{q}$ *lies above* $\mathfrak{p}$ or $\mathfrak{p}$ *lies below* $\mathfrak{q}$. Let $\mathfrak{p}$ be a prime ideal of A. Then, the ideal it generates in B decomposes as a finite product of distinct prime ideals over B as $\mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}$, where the positive integers e_i are called the *ramification indices of* $\mathfrak{q}_i$ *over* $\mathfrak{p}$ and denoted by $e(\mathfrak{p}, \mathfrak{q}_i)$. Then, $\{\mathfrak{q}_i\}$ coincides with the set of primes lying above $\mathfrak{p}$.

The residue field $A/\mathfrak{p}$ is embedded naturally into $B/\mathfrak{q}_i$; hence, $B/\mathfrak{q}_i$ may be regarded as a field extension of $A/\mathfrak{p}$. Since B is a finitely generated A-module, it is a finite extension. The degree of the extension $[B/\mathfrak{q}_i : A/\mathfrak{p}]$ is called the *residue degree of* $\mathfrak{q}_\mathrm{i}$ *over* $\mathfrak{p}$ and denoted by $f(\mathfrak{p}, \mathfrak{q}_i)$. We say $\mathfrak{p}$ is *totally decomposed* in L if $g = [L : K]$. If $e(\mathfrak{p}, \mathfrak{q}_i) = 1$ and $B/\mathfrak{q}_i$ is a separable extension of $A/\mathfrak{p}$, we say $\mathfrak{q}_i$ is *unramified* over K. We say $\mathfrak{p}$ is *unramified* in L if all primes lying above $\mathfrak{p}$ are unramified over K. Otherwise, $\mathfrak{p}$ is said to be *ramified.* Lastly, note that the completion of L at $\mathfrak{q}_i$ can be regarded as a field extension of $K_\mathfrak{p}$ by noting that coherent tuples in K modulo $\mathfrak{p}$ can be regarded as coherent tuples in L modulo $\mathfrak{q}$.

The following proposition shows a basic relation of these concepts which is known from algebraic number theory; thus, we omit its proof.

Proposition 2.9. *Let L/K be a finite field extension. Then,*

$$[L : K] = \sum_{j=1}^{g} e(\mathfrak{p}, \mathfrak{q}_\mathrm{j}) f(\mathfrak{p}, \mathfrak{q}_j).$$

When the underlying field is a local field we have a simple description of prime ideals on its finite extensions.

We shall prove that if A is a complete discrete valuation ring, then B is so. First, recall a result from commutative algebra.

Lemma 2.10. *Let R be a commutative ring and let I, J be ideals of R satisfying $I + J = R$. Then, $IJ = I \cap J$ and the natural map $R/IJ \to (R/I) \times (R/J)$ is an isomorphism.*

Note the isomorphism in this lemma is a diagonal isomorphism, which we should keep in mind for the following results. Now, recall non-zero prime ideals in a Dedekind domain are maximal.

Corollary 2.11. *Let R be a Dedekind Domain and let $\mathfrak{q}_\mathfrak{i}$ be distinct nonzero prime ideals of R for $i = 1, \ldots, g$. Let $n_i \geq 1$ for $i = 1, \ldots, g$. Then,*

$$\frac{R}{\mathfrak{q}_1^{n_1} \cdots \mathfrak{q}_g^{n_g}} \cong \prod_{i=1}^{g} R/\mathfrak{q}_i^{n_i}.$$

Now, if we set $R = B$ and $\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g}$ with $e_i \geq 1$, by the previous corollary, we get the isomorphism,

$$B/\mathfrak{p}^n B = \frac{B}{\mathfrak{q}_1^{e_1 n} \cdots \mathfrak{q}_g^{e_g n}} \cong \prod_{i=1}^{g} B/\mathfrak{q}_i^{e_i n}.$$

Since the isomorphisms are compatible with the reductions modulo the prime ideals, passing to the inverse limit, we obtain the following result.

Corollary 2.12. *In the above situation, we get the isomorphism $\varprojlim_n B/\mathfrak{p}^n B \cong \prod_{i=1}^{g} \mathcal{O}_{\mathfrak{q}_i}$.*

Note all previous isomorphisms are diagonal. We now prove some technical results needed to show B is again a complete discrete valuation ring.

Lemma 2.13. *Let $\alpha_1, \ldots, \alpha_n$ be a K-basis of L. Then, $\alpha_1, \ldots, \alpha_n$ form a $K_\mathfrak{p}$-basis of $\prod_{i=1}^{g} L_{\mathfrak{q}_i}$. Here, each α_i is regarded as an element of $\prod_{i=1}^{g} L_{\mathfrak{q}_i}$ through a diagonal embedding $L \hookrightarrow \prod_{i=1}^{g} L_{\mathfrak{q}_i}$.*

Proof. We shall construct an explicit isomorphism $K_\mathfrak{p}^{\oplus n} \cong \prod_{i=1}^{g} L_{\mathfrak{q}_i}$. Note B is a finitely generated A-module. Thus, we can find nonzero elements $a, b \in A$ such that $aB \subseteq A\alpha_1 + \cdots + A\alpha_n$ and $b(A\alpha_1 + \cdots + A\alpha_n) \subseteq B$. Note a can be taken as the product of all the denominators of the coefficients of the generators of B in terms of the basis $\alpha_1, \ldots, \alpha_n$. Also, b can be taken to be the product of all denominators of the α_i when they are written in the form b_i/a_i with $b_i \in B$ and $a_i \in A$. For that, note any $u \in L$ satisfies an equation $a_n u^n + \cdots + a_1 u + a_0 = 0$ with all $a_i \in A$. Then, multiplying by a_n^{n-1} we obtain the expression $(a_n u)^n + \cdots + a_1 a_n^{n-2}(a_n u)$=0, i.e. $a_n u \in B$. Thus, $a_n u = b$ for some b in B and any element in L can be written as a quotient b/a with $b \in B$ and $a \in A$. Now, by the universal property of free modules, we define the isomorphism,

$$\begin{aligned} \iota : A^{\oplus n} &\to A\alpha_1 + \cdots + A\alpha_n \\ (x_i) &\mapsto \sum x_i \alpha_i. \end{aligned}$$

Now we define the maps $s : B \to A^{\oplus n}$ and $t : A^{\oplus n} \to B$ as the compositions $s = l_a \iota^{-1}$ and $t = \iota l_b$, where l_a and l_b are left multiplication maps by a and b respectively. Note $st = ts = l_{ab}$, where l_{ab} is multiplication by ab in the appropiate context, i.e. usual multiplication by ab when in B and the product by ab componentwise in $A^{\oplus n}$. Now, passing to the inverse limit (with respect to the ideals $\mathfrak{p}^n$) and applying Corollary 2.12, s and t induce the following homomorphisms of $\mathcal{O}_\mathfrak{p}$-modules,

$$\hat{s} : \prod_{i=1}^{g} \mathcal{O}_{\mathfrak{q}_i} \to \mathcal{O}_\mathfrak{p}^{\oplus n}, \quad \hat{t} : \mathcal{O}_\mathfrak{p}^{\oplus n} \to \prod_{i=1}^{g} \mathcal{O}_{\mathfrak{q}_i}, \tag{2.1}$$

where $\hat{s}\hat{t} = \hat{t}\hat{s} = l_{ab}$ again, understood componentwise again. By a little abuse of notation we shall denote by $\hat{s} : \prod_{i=1}^{g} L_{\mathfrak{q}_i} \to K_\mathfrak{p}^{\oplus n}$ and $\hat{t} : K_\mathfrak{p}^{\oplus n} \to \prod_{i=1}^{g} L_{\mathfrak{q}_\mathfrak{i}}$ the homomorphisms induced in the respective fields of fractions. Note here $\hat{s}\hat{t} = \hat{t}\hat{s} = l_{ab}$ happens too in the exact same sense as before. Now, the homomorphism $\varphi : K_\mathfrak{p}^{\oplus n} \to \prod_{i=1}^{g} L_{\mathfrak{q}_i}$ given by $(x_i) \mapsto \sum x_i \alpha_i$, coincides with $l_{b^{-1}}\hat{t}$, whose inverse is given by $l_{a^{-1}}\hat{s}$. Thus, φ is an isomorphism as wanted. □

Remark. When we introduce the tensor product in Chapter 3, we could state this lemma in the form $K_\mathfrak{p} \otimes_K L \cong \prod_{i=1}^{g} L_{\mathfrak{q}_i}$.

Proposition 2.14. *Let $\mathfrak{p}$ be a non-zero prime ideal of A and $\mathfrak{q}_1, \dots, \mathfrak{q}_g$ all the prime ideals of B lying above $\mathfrak{p}$. Let α be such that $L = K(\alpha)$ and let f be the minimal polynomial of α over K. Let $f = \prod_{i=1}^{h} f_i$ be the factorization into irreducible polynomials over $K_\mathfrak{p}$ and α_i a root of f_i. Then, $h = g$. We obtain the field isomorphisms, $\frac{K_\mathfrak{p}[t]}{(f_i)} \cong L_{\mathfrak{q}_i}$, via the assignments $t \mapsto \alpha_i$ for $i = 1, \dots, g$.*

Proof. By the universal property of $K_\mathfrak{p}$-algebras, we define the diagonal homomorphism $K_\mathfrak{p}[t] \to \prod L_{\mathfrak{q}_i}$, $t \mapsto (\alpha)$. This is onto for $1, \dots, \alpha^{n-1}$ being a basis and applying previous lemma. Note $f(\alpha) = 0$; hence, (f) is in the kernel, and the equality follows from dimension counting. Thus, $\frac{K_\mathfrak{p}[t]}{(f)} \cong \prod_{i=1}^{g} L_{\mathfrak{q}_i}$ via this diagonal embedding. What is more, by Corollary 2.11, we have the diagonal isomorphism, $\frac{K_\mathfrak{p}[t]}{(f)} \cong \prod_{i=1}^{h} K_\mathfrak{p}[t]/(f_i)$. Now, each $K_\mathfrak{p}[t]/(f_i)$ can be regarded as a subfield of $\prod_{i=1}^{g} L_{\mathfrak{q}_i}$ via the usual embedding $K_\mathfrak{p}[t]/(f_i) \to K_\mathfrak{p}[t]/(f) \overset{\cong}{\to} \prod L_{\mathfrak{q}_i}$, $t \mapsto t \mapsto (\alpha_i)$ for a root α_i of f_i. If we compose it with the projection into a field $L_{\mathfrak{q}_i}$, it is a field homomorphism since it maps 1 to 1. Then, each $K_\mathfrak{p}[t]/(f_i)$ must be isomorphic to a subfield of one of the $L_{\mathfrak{q}_i}$. By dimension counting and the isomorphisms seen beforehand, $h = g$ and the isomorphisms in the assertion follow. □

Proposition 2.15. *Let $\mathfrak{p}$ be a nonzero prime ideal of A and $\mathfrak{q}$ a prime ideal of B lying above $\mathfrak{p}$. Then,*

1. *The valuation ring $\mathcal{O}_\mathfrak{q}$ of $L_\mathfrak{q}$ coincides with the integral closure of the valuation ring $\mathcal{O}_\mathfrak{p}$ of $K_\mathfrak{p}$ in $L_\mathfrak{q}$.*

2. *The ramification index and the residue degree of the prime ideal $\mathfrak{q}\mathcal{O}_\mathfrak{q}$ with respect to the prime ideal $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ of $\mathcal{O}_\mathfrak{p}$ are given by,*

$$e(\mathfrak{p}\mathcal{O}_\mathfrak{p}, \mathfrak{q}\mathcal{O}_\mathfrak{q}) = e(\mathfrak{p}, \mathfrak{q}), \quad f(\mathfrak{p}\mathcal{O}_\mathfrak{p}, \mathfrak{q}\mathcal{O}_\mathfrak{q}) = f(\mathfrak{p}, \mathfrak{q}).$$

3. $\mathfrak{q}$ *is unramified over* K *if and only if* $\mathfrak{q}\mathcal{O}_{\mathfrak{q}}$ *is unramified over* $K_{\mathfrak{p}}$*.*

Proof. We prove the first statement. We shall see first $\mathcal{O}_{\mathfrak{q}_i}$ is a finitely generated $\mathcal{O}_{\mathfrak{p}}$-module. Recall the homomorphism $\hat{s} : \prod_{i=1}^{g} \mathcal{O}_{\mathfrak{q}_i} \to \mathcal{O}_{\mathfrak{p}}^{\oplus n}$ of $\mathcal{O}_{\mathfrak{p}}$-modules appearing in the proof of Lemma 2.13. Now, note $\hat{s}\hat{t} = l_{ab}$ left multiplication understood componentwise and this composition is then injective, since l_{ab} is injective. Now, if a composition of two maps is injective, necessarily the first map is injective. Thus, $\hat{s}$ is injective and $\mathcal{O}_{\mathfrak{q}_i}$ is isomorphic to an $\mathcal{O}_{\mathfrak{p}}$-submodule of $\mathcal{O}_{\mathfrak{p}}^{\oplus n}$; hence, it is a finitely generated $\mathcal{O}_{\mathfrak{p}}$-module for being $\mathcal{O}_{\mathfrak{p}}$ a PID. Recall from commutative ring theory that this is equivalent to $\mathcal{O}_{\mathfrak{q}_i}$ being integral over $\mathcal{O}_{\mathfrak{p}}$. Then, since $\mathcal{O}_{\mathfrak{q}_i}$ is integrally closed, it is the integral closure of $\mathcal{O}_{\mathfrak{p}}$ in $L_{\mathfrak{q}_i}$.

Statement 2 is easy to prove, we prove the equality of indices for the sake of illustration. Let $\mathfrak{p}B = \mathfrak{q}^e \prod \mathfrak{q}_i^{e_i} B$. Then, since $\mathfrak{q}$ is the unique prime ideal of $\mathcal{O}_{\mathfrak{q}}$ and $B \subseteq \mathcal{O}_{\mathfrak{q}}$, $\mathfrak{p}\mathcal{O}_{\mathfrak{q}} = \mathfrak{q}^e\mathcal{O}_{\mathfrak{q}}$. Thus, the statement follows. Statement 3 is immediate now from statement 2. □

Finally we can prove our main result.

