ALGEBRAIC NUMBER THEORY

Romyar Sharifi

Contents

Introduction

At its core, the ancient subject of number theory is concerned with the arithmetic of the integers. The Fundamental Theorem of Arithmetic, which states that every positive integer factors uniquely into a product of prime numbers, was contained in Euclid's Elements, as was the infinitude of the set of prime numbers. Over the centuries, number theory grew immensely as a subject, and techniques were developed for approaching number-theoretic problems of a various natures. For instance, unique factorization may be viewed as a ring-theoretic property of $\mathbb{Z}$, while Euler used analysis in his own proof that the set of primes is infinite, exhibiting the divergence of the infinite sum of the reciprocals of all primes.

Algebraic number theory distinguishes itself within number theory by its use of techniques from abstract algebra to approach problems of a number-theoretic nature. It is also often considered, for this reason, as a subfield of algebra. The overriding concern of algebraic number theory is the study of the finite field extensions of $\mathbb{Q}$, which are known as number fields, and their rings of integers, analogous to $\mathbb{Z}$.

The ring of integers $\mathscr{O}$ of a number field F is the subring of F consisting of all roots of all monic polynomials in $\mathbb{Z}[x]$. Unlike $\mathbb{Z}$, not all integer rings are UFDs, as one sees for instance by considering the factorization of 6 in the ring $\mathbb{Z}[\sqrt{-5}]$. However, they are what are known as Dedekind domains, which have the particularly nice property that every nonzero ideal factors uniquely as a product of nonzero prime ideals, which are all in fact maximal. In essence, prime ideals play the role in $\mathscr{O}$ that prime numbers do in $\mathbb{Z}$.

A Dedekind domain is a UFD if and only if it is a PID. The class group of a Dedekind domain is roughly the quotient of its set of nonzero ideals by its nonzero principal ideals, and it thereby serves as something of a measure of how far a Dedekind domain is from being a principal ideal domain. The class group of a number field is finite, and the classical proof of this is in fact a bit of analysis. This should not be viewed as an anomalous encroachment: algebraic number theory draws heavily from the areas it needs to tackle the problems it considers, and analysis and geometry play important roles in the modern theory.

Given a prime ideal $\mathfrak{p}$ in the integer ring $\mathscr{O}$ of a number field F, one can define a metric on F that measures the highest power of $\mathfrak{p}$ dividing the difference of two points in F. If the finite field $\mathscr{O}/\mathfrak{p}$ has characteristic p, then the completion $F_{\mathfrak{p}}$ of F with respect to this metric is known as a p-adic field, and the subring $\mathscr{O}_{\mathfrak{p}}$ that is the completion of $\mathscr{O}$ is called its valuation ring. In the case that $F = \mathbb{Q}$,

one obtains the p-adic numbers $\mathbb{Q}_p$ and p-adic integers $\mathbb{Z}_p$. The archimedean fields $\mathbb{R}$ and $\mathbb{C}$ are also completions of number fields with respect to the more familiar Euclidean metrics, and are in that sense similar to p-adic fields, but the geometry of p-adic fields is entirely different. For instance, a sequence of integers converges to 0 in $\mathbb{Z}_p$ if and only it is eventually congruent to zero modulo arbitrarily high powers of p.

It is often easier to work with p-adic fields, as solutions to polynomial equations can be found in them by successive approximation modulo increasing powers of a prime ideal. The "Hasse principle" asserts that the existence of a solution to polynomial equations in a number field should be equivalent to the existence of a solution in every completion of it. (The Hasse principle does not actually hold in such generality, which partially explains the terminology.)

Much of the formalism in the theory of number fields carries over to a class of fields of finite characteristic, known as function fields. The function fields we consider are the finite extensions of the fields of rational functions $\mathbb{F}_p(t)$ in a single indeterminate t, for some prime p. Their "rings of integers", such as $\mathbb{F}_p[t]$ in the case of $\mathbb{F}_p(t)$, are again Dedekind domains. Since function fields play a central role in algebraic geometry, the ties here with geometry are much closer, and often help to provide intuition in the number field case. For instance, instead of the class group, one usually considers the related Picard group of divisors of degree 0 modulo principal divisors. The completions of function fields are fields of Laurent series over finite fields. We use the term "global field" refer to number fields and function fields in general, while the term "local field" refers to their nonarchimedean completions.

An introductory course in algebraic number theory can only hope to touch on a minute but essential fraction of the theory as it is today. Much more of this beautiful edifice can be seen in some of the great accomplishments in the number theory of recent decades. Chief among them, of course, is the proof of Fermat's last theorem, the statement of which is surely familiar to you. Wiles' proof of FLT is actually rather round-about. It proceeds first by showing that a certain rational elliptic curve that can be constructed out of a solution to Fermat's equation is not modular, and then that all (or really, enough) rational elliptic curves are modular. In this latter aspect of the proof are contained advanced methods in the theory of Galois representations, modular forms, abelian varieties, deformation theory, Iwasawa theory, and commutative ring theory, none of which we will be able to discuss.

NOTATION 0.0.1. Throughout these notes, we will use the term ring to refer more specifically to a nonzero ring with unity.

Part 1

Algebraic number theory

CHAPTER 1

Abstract algebra

In this chapter, we introduce the many of the purely algebraic results that play a major role in algebraic number theory, pausing only briefly to dwell on number-theoretic examples. When we do pause, we will need the definition of the objects of primary interest in these notes, so we make this definition here at the start.

DEFINITION 1.0.1. A *number field* (or *algebraic number field*) is a finite field extension of $\mathbb{Q}$.

We have the following names for extensions of $\mathbb{Q}$ of various degrees.

DEFINITION 1.0.2. A *quadratic* (resp., *cubic, quartic, quintic*, ...) *field* is a degree 2 (resp., 3, 4, 5, ...) extension of $\mathbb{Q}$.

1.1. Tensor products of fields

PROPOSITION 1.1.1. *Let K be a field, and let $f \in K[x]$ be monic and irreducible. Let M be a field extension of K, and suppose that f factors as $\prod_{i=1}^{m} f_i^{e_i}$ in $M[x]$, where the f_i are irreducible and distinct and each e_i is positive. Then we have an isomorphism*

$$\kappa\colon K[x]/(f) \otimes_K M \xrightarrow{\sim} \prod_{i=1}^{m} M[x]/(f_i^{e_i})$$

of M-algebras such that if $g \in K[x]$, then $\kappa((g+(f)) \otimes 1) = (g + (f_i^{e_i}))_i$.

PROOF. Note that we have a canonical isomorphism $K[x] \otimes_K M \xrightarrow{\sim} M[x]$ that gives rise to the first map in the composition

$$K[x]/(f) \otimes_K M \xrightarrow{\sim} M[x]/(f) \xrightarrow{\sim} \prod_{i=1}^{m} M[x]/(f_i^{e_i}),$$

the second isomorphism being the Chinese remainder theorem. The composition is κ. □

We have the following consequence.

LEMMA 1.1.2. *Let L/K be a finite separable extension of fields, and let M be an algebraically closed field containing K. Then we have an isomorphism of M-algebras*

$$\kappa\colon L \otimes_K M \xrightarrow{\sim} \prod_{\sigma\colon L \hookrightarrow M} M,$$

where the product is taken over field embeddings of L in M fixing K, such that

$$\kappa(\beta \otimes 1) = (\sigma\beta)_\sigma$$

for all $\beta \in L$.

PROOF. Write $L = K(\theta)$, and let $f \in K[x]$ be the minimal polynomial of θ. Then we define κ as the composition

$$L \otimes_K M \xrightarrow{\sim} \prod_{\sigma\colon L \hookrightarrow M} \frac{M[x]}{(x - \sigma(\theta))} \xrightarrow{\sim} \prod_{\sigma\colon L \hookrightarrow M} M,$$

where the first isomorphism is that of Proposition 1.1.1 and the second takes x to $\sigma(\theta)$ in the coordinate corresponding to σ. Any $\beta \in L$ has the form $g(\theta)$ for some $g \in K[x]$, and since any $\sigma\colon L \hookrightarrow M$ fixing K fixes the coefficients of g, we have $\kappa(\beta \otimes 1)$ is as stated. □

REMARK 1.1.3. If we compose κ of Lemma 1.1.2 with the natural embedding $L \hookrightarrow L \otimes_K M$ that takes $\alpha \in L$ to $\alpha \otimes 1$, then the composition

$$\iota_M\colon L \to \prod_{\sigma\colon L \hookrightarrow M} M$$

is the product of the field embeddings σ of L in M fixing K.

DEFINITION 1.1.4. Let K be a field and L and M be extensions of K both contained in some field Ω. We say that L and M are *linearly disjoint* over K if every K-linearly independent subset of L is M-linearly independent.

LEMMA 1.1.5. *Let K be a field and L and M be extensions of K both contained in some field Ω. If L and M are linearly disjoint over K, then $L \cap M = K$.*

PROOF. If $x \in L \cap M$ with $x \notin K$, then x and 1 are elements of L that are K-linearly independent but not M-linearly independent, so L and M are not linearly disjoint over K. □

From the definition, it may not be clear that the notion of linear disjointness is a symmetric one. However, this follows from the following.

PROPOSITION 1.1.6. *Let K be a field and L and M be extensions of K both contained in some field Ω. Then L and M are linearly disjoint over K if and only if the map $\varphi\colon L \otimes_K M \to LM$ induced by multiplication is an injection.*

PROOF. Suppose that $\gamma_1, \ldots, \gamma_s \in M$ are L-linearly dependent, and write $\sum_{i=1}^s \beta_i \gamma_i = 0$ for some $\beta_i \in L$. If φ is injective, then we must have $\sum_{i=1}^s \beta_i \otimes \gamma_i = 0$, which means that the γ_i are K-linearly dependent.

Conversely, let L and M be linearly disjoint over K. Suppose that we have a nonzero

$$x = \sum_{i=1}^s \beta_i \otimes \gamma_i \in \ker \varphi$$

for some $\beta_i \in L$ and $\gamma_i \in M$, with s taken to be minimal. If $x \neq 0$, then the γ_i are L-linearly dependent, so they are K-linearly dependent. In this case, without loss of generality, we may suppose that

$$\gamma_s + \sum_{i=1}^{s-1} \alpha_i \gamma_i = 0$$

for some α_i in K. Then

$$x = \sum_{i=0}^{s-1} (\beta_i - \alpha_i \beta_s) \otimes \gamma_i,$$

contradicting minimality. Thus $\ker \varphi = 0$. □

COROLLARY 1.1.7. *Let K be a field and L and M be extensions of K both contained in a given algebraic closure of K. Then L and M are linearly disjoint over K if and only if $L \otimes_K M$ is a field.*

PROOF. Note that LM is a union of subfields of the form $K(\alpha, \beta)$ with $\alpha \in L$ and $\beta \in M$. Since α and β are algebraic over K, we have $K(\alpha, \beta) = K[\alpha, \beta]$, and every element of the latter ring is a K-linear combination of monomials in α and β. Thus φ of Proposition 1.1.6 is surjective, and the result follows from the latter proposition. □

COROLLARY 1.1.8. *Let K be a field and L and M be finite extensions of K inside a given algebraic closure of K. Then $[LM : K] = [L : K][M : K]$ if and only if L and M are linearly disjoint over K.*

PROOF. Again, we have the surjection $\varphi \colon L \otimes_K M \to LM$ given by multiplication which is an injection if and only if L and M are linearly disjoint by Proposition 1.1.6. As $L \otimes_K M$ has dimension $[L : K][M : K]$ over K, the result follows. □

REMARK 1.1.9. Suppose that $L = K(\theta)$ is a finite extension of K. To say that L is linearly disjoint from a field extension M of K is by Propostion 1.1.1 exactly to say that the minimal polynomial of θ in $K[x]$ remains irreducible in $M[x]$.

We prove the following in somewhat less generality than possible.

LEMMA 1.1.10. *Let L be a finite Galois extension of a field K inside an algebraic closure Ω of K, and let M be an extension of K in Ω. Then L and M are linearly disjoint if and only if $L \cap M = K$.*

PROOF. We write $L = K(\theta)$ for some $\theta \in L$, and let $f \in K[x]$ be the minimal polynomial of θ. As $\mathrm{Gal}(LM/M) \cong \mathrm{Gal}(L/(L \cap M))$ by restriction, we have $L \cap M = K$ if and only if $[LM : M] = [L : K]$. Since $LM = M(\theta)$, this occurs if and only if f is irreducible in $M[x]$. The result then follows from Remark 1.1.9. □

1.2. Integral extensions

DEFINITION 1.2.1. We say that B/A is an *extension of commutative rings* if A and B are commutative rings such that A is a subring of B.

DEFINITION 1.2.2. Let B/A be an extension of commutative rings. We say that $\beta \in B$ is *integral over* A if β is the root of a monic polynomial in $A[x]$.

EXAMPLES 1.2.3.

a. Every element $a \in A$ is integral over A, in that a is a root of $x-a$.

b. If L/K is a field extension and $\alpha \in L$ is algebraic over K, then α is integral over K, being a root of its minimal polynomial, which is monic.

c. If L/K is a field extension and $\alpha \in L$ is transcendental over K, then α is not integral over K.

d. The element $\sqrt{2}$ of $\mathbb{Q}(\sqrt{2})$ is integral over $\mathbb{Z}$, as it is a root of x^2-2.

e. The element $\alpha = \frac{1-\sqrt{5}}{2}$ of $\mathbb{Q}(\sqrt{5})$ is integral over $\mathbb{Z}$, as it is a root of x^2-x-1.

PROPOSITION 1.2.4. *Let B/A be an extension of commutative rings. For $\beta \in B$, the following conditions are equivalent:*

i. the element β is integral over A,

ii. there exists $n \geq 0$ such that $\{1, \beta, \ldots, \beta^n\}$ generates $A[\beta]$ as an A-module,

iii. the ring $A[\beta]$ is a finitely generated A-module, and

iv. there exists a finitely generated A-submodule M of B that such that $\beta M \subseteq M$ and which is faithful over $A[\beta]$.

PROOF. Suppose that (i) holds. Then β is a root of a monic polynomial $g \in A[x]$. Given any $f \in A[x]$, the division algorithm tells us that $f = qg + r$ with $q, r \in A[x]$ and either $r = 0$ or $\deg r < \deg g$. It follows that $f(\beta) = r(\beta)$, and therefore that $f(\beta)$ is in the A-submodule generated by $\{1, \beta, \ldots, \beta^{\deg g - 1}\}$, so (ii) holds. Since this set is independent of f, it generates $A[\beta]$ as an A-module, so (iii) holds. Suppose that (iii) holds. Then we may take $M = A[\beta]$, which being free over itself has trivial annihilator.

Finally, suppose that (iv) holds. Let

$$M = \sum_{i=1}^{n} A\gamma_i \subseteq B$$

be such that $\beta M \subseteq M$, and suppose without loss of generality that $\beta \neq 0$. We have

$$\beta \gamma_i = \sum_{j=1}^{n} a_{ij} \gamma_j$$

for some $a_{ij} \in A$ with $1 \leq i \leq n$ and $1 \leq j \leq n$. Consider A-module homomorphism $T \colon B^n \to B^n$ represented by (a_{ij}). The characteristic polynomial $f(x) \in A[x]$ of T is monic, and $f(\beta)$ acts as zero on M. Since M is a faithful $A[\beta]$-module, we must have $f(\beta) = 0$. Thus, β is integral. □

EXAMPLE 1.2.5. The element $\frac{1}{2} \in \mathbb{Q}$ is not integral over $\mathbb{Z}$, as $\mathbb{Z}[1, 2^{-1}, \ldots, 2^{-n}]$ for $n \geq 0$ is equal to $\mathbb{Z}[2^{-n}]$, which does not contain $2^{-(n+1)}$.

DEFINITION 1.2.6. Let B/A be an extension of commutative rings. We say that B is an *integral extension of* A if every element of B is integral over A.

EXAMPLE 1.2.7. The ring $\mathbb{Z}[\sqrt{2}]$ is an integral extension of $\mathbb{Z}$. Given $\alpha = a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$, note that α is a root of $x^2 - 2ax + a^2 - 2b^2$.

LEMMA 1.2.8. *Suppose that B/A is an extension of commutative rings such that B is finitely generated as an A-module, and let M be a finitely generated B-module. Then M is a finitely generated A-module.*

PROOF. Let $\{m_1, \ldots, m_n\}$ be a set of generators of M as a B-module, and let $\{\beta_1, \ldots, \beta_k\}$ be a set of generators of B as an A-module. We claim that $\{\beta_i m_j \mid 1 \leq i \leq k, 1 \leq j \leq n\}$ is a set of generators of M as an A-module. To see this, let $m \in M$ and write

$$m = \sum_{j=1}^{n} b_j m_j$$

with $b_j \in B$ for $1 \leq j \leq n$. For $1 \leq j \leq n$, we then write

$$b_j = \sum_{i=1}^{k} a_{ij} \beta_i$$

with $a_{ij} \in A$ for $1 \leq i \leq k$. We then have

$$m = \sum_{i=1}^{k} \sum_{j=1}^{n} a_{ij} \beta_i m_j,$$

as desired. □

We now give a criterion for a finitely generated algebra over a ring to be finitely generated as a module.

PROPOSITION 1.2.9. *Let B/A be an extension of commutative rings and suppose that*

$$B = A[\beta_1, \beta_2, \ldots, \beta_k]$$

for some $k \geq 0$ and $\beta_i \in B$ with $1 \leq i \leq k$. Then the following are equivalent.

i. the ring B is integral over A,

ii. each β_i with $1 \leq i \leq k$ is integral over A, and

iii. the ring B is finitely generated as an A-module.

PROOF. Clearly, (i) implies (ii), so suppose that (ii) holds. By definition, each β_i is then integral over any commutative ring containing A. By Proposition 1.2.4, each $A[\beta_1, \ldots, \beta_j]$ with $1 \leq j \leq k$ is a finitely generated $A[\beta_1, \ldots, \beta_{j-1}]$-module, generated by $\{1, \beta_j, \ldots, \beta_j^{n_j}\}$ for some $n_j \geq 0$. Assuming recursively that $A[\beta_1, \ldots, \beta_{j-1}]$ is finitely generated as an A-module, Lemma 1.2.8 implies that $A[\beta_1, \ldots, \beta_j] = A[\beta_1, \ldots, \beta_{j-1}][\beta_j]$ is finitely generated as an A-module as well. Therefore, (iii) holds.

Finally, if (iii) holds and $\beta \in B$, then since $\beta B \subseteq B$, the element β is integral over a by Proposition 1.2.4. Thus (i) holds. □

We derive the following important consequence.

PROPOSITION 1.2.10. *Suppose that C/B and B/A are integral extensions of commutative rings. Then C/A is an integral extension as well.*

PROOF. Let $\gamma \in C$, and let $f \in B[x]$ be a monic polynomial which has γ as a root. Let B' be the subring of B generated over A by the coefficients of f, which is integral over A as B is. By Proposition 1.2.9, the ring B' is then finitely generated over A. As $B'[\gamma]$ is finitely generated over B' as well, we have $B'[\gamma]$ is finitely generated over A. Hence, $B[\gamma]$ is itself an integral extension of A. By definition of an integral extension, the element γ is integral over A. Since $\gamma \in C$ was arbitrary, we conclude that C is integral over A. □

DEFINITION 1.2.11. Let B/A be an extension of commutative rings. The *integral closure* of A in B is the set of elements of B that are integral over A.

PROPOSITION 1.2.12. *Let B/A be an extension of commutative rings. Then the integral closure of A in B is a subring of B.*

PROOF. If α and β are elements of B that are integral over A, then $A[\alpha,\beta]$ is integral over A by Proposition 1.2.9. Therefore, every element of $A[\alpha,\beta]$, including $\alpha+\beta$ and $\alpha\cdot\beta$, is integral over A as well. That is, the integral closure of A in B is closed under addition, additive inverses, and multiplication, and it contains 1, so it is a ring. □

EXAMPLE 1.2.13. The integral closure of $\mathbb{Z}$ in $\mathbb{Z}[x]$ is $\mathbb{Z}$, since if $f \in \mathbb{Z}[x]$ is of degree at least 1 and $g \in \mathbb{Z}[x]$ is nonconstant, then $g(f(x))$ has degree $\deg g \cdot \deg f$ in x, hence cannot be 0.

DEFINITION 1.2.14.

a. The *ring of algebraic integers* is the integral closure $\overline{\mathbb{Z}}$ of $\mathbb{Z}$ inside $\mathbb{C}$.

b. An *algebraic integer* is an element of $\overline{\mathbb{Z}}$.

DEFINITION 1.2.15. Let B/A be an extension of commutative rings. We say that A is *integrally closed* in B if A is its own integral closure in B.

DEFINITION 1.2.16. We say that an integral domain A is *integrally closed* if it is integrally closed in its quotient field.

EXAMPLE 1.2.17. Every field is integrally closed.

PROPOSITION 1.2.18. *Let A be an integrally closed domain, let K be the quotient field, and let L be a field extension of K. If $\beta \in L$ is integral over A with minimal polynomial $f \in K[x]$, then $f \in A[x]$.*

PROOF. Since $\beta \in L$ is integral, it is the root of some monic polynomial $g \in A[x]$ such that f divides g in $K[x]$. As g is monic, every root of g in an algebraic closure $\overline{K}$ containing K is integral over K. As every root of f is a root of g, the same is true of the roots of f. Write $f = \prod_{i=1}^{n}(x-\beta_i)$ for $\beta_i \in \overline{K}$ integral over A. As the integral closure of A in $\overline{K}$ is a ring, it follows that every coefficient of f is integral over A, being sums of products of the elements β_i. Since $f \in K[x]$ and A is integrally closed, we then have $f \in A[x]$. □

The following holds in the case of UFDs.

PROPOSITION 1.2.19. *Let A be a UFD, let K be the quotient field of A, and let L be a field extension of K. Suppose that $\beta \in L$ is algebraic over K with minimal polynomial $f \in K[x]$. If β is integral over A, then $f \in A[x]$.*

PROOF. Let $\beta \in L$ be integral over A, let $g \in A[x]$ be a monic polynomial of which it is a root, and let $f \in K[x]$ be the minimal polynomial of β. Since f divides g in $K[x]$ and A is a UFD with quotient field K, there exists $d \in K$ such that $df \in A[x]$ and df divides g in $A[x]$. Since f is monic, d must be an element of A (and in fact may be taken to be a least common denominator of the coefficients of f). The coefficient of the leading term of any multiple of df will be divisible by d, so this forces d to be a unit, in which case $f \in A[x]$. □

COROLLARY 1.2.20. *Every unique factorization domain is integrally closed.*

PROOF. The minimal polynomial of an element a of the quotient field K of a UFD A is $x-a$. If $a \notin A$, it follows from Proposition 1.2.19 that a is not integral over A. □

EXAMPLES 1.2.21. The ring $\mathbb{Z}$ is integrally closed.

EXAMPLE 1.2.22. The ring $\mathbb{Z}[\sqrt{17}]$ is not integrally closed, since $\alpha = \frac{1+\sqrt{17}}{2}$ is a root of the monic polynomial $x^2 - x - 4$. In particular, $\mathbb{Z}[\sqrt{17}]$ is not a UFD.

PROPOSITION 1.2.23. *Let B/A be an extension of commutative rings, and suppose that B is an integrally closed domain. Then the integral closure of A in B is integrally closed.*

PROOF. Let $\overline{A}$ denote the integral closure of A in B, and let Q denote the quotient field of $\overline{A}$. Let $\alpha \in Q$, and suppose that α is integral over $\overline{A}$. Then $\overline{A}[\alpha]$ is integral over $\overline{A}$, so $\overline{A}[\alpha]$ is integral over A, and therefore α is integral over A. That is, α is an element of $\overline{A}$, as desired. □

EXAMPLE 1.2.24. The ring $\overline{\mathbb{Z}}$ of algebraic integers is integrally closed.

PROPOSITION 1.2.25. *Let A be an integral domain with quotient field K, and let L be an algebraic extension of K. Then the integral closure B of A in L has quotient field equal to L inside L. In fact, every element of L may be written as $\frac{b}{d}$ for some $d \in A$ and $b \in B$.*

PROOF. Any $\beta \in L$ is the root of a monic polynomial $f = \sum_{i=0}^{n} a_i x^i \in K[x]$. Let $d \in A$ be such that $df \in A[x]$. Then

$$d^n f(d^{-1}x) = \sum_{i=0}^{n} a_i d^{n-i} x^i \in A[x]$$

is both monic and has $d\beta$ as a root. In other words, $d\beta$ is contained in B, as desired. □

EXAMPLE 1.2.26. The quotient field of $\overline{\mathbb{Z}}$ is $\overline{\mathbb{Q}}$.

DEFINITION 1.2.27. The *ring of integers* (or *integer ring*) $\mathcal{O}_K$ of a number field K is the integral closure of $\mathbb{Z}$ in K.

The prototypical examples of rings of integers arise in the setting of quadratic fields.