Proposition 2.16. *If* A *is a complete discrete valuation ring, then* B *is also a complete discrete valuation ring. Thus, there is a unique prime ideal of* B *that lies above the unique nonzero prime ideal of* A*.*

Proof. This follows from Propositions 2.14 and 2.15. Since A is complete, $g = 1$ and there is a unique prime ideal $\mathfrak{q}$ lying above the unique prime ideal of A, $\mathfrak{p}$, by Proposition 2.14. This proposition gives us the isomorphism $K_{\mathfrak{p}}[t]/(f) \cong L_{\mathfrak{q}}$, via the assignment $t \mapsto \alpha$, which together with the isomorphism $K[t]/(f) \cong L$ given by $t \mapsto \alpha$ and completeness of K ($K_{\mathfrak{p}} = K$) shows completeness of L, i.e. $L_{\mathfrak{q}} = L$. Thus, B is the integral closure of A in $L_{\mathfrak{q}}$ and by Proposition 2.15, $B = \mathcal{O}_{\mathfrak{q}}$. This proves B is a complete discrete valuation ring, as wanted. □

Note that in a separable extension of a complete valuation field L/K there is a unique prime in B $\mathfrak{q}$ lying above the unique prime in A, namely $\mathfrak{p}$. If p' generates $\mathfrak{p}$, then, it generates $\mathfrak{p}B = \mathfrak{q}^e$, and if $\mathfrak{q}$ is generated by π, then $p' = \epsilon\pi^e$ with ϵ a unit in B. Thus, for any $k \in K$ we have the relation $\nu_L(k) = e\nu_K(k)$, since any element can be written as $k = u(\epsilon\pi^e)^n$ with u a unit in A and taking valuations in K yields n, but looking from L it yields en.

Proposition 2.17. *Let* K *be a complete discrete valuation field,* L *a finite separable extension of* K *and* ν_K *and* ν_L *their respective discrete valuations. If* f *is the residue degree of* L *over* K*, then for any* $a \in L^\times$*, we have*

$$\nu_K(\mathrm{N}_{L/K}(a)) = f \cdot \nu_L(a).$$

Proof. Since K is a complete discrete valuation field, its separable extension L is also a complete discrete valuation field by Proposition 2.16. Then, there is a unique prime ideal, $\mathfrak{q}$, lying above $\mathfrak{p}$. Let e denote its ramification index and f the residue degree. Let $a \in L^\times$. Then, since $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}^e$, we have $a^e = ku$ where $k \in K^\times$ and $u \in \mathcal{O}_L^\times$. Note this holds because $\epsilon\pi^e$ generates $\mathfrak{p}$ with $\epsilon \in \mathcal{O}_L^\times$ and then any element a can be written as a product of an integral unit $u \in \mathcal{O}_L^\times$ and an integral power of π. Now, since

$$\nu_K(N_{L/K}(a^e)) = e\nu_K(N_{L/K}(a)) \quad \text{and} \quad \nu_L(a^e) = e\nu_L(a),$$

by the properties of discrete valuations and the norm map, it is sufficient to show

$$\nu_K(N_{L/K}(k)) = f \cdot \nu_L(k),$$

since u is an integral unit; thus, of null valuation. Now, note that the left-hand side is equal to $\nu_K(N_{L/K}(k)) = \nu_K(k^{[L:K]}) = [L:K]\nu_K(k)$ and the right-hand side is equal to $f\nu_L(k) = fe\nu_K(k) = [L:K]\nu_K(k)$ by Proposition 2.9, proving the desired equality. □

Proposition 2.18. *Let K be a local field of null characteristic. Then,*

1. *For $n \in \mathbb{N}$, $(K^\times)^n$ is an open subgroup of finite index of $K^\times$.*
2. *Every subgroup of finite index of $K^\times$ is an open subgroup.*

Proof. $(K^\times)^n$ is clearly a subgroup of $K^\times$. We shall see first it is open. For that, let $\mathfrak{p}$ and π be as before and note for any $\epsilon \in 1 + \mathfrak{p}^k$,

$$\epsilon^n = (1 + \pi^k\alpha)^n = 1 + n\pi^k\alpha + \pi^{k+1}\beta \equiv 1 + n\pi^k\alpha \pmod{\mathfrak{p}^{k+1}}.$$

Thus, any unit $\epsilon \in 1 + \mathfrak{p}^k$ is of the form

$$\epsilon = (1 + n^{-1}\pi^k\alpha)^n + \pi^{k+1}\beta = (1 + n^{-1}\pi^k\alpha)^n(1 + \pi^{k+1}\gamma),$$

where $\beta, \gamma \in \mathcal{O}$. Since K is a local field, it is complete and we may follow this process until we obtain an nth root of ϵ. Thus, $\epsilon \in (K^\times)^n$. This shows that the open subgroup $1 + \mathfrak{p}$ is contained in $(K^\times)^n$; hence, $(K^\times)^n$ is open. Now, note that the units of a local field are generated by the unique prime element and a set of representatives of the residue field, Since the residue field is finite, it is finitely generated, and it is abelian for being a field. Thus, since $K^\times/(K^\times)^n$ is torsion by noting that any $x \in K^\times$ satisfies $x^n(K^\times)^n = (K^\times)^n$, it must be of finite order, proving $|K^\times : (K^\times)^n| < \infty$. Lastly, let H be a subgroup of finite index n. Then, $(K^\times)^n \leq H$ since for any $x \in K^\times$, $x^nH = H$ by Lagrange's Theorem. Then, H is open too. □

Lastly, note that $K^\times$ is generated by the prime elements in K. For that, note that a prime element is of valuation 1 and since a unit in the valuation ring has valuation 0, their product is again a prime; thus, all elements of valuation 0 can be obtained as division of primes and any nonzero element can be obtained from primes, as a power of a prime times an element of null valuation. This will be important in Chapter 4 to reduce proofs to the case of a prime element.

Chapter 3

The Brauer Group

In the axiomatic definition of a field K, we assume K to be a commutative ring. We may relax this definition not asking for commutativity. If we do so, we get a kind of non (necessarily) commutative fields. These will be called *division algebras* or *skew fields* and they are nothing but identity rings where division is possible, i.e. all non zero elements are invertible. Most of the division algebras seen in undergraduate courses are usually commutative and thus, usual fields. The first example of a non commutative division algebra was the so-called quaternion algebra, $\mathbb{H}$, discovered by William Rowan Hamilton (1805-1865) in 1843 while walking along the Royal Canal in Dublin (he carved the defining formula for quaternions $i^2 = j^2 = k^2 = ijk = -1$ into the stone of Broome Bridge in an impulse after years of thinking). Quaternions came to existence as an effort to understand rotations in a three dimensional space, just as complex numbers describe rotations in two dimensions.

The theory presented in this chapter is further richer and more extensive than the one given in our presentation. We have developed just a minimal amount of theory due to space constraints. Thus, the interested reader is strongly encouraged to check [Jac85], for example, for more details.

Even if not stated explicitly, all k-algebras in this work are assumed to be associative.

3.1 Central simple algebras and the Brauer group

Let k be a field and A a k-algebra. If the center of A is exactly k, A is said to be *central* over k and if the only (two-sided) ideals of A are 0 and A itself, A is said to be *simple.* If A is both central over k and simple, A is called a *central simple algebra* over k. As an example of central simple algebras we have division algebras over their center. For instance, $\mathbb{H}$ is a central simple algebra over $\mathbb{R}$.

Our aim is to define a group, for a field k, whose elements will be some similarity classes defined upon simple central algebras over k. To define a group, we need an operation, and this operation will be based on the *tensor product*. Then, we need first to define the tensor product of two vector spaces. For that, let A and B be two k-vector spaces. A *balanced product* of A and B is defined to be an abelian group G together with a map $f : A \times B \to G$ satifying for all $a, a' \in A$, $b, b' \in B$ and $\lambda \in k$,

1. $f(a + a', b) = f(a, b) + f(a', b)$,
2. $f(a, b + b') = f(a, b) + f(a, b')$,
3. $f(\lambda a, b) = f(a, \lambda b)$.

It is denoted as (G, f). If (G', f') is another balanced product, a *morphism* from (G, f) to (G', f') is a group homomorphism $\eta : G \to G'$ such that $f' = f\eta$. Now, the *tensor product* of A and B is a balanced product $(A \otimes_k B, \otimes)$ such that for any other balanced product (G, f), there exists a unique morphism from $(A \otimes_k B, \otimes)$ to (G, f), i.e. $(A \otimes_k B, \otimes_k)$ is universal for this property. An explicit construction of the tensor product via the cartesian product $A \times B$ where its elements are written as sums of the elementary tensors $a \otimes_k b$ with $(a, b) \in A \times B$ is given in Problem A.6. Note $\dim_k(A \otimes_k B) = \dim_k(A) \dim_k(B)$ and that $A \otimes_k B$ can be endowed with a natural product $(a \otimes_k b)(a' \otimes_k b') = (aa' \otimes_k bb')$, making $A \otimes_k B$ a k-algebra.

Now, we need to define the aforementioned similarity relation on central simple algebras over a field k. With that goal in mind, we state and prove a criterion to know under which conditions can an algebra over a field k be factored as the tensor product of two k-subalgebras. We consider just the finite dimensional case.

Proposition 3.1. *Let A and B be subalgebras of a finite dimensional algebra D over a field k. Then, $D \cong A \otimes_k B$ if the following conditions are satisfied.*

1. $ab = ba$ for all $a \in A$ and $b \in B$.

2. $D = AB$ and $[D : k] = [A : k][B : k]$.

Proof. The first condition ensures the map $\varphi : A \otimes_k B \to D$ mapping $a \otimes b \to ab$ is a ring homomorphism and k-linear. For the sake of illustration we shall show that the product is preserved thanks to first condition, other properties are easy to check from the definition of the tensor product and are left to the reader.

$$\varphi((a \otimes b)(a' \otimes b')) = \varphi(aa' \otimes bb') = aa'bb' = aba'b' = \varphi(a \otimes b)\varphi(a' \otimes b').$$

The second condition implies φ is surjective; thus, an isomorphism by dimension counting of vector spaces. □

Let us see a direct application of this criterion.

Proposition 3.2. *Let A be a k-algebra. Then, $M_n(A) \cong M_n(k) \otimes_k A$. In particular, $M_{mn}(k) \cong M_m(k) \otimes_k M_n(k)$.*

Proof. It is straightforward to check that the subalgebras $M_n(k)$ and $A1_n$ where 1_n is the identity in $M_n(A)$, satisfy the conditions in Proposition 3.1. Just note $Ma1_m = a1_mM$ for any $M \in M_n(k)$ and any $a \in A$ and that any $M \in M_n(A)$ can be expressed uniquely as an A-linear combination of elements of a given basis $\{e_{ij}\}$ for $M_n(k)$ since a k-basis for $M_n(k)$ automatically gives an A-basis for $M_n(A)$. Last assertion follows now from the first one by taking $A := M_m(k)$. □

Now, we are in position to define the similarity relation. Let A and B be two finite dimensional central simple algebras over k. We will say A and B are *similar* and write $A \sim B$ when $M_n(A) \cong M_m(B)$ for some positive integers n, m. This similarity relation is clearly reflexive and symmetric. To see transitivity, let $M_n(A) \cong M_m(B)$ and $M_l(B) \cong M_r(C)$, then

$$\begin{aligned} M_{nl}(A) &\cong M_{nl}(k) \otimes A \cong M_n(k) \otimes M_l(k) \otimes A \cong M_l(k) \otimes M_n(A) \\ &\cong M_l(k) \otimes M_m(B) \cong M_l(k) \otimes M_m(k) \otimes B \cong M_m(k) \otimes M_l(B) \\ &\cong M_m(k) \otimes M_r(C) \cong M_m(k) \otimes M_r(k) \otimes C \cong M_{mr}(k) \otimes C \\ &\cong M_{mr}(C), \end{aligned}$$

where we have used associativity and commutativity of the tensor product and the formulas obtained in Proposition 3.2. Thus, $\sim$ is an equivalence relation and we may consider equivalence classes

$$[A] = \{B \text{ finite dimensional simple central algebra} : B \sim A\}.$$

Now we shall define a binary operation via the tensor product for the set of these equivalence classes. Let $A \sim A'$ and $B \sim B'$. We claim now $A \otimes B \sim A' \otimes B'$. Since $A \sim A'$ and $B \sim B'$ we know by definition of $\sim$ that $M_n(A) \cong M_m(A')$ and $M_l(B) \cong M_r(B')$, or equivalently by Proposition 3.2, $A \otimes M_n(k) \cong A' \otimes M_m(k)$ and $B \otimes M_l(k) \cong B' \otimes M_r(k)$ for positive integers n, m, l, r. Then

$$\begin{aligned} M_{nl}(A \otimes B) &\cong A \otimes B \otimes M_{nl}(k) \cong A \otimes M_n(k) \otimes B \otimes M_l(k) \\ &\cong A' \otimes M_m(k) \otimes B' \otimes M_r(k) \cong A' \otimes B' \otimes M_{mr}(k) \\ &\cong M_{mr}(A' \otimes B'), \end{aligned}$$

proving our claim. This means that the binary operation $[A] + [B] := [A \otimes B]$ is well defined.

The *opposite algebra* of A, denoted A^{op}, is defined by dualizing the product in A, i.e. reversing the product in A or, in other words, assigning the element ba to the product $a \cdot b$. The *enveloping algebra* of A, denoted A^e, is defined as the tensor product $A^e = A \otimes_k A^{op}$.

To make this set of equivalence classes into an abelian group we need to prove first associativity, commutativity, existence of an identity and an inverse for all equivalence classes. Associativity and commutativity follows directly from associativity and commutativity of the tensor product. Note that $M_n(A) \cong A \otimes M_n(k)$; thus, $A \sim A \otimes M_n(k)$. Hence, $[M_n(k)] = 0$ acts as the identity for $+$. We shall see $[A] + [A^{op}] = 0$ and $[A^{op}]$ acts as the inverse of $[A]$ with respect to $+$, or equivalently by definition, that the enveloping algebra acts always as the identity.

Primitive rings and the Density Theorem

For an abelian group M, the set of endomorphisms of M, $\mathrm{End}_{\mathbb{Z}}\, M$ or $\mathrm{End}\, M$, has a natural ring structure. With *ring of endomorphisms*, we mean a subring of $\mathrm{End}\, M$ for an abelian group M. We define a *ring representation*, as a ring homomorphism $\rho : R \to \mathrm{End}\, M$ for an abelian group M. A representation ρ of R acting on M, i.e. its image is in $\mathrm{End}\, M$, yields a left R-module structure for M by defining $am = \rho(a)m$ for any $a \in R$ and $m \in M$. Conversely, given a left R-module M, M is an abelian group and we can define $\rho = \rho_M : R \to \mathrm{End}\, M$ via the assignment $a \to a_M$ for any $a \in R$, where $a_M \in \mathrm{End}\, M$ is left multiplication by a. Thus, ρ is a ring representation. For an R-module M, $\mathrm{End}_R\, M$ will denote the group of R-linear endomorphisms.

An *irreducible representation* of a ring is a representation such the module M is nonzero and whose only submodules are 0 and itself. We may say M is *R-irreducible* if there is such a representation and it is *completely reducible* if it is the direct sum of irreducible R-modules. The kernel of a representation ρ is called the *annihilator of M*, $\mathrm{Ann}_R(M) := \{r \in R : rm = 0,\ \forall m \in M\}$. If $\mathrm{Ann}_R(M) = \ker \rho = 0$, we say ρ (or sometimes the R-module M) is *faithful.* This kernel is obviously an ideal of R. A ring R is called *(left) primitive* if it has an irreducible and faithful representation.

The structure of primitive rings is totally determined by the important Density Theorem from Nathan Jacobson ([Jac85], p. 199). For our means we only need the partial result on finite dimensional case that given a primitive ring R acting on an abelian group M, R is isomorphic to the finitely dimensional vector space[1] $\mathrm{End}_\Delta\, M$ where $\Delta = \mathrm{End}_R\, M$. Thus, when refering to the Density Theorem we will be refering to this partial result. Note irreducibility

[1] We shall use the term *vector space* for modules over a division ring and not just over fields, just to agree with the terminology in [Jac85].

of M is just needed to ensure $\Delta = \operatorname{End}_R M$ is a division algebra via Schur's Lemma. Then, if we can ensure this ring of endomorphisms is a division algebra, it is enough M being completely reducible. For a more in detail discussion on this see [Jac85].

We have a natural module action of A^e on A defined by $(\sum a_i \otimes a_i')x = \sum a_i x a_i'$. Direct verification shows it is a well defined module action. A^e-submodules of A are two-sided ideals of A; thus, if A is simple A is A^e-irreducible.

Regarding A as a left (right) A-module in the natural way, the elements of $\operatorname{End}_A A$ are the right (left) multiplication maps $x \mapsto xa$ ($x \mapsto ax$) since if an endomorphism f maps $1 \mapsto a$, then, $f(x) = f(x \cdot 1) = xa$. Note the reversing of left and right. Then, $\operatorname{End}_{A^e} A$ is the set of maps that are both left and right multiplications. Just note that if f maps $1 \mapsto a$ then, $f(x) = f(1 \cdot 1 \cdot x) = ax = xa = f(x \cdot 1 \cdot 1) = f(x)$. These are precisely the ones $x \mapsto cx$ where c is in the center of A. If A is central over k, then $x \mapsto \alpha x$, where $\alpha \in k$.

Theorem 3.3. *Let A be a finite dimensional central simple algebra over a field k. Then, $A^e = A \otimes_k A^{op} \cong M_n(k)$ where $n = \dim_k A$.*

Proof. Regarding A as an A^e-module as above, A is A^e-irreducible and $\operatorname{End}_{A^e} A = k$ for being simple and central over k respectively. Since A is finite dimensional over k, by the Density Theorem A^e maps onto $\operatorname{End}_k A$. Now, since both vector spaces are of dimension n^2 over k (note $\dim_k(A^e) = \dim_k(A)\dim_k(A^{op}) = n^2$), it is an isomorphism $A^e \cong \operatorname{End}_k A \cong M_n(k)$. □

$A^e \cong M_n(k)$ is known to be simple (see [Gri07], Proposition 1.4, p. 360). Thus it is simple central over k and by Theorem 3.3, $[A^{op}]$ acts as the inverse of $[A]$ with respect to $+$. Thus, it is only left to check this set of equivalent classes is closed under the operation $+$.

Theorem 3.4. *Let A be a finite dimensional central simple subalgebra of an algebra B. Then, $B \cong A \otimes_k C$ where C is the centralizer of A in B. The ideals of B are in correspondence with the ideals of C by the bijection $\mathfrak{a} \to A\mathfrak{a}$. Moreover, the center of B coincides with the center of C.*

Proof. We shall use Proposition 3.1. Since A^e is simple B is a direct sum of irreducible A^e-modules and for A being A^e-irreducible, they are all isomorphic to A (note that two irreducible A^e-modules are always isomorphic since if M is an irreducible R-module then $M \cong R/\mathfrak{m}$ for a maximal ideal $\mathfrak{m}$ and since R is simple they are all isomorphic, see Problem A.7). Now, note that the generator of A as an A^e-module, 1, satisfies the condition $(a \otimes_k 1)1 = a1 = 1a = 1(1 \otimes_k a)$ and $(a \otimes_k 1)1 = 0$ implies $a = 0$. Thus, since all irreducible A^e-modules are isomorphic we may choose an element c_j in each irreducible A^e-module satisfying $(a \otimes_k 1)c_j = ac_j = c_j a = c_j(a \otimes_k 1)$ and $(a \otimes_k 1)c_j = 0$ impliyng $a = 0$.

Applying this to B as an A^e-module and noting the map from A to each irreducible A^e-module mapping $1 \mapsto c_j$ extends to an isomorphism by linearity, we may write $B = \bigoplus Ac_j$ where $ac_j = c_j a$ for all $a \in A$ and $ac_j = 0$ implies $a = 0$. Then, clearly $c_j \in C$ and any element of B can be uniquely written as a finite sum $\sum a_j c_j$ for $a_j \in A$. For any $c \in C$, $c = \sum a_j c_j$, but $ac = ca$ implies $aa_j = a_j a$ for any $a \in A$. Thus, $a_j \in k$ (for A being central over k) and $c \in \sum kc_j$. Hence, $C = \sum kc_j$ and c_j is a basis for C and clearly $B = AC$ and $[B : k] = [A : k][C : k]$. Thus, by Proposition 3.1, $B \cong A \otimes_k C$, as wanted.

Now, let $\mathfrak{a}$ be an ideal in C. Then, $A\mathfrak{a}$ is an ideal in $B = AC$. We claim that $A\mathfrak{a} \cap C = \mathfrak{a}$. Let $\beta_A = \{x_1 = 1, \ldots, x_n\}$ be a k-basis for A. Since $B \cong A \otimes_k C$, any element in B can be uniquely written as a C-linear combination of the k-basis β_A. Thus, the elements of $A\mathfrak{a}$ are $\mathfrak{a}$-linear combinations of β_A. In particular, elements both in $A\mathfrak{a}$ and in C are of the form $c_1 x_1 = c_1 \in \mathfrak{a}$. Hence, $A\mathfrak{a} \cap C = \mathfrak{a}$ as claimed. This proves that the map $\mathfrak{a} \mapsto A\mathfrak{a}$ is injective since $A\mathfrak{a} = A\mathfrak{b}$ implies $\mathfrak{a} = \mathfrak{b}$ by taking the intersection with C. To check surjectivity, let $\mathfrak{b}$ be an ideal of B. Then, $\mathfrak{b}$ is an A^e-submodule of B. Hence, $\mathfrak{b} = \sum Ab_j$ where $b_j \in \mathfrak{a} := \mathfrak{b} \cap C$. This implies, $\mathfrak{b} = A\mathfrak{a}$, proving surjectivity. Thus, we get a one-to-one correspondence between the ideals of C and those of B.

Lastly, we show the center of B coincides with the center of C. Clearly the center of B is contained in C and thus, in the center of C. For the converse, any element in the center of C commutes with every element of $B = AC$ and thus, it is in the center of B. □

Thus, when C is simple and central over k, B is simple and central over k.

Corollary 3.5. *The tensor product of two finite dimensional central simple algebras over a field k is again a finite dimensional central simple algebra over k. In general, the tensor product of a finite number of finite dimensional central simple algebras over a field k is again a finite dimensional central simple algebra over k.*

Then, the set of equivalent classes is closed under $+$ and it can be regarded as an abelian group. This group is called the *Brauer group* of k and it is denoted by $\mathrm{Br}(k)$. The Brauer group was first introduced by Richard Brauer (1901-1977) in 1929.

Now, let L be a field extension of k. Then, for any k-algebra A, $A \otimes_k L$ can be regarded as an L-algebra. This L-algebra is denoted as A_L and is called the *algebra obtained from A by extending the base field to L*. If A is finite dimensional central simple over k, it can be seen as a corollary to Theorem 3.4 that A_L is finite dimensional central simple over L. Let A be a finite dimensional central simple algebra over k. A field L is called a *splitting field* for

A if $A_L = A \otimes_k L \cong M_n(L)$ for some positive integer n.

Now, let L be a finite extension of k. Then, if A is finite dimensional central simple over k, A_L is finite dimensional central simple over L. We have $(A \otimes_k B)_L \cong A_L \otimes_L B_L$ and $M_n(k)_L \cong M_n(L)$. Thus, a group homomorphism may be defined from $\mathrm{Br}(k)$ to $\mathrm{Br}(L)$ mapping $[A] \mapsto [A_L]$. The kernel of this homomorphism, i.e. the classes $[A]$ in $\mathrm{Br}(k)$ such that $A_L \sim 0$, are exactly the classes of k-algebras with splitting field L. This kernel forms a subgroup that is denoted by $\mathrm{Br}(L/k)$.

Recall that for a field F and an n-dimensional F-vector space V, $\mathrm{End}_F(V) \cong M_n(F)$. If commutativity is not assumed, we should take the opposite ring when passing from endomorphisms to matrices (see Problem A.8).

Lemma 3.6. *Let A be a central simple algebra over k and L/k a finite field extension such that L is a subfield of $M_n(A) \cong \mathrm{End}_{A^{op}}\ V$ for V an A^{op}-vector space. Then, the centralizer of L in $M_n(A)$ coincides with* $\mathrm{End}_{A^{op}\otimes_k L}\ V$.

Proof. We shall see the centralizing L condition is equivalent to $A^{op} \otimes_k L$-linearity regarding V as an $A^{op} \otimes_k L$-module via the action $(d \otimes_k l)x = dlx = ldx$. Let $l \in L \subseteq \mathrm{End}_{A^{op}}\ V$. Then, $lc = cl$ for some endomorphism c means $lc(v) = c(l(v))$ for all $v \in V$. But c is A^{op}-linear; thus, $c((l \otimes_k a)v) = c(lav) = lac(v) = (l \otimes_k a)c(v)$ and it is $A^{op} \otimes_k L$-linear. The same reasoning proves the converse. □

Theorem 3.7. *Let Δ be a finite dimensional central division algebra over k. Then, a finite extension L/k is a splitting field for Δ if and only if L is a subfield of an algebra $A = M_n(\Delta)$ such that $C_A(L) = L$.*

Proof. We just need the only if part, for a proof of the converse see [Jac85]. Let L be a subfield of $A = M_n(\Delta)$ which is self-centralised. Recall A may be identified with $\mathrm{End}_{\Delta'}\ V$ for an n-dimensional vector space V over $\Delta' = \Delta^{op}$. Then, we regard V as an $\Delta' \otimes_k L$-module as before. Since both Δ' and L are simple, by Corollary 3.5, $\Delta' \otimes_k L$ is simple too and this action is necessarily faithful. Now, since $\Delta' \otimes_k L$ is finite dimensional over k, V is completely reducible as a $\Delta' \otimes L$-module. By previous lemma, the centralizer of L in A is $\mathrm{End}_{\Delta' \otimes L}\ V$ and this is L by assumption, which is a field; thus, a division algebra. Then, we may apply the Density Theorem to obtain $\Delta' \otimes L \cong \mathrm{End}_L\ V \cong M_r(L)$ and L is a splitting field for Δ'; hence, for Δ. □

3.2 Group cohomology, crossed products and cyclic algebras

Given a group G and an abelian group M, we say M is a (left) G-module if we can define a (left) G-action on M, i.e. a map $G \times M \to M$, such that for any $g, h \in G$ and any $n, m \in M$ we have

$$g(m+n) = gm + gn, \quad g(hm) = (gh)m, \quad 1m = m.$$

Now, let G be a group and M a G-module. We define the *group of n-cochains*, denoted as $C^n(G,M)$ as the set of maps from G^n to M for any $n \in \mathbb{N}$. For $n = 0$, $C^0(G,M) = M$ by convention. This set can be endowed with a group operation by defining the sum of maps componentwise. This way, it becomes an abelian group.

Let us define the maps $\delta_n : C^n(G,M) \to C^{n+1}(G,M)$ via the assignments,

$$\begin{aligned}\delta_n(f)(\sigma_1, ..., \sigma_{n+1}) =& \sigma_1 f(\sigma_2, ..., \sigma_{n+1}) \\ &+ \sum_{j=1}^{n} (-1)^j f(\sigma_1, ..., \sigma_j\sigma_{j+1}, ..., \sigma_{n+1}) \\ &+ (-1)^{n+1} f(\sigma_1, ..., \sigma_n),\end{aligned}$$

for $n \in \mathbb{N}$ and $\delta_0(m)(\sigma) = \sigma m - m$ for $n = 0$. The maps δ_n define group homomorphisms and $\delta^2 = \delta_n\delta_{n+1}$ is the trivial map. Comprobation of these facts is straightforward but tedious; thus, it is left to the reader. The maps δ_n are called *differentials*.

Since $\delta^2 = 0$, Im δ_{n-1} is inside $\ker \delta_n$, and it makes sense to define the quotient group $H^n(G,M) = Z^n(G,M)/B^n(G,M)$, where $Z^n(G,M) := \ker \delta_n$ and its elements are called *n-cocycles* and $B^n(G,M) :=$ Im δ_{n-1} and its elements are called *n-coboundaries*. For $n = 0$ we define $B^0(G,M) = 0$. The group $H^n(G,M)$ is called the *nth cohomology group* of G with coefficients in M. Two n-cocycles are called *cohomologous* if they are equal up to a coboundary, i.e. if they represent the same element of $H^n(G,M)$.

The *G-invariant* part of M is defined as the subset of M that is invariant under the action of G, i.e. $M^G = \{m \in M \ : \ \sigma m = m, \ \sigma \in G\}$. Whenever G is cyclic with generator σ, the *norm group*, $\mathrm{N}(G)$, is defined as the set $\mathrm{N}(G) := \{\sum \sigma^k m : m \in M\}$. In this cyclic case, the second cohomology group can be described by these constructions (Problem 16 in [Mor96], p. 105-106).

Theorem 3.8. *Let G be a cyclic group and M a G-module. Then, $H^2(G,M) \cong M^G/\mathrm{N}(G)$.*

Proof. See Problem A.9. □

We introduce now a way of constructing a k-algebra based on a finite Galois field extension. Let L/k be a finite Galois field extension and let $\{x_\sigma\}$ be a collection of symbols in 1-1 correspondence with the elements of $G := \mathrm{Gal}(L/k)$. We regard the k-algebra A as a vector space over L with basis $\{x_\sigma\}$, i.e. $A = \bigoplus Lx_\sigma$, and we define a product on A by the relations

$$x_\sigma x_\tau = \kappa_{\sigma,\tau} x_{\sigma\tau}, \quad x_\sigma l = \sigma x_\sigma, \quad \forall l \in L,$$

where $\kappa_{\sigma,\tau}$ are elements of $L^\times$ and L is regarded as a G-module by the natural action of G, i.e. $\sigma l = \sigma(l)$ for any $\sigma \in G$ and any $l \in L$.

Since $\{x_\sigma\}$ is an L-basis for A, any element of A can be uniquely represented as a finite sum $\sum l_\sigma x_\sigma$ with coefficients in L. Thus, the product of two elements $\sum l_\sigma x_\sigma$ and $\sum l'_\sigma x_\sigma$ is defined as $\sum \kappa_{\sigma,\tau} l_\sigma \sigma l'_\tau x_{\sigma\tau}$, by the above relations.