THEOREM 1.2.28. *Let $d \neq 1$ be a square-free integer. The ring of integers of $\mathbb{Q}(\sqrt{d})$ is*

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \bmod 4, \\ \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2,3 \bmod 4. \end{cases}$$

PROOF. Suppose that $\alpha = a + b\sqrt{d}$ is integral for $a, b \in \mathbb{Q}$. If $b = 0$, then we must have $a \in \mathbb{Z}$. If $b \neq 0$, then the minimal polynomial of α is $f = x^2 - 2ax + a^2 - b^2 d$. Since α is integral, we must have $f \in \mathbb{Z}[x]$, so $2a \in \mathbb{Z}$. If $a \in \mathbb{Z}$, then since $a^2 - b^2 d \in \mathbb{Z}$ and d is square-free, we have $b \in \mathbb{Z}$ as well. If $a \notin \mathbb{Z}$, then $2a = a'$ and $2b = b'$ for some odd $a', b' \in \mathbb{Z}$, and $(a')^2 \equiv (b')^2 d \bmod 4$. As $(\mathbb{Z}/4\mathbb{Z})^2 = \{0,1\}$, this is impossible if $d \not\equiv 1 \bmod 4$. If $d \equiv 1 \bmod 4$, then $a + b\sqrt{d}$ lies in the claimed ring, since it contains $\sqrt{d}$, and clearly $(1+\sqrt{d})/2$ is integral. □

1.3. Norm and trace

DEFINITION 1.3.1. Let L/K be a finite extension of fields. For $\alpha \in L$, let $m_\alpha \colon L \to L$ denote the linear transformation of K-vector spaces defined by left multiplication by α.

a. The *norm map* $N_{L/K} \colon L \to K$ is defined by $N_{L/K}(\alpha) = \det m_\alpha$ for $\alpha \in L$.

b. The *trace map* $\mathrm{Tr}_{L/K} \colon L \to K$ is defined by $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{tr}\, m_\alpha$ for $\alpha \in L$.

REMARK 1.3.2. For a finite field extension L/K, the trace map $\mathrm{Tr}_{L/K}$ is a homomorphism, and the norm map $N_{L/K}$ is a homomorphism to $K^\times$ upon restriction to $L^\times$.

PROPOSITION 1.3.3. *Let L/K be a finite extension of fields, and let $\alpha \in L$. Let $f \in K[x]$ be the minimal polynomial of α over K, let $d = [K(\alpha) : K]$, let $s = [L : K(\alpha)]$, and let $\overline{K}$ be an algebraic closure of K. Suppose that f factors in $\overline{K}[x]$ as*

$$f = \prod_{i=1}^{d} (x - \alpha_i)$$

for some $\alpha_1, \ldots, \alpha_d \in \overline{K}$. Then the characteristic polynomial of m_α is f^s, and we have

$$N_{L/K}(\alpha) = \prod_{i=1}^{d} \alpha_i^s \quad \text{and} \quad \mathrm{Tr}_{L/K}(\alpha) = s \sum_{i=1}^{d} \alpha_i.$$

PROOF. We claim that the characteristic polynomial of the K-linear transformation m_α is f^s. First suppose that $L = K(\alpha)$. Note that $\{1, \alpha, \ldots, \alpha^{d-1}\}$ forms a K-basis of $K(\alpha)$, and with respect to this basis, m_α is given by the matrix

$$A = \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & \ddots & \ddots & & \vdots \\ & & 1 & 0 & -a_{d-2} \\ & & & 1 & -a_{d-1} \end{pmatrix},$$

where $a_i \in K$ for $1 \leq i \leq d$ are such that

$$f = x^d + \sum_{i=0}^{d-1} a_i x^i.$$

Expanding the determinant of $xI - A$ using its first row, we see that

$$\begin{aligned} \mathrm{char}\, m_\alpha = \det(xI - A) &= x \det(xI - A') + (-1)^{d-1} a_0 \det \begin{pmatrix} -1 & x & & \\ & \ddots & \ddots & \\ & & -1 & x \\ & & & -1 \end{pmatrix} \\ &= x \det(xI - A') + a_0, \end{aligned}$$

where A' is the $(1,1)$-minor of A. By induction on the dimension of A, we may assume that

$$\det(xI - A') = x^{d-1} + \sum_{i=0}^{d-2} a_{i+1} x^i,$$

so $\mathrm{char}\, m_\alpha = f$. Since

$$f = x^d - \mathrm{tr}(m_\alpha) x^{d-1} + \cdots + (-1)^d \det(m_\alpha),$$

we have by expanding out the factorization of f in $\overline{K}[x]$ that $N_{L/K}\alpha$ and $\mathrm{Tr}_{L/K}\alpha$ are as stated in this case.

In general, if $\{\beta_1, \ldots, \beta_s\}$ is a basis for $L/K(\alpha)$, then $\{\beta_i \alpha^j \mid 1 \leq i \leq s, 0 \leq j \leq d-1\}$ is a basis for L/K. The matrix of m_α with respect to this basis (with the lexicographical ordering on the pairs (i,j)) is the block diagonal matrix consisting of s copies of A. In other words, $\mathrm{char}\, m_\alpha$ is the f^s, from which the result now follows easily. □

We can also express the norm as a power of a product of conjugates and the trace as a multiple of a sum of conjugates.

PROPOSITION 1.3.4. *Let L/K be a finite extension of fields, and let $m = [L:K]_i$ be its degree of inseparability. Let $\mathfrak{S}$ denote the set of embeddings of L fixing K in a given algebraic closure of K. Then, for $\alpha \in L$, we have*

$$N_{L/K}(\alpha) = \prod_{\sigma\in\mathfrak{S}} \sigma\alpha^m \quad \textit{and} \quad \mathrm{Tr}_{L/K}(\alpha) = m\sum_{\sigma\in\mathfrak{S}} \sigma\alpha.$$

PROOF. The distinct conjugates of α in a fixed algebraic closure $\overline{K}$ of K are exactly the $\tau\alpha$ for τ in the set $\mathfrak{T}$ of distinct embeddings of $K(\alpha)$ in $\overline{K}$. These $\tau\alpha$ are the distinct roots of the minimal polynomial of α over K, each occuring with multiplicity the degree $[K(\alpha):K]_i$ of inseparability of $K(\alpha)/K$. Now, each of these embeddings extends to $[L:K(\alpha)]_s$ distinct embeddings of L into $\overline{K}$, and each extension $\sigma \in \mathfrak{S}$ of τ sends α to $\tau(\alpha)$. By Proposition 1.3.3, we have

$$N_{L/K}\alpha = \prod_{\tau\in\mathfrak{T}} (\tau\alpha)^{[L:K(\alpha)][K(\alpha):K]_i} = \prod_{\sigma\in\mathfrak{S}} \sigma\alpha^{[L:K]_i},$$

and similarly for the trace. □

We have the following immediate corollary.

COROLLARY 1.3.5. *Let L/K be a finite separable extension of fields. Let $\mathfrak{S}$ denote the set of embeddings of L fixing K in a given algebraic closure of K. Then, for $\alpha \in L$, we have*

$$N_{L/K}(\alpha) = \prod_{\sigma\in\mathfrak{S}} \sigma\alpha \quad \textit{and} \quad \mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma\in\mathfrak{S}} \sigma\alpha.$$

We also have the following.

PROPOSITION 1.3.6. *Let M/K be a finite field extension and L be an intermediate field in the extension. Then we have*

$$N_{M/K} = N_{L/K} \circ N_{M/L} \quad \textit{and} \quad \mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}.$$

PROOF. We prove this for norm maps. Let $\mathfrak{S}$ denote the set of embeddings of L into $\overline{K}$ that fix K, let $\mathfrak{T}$ denote the set of embeddings of M into $\overline{K}$ that fix L, and let $\mathfrak{U}$ denote the set of embeddings of M into $\overline{K}$ that fix K. Since $[M:K]_i = [M:L]_i \cdot [L:K]_i$, it suffices by Proposition 1.3.4 to show that

$$\prod_{\delta\in\mathfrak{U}} \delta\alpha = \prod_{\sigma\in\mathfrak{S}} \sigma\left(\prod_{\tau\in\mathfrak{T}} \tau\alpha\right).$$

We extend each σ to an automorphism $\tilde{\sigma}$ of $\overline{K}$ fixing K. We then have

$$\prod_{\sigma\in\mathfrak{S}} \sigma\left(\prod_{\tau\in\mathfrak{T}} \tau\alpha\right) = \prod_{\sigma\in\mathfrak{S}} \prod_{\tau\in\mathfrak{T}} (\tilde{\sigma}\circ\tau)\alpha.$$

For the trace map, we simply replace the products by sums.

We claim that the subset $X = \{\tilde{\sigma} \circ \tau \mid \sigma \in \mathfrak{S}, \tau \in \mathfrak{T}\}$ of $\mathfrak{U}$ is exactly $\mathfrak{U}$, which will finish the proof. Let $\sigma, \sigma' \in \mathfrak{S}$ and $\tau, \tau' \in \mathfrak{T}$, and suppose that

$$\tilde{\sigma} \circ \tau = \tilde{\sigma}' \circ \tau'. \tag{1.3.1}$$

Since $\tilde{\sigma} \circ \tau|_L = \sigma|_L$, we have that $\sigma = \sigma'$. Since $\tilde{\sigma}$ is an automorphism, we then apply its inverse to (1.3.1) to obtain $\tau = \tau'$. As there are then $|\mathfrak{S}||\mathfrak{T}| = |\mathfrak{U}|$ elements of X, we have the result. □

EXAMPLE 1.3.7. The norm for the extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, where d is a square-free integer, is given by

$$N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x + y\sqrt{d}) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2$$

for $x, y \in \mathbb{Q}$.

EXAMPLE 1.3.8. For $a, b, c \in \mathbb{Q}$, we have

$$\begin{aligned} N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(a + b\sqrt[3]{2} + c\sqrt[3]{4}) &= (a + b\sqrt[3]{2} + c\sqrt[3]{4})(a + b\omega\sqrt[3]{2} + c\omega^2\sqrt[3]{4})(a + b\omega^2\sqrt[3]{2} + c\omega\sqrt[3]{4}) \\ &= a^3 + 2b^3 + 4c^3 - 6abc, \end{aligned}$$

for ω a primitive cube root of unity. The trace is simpler:

$$\mathrm{Tr}_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = 3a.$$

DEFINITION 1.3.9. A K-valued *linear character of a group* G is a group homomorphism $\chi : G \to K^\times$, where K is a field.

DEFINITION 1.3.10. We say that a set of K-valued linear characters X of a group G is *K-linearly independent* if it is linearly independent as a subset of the K-vector space of functions $G \to K$.

THEOREM 1.3.11. *Any set of K-valued linear characters $G \to K^\times$ of a group G is K-linearly independent.*

PROOF. Let X be a set of linear characters $G \to K^\times$. Suppose by way of contradiction that $m \geq 2$ is minimal such that there m distinct, linearly dependent elements of G. Choose $a_i \in K$ and $\chi_i \in X$ with $1 \leq i \leq m$ for which $a_1 \neq 0$ and

$$\sum_{i=1}^{m} a_i \chi_i = 0.$$

Also, let $h \in G$ be such that $\chi_1(h) \neq \chi_m(h)$. Set $b_i = a_i(\chi_i(h) - \chi_m(h))$ for $1 \leq i \leq m-1$. For any $g \in G$, we then have

$$\sum_{i=1}^{m-1} b_i \chi_i(g) = \sum_{i=1}^{m} a_i(\chi_i(h) - \chi_m(h))\chi_i(g) = \sum_{i=1}^{m} a_i \chi_i(hg) - \chi_m(h) \sum_{i=1}^{m} a_i \chi_i(g) = 0.$$

Since $b_1 \neq 0$ and $\sum_{i=1}^{m-1} b_i \chi_i$ has only $m-1$ terms, this contradicts the existence of m. □

In the case of cyclic extensions, the kernel of the norm map bears a simple description.

THEOREM 1.3.12 (Hilbert's Theorem 90). *Let L/K be a finite cyclic extension of fields, and let σ be a generator of its Galois group. Then*

$$\ker N_{L/K} = \left\{ \frac{\sigma(\beta)}{\beta} \mid \beta \in L^\times \right\}.$$

PROOF. Set $n = [L:K]$. Let $\beta \in L$, and note that

$$N_{L/K}\left(\frac{\sigma(\beta)}{\beta}\right) = \prod_{i=0}^{n-1} \frac{\sigma^{i+1}(\beta)}{\sigma^i(\beta)} = \frac{N_{L/K}(\beta)}{N_{L/K}(\beta)} = 1.$$

Next, suppose that $\alpha \in \ker N_{L/K}$, and set

$$x_\gamma = \gamma + \alpha\sigma(\gamma) + \alpha\sigma(\alpha)\sigma^2(\gamma) + \cdots + \alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(\gamma)$$

for $\gamma \in L$. The elements of $\mathrm{Gal}(L/K)$, which is to say the powers of σ, are distinct L-valued characters on $L^\times$, and therefore they are L-linearly independent. Thus, there exists $\gamma \in L^\times$ such that $x_\gamma \neq 0$. We then note that

$$\alpha\sigma(x_\gamma) = \alpha\sigma(\gamma) + \alpha\sigma(\alpha)\sigma^2(\gamma) + \cdots + \alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(\gamma) + N_{L/K}(\alpha)\gamma = x_\gamma,$$

so $\alpha^{-1} = \sigma(x_\gamma)x_\gamma^{-1}$, finishing the proof. □

There is also an additive form of Hilbert's Theorem 90, which describes the kernel of the trace. We leave the proof to the reader.

PROPOSITION 1.3.13 (Additive Hilbert's Theorem 90). *Let L/K be a finite cyclic extension of fields, and let σ be a generator of its Galois group. Then*

$$\ker \mathrm{Tr}_{L/K} = \{\sigma(\beta) - \beta \mid \beta \in L\}.$$

LEMMA 1.3.14. *Let B/A be an integral extension of domains, and suppose that A is integrally closed in its quotient field K. Let L denote the quotient field of B, and suppose that L/K is finite. Then $N_{L/K}(\beta)$ and $\mathrm{Tr}_{L/K}(\beta)$ are elements of A for every $\beta \in B$.*

PROOF. Since β is integral over A, so are all of its conjugates in an algebraic closure $\bar{L}$ of L, since they are also roots of the monic polynomial of which β is a root. It follows from Proposition 1.3.4 and the fact that the integral closure of A in $\bar{L}$ is a ring that $N_{L/K}(\beta)$ and $\mathrm{Tr}_{L/K}(\beta)$ are elements of K integral over A, so A is integrally closed. □

1.4. Discriminants

DEFINITION 1.4.1. Let K be a field and V a finite-dimensional K-vector space. A *K-bilinear form* (or simply, *bilinear form*) $\psi\colon V \times V \to K$ on V is a function satisfying

$$\psi(v+v', w) = \psi(v,w) + \psi(v',w) \quad \text{and} \quad \psi(v, w+w') = \psi(v,w) + \psi(v,w')$$

and

$$\psi(av,w) = a\psi(v,w) = \psi(v,aw)$$

for all $a \in K$ and $v, v', w, w' \in V$.

DEFINITION 1.4.2. A K-bilinear form ψ on a K-vector space V is said to be *symmetric* if

$$\psi(v,w) = \psi(w,v)$$

for all $v, w \in V$.

EXAMPLE 1.4.3. Given a matrix $Q \in M_n(K)$, we can define a bilinear form on K^n by

$$\psi(v,w) = v^T Q w$$

for $v, w \in K^n$, where we use a superscript T to denote the transpose. It is symmetric if and only if Q is.

EXAMPLE 1.4.4. If L/K is a finite extension of fields, then $\psi\colon L \times L \to K$ defined by

$$\psi(\alpha,\beta) = \mathrm{Tr}_{L/K}(\alpha\beta)$$

for $\alpha, \beta \in L$ is a symmetric K-bilinear form on L.

DEFINITION 1.4.5. The *discriminant* of a bilinear form ψ on a finite dimensional K-vector space V relative to an ordered basis $(v_1, \ldots, v_n)$ of V is the determinant of the matrix $(\psi(v_i, v_j))_{i,j}$.

LEMMA 1.4.6. *Let $\psi\colon V \times V \to K$ be a K-bilinear form on a finite-dimensional vector space V of dimension $n \geq 1$. Let $v_1, \ldots, v_n \in V$, and let $T\colon V \to V$ be a linear transformation. Then*

$$\det(\psi(Tv_i, Tv_j))_{i,j} = (\det T)^2 \cdot \det(\psi(v_i, v_j))_{i,j}.$$

PROOF. Suppose first that the v_i form a basis of V. Let $A = (a_{ij})$ denote the matrix of T with respect to the ordered basis $(v_1, \ldots, v_n)$. for each i. We may then write

$$\psi(Tv_i, Tv_j) = \sum_{k=1}^{n} a_{ik} \sum_{l=1}^{n} a_{jl} \psi(v_k, v_l).$$

As matrices, we then have

$$(\psi(Tv_i, Tv_j)) = A(\psi(v_i, v_j))A^T,$$

and the result follows as $\det T = \det A = \det A^T$.

If the v_i do not form a basis of V, then there is an ordered basis $(e_1, \ldots, e_n)$ of V and a linear transformation $U\colon V \to V$ of with $U(e_i) = v_i$ for all i. As $\det U = 0$, we have

$$\det(\psi(v_i, v_j))_{i,j} = (\det U)^2 \det(\psi(e_i, e_j))_{i,j} = 0.$$

As the $Tv_1, \ldots, Tv_n$ cannot be a basis, we have that both sides in the formula are zero. □

REMARKS 1.4.7. Let $\psi\colon V\times V\to K$ be a K-bilinear form on a finite-dimensional vector space V of dimension $n\geq 1$. Then Lemma 1.4.6 implies the following.

a. The discriminant of ψ to a basis is independent of its ordering, since a permutation matrix has determinant ± 1.

b. We have $\det(\psi(v_i,v_j))_{i,j}=0$ if $v_1,\dots,v_n\in V$ are linearly dependent.

DEFINITION 1.4.8. Let L/K be a finite extension of fields. The *discriminant* of L/K relative to a basis of L as a K-vector space is the discriminant of the bilinear form

$$(\alpha,\beta)\mapsto \mathrm{Tr}_{L/K}(\alpha\beta)$$

relative to the basis.

NOTATION 1.4.9. If L/K is a finite extension of fields and $\beta_1,\dots,\beta_n\in L$ are arbitrary, we set

$$\mathrm{D}(\beta_1,\dots,\beta_n)=\det(\mathrm{Tr}_{L/K}(\beta_i\beta_j))_{i,j}.$$

If $(\beta_1,\dots,\beta_n)$ is an ordered basis of L/K, then $\mathrm{D}(\beta_1,\dots,\beta_n)$ is its discriminant.

PROPOSITION 1.4.10. *Let L/K be a finite separable extension of fields. Then for any $\beta_1,\dots,\beta_n\in L$, we have*

$$\mathrm{D}(\beta_1,\dots,\beta_n)=(\det(\sigma_i\beta_j)_{i,j})^2,$$

where $\{\sigma_1,\dots,\sigma_n\}$ is the set of embeddings of L in an algebraic closure of K that fix K.

PROOF. Note that

$$\mathrm{Tr}_{L/K}(\beta_i\beta_j)=\sum_{k=1}^{n}\sigma_k(\beta_i)\sigma_k(\beta_j),$$

so the matrix $(\mathrm{Tr}_{L/K}(\beta_i\beta_j))$ equals Q^TQ, where $Q\in M_n(L)$ satisfies $Q_{ij}=\sigma_i(\beta_j)$. □

DEFINITION 1.4.11. Let K be a field, and let $\alpha_1,\dots,\alpha_n\in K$. Then the matrix

$$Q(\alpha_1,\dots,\alpha_n)=\begin{pmatrix}1 & \alpha_1 & \cdots & \alpha_1^{n-1}\\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1}\\ \vdots & \vdots & & \vdots\\ 1 & \alpha_n & \cdots & \alpha_n^{n-1}\end{pmatrix}$$

is called the *Vandermonde matrix* for $\alpha_1,\dots,\alpha_n$.

LEMMA 1.4.12. *Let K be a field, and let $Q(\alpha_1,\dots,\alpha_n)$ be the Vandermonde matrix for elements $\alpha_1,\dots,\alpha_n$ of K. Then*

$$\det Q(\alpha_1,\dots,\alpha_n)=\prod_{1\leq i<j\leq n}(\alpha_j-\alpha_i).$$

PROOF. We work by induction on $n \geq 1$, the case $n = 1$ asserting the obvious fact that $\det Q(\alpha) = 1$ for any $\alpha \in K$. To compute the determinant of $Q = Q(\alpha_1, \ldots, \alpha_n)$, subtract α_1 times its ith column from its $(i+1)$th column for each $1 \leq i \leq n-1$, which leaves the determinant unchanged. We then obtain

$$\begin{aligned}\det Q &= \begin{vmatrix} 1 & 0 & \cdots & 0 \\ 1 & \alpha_2 - \alpha_1 & \cdots & \alpha_2^{n-2}(\alpha_2 - \alpha_1) \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n - \alpha_1 & \cdots & \alpha_n^{n-2}(\alpha_n - \alpha_1) \end{vmatrix} = \begin{vmatrix} \alpha_2 - \alpha_1 & \cdots & \alpha_2^{n-2}(\alpha_2 - \alpha_1) \\ \vdots & & \vdots \\ \alpha_n - \alpha_1 & \cdots & \alpha_n^{n-2}(\alpha_n - \alpha_1) \end{vmatrix} \\ &= \prod_{i=2}^{n} (\alpha_i - \alpha_1) \cdot \det Q(\alpha_2, \ldots, \alpha_n),\end{aligned}$$

and the result now follows by induction. □

PROPOSITION 1.4.13. *Suppose that L/K is a separable extension of degree n, and let $\alpha \in L$ be such that $L = K(\alpha)$. Then*

$$\mathrm{D}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)^2 \neq 0,$$

where $\alpha_1, \ldots, \alpha_n$ are the conjugates of α in an algebraic closure of K.

PROOF. By Proposition 1.4.10, we have that $\mathrm{D}(1, \alpha, \ldots, \alpha^{n-1})$ is the square of the determinant of the Vandermonde matrix $Q(\alpha_1, \ldots, \alpha_n)$, and the result then follows from Lemma 1.4.12. □

EXAMPLE 1.4.14. Let d be a square-free integer with $d \neq 1$. Consider the basis $\{1, \sqrt{d}\}$ of $\mathbb{Q}(\sqrt{d})$ as a $\mathbb{Q}$-vector space. Since the distinct conjugates of $\sqrt{d}$ are $\pm\sqrt{d}$, we have $\mathrm{D}(1, \sqrt{d}) = 4d$.

The following is basically a rephrasing of Proposition 1.4.13.

COROLLARY 1.4.15. *Suppose that L/K is a separable extension of degree n, and let $\alpha \in L$ be such that $L = K(\alpha)$, and let $f \in K[x]$ be the minimal polynomial of α. Then*

$$\mathrm{D}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(\alpha)),$$

where $f' \in K[x]$ is the derivative of f.

PROOF. Let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α in an algebraic closure $\overline{K}$ of K. Then

$$f'(x) = \sum_{i=1}^{n} \prod_{\substack{j=1 \\ j \neq i}}^{n} (x - \alpha_j),$$

so we have

$$f'(\alpha_i) = \prod_{\substack{j=1 \\ j \neq i}}^{n} (\alpha_i - \alpha_j)$$

for each i, and the conjugates of $f'(\alpha)$ in $\overline{K}$ are the $f'(\alpha_i)$. We then have

$$N_{L/K}(f'(\alpha)) = \prod_{i=1}^{n} \prod_{\substack{j=1 \\ j \neq i}}^{n} (\alpha_i - \alpha_j) = (-1)^{n(n-1)/2} \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)^2.$$

□

COROLLARY 1.4.16. *Let L/K be a finite separable extension of fields. Then the discriminant of L/K relative to an ordered basis $(\beta_1, \ldots, \beta_n)$ of L is nonzero.*

PROOF. Since L/K is separable, there exists $\alpha \in L$ such that $L = K(\alpha)$. Then $(1, \alpha, \ldots, \alpha^{n-1})$ is an ordered basis of L/K, and there exists an invertible K-linear transformation $T \colon L \to L$ with $T(\alpha^{i-1}) = \beta_i$ for $1 \leq i \leq n$. By Lemma 1.4.6, we have that

$$\mathrm{D}(\beta_1, \beta_2, \ldots, \beta_n) = (\det T)^2 \mathrm{D}(1, \alpha, \ldots, \alpha^{n-1}).$$

It follows Proposition 1.4.13 that $\mathrm{D}(1, \alpha, \ldots, \alpha^{n-1}) \neq 0$, so we have the result. □

REMARK 1.4.17. Together, Lemma 1.4.6 and Corollary 1.4.16 tell us that the discriminant of a finite separable field extension L/K (relative to an ordered basis) reduces to an element of $K^\times/K^{\times 2}$ that is independent of the choice of basis.