To make A into an associative k-algebra, the $\kappa_{s,t}$ must be chosen appropriately. Since

$$\begin{aligned}(x_\sigma x_\tau)x_\rho &= \kappa_{\sigma,\tau} x_{\sigma\tau} x_\rho = \kappa_{\sigma,\tau}\kappa_{\sigma\tau,\rho} x_{\sigma_{\sigma\tau\rho}} \\ x_\sigma(x_\tau x_\rho) &= x_\sigma \kappa_{\tau,\rho} x_{\tau\rho} = (\sigma\kappa_{\tau,\rho})\kappa_{\sigma,\tau\rho} x_{\sigma\tau\rho},\end{aligned}$$

and to ensure associativity we need, $\kappa_{\sigma,\tau}\kappa_{\sigma\tau,\rho} = (\sigma\kappa_{\tau,\rho})\kappa_{\sigma,\tau\rho}$, which is exactly the 2-cocycle condition we have seen before in multiplicative notation for the map $\kappa : G \times G \to L^\times$, $(\sigma,\tau) \mapsto \kappa_{\sigma,\tau}$. Distributive laws are straightforward to check from definition. Since by the 2-cocycle condition $\kappa_{1,\sigma} = \kappa_{1,1}$ and $\kappa_{\sigma,1} = \sigma\kappa_{1,1}$, the element $1 = \kappa_{1,1}^{-1} x_1$ is the identity for the multiplication as a simple computation shows. Finally, since the elements of k are fixed by all k-automorphisms of L, the ring multiplication and the k-scalar multiplication as a vectorial space are compatible, i.e. $\lambda(ab) = (\lambda a)b = a(\lambda b)$ for all $\lambda \in k$ and $a, b \in A$. Thus, A is a k-algebra. We shall denote A in the following as (L, G, κ). We shall see these k-algebras are simple central over k and identify the subgroup $\mathrm{B}r(L/k)$ with the second cohomology group $H^2(G, L^\times)$.

Proposition 3.9. *Let $A = (L, G, \kappa)$. Then, A is a simple central algebra over k and $[A : k] = n^2$ where $n = [L : k]$. Regarding L as a subfield of A $(L1_A)$ it coincides with its centralizer in A, i.e. $C_A(L) = L$.*

Proof. The relation $[A : k] = [A : L][L : k] = [L : k]^2 = n^2$ holds from the definition of the crossed product. Now we shall see A is simple. For that, we shall see first all x_σ are invertible. The product $x_\sigma x_{\sigma^{-1}} = \kappa_{\sigma,\sigma^{-1}}\kappa_{1,1}1$ is a nonzero element of L; thus, x_σ is invertible in A. Now, let $\mathfrak{a}$ be a proper ideal of A. We shall see it is trivial. We write $\overline{a} = a + \mathfrak{a}$ for $a \in A$. Then, $\overline{A} = A/\mathfrak{a} \neq 0$ since it is proper. Hence, the usual projection restricted to L, $l \mapsto \bar{l}$ is a monomorphism into A, since L is a field and this homomorphism is non-trivial. Therefore, the elements $\overline{x}_\sigma$ are all invertible in $\overline{A}$. The relations $\overline{x}_\sigma \overline{l} = \overline{\sigma l}\overline{x}_\sigma$ hold for all $\sigma \in G$ and by the Dedekind independence argument on shortest relations (see Problem A.10) the $\overline{x}_\sigma$ are all left linearly independent over $\overline{L} = \{\overline{l} : l \in L\}$. Thus, $[\overline{A} : \overline{L}] = n$ and since $\mathfrak{a}$ is proper, $L \cap \mathfrak{a} = 0$ and we get $\overline{L} \cong L$ and $\overline{k} \cong k$ via the canonical isomorphisms $x \mapsto \overline{x}$. Thus, $[\overline{A} : \overline{k}] = [\overline{A} : \overline{L}][\overline{L} : \overline{k}] = n^2 = [A : k]$ and we get $\overline{A} \cong A$ as k-vector spaces and it follows $\mathfrak{a}$ is trivial; hence, A is simple. Now we see it is central over k. Let $l \in L$ and suppose an element $\sum l_\sigma x_\sigma \in A$ commutes with l. Then, rearranging terms, $\sum (l - \sigma l) l_\sigma x_\sigma = 0$, which implies $l = \sigma(l)$ for all σ such that $l_\sigma \neq 0$ for L being an integral domain. Thus, for $\sum l_\sigma x_\sigma$ to commute with every $l \in L$, necessarily $l_\sigma = 0$ for all $\sigma \neq 1$. Then, $\sum l_\sigma x_\sigma = l_1 x_1 = l_1 \kappa_{1,1} 1 \in L$ and $C_A(L) = L$ as wanted. Lastly, let c be in the center of A. Then, $c \in C_A(L) = L$ and in particular, $c x_\sigma = x_\sigma c$ for all $\sigma \in G$. Thus, $\sigma c = c$ for all $\sigma \in G$ and c is in the fixed field of G, i.e. in k. Hence, k is the center of A and A is simple central over k. □

Then, we may define the map $\varphi : H^2(G, L^\times) \to \mathrm{Br}(L/k)$ via the assignment $\kappa \to (L, G, \kappa)$ which is well defined since $A = (L, G, \kappa)$ is a central simple algebra over k with splitting field L, for L being a subfield of A such that $C_A(L) = L$ and a direct application of Theorem 3.7. We shall see φ is indeed a group isomorphism. This is summarized in the following proposition: the first assertion shows it is onto, the second one makes it into a group homomorphism and the third one proves injectivity. We omit the proofs due to lack of space and refer the reader to [Jac85] instead.

Proposition 3.10. *Let A be a finite dimensional central simple algebra over k with splitting field the finite extension L/k. Then,*

1. *There exists a factor set κ such that $A \sim (L, G, \kappa)$.*
2. *$(L, G, \kappa) \otimes_k (L, G, \eta) \sim (L, G, \kappa\eta)$ for any pair of factor sets κ and ν.*
3. *$(L, G, \kappa) \sim 0$ if and only if κ is a 2-coboundary.*

Summarizing, we have reached the following important theorem.

Theorem 3.11. *The map $\varphi : H^2(G, L^\times) \to \mathrm{Br}(L/k)$ given by $[\kappa] \mapsto [(L, G, \kappa)]$ is an isomorphism. Thus,* Br(L/k) *can be identified with $H^2(G, L^\times)$.*

Now we turn our atention to the special case when L/k is a cyclic extension. In this case, a crossed product (L, G, κ) takes a very simple form. In this situation $G = \langle \sigma \rangle$ and let $\kappa : G \times G \to L^\times$ be defined as,

$$\kappa_{\sigma^i, \sigma^j} = \begin{cases} 1, & i + j < n, \\ \alpha, & i + j \geq n, \end{cases}$$

for $\alpha \in k^\times$. We shall denote $\kappa_{\sigma^i,\sigma^j}$ simply by $\kappa_{i,j}$. Then, it is straightforward to check κ is indeed a 2-cocycle as we did in Problem A.9. In fact, any crossed product for a cyclic extension can be obtained through such a simple 2-cocycle. The k-algebra A will be called a *cyclic algebra* and denoted by (L, σ, α).

Combining the isomorphism in Theorem 3.8 with the one obtained in Theorem 3.11, we obtain the fundamental property of cyclic algebras.

Theorem 3.12. *Let L/k be a cyclic finite field extension. Then, the map $\varphi : L^\times/N_{L/k}(L^\times) \to \mathrm{Br}(L/k)$ such that $[\alpha] \mapsto [(A, \sigma_L, \alpha)]$ is an isomorphism.*

A cyclic algebra is completely determined by a character $\chi : G \to \mathbb{Q}/\mathbb{Z}$ and α. If we consider a character χ of $\mathrm{Gal}(k^{ab}/k)$, its kernel is open; thus it is of the form $\mathrm{Gal}(K^{ab}/L)$ and L is the cyclic extension associated to the kernel of χ. What is more, there is one and only one character with kernel $\mathrm{Gal}(K^{ab}/L)$ for each generator of $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(K^{ab}/K)/\mathrm{Gal}(K^{ab}/K)$ if we fix the image of the generator. Then, we may determine a cyclic algebra by the pair (χ, α). From now on a cyclic algebra will be denoted via such a pair (χ, α) and the operations on the Brauer group can be written as $(\chi, \alpha) \otimes (\chi, \beta) \sim (\chi, \alpha\beta)$ from Proposition 3.10, $(\chi + \chi', \alpha) \sim (\chi, \alpha) \otimes (\chi', \alpha)$ and $(\chi, \alpha) \sim 0$ if and only if $\alpha \in N_{L/k}(L^\times)$ where L is the cyclic extension corresponding to the kernel of χ from Proposition 3.10 too and Theorem 3.12.

3.3 Brauer group of a local field

We will turn our attention now to local fields. In this context, we know that there is a unique prime in a Galois extension field L lying above the unique prime in the local field K by Proposition 2.16. Thus, we will say L/K is an *unramified* extension when the unique prime in L lying above the unique prime in K is unramified. We say a character is *unramified* if the corresponding cyclic extension is unramified. Unramified extensions of local fields are very easy to study since we claim they are in one-to-one correspondence with separable extensions of their residue fields. Since these are finite fields, we know there is a unique cyclic unramified extension for a local field of degree n for any $n \in \mathbb{N}$.

To prove our claim, recall from Chapter 2 the degree formula $[L : K] = ef$ since in a finite extension of a local field $g = 1$. If the finite extension L/K is also unramified, then $e = 1$ and $[L : K] = f = [E : F]$ where E and F are the residues fields of L and K respectively. We shall see $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(E/F)$. For that, we shall construct an explicit isomorphism $\varphi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/F)$ in the natural way, i.e. restricting each automorphism in $\mathrm{Gal}(L/K)$ to $\mathcal{O}_L$ and composing with the natural projection onto E. Note this is well defined since automorphisms fix minimal polynomials and if $\mathfrak{p}$ is the unique prime in $\mathcal{O}_K$ and $\mathfrak{q}$ the unique prime in $\mathcal{O}_L$ above

$\mathfrak{p}\mathcal{O}_L$, any automorphism fixes $\mathfrak{q}$ for being an isomorphism. Note φ is a group homomorphism since it preserves composition. By order counting we just need to prove φ is injective to make it into an isomorphism. For that, note the kernel of this homomorphism is precisely the inertia subgroup of $\mathrm{Gal}(L/K)$, i.e. the automorphisms that restrict to the identity in $\mathrm{Gal}(E/F)$. This subgroup is known to have order e from the course on algebraic number theory [lang ANT]; thus, since the extension is unramified $e = 1$ and it is trivial. Hence, the homomorphism is injective and $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(E/F)$ as wanted by order counting.

From this result we see unramified extensions of local fields are all cyclic and thus abelian for being essentially the same as the corresponding extensions of the residue field which is finite for the base field being local. For that, note the composite of unramified extensions is again unramified since the degree of the composite is equal to the degree of its residue field; thus, $e = 1$. Hence, we may define the *maximal unramified extension* of K and denoted it by K^{ur}. Thus, $K^{ur} \subseteq K^{ab}$, and $\mathrm{Gal}(K^{ur}/K) \cong \mathrm{Gal}(F^{ab}/F)$, where last isomorphism is obtained via the universal property of the inverse limit since each isomorphism $\mathrm{Gal}(K^{ur}/K) \cong \mathrm{Gal}(F^{ab}/F)$ is compatible with the restrictions.

Also, it is known any finite dimensional central division algebra over a local field K has an unramified cyclic extension field K_n/K as splitting field (see Theorem 9.21 and its converse in [Jac85], p. 607-608) and we shall write χ_n for its corresponding character. Thus, any element of $\mathrm{Br}(K)$ is contained in $\mathrm{Br}(K_n/K)$ for some unramified extension K_n/K of degree n. Note, any element of $\mathrm{Br}(K_n/K)$ may be lifted to an element in $\mathrm{Br}(K_m/K)$ whenever n divides m by simple tensoring by K_m. Then, $\mathrm{Br}(K)$ may be seen as a direct limit.

Proposition 3.13. *Let K be a local field and K_n the unique unramified extension of K of degree n. Then,* $\mathrm{Br}(K) \cong \varinjlim \mathrm{Br}(K_n/K) \cong \bigcup_n \mathrm{Br}(K_n/K)$.

We want to show each $\mathrm{Br}(K_n/K)$ can be generated by the algebra (χ_n, π), with π a prime in K.

Lemma 3.14. *Let K be a complete discrete valuation field, $\mathcal{O}_K$ its valuation ring, $\mathfrak{m}$ its maximal ideal and F the residue field $\mathcal{O}_K/\mathfrak{m}$. Let A be an $\mathcal{O}_K$-algebra that is a finitely generated free $\mathcal{O}_K$-module such that $A/\mathfrak{m}A \cong M_n(F)$ as an F-algebra. Then, $A \cong M_n(\mathcal{O}_K)$ as an $\mathcal{O}_K$-algebra.*

Proof. Since A is a finitely generated free $\mathcal{O}_K$-module, we can write $A \cong \bigoplus_{i=1}^m \mathcal{O}_K$ for some positive integer m. Hence, we have the following isomorphisms as F-vector spaces

$$\bigoplus_{i=1}^{m} F = \bigoplus_{i=1}^{m} \frac{\mathcal{O}_K}{\mathfrak{m}} \cong \frac{\bigoplus_{i=1}^m \mathcal{O}_K}{\bigoplus_{i=1}^m \mathfrak{m}} \cong \frac{A}{\mathfrak{m}A} \cong M_n(F) \cong \bigoplus_{i=1}^{n^2} F,$$

and as both sides are finite vector spaces over the residue field F, their dimensions must be equal, yielding $m = n^2$. Now, we need to show existence of a ring homomorphism $\varphi : A \to M_n(\mathcal{O}_K)$. For that, we may define such a map using the universal property of modules, giving an image for an $\mathcal{O}_K$-basis of A. Then, these images must satisfy some multivariate square-free equations over $\mathcal{O}_K$ in order to ensure this to be a ring homomorphism, namely $\varphi(v_i v_j) = \varphi(v_i)\varphi(v_j)$ for all the elements in the $\mathcal{O}_K$-basis $\{v_i\}$. But, these are known to have a solution over the residue field F by assumption. Then, by the multivariate Hensel's Lemma[1], there exists a solution over $\mathcal{O}_K$ and it gives us the desired isomorphism as an $\mathcal{O}_K$-algebra. □

Proposition 3.15. *Let K and K_n as in Proposition 3.13. Let $\mathcal{O}_k$ be the valuation ring of K and π a prime element of K. Then, $\mathrm{N}_{K_n/K}(K_n^\times)$ coincides with the subgroup of $K^\times$ generated by $\mathcal{O}_K^\times$ and π^n. Thus, $K^\times/\mathrm{N}_{K_n/K}(K_n^\times)$ is a cyclic group of order n generated by the class of π.*