DEFINITION 1.4.18. Let B/A be an integral extension of domains such that A is integrally closed, and suppose that B is free of rank n as an A-module. Let $(\beta_1, \ldots, \beta_n)$ be an ordered basis of B as a free A-module. The *discriminant B* over A relative to the basis $(\beta_1, \ldots, \beta_n)$ is $\mathrm{D}(\beta_1, \ldots, \beta_n)$.

LEMMA 1.4.19. *Let A be an integrally closed domain with quotient field K. Let L be a finite separable extension of K, and let B denote the integral closure of A in L. Let $(\alpha_1, \ldots, \alpha_n)$ be any ordered basis of L as a K-vector space that is contained in B. Let $\beta \in L$ be such that $\mathrm{Tr}_{L/K}(\alpha\beta) \in A$ for all $\alpha \in B$. Then*

$$\mathrm{D}(\alpha_1, \ldots, \alpha_n)\beta \in \sum_{i=1}^{n} A\alpha_i.$$

PROOF. Since $\beta \in L$, we may write

$$\beta = \sum_{i=1}^{n} a_i \alpha_i$$

for some $a_i \in K$ for $1 \leq i \leq n$. For any i, we have that

$$\mathrm{Tr}_{L/K}(\alpha_i \beta) = \sum_{j=1}^{n} a_j \mathrm{Tr}_{L/K}(\alpha_i \alpha_j). \tag{1.4.1}$$

The right-hand side of (1.4.1) is the ith term of the product of the matrix $Q = (\mathrm{Tr}_{L/K}(\alpha_i \alpha_j))$ times the column vector with ith entry a_i. Since the determinant of Q is $d = \mathrm{D}(\alpha_1, \ldots, \alpha_n)$, letting $Q^* \in M_n(A)$ denote the adjoint matrix to Q, we have $Q^*Q = dI_n$. Thus, we have $da_i \in A$ for each i. In other words, $d\beta$ lies in the A-module generated by the α_i, so we are done. □

PROPOSITION 1.4.20. *Let A be an integrally closed domain with quotient field K. Let L be a finite separable extension of K, and let B denote the integral closure of A in L. There exists an ordered basis $(\alpha_1, \ldots, \alpha_n)$ of L as a K-vector space contained in B. Moreover, for any such basis, we have*

$$\sum_{i=1}^{n} A\alpha_i \subseteq B \subseteq \sum_{i=1}^{n} Ad^{-1}\alpha_i,$$

where $d = \mathrm{D}(\alpha_1, \ldots, \alpha_n)$.

PROOF. First, take any ordered basis $(\beta_1, \ldots, \beta_n)$ of L/K. By Proposition 1.2.25, there exists $a \in A - \{0\}$ such that $\alpha_i = a\beta_i \in B$ for each $1 \leq i \leq n$. Clearly, $(\alpha_1, \ldots, \alpha_n)$ is a basis of L/K, so in particular, the A-module generated by the α_i is free and contained in B. The other containment is simply a corollary of Lemma 1.4.19 and the fact that $\mathrm{Tr}_{L/K}(B) \subseteq A$. □

The following notion of rank is most interesting for finitely generated modules, though we shall have occasion to use it without this assumption.

DEFINITION 1.4.21. The *rank* of a module M over a domain A is

$$\mathrm{rank}_A(M) = \dim_K(K \otimes_A M).$$

COROLLARY 1.4.22. *Let A be an integrally closed Noetherian domain with quotient field K. Let L be a finite separable extension of K, and let B denote the integral closure of A in L. Then B is a finitely generated, torsion-free A-module of rank $[L : K]$.*

PROOF. By Proposition 1.4.20, we have free A-modules M and M' of rank $n = [L : K]$ such that $M \subseteq B \subseteq M'$. Since M' has no A-torsion, neither does B. We have

$$K \otimes_A M \subseteq K \otimes_A B \subseteq K \otimes_A M'.$$

As M and M' are both isomorphic to A^n, their tensor products over A with K are n-dimensional K-vector spaces, which forces $K \otimes_A B$ to have K-dimension n as well. Moreover, B is finitely generated being a submodule of a finitely generated module over A, as A is Noetherian. □

PROPOSITION 1.4.23. *Let A be an integrally closed Noetherian domain with quotient field K. Let L be a finite separable extension of K, and let B denote the integral closure of A in L. Then any finitely generated, nonzero B-submodule of L is a torsion-free A-module of rank $[L : K]$.*

PROOF. Let M be a finitely generated, nonzero B-submodule of L. If $\beta \in L^\times$, then the multiplication-by-β map $B \to B\beta$ is an isomorphism of B-modules, so $B\beta$ has rank $[L : K]$ as an A-module. In particular, $\mathrm{rank}_A(M) \geq \mathrm{rank}_A(B)$, taking $\beta \in M$. Since M is B-finitely generated and contained in the quotient field of B, there exists $\alpha \in B$ such that $\alpha M \subseteq B$. Since multiplication by α is an isomorphism, $\mathrm{rank}_A(M) \leq \mathrm{rank}_A(B)$. The result now follows from Corollary 1.4.22. □

COROLLARY 1.4.24. *Let A be a PID with quotient field K, let L be a finite separable extension of K, and let B denote the integral closure of K in L. Then any finitely generated, nonzero B-submodule of L is a free A-module of rank $[L:K]$.*

PROOF. By the structure theorem for modules over a PID, any torsion-free rank n module over A is isomorphic to A^n. The result is then immediate from Proposition 1.4.23. □

We have the following application to number fields.

LEMMA 1.4.25. *Let K be a number field. Then the discriminant of $\mathscr{O}_K$ over $\mathbb{Z}$ is independent of the choice of ordered basis of $\mathscr{O}_K$ as a free $\mathbb{Z}$-module.*

PROOF. By Corollary 1.4.24, the ring $\mathscr{O}_K$ is free of rank $n = [K:\mathbb{Q}]$ over $\mathbb{Z}$. If $\beta_1,\dots,\beta_n$ and $\alpha_1,\dots,\alpha_n$ are bases of $\mathscr{O}_K$ as a free $\mathbb{Z}$-module, then there exists a $\mathbb{Q}$-linear homomorphism $T: K \to K$ such that $T(\alpha_i) = \beta_i$ for all i. Then

$$\mathrm{D}(\beta_1,\dots,\beta_n) = \det(T)^2 \mathrm{D}(\alpha_1,\dots,\alpha_n),$$

and $\det(T)$ is a unit in $\mathbb{Z}$, so in $\{\pm 1\}$, which is to say that $\det(T)^2 = 1$. □

DEFINITION 1.4.26. If K is a number field, the *discriminant* $\mathrm{disc}(K)$ of K is the discriminant of $\mathscr{O}_K$ over $\mathbb{Z}$ relative to any basis of $\mathscr{O}_K$ as a free $\mathbb{Z}$-module.

Noting Theorem 1.2.28, the case of quadratic fields is immediately calculated as in Example 1.4.14.

PROPOSITION 1.4.27. *Let $K = \mathbb{Q}(\sqrt{d})$, where $d \neq 1$ is a square-free integer. Then*

$$\mathrm{disc}(K) = \begin{cases} d & d \equiv 1 \bmod 4, \\ 4d & d \equiv 2,3 \bmod 4. \end{cases}$$

We end with the following general result.

PROPOSITION 1.4.28. *Let A be an integrally closed domain with quotient field K. Let L and L' be finite separable extensions of K that are linearly disjoint, and let B and B' denote the integral closures of A in these fields, respectively. Suppose that B is A-free with basis $\beta_1,\dots,\beta_n$ and that B' is A-free with basis $\gamma_1,\dots,\gamma_m$. Set $d = \mathrm{D}(\beta_1,\dots,\beta_n)$ and $d' = \mathrm{D}(\gamma_1,\dots,\gamma_m)$. Then the K-basis of LL' consisting of the elements $\beta_i\gamma_j$ for $1 \le i \le m$ and $1 \le j \le n$ has discriminant $d^m(d')^n$. Moreover, if we let C denote the integral closure of A in LL' and C' denote the A-algebra that is the A-span of the $\beta_i\gamma_j$, then $(d,d')C \subseteq C'$.*

PROOF. Since L and L' are linearly disjoint, LL' is a field extension of K of degree $[L:K][L':K]$ with K-basis the $\beta_i\gamma_j$. Let $\alpha \in C$, and write

$$\alpha = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}\beta_i\gamma_j$$

for some $a_{ij} \in K$. Set

$$\delta_j = \sum_{i=1}^{n} a_{ij}\beta_i \in L$$

for each $1 \leq j \leq m$, so $\alpha = \sum_{j=1}^{m} \delta_j \gamma_j$.

Let $\overline{K}$ be an algebraic closure of K containing L, and let $\tau_1, \ldots, \tau_m$ be the distinct field embeddings of LL' in $\overline{K}$ that fix L. Let $M = (\tau_i \gamma_j) \in M_m(\overline{K})$, and let $w = (\delta_1, \ldots, \delta_m) \in L^m$. Then $Mw = v$, where

$$v = (\tau_1\alpha, \ldots, \tau_m\alpha).$$

Let M^* be the adjoint matrix to M, so we have $M^*v = \det(M)w$. As the entries of M and v are contained in the integral closure $\overline{A}$ of A in $\overline{K}$, the vector $\det(M)w \in \overline{K}^n$ has entries in $\overline{A}$ as well. Note that $\det(M)^2 = d'$ by Proposition 1.4.10, so in fact $d'w$ has entries in $\overline{A} \cap L$, which is to say that $d'\delta_j \in B$ for each j. Since the β_i form a basis for B over A, we have that $d'a_{ij} \in A$ for all i and j. The analogous argument tells us that $da_{ij} \in A$ for all i and j as well, so $(d, d')\alpha \in C'$, as we set out to prove.

Finally, we compute the discriminant of the basis $\beta_i\gamma_j$. Let $\sigma_1, \ldots, \sigma_n$ be the field embeddings of LL' in an algebraic closure $\overline{K}$ of K that fix L', so

$$\{\sigma_i\tau_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$$

is the set of field embeddings of LL' in $\overline{K}$ that fix K. Let Q be the matrix in $M_{nm}(\overline{K})$ which we think of as consisting of n^2 square blocks of size m by m each, the (i,j)th of which is the matrix $\sigma_i\beta_j M$. Then Q is a product of two matrices, the first of which is block diagonal with m copies of $N = (\sigma_i\beta_j)_{i,j}$, and the second of which consists of n^2 square blocks, the (i', j')th of which is the identity times $\tau_{i'}\gamma_{j'}$. Letting M be as before, a simple computation then tells us that

$$\mathrm{D}(\beta_i\gamma_j \mid 1 \leq i \leq n, 1 \leq j \leq m) = \det(Q)^2 = \det(N)^{2m}\det(M)^{2n} = d^m(d')^n.$$

□

1.5. Normal bases

DEFINITION 1.5.1. A *normal basis* of a finite Galois extension L/K is a basis of L as a K-vector space of the form $\{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(L/K)\}$ for some $\alpha \in L$.

The goal of this section is to prove E. Noether's theorem that every finite Galois extension has a normal basis. We start with the following lemma.

LEMMA 1.5.2. *Let L/K be a finite Galois extension with Galois group $\{\sigma_1, \ldots, \sigma_n\}$, where $n = [L : K]$. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of L as a K-vector space. Then the set*

$$\{(\sigma_1(\alpha_j), \ldots, \sigma_n(\alpha_j)) \mid 1 \leq j \leq n\}$$

is an L-basis of L^n.

PROOF. By Corollary 1.4.16, the discriminant $D(\alpha_1,\dots,\alpha_n)$ is nonzero. By Proposition 1.4.10, this discriminant is the square of $\det(\sigma_i\alpha_j)_{i,j}$. Since the latter determinant is therefore nonzero, the vectors in question are linearly independent over L. □

LEMMA 1.5.3. *Every finite cyclic extension of fields has a normal basis.*

PROOF. Let L/K be finite cyclic of degree n, generated by an element σ. Then $K[\mathrm{Gal}(L/K)]$ is isomorphic to $K[x]/(x^n-1)$ via the unique K-algebra homomorphism that takes σ to x. As L is a $K[\mathrm{Gal}(L/K)]$-module, it becomes a $K[x]$-module annihilated by x^n-1. If $f=\sum_{i=0}^{n-1} c_i x^i \in K[x]$ annihilates L, then $\sum_{i=0}^{n-1} c_i\sigma^i(\alpha)=0$ for all $\alpha\in L$, which by the linear independence of the σ^i forces f to be zero. Thus, the annihilator of L is (x^n-1), and by the structure theorem for finitely generated modules over the PID $K[x]$, this means that L has a $K[x]$-summand isomorphic to $K[x]/(x^n-1)$, generated by some $\alpha\in L$. Since the latter module has K-dimension n, as does L, the elements $\{\alpha,\sigma(\alpha),\dots,\sigma^{n-1}(\alpha)\}$ form a K-basis of L.

□

THEOREM 1.5.4 (Normal basis theorem). *Every finite Galois extension of fields has a normal basis.*

PROOF. Let L/K be a finite Galois extension of degree n. Since any finite extension of finite fields is cyclic, we may by Lemma 1.5.3 suppose that K is infinite. Write $\mathrm{Gal}(L/K)=\{\sigma_1,\dots,\sigma_n\}$ and $\sigma_1=1$. Let $\{\alpha_1,\dots,\alpha_n\}$ be a basis of L as a K-vector space. It suffices to find $\beta\in L$ with $\mathrm{D}(\sigma_1(\beta),\dots,\sigma_n(\beta))\neq 0$ by Corollary 1.4.16.

Define an element $p\in L[x_1,\dots,x_n]$ by

$$p(x_1,\dots,x_n)=\det\left(\sum_{k=1}^{n}\sigma_j^{-1}\sigma_i(\alpha_k)x_k\right)^2.$$

Note that the coefficients of p are fixed by the elements of $\mathrm{Gal}(L/K)$, since they permute the columns of the matrix. By Lemma 1.5.2, we can find $\beta_j\in L$ for $1\le j\le n$ be such that

$$\sum_{j=1}^{n}\beta_j(\sigma_1(\alpha_j),\sigma_2(\alpha_j),\dots,\sigma_n(\alpha_j))=(1,0,\dots,0).$$

Then for all $1\le i,j\le n$, we have

$$\sum_{k=1}^{n}\sigma_j^{-1}\sigma_i(\alpha_k)\beta_k=\delta_{i,j},$$

so $p(\beta_1,\dots,\beta_n)=\det(I_n)^2=1$, so $p\neq 0$. Since K is infinite, there exist $a_1,\dots,a_n\in K$ with $p(a_1,\dots,a_n)\neq 0$. For $\gamma=\sum_{j=1}^{n}a_i\alpha_i$, we have by Proposition 1.4.10 the first equality in

$$\mathrm{D}(\sigma_1(\gamma),\dots,\sigma_n(\gamma))=\det(\sigma_j^{-1}\sigma_i(\gamma))^2=p(a_1,\dots,a_n)\neq 0.$$

□

CHAPTER 2

Dedekind domains

2.1. Fractional ideals

We make the following general definition.

DEFINITION 2.1.1. A *fractional ideal* of a domain A is a nonzero A-submodule $\mathfrak{a}$ of the quotient field of A for which there exists a nonzero $d \in A$ such that $d\mathfrak{a} \subseteq A$.

REMARK 2.1.2. Every nonzero ideal in a domain A is a fractional ideal, which is sometimes referred to as an integral ideal. Every fractional ideal of A that is contained in A is an integral ideal.

EXAMPLE 2.1.3. The fractional ideals of $\mathbb{Z}$ are exactly the $\mathbb{Z}$-submodules of $\mathbb{Q}$ generated by a nonzero rational number.

LEMMA 2.1.4. *Let A be a Noetherian domain. A nonzero A-submodule of the quotient field of A is a fractional ideal if and only if it is finitely generated.*

PROOF. If $\mathfrak{a}$ is a finitely generated A-submodule of the quotient field of A, then let $d \in A$ denote the product of the denominators of a set of generators. Then $d\mathfrak{a} \subseteq A$. Conversely, suppose that $\mathfrak{a}$ is a fractional ideal and $d \in A$ is nonzero and satisfies $d\mathfrak{a} \subseteq A$. Then $d\mathfrak{a}$ is an ideal of A, hence finitely generated. Moreover, the multiplication-by-d map carries $\mathfrak{a}$ isomorphically onto $d\mathfrak{a}$. □

DEFINITION 2.1.5. Let A be a domain with quotient field K, and let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional ideals of A.

a. The inverse of $\mathfrak{a}$ is $\mathfrak{a}^{-1} = \{b \in K \mid b\mathfrak{a} \subseteq A\}$.

b. The product of $\mathfrak{a}$ and $\mathfrak{b}$ is the A-submodule of K generated by the set $\{ab \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$.

REMARK 2.1.6. By definition, multiplication of fractional ideals is an associative (and commutative) operation.

LEMMA 2.1.7. *Let A be a domain, and let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional ideals of A. Then $\mathfrak{a}^{-1}$, $\mathfrak{a}+\mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$, $\mathfrak{a} \cap \mathfrak{b}$ are fractional ideals of A as well.*

PROOF. Let K denote the quotient field of A. Let $c, d \in A$ be nonzero such that $c\mathfrak{a} \subseteq A$ and $d\mathfrak{b} \subseteq A$. Then $c(\mathfrak{a} \cap \mathfrak{b}) \subseteq A$, $cd(\mathfrak{a}+\mathfrak{b}) \subseteq A$, and $cd\mathfrak{a}\mathfrak{b} \subseteq A$.

Note that $\mathfrak{a}^{-1}$ is an A-submodule of K which is nonzero since there exists $d \in A$ with $d\mathfrak{a} \subset A$ in that $\mathfrak{a}$ is a fractional ideal. Let $a \in \mathfrak{a}$ be nonzero, and let $e \in A$ be its numerator in a representation

of a as a fraction, so $e \in \mathfrak{a}$ as well. For any $c \in \mathfrak{a}^{-1}$, we have $ce \in A$ by definition, so $e\mathfrak{a}^{-1} \subseteq A$, and therefore $\mathfrak{a}^{-1}$ is a fractional ideal. □

DEFINITION 2.1.8. We say that a fractional ideal $\mathfrak{a}$ of a domain A is *invertible* if there exists a fractional ideal $\mathfrak{b}$ of A such that $\mathfrak{ab} = A$.

LEMMA 2.1.9. *A fractional ideal $\mathfrak{a}$ of a domain A is invertible if and only if $\mathfrak{a}\mathfrak{a}^{-1} = A$.*

PROOF. For the nonobvious direction, suppose that $\mathfrak{a}$ is invertible. Then we must have $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$ by definition of $\mathfrak{a}^{-1}$. On the other hand,

$$A = \mathfrak{ba} \subseteq \mathfrak{a}^{-1}\mathfrak{a} \subseteq A,$$

so we must have $\mathfrak{a}^{-1}\mathfrak{a} = A$. □

EXAMPLE 2.1.10. Consider the maximal ideal (x,y) of $\mathbb{Q}[x,y]$. If $f \in \mathbb{Q}(x,y)^\times$ is such that $fx \in \mathbb{Q}[x,y]$ (resp., $fy \in \mathbb{Q}[x,y]$) then its denominator is a divisor of x (resp., y). Therefore $(x,y)^{-1} = \mathbb{Q}[x,y]$, and we have

$$(x,y) \cdot (x,y)^{-1} = (x,y) \neq \mathbb{Q}[x,y].$$

Thus, (x,y) is not invertible as a fractional ideal.

DEFINITION 2.1.11. A *principal fractional ideal* of A is an A-submodule (a) generated by a nonzero element a of the quotient field of A.

LEMMA 2.1.12. *Let $\mathfrak{a}$ be a fractional ideal of a PID. Then $\mathfrak{a}$ is principal.*

PROOF. There exists $d \in A$ such that $d\mathfrak{a} = (b)$ for some $b \in A$. Then $\frac{b}{d} \in \mathfrak{a}$ and given any $c \in \mathfrak{a}$, we have $dc = ba$ for some $a \in A$, so $c = a\frac{b}{d}$. That is, $\mathfrak{a} = (\frac{b}{d})$. □

LEMMA 2.1.13. *Let A be a domain, and let a be a nonzero element of its quotient field. Then (a) is invertible, and $(a)^{-1} = (a^{-1})$.*

PROOF. If $x \in (a)^{-1}$, then $xa = b$ for some $b \in A$, so $x = ba^{-1} \in (a^{-1})$. If $x \in (a^{-1})$, then $x = a^{-1}b$ for some $b \in A$. On other hand, any $z \in (a)$ has the form $z = ya$ for some $y \in A$, and we have $xz = a^{-1}bya = by \in A$, so $x \in (a)^{-1}$. We then have

$$(a)(a)^{-1} = (a)(a^{-1}) = (aa^{-1}) = A,$$

completing the proof. □

2.2. Dedekind domains

DEFINITION 2.2.1. A *Dedekind domain* is a Noetherian, integrally closed domain, every nonzero prime ideal of which is maximal.

We have the following class of examples.

LEMMA 2.2.2. *Every PID is a Dedekind domain.*

PROOF. A PID is Noetherian, and it is a UFD, so it is integrally closed. Its nonzero prime ideals are maximal, generated by its irreducible elements. □

EXAMPLES 2.2.3.

a. The ring $\mathbb{Z}$ is a Dedekind domain by Lemma 2.2.2, since $\mathbb{Z}$ is a PID.

b. If K is a field, then $K[x]$ is a Dedekind domain, since $K[x]$ is a PID.

LEMMA 2.2.4. *Let A be an integral domain, and let B be a commutative ring extension of A that is integral over A. If $\mathfrak{b}$ is an ideal of B that contains a nonzero element which is not a zero divisor, then $\mathfrak{b} \cap A$ is a nonzero ideal of A.*

PROOF. That $\mathfrak{b} \cap A$ is an ideal is clear, so it suffices to show that $\mathfrak{b} \cap A$ is nonzero. Let $\beta \in \mathfrak{b}$ be nonzero and not a zero divisor. Then β is a root of some monic polynomial $g \in A[x]$. Write $g = x^n f$ for some nonzero $f \in A[x]$ with nonzero constant term. Since $\beta \in \mathfrak{b}$, we have $f(\beta) - f(0) \in \mathfrak{b}$, and as $f(\beta) = 0$ given that β is not a zero divisor, we have $f(0) \in \mathfrak{b}$. But $f(0) \neq 0$, so $\mathfrak{b}$ has a nonzero element. □

The following proposition allows us to produce many more examples of Dedekind domains.

PROPOSITION 2.2.5. *Let A be an integral domain in which every nonzero prime ideal is maximal, and let B be a domain that is an integral extension of A. Then every nonzero prime ideal in B is maximal.*

PROOF. Let $\mathfrak{P}$ be a nonzero prime ideal in B, and let $\mathfrak{p} = \mathfrak{P} \cap A$. Note that $F = A/\mathfrak{p}$ is a field as $\mathfrak{p}$ is a nonzero (prime) ideal of A by Lemma 2.2.4. For $\beta \in B$, let $f \in A[x]$ be a monic polynomial such that β is a root of f. Let $\bar{f} \in F[x]$ denote the image of f under the natural quotient map $A[x] \to F[x]$. Let $\bar{\beta}$ denote the image of β in $B/\mathfrak{P}$. Then $\bar{f}(\bar{\beta})$ is the image of $f(\beta) = 0$ in $B/\mathfrak{P}$ so is itself 0. In other words, $\bar{\beta}$ is algebraic over F. Thus, $B/\mathfrak{P} = F[\{\bar{\beta} \mid \beta \in B\}]$ is a field. In other words, $\mathfrak{P}$ is maximal. □

COROLLARY 2.2.6. *Let A be a Dedekind domain, and let B be the integral closure of A in a finite, separable extension of the quotient field of A. Then B is a Dedekind domain.*

PROOF. Note that B is a finitely generated A-module by Corollary 1.4.22. If $\mathfrak{b}$ is an ideal of B, then $\mathfrak{b}$ is an A-submodule of B, and as A is Noetherian, it is therefore finitely generated. Thus, B is Noetherian. That B is integrally closed is just Proposition 1.2.23. That every nonzero prime ideal in A is maximal is Proposition 2.2.5. □

We have the following immediate corollary.

COROLLARY 2.2.7. *The ring of integers of any number field is a Dedekind domain.*

More examples of Dedekind domains can be produced as follows.