Proof. Since K_n/K is an unramified extension, the prime element π is still a prime element in the valuation ring $\mathcal{O}_{K_n}$. Thus, the group of units $K_n^\times$ is generated by $\mathcal{O}_{K_n}^\times$ and π. Since the norm map has image on the base field, we have the inclusion $N_{K_n/K}(\mathcal{O}_{K_n}^\times) \subseteq \mathcal{O}_{K_n}^\times \cap K = \mathcal{O}_K^\times$. Then, the norm group $N_{K_n/K}(K_n^\times)$ is contained in the group generated by $\mathcal{O}_K^\times$ and $N_{K_n/K}(\pi) = \pi^n$. We are only left to prove $\mathcal{O}_K^\times \subseteq N_{K_n/K}(K_n^\times)$. For that, let $\alpha \in \mathcal{O}_K^\times$. By the isomorphism φ in Theorem 3.12, it is sufficient to show that $\varphi([\alpha]) = [(\chi_n, \alpha)] = 0$, i.e.

$$(\chi_n, \alpha) \cong M_n(K),$$

as a K-algebra. Let R be the subring of $(\chi_n, \alpha) = \bigoplus_{i=0}^{n-1} K_n$ such that

$$R := \bigoplus_{i=0}^{n-1} \mathcal{O}_{K_n}.$$

R is clearly an $\mathcal{O}_K$-algebra and a finitely generated free $\mathcal{O}_K$-module. If the residue field of K is of order q, i.e. $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_q$, we get

$$\frac{R}{\mathfrak{p}R} \cong \bigoplus_{i=0}^{n-1} \mathbb{F}_{q^n},$$

which is clearly a cyclic algebra over the finite field $\mathbb{F}_q$. But, by Problem A.11 $\mathrm{Br}(\mathbb{F}_q) = 0$; thus, $R/\mathfrak{p}R \cong M_n(\mathbb{F}_q)$ as an $\mathbb{F}_q$-algebra. Now, it follows from Lemma 3.14, $R \cong M_n(\mathcal{O}_K)$ as an $\mathcal{O}_K$-algebra. Tensoring the isomorphism with $\otimes_{\mathcal{O}_K} K$ yields the wanted isomorphism of K-algebras. □

[1] See `https://en.wikipedia.org/wiki/Hensel%27s_lemma#Generalizations`

From this last proposition and Theorem 3.12, we have the isomorphisms

$$\mathrm{Br}(K_n/K) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}, \tag{3.1}$$

for all $n \in \mathbb{N}$ given by the assignment $(\chi_n, \pi) \to 1/n + \mathbb{Z}$. Note that if n divides m the diagram

$$\begin{tikzcd}
\mathrm{Br}(K_n/K) \arrow[r, "\subseteq"] \arrow[d, "\cong"'] & \mathrm{Br}(K_m/K) \arrow[d, "\cong"] \\
\frac{1}{n}\mathbb{Z}/\mathbb{Z} \arrow[r, "\subseteq"] & \frac{1}{m}\mathbb{Z}/\mathbb{Z}
\end{tikzcd}$$

commutes. Thus, we may combine the isomorphisms in (3.1) applying Proposition 3.13 to obtain

$$\mathrm{Br}(K) = \bigcup_n \mathrm{Br}(K_n/K) \cong \bigcup_n \frac{1}{n}\mathbb{Z}/\mathbb{Z} = \mathbb{Q}/\mathbb{Z},$$

where this isomorphism is denoted by inv_K.

Theorem 3.16 (Brauer group of a local field). *The aforedefined map* $\mathrm{inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$ *is a group isomorphism.*

Chapter 4

Class Field Theory

The reader may be wondering what the last chapter has to do with abelian extensions of local fields. The aim of this chapter is to establish these links and to use the theory of the previous chapters to prove the main theorem of local class field theory following [KKS11].

4.1 Finite fields

We start by considering finite fields. It is already known that $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is isomorphic to the additive group $\mathbb{Z}/n\mathbb{Z}$, which is very well understood. Our aim is to approximate the absolute Galois group $\mathrm{Gal}(\mathbb{F}_q^{ab}/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}$ by an easier group. In this case, by $\mathbb{Z}$. The reason for this choice is we are interested in the Galois group for the Galois correspondence of finite extensions, i.e. we are interested in its open subgroups. Then, the Galois group $\mathrm{Gal}(\mathbb{F}_q^{ab}/\mathbb{F}_q)$ is isomorphic to the profinite completion of $\mathbb{Z}$ and by Proposition 1.4 its open subgroups are in one-to-one correspondence with open subgroups of $\mathbb{Z}$, which are precisely $n\mathbb{Z}$ for each $n \in \mathbb{N}$. Then, $\mathbb{Z}$ gives us a one-to-one correspondence between its open subgroups and the finite abelian extensions of a finite field. What is more, we may define a map $\rho_{\mathbb{F}_q} : \mathbb{Z} \to \widehat{\mathbb{Z}} \cong \mathrm{Gal}(\mathbb{F}_q^{ab}/\mathbb{F}_q)$, which is no more than the usual inclusion of a group in its profinite completion composed with the isomorphism of profinite groups $\widehat{\mathbb{Z}} \cong \mathrm{Gal}(\mathbb{F}_q^{ab}/\mathbb{F}_q)$, namely $n \mapsto (n\mathbb{Z})_n \mapsto (\sigma_n)_n$, where $o(\sigma_n) = n$ for each $n \in \mathbb{N}$. In addition, this map induces the isomorphisms $\mathbb{Z}/n\mathbb{Z} \cong \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ for each natural n.

This does not shed any new light on abelian finite extensions of a finite field since we knew already there is one for each natural number. But, this way of reasoning will be mimicked in the case of a local field, where we use the group of units instead of $\mathbb{Z}$ to define such a map $K^\times \to \mathrm{Gal}(K^{ab}/K)$ giving this one-to-one correspondence between open subgroups and inducing the isomorphisms $K^\times/N_{L/K}(L^\times) \cong \mathrm{Gal}(L/K)$. What is more, local class field theory can be seen as proving the open subgroups of finite index with respect to the $\mathfrak{p}$-adic topology in $K^\times$ are precisely those norm groups, and its profinite completion being isomorphic to the Galois group $\mathrm{Gal}(K^{ab}/K)$.

4.2 Local fields

Theorem 4.1 (Local Class Field Theory). *Let K be a local field. Then,*

1. *There exists a unique continuous homomorphism*

$$\rho_K : K^\times \to \mathrm{Gal}(K^{ab}/K),$$

   satisfying the following conditions.

   a) *For a finite abelian extension L of K, ρ_K induces an isomorphism*

$$K^\times/\mathrm{N}_{L/K}(L^\times) \overset{\cong}{\to} \mathrm{Gal}(L/K).$$

   b) *If K is a complete discrete valuation field with finite residue field $\mathbb{F}_q$, then the diagram*

$$\begin{tikzcd}
K^\times \arrow[r, "\rho_K"] \arrow[d, "\nu_K"'] & \mathrm{Gal}(K^{ab}/K) \arrow[d] \\
\mathbb{Z} \arrow[r, "\rho_{\mathbb{F}_q}"] & \mathrm{Gal}(\mathbb{F}_q^{ab}/\mathbb{F}_q).
\end{tikzcd}$$

   is commutative, where ν_K is the discrete valuation in K and the map $\mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(\mathbb{F}_q^{ab}/\mathbb{F}_q)$ is the composition

$$\mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(K^{ur}/K) \overset{\cong}{\to} \mathrm{Gal}(\mathbb{F}_q^{ab}/\mathbb{F}_q),$$

   where $\mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(K^{ur}/K)$ is the restriction of automorphism of K^{ab} to K^{ur}.

2. *There is a one-to-one correspondence through ρ_K between open subgroups of $\mathrm{Gal}(K^{ab}/K)$ and open subgroups of finite index of $K^\times$, i.e. finite abelian extensions of K lie in one-to-one correspondence with open subgroups of finite index of $K^\times$.*

The remainder of the section is devoted to proving this important theorem. We will assume at some points K has characteristic 0 for the sake of simplicity, but the results are still valid in positive characteristic even if the proofs tend to be more tedious. The cases $K = \mathbb{R}$ and $\mathbb{C}$ are dealt separately (see Problem A.12). Now, let K be a complete discrete valuation field with finite residue field.

Proposition 4.2. *Let K be a local field and L a finite separable extension of K. Then,*

1. *The following diagram is commutative.*

$$\begin{tikzcd}
\mathrm{Br}(K) \arrow[r, "\mathrm{inv}_K"] \arrow[d] & \mathbb{Q}/\mathbb{Z} \arrow[d, "\text{multiplication by } {[L{:}K]}"] \\
\mathrm{Br}(L) \arrow[r, "\mathrm{inv}_L"] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

2. *The order of* $\mathrm{Br}(L/K)$ *is exactly* $[L : K]$.

Proof. First note second assertion follows from the first one. Since inv is an isomorphism, the kernel of the multiplication by $[L : K]$ in $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the kernel of the restriction $\mathrm{Br}(K) \to \mathrm{Br}(L)$, which we denoted by $\mathrm{Br}(L/K)$. Since the first kernel is precisely $\{n/[L : K] + \mathbb{Z}\}$ and has order $[L : K]$, $\mathrm{Br}(L/K)$ has order $[L : K]$ too. Now we prove the first assertion. Let e and f be the ramification index and residue degree of L over K respectively. By Proposition 2.9 we have $[L : K] = ef$. Let π be a prime element in L and $\epsilon\pi^e$ a corresponding prime element in K and recall from Lemma 1.7 the following diagram is commutative

$$\begin{tikzcd}
X(\mathbb{F}_q) \arrow[r] \arrow[d, "\text{restriction}"'] & \mathbb{Q}/\mathbb{Z} \arrow[d, "\text{multiplication by } f"] \\
X(\mathbb{F}_{q^f}) \arrow[r] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

where the horizontal arrows are mapping $\chi \mapsto \chi(\sigma)$ and $\chi_L \mapsto \chi(\sigma^f)$, where χ_L is the restriction of χ to $X(\mathbb{F}_{q^f})$ viewed as an element of $X(L)$ and σ and σ^f are the Frobenius automorphisms in the corresponding absolute Galois groups. Now the first assertion follows from this since the isomorphism inv_K is mapping $(\chi, \epsilon\pi^e) \mapsto \chi(\sigma)$ whilst inv_L is mapping $(\chi, \pi) \mapsto \chi(\sigma^f)$. Then, since $[L : K] = ef$, we see $(\chi, \epsilon\pi^e) \mapsto \chi(\sigma) \mapsto ef\chi(\sigma)$ and $(\chi, \epsilon\pi^e) \mapsto (\chi_L, \epsilon\pi^e) = (\chi_L, \pi^e) = e(\chi_L, \pi) \mapsto e\chi(\sigma^f) = ef\chi(\sigma)$ coincide proving the commutativity of the diagram in the first assertion. □

Proposition 4.3. *For each finite abelian extension L of K, there is an isomorphism*

$$K^\times/\mathrm{N}_{L/K}(L^\times) \overset{\cong}{\to} \mathrm{Gal}(L/K)^{**} \overset{\cong}{\to} \mathrm{Gal}(L/K),$$

given by the composition $\alpha \mapsto (\chi \to \mathrm{inv}_K(\chi, \alpha)) \mapsto \sigma$.

Proof. First note the map $K^\times \to \mathrm{Gal}(L/K)^{**} \to \mathrm{Gal}(L/K)$ given by the composition $\alpha \mapsto (\chi \mapsto \mathrm{inv}_K(\chi, \alpha)) \mapsto \sigma$, has kernel containing the norm map. For that, since the last homomorphism is the evaluation isomorphism from Pontrjagin's duality and since in finite abelian groups $\bigcap_{\chi\in G^*}\ker\chi = 1$, it is enough to check that the cyclic algebras $(\chi, N_{L/K}(L^\times))$ are trivial in $\mathrm{Br}(K)$ for any character $\chi \in \mathrm{Gal}(L/K)^*$. Let K_χ the cyclic extension corresponding to the character χ. Then, by Theorem 3.12, $(\chi, N_{K_\chi/K}(K_\chi^\times)) = 0$ in $\mathrm{Br}(K)$. But, by the transitive property of the norm, we get $N_{L/K}(L^\times) = N_{K_\chi/K}(N_{L/K_\chi}(L^\times)) \subseteq N_{K_\chi/K}(K_\chi^\times)$ and the induced map $K^\times/N_{L/K}(L^\times) \to \mathrm{Gal}(L/K)$ is well defined.

For injectivity it is enough to prove the inequality $|K^\times/N_{L/K}(L^\times)| \leq |\mathrm{Gal}(L/K)|$ once we prove it is onto. Note for two field extensions $K \subseteq E \subseteq L$, $N_{L/K} = N_{L/E}N_{E/K}$. Then, $E^\times/N_{L/E}(L^\times) \overset{N_{E/K}}{\to} K^\times/N_{L/K}(L^\times)$ is well defined and the sequence

$$E^\times/N_{L/E}(L^\times) \overset{N_{E/K}}{\to} K^\times/N_{L/K}(L^\times) \to K^\times/N_{E/K}(E^\times) \to 1$$

is exact. Then, $|K^\times/N_{L/K}(L^\times)| \leq |E^\times/N_{L/E}(L^\times)||K^\times/N_{E/K}(E^\times)|$, showing it is enough to consider finite extensions of prime degree by induction on the prime factors of $[L:K]$. But, in this case the extension is cyclic and combining Theorem 3.12 and previous proposition $|K^\times/N_{L/K}(L^\times)| = |\mathrm{Br}(L/K)| = [L:K] = |\mathrm{Gal}(L/K)|$, which implies $|K^\times/N_{L/K}(L^\times)| \leq |\mathrm{Gal}(L/K)|$ for a separable extension L/K. Hence, we are only left to prove it is onto to obtain an isomorphism. For that, we have seen in Section 1.4 that this homomorphism will be onto if the only character annihilating its image is the trivial character. Such a character must satisfy $(\chi, K^\times) = 0$ in $\mathrm{Br}(K)$ by definition. Then, by Theorem 3.12 we have $\mathrm{Br}(K_\chi/K) = 0$ and by the second assertion in Proposition 4.2, we have the formula $[K_\chi : K] = |\mathrm{Br}(K_\chi/K)| = 1$; thus, $K_\chi = K$ and $\chi = 0$ proving surjectivity. □

Now, note that for any finite Galois extensions $M \subseteq L$ of K, the diagram

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

commutes where the horizontal arrows are precisely the ones defined in the previous proposition and the left vertical arrow is a usual projection since $N_{L/K}(L^\times) \subseteq N_{M/K}(M^\times)$. Then, the isomorphisms from the previous Proposition are compatible with the connection homomorphisms and by the universal property of the inverse limit they induce a homomorphism $\rho_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$, $\alpha \mapsto \sigma := (\sigma_L)_L$. This is the celebrated homomorphism of local class field theory. We shall show it has the properties described in Theorem 4.1.