PROPOSITION 2.2.8. *Let A be a Dedekind domain, and let S be a multiplicatively closed subset of A. Then $S^{-1}A$ is also a Dedekind domain.*

PROOF. Given an ideal $\mathfrak{b}$ of $S^{-1}A$, set $\mathfrak{a} = A \cap \mathfrak{b}$. Then $\mathfrak{a}$ is an ideal of A, and $\mathfrak{b} = S^{-1}\mathfrak{a}$. It follows that any set of generators of $\mathfrak{a}$ as an ideal of A generates $S^{-1}\mathfrak{a}$ as an ideal of $S^{-1}A$. Hence $S^{-1}A$ is Noetherian. If, moreover, $\mathfrak{b}$ is a nonzero prime, then clearly $\mathfrak{a}$ is as well, and $\mathfrak{a}$ is maximal since A is a Dedekind domain. Then $S^{-1}A/\mathfrak{b} \cong A/\mathfrak{a}$ is a field, so $\mathfrak{b}$ is maximal as well.

Let K be the quotient field of A. Any $\alpha \in K$ that is integral over $S^{-1}A$ satisfies a monic polynomial f with coefficients in $S^{-1}A$. Set $n = \deg f$. If $d \in S$ is the product of the denominators of these coefficients, then $d^n f(d^{-1}x) \in A[x]$ is monic with $d\alpha \in K$ as a root. Since A is integrally closed, we have $d\alpha \in A$, so $\alpha \in S^{-1}A$. That is, $S^{-1}A$ is integrally closed. □

LEMMA 2.2.9. *Let A be a Noetherian domain, and let $\mathfrak{a}$ be a nonzero ideal of A.*

a. There exist $k \geq 0$ and nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ of A such that $\mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq \mathfrak{a}$.

b. Suppose that every nonzero prime ideal of A is maximal. If $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are as in part a and $\mathfrak{p}$ is a prime ideal of A containing $\mathfrak{a}$, then $\mathfrak{p} = \mathfrak{p}_i$ for some positive $i \leq k$.

PROOF. Consider the set X of nonzero ideals of A for which the statement of the first part of the lemma fails, and order X by inclusion. Suppose by way of contradiction that X is nonempty. Let C be a chain in X. Either C has a maximal element or there exist $\mathfrak{a}_i \in C$ for $i \geq 1$ with $\mathfrak{a}_i \subsetneq \mathfrak{a}_{i+1}$ for each i. The latter is impossible as A is a Noetherian. By Zorn's lemma, X contains a maximal element $\mathfrak{a}$. Now $\mathfrak{a}$ is not prime since it lies in X, so let $a, b \in A - \mathfrak{a}$ with $ab \in \mathfrak{a}$. Then $\mathfrak{a} + (a)$ and $\mathfrak{a} + (b)$ both properly contain $\mathfrak{a}$, so by maximality of $\mathfrak{a}$, there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_l$ of A for some $k, l \geq 0$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq \mathfrak{a} + (a)$ and $\mathfrak{q}_1 \cdots \mathfrak{q}_l \subseteq \mathfrak{a} + (b)$. We then have

$$\mathfrak{p}_1 \cdots \mathfrak{p}_k \mathfrak{q}_1 \cdots \mathfrak{q}_l \subseteq (\mathfrak{a} + (a))(\mathfrak{a} + (b)) \subseteq \mathfrak{a},$$

a contradiction of $\mathfrak{a} \in X$. This proves part a.

Now, suppose that $\mathfrak{a}$ is proper, and let $\mathfrak{p}$ be a prime ideal containing $\mathfrak{a}$. Assume that every nonzero prime ideal of A is maximal. If no $\mathfrak{p}_i$ equals $\mathfrak{p}$, then since $\mathfrak{p}_i$ is maximal, there exist $b_i \in \mathfrak{p}_i$ with $b \notin \mathfrak{p}$ for each $1 \leq i \leq k$. We then have $b_1 \cdots b_k \notin \mathfrak{p}$ as $\mathfrak{p}$ is prime, so $b_1 \cdots b_k \notin \mathfrak{a}$, a contradiction. Hence we have part b. □

LEMMA 2.2.10. *Let A be a Dedekind domain, and let $\mathfrak{p}$ be a nonzero prime ideal of A. Then $\mathfrak{p}\mathfrak{p}^{-1} = A$.*

PROOF. Let $a \in \mathfrak{p}$ be nonzero. Noting Lemma 2.2.9a, we let $k \geq 1$ be minimal such that there exist nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ of A with $\mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq (a)$. By Lemma 2.2.9b, we may without loss of generality suppose that $\mathfrak{p}_k = \mathfrak{p}$. Let $b \in \mathfrak{p}_1 \cdots \mathfrak{p}_{k-1}$ be such that $b \notin (a)$. Then $a^{-1}b \notin A$, but

we have

$$a^{-1}b\mathfrak{p} \subseteq a^{-1}\mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq A,$$

which implies that $a^{-1}b \in \mathfrak{p}^{-1}$. Moreover, if $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$, then $a^{-1}b\mathfrak{p} \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is finitely generated, Proposition 1.2.4 tells us that $a^{-1}b$ is integral over A. But A is integrally closed, so we have a contradiction. That is, we must have $\mathfrak{p} \subsetneq \mathfrak{p}^{-1}\mathfrak{p} \subseteq A$, from which it follows that $\mathfrak{p}^{-1}\mathfrak{p} = A$ by maximality of $\mathfrak{p}$. □

THEOREM 2.2.11. *Let A be a Dedekind domain, and let $\mathfrak{a}$ be a fractional ideal of A. Then there exist $k \geq 0$, distinct nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$, unique up to ordering, and unique nonzero $r_i \in \mathbb{Z}$ for $1 \leq i \leq k$ such that $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$. Moreover, $\mathfrak{a}$ is an ideal of A if and only if every r_i is positive.*

PROOF. First suppose that $\mathfrak{a}$ is a nonzero ideal of A. We work by induction on a nonnegative integer m such that there are nonzero prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ of $\mathfrak{a}$ (not necessarily distinct) with $\mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq \mathfrak{a}$, which exists by Lemma 2.2.9a. If $m = 0$, then $A \subseteq \mathfrak{a}$, so $\mathfrak{a} = A$. For $m \geq 1$, we may suppose that $\mathfrak{a}$ is proper, so there exists a nonzero prime ideal $\mathfrak{p}$ that contains $\mathfrak{a}$ and $\mathfrak{p} = \mathfrak{q}_i$ for some $i \leq m$. Without loss of generality, we take $i = m$. Then

$$\mathfrak{q}_1 \cdots \mathfrak{q}_{m-1} \subseteq \mathfrak{q}_1 \cdots \mathfrak{q}_m\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq A.$$

By induction, there exist nonzero prime ideals $\mathfrak{q}_1', \ldots, \mathfrak{q}_\ell'$ of A for some $\ell < m$ such that $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{q}_1' \cdots \mathfrak{q}_\ell'$. The desired factorization is given by multiplying by $\mathfrak{p}$, applying Lemma 2.2.10, and gathering together nondistinct primes.

In general, for a fractional ideal $\mathfrak{a}$, we let $d \in A$ be such that $d\mathfrak{a} \subseteq A$. We write $d\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_m$ for some $m \geq 0$ and prime ideals $\mathfrak{q}_i$ for $1 \leq i \leq m$. We also write $(d) = \mathfrak{l}_1 \cdots \mathfrak{l}_n$ for some $n \geq 0$ and prime ideals $\mathfrak{l}_i$ for $1 \leq i \leq n$. By Lemma 2.2.10, we then have

$$\mathfrak{a} = (d)^{-1}(d\mathfrak{a}) = \mathfrak{l}_1^{-1} \cdots \mathfrak{l}_n^{-1}\mathfrak{q}_1 \cdots \mathfrak{q}_m.$$

If $\mathfrak{q}_i = \mathfrak{l}_j$ for some i and j, then we may use Lemma 2.2.10 to remove $\mathfrak{q}_i\mathfrak{l}_j^{-1}$ from the product. Hence we have the desired factorization.

Now suppose that

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k} = \mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_l^{s_l}$$

for some $k, l \geq 0$, distinct primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$, distinct primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_l$, nonzero $r_1, \ldots, r_k$, and nonzero $s_1, \ldots, s_l$. If $r_i < 0$ (resp., $s_i < 0$) for some i, we multiply both sides by $\mathfrak{p}_i^{-r_i}$ (resp., $\mathfrak{q}_i{}^{-s_i}$) and obtain an equality of two products that involve only integral ideals. So, we assume without loss of generality that all r_i and s_i are positive. We may suppose that $t = \sum_{i=1}^k r_i$ is minimal among all factorizations of $\mathfrak{a}$. If $t = 0$, then $k = 0$, and then l must be zero so that $\mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_l^{s_l}$ is non-proper. If t is positive, then $\mathfrak{p}_k$ contains $\mathfrak{a}$, so Lemma 2.2.9b tells us that $\mathfrak{p}_k = \mathfrak{q}_i$ for some $1 \leq i \leq l$. Multiplying both sides by $\mathfrak{p}_k^{-1}$, the quantity t is decreased by one. By induction, we have that the remaining terms are the same up to reordering, hence the result. □

DEFINITION 2.2.12. We say that an ideal $\mathfrak{b}$ of a commutative ring A *divides* an ideal $\mathfrak{a}$ of A if there exists an ideal $\mathfrak{c}$ of A such that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. We write $\mathfrak{b} \mid \mathfrak{a}$ to denote that $\mathfrak{b}$ divides $\mathfrak{a}$.

COROLLARY 2.2.13. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be nonzero ideals in a Dedekind domain A.*

a. The ideals $\mathfrak{a}$ and $\mathfrak{b}$ are not divisible by a common prime ideal if and only if $\mathfrak{a}+\mathfrak{b} = A$.

b. Suppose that $\mathfrak{a} \subseteq \mathfrak{b}$. Then $\mathfrak{b}$ divides $\mathfrak{a}$.

PROOF. For part a, note that if $\mathfrak{p} \mid \mathfrak{a}$ and $\mathfrak{p} \mid \mathfrak{b}$ for some prime ideal $\mathfrak{p}$, then $\mathfrak{p} \mid (\mathfrak{a}+\mathfrak{b})$, so $\mathfrak{a}+\mathfrak{b} \neq A$. On the other hand, if there is no such $\mathfrak{p}$, then $\mathfrak{a}$ and $\mathfrak{b}$ are not contained in any common maximal ideal (since $\mathfrak{p}$ divides $\mathfrak{a}$ if and only if it occurs in its factorization), so $\mathfrak{a}+\mathfrak{b} = A$.

For part b, using Theorem 2.2.11, write $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ (resp., $\mathfrak{b} = \mathfrak{q}_1 \cdots \mathfrak{q}_l$) for some nonzero prime ideals $\mathfrak{p}_i$ (resp., $\mathfrak{q}_j$) of A. Suppose without loss of generality that $\mathfrak{p}_i = \mathfrak{q}_i$ for all $1 \leq i \leq t$ for some nonnegative $t \leq \min(k,l)$ and that $\mathfrak{p}_i$ (resp., $\mathfrak{q}_i$) does not occur in the factorization of $\mathfrak{b}$ (resp., $\mathfrak{a}$) for $i > t$. Then

$$\mathfrak{b} = \mathfrak{a}+\mathfrak{b} = \mathfrak{q}_1 \cdots \mathfrak{q}_t(\mathfrak{p}_{t+1} \cdots \mathfrak{p}_k + \mathfrak{q}_{t+1} \cdots \mathfrak{q}_l) = \mathfrak{q}_1 \cdots \mathfrak{q}_t,$$

the last step using part a. We therefore have $t = l$, so $\mathfrak{b}$ divides $\mathfrak{a}$. □

DEFINITION 2.2.14. Let A be a Dedekind domain, and let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of A. The *greatest common divisor* of $\mathfrak{a}$ and $\mathfrak{b}$ is $\mathfrak{a}+\mathfrak{b}$.

REMARK 2.2.15. By Lemma 2.2.13, $\mathfrak{a}+\mathfrak{b}$ contains and hence divides both $\mathfrak{a}$ and $\mathfrak{b}$ and is the smallest ideal that does so. (The use of the word "greatest", as opposed to "smallest", is in analogy with greatest common divisors of pairs of integers.)

DEFINITION 2.2.16. Let A be a Dedekind domain. The set $I(A)$ of fractional ideals of A is called the *ideal group* of A.

We have the following immediate corollary of Theorem 2.2.11.

COROLLARY 2.2.17. *The ideal group $I(A)$ of a Dedekind domain A is a group under multiplication of fractional ideals with identity A, the inverse of $\mathfrak{a} \in I(A)$ being $\mathfrak{a}^{-1}$.*

DEFINITION 2.2.18. Let A be a Dedekind domain. Then we let $P(A)$ denote the set of its principal fractional ideals. We refer to this as the *principal ideal group*.

COROLLARY 2.2.19. *Let A be a Dedekind domain. The group $P(A)$ is a subgroup of $I(A)$.*

DEFINITION 2.2.20. The *class group* (or *ideal class group*) of a Dedekind domain A is $\mathrm{Cl}(A) = I(A)/P(A)$, the quotient of the ideal group by the principal ideal group.

LEMMA 2.2.21. *A Dedekind domain A is a PID if and only if $\mathrm{Cl}(A)$ is trivial.*

PROOF. Every element of $I(A)$ has the form $\mathfrak{a}\mathfrak{b}^{-1}$ where $\mathfrak{a}$ and $\mathfrak{b}$ are nonzero ideals of A. If A is a PID, then both $\mathfrak{a}$ and $\mathfrak{b}$ are principal and, therefore, so is $\mathfrak{a}\mathfrak{b}^{-1}$. On the other hand, if $\mathfrak{a}$ is a nonzero ideal of A with $\mathfrak{a} = (a)$ for some $a \in K$, then clearly $a \in A$, so $\mathrm{Cl}(A)$ being trivial implies that A is a PID. □

NOTATION 2.2.22. Let K be a number field. We let I_K, P_K, and Cl_K denote the ideal group, principal ideal group, and class group of $\mathscr{O}_K$, respectively. We refer to these as the *ideal group* of K, the *principal ideal group* of K, and the *class group* of K, respectively.

EXAMPLE 2.2.23. Let $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathscr{O}_K = \mathbb{Z}[\sqrt{-5}]$. The ideal $\mathfrak{a} = (2, 1+\sqrt{-5})$ is non-principal. To see this, note that $N_{K/\mathbb{Q}}(2) = 4$ and $N_{K/\mathbb{Q}}(1+\sqrt{-5}) = 6$, so any generator x of $\mathfrak{a}$ must satisfy $N_{K/\mathbb{Q}}(x) \in \{\pm 1, \pm 2\}$. But

$$N_{K/\mathbb{Q}}(a+b\sqrt{-5}) = a^2 + 5b^2$$

for $a, b \in \mathbb{Z}$, which forces $x = \pm 1$. This would mean that $\mathfrak{a} = \mathbb{Z}[\sqrt{-5}]$. To see that this cannot happen, define $\phi\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}/6\mathbb{Z}$ by $\phi(a+b\sqrt{-5}) = a-b$ for $a, b \in \mathbb{Z}$. This is a ring homomorphism as

$$\begin{aligned}\phi((a+b\sqrt{-5})(c+d\sqrt{-5})) = \phi(ac-5bd+(ad+bc)\sqrt{-5}) &= ac-5bd-ad-bc \\ &= ac+bd-ad-bc = (a-b)(c-d).\end{aligned}$$

Moreover, $\phi(1+\sqrt{-5}) = 0$, so the kernel of ϕ contains (and is in fact equal to) $(1+\sqrt{-5})$. Therefore, ϕ induces a surjection (in fact, isomorphism),

$$\mathbb{Z}[\sqrt{-5}]/\mathfrak{a} \to \mathbb{Z}/6\mathbb{Z}/(2) \to \mathbb{Z}/2\mathbb{Z},$$

so $\mathfrak{a} \neq \mathbb{Z}[\sqrt{-5}]$, and x does not exist. Therefore, $\mathrm{Cl}_{\mathbb{Q}(\sqrt{-5})}$ is nontrivial.

We end with the following important theorem.

THEOREM 2.2.24. *A Dedekind domain is a UFD if and only if it is a PID.*

PROOF. We need only show that a Dedekind domain that is a UFD is a PID. Let A be such a Dedekind domain. By Theorem 2.2.11, it suffices to show that each nonzero prime ideal $\mathfrak{p}$ of A is principal. Since $\mathfrak{p}$ is prime and A is a UFD, any nonzero element of $\mathfrak{p}$ is divisible by an irreducible element in $\mathfrak{p}$. If π is such an element, then (π) is maximal and contained in $\mathfrak{p}$, so $\mathfrak{p} = (\pi)$. □

2.3. Discrete valuation rings

DEFINITION 2.3.1. A *discrete valuation ring*, or *DVR*, is a principal ideal domain that has exactly one nonzero prime ideal.

LEMMA 2.3.2. *The following are equivalent conditions on a principal ideal domain A.*

i. A is a DVR,

ii. A has a unique nonzero maximal ideal,

iii. A has a unique nonzero irreducible element up to associates.

PROOF. This is a simple consequence of the fact that in a PID, every nonzero prime ideal is maximal generated by any irreducible element it contains. □

DEFINITION 2.3.3. A *uniformizer* of a DVR is a generator of its maximal ideal.

Moreover, we have the following a priori weaker but in fact equivalent condition for a domain to be a DVR.

PROPOSITION 2.3.4. *A domain A is a DVR if and only if it is a local Dedekind domain that is not a field.*

PROOF. A DVR is a PID, hence a Dedekind domain, and it is local by definition. Conversely, suppose that A is Noetherian, integrally closed, and has a unique nonzero prime ideal $\mathfrak{p}$. We must show that A is a PID. Since nonzero ideals factor uniquely as products of primes in A, every ideal of A has the form $\mathfrak{p}^n$ for some n. In particular, $\mathfrak{p} = (\pi)$ for any $\pi \in \mathfrak{p} - \mathfrak{p}^2$, and then $\mathfrak{p}^n = (\pi^n)$ for all n. Therefore, A is a PID and hence a DVR. □

THEOREM 2.3.5. *A Noetherian domain A is a Dedekind domain if and only if its localization at every nonzero prime ideal is a DVR.*

PROOF. We have seen in Proposition 2.2.8 that $A_\mathfrak{p}$ is a Dedekind domain for all nonzero prime ideals $\mathfrak{p}$. By Proposition 2.3.4, each such localization is therefore a DVR.

Conversely, suppose A is a Noetherian integral domain such that $A_\mathfrak{p}$ is a DVR for every nonzero prime ideal $\mathfrak{p}$. We can and do assume that A is not a field and consider the intersection $B = \bigcap_\mathfrak{p} A_\mathfrak{p}$ over all nonzero prime ideals $\mathfrak{p}$ of A, taken inside the quotient field K of A. Clearly, B contains A, and if $\frac{c}{d} \in B$ for some $c, d \in A$ with $d \neq 0$, then we set

$$\mathfrak{a} = \{a \in A \mid ac \in (d)\}.$$

By definition of B, we may write $\frac{c}{d} = \frac{r}{s}$ with $r \in A$ and $s \in A - \mathfrak{p}$, and we see that $sc = rd$, so $s \in \mathfrak{a}$. In other words, we have $\mathfrak{a} \not\subseteq \mathfrak{p}$ for all prime ideals $\mathfrak{p}$ of A, which forces $\mathfrak{a} = A$. This implies that $c \in (d)$, so $\frac{c}{d} \in A$.

Next, suppose that $\mathfrak{q}$ is a nonzero prime ideal of A, and let $\mathfrak{m}$ be a maximal ideal containing it. Then $\mathfrak{q}A_\mathfrak{m}$ is a nonzero prime ideal of $A_\mathfrak{m}$, which is a DVR, so $\mathfrak{q}A_\mathfrak{m} = \mathfrak{m}A_\mathfrak{m}$. Since $\mathfrak{q}$ and $\mathfrak{m}$ are prime ideals contained in $\mathfrak{m}$, we therefore have

$$\mathfrak{q} = A \cap \mathfrak{q}A_\mathfrak{m} = A \cap \mathfrak{m}A_\mathfrak{m} = \mathfrak{m}.$$

Thus, every nonzero prime ideal is maximal.

Finally, each $A_{\mathfrak{p}}$ is integrally closed in K by Corollary 1.2.20, and then the intersection A is as well, since any element of K that is integral over A is integral over each $A_{\mathfrak{p}}$, hence contained in each $A_{\mathfrak{p}}$. That is, A satisfies the conditions in the definition of a Dedekind domain. □

To make some sense of the name "discrete valuation ring", we define the notion of a discrete valuation. For this purpose, we adjoin an element ∞ to $\mathbb{Z}$ which is considered larger than any element of $\mathbb{Z}$, and we set $x+y=\infty$ if $x,y\in\mathbb{Z}\cup\{\infty\}$ and either x or y equals ∞.

DEFINITION 2.3.6. Let K be a field. A *discrete valuation* on K is a surjective map $v\colon K\to\mathbb{Z}\cup\{\infty\}$ such that

i. $v(a)=\infty$ if and only $a=0$,

ii. $v(ab)=v(a)+v(b)$, and

iii. $v(a+b)\geq\min(v(a),v(b))$

for all $a,b\in K$.

DEFINITION 2.3.7. If v is a discrete valuation on a field K, then the quantity $v(a)$ for $a\in K$ is said to be the *valuation* of a with respect to v.

The following are standard examples of discrete valuations.

EXAMPLE 2.3.8. Let p be a prime number. Then the p-adic valuation v_p on $\mathbb{Q}$ is defined by $v_p(0)=\infty$ and $v_p(a)=r$ for $a\in\mathbb{Q}^\times$ if $a=p^ra'$ for some $r\in\mathbb{Z}$ and $a'\in\mathbb{Q}^\times$ such that p divides neither the numerator nor denominator of a' in reduced form.

EXAMPLE 2.3.9. Let F be a field, and consider the function field $F(t)$. The valuation at ∞ on $F(t)$ is defined by $v_\infty(\frac{g}{h})=\deg h-\deg g$ for $g,h\in F[t]$ with $h\neq 0$, taking $\deg 0=-\infty$.

More generally, we have the following.

DEFINITION 2.3.10. Let A be a Dedekind domain with quotient field K, and let $\mathfrak{p}$ be a nonzero prime ideal of A. The $\mathfrak{p}$-*adic valuation* $v_{\mathfrak{p}}$ on K is defined on $a\in K^\times$ as the unique integer such that $(a)=\mathfrak{p}^{v_p(a)}\mathfrak{b}\mathfrak{c}^{-1}$ for some nonzero ideals $\mathfrak{b}$ and $\mathfrak{c}$ of A that are not divisible by $\mathfrak{p}$.

EXAMPLE 2.3.11. For the valuation at ∞ on $F(t)$, where F is a field, we may take $A=K[t^{-1}]$ and $\mathfrak{p}=(t^{-1})$. Then the valuation v_∞ on $F(t)$ is the (t^{-1})-adic valuation. To see this, note that for nonzero $g,h\in F[t]$, one has

$$\frac{g(t)}{h(t)}=(t^{-1})^{\deg h-\deg g}\frac{G(t^{-1})}{H(t^{-1})},$$

where $G(t^{-1})=t^{-\deg g}g(t)$ and $H(t^{-1})=t^{-\deg h}h(t)$ are polynomials in t^{-1} which have nonzero constant term.

LEMMA 2.3.12. *Let A be a Dedekind domain with quotient field K, and let $\mathfrak{p}$ be a prime ideal of A. The $\mathfrak{p}$-adic valuation on K is a discrete valuation.*

PROOF. Let $a,b \in K$ be nonzero (without loss of generality). Write $(a) = \mathfrak{p}^r\mathfrak{a}$ and $(b) = \mathfrak{p}^s\mathfrak{b}$ for $r = v_\mathfrak{p}(a)$ and $s = v_\mathfrak{p}(b)$ and fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ of A. Note that $(ab) = \mathfrak{p}^{r+s}\mathfrak{a}\mathfrak{b}$, so $v_p(ab) = r+s$. We have

$$(a+b) = \mathfrak{p}^r\mathfrak{a} + \mathfrak{p}^s\mathfrak{b} = \mathfrak{p}^{\min(r,s)}(\mathfrak{p}^{r-\min(r,s)}\mathfrak{a} + \mathfrak{p}^{s-\min(r,s)}\mathfrak{b}),$$

so

$$v_\mathfrak{p}(a+b) = \min(r,s) + v_\mathfrak{p}(\mathfrak{p}^{r-\min(r,s)}\mathfrak{a} + \mathfrak{p}^{s-\min(r,s)}\mathfrak{b}) \geq \min(r,s).$$

□

LEMMA 2.3.13. *Let v be a discrete valuation on a field K. Then we have $v(-a) = v(a)$ for all $a \in K$.*

PROOF. Note that $2v(-1) = v(1) = 0$, so we have $v(-a) = v(-1) + v(a) = v(a)$. □

LEMMA 2.3.14.

$$v(a+b) = \min(v(a), v(b))$$

for all $a,b \in K$ with $v(a) \neq v(b)$.