Proposition 4.4. *Let K be a complete discrete valuation field with finite residue field. Then, ρ_K has the property (b) in Theorem 4.1(1).*

Proof. Let us see commutativity of the diagram for a prime element π since $K^\times$ is generated by prime elements. The valuation of a prime element is 1 and 1 generates $\mathbb{Z}$ as a group and $\mathrm{Gal}(\mathbb{F}_q^{ab}/\mathbb{F}_q)$ is isomorphic to the procyclic profinite completion of $\mathbb{Z}$, $\widehat{\mathbb{Z}}$, generated topologically by the Frobenius automorphism $x \mapsto x^q$. Then, the image of the prime π through the composite $\nu_K \rho_{\mathbb{F}_q}$ is the Frobenius automorphism in $\mathrm{Gal}(\mathbb{F}_q^{ab}/\mathbb{F}_q)$. On the other way, the image of π through ρ_K satisfies $\chi(\rho_K(\pi)) = \mathrm{inv}_K(\chi, \pi) = 1/n + \mathbb{Z}$ for each unramified character χ, where n is the index of the kernel of χ in $\mathrm{Gal}(K^{ab}/K)$. This element of the bidual is mapped via the evaluation isomorphism to an automorphism σ in $\mathrm{Gal}(K^{ab}/K)$ such that $\chi(\sigma) = 1/n + \mathbb{Z}$ for each unramified character, i.e. it induces generators in each cyclic unramified extension K_χ; thus, its restriction is a generator of $\mathrm{Gal}(K^{ur}/K)$, which is mapped to the Frobenius automorphism in $\mathrm{Gal}(\mathbb{F}_q^{ab}/\mathbb{F}_q)$ by the canonical isomorphism $\mathrm{Gal}(K^{ur}/K) \cong \mathrm{Gal}(\mathbb{F}_q^{ab}/\mathbb{F}_q)$, proving commutativity of the diagram. □

Proposition 4.5. *For a local field K, ρ_K is continuous.*

Proof. Assume for simplicity char $K = 0$. Since $\mathrm{Gal}(K^{ab}/K)$ is a profinite group, to check continuity of the map $\rho_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$ it is enough to show continuity of each induced map $K^\times \to \mathrm{Gal}(L/K)$, by the universal property of the inverse limit noting we are working over the category of topological groups. Since each finite Galois group is discrete, it is enough to check the kernel is open by Lemma 1.2. Since the kernel is of finite index for the image group being finite, it follows from Proposition 2.18 it is open. □

Remark. We assumed K to be of null characteristic in order to apply Proposition 2.18.

Now, we show the map ρ_K is unique in the sense of Theorem 4.1.

Proposition 4.6. *Let $\tilde{\rho} : K^\times \to \mathrm{Gal}(K^{ab}/K)$ be an homomorphism satisfying,*

1. *Let L be a cyclic extension of K. Then, the composite map,*

$$K^\times \xrightarrow{\tilde{\rho}} \mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(L/K),$$

   maps $\mathrm{N}_{L/K}(L^\times)$ to $\{1\}$.

2. *Let L be a finite unramified extension of K. Then, the image of a prime by the same composite map of (1), is a generator of the cyclic Galois group.*

Then, $\tilde{\rho} = \rho_K$.

Proof. As before, it is enough to prove $\rho'(\pi) = \rho_K(\pi)$ for prime elements $\pi \in K^\times$, as they generate the group of units. We shall see $\chi(\rho'(\pi)) = \chi(\rho_K(\pi))$ for all χ, which is easier to check and implies previous equality since the isomorphism in Pontrjagin's duality is the evaluation isomorphism. Let n be the order of $\chi(\rho_K(\pi))$. Let K_n/K be the unique unramified extension of degree n. Then, $\rho_K(\pi)$ restricts to a generator of $\mathrm{Gal}(K_n/K)$. Hence, there is some unramified character $\psi \in X(K)$ such that $\psi(\rho_K(\pi)) = \chi(\rho_K(\pi))$. Now, let L/K be the cyclic extension corresponding to the character $\psi - \chi$. Then, the composite $K^\times \overset{\rho_K}{\to} \mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(L/K)$ maps π to 1. Thus, by Proposition 4.4, π is in the norm group $N_{L/K}(L^\times)$. By the first property of ρ', $\rho'(\pi)$ maps to 1 too, and we obtain $(\psi - \chi)(\rho'(\pi)) = 0$. By the second property, $\psi(\rho'(\pi)) = \psi(\rho_K(\pi))$ and we have the equality

$$\chi(\rho'(\pi)) = \psi(\rho'(\pi)) = \psi(\rho_K(\pi)) = \chi(\rho_K(\pi)),$$

concluding the proof. □

Now, to conclude we need to prove there is a one-to-one correspondence between abelian extensions and open subgroups of finite index of the group of units of the base field. We have seen this is equivalent to having a one-to-one correspondence between open subgroups of finite index in $\mathrm{Gal}(K^{ab}/K)$ and open subgroups of finite index in $K^\times$. For a profinite abelian group G, we claim its open subgroups of finite index are in one-to-one correspondence with the finite subgroups of its character group G^* given via the assignments $H \leq G \mapsto \varphi(H) := \{\chi \in G^* : \chi_H = 0\}$ and $H \leq G^* \mapsto \psi(H) := \bigcap_{\chi \in H} \ker \chi$ (see Problem A.13). Thus, if we set $X(K^\times) := \hom_{\mathrm{cont}}(K^\times, \mathbb{Q}/\mathbb{Z})$, it is sufficient to prove there is an isomorphism $X(K) \cong X(K^\times)$ given by the assignment $\chi \mapsto \rho_K \chi$. To prove injectivity, just note that the composite $K^\times \overset{\rho_K}{\to} \mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(L/K)$ is surjective for all abelian extensions L/K; thus, since taking the dual $\hom_{\mathrm{cont}}(-, \mathbb{Q}/\mathbb{Z})$ is a contravariant functor mapping an exact sequence $K^\times \to \mathrm{Gal}(L/K) \to 0$ to an exact sequence $0 \to \mathrm{Gal}(L/K)^* \to X(K^\times)$, this inclusion is injective for the duals of each finite Galois groups; hence, for the dual of the Galois group $\mathrm{Gal}(K^{ab}/K)$ too. Now, we prove surjectivity.

First, we shall check L^{ab} is an extension of K^{ab} for any separable extension L/K. By definition, it is enough to see K^{ab}/L is an abelian extension. Note that $\mathrm{Gal}(K^{ab}/K)$ is abelian and $\mathrm{Gal}(K^{ab}/L)$ is one of its subgroups; thus it is abelian too. This shows the restriction $\mathrm{Gal}(L^{ab}/L) \to \mathrm{Gal}(K^{ab}/K)$ given by the usual restriction of automorphisms is well defined. Then, we may define a natural map $X(K) \to X(L)$ by plugging the Galois group of the maximal abelian extension of L through the usual restriction in the left hand side, i.e. $\chi \mapsto \chi_L := \pi_{L/K}\chi$ where $\pi_{L/K}$ denotes this restriction.

Proposition 4.7. *Let K be a local field and L a finite separable extension of K. Then, the diagram*

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

is commutative, where the right vertical map is the homomorphism obtained by restriction of automorphisms of L^{ab} to K^{ab}.

Proof. Let K be a complete valuation field with finite residue field, since the real and complex cases are easy to check and thus left to the reader. Note that, as before, it is sufficient to prove $\mathrm{inv}_K(\chi, N_{L/K}(\pi)) = \mathrm{inv}_L(\chi_L, \pi)$ for all $\chi \in X(K)$, where χ_L denotes the image of χ by the inclusion map $X(K) \to X(L)$. Let f be the residue degree of the extension L/K. Then, we may choose an unramified element $\psi \in X(\mathbb{F}_{q^f}) \subseteq X(L)$ such that $(\psi, \pi) = (\chi_L, \pi)$. Note such an element exists since all the classes of the Brauer group contain such an element. Now, since the multiplication by f map $\mathbb{Q}/\mathbb{Z} \cong X(\mathbb{F}_q) \to X(\mathbb{F}_{q^f}) \cong \mathbb{Q}/\mathbb{Z}$ is surjective we may choose an unramified element $\varphi \in X(\mathbb{F}_q) \subseteq X(K)$ such that $\varphi_L = \psi$. Let L'/L be the cyclic extension corresponding to $\varphi_L - \chi_L$. Since $(\varphi_L - \chi_L, \pi) = 0$, π is a norm element by the main property of cyclic algebras, i.e. $\pi = N_{L'/L}(b)$ for some $b \in (L')^{\times}$. Now, consider the cyclic extension K'/K corresponding to the character $\varphi - \chi$. Since $(\varphi - \chi)_{L'} = 0$, $K' \subseteq L'$. Thus, by transitivity of the norm,

$$N_{L/K}(\pi) = N_{L/K}(N_{L'/L}(b)) = N_{L'/K}(b) = N_{K'/K}(N_{L'/K'}(b)) \in N_{K'/K}((K')^{\times}).$$

Thus, $(\varphi - \chi, N_{L/K}(\pi)) = 0$ and we get

$$\begin{aligned}
\mathrm{inv}_K(\chi, N_{L/K}(\pi)) &= \mathrm{inv}_K(\varphi, N_{L/K}(\pi)) \\
&= \nu_K(N_{L/K}(\pi))(\text{image of } \varphi \text{ by } X(\mathbb{F}_q) \overset{\cong}{\to} \mathbb{Q}/\mathbb{Z}) \\
&= f \cdot (\text{image of } \varphi \text{ by } X(\mathbb{F}_q) \overset{\cong}{\to} \mathbb{Q}/\mathbb{Z}) \\
&= (\text{image of } \varphi_L \text{ by } X(\mathbb{F}_{q^f}) \overset{\cong}{\to} \mathbb{Q}/\mathbb{Z}) \\
&= \mathrm{inv}_L(\varphi_L, \pi) = \mathrm{inv}_L(\chi_L, \pi),
\end{aligned}$$

where ν_K is the discrete valuation of K and second and fifth equalities follow from Proposition 4.4, third from Proposition 2.17 and π being a prime element in L and fourth equality from the map $X(\mathbb{F}_q) \to X(\mathbb{F}_{q^f})$ being multiplication by f. This concludes the proof. □

Lemma 4.8. *Let K be a local field of characteristic 0. Then,*

1. *For $n \in \mathbb{N}$, let $X_n(K) := \{\chi \in X(K) \ : \ n\chi = 0\}$ and $X_n(K^{\times}) := \{\chi \in X(K^{\times}) \ : \ n\chi = 0\}$. If K contains a primitive nth root of unity, we have an isomorphism $X_n(K) \overset{\cong}{\to} X_n(K^{\times})$, given by $\chi \mapsto \rho_K\chi$.*

2. Let L be a finite extension of K and $\chi \in X(K^\times)$. If $N_{L/K}\chi \in X(L^\times)$ lies in the image of $X(L) \to X(L^\times)$, χ lies in the image of $X(K) \to X(K^\times)$.

Proof. Let us prove first the first assertion. We shall see the sequence of maps

$$K^\times/(K^\times)^n \to X_n(K) \to X_n(K^\times),$$

is a sequence of injective maps and that $K^\times/(K^\times)^n$ and $X_n(K^\times)$ are finite and have same order, implying the desired isomorphism $X_n(K) \cong X_n(K^\times)$. Note the second map is given by $\chi \mapsto \rho_K\chi$, i.e. it is obtained by plugging the group $K^\times$ in the left hand side.

Let K contain a primitive nth root of unity ζ_n. Then, $K(\sqrt[n]{a})$ is an abelian extension for any $a \in K^\times$. Thus, we may define a group homomorphism $K^\times \to X_n(K)$ via the assignment $a \mapsto \chi_a$ where $\chi_a(\sigma) = r/n$ and r is chosen such that $\sigma(\sqrt[n]{a}) = \zeta_n^r \sqrt[n]{a}$. This is a well-defined group homomorphism and note that $\chi_a = 0$ for all $a \in (K^\times)^n$; thus, it induces a group homomorphism $K^\times/(K^\times)^n \to X_n(K)$. We shall see it is injective, it is actually an isomorhism by Kummer Theory but we just need injectivity for our means. For that, we see the kernel is trivial. For $a \in K^\times$ and $\chi_a = 0$, we have $\sqrt[n]{a}$ is fixed by the Galois group, i.e. it is in $K^\times$; hence, $a \in (K^\times)^n$ and the kernel is trivial proving injectivity. We show in Proposition 2.18 that $[K^\times : (K^\times)^n]$ is finite; thus, the quotient group is finite. Since $X_n(K^\times)$ can be identified with $X(K^\times/(K^\times)^n)$ via $\chi(k) \leftrightarrow \chi(k(K^\times)^n)$ and the character group of a finite abelian group has same order as the group itself since they are isomorphic, although not naturally, we obtain the desired isomorphism.

Now we prove the second assertion of the lemma. By transitivity of the norm, it is sufficient to consider intermediate fields of the finite abelian extension L/K, i.e. we may assume without loss of generality that L/K is cyclic. Let $G := \mathrm{Gal}(L/K)$ and consider the action of G over the groups $X(L)$ and $X(L^\times)$ defined by $\sigma\chi : \mathrm{Gal}(L^{ab}/L) \to \mathbb{Q}/\mathbb{Z}$, $\tau \mapsto \chi(\tilde{\sigma}^{-1}\tau\tilde{\sigma})$, where $\tilde{\sigma}$ is an element of $\mathrm{Gal}(L^{ab}/K)$ whose image in $\mathrm{Gal}(L/K)$ is σ for $\chi \in X(L)$; and $\sigma\chi = \sigma^{-1}\chi$ for $\chi \in X(L^\times)$ respectively for each $\sigma \in G$. Now, let $\chi_1 \in X(K^\times)$ and assume $N_{L/K}\chi_1 \in X(L^\times)$ is the image of $\chi_2 \in X(L)$. Recall from previous chapter that we write M^G for the elements of a G-module M invariant under the G-action. Then, clearly $N_{L/K}\chi_1 \in X(L^\times)^G$, since Galois conjugates have the same norm. Note the map $X(L) \to X(L^\times)$ is a homomorphism of G-modules, this is easy and left to the reader, and injective; thus, neccesarily $\chi_2 \in X(L)^G$ noting that $\sigma N_{L/K}\chi_1 = N_{L/K}\chi_1$ and using injectivity to obtain $\sigma\chi_2 = \chi_2$. Now let us prove $X(L)^G$ is contained in the image of the map $X(K) \to X(L)$, $\chi \mapsto \chi_L$. Let σ be a generator of G and fix an element $\tilde{\sigma}$. Then, if p is the order of G any element of the group $\mathrm{Gal}(L^{ab}/K)$ can be uniquely written as $h\tilde{\sigma}^j$ for some $h \in \mathrm{Gal}(L^{ab}/L)$ and some $j = 0, 1, \ldots, p-1$ since $\mathrm{Gal}(L^{ab}/K) \cong \mathrm{Gal}(L^{ab}/L) \times \mathrm{Gal}(L/K)$. Now, for $\chi \in X(L)^G$, choose an element $s \in \mathbb{Q}/\mathbb{Z}$ such that $\chi(\sigma) = ps$ and define the map $\chi' := \mathrm{Gal}(L^{ab}/K) \to \mathbb{Q}/\mathbb{Z}$ via the assignment $\tau = h\tilde{\sigma}^j \mapsto \chi(h) + js$. This map is clearly a group homomorphism (note $\mathrm{Gal}(L^{ab}/K)$ is abelian and thus it is easily verified $\chi'(\tau\rho) = \chi'(\tau)\chi'(\rho)$) and it induces a map $\mathrm{Gal}(K^{ab}/K) \to \mathbb{Q}/\mathbb{Z}$ and it can be regarded as an element of $X(K)$ and its image χ'_L coincides with χ. For that, note that any automorphism $\tau \in \mathrm{Gal}(L^{ab}/L)$ has $j = 0$ in the above form; thus, $\chi'_L(\tau) = \chi(\tau)$ and $\chi'_L = \chi$. Thus, the homomorphism $X(K) \to X(L)^G$ is surjective and there exists an element $\chi_3 \in X(K)$ such that $(\chi_3)_L = \chi_2$. From previous proposition $\rho_K\chi_3$ and χ_1 map to the same element in $X(L^\times)$ via $N_{L/K}$; thus, $\chi_1 - \rho_K\chi_3$ annihilates $N_{L/K}(L^\times)$. Hence, the composition $\chi_4 : \mathrm{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z}$ of $\chi_1 - \rho_K\chi_3 : K^\times/N_{L/K}(L^\times) \to \mathbb{Q}/\mathbb{Z}$ and the induced isomorphism $K^\times/N_{L/K}(L^\times) \cong \mathrm{Gal}(L/K)$ can be seen as an element of $X(K)$ and we have $\chi_1 = \rho_K(\chi_3 + \chi_4)$, i.e. χ_1 lies in the image of $X(K) \to X(K^\times)$ concluding the proof. □