PROOF. If $v(a) < v(b)$, then

$$v(a) = v((a+b)-b) \geq \min(v(a+b), v(b)) \geq \min(v(a), v(b)) = v(a),$$

so we have $v(a) = \min(v(a+b), v(b))$, which forces $v(a+b) = v(a)$. □

DEFINITION 2.3.15. Let K be a field, and let v be a discrete valuation on K. Then

$$\mathscr{O}_v = \{a \in K \mid v(a) \geq 0\}$$

is called the *valuation ring* of v.

LEMMA 2.3.16. *Let K be a field, and let v be a discrete valuation on K. Then $\mathscr{O}_v$ is a DVR with maximal ideal*

$$\mathfrak{m}_v = \{a \in K \mid v(a) \geq 1\}.$$

PROOF. That $\mathscr{O}_v$ is a ring follows from the fact that if $a,b \in \mathscr{O}_v$, then $v(ab) = v(a) + v(b) \geq 0$, $v(-a) = v(a) \geq 0$, and $v(a+b) \geq \min(v(a), v(b)) \geq 0$. For $a \in \mathscr{O}_v$ and $x,y \in \mathfrak{m}_v$, we have $v(x+y) \geq \min(v(x), v(y)) \geq 1$ and $v(ax) = v(a) + v(x) \geq 1$, so $\mathfrak{m}_v$ is an ideal. It is also the unique maximal ideal: given $a \in \mathscr{O}_v - \mathfrak{m}_v$, we have $v(a^{-1}) = v(a) + v(a^{-1}) = v(1) = 0$, so $a \in \mathscr{O}_v^\times$. Given an ideal $\mathfrak{a}$ of $\mathscr{O}_v$, let $a \in \mathfrak{a}$ be an element of minimal valuation n. Let $\pi \in \mathscr{O}_v$ with $v(\pi) = 1$, and write $a = \pi^n u$ for some $u \in \mathscr{O}_v^\times$. Then $v(u) = 0$, so $u \in \mathscr{O}_v^\times$. Therefore, $(\pi^n) \subseteq \mathfrak{a}$. On the other hand, since n is minimal, we have $\mathfrak{a} \subseteq (\pi^n)$, and therefore $\mathfrak{a}$ is a principal. By Lemma 2.3.2, we conclude that $\mathscr{O}_v$ is a DVR. □

EXAMPLE 2.3.17. In $\mathbb{Q}$, we have

$$\mathscr{O}_{v_p} = \mathbb{Z}_{(p)} = \left\{\frac{a}{b} \mid a,b \in \mathbb{Z} \text{ such that } p \nmid b\right\}.$$

2.4. Orders

In this section, we investigate rings that would be Dedekind domains but for the removal of the hypothesis of integral closedness. The following definition is perhaps nonstandard outside of the context of number fields, but it works well for our purposes.

DEFINITION 2.4.1. A Noetherian domain R in which every nonzero prime ideal is maximal is called is called an *order*. For a Dedekind domain A, an *order* in A is an order contained in A with integral closure A in its quotient field.

By Lemma 2.2.5, we have the following.

LEMMA 2.4.2. *Let R be an order, and let B be an integral extension of R that is a domain and finitely generated as an R-algebra. Then B is an order.*

We omit the proof of the following theorem.

THEOREM 2.4.3 (Krull-Akizuki). *If A is a Noetherian domain in which every nonzero prime ideal is maximal and L is finite extension of the quotient field K of A, then every subring B of L containing A is also a Noetherian domain in which every nonzero prime ideal is maximal. Moreover, for any nonzero ideal $\mathfrak{b}$ of R, the quotient ring $B/\mathfrak{b}B$ is a finitely generated A-module.*

The following corollary generalizes Theorem 2.2.6 by both by removing the condition of separability of the extension and by removing the condition that the ground ring be integrally closed.

COROLLARY 2.4.4. *Let A be an order, let K denote the quotient field of A, let L be a finite extension of K, and let B be the integral closure of A in L. Then B is a Dedekind domain.*

DEFINITION 2.4.5. Let R be an order, and let A be the integral closure of R in its quotient field. The *conductor* of R is the ideal $\mathfrak{f}_R$ of A defined by

$$\mathfrak{f}_R = \{a \in A \mid aA \subseteq R\}.$$

REMARK 2.4.6. The conductor of R is the largest ideal of A that is contained in R. In particular, it is also an ideal of R.

LEMMA 2.4.7. *Let R be an order, and let A be the integral closure of R in its quotient field. Then A is a finitely generated R-module if and only if the conductor of R is nonzero.*

PROOF. Let $\{a_1, \ldots, a_m\}$ be a set of generators of A as an R-module, and for each $i \leq m$, let $r_i \in R - \{0\}$ be such that $r_i a_i \in R$. Note that r_i exists as A is contained in the quotient field of R. Then $r = r_1 \cdots r_n$ is a nonzero element of $\mathfrak{f}_R$.

Conversely, let $r \in \mathfrak{f}_R$ be nonzero. Then multiplication by r is an R-module isomorphism from A to an ideal of R, which is finitely generated as R is noetherian. □

EXAMPLE 2.4.8. The conductor of $\mathbb{Z}[\sqrt{d}]$ as a subring of $\mathscr{O}_{\mathbb{Q}(\sqrt{d})}$ is (1) if $d \equiv 2,3 \bmod 4$ and (2) if $d \equiv 1 \bmod 4$.

LEMMA 2.4.9. *Let A be a Dedekind domain with quotient field K. Let L be a finite separable extension of K, and let B be the integral closure of A in K. Suppose that $L = K(\alpha)$ for some $\alpha \in B$. Then $A[\alpha]$ is an order in B, and $\mathrm{D}(1, \alpha, \ldots, \alpha^{[L:K]-1}) \in \mathfrak{f}_{A[\alpha]}$.*

PROOF. This is a direct consequence of Proposition 1.4.20. □

PROPOSITION 2.4.10. *Let R be an order, and let $\mathfrak{p}$ be a nonzero prime ideal of R. Let A denote the integral closure of R in its quotient field. Suppose that the conductor $\mathfrak{f}_R$ is nonzero. Then $\mathfrak{p}$ does not contain $\mathfrak{f}_R$ if and only if $R_\mathfrak{p}$ is a DVR. In this case, $\mathfrak{p}A$ is a prime ideal and the inclusion map $R_\mathfrak{p} \to A_{\mathfrak{p}A}$ is an isomorphism.*

PROOF. First, suppose that $\mathfrak{f}_R \not\subseteq \mathfrak{p}$, and let $x \in \mathfrak{f}_R$ with $x \notin \mathfrak{p}$. We have that $xA \subseteq R$ and $x \in R_\mathfrak{p}^\times$, so $A \subseteq R_\mathfrak{p}$. Let $\mathfrak{q} = A \cap \mathfrak{p}R_\mathfrak{p}$, which is a prime ideal of A containing $\mathfrak{p}$. We must then have $\mathfrak{p} = \mathfrak{q} \cap R$, since $\mathfrak{q} \cap R$ is a prime ideal of R. Note that $R_\mathfrak{p} \subseteq A_\mathfrak{q}$. On the other hand, if $\frac{a}{s} \in A_\mathfrak{q}$ for some $a \in A$ and $s \in A - \mathfrak{q}$, then note that $xa \in R$ and $xs \notin \mathfrak{p}$, so $\frac{a}{s} \in R_\mathfrak{p}$ as well. Thus, $R_\mathfrak{p} = A_\mathfrak{q}$ is a DVR by Proposition 2.3.4.

We claim that $\mathfrak{q} = \mathfrak{p}A$. Clearly, $\mathfrak{q}$ occurs in the factorization of $\mathfrak{p}A$, and if any other prime ideal $\mathfrak{q}'$ occurred in said factorization, then $A_{\mathfrak{q}'}$ would contain $R_\mathfrak{p} = A_\mathfrak{q}$, contradicting the fact that $\mathfrak{q}'$ is maximal. So $\mathfrak{p}A = \mathfrak{q}^e$ for some $e \geq 1$, but $\mathfrak{p}R_\mathfrak{p} = \mathfrak{p}A_\mathfrak{q} = \mathfrak{q}^e A_\mathfrak{q}$ is the maximal ideal of $R_\mathfrak{p} = A_\mathfrak{q}$, so it equals $\mathfrak{q}A_\mathfrak{q}$, which forces $e = 1$.

Conversely, suppose that $R_\mathfrak{p}$ is a DVR, hence integrally closed. Since A is integral over R, every element of A is integral over the larger ring $R_\mathfrak{p}$. In other words, we have that $A \subseteq R_\mathfrak{p}$. Note that this also implies that $\mathfrak{p} = \mathfrak{p}A \cap R$ since $\mathfrak{p} = \mathfrak{p}R_\mathfrak{p} \cap R \supseteq \mathfrak{p}A \cap R$, while the other containment is immediate. Let $\{a_1, \ldots, a_n\}$ be a set of generators of A as an R-module, and write $a_i = \frac{y_i}{s_i}$ for some $y_i \in R$ and $s_i \in R - \mathfrak{p}$ for each $1 \leq i \leq n$. Let $s = s_1 \cdots s_n$. Then $sa_i \in R$ for each i, so $s \in \mathfrak{f}_R$. Since $s \in R - \mathfrak{p}$, we have that $\mathfrak{f}_R \not\subseteq \mathfrak{p}$. □

Let us focus now on the setting of number fields. The following is immediate from the definition of integral closure.

LEMMA 2.4.11. *Every subring of a number field K that is finitely generated as an abelian group is contained in $\mathscr{O}_K$.*

We note the following.

LEMMA 2.4.12. *A subring of K is an order in $\mathscr{O}_K$ if and only if it is finitely generated of rank $[K : \mathbb{Q}]$ as a $\mathbb{Z}$-module.*

PROOF. Let R be a finitely generated $\mathbb{Z}$-submodule of K of rank $[K:\mathbb{Q}]$. That R is an order is an immediate corollary of Lemma 2.4.2. On the other hand, if R is an order in $\mathscr{O}_K$, then its quotient field is K, so its rank as a $\mathbb{Z}$-module is $[K:\mathbb{Q}]$. □

REMARK 2.4.13. The ring of integers of a number field K is often referred to as the *maximal order* of K.

Along with the notion of conductor, we also have a notion of discriminant of an order in a number field.

DEFINITION 2.4.14. Let K be a number field, and let R be an order in $\mathscr{O}_K$. The *discriminant* $\mathrm{disc}(R)$ of R is the discriminant of R relative to a basis of R as a $\mathbb{Z}$-module.

REMARK 2.4.15. That the discriminant of R is well-defined follows by the same argument as in Proposition 1.4.25.

The following is a consequence of Lemma 1.4.6 and the fact that a $\mathbb{Z}$-linear transformation that carries one subgroup of rank n in an n-dimensional $\mathbb{Q}$-vector space to another in which it is contained has determinant equal to the index of the first subgroup in the second.

LEMMA 2.4.16. *Let R be an order in $\mathscr{O}_K$ for a number field K. Then*

$$\mathrm{disc}(R) = [\mathscr{O}_K : R]^2 \,\mathrm{disc}(\mathscr{O}_K).$$

COROLLARY 2.4.17. *Let K be a number field and R be an order in its ring of integers. If* $\mathrm{disc}(R)$ *is a square-free integer, then $R = \mathscr{O}_K$.*

LEMMA 2.4.18. *Let K be a number field, and let R be an order in $\mathscr{O}_K$. Then the prime numbers dividing $[\mathscr{O}_K : R]$ are exactly those that divide the unique positive generator of $\mathfrak{f}_R \cap \mathbb{Z}$.*

PROOF. Let $f \geq 1$ be such that $(f) = \mathfrak{f}_R \cap \mathbb{Z}$. Since $f \cdot \mathscr{O}_K \subseteq R$, we have that f is a multiple of the exponent of $\mathscr{O}_K/R$. On the other hand, suppose that some prime number p divides f but not $[\mathscr{O}_K : R]$. Since $p \mid f$, there exists a nonzero prime ideal $\mathfrak{p}$ of $\mathscr{O}_K$ with $\mathfrak{p} \cap \mathscr{O}_K = p\mathbb{Z}$ that divides $\mathfrak{f}_R$. Let $\mathfrak{g} = \mathfrak{p}^{-1}\mathfrak{f}_R$, which is an ideal of $\mathscr{O}_K$. Since multiplication by p is invertible on $\mathscr{O}_K/R$, we have

$$\mathfrak{g}(\mathscr{O}_K/R) = p\mathfrak{g}(\mathscr{O}_K/R) = (p\mathfrak{p}^{-1})\mathfrak{f}_R(\mathscr{O}_K/R) = 0.$$

In other words, we have $\mathfrak{g}\mathscr{O}_K \subseteq R$. But $\mathfrak{f}_R \subsetneq \mathfrak{g}$, which is a contradiction. □

2.5. Ramification of primes

The integral closure B of a Dedekind domain A in a finite extension L of its quotient field K is also a Dedekind domain. If $\mathfrak{p}$ is a nonzero prime ideal of A, then we can consider the ideal $\mathfrak{p}B$ of B. This ideal may no longer be prime. Instead, it has a factorization

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \tag{2.5.1}$$

for some distinct nonzero prime ideals $\mathfrak{P}_i$ of B and positive integers e_i, for $1 \leq i \leq g$ for some $g \geq 1$. We make the following definitions.

DEFINITION 2.5.1. Let B/A be an extension of commutative rings. We say that a prime ideal $\mathfrak{P}$ of B *lies over* (or *above*) a prime ideal $\mathfrak{p}$ of A if $\mathfrak{p} = \mathfrak{P} \cap A$. We then say that $\mathfrak{p}$ *lies under* (or *below*) $\mathfrak{P}$.

In (2.5.1), the prime ideals of B lying over $\mathfrak{p}$ are exactly the $\mathfrak{P}_i$ for $1 \leq i \leq g$.

DEFINITION 2.5.2. Let A be a Dedekind domain, and let B be the integral closure of A in a finite extension L of the quotient field K of A. Let $\mathfrak{p}$ be a nonzero prime ideal of A.

a. We say that $\mathfrak{p}$ *ramifies* (or *is ramified*) in L/K if $\mathfrak{p}B$ is divisible by the square of a prime ideal of B. Otherwise, it is said to be *unramified*.

b. We say that $\mathfrak{p}$ is *inert* in L/K if $\mathfrak{p}B$ is a prime ideal.

c. We say that $\mathfrak{p}$ is *split* in L/K if there exist two distinct prime ideals of B lying over $\mathfrak{p}$. Otherwise, $\mathfrak{p}$ is *non-split*.

It follows directly that $\mathfrak{p}$ is ramified in L/K if some e_i in (2.5.1) is at least 2. On the other hand, $\mathfrak{p}$ is inert in L/K if there is exactly one prime ideal of B lying over $\mathfrak{p}$ and its ramification index is 1, which is to say that $g = 1$ and $e_1 = 1$ in (2.5.1). Finally, $\mathfrak{p}$ is split in L/K if $g > 1$.

EXAMPLE 2.5.3. Let $A = \mathbb{Z}$ and $L = \mathbb{Q}(\sqrt{2})$. The integral closure of A in L is $B = \mathscr{O}_L = \mathbb{Z}[\sqrt{2}]$. The prime $\mathfrak{p} = (2)$ ramifies in $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, since

$$2\mathbb{Z}[\sqrt{2}] = (\sqrt{2})^2.$$

Moreover, $\mathfrak{P} = (\sqrt{2})$ is a prime ideal of $\mathbb{Z}[\sqrt{2}]$, since $\mathbb{Z}[\sqrt{2}]/(\sqrt{2}) \cong \mathbb{Z}/2\mathbb{Z}$ via the map that takes $a + b\sqrt{2}$ to a mod 2. Therefore, $\mathfrak{p}$ is ramified and non-split.

Next, consider the prime ideal (3) of $\mathbb{Z}$. We have $\mathbb{Z}[\sqrt{2}]/(3) \cong \mathbb{F}_3[\sqrt{2}] \cong \mathbb{F}_9$, so (3) is inert in $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. On the other hand, the prime factorization of $7\mathbb{Z}[\sqrt{2}]$ is exactly

$$7\mathbb{Z}[\sqrt{2}] = (3 + \sqrt{2})(3 - \sqrt{2}),$$

since $\mathbb{Z}[\sqrt{2}]/(3 \pm \sqrt{2})$ is isomorphic to $\mathbb{Z}/7\mathbb{Z}$ via the map that takes $a + b\sqrt{2}$ to $a \mp 3b$. That is, (7) splits in $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.

DEFINITION 2.5.4. Let A be a Dedekind domain, and let $\mathfrak{p}$ be a nonzero prime ideal of A. The *residue field* of $\mathfrak{p}$ is $A/\mathfrak{p}$.

REMARK 2.5.5. Let A be a Dedekind domain, and let B be the integral closure of A in a finite extension L the quotient field K of A. Let $\mathfrak{p}$ be a nonzero prime ideal of A, and let $\mathfrak{P}$ be a prime ideal of L lying over K. Then $B/\mathfrak{P}$ is a field extension of $A/\mathfrak{p}$ via the natural map induced on quotients by the inclusion $A \hookrightarrow B$.

DEFINITION 2.5.6. Let A be a Dedekind domain, and let B be the integral closure of A in a finite extension L of the quotient field K of A. Let $\mathfrak{p}$ be a nonzero prime ideal of A, and let $\mathfrak{P}$ be a prime ideal of B lying over $\mathfrak{p}$.

a. The *ramification index* $e_{\mathfrak{P}/\mathfrak{p}}$ of $\mathfrak{P}$ over $\mathfrak{p}$ is the largest $e \geq 1$ such that $\mathfrak{P}^e$ divides $\mathfrak{p}B$.

b. The *residue degree* $f_{\mathfrak{P}/\mathfrak{p}}$ of a prime ideal of $\mathfrak{P}$ lying over $\mathfrak{p}$ is $[B/\mathfrak{P} : A/\mathfrak{p}]$.

REMARK 2.5.7. It follows quickly from the definitions that ramification indices and residue degrees are multiplicative in extensions. That is, if $A \subseteq B \subseteq C$ are Dedekind domains with the quotient field of C a finite extension of that of A and $\mathfrak{P}$ is a prime ideal of C lying over P of B and $\mathfrak{p}$ of A, then

$$e_{\mathfrak{P}/\mathfrak{p}} = e_{\mathfrak{P}/P} e_{P/\mathfrak{p}} \quad \text{and} \quad f_{\mathfrak{P}/\mathfrak{p}} = f_{\mathfrak{P}/P} f_{P/\mathfrak{p}}.$$

EXAMPLE 2.5.8. In Example 2.5.3, the residue degree of $(\sqrt{2})$ over $2\mathbb{Z}$ is 1, the residue degree of $3\mathbb{Z}[\sqrt{2}]$ over $3\mathbb{Z}$ is 2, and the residue degrees of $(3 \pm \sqrt{2})$ over $7\mathbb{Z}$ are each 1. The ramification indices are 2, 1, and 1, repsectively.

We shall require the following lemmas.

LEMMA 2.5.9. *Let $\mathfrak{p}$ be a nonzero prime ideal in a Dedekind domain A. For each $i \geq 0$, the $A/\mathfrak{p}$-vector space $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ is one-dimensional.*

PROOF. Let $x \in \mathfrak{p}^i - \mathfrak{p}^{i+1}$ for some $i \geq 0$. (Such an element exists by unique factorization of ideals.) We need only show that the image of x spans $\mathfrak{p}^i/\mathfrak{p}^{i+1}$. For this, note that $(x) = \mathfrak{p}^i\mathfrak{a}$ for some nonzero ideal of A not divisible by $\mathfrak{p}$. Then

$$(x) + \mathfrak{p}^{i+1} = \mathfrak{p}^i(\mathfrak{a} + \mathfrak{p}) = \mathfrak{p}^i,$$

the last step by the Chinese remainder theorem. □

LEMMA 2.5.10. *Let A be a Dedekind domain and P be a set of nonzero prime ideals of A. Let S a multiplicatively closed subset of A such that $S \cap \mathfrak{p} = \varnothing$ for all $\mathfrak{p} \in P$. Let $\mathfrak{a}$ be a nonzero ideal of A that is divisible only by prime ideals in P. Then the natural map*

$$A/\mathfrak{a} \to S^{-1}A/S^{-1}\mathfrak{a}$$

is an isomorphism.

PROOF. Suppose that $b \in S^{-1}\mathfrak{a} \cap A$, and write $b = \frac{a}{s}$ for some $a \in \mathfrak{a}$ and $s \in S$. Then $a = bs$, and since $\mathfrak{a}$ divides (a) while (s) is relatively prime to $\mathfrak{a}$, we must have that $\mathfrak{a}$ divides (b). In other words, $b \in \mathfrak{a}$, and therefore the map is injective. Given $c \in A$ and $t \in S$, the ideals (t) and $\mathfrak{a}$ have no common prime factor, so in that A is a Dedekind domain, satisfy $(t) + \mathfrak{a} = A$. Thus, there exists $u \in A$ such that $ut - 1 \in \mathfrak{a}$. Then $cu + \mathfrak{a}$ maps to $\frac{c}{t} + S^{-1}\mathfrak{a}$, so the map is surjective. □

The ramification indices and residue degrees of the primes over $\mathfrak{p}$ satisfy the following degree formula.

THEOREM 2.5.11. *Let A be a Dedekind domain, and let B be the integral closure of A in a finite separable extension L the quotient field K of A. Let $\mathfrak{p}$ be a nonzero prime ideal of A, and write*

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

for some distinct nonzero prime ideals $\mathfrak{P}_i$ of B and positive integers e_i, for $1 \leq i \leq g$ and some $g \geq 1$. For each i, let $f_i = f_{\mathfrak{P}_i/\mathfrak{p}}$. Then

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

PROOF. We prove that $\dim_{A/\mathfrak{p}} B/\mathfrak{p}B$ equals both quantities in the desired equality. By the Chinese remainder theorem, we have a canonical isomorphism

$$B/\mathfrak{p}B \cong \prod_{i=1}^{g} B/\mathfrak{P}_i^{e_i},$$

of $A/\mathfrak{p}$-vector spaces, so

$$\dim_{A/\mathfrak{p}} B/\mathfrak{p}B = \sum_{i=1}^{g} \dim_{A/\mathfrak{p}} B/\mathfrak{P}_i^{e_i} = \sum_{i=1}^{g} \sum_{j=0}^{e_i-1} \dim_{A/\mathfrak{p}} \mathfrak{P}_i^j/\mathfrak{P}_i^{j+1}.$$

By Lemma 2.5.9, each $\mathfrak{P}_i^j/\mathfrak{P}_i^{j+1}$ is a 1-dimensional $B/\mathfrak{P}_i$-vector space, and we therefore have

$$\dim_{A/\mathfrak{p}} B/\mathfrak{p}B = \sum_{i=1}^{g} e_i \dim_{A/\mathfrak{p}} B/\mathfrak{P}_i = \sum_{i=1}^{g} e_i f_i.$$

Let S denote the complement of $\mathfrak{p}$ in A. Then $S^{-1}A = A_{\mathfrak{p}}$ and $S^{-1}B$ are Dedekind domains, and $A_{\mathfrak{p}}$ is a DVR, hence a PID. Moreover, $S^{-1}B$ is the integral closure of $A_{\mathfrak{p}}$ in L, being both integrally closed and contained in said integral closure. Thus, Corollary 1.4.24 tells us that $S^{-1}B$ is free of rank $[L : K]$ over $A_{\mathfrak{p}}$. In particular, $S^{-1}B/\mathfrak{p}S^{-1}B$ is an $[L : K]$-dimensional $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$-vector space. On the other hand, note that

$$S \cap \mathfrak{P}_i = S \cap A \cap \mathfrak{P}_i = S \cap \mathfrak{p} = \varnothing$$

for each $1 \leq i \leq g$. Therefore, Lemma 2.5.10 tells us that

$$S^{-1}B/\mathfrak{p}S^{-1}B \cong B/\mathfrak{p}B$$

and $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \cong A/\mathfrak{p}$. We thus have that $\dim_{A/\mathfrak{p}} B/\mathfrak{p}B = [L : K]$, as required. □

In other words, Theorem 2.5.11 tells us that the sum over all primes lying over $\mathfrak{p}$ of the products of their ramification indices with their residue degrees equals the degree of the field extension L/K.

The following theorem provides a very useful method for determining prime factorizations in extensions of Dedekind domains.

THEOREM 2.5.12 (Kummer-Dedekind). *Let A be a Dedekind domain, let K be the field of fractions of A, let L be a finite separable extension of K, and let B be the integral closure of A in L. Write $L = K(\alpha)$ for some $\alpha \in B$. Let $\mathfrak{p}$ be a nonzero prime ideal of A such that $\mathfrak{p}B$ is prime to $\mathfrak{f}_{A[\alpha]}$. Let $h \in A[x]$ be the minimal polynomial of α, and let $\bar{h} \in (A/\mathfrak{p})[x]$ be its reduction modulo $\mathfrak{p}$. Write*

$$\bar{h} = \bar{h}_1^{e_1} \cdots \bar{h}_g^{e_g}$$

where the $\bar{h}_i \in (A/\mathfrak{p})[x]$ are distinct nonconstant, irreducible polynomials and the e_i are positive integers for $1 \leq i \leq g$, for some $g \geq 1$. Let $h_i \in A[x]$ be any lift of $\bar{h}_i$. Then the ideals

$$\mathfrak{P}_i = \mathfrak{p}B + (h_i(\alpha))$$

of B are distinct prime ideals over $\mathfrak{p}$ of ramification index e_i and residue degree $\deg \bar{h}_i$. In particular, we have the prime factorization $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$.

PROOF. Set $F = A/\mathfrak{p}$. The canonical composite map

$$A[x] \to F[x] \to F[x]/(\bar{h})$$

has kernel $\mathfrak{p}A[x] + (h)$, and

$$A[x]/(\mathfrak{p}A[x] + (h)) \cong A[\alpha]/\mathfrak{p}A[\alpha]$$

by the third isomorphism theorem. Combining this with the Chinese remainder theorem, we have

$$A[\alpha]/\mathfrak{p}A[\alpha] \cong F[x]/(\bar{h}) \cong \prod_{i=1}^{g} F[x]/(\bar{h}_i^{e_i}),$$

Set $P_i = \mathfrak{p}A[\alpha] + (h_i(\alpha))$. We claim that $P_i^{e_i}$ is the kernel of the surjective map

$$\phi_i \colon A[\alpha] \to F[x]/(\bar{h}_i^{e_i}).$$

By definition, the P_i are distinct and coprime, and we have

$$A[\alpha]/P_i \cong F[x]/(\bar{h}_i),$$

so $A[\alpha]/P_i$ is a field extension of F of degree $\deg \bar{h}_i$, which is to say that P_i is maximal. The image of $h_i^{e_i - 1}$ is not in the kernel of ϕ_i so $P_i^{e_i}$ is the smallest power of P_i contained in $\ker \phi_i$, which is contained in P_i. In that P_i is maximal, we have

$$A[\alpha]/P_i^{e_i} \cong A[\alpha]_{P_i}/P_i^{e_i} A[\alpha]_{P_i}.$$

Note that $A[\alpha]$ is an order by Lemma 2.4.2. The prime ideal $P_i = \mathfrak{P}_i \cap A[\alpha]$ is relatively prime to $\mathfrak{f}_{A[\alpha]} \subseteq A[\alpha]$ as $\mathfrak{P}_i$ does not divide $\mathfrak{f}_{A[\alpha]}$ in B. Thus, we have that $A[\alpha]_{P_i}$ is a DVR by Proposition 2.4.10. So, the only ideals of $A[\alpha]/P_i^{e_i}$ are $P_i^m/P_i^{e_i}$ for $0 \leq m \leq e_i$. The kernel of $A[\alpha]/P_i^{e_i} \to F[x]/(\bar{h}_i^{e_i})$ can then only be zero, which means that $\ker \phi_i = P_i^{e_i}$, as claimed.

Since the product of the induced maps

$$\prod_{i=1}^{g} A[\alpha]/P_i^{e_i} \to \prod_{i=1}^{g} F[x]/(\bar{h}_i^{e_i})$$

is injective, we have $\mathfrak{p}A[\alpha] = P_1^{e_1} \cdots P_g^{e_g}$, and then by definition, we have $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ as well. Proposition 2.4.10 tells us that each $\mathfrak{P}_i$ is prime, $B_{\mathfrak{P}_i} \cong A_{P_i}$, and $P_i = \mathfrak{P}_i \cap A[\alpha]$. In particular, the $\mathfrak{P}_i$ are distinct, and as they are the only primes occuring in the factorization of $\mathfrak{p}B$, they are the only primes of B lying over $\mathfrak{p}$. Since $B/\mathfrak{P}_i \cong F[x]/(\bar{h}_i)$, the residue degree of $\mathfrak{P}_i$ is $\deg \bar{h}_i$, and by the factorization of $\mathfrak{p}B$, the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$ is e_i. □

EXAMPLE 2.5.13. Let $h(x) = x^3 + x + 1 \in \mathbb{Z}[x]$. Note that it is irreducible in $\mathbb{Q}[x]$ since it is monic with no integral roots (or since it has no roots modulo 2). Let $L = \mathbb{Q}(\alpha)$ for a root α of F in $\mathbb{C}$. Then $\mathbb{Z}[\alpha]$ is integral over $\mathbb{Z}$ and has discriminant -31 (which of course one should check), so must be the ring of integers of L. Since $h(0)$ and $h(1)$ are both odd, $h(x)$ remains irreducible modulo (2), so (2) is inert in $L/\mathbb{Q}$. On the other hand,

$$h(x) \equiv (x^2 + x - 1)(x - 1) \bmod 3,$$

so

$$3\mathbb{Z}[\alpha] = \mathfrak{P}_1\mathfrak{P}_2$$

where $\mathfrak{P}_1 = (3, \alpha^2 + \alpha - 1)$ has residue degree 2 and $\mathfrak{P}_2 = (3, \alpha - 1)$ has residue degree 1.

COROLLARY 2.5.14. *Let p be an odd prime number, and let $a \in \mathbb{Z}$ be square-free and not divisible by p. Then a is a square modulo p if and only if (p) splits in $\mathbb{Q}(\sqrt{a})$.*

PROOF. Since the conductor of $\mathbb{Z}[\sqrt{a}]$ divides (2), Theorem 2.5.12 applies. We may therefore determine the decomposition of (p) in $\mathscr{O}_{\mathbb{Q}(\sqrt{a})}$ via the factorization of $x^2 - a$ modulo p. Since p does not divide a, the polynomial $x^2 - a$ is not a square modulo p. Therefore, (p) will split if and only if the polynomial splits, which is to say exactly when a is a square modulo p. □

PROPOSITION 2.5.15. *Let A be a Dedekind domain, let K be the field of fractions of A, let L be a finite separable extension of K, and let B be the integral closure of A in L. Write $L = K(\alpha)$ for some $\alpha \in B$. If a nonzero prime ideal of A is ramified in B, then it divides* $\mathrm{D}(1, \alpha, \ldots, \alpha^{[L:K]-1})$.

PROOF. Let $f \in A[x]$ be the minimal polynomial of α. Let $\mathfrak{p}$ be a nonzero prime ideal of A such that $\mathfrak{p}B$ is relatively prime to $\mathfrak{f}_{A[\alpha]}$. By Theorem 2.5.12, the prime $\mathfrak{p}$ is ramified in B if and only if the reduction $\bar{f} \in (A/\mathfrak{p})[x]$ is divisible by the square of an irreducible polynomial. For this to occur, $\bar{f}$ would have to have a multiple root in any algebraic closure of $A/\mathfrak{p}$. By Proposition 1.4.13, this means that $\mathrm{D}(1, \alpha, \ldots, \alpha^{[L:K]-1}) \equiv 0 \bmod \mathfrak{p}$.

Finally, note that $\mathfrak{f}_{A[\alpha]}$ divides $\mathrm{D}(1, \alpha, \ldots, \alpha^{[L:K]-1}) \in A$ by Lemma 2.4.9, so any prime $\mathfrak{p}$ of A for which $\mathfrak{p}B$ is not relatively prime to $\mathfrak{f}_{A[\alpha]}$ divides $\mathrm{D}(1, \alpha, \ldots, \alpha^{[L:K]-1})$. □

COROLLARY 2.5.16. *Let A be a Dedekind domain and B the integral closure of A in a finite separable extension of the quotient field of A. Then only finitely many prime ideals of A are ramified in B.*

The following is also useful.

LEMMA 2.5.17. *Let A be a Dedekind domain, K its quotient field, L a finite separable extension of K, and B the integral closure in K. Let $b \in B$. Every nonzero prime ideal of B dividing bB lies above a prime ideal of A dividing $N_{L/K}(b)A$. Conversely, every prime ideal of A dividing $N_{L/K}(b)A$ lies below a prime ideal of B dividing bB.*

PROOF. If $\mathfrak{P}$ divides (b), then $N_{L/K}b \in \mathfrak{p} = \mathfrak{P} \cap A$, so $\mathfrak{p}$ divides $(N_{L/K}b)$. Conversely, if no prime over $\mathfrak{p}$ divides b, then for any field embedding σ of L in an algebraic closure of K fixing L, no prime over $\mathfrak{p}$ in $\sigma(B)$ divides $(\sigma(b))$. But then no prime over $\mathfrak{p}$ in the integral closure C of B in the Galois closure of L divides $(N_{L/K}(b))$, which is to say the ideal generated by the product of the elements $\sigma(b)$. Hence $\mathfrak{p}$ cannot divide $(N_{L/K}(b))$ either. □

We have the following immediate corollary.

COROLLARY 2.5.18. *Let A be a Dedekind domain, K its quotient field, L a finite separable extension of K, and B the integral closure in K. An element $b \in B$ is a unit if and only if $N_{L/K}(b) \in A^\times$.*

2.6. Decomposition groups

Throughout this section, we let A be a Dedekind domain with quotient field K. We let L be a finite Galois extension of K, and we let B denote the integral closure of A in L. Moreover, set $G = \mathrm{Gal}(L/K)$.

TERMINOLOGY 2.6.1. We frequently refer to a nonzero prime ideal of a Dedekind domain as a *prime*.

DEFINITION 2.6.2. A *conjugate* of a prime $\mathfrak{P}$ of B is $\sigma(\mathfrak{P})$ for some $\sigma \in G$.

LEMMA 2.6.3. *Let $\mathfrak{p}$ be a prime of A, and let $\mathfrak{P}$ be a prime of B lying over $\mathfrak{p}$. Then any conjugate of $\mathfrak{P}$ is also a prime of B lying over $\mathfrak{p}$.*

PROOF. Since any $\sigma \in G$ is an automorphism, $\mathfrak{P}$ is an ideal. The rest is simply that

$$\sigma(\mathfrak{P}) \cap A = \sigma(\mathfrak{P} \cap A) = \sigma(\mathfrak{p}) = \mathfrak{p}.$$

□

Clearly, we have an action of the group G on the set of primes of B lying over a prime $\mathfrak{p}$ of A.

PROPOSITION 2.6.4. *The action of G on the set of primes of B lying over a prime $\mathfrak{p}$ of A is transitive.*

PROOF. Let $\mathfrak{P}$ and $\mathfrak{Q}$ be primes of B lying over $\mathfrak{p}$. Suppose by way of contradiction that $\mathfrak{Q}$ is not a conjugate of $\mathfrak{P}$. By the Chinese Remainder Theorem, we may choose $b \in B$ such that $b \in \mathfrak{Q}$

but $b \equiv 1 \bmod \sigma(\mathfrak{P})$ for all $\sigma \in G$. The latter condition may be rewritten as $\sigma(b) \equiv 1 \bmod \mathfrak{P}$ for all $\sigma \in G$. Then $a = N_{L/K}(b) \in \mathfrak{p}$ since $b \in \mathfrak{Q}$, but

$$a = \prod_{\sigma \in G} \sigma(b) \equiv 1 \bmod \mathfrak{P}.$$

Since $a \in A$, this tells us that $a \equiv 1 \bmod \mathfrak{p}$, which is a contradiction. □

DEFINITION 2.6.5. Let $\mathfrak{P}$ be a prime of B. The *decomposition group* $G_{\mathfrak{P}}$ of $\mathfrak{P}$ is the stabilizer of $\mathfrak{P}$ under the action of G. That is,

$$G_{\mathfrak{P}} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

COROLLARY 2.6.6. *Let $\mathfrak{p}$ be prime of A, and let $\mathfrak{P}$ be a prime of B lying over $\mathfrak{p}$. Then there is a bijection*

$$G/G_{\mathfrak{P}} \to \{\mathfrak{Q} \text{ prime of } B \mid \mathfrak{Q} \cap B = \mathfrak{p}\}$$

that takes a left coset $\sigma G_{\mathfrak{P}}$ to $\sigma(\mathfrak{Q})$.

PROPOSITION 2.6.7. *Let $\mathfrak{P}$ be a prime of B lying over a prime $\mathfrak{p}$ of A, and let $\sigma \in G$. Then $e_{\sigma(\mathfrak{P})/\mathfrak{p}} = e_{\mathfrak{P}/\mathfrak{p}}$ and $f_{\sigma(\mathfrak{P})/\mathfrak{p}} = f_{\mathfrak{P}/\mathfrak{p}}$.*

PROOF. Let S be a set of $G_{\mathfrak{P}}$-coset representatives of $G/G_{\mathfrak{P}}$. By Corollary 2.6.6, we have

$$\mathfrak{p}B = \prod_{\sigma \in S} (\sigma\mathfrak{P})^{e_{\sigma(\mathfrak{P})/\mathfrak{p}}}.$$

Since $\tau \in G$ acts trivially on $\mathfrak{p}$, we have that $\tau(\mathfrak{p}B) = \mathfrak{p}\tau(B) = \mathfrak{p}B$. We therefore have

$$\mathfrak{p}B = \tau(\mathfrak{p}B) = \prod_{\sigma \in S} (\sigma\mathfrak{P})^{e_{\tau^{-1}\sigma(\mathfrak{P})/\mathfrak{p}}}.$$

By unique factorization of ideals in E, this forces all $e_{\sigma(\mathfrak{P})/\mathfrak{p}}$ for $\sigma \in G$ to be equal.

Moreover, any $\sigma \in G$ restricts to an isomorphism $\sigma\colon B \to B$ (since for $\beta \in B$, the element $\sigma(\beta)$ has the same monic minimal polynomial over K) that fixes A. It then induces an isomorphism

$$\sigma\colon B/\mathfrak{P} \xrightarrow{\sim} B/\sigma(\mathfrak{P})$$

of residue fields fixing the subfield $A/\mathfrak{p}$. In particular, this is an isomorphism of $A/\mathfrak{p}$-vector spaces, so all $f_{\sigma(\mathfrak{P})/\mathfrak{p}}$ are equal. □

REMARK 2.6.8. For L/K Galois, and $\mathfrak{P}$ lying over $\mathfrak{p}$, we often set $e_{\mathfrak{p}} = e_{\mathfrak{P}/\mathfrak{p}}$ and $f_{\mathfrak{p}} = f_{\mathfrak{P}/\mathfrak{p}}$.

COROLLARY 2.6.9. *Let $\mathfrak{p}$ be a prime of A, and let $\mathfrak{P}$ be a prime of B lying above $\mathfrak{p}$. Set $e = e_{\mathfrak{P}/\mathfrak{p}}$, $f = f_{\mathfrak{P}/\mathfrak{p}}$, and $g = [G : G_{\mathfrak{P}}]$. Then*

$$\mathfrak{p}B = \prod_{i=1}^{g} (\sigma_i\mathfrak{P})^e$$

for $\{\sigma_1, \cdots, \sigma_g\}$ a set of $G_{\mathfrak{P}}$-coset representatives of $G/G_{\mathfrak{P}}$. Moreover, we have

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

LEMMA 2.6.10. *Let $\mathfrak{P}$ be a prime of B. Let $\sigma \in G$. Then*

$$G_{\sigma(\mathfrak{P})} = \sigma G_{\mathfrak{P}} \sigma^{-1}.$$

PROOF. Since G is finite, it suffices to show one containment. Let $\tau \in G_{\mathfrak{P}}$. Then we have

$$\sigma\tau\sigma^{-1}(\sigma\mathfrak{P}) = \sigma(\tau\mathfrak{P}) = \sigma\mathfrak{P},$$

so $\sigma\tau\sigma^{-1} \in G_{\sigma\mathfrak{P}}$, as needed. □

COROLLARY 2.6.11. *Suppose that L/K is an abelian extension and $\mathfrak{P}$ is a prime of B. Then $G_{\sigma(\mathfrak{P})} = G_{\mathfrak{P}}$ for all $\sigma \in G$.*

REMARK 2.6.12. One often writes $G_{\mathfrak{p}}$ for the decomposition group of a prime $\mathfrak{P}$ of B lying above a prime $\mathfrak{p}$ of A, and this is independent of the choice of $\mathfrak{P}$ if L/K is abelian.

LEMMA 2.6.13. *Let $\mathfrak{p}$ be a prime of A, and let $\mathfrak{P}$ be a prime of B lying above $\mathfrak{p}$. Let E be the fixed field of $G_{\mathfrak{P}}$, and let C be the integral closure of A in E. Then $\mathfrak{P}$ is the only prime of B lying above $P = C \cap \mathfrak{P}$, and $e_{P/\mathfrak{p}} = f_{P/\mathfrak{p}} = 1$.*

PROOF. Since $G_{\mathfrak{P}}$ fixes $\mathfrak{P}$ and the action of $G_{\mathfrak{P}}$ on the primes of B lying above P is transitive, $\mathfrak{P}$ is the unique prime over P. Note that $e_{\mathfrak{P}/\mathfrak{p}} \geq e_{\mathfrak{P}/P}$ and $f_{\mathfrak{P}/\mathfrak{p}} \geq f_{\mathfrak{P}/P}$. We have $e_{\mathfrak{P}/P} f_{\mathfrak{P}/P} = [L : E]$, while the number of primes g above $\mathfrak{p}$ in L equals $[E : K]$, so $e_{\mathfrak{P}/P} f_{\mathfrak{P}/P} g = [L : K]$. On the other hand, Corollary 2.6.9 tells us that $e_{\mathfrak{P}/\mathfrak{p}} f_{\mathfrak{P}/\mathfrak{p}} g = [L : K]$, so we must have $e_{\mathfrak{P}/\mathfrak{p}} = e_{\mathfrak{P}/P}$ and $f_{\mathfrak{P}/\mathfrak{p}} = f_{\mathfrak{P}/P}$. In other words $e_{P/\mathfrak{p}} = f_{P/\mathfrak{p}} = 1$. □

PROPOSITION 2.6.14. *Let $\mathfrak{p}$ be a prime of A, and let $\mathfrak{P}$ be a prime of B lying over $\mathfrak{p}$. Then the extension $B/\mathfrak{P}$ of $A/\mathfrak{p}$ is normal, and the map*

$$\pi_{\mathfrak{P}} \colon G_{\mathfrak{P}} \to \mathrm{Gal}((B/\mathfrak{P})/(A/\mathfrak{p}))$$

with $\pi_{\mathfrak{P}}(\sigma)(b+\mathfrak{P}) = \sigma(b)+\mathfrak{P}$ for $\sigma \in G_{\mathfrak{P}}$ is a well-defined, surjective homomorphism.

PROOF. Let $\alpha \in B$, and let $\bar{\alpha}$ denote its image in $B/\mathfrak{P}$. Let $f \in A[x]$ be the minimal polynomial for α over K, and let $\bar{f}$ be its image in $(A/\mathfrak{p})[x]$. Clearly, $\bar{\alpha} \in B/\mathfrak{P}$ is a root of $\bar{f}$. Since f splits completely over L, with roots in B, its reduction $\bar{f}$ splits completely over $B/\mathfrak{P}$. Since the minimal polynomial of $\bar{\alpha}$ divides $\bar{f}$, we have that $B/\mathfrak{P}$ is a normal extension of $A/\mathfrak{p}$.

Let $\sigma \in G_{\mathfrak{P}}$, and let $b, c \in B$. If $b+\mathfrak{P} = c+\mathfrak{P}$, then $b-c \in \mathfrak{P}$. Since $\sigma(\mathfrak{P}) = \mathfrak{P}$, we have that $\sigma(b-c) \in \mathfrak{P}$ as well, so $\pi_{\mathfrak{P}}(\sigma)(b+\mathfrak{P}) = \pi_{\mathfrak{P}}(\sigma)(c+\mathfrak{P})$. The image $\pi_{\mathfrak{P}}(\sigma)$ is also easily seen to be a field isomorphism by such computations as

$$\sigma(bc)+\mathfrak{P} = \sigma(bc+\mathfrak{P}) = \sigma((b+\mathfrak{P})(c+\mathfrak{P})) = (\sigma(b)+\mathfrak{P})(\sigma(c)+\mathfrak{P})$$

for any $b, c \in \mathfrak{P}$, and it clearly fixes $A/\mathfrak{p}$. That $\pi_{\mathfrak{P}}$ is a homomorphism is similarly easily checked.

It remains to show surjectivity. Let $\bar{\sigma}$ be an automorphism of $B/\mathfrak{P}$ fixing $A/\mathfrak{p}$. Let E be the fixed field of $G_{\mathfrak{P}}$, let C be the integral closure of A in E, and let $P = C \cap \mathfrak{P}$. Suppose that $\bar{\theta} \in B/\mathfrak{P}$ generates

the maximal separable subextension of $B/\mathfrak{P}$ over $A/\mathfrak{p} = C/P$. Let $\theta \in B$ be a lift of $\bar{\theta}$. Let $g \in C[x]$ be the minimal polynomial of θ, let $\bar{g}$ be its reduction modulo P, and let $h \in (A/\mathfrak{p})[x]$ be the minimal polynomial of $\bar{\theta}$. Since $\bar{\sigma}(\bar{\theta})$ is also a root of h, it is a root of $\bar{g}$, and therefore there exists a root θ' of g such that θ' reduces to $\bar{\sigma}(\bar{\theta})$. Let $\sigma \in G_{\mathfrak{P}}$ be such that $\sigma(\theta) = \theta'$. Then $\pi_{\mathfrak{P}}(\sigma)(\bar{\theta}) = \bar{\sigma}(\bar{\theta})$, so $\pi_{\mathfrak{P}}(\sigma) = \bar{\sigma}$ by choice of θ. □

DEFINITION 2.6.15. Let $\mathfrak{P}$ be a prime of B. The *inertia group* $I_{\mathfrak{P}}$ of $\mathfrak{P}$ is the kernel of the map $G_{\mathfrak{P}} \to \mathrm{Gal}((B/\mathfrak{P})/(A/\mathfrak{p}))$.

COROLLARY 2.6.16. *Let $\mathfrak{p}$ be a prime of K and $\mathfrak{P}$ a prime of B lying over $\mathfrak{p}$. Then there is an exact sequence of groups*

$$1 \to I_{\mathfrak{P}} \to G_{\mathfrak{P}} \xrightarrow{\pi_{\mathfrak{p}}} \mathrm{Gal}((B/\mathfrak{P})/(A/\mathfrak{p})) \to 1.$$

REMARK 2.6.17. The inertia group is a normal subgroup of the decomposition group of a prime. If the corresponding extension of residue fields is separable, then its order is the ramification index of the prime.

EXAMPLE 2.6.18. Let $L = \mathbb{Q}(\omega, \sqrt[3]{2})$, where ω is a primitive cube root of 1. Let $K = \mathbb{Q}(\omega)$. Let $G = \mathrm{Gal}(L/\mathbb{Q})$ and $N = \mathrm{Gal}(L/K)$. Note that

$$D(1, \sqrt[3]{2}, (\sqrt[3]{2})^2) = N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(3(\sqrt[3]{2})^2) = 27 \cdot 4 = 108,$$

so 2 and 3 are the only primes that can divide the conductor of $\mathbb{Z}[\sqrt[3]{2}]$ (which is in fact the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$, though we shall not use this).

- The prime 2 is inert in $K/\mathbb{Q}$ and ramifies in L/K; the decomposition is $2\mathscr{O}_L = (\sqrt[3]{2})^3$. We therefore have $G_{(\sqrt[3]{2})} = G$ and $I_{(\sqrt[3]{2})} = N$.
- The prime 3 is totally ramified in $L/\mathbb{Q}$. To see this, note first that it ramifies as $3\mathscr{O}_K = (1-\omega)^2$ in K. Moreover, $N_{L/K}(1+\sqrt[3]{2}) = 3$, while $1+\sqrt[3]{2}$ is congruent to its conjugates modulo $(1-\omega)$. This tells us that $3\mathscr{O}_L = \mathfrak{P}^6$ for

  $$\mathfrak{P} = (1+\sqrt[3]{2}, 1-\omega) = \left(\frac{1-\omega}{1+\sqrt[3]{2}}\right).$$

  Then $G_{\mathfrak{P}} = I_{\mathfrak{P}} = G$.
- The prime 5 is inert in $K/\mathbb{Q}$ and splits in L/K: for the latter, we may apply the Kummer-Dedekind criterion, noting that $3^3 \equiv 2 \bmod 5$, so $x^3 - 2$ splits completely over the residue field $\mathbb{F}_{25}$ of K at (5). We then have $5\mathscr{O}_L = \mathfrak{Q}_1\mathfrak{Q}_2\mathfrak{Q}_3$ for primes

  $$\mathfrak{Q}_i = (5, \omega^{i-1}\sqrt[3]{2} - 3)$$

  with $G_{\mathfrak{Q}_i} = \mathrm{Gal}(L/E_i)$, where $E_i = \mathbb{Q}(\omega^{i-1}\sqrt[3]{2})$ for $1 \le i \le 3$. We have $5\mathscr{O}_{E_1} = \mathfrak{q}_1\mathfrak{q}_2$ where $\mathfrak{Q}_1$ lies over $\mathfrak{q}_1 = (5, \sqrt[3]{2} - 3)$ and $\mathfrak{Q}_2$ and $\mathfrak{Q}_3$ lie over $\mathfrak{q}_2 = (5, (\sqrt[3]{2})^2 + 3\sqrt[3]{2} + 4)$, which have $f_{\mathfrak{q}_1/(5)} = 1$ and $f_{\mathfrak{q}_2/(5)} = 2$.