Now, assuming char $K = 0$ let $\chi \in X(K^\times)$. We shall see it lies in the image of $X(K) \to X(K^\times)$. Note both groups are torsion; thus, let n be the order of χ. We shall assume K contains an nth primitive root of unity, since $K(\zeta_n)/K$ is a finite abelian extension, and by Lemma 4.8.2 all cases are reduced to this one. Then, by Lemma 4.8.1, the map $X_n(K) \to X_n(K^\times)$, $\chi' \mapsto \rho_K\chi'$ is an isomorphism for all natural n and surjectivity follows and we are done with the proof of the local class field theory. As usual, these isomorphisms are compatible with usual inclusions whenever n divides m and we obtain an isomorphism of the direct limits, i.e. $X(K) \cong X(K^\times)$, concluding the proof of Theorem 4.1.

To conclude, I would like to highlight again the astonishing beauty of local class field theory: how local fields encode the data of all their finite abelian extensions in their inner arithmetic in a rather unexpected but simple way. This is a nice representative of the charm of algebra and number theory: objects may seem to be so distant from each other but happen to be linked in an out of the blue but easy way. And, generation after generation more of these links are developed and we realize that even if we thought we fully understood a theory, we were just scratching the surface of a whole new world making you to keep learning constantly, which, for me, is the most captivating aspect of the queen of mathematics.

Appendix A

Solved Problems

A.1 Preliminaries

Problem A.1. Show the Krull topology and the profinite topology need not coincide.

Solution. We shall follow the procedure in [Mil20]. It is enough to show there is some Galois group with at least one subgroup of finite index non-open. Let $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and the intermediate field $E := \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \dots, \sqrt{p}, \dots)$. Then, it is an easy exercise to check $G := \mathrm{Gal}(E/K) = \varprojlim \mathrm{Gal}(\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \dots, \sqrt{p})/\mathbb{Q})$ and since each finite Galois group is a finite product of groups $\mathbb{Z}/2\mathbb{Z}$, G is a closed subgroup of the direct product of a countable number of groups $\mathbb{Z}/2\mathbb{Z}$. Now, consider the subgroup N of G of tuples with only a finite number of non-trivial components, i.e. a direct sum of a countable number of groups $\mathbb{Z}/2\mathbb{Z}$. Also, it is clearly dense in G and we may make the quotient $\Gamma := G/N$, which is a vector space over $\mathbb{F}_2$. Then, by Zorn's Lemma Γ contains a maximal set of linearly independent vectors, which is necessarily a basis. Then, take n elements out of the basis and define the subspace spanned by the remaining set as G_n. Then, Γ/G_n is of dimension n over $\mathbb{F}_2$, i.e. of index 2^n in Γ. If G_n were open in Γ, it would be closed too, but that it is impossible since N is dense in G. Then, G_n is of finite index and non-open, proving our claim. □

A.2 Global and local fields

Problem A.2. Let A be a complete valuation ring and $\mathfrak{m}$ its unique maximal ideal. Then, $A \cong \varprojlim_n A/\mathfrak{m}^n$ as topological rings.

Proof. We shall see the canonical map $\varphi : A \to \varprojlim_n A/\mathfrak{m}^n$ is an isomorphism. It is clearly a ring homomorphism. Thus, since the kernel is $\bigcap_{n\geq 1} \mathfrak{m}^n = 0$, it is injective. To check surjectivity, note that an element $s \in \varprojlim_n A/\mathfrak{m}^n$ is given by an infinite tuple $s = (s_n)$ where

$$s_n = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1},$$

for a_i are taken in a set of representatives of the cosets and π a uniformizer of A. Thus, (s_n) is nothing but the image by φ of the element $\sum_{n\geq 0} a_n\pi^n \in A$. Hence, φ is bijective and an isomorphism of rings.

We are left to see it is continuous for it to be a homemorphism too. It is enough to check that the basis of neighborhoods $\mathfrak{m}^n$ of 0 in A are mapped to a basis of neighborhoods of 0 in $\varprojlim_n A/\mathfrak{m}^n$. Since the open sets $N_n = \prod_{k\geq n} A/\mathfrak{m}^k$ form a basis of neighborhoods of 0 in $\prod_{n\geq 1} A/\mathfrak{m}^k$ and $\varphi(\mathfrak{m}^n) = N_n \cap \varprojlim_n A/\mathfrak{m}^n$, φ is continuous and thus an homemorphism. □

Problem A.3. Let A be a complete valuation ring and $\mathfrak{m}$ its unique maximal ideal. Then, $\mathfrak{m}^n/\mathfrak{m}^{n+1} \cong A/\mathfrak{m}$.

Proof. Note the elements $a \in A$ may be written as the sums

$$a = \sum_{n\geq 0} a_n\pi^n,$$

where a_n are taken in a set of representatives of the cosets and π is a uniformizer of A. The elements of the ideal $\mathfrak{m}^n$ are the sums

$$m_n = \sum_{k\geq n} a_k\pi^k.$$

Thus, the elements in $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ are of the form $a_n\pi^n + \mathfrak{m}^{n+1}$ and are in a clear one-to-one correspondence with the elements in the residue field (given by the canonical epimorphism) proving the result. □

Problem A.4. The residue field of a global field K is finite.

Proof. Let first K be a global function field. Then, $K = \mathbb{F}_q[t]$ and it is a principal ideal domain (PID) and a nonzero prime ideal is a maximal ideal given by a nonzero irreducible polynomial f. Then

$$\frac{\mathbb{F}_q[t]}{(f)} = \{a_0 + a_1 t + \cdots + a_{n-1}t^{n-1} : a_i \in \mathbb{F}_q\} \cong \mathbb{F}_{q^n},$$

where $n = \deg f$. Hence, the residue field is finite as it is a finite dimensional vector space over a finite field.

Now, let K be a number field, i.e. a finite extension of $\mathbb{Q}$. Then, $\mathcal{O}_K$ is finite dimensional over $\mathbb{Z}$. Thus, it is enough to show that for any positive prime integer p, and $\nu = \operatorname{ord}_p$, the residue field $\mathcal{O}_\nu/\mathfrak{p}$ is finite where $\mathcal{O}_\nu = \mathbb{Z}_{(p)}$ (i.e. the localization of $\mathbb{Z}$ at the prime ideal (p)) and $\mathfrak{p} = p\mathbb{Z}_{(p)}$. We shall see $\mathcal{O}_\nu/\mathfrak{p} = \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{F}_p$. This follows directly from the following Lemma. □

Lemma A.5. *Let A be a commutative ring and $\mathfrak{m}$ be a maximal ideal. Then, $A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m} \cong A/\mathfrak{m}$.*

Proof. Since $\mathfrak{m}$ is maximal, $A/\mathfrak{m}$ is a field and any $k \in A \setminus \mathfrak{m}$ is a unit in the quotient. Then, the map

$$\begin{aligned}\varphi : A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m} &\to A/\mathfrak{m}\\ \frac{a}{k} + \mathfrak{m}A_\mathfrak{m} &\mapsto ak^{-1} + \mathfrak{m},\end{aligned}$$

is well defined since for two representatives $a/k + \mathfrak{m}A_\mathfrak{m} = b/l + \mathfrak{m}A_\mathfrak{m}$, we get their images $ak^{-1} + \mathfrak{m} = bl^{-1} + \mathfrak{m}$ noting

$$ak^{-1} - bl^{-1} = (al - bk)k^{-1}l^{-1} \in \mathfrak{m}.$$

It is indeed a ring homomorphism since

$$\begin{aligned}\varphi\left(\frac{a}{k} + \frac{b}{l} + \mathfrak{m}A_\mathfrak{m}\right) &= (al + bk)k^{-1}l^{-1} = ak^{-1} + bl^{-1}\\ &= \varphi\left(\frac{a}{k} + \mathfrak{m}A_\mathfrak{m}\right) + \varphi\left(\frac{b}{l} + \mathfrak{m}A_\mathfrak{m}\right).\end{aligned}$$

For the product it is straightforward to check it too.

The homomorphism φ is clearly surjective since for any $a + \mathfrak{m} \in A/\mathfrak{m}$ we have $\varphi(a + \mathfrak{m}A_\mathfrak{m}) = a + \mathfrak{m}$.

To check injectivity, we compute the kernel of the homomorphism, which is easily computed noting

$$\varphi\left(\frac{a}{k} + \mathfrak{m}A_\mathfrak{m}\right) = \mathfrak{m} \implies ak^{-1} \in \mathfrak{m}.$$

Since $\mathfrak{m}$ is an ideal, $ak^{-1}k = a \in \mathfrak{m}$ and consequently, $a/k \in \mathfrak{m}A_\mathfrak{m}$, i.e. $\ker\varphi \subseteq \mathfrak{m}A_\mathfrak{m} = \{\overline{0}\}$, and φ is injective. Thus, φ is an isomorphism as wanted. □

Remark. We only needed φ to be an injective map, since such a map would give us the inequality in the orders of the fields necessary to prove finiteness of the one in the left hand side.

A.3 The Brauer group

Problem A.6 (Explicit construction of the tensor product). Let A and B be two k-algebras. Then, give an explicit construction of the tensor product $A \otimes_k B$.

Solution. Let $F(A \times B)$ be the free abelian group with basis all elements in the cartesian product $A \times B$ denoted by $a * b$. We shall define the normal subgroup N generated by the elements of the form:

1. $-a * (b + b') + a * b + a * b'$,
2. $-(a + a') * b + a * b + a' * b$,
3. $-(a \cdot \lambda) * b + a * (\lambda \cdot b)$,

where $a, a' \in A$, $b, b' \in B$ and $\lambda \in k$. This subgroup N has been chosen so that the natural map

$$\otimes_k : A \times B \to F(A \times B)/N,$$

is a balanced product. What is more, it has been chosen minimal satisfying this property; hence we shall show the pair $(F(A\times B)/N, \otimes_k)$ satisfies the universal property of the tensor product. For that, recall the universal property of free modules. Let $A \times B$ be a basis for the k-module $F(A \times B)$, then, the inclusion map $\iota : A\times B \to F(A\times B)$ is universal in the sense that any arbitrary function $\varphi : A \times B \to C$ to another k-module C factors through $\mathrm{ev}_\varphi : F(A \times B) \to C$ where this module homomorphism is obtained by $\sum_i \lambda_i v_i \mapsto \sum_i \lambda_i \varphi(v_i)$, i.e. evaluating the function φ on the basis $A\times B$. Also, recall the universal property of the quotient of abelian groups. Given an abelian group G and a normal subgroup N, any group homomorphism $\varphi : G \to H$ for an abelian group H such that $N \subseteq \ker \varphi$, factors through π_N, i.e. there exists a unique group homomorphism $\psi : G/N \to H$ such that $\varphi = \pi_n \psi$. Putting all of this together, we see if (C, f) is another balanced product, then, the following diagram,

$$\begin{tikzcd}
A \times B \arrow[r, "\iota"] \arrow[dr, "f"'] & F(A \times B) \arrow[r, "\pi_N"] \arrow[d, "\mathrm{ev}_f"] & F(A \times B)/N \arrow[dl, "\eta"] \\
& C &
\end{tikzcd}$$

commutes, since clearly $N \subseteq \ker \mathrm{ev}_f$ by the choice of N and thus, η is unique and gives the desired morphism on the universal property of the tensor product, by noting $\otimes_k = \iota\pi_N$. It is only left to check it is a k-algebra (we have proved it is a k-module), but this is straightforward to do if we define the natural product on $F(A \times B)/N$, $[a * b][a' * b'] = [(a \cdot a') * (b \cdot b')]$. □

Problem A.7. Let M be an irreducible module over a ring R. Then, $M \cong R/\mathfrak{m}$ for a maximal ideal $\mathfrak{m}$ of R. In particular, if R is simple, any two nontrivial irreducible modules over R are isomorphic.

Proof. Let $m \in M \setminus \{0\}$ and consider the corresponding nonzero submodule $Rm \subseteq M$. Since M is irreducible, necessarily, $Rm = M$, i.e. it is cyclic. Thus, $M \cong R/\mathfrak{a}$ for $\mathfrak{a} := \mathrm{Ann}_R(m)$. To see that, note the canonical homorphism

$r \mapsto rm$ is clearly onto and has kernel $\mathrm{Ann}_R(m)$. Now, since the ideals in $R/\mathfrak{a}$ are in one to one correspondence with the nontrivial R-submodules of M and M is irreducible, we must have $\mathfrak{a}$ is maximal as wanted. Lastly, if R is simple, the only possibility is $M \cong R$ if M is taken to be non-trivial; hence, all such R-modules must be isomorphic. □

Problem A.8. For a central simple algebra A and an n-dimensional A^{op}-vector space V we have the isomorphism $\mathrm{End}_{A^{op}}\, V \cong M_n(A)$.

Proof. An endomorphism is completely determined by its image on an A-basis. Let us fix an A-basis β and let M be the matrix whose columns are precisely the images of the elements of β of a given endomorphism φ. We check A^{op}-linearity and leave the rest of the properties that make this map an isomorphism to the reader since they are analogous to those in linear algebra. Let us denote the product on A^{op} via $*$. We shall check $\varphi(a * v) = a * \varphi(v) = a * (Mv)$. For that, note

$$\varphi(a*v) = M\begin{pmatrix} a*v_1 \\ \vdots \\ a*v_n \end{pmatrix} = \begin{pmatrix} m_{11}a*v_1 + \cdots + m_{1n}a*v_n \\ \vdots \\ m_{n1}a*v_1 + \cdots + m_{nn}a*v_n \end{pmatrix}$$

$$= \begin{pmatrix} m_{11}v_1a + \cdots + m_{1n}v_na \\ \vdots \\ m_{n1}v_1a + \cdots + m_{nn}v_na \end{pmatrix} = (Mv)a = a*(Mv) = a*\varphi(v),$$

proving our claim. □

Problem A.9. Proof of Theorem 3.8.

Proof. Let $m \in M^G$, $n = |G|$ and f_m be the cochain defined as,

$$f_m(\sigma^i, \sigma^j) := \begin{cases} 1, & i+j < n, \\ m, & i+j \geq n. \end{cases}$$

It is straightforward to check f_m satisfies the 2-cocycle condition,

$$f_m(\sigma^i, \sigma^j) f_m(\sigma^{i+j}, \sigma^k) = (\sigma^i f_m(\sigma^j, \sigma^k)) f_m(\sigma^i, \sigma^{j+k}).$$

Just classify the possible choices of i, j, k depending upon their pairwise sums and their total sum is lesser than n or not, and check in all possible choices the 2-cocycle condition is satisfied. Note for these computations that if $i + j \geq n$, then $\sigma^{i+j} = \sigma^{i+j \mod n}$. A cocycle of this form is called a *normalized* cocycle.

Now, we can define a map $\varphi : M^G \to H^2(G, M)$ such that $m \mapsto f_m$, which is clearly a group homomorphism by the definition of f_m.

We claim $\ker\varphi = N(G)$ and Im $\varphi = H^2(G, M)$.

For the first part, we show that f_m and f_l are cohomologous if and only if $m/l \in N(G)$. For f_m and f_l to be cohomologous there must exist $c_i \in M$ such that $f_m(\sigma^i, \sigma^j) = f_l(\sigma^i, \sigma^j)c_i\sigma^i(c_i)c_{i+j}^{-1}$. For the only if part, recall that $N(c_1) = \prod \sigma^i(c_1)$. Thus, by the 2-coboundary condition,

$$f_m(\sigma^i, \sigma^j) = f_l(\sigma^i, \sigma^j)c_i\sigma^i(c_j)c_{i+j}^{-1},$$

and taking the product over all i and fixing $j = 1$,

$$\prod_i f_m(\sigma^i, \sigma) = \prod_i f_l(\sigma^i, \sigma)c_i\sigma^i(c_1)c_{i+1}^{-1} \implies \quad m = l\prod_i c_i\sigma^i(c_1)c_{i+1}^{-1}$$
$$\implies \frac{m}{l} = \prod_i \sigma^i(c_1).$$

Hence, $m/l \in \mathrm{N}(G)$ as claimed. For the converse, let $m \in N(G)$. Then, by a little abuse of notation define $f_m := f_{\prod \sigma^k(m)}$. We shall see f_m satisfies the coboundary condition $f_m(\sigma^i, \sigma^j) = c_i\sigma^i(c_j)c_{i+j}^{-1}$ for some $c_i \in M$. Let

$$c_i := \prod_{k=1}^{i \bmod n} \sigma^k(m).$$

Then, it is straightforward to check f_m satisfies the coboundary condition.

For the second part, we show any cocycle $f \in Z^2(G, M)$ is cohomologous to a normalized cocycle f_m for $m = \prod_i^{n-1} f(\sigma^i, \sigma)$, i.e. there exist c_i such that $f_m(\sigma^i, \sigma^j) = f(\sigma^i, \sigma^j)c_i\sigma^i(c_j)c_{i+j}^{-1}$. For that, let $c_0 = c_1 := 1$ and $c_i := \prod_j^{i-1} f(\sigma^j, \sigma)^{-1}$ for $1 < i < n$. Then, the reader can check the 2-coboundary condition is satisfied and that $m \in M^G$ using the 2-cocycle condition (hint: prove it for $j = 1$ and then use induction). Thus, by the First Isomorphism Theorem for groups, we obtain the desired isomorphism $H^2(G, M) \cong M^G/\mathrm{N}(G)$. □

Problem A.10 (Dedekind independence theorem). Distinct characters of a group[1] into a field are linearly independent, i.e. if $\chi_1, \dots, \chi_n$ are distinct characters of a group H into a field F, then the only elements $a_1, \dots, a_n \in F$ such that

$$a_1\chi_1(h) + \cdots + a_n\chi_n(h) = 0, \tag{A.1}$$

for all $h \in H$ are $a_1 = \cdots = a_n = 0$.

[1] We shall just use this theorem once for a group, but we could have replaced *group* with *monoid* flawlessly.

Proof. For $n = 1$ the result is clear since otherwise, $a\chi(h) = 0$ for all $h \in H$ with $a \neq 0$ implies $\chi(h) = 0$ for all $h \in H$ for F being an integral domain, which is a clear contradiction since $\chi(1) = 1 \neq 0$ (see next remark). Now, we proceed by strong induction on n. Let $n > 1$ and assume the result true for $k < n$ characters. We shall prove the result by means of contradiction. Thus, suppose there exist $a_i \neq 0$ satisfying (A.1), we may assume all are distinct from zero since we are assuming the result holds for $k < n$. Since $\chi_1 \neq \chi_2$, there exists an $a \in H$ such that $\chi_1(a) \neq \chi_2(a)$. Thus, let us replace h by ah in (A.1) giving us the relation

$$a_1\chi_1(a)\chi_1(h) + a_2\chi_2(a)\chi_2(h) + \cdots + a_n\chi_n(a)\chi_n(h) = 0,$$

since χ_i are characters into a field. On contrast, if we multiply the expression (A.1) by $\chi_1(a)$ we get the expression

$$a_1\chi_1(a)\chi_1(h) + a_2\chi_1(a)\chi_2(h) + \cdots + a_n\chi_1(a)\chi_n(h) = 0.$$

Substracting both expressions we get a new relation $a_2'\chi_2(h)+\cdots+a_n'\chi_n(h) = 0$ where $a_i' = a_i(\chi_i(a) - \chi_1(a))$ for $i = 2, \ldots, n$. Since $a_2' \neq 0$ this is a contradiction by the induction hypothesis, completing the proof. □

Remark. It is known that $0 = 1$ happens just in the trivial ring, i.e. when $R = \{0\}$. But, in the axiomatic definition of a field we impose all elements but 0 are units, and if we apply this to the trivial ring we see the 0 is a unit which is not appealing to us. Thus, we do not consider such a concept as a trivial field or a field of one element.

Problem A.11 (Wedderburn's Litlle Theorem). Let F be a finite field. Then, $\mathrm{Br}(F) = 0$.

Proof. We shall see that any finite division algebra Δ is commutative, i.e. a field. Thus, $\mathrm{Br}(F) = 0$ since the only possible simple central algebra over F is F itself. To prove that, let us proceed by strong induction on the order of Δ. Clearly, the center of Δ, $Z(\Delta)$, is a field, so Δ is a finite dimensional vector space over $Z(\Delta)$. Let $n := \dim_{Z(\Delta)} \Delta$ and $q := |Z(\Delta)|$. We shall see $n = 1$. Now, for any $d \in \Delta \setminus Z(\Delta)$, the ring centralizer $C_\Delta(d)$ is a division algebra and thus a field, since it is a strict subring of Δ, by induction hypothesis and it is also a vector space over $Z(\Delta)$. We may see Δ as a vector space over $C_{Z(\Delta)}(d)$ too; hence, the order of the centralizer is q^l with l a strict divisor of n by the multiplicative property of dimensions. Now, if we consider the unit groups $\Delta^\times$, $Z(\Delta)^\times$ and $C_{Z(\Delta)}(d)^\times$ we may consider the class equation

$$|\Delta^\times| = |Z(\Delta)^\times| + \sum_d |\Delta : C_{Z(\Delta)}(d)^\times| \implies q^n - 1 = q - 1 + \sum_{l|n} \frac{q^n - 1}{q^l - 1},$$

where the sum over the elements d is taken over a set of representatives of nontrivial conjugacy classes. Now, recall the polynomial identity,

$$x^n - 1 = \prod_{l|n} \Phi_l(x),$$

where Φ_l is the lth cyclotomic polynomial. Then, since all l in the class equation divide n, necessarily, $\Phi_n(q)$ divides $q-1$ and we get $|\Phi_n(q)| \leq q-1$. We shall see $|\Phi_n(q)| > q-1$ for $n > 1$; thus, forcing $n = 1$. But, this is straightforward to see. Just note that over the complex numbers we have the factorization

$$\Phi_n(x) = \prod_{i=0}^{n-1} (x - \zeta_n^i),$$

where ζ_n denotes an nth primitive root of unity. Then, evaluating it at $x = q$ and noting that for any $n > 1$ and $q \geq 2$ we have the inequality $|q - \zeta_n^i| > |q-1|$ for $i = 1, \ldots, n-1$ and the equality at $i = 0$, we get the desired result. □

Remark. This proof and a nice discussion can be found at [Art50].

A.4 Class field theory

Problem A.12. Describe the local class field homomorphism of $\mathbb{R}$ and $\mathbb{C}$.

Solution. Let us consider first $\mathbb{R}$. Then, $\mathbb{R}^{ab} = \mathbb{C}$ and $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong C_2$. The only open subgroups of finite index of $\mathbb{R}^\times$ are $\mathbb{R}_+^\times$ and itself, where the former is the one of positive real numbers. For that, note that for a subgroup H of index $n < \infty$, we have $\mathbb{R}_+^\times \leq H$ since $x = (\sqrt[n]{x})^n \in H$ for all $x \in \mathbb{R}_+^\times$; thus, H is either $\mathbb{R}_+^\times$ or $\mathbb{R}^\times$ since $\mathbb{R}_+^\times$ is of index 2. It is straightforward to see that $N_{\mathbb{R}/\mathbb{R}}(\mathbb{R}^\times) = \mathbb{R}^\times$ and $N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times) = \{|z|^2 : z \in \mathbb{C}^\times\} = \mathbb{R}_+^\times$. Thus, the only homomorphism satisfying the conditions of the Theorem 4.1 is precisely $\rho_{\mathbb{R}} : \mathbb{R}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ mapping positive real numbers to the identity and negative ones to conjugation.

The case of $\mathbb{C}$ is even easier as $\mathbb{C}^{ab} = \mathbb{C}$. Thus, the Galois group $\mathrm{Gal}(\mathbb{C}^{ab}/\mathbb{C})$ is trivial and the only possible homomorphism with image on it is the trivial one. Thus, if there is just one open subgroup of finite index in $\mathbb{C}^\times$ conditions of Theorem 4.1 are satisfied by this unique trivial homomorphism. But, this is precisely the case of $\mathbb{C}^\times$, since its only open subgroup of finite index is itself arguing by taking roots as before. Thus, local class field theory is proved for $\mathbb{R}$ and $\mathbb{C}$. □

Problem A.13. Let G be an abelian profinite group. Then, there is a one-to-one inclusion-reversing correspondence between its open subgroups of finite index and finite subgroups of its character group via the assignments $H \leq G \mapsto \varphi(H) := \{\chi \in G^* : \chi_{|H} = 0\}$ and $H \leq G^* \mapsto \psi(H) := \bigcap_{\chi \in H} \ker \chi$.

Proof. First we see these maps are well defined. For that, let $H \leq G$ be open of finite index. Then, the characters in $\varphi(H)$ are in one-to-one correspondence with the ones of G/H and since H is of finite index $|\varphi(H)| = |(G/H)^*| = |G : H| < \infty$. Now, let $H \leq G^*$ be finite. Then, $\psi(H)$ is mapped into $\bigoplus_{\chi \in H} G/\ker \chi$ and since each $G/\ker \chi$ is finite and H too, G/H is finite proving it is of finite index. Also, it is the intersection of open sets; thus, open.

Now, we shall see $\psi(\varphi(H)) = H$ and $\varphi(\psi(H)) = H$. First, let $H \leq G$ open of finite index. Clearly, $\psi(\varphi(H)) \leq H$. Should this inclusion not be an equality, the quotient $\psi(\varphi(H))/H$ would be non-trivial and there would be a character $\chi \in G^*$ such that $\chi \in \varphi(H)$ but $\chi_{|\psi(\varphi(H))} \neq 0$, which is a contradiction.

Now, let $H \leq G^*$ finite. Clearly, $H \leq \varphi(\psi(H))$. Now, $\varphi(\psi(H))$ can be identified with $(G/\psi(H))^*$ and H with a subgroup of it. But H clearly separates any two points in $G/\psi(H)$, but no proper subgroup of $(G/\psi(H))^*$ does so; thus, H cannot be proper and we get the equality $H = \varphi(\psi(H))$. □

Bibliography

[Art50] Emil Artin. The influence of J. H. M. Wedderburn on the development of modern algebra. *Bull. Amer. Math. Soc.*, 56(1):65–72, 1950.

[AT09] Emil Artin and John Tate. *Class Field Theory.* American Mathematical Society, 2009.

[FV02] I. B. Fesenko and S. V. Vostokov. *Local Fields and their Extensions.* American Mathematical Society, 2002.

[Gau01] Carl F. Gauss. *Disquisitiones Arithmeticae.* Leipzig, 1801.

[Gri07] Pierre Antoine Grillet. *Abstract Algebra.* Springer-Verlag New York, 2007.

[Hil00] David Hilbert. Mathematische probleme. vortrag, gehalten auf dem internationalen mathematiker-kongreß zu paris 1900. *Nachrichten von der Königl. Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-Physikalische Klasse*, page 253, 1900.

[Jac85] Nathan Jacobson. *Basic Algebra I.* W. H. Freeman & Co (Sd), second edition edition, 1985.

[Jac09] Nathan Jacobson. *Basic Algebra II.* Dover Publications, second edition edition, 2009.

[KKS11] Kazuya Kato, Noboshige Kurokawa, and Takeshi Saito. *Number Theory 2: Introduction to Class Field Theory.* American Mathematical Society, 2011.

[Kle03] Felix Klein. Gauß' wissenschaftliches tagebuch 1796-1814, mit anmerkungen. *Mathematische Annalen*, 57:1–34, 1903.

[Lan94] Serge Lang. *Algebraic Number Theory.* Springer-Verlag, New York, 2 edition, 1994.

[Mil17] James S. Milne. *Algebraic Number Theory* (v3.07), 2017. Available at `www.jmilne.org/math/`.

[Mil20] James S. Milne. *Fields and Galois Theory* (v4.61), 2020. Available at `www.jmilne.org/math/`.

[Mor96] P. Morandi. *Fields and Galois Theory.* Springer, New York, 1996.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory.* Springer-Verlag, 1999.

[Pon46] Leo Pontrjagin. *Topological Groups.* Princeton University Press, Princeton, 1946.

[Poo14] Bjorn Poonen. Why all rings should have a 1. ***https://arxiv.org/abs/1404.0135v1***, page 4, 2014.

[RZ10] Luis Ribes and Pavel Zalesskii. *Profinite Groups.* 2010.

[SG80] Jean-Pierre Serre and Marvin J. Greenberg. *Local Fields.* Springer, second edition edition, 1980.