TERMINOLOGY 2.6.19. If K is a number field, then we often refer to a nonzero prime ideal of $\mathscr{O}_K$ as a *prime* of K.

DEFINITION 2.6.20. Let K be a number field and $\mathfrak{a}$ be a nonzero ideal in $\mathscr{O}_K$. The *absolute norm* of $\mathfrak{a}$ is the integer $N\mathfrak{a} = [\mathscr{O}_K : \mathfrak{a}]$.

REMARK 2.6.21. If $\mathfrak{p}$ is a prime in the ring of integers of a number field K lying above $p\mathbb{Z}$, then $N\mathfrak{p} = p^f$, where f is the residue degree of $\mathfrak{p}$ over $p\mathbb{Z}$.

REMARK 2.6.22. The absolute norm extends to a homomorphism $N\colon I_K \to \mathbb{Q}^\times$ with $N(\mathfrak{a}\mathfrak{b}^{-1}) = N\mathfrak{a} \cdot (N\mathfrak{b})^{-1}$ for any nonzero ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathscr{O}_K$.

For number fields, the residue fields of primes are finite. Recall that the Frobenius element $\varphi \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ for q a power of a prime and $n \geq 1$ is defined by $\varphi(x) = x^q$ for all $x \in \mathbb{F}_q$. That is, we have canonical generators of Galois groups of extensions of residue fields. Since the map of Proposition 2.6.14 is surjective, these lift to elements of decomposition groups.

DEFINITION 2.6.23. Let L/K be a finite Galois extension of number fields with $G = \mathrm{Gal}(L/K)$. Let $\mathfrak{p}$ be a prime of K and $\mathfrak{P}$ a prime of L lying over $\mathfrak{p}$. A *Frobenius element* of $G_\mathfrak{P}$ is an automorphism $\varphi_\mathfrak{P} \in G_\mathfrak{P}$ satisfying

$$\varphi_\mathfrak{P}(\alpha) \equiv \alpha^{N\mathfrak{p}} \bmod \mathfrak{P}$$

for all $\alpha \in \mathscr{O}_L$.

REMARK 2.6.24. If $\mathfrak{p}$ is unramified in L/K, then $\varphi_\mathfrak{P}$ is unique given a choice of $\mathfrak{P}$. If, in addition, L/K is abelian, then $\varphi_\mathfrak{P}$ is independent of the choice of $\mathfrak{P}$.

CHAPTER 3

Applications

3.1. Cyclotomic fields

Let n be a positive integer.

NOTATION 3.1.1. Let n be a positive integer and K a field. The group $\mu_n(K)$ will denote the group of nth roots of unity in K.

REMARK 3.1.2. Let n be a positive integer and K a field of characteristic not divisible by n. The group μ_n to denote the group of nth roots of unity in an algebraic closure of K, fixed beforehand. This group always has order n.

EXAMPLE 3.1.3. Let ℓ and p be prime numbers.

a. The group $\mu_\ell(\overline{\mathbb{F}_p})$ of ℓth roots of unity in an algebraic closure of $\mathbb{F}_p$ has order ℓ for $\ell \neq p$ and is trivial if $\ell = p$.

b. The group $\mu_\ell(\mathbb{F}_p)$ is μ_ℓ for ℓ dividing $p-1$ and 1 for all other ℓ.

NOTATION 3.1.4. Let K be a field and L be an extension of K. If S is a set of elements of L, then the field $K(S)$ is the subfield of L given by adjoining to K all elements of S.

DEFINITION 3.1.5. The field $\mathbb{Q}(\mu_n)$ is the *nth cyclotomic field*.

REMARK 3.1.6. More generally, if F is a field of characteristic not dividing n, we let $F(\mu_n)$ denote the field obtained from F by adjoining all nth roots of unity in an algebraic closure of F.

REMARK 3.1.7. The field $\mathbb{Q}(\mu_n)$ is Galois over $\mathbb{Q}$, as it is the splitting field of $x^n - 1$. All nth roots of unity are powers of any primitive nth root of unity ζ_n, so $\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta_n)$.

DEFINITION 3.1.8. The nth *cyclotomic polynomial* $\Phi_n \in \mathbb{Z}[x]$ is the polynomial which has as its roots the primitive nth roots of unity.

Note that $x^n - 1 = \prod_{d|n} \Phi_d$. We recall the definition of the Möbius function.

DEFINITION 3.1.9. The *Möbius function* $\mu\colon \mathbb{Z}_{\geq 1} \to \mathbb{Z}$ is defined as follows. Let $n = p_1^{r_1} \cdots p_k^{r_k}$ for distinct primes p_i and positive integers r_i for $1 \leq i \leq k$ for some $k \geq 0$. Then

$$\mu(n) = \begin{cases} (-1)^k & \text{if } r_i = 1 \text{ for all } 1 \leq i \leq k, \\ 0 & \text{otherwise.} \end{cases}$$

We omit the proof of the following, which uses the Möbius inversion formula.

LEMMA 3.1.10. *For all $n \geq 1$, we have*

$$\Phi_n = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

EXAMPLES 3.1.11.

a. $\Phi_1 = x-1, \Phi_2 = x+1, \Phi_3 = x^2+x+1, \Phi_4 = x^2+1, \Phi_5 = x^4+x^3+x^2+x+1, \Phi_6 = x^2-x+1.$

b. $\Phi_{15} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1.$

c. $\Phi_{p^r} = x^{p^{r-1}(p-1)} + \cdots + x^{p^{r-1}} + 1$ for every prime p and $r \geq 1$.

For $n \geq 1$, we will use ζ_n to denote a primitive nth root of unity in an algebraic closure of $\mathbb{Q}$.

LEMMA 3.1.12. *Let $n \geq 1$ and let $i, j \in \mathbb{Z}$ be relatively prime to n. Then*

$$\frac{1-\zeta_n^i}{1-\zeta_n^j} \in \mathscr{O}^\times_{\mathbb{Q}(\mu_n)}.$$

PROOF. Let $k \in \mathbb{Z}$ with $jk \equiv 1 \bmod n$. Then

$$\frac{1-\zeta_n^i}{1-\zeta_n^j} = \frac{1-\zeta_n^{ijk}}{1-\zeta_n^j} = 1 + \zeta_n^j + \cdots + \zeta_n^{j(ik-1)}$$

is an algebraic integer since ζ_n is. The same being true after reversing i and j, we have the result. □

We let $\mathbb{Z}[\mu_n]$ denote the ring generated over $\mathbb{Z}$ by the nth roots of unity.

LEMMA 3.1.13. *Let p be a prime number and $r \geq 1$. Then the absolute value of the discriminant of $\mathbb{Z}[\mu_{p^r}]$ is a power of p, and (p) is the only prime of $\mathbb{Z}$ that ramifies in $\mathbb{Q}(\mu_{p^r})$. It is totally ramified and lies below $(1-\zeta_{p^r})$. Moreover, $[\mathbb{Q}(\mu_{p^r}) : \mathbb{Q}] = p^{r-1}(p-1)$.*

PROOF. Note that $[\mathbb{Q}(\mu_{p^r}) : \mathbb{Q}] \leq \deg \Phi_{p^r} = p^{r-1}(p-1)$. We have

$$\prod_{\substack{i=1 \\ p \nmid i}}^{p^r-1} (1-\zeta_{p^r}^i) = \Phi_{p^r}(1) = p,$$

which forces $1-\zeta_{p^r}^i$ to be divisible by a prime $\mathfrak{p}$ over p for some i with $p \nmid i$. By Lemma 3.1.12, this implies that each $1-\zeta_{p^r}^j$ with $p \nmid j$ is divisible by $\mathfrak{p}$. Therefore, $\mathfrak{p}^{p^{r-1}(p-1)}$ divides (p), which forces $[\mathbb{Q}(\mu_{p^r}) : \mathbb{Q}] = p^{r-1}(p-1)$ and

$$p\mathscr{O}_{\mathbb{Q}(\mu_{p^r})} = \mathfrak{p}^{p^{r-1}(p-1)} = (1-\zeta_{p^r})^{p^{r-1}(p-1)}.$$

Finally, note that

$$\operatorname{disc}(\mathscr{O}_{\mathbb{Q}(\mu_{p^r})}) \mid \operatorname{disc}(\mathbb{Z}[\mu_{p^r}]),$$

which is a product of terms of the form $\zeta_{p^r}^i - \zeta_{p^r}^j$ for $i \neq j$ both not divisible by p, which from what we have seen is only divisible by the prime $\mathfrak{p} = (1-\zeta_{p^r})$. In other words, no prime other than p can ramify. □

PROPOSITION 3.1.14. *The nth cyclotomic polynomial is irreducible for all $n \geq 1$. In other words, $[\mathbb{Q}(\mu_n) : \mathbb{Q}] = \varphi(n)$, where φ is Euler's phi-function. Moreover, the prime ideals of $\mathbb{Z}$ that ramify in $\mathscr{O}_{\mathbb{Q}(\mu_n)}$ are the odd primes dividing n and, if n is a multiple of 4, the prime 2.*

PROOF. If we write $n = p_1^{r_1} \cdots p_k^{r_k}$ for distinct primes p_i and $r_i \geq 1$, then

$$\deg \Phi_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) d = \prod_{i=1}^{k} p_i^{r_i-1}(p_i - 1) = \varphi(n).$$

Hence, the second statement implies the first. In n is even and not divisible by 4, then $\mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_{n/2})$ and $\varphi(n) = \varphi(n/2)$, so we may assume that either n is odd or divisible by 4.

The result holds for $k = 1$ by Lemma 3.1.13. Write $n = mp^r$ for some $m, r \geq 1$ and prime p not dividing m. As p does not not ramify in $\mathbb{Q}(\mu_m)$ by induction on k but is totally ramified in $\mathbb{Q}(\mu_{p^r})$ by Lemma 3.1.13, the fields $\mathbb{Q}(\mu_m)$ and $\mathbb{Q}(\mu_{p^r})$ are linearly disjoint. So by induction, the primes which divide n are exactly those which ramify in $\mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_m)\mathbb{Q}(\mu_{p^r})$, and we have

$$[\mathbb{Q}(\mu_n) : \mathbb{Q}] = [\mathbb{Q}(\mu_m) : \mathbb{Q}][\mathbb{Q}(\mu_{p^r}) : \mathbb{Q}] = \varphi(m)\varphi(p^r) = \varphi(n).$$

□

For an arbitrary field of good characteristic, let us make the following definition.

DEFINITION 3.1.15. Let F be a field of characteristic not dividing $n \geq 1$. Define a homomorphism

$$\chi_n \colon \mathrm{Gal}(F(\mu_n)/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

on $\sigma \in \mathrm{Gal}(F(\mu_n)/F)$ as follows. If i_σ is the unique integer with $1 \leq i \leq n$ such that $\sigma(\zeta) = \zeta^{i_\sigma}$ for all nth roots of unity ζ in F, then $\chi_n(\sigma) = i_\sigma \bmod n$. Then χ_n is called the *nth cyclotomic character* for F.

NOTATION 3.1.16. If $a \in \mathbb{Z}/n\mathbb{Z}$, then ζ^a for ζ an nth root of unity denotes ζ^b for any $b \in \mathbb{Z}$ with image a modulo n.

REMARK 3.1.17. The homomorphism χ_n is always injective, as any element such that $\chi_n(\sigma) = 1$ for all $\sigma \in \mathrm{Gal}(F(\mu_n)/F)$ fixes μ_n and hence $F(\mu_n)$.

We have the following corollary of Proposition 3.1.14, since χ_n for $F = \mathbb{Q}$ is an injective homomorphism between groups of equal order.

COROLLARY 3.1.18. *The nth cyclotomic character $\chi_n \colon \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism.*

REMARK 3.1.19. In particular, $\mathbb{Q}(\mu_{p^r})/\mathbb{Q}$ for an odd prime p and $r \geq 1$ has cyclic Galois group.

PROPOSITION 3.1.20. *The ring $\mathbb{Z}[\mu_n]$ is the ring of integers of $\mathbb{Q}(\mu_n)$.*

PROOF. We first consider $n = p^r$ for a prime p and $r \geq 1$. In this case, we know that the absolute value of $\mathrm{disc}(\mathbb{Z}[\mu_{p^r}])$ is a power of p, say p^m. In particular, $\mathfrak{f}_{\mathbb{Z}[\mu_{p^r}]}$ divides (p^m). Let $\lambda_r = 1 - \zeta_{p^r}$, which generates the unique prime over (p) in $\mathbb{Q}(\mu_{p^r})$. Since (p) is totally ramified in $\mathbb{Q}(\mu_{p^r})/\mathbb{Q}$, we have that

$$\mathscr{O}_{\mathbb{Q}(\mu_{p^r})}/(\lambda_r) \cong \mathbb{Z}/p\mathbb{Z}.$$

In particular,

$$\mathscr{O}_{\mathbb{Q}(\mu_{p^r})} = \mathbb{Z} + \lambda_r \mathscr{O}_{\mathbb{Q}(\mu_{p^r})} = \mathbb{Z}[\mu_{p^r}] + \lambda_r \mathscr{O}_{\mathbb{Q}(\mu_{p^r})}. \tag{3.1.1}$$

Replacing $\mathscr{O}_{\mathbb{Q}(\mu_{p^r})}$ on the right-hand side of (3.1.1) using the formula for $\mathscr{O}_{\mathbb{Q}(\mu_{p^r})}$ given by (3.1.1) itself, we have

$$\mathscr{O}_{\mathbb{Q}(\mu_{p^r})} = \mathbb{Z}[\mu_{p^r}] + \lambda_r(\mathbb{Z}[\mu_{p^r}] + \lambda_r \mathscr{O}_{\mathbb{Q}(\mu_{p^r})}) = \mathbb{Z}[\mu_{p^r}] + \lambda_r^2 \mathscr{O}_{\mathbb{Q}(\mu_{p^r})}.$$

Repeatedly replacing $\mathscr{O}_{\mathbb{Q}(\mu_{p^r})}$ on the right, we eventually obtain

$$\mathscr{O}_{\mathbb{Q}(\mu_{p^r})} = \mathbb{Z}[\mu_{p^r}] + p^m \mathscr{O}_{\mathbb{Q}(\mu_{p^r})}, = \mathbb{Z}[\mu_{p^r}]$$

the latter step by definition of the conductor.

For the general case, we write $n = p_1^{r_1} \cdots p_k^{r_k}$ for distinct primes p_i and $r_i \geq 1$. Then $\mathbb{Q}(\mu_n)$ is the compositum of the $\mathbb{Q}(\mu_{p_i^{r_i}})$ and the discriminants of the fields $\mathbb{Q}(\mu_{p_i^{r_i}})$ are relatively prime, we have by Proposition 1.4.28 that the elements

$$\zeta_{p_1^{r_1}}^{i_1} \cdots \zeta_{p_k^{r_k}}^{i_k}$$

with $0 \leq i_t \leq p_t^{r_t - 1}(p_t - 1) - 1$ for each $1 \leq t \leq k$ form an integral basis of $\mathscr{O}_{\mathbb{Q}(\mu_n)}$. Since these elements are all contained in the order $\mathbb{Z}[\mu_n]$ in $\mathbb{Q}(\mu_n)$, we have the result. □

The factorization in $\mathbb{Q}(\mu_n)$ of the ideals generated by prime numbers is rather easy to describe.

PROPOSITION 3.1.21. *Let p be a prime, and let $r \geq 0$ be such that p^r exactly divides n. Let $m = \frac{n}{p^r}$, and let f be the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$. Then*

$$p\mathbb{Z}[\mu_n] = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^{\varphi(p^r)},$$

where φ is the Euler phi-function, $g = f^{-1}\varphi(m)$ and the $\mathfrak{p}_i$ are distinct primes of $\mathbb{Z}[\mu_n]$ of residue degree f.

PROOF. First, we note that p is totally ramified in $\mathbb{Q}(\mu_{p^r})$ of degree $\varphi(p^r)$ and unramified in $\mathbb{Q}(\mu_m)$. It follows from Remark 2.5.7 that the ramification index of p in $\mathbb{Q}(\mu_n)$ is then $\varphi(p^r)$, and the residue degree of p in $\mathbb{Q}(\mu_n)$ is the residue degree of p in $\mathbb{Q}(\mu_m)$.

So, let $\mathfrak{q}$ be a prime ideal over p in $\mathbb{Z}[\mu_m]$. Its residue field is

$$F = \mathbb{Z}[\mu_m]/\mathfrak{q} = \mathbb{F}_p(\mu_m).$$

As $F^\times$ is cyclic of order $|F|-1$, we have $F = \mathbb{F}_{p^f}$ for the smallest $f \geq 1$ such that $m \mid (p^f - 1)$, which is to say that the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$. Finally, g is constrained to be $f^{-1}\varphi(m)$ by the degree formula. □

We have the following corollary.

COROLLARY 3.1.22. *An odd prime p splits completely in $\mathbb{Q}(\mu_n)/\mathbb{Q}$ if and only if $p \equiv 1 \bmod n$. The prime 2 does not split completely in a nontrivial cyclotomic extension of $\mathbb{Q}$.*

PROOF. By Proposition 3.1.21, to say that a prime p splits completely is exactly to say that $\varphi(p^r) = 1$ and the order of p in $(\mathbb{Z}/(n/p^r)\mathbb{Z})^\times$ is 1. If p is odd, then this means $r = 0$ and $p \equiv 1 \bmod n$. If $p = 2$, this forces $n = 1$ or $n = 2$, which is to say that $\mathbb{Q}(\mu_n) = \mathbb{Q}$. □

3.2. Quadratic reciprocity

In this section, we briefly explore the relationship between cyclotomic and quadratic fields.

DEFINITION 3.2.1. For an odd prime p, we set $p^* = (-1)^{(p-1)/2}p$.

The reason for this definition is the following.

LEMMA 3.2.2. *Let p be an odd prime. The field $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic field contained in $\mathbb{Q}(\mu_p)$.*

PROOF. Recall that $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ is cyclic of order $p-1$, so it has a unique quotient of order 2. As p is totally ramified in $\mathbb{Q}(\mu_p)/\mathbb{Q}$, it is ramified in K, so $K = \mathbb{Q}(\sqrt{p'})$, where $p' = \pm p$. Moreover, no other prime is ramified in $\mathbb{Q}(\mu_p)/\mathbb{Q}$. If $p' \equiv 3 \bmod 4$, then K has ring of integers $\mathbb{Z}[\sqrt{p'}]$, and we have

$$\mathbb{Z}[\sqrt{p'}]/(2) \cong \mathbb{F}_2[x]/(x^2 - p') \cong \mathbb{F}_2[x]/(x+1)^2,$$

which means that 2 ramifies in K. Since $p^* \equiv 1 \bmod 4$, we must have $p' = p^*$. □

We prove the following consequence of results of Proposition 3.1.21.

PROPOSITION 3.2.3. *Let p and q be odd prime numbers. Then q splits in $\mathbb{Q}(\sqrt{p^*})$ if and only if q splits into an even number of primes in $\mathbb{Q}(\mu_p)$.*

PROOF. The prime q splits into an even number of primes in $\mathbb{Q}(\mu_p)$ if and only if the decomposition group G_q of any prime over q has even index in $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$. Since the latter Galois group is cyclic with unique subgroup of index 2 having fixed field $\mathbb{Q}(\sqrt{p^*})$ by Lemma 3.2.2, this occurs if and only if G_q fixes $\mathbb{Q}(\sqrt{p^*})$, which is to say, if and only if q splits in $\mathbb{Q}(\sqrt{p^*})$. □

DEFINITION 3.2.4. Let a be an integer and q be an odd prime number with $q \nmid a$. The *Legendre symbol* $(\frac{a}{q})$ is defined to be

$$\left(\frac{a}{q}\right) = \begin{cases} 1 & \text{if } a \text{ is a square mod } q, \\ -1 & \text{otherwise.} \end{cases}$$

In other words, $(\frac{a}{q})$ is the unique unit in $\mathbb{Z}$ such that

$$a^{\frac{q-1}{2}} \equiv \left(\frac{a}{q}\right) \bmod q.$$

Gauss' law of quadratic reciprocity is the following.

THEOREM 3.2.5 (Quadratic reciprocity). *If p and q are distinct odd prime numbers, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

PROOF. Note that

$$p^{\frac{q-1}{2}} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \bmod q.$$

if and only if

$$(p^*)^{\frac{q-1}{2}} \equiv 1 \bmod q,$$

which is to say if and only if $(\frac{p^*}{q}) = 1$. This says exactly that there exists $a \in \mathbb{Z}$ such that

$$a^2 \equiv p^* \bmod q.$$

But then $x^2 - p^*$ factors modulo q, so (q) splits in $\mathbb{Z}[\sqrt{p^*}]$. Now, Proposition 3.2.3 tells us that this happens if and only if (q) splits in $\mathbb{Z}[\mu_p]$ into an even number of primes. By Proposition 3.1.21, the prime (q) splits into $(p-1)/f$ primes in $\mathbb{Q}(\mu_p)$, where f is the order of q modulo p. So, it splits into an even number if and only if f divides $(p-1)/2$, which is to say that

$$q^{\frac{p-1}{2}} \equiv 1 \bmod p,$$

In other words, $(\frac{p}{q}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ if and only if $(\frac{q}{p}) = 1$, as desired. □

REMARK 3.2.6. To complete the law of quadratic reciprocity, we note that the definitions imply that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

and we note without proof that

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

3.3. Fermat's last theorem

Recall that Fermat's last theorem (or FLT) asserts the nonexistence of integer solutions to $x^n + y^n = z^n$ with $xyz \neq 0$ for all $n \geq 3$. Fermat proved this conjecture for $n = 4$, and given this it clearly suffices to show the nonexistence for odd prime exponents. While FLT was proven by Wiles in 1995 using methods far beyond the scope of these notes, we are able to prove here the following so-called "first case" of Fermat's last theorem for odd prime exponents of a special form.

Fix an odd prime p and a primitive pth root of unity ζ_p in $\mathbb{Q}(\mu_p)$. We require a couple of lemmas.

LEMMA 3.3.1. *Let $x, y \in \mathbb{Z}$ be relatively prime, and suppose that $p \nmid x+y$. Then the elements $x + \zeta_p^i y$ of $\mathbb{Z}[\mu_p]$ for $0 \leq i \leq p-1$ are pairwise relatively prime.*

PROOF. If $\mathfrak{q}$ is a prime ideal of $\mathbb{Z}[\mu_p]$ dividing both $x + \zeta_p^i y$ and $x + \zeta_p^j y$ for $0 \leq i < j < p$, then $\mathfrak{q}$ divides both $(\zeta_p^j - \zeta_p^i)y$ and $(\zeta_p^j - \zeta_p^i)x$. If $\mathfrak{q}$ does not lie over p, then it must divide both x and y, which is impossible. Thus, $\mathfrak{q}$ lies over p, so it equals $(1 - \zeta_p)$. On the other hand, $x + \zeta_p^i y \equiv x + y \bmod (1 - \zeta_p)$, which implies that $x + y \equiv 0 \bmod p$, since $x + y$ is an integer. Thus, no such $\mathfrak{q}$ can exist. □

TERMINOLOGY 3.3.2. For any $n \geq 3$, we refer to the unique element of $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ with image -1 under the nth cyclotomic character as *complex conjugation*, and we write $\bar{\alpha}$ to denote the image of $\alpha \in \mathbb{Q}(\mu_n)$ under this element.

LEMMA 3.3.3. *Let $\varepsilon \in \mathbb{Z}[\mu_p]^\times$. Then there exists $j \in \mathbb{Z}$ such that $\varepsilon \zeta_p^j$ is fixed by complex conjugation.*

PROOF. Note that $\sigma(\bar{\varepsilon}\varepsilon^{-1})$ has absolute value 1 for every $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$, so it is a root of unity by Corollary 4.4.2 below, hence a $2p$th root of unity. If the lemma did not hold, then each

$$\frac{\bar{\varepsilon}\zeta_p^{-j}}{\varepsilon\zeta_p^j} = \zeta_p^{-2j}\frac{\bar{\varepsilon}}{\varepsilon}$$

would have to be nontrivial for every j, which means that $\bar{\varepsilon}\varepsilon^{-1}$ would not be a pth root of unity. Thus, we would have $\bar{\varepsilon}\varepsilon^{-1} = -\zeta_p^i$ for some $i \in \mathbb{Z}$. We may write $\varepsilon \equiv c \bmod (1 - \zeta_p)$ for some $c \in \mathbb{Z}$, and so $\bar{\varepsilon} \equiv c \bmod (1 - \zeta_p)$ as well. On the other hand,

$$\bar{\varepsilon} = -\zeta_p^i \varepsilon \equiv -\varepsilon \equiv -c \bmod (1 - \zeta_p),$$

so $(1 - \zeta_p)$ in fact divides ε, which is a contradiction as ε is a unit. □

LEMMA 3.3.4. *The images of any $p-1$ of the pth roots of unity in $\mathbb{Z}[\mu_p]/(p)$ are $\mathbb{F}_p$-linearly independent.*

PROOF. We have

$$\mathbb{Z}[\mu_p]/(p) \cong \mathbb{Z}[x]/(\Phi_p, p) \cong \mathbb{F}_p[x]/(\Phi_p) \cong \mathbb{F}_p[x]/(x-1)^{p-1},$$

and the images of any $p-1$ among $1, x, \ldots, x^{p-1}$ are $\mathbb{F}_p$-linearly independent in the last term. $\square$

We now prove the result.

THEOREM 3.3.5 (Kummer). *Let p be an odd prime such that $\mathrm{Cl}_{\mathbb{Q}(\mu_p)}$ contains no elements of order p. Then there do not exist integers x, y, z with $p \nmid xyz$ such that $x^p + y^p = z^p$.*

PROOF. Suppose that $x^p + y^p = z^p$ for some integers x, y, z with $p \nmid xyz$ and $(x, y) = (1)$. For $p = 3$, we note that the set of nonzero cubes modulo 9 is $\{\pm 1\}$, and no sum of two elements of this set equals a third element modulo 9. Thus, we may assume that $p \geq 5$ from now on.

Note that if $x \equiv y \equiv -z \bmod p$, then $2x^p \equiv -x^p \bmod p$, so p divides $3x^p$. As $p \nmid xyz$, this cannot happen. Therefore, if $p \mid x - y$, then $p \nmid x + z$. Switching the roles of y and $-z$ by writing $x^p + (-z)^p = (-y)^p$ if needed, we may therefore assume that $p \nmid x - y$.

In $\mathbb{Z}[\mu_p]$, the quantity $x^p + y^p$ factors, and we have

$$\prod_{i=0}^{p-1} (x + \zeta_p^i y) = z^p.$$

Note that $z \equiv x + y \bmod p$, so p does not divide $x + y$. By Lemma 3.3.1, we have that the ideals $(x + \zeta_p^i y)$ are coprime, so in order that their product be a pth power of an ideal, each must itself be a pth power. Write

$$(x + \zeta_p y) = \mathfrak{a}^p$$

for some ideal $\mathfrak{a}$ of $\mathbb{Z}[\mu_p]$. Since we have assumed that $\mathrm{Cl}_{\mathbb{Q}(\mu_p)}$ has no elements of order p, the ideal $\mathfrak{a}$ is principal, so let $\alpha \in \mathbb{Z}[\mu_p]$ be a generator of $\mathfrak{a}$. We then have

$$x + \zeta_p y = \varepsilon \alpha^p$$

for some $\varepsilon \in \mathbb{Z}[\mu_p]^\times$.

Now, note that we may write $\alpha = c + d(1 - \zeta)$ for some $c \in \mathbb{Z}$ and $d \in \mathbb{Z}[\mu_p]$, and

$$\alpha^p \equiv c^p + d^p (1 - \zeta)^p \equiv c \bmod (p).$$

By Lemma 3.3.3, we that there exists $j \in \mathbb{Z}$ such that $\varepsilon' = \zeta_p^j \varepsilon$ is fixed by complex conjugation. We thus have

$$x + \zeta_p y \equiv \zeta_p^{-j} \varepsilon' c \bmod (p),$$

so

$$x + \zeta_p^{-1} y \equiv \zeta_p^j \varepsilon' c \bmod (p).$$

We therefore have

$$\zeta_p^{2j} (x + \zeta_p y) \equiv x + \zeta_p^{-1} y \bmod (p).$$

If ζ_p^{2j}, ζ_p^{2j+1}, 1 and ζ_p^{-1} are distinct pth roots of unity, then since $p - 1 \geq 4$, they are linearly independent modulo p. This would force both x and y to be divisible by p, a contradiction.

It follows that $1 = \zeta_p^{2j}$, ζ_p^{2j+1} or ζ_p^{2j+2}. In the first of these cases, we have

$$x + \zeta_p y \equiv x + \zeta_p^{-1} y \bmod (p),$$

so p divides y, a contradiction. In the second case, we have

$$\zeta_p^{-1} x + y \equiv x + \zeta_p^{-1} y \mod (p),$$

so p divides $x - y$, again a contradiction. In the final case, we have

$$\zeta_p^{-2} x + \zeta_p^{-1} y \equiv x + \zeta_p^{-1} y \mod (p),$$

so p divides x, a contradiction, finishing the proof. □

REMARK 3.3.6. The "first case" of FLT refers to the nonexistence of solutions to $x^p + y^p = z^p$ with $p \nmid xyz$. The "second case" refers to the nonexistence of solutions with $p \mid xyz$ and $xyz \neq 0$.

CHAPTER 4

Geometry of numbers

4.1. Lattices

DEFINITION 4.1.1. A *lattice* in an finite-dimensional $\mathbb{R}$-vector space V is an abelian subgroup of V that is generated by a finite set of $\mathbb{R}$-linearly independent vectors.

DEFINITION 4.1.2. A lattice in a finite-dimensional $\mathbb{R}$-vector space V is said to be *complete*, or *full*, if its elements span V.

The following is an immediate consequence of the definitions.

LEMMA 4.1.3. *If Λ is a complete lattice in a finite-dimensional $\mathbb{R}$-vector space V, then Λ is generated by a basis of V.*

DEFINITION 4.1.4. Let Λ be a complete lattice in a finite-dimensional vector space V. The *fundamental domain* of Λ relative to a $\mathbb{Z}$-basis $\{v_1, \ldots, v_n\}$ of Λ is the set

$$D = \left\{ \sum_{i=1}^{n} c_i v_i \,\middle|\, c_i \in [0,1) \text{ for all } 1 \leq i \leq n \right\}.$$

The following is essentially immediate.

LEMMA 4.1.5. *If D is a fundamental domain of a complete lattice Λ in a vector space V, then every element of V may be written uniquely in the form $x+y$ for some $x \in \Lambda$ and some $y \in D$.*

Of course, a finite-dimensional $\mathbb{R}$-vector space V has a Euclidean metric with respect to any basis of V (as such a basis defines an isomorphism $V \cong \mathbb{R}^n$ for some n). Though the metric depends upon the choice of basis, the resulting topology is independent of the choice of basis.

DEFINITION 4.1.6. We say that a subgroup of an finite-dimensional $\mathbb{R}$-vector space V is *discrete* if it has the discrete topology as a subspace of V.

In other words, a subgroup Λ of a finite-dimensional real vector space V is discrete if for every $v \in \Lambda$ there exists an open neighborhood U of v in V such that $U \cap \Lambda = \{v\}$. The following is elementary.

LEMMA 4.1.7. *A discrete subgroup of a finite-dimensional $\mathbb{R}$-vector space V is a closed subset of V.*

PROPOSITION 4.1.8. *A subgroup of a finite-dimensional $\mathbb{R}$-vector space is discrete if and only if it is a lattice.*

PROOF. Let V be an n-dimensional $\mathbb{R}$-vector space for some $n \geq 0$, and let Λ be a subgroup. If Λ is a lattice, then $\Lambda = \sum_{i=1}^{m} \mathbb{Z} v_i$ for some linearly independent $v_i \in \Lambda$ and $m \leq n$. Extend these to an ordered basis $v_1, \ldots, v_n$ of V. Let $v = \sum_{i=1}^{m} a_i v_i \in \Lambda$ for some $a_i \in \mathbb{Z}$. Then

$$U = \left\{ v + \sum_{i=1}^{n} c_i v_i \,\middle|\, c_i \in (-1,1) \text{ for all } 1 \leq i \leq n \right\}$$

is an open neighborhood in V containing v but no other elements of Λ. Thus Λ is discrete.

Conversely, suppose Λ is discrete. Let W be the subspace of V spanned by Λ, and let $v_1, \ldots, v_m \in \Lambda$ be linearly independent with m maximal, so that the v_i necessarily span W. Let $\Sigma = \sum_{i=1}^{m} \mathbb{Z} v_i \leq \Lambda$. We claim that Σ is of finite index in Λ. By definition, Σ is a complete lattice in W, so so we may choose a system S of representatives of the cosets Λ/Σ inside the fundamental domain D of Σ in W. That is, $S \subset \Lambda \cap D$. However, Λ is discrete and closed and D is a bounded set, so the intersection of Λ with the closure of D is discrete and compact, hence finite. Since $\Lambda \cap D$ is then finite, S has only finitely many elements.

Now set $d = [\Lambda : \Sigma]$. Then $\Lambda \subseteq \frac{1}{d}\Sigma$, and $\frac{1}{d}\Sigma \cong \Sigma$ is a free abelian group of rank m, so Λ is free of rank (at most) m. In other words, Λ is a lattice. □

LEMMA 4.1.9. *A lattice Λ in V is complete if and only if there exists a bounded subset B of V such that every element of V is the sum of an element of B and an element of Λ.*

PROOF. If Λ is a complete lattice, we may let B be the fundamental domain of V relative to a basis, and in fact every element of V may in that case be written uniquely as an element of $B + \Lambda$.

Suppose that there exists a B as in the statement of the lemma. Let W be the $\mathbb{R}$-span of Λ, and let $v \in V$. For each $k \geq 1$, write $kv = b_k + x_k$ with $b_k \in B$ and $x_k \in \Lambda$. As B is bounded, we have

$$\lim_{k \to \infty} \frac{1}{k} b_k = 0,$$

so

$$v = \lim_{k \to \infty} \frac{1}{k} x_k.$$

But $\frac{1}{k} x_k \in W$ for all k and W is closed, so $v \in W$. □

We will suppose now that our finite-dimensional vector space V comes equipped with a symmetric, positive definite inner product

$$\langle \, , \, \rangle \colon V \times V \to \mathbb{R}.$$

In other words, V is an finite-dimensional real inner product space. The Euclidean metric defined by a choice of an orthonormal basis of V is independent of the choice. The resulting Lebesgue measure μ_V on V has the property that the cube defined by an orthonormal basis of V has volume (i.e., measure) one.

DEFINITION 4.1.10. Let V be an finite-dimensional real vector space with a symmetric, positive definite inner product $\langle\ ,\ \rangle$. Let Λ be a complete lattice in V. The *volume* $\mathrm{Vol}(\Lambda)$ of lattice is the volume of the fundamental domain of Λ relative to a $\mathbb{Z}$-basis of Λ.

REMARK 4.1.11. That the volume of Λ is indepedendent of the choice of basis is a consequence of the following lemma.

LEMMA 4.1.12. *Let V be an n-dimensional real inner product space. Let $e_1,\dots,e_n$ be an orthonormal basis of V. Let Λ be a complete lattice in V with basis $v_1,\dots,v_n$, write*

$$v_i = \sum_{j=1}^{n} a_{ij} e_j,$$

and let $A = (a_{ij})$. Then

$$\mathrm{Vol}(\Lambda) = |\det A| = |\det(\langle v_i, v_j\rangle)|^{1/2}.$$

PROOF. The first equality is a standard statement of linear algebra. The second is the fact that

$$\langle v_i, v_j\rangle = \sum_{k=1}^{n}\sum_{l=1}^{n} a_{ik}a_{jl}\langle e_k, e_l\rangle = \sum_{k=1}^{n} a_{ik}a_{jk} = (AA^T)_{ij},$$

since $\det(AA^T) = \det(A)^2$. □

DEFINITION 4.1.13. Let T be a subset of a finite-dimensional vector space V.

a. We say that T is *convex* if it contains the line segment

$$\ell = \{(1-c)v + cw \mid c \in [0,1]\}$$

between any two vectors $v, w \in T$.

b. We say that T is *symmetric about the origin* if $-v \in T$ for all $v \in T$.

Now we come to the main theorem of this subsection.

THEOREM 4.1.14 (Minkowski's theorem). *Let V be an n-dimensional real inner product space, and let Λ be a complete lattice in V. Let X be a convex, measurable subset of V that is symmetric about the origin, and suppose that*

$$\mu_{K\otimes_{\mathbb{Q}}\mathbb{R}}(X) > 2^n \mathrm{Vol}(\Lambda).$$

Then $X \cap \Lambda \neq \{0\}$.

PROOF. Let

$$Y = \frac{1}{2}X = \left\{\frac{1}{2}x \mid x \in X\right\}.$$

If $y \in Y$, then $2y \in X$, so $-2y \in X$ as X is symmetric about the origin. If $y' \in Y$ as well, then

$$y' - y = \frac{1}{2}(2y') + \frac{1}{2}(-2y) \in X,$$

since X is convex. We therefore have that the difference of any two points of Y is in X. Note also that $\mu_V(Y) = \frac{1}{2^n}\mu_V(X) > \mathrm{Vol}(\Lambda)$.

Let D a the fundamental domain for Λ. Suppose that the sets $v+Y$ for $v \in \Lambda$ were pairwise disjoint. Then we would have

$$\mathrm{Vol}(\Lambda) \geq \sum_{v\in\Lambda} \mu_V(D \cap (v+Y)) = \sum_{v\in\Lambda} \mu_V((D-v)\cap Y) = \mu_V(Y),$$

the latter equality following since the sets $D-v$ cover V. This does not hold by assumption, so there exist distinct $v, w \in \Lambda$ such that $(v+Y)\cap(w+Y)$ is nonempty. But then $v-w \in X$, so $X \cap \Lambda \neq \{0\}$. □

4.2. Real and complex embeddings

Let K be an number field of degree n over $\mathbb{Q}$. Then, since $K/\mathbb{Q}$ is separable and $\mathbb{C}$ is algebraically closed, then we obtain the product

$$K \hookrightarrow K \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\sim} \prod_{\sigma\colon K\hookrightarrow\mathbb{C}} \mathbb{C}$$

of embeddings of K in $\mathbb{C}$.

DEFINITION 4.2.1. Let K be a number field.

a. A *real embedding* (or *real prime*) of K is a field embedding of K in $\mathbb{R}$.

b. A *complex embedding* of K is a field embedding of K in $\mathbb{C}$ that does not have image contained in $\mathbb{R}$.

c. A *complex prime* of K is an unordered pair $\{\sigma, \bar{\sigma}\}$ of complex embeddings such that $\bar{\sigma}(\alpha) = \overline{\sigma(\alpha)}$ for $\alpha \in K$, where $\bar{z}$ denotes the complex conjugate of $z \in \mathbb{C}$.

d. An *archimedean prime* of K is either a real prime or a complex prime.

NOTATION 4.2.2. The number of real (resp., complex) primes of a number field K is denoted $r_1(K)$ (resp., $r_2(K)$).

We can also apply Proposition 1.1.1 to obtain the following.

THEOREM 4.2.3. *Let K be a number field. Then $r_1(K) + 2r_2(K) = [K:\mathbb{Q}]$. In fact, we have an isomorphism of $\mathbb{R}$-algebras*

$$\kappa_{\mathbb{R}}\colon K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \mathbb{R}^{r_1(K)} \times \mathbb{C}^{r_2(K)}$$

where $\kappa_{\mathbb{R}}(\alpha\otimes 1)$ for $\alpha \in K$ is the product of the real embeddings of K applied to α and one complex embedding from each complex prime of $\mathbb{Q}$ applied to α.

PROOF. Let $K = \mathbb{Q}(\theta)$ and $f \in K[x]$ be the minimal polynomial of θ. In $\mathbb{R}[x]$, we may write

$$f = \prod_{i=1}^{r_1}(x-\alpha_i)\cdot\prod_{j=1}^{r_2} f_j,$$

for some $r_1, r_2 \geq 0$ with $r_1 + 2r_2 = [K : \mathbb{Q}]$, where $\alpha_i \in \mathbb{R}$ and f_j is irreducible quadratic. Note that $\mathbb{R}[x]/(f_j) \cong \mathbb{C}$ for each $1 \leq j \leq r_2$ via maps that take $x + (f_j)$ to a chosen root of f_j in $\mathbb{C}$. By Proposition 1.1.1, we then have

$$K \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{i=1}^{r_1} \mathbb{R} \times \prod_{i=1}^{r_2} \mathbb{C}$$

and the composition of the natural inclusion of K in $K \otimes_{\mathbb{Q}} \mathbb{R}$ is the product of the real embeddings of K and one choice of complex embedding of K among pairs of complex conjugate embeddings (i.e., complex primes). We therefore have $r_1 = r_1(K)$ and $r_2 = r_2(K)$. □

EXAMPLES 4.2.4.

a. The field $\mathbb{Q}(i)$ has one complex prime, corresponding to the two complex embeddings of $\mathbb{Q}(i)$ taking i to $\pm i$.

b. The field $\mathbb{Q}(\sqrt[3]{2})$ has one real prime and that takes $\sqrt[3]{2}$ to $\sqrt[3]{2}$ one complex prime corresponding to the two complex embeddings taking $\sqrt[3]{2}$ to $\omega^{\pm 1}\sqrt[3]{2}$.

REMARK 4.2.5. Given a number field K, Theorem 4.2.3 provides us with a product of embeddings

$$\iota_K \colon K \to \prod_{i=1}^{r_1} \mathbb{R} \times \prod_{i=1}^{r_2} \mathbb{C}$$

corresponding to the real and complex primes of K.

4.3. Finiteness of the class group

Throughout this section, we let K be a number field of degree n over $\mathbb{Q}$. We set $r_1 = r_1(K)$ and $r_2 = r_2(K)$. We let σ_i for $1 \leq i \leq r_1$ be the real embeddings of K, and we let τ_i for $1 \leq i \leq r_2$ be a choice of complex embedding from each complex prime of K. We identify $K \otimes_{\mathbb{Q}} \mathbb{R}$ with $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as in Theorem 4.2.3.

We endow $K \otimes_{\mathbb{Q}} \mathbb{R}$ with the Lebesgue measure $\mu_{K \otimes_{\mathbb{Q}} \mathbb{R}}$ on $\mathbb{R}^n \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, where the inverse of said isomorphism is defined by

$$(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \mapsto (x_1, \ldots, x_{r_1}, \mathrm{Re}(z_1), \mathrm{Im}(z_1), \ldots, \mathrm{Re}(z_{r_2}), \mathrm{Im}(z_{r_2})).$$

PROPOSITION 4.3.1. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathscr{O}_K$. Then $\iota_K(\mathfrak{a})$ is a complete lattice in $K \otimes_{\mathbb{Q}} \mathbb{R}$ and*

$$\mathrm{Vol}(\iota_K(\mathfrak{a})) = 2^{-r_2} \cdot N\mathfrak{a} \cdot |\mathrm{disc}(K)|^{1/2}.$$

PROOF. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$. Consider the matrix $A \in M_n(\mathbb{C})$ with ith row

$$(\sigma_1(\alpha_i), \ldots, \sigma_{r_1}(\alpha_i), \tau_1(\alpha_i), \overline{\tau_1(\alpha_i)}, \ldots, \tau_{r_2}(\alpha_i), \overline{\tau_{r_2}(\alpha_i)})$$

and the matrix $B \in M_n(\mathbb{R})$ with ith row

$$(\sigma_1(\alpha_i), \ldots, \sigma_{r_1}(\alpha_i), \mathrm{Re}(\tau_1(\alpha_i)), \mathrm{Im}(\tau_1(\alpha_i)), \ldots, \mathrm{Re}(\tau_{r_2}(\alpha_i)), \mathrm{Im}(\tau_{r_2}(\alpha_i))).$$

Simple column operations yield that $\det A = (-2i)^{r_2} \det B$, and Lemmas 1.4.10 and 1.4.6 imply that

$$|\det A| = |\mathrm{D}(\alpha_1, \dots, \alpha_n)|^{1/2} = N\mathfrak{a} \cdot |\operatorname{disc}(K)|^{1/2}.$$

In particular, $\det B \neq 0$, so the rows of images of the α_i in $K \otimes_{\mathbb{Q}} \mathbb{R}$ are $\mathbb{R}$-linearly independent, which is to say that $\iota_K(\mathfrak{a})$ is complete. Since Lemma 4.1.12 implies that $\operatorname{Vol}(\iota_K(\mathfrak{a})) = |\det B|$, we have the result. □

NOTATION 4.3.2. We define a norm on $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ by

$$\|v\|_K = \sum_{i=1}^{r_1} |x_i| + 2 \sum_{j=1}^{r_2} |z_j|$$

for $v = (x_1, \dots, x_{r_1}, z_1, \dots, z_{r_2})$. For $t > 0$, let

$$D_t = \{v \in K \otimes_{\mathbb{Q}} \mathbb{R} \mid \|v\|_K < t\}.$$

We compute the volume of D_t.

LEMMA 4.3.3. *We have*

$$\mu_{K \otimes_{\mathbb{Q}} \mathbb{R}}(D_t) = 2^{r_1 - r_2} \pi^{r_2} \frac{t^n}{n!}$$

PROOF. We treat this as a problem about the real inner product space $V = R^{r_1} \times \mathbb{C}^{r_2}$ of dimension $n = r_1 + 2r_2$. Let $B_t^{(r_1, r_2)}$ be the subset of $D_t = D_t^{(r_1, r_2)}$ inside V of elements with nonnegative real coordinates. Then $\mu_V(B_t^{(r_1, r_2)}) = 2^{-r_1} \mu_V(D_t^{(r_1, r_2)})$. Suppose first that $r_2 = 0$ and the result holds for $(r_1 - 1, 0)$. Then we have

$$\mu_V(B_t^{(r_1, 0)}) = \int_{x=0}^{t} \mu_V(B_{t-x}^{(r_1 - 1, 0)}) dx = \int_{x=0}^{t} \frac{x^{n-1}}{(n-1)!} dx = \frac{t^n}{n!}.$$

Next, suppose that $r_2 > 0$ and the result holds for $(r_1, r_2 - 1)$. By elementary calculation, we obtain

$$\mu_V(B_t^{(r_1, r_2)}) = \int_{r=0}^{t/2} \int_{\theta=0}^{2\pi} \mu_V(B_{t-2r}^{(r_1, r_2 - 1)}) r dr d\theta = 2\pi \left(\frac{\pi}{2}\right)^{r_2 - 1} \int_{r=0}^{t/2} \frac{(2r)^{n-2}}{(n-2)!} (t - 2r) dr = \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}.$$

□

PROPOSITION 4.3.4. *For any nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, there exists $\alpha \in \mathfrak{a} - \{0\}$ such that*

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \cdot N\mathfrak{a} \cdot |\operatorname{disc}(K)|^{1/2}.$$

PROOF. Let t be such that

$$\mu_{K \otimes_{\mathbb{Q}} \mathbb{R}}(D_t) > 2^n \operatorname{Vol}(\iota_K(\mathfrak{a})). \tag{4.3.1}$$

Since $\iota_K(\mathfrak{a})$ is a lattice, Minkowski's theorem ensures that D_t contains $\iota_K(\alpha)$ for some nonzero $\alpha \in \mathfrak{a}$. Note that $N_{K/\mathbb{Q}}(\alpha)$ is the product of images of α under the distinct field embeddings of K in $\mathbb{C}$. Hence, we have

$$|N_{K/\mathbb{Q}}(\alpha)| = |\sigma_1(\alpha)| \cdots |\sigma_{r_1}(\alpha)| |\tau_1(\alpha)|^2 \cdots |\tau_{r_2}(\alpha)|^2,$$

and since the arithmetic mean bounds the geometric mean, this is at most the nth power of

$$\frac{1}{n}\left(\sum_{i=1}^{r_1}|\sigma_i(\alpha)|+2\sum_{j=1}^{r_2}|\tau_j(\alpha)|\right).$$

On the other hand, since $\alpha \in D_t$, the latter quantity is less than $\frac{t}{n}$, so we have $|N_{K/\mathbb{Q}}(\alpha)| < (\frac{t}{n})^n$. Now, Lemma 4.3.3 and Proposition 4.3.1 allow us to rewrite (4.3.1) as

$$2^{r_1-r_2}\pi^{r_2}\frac{t^n}{n!} > 2^{n-r_2}\cdot N\mathfrak{a}\cdot|\operatorname{disc}(K)|^{1/2}.$$

Set

$$C = \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\cdot N\mathfrak{a}\cdot|\operatorname{disc}(K)|^{1/2},$$

so $(\frac{t}{n})^n > C$. We can and do choose $(\frac{t}{n})^n$ to be less than the smallest integer greater than C. Since $|N_{K/\mathbb{Q}}(\alpha)|$ is an integer, we must then have that $|N_{K/\mathbb{Q}}(\alpha)| \leq C$. □

DEFINITION 4.3.5. Let K be a number field of degree n over $\mathbb{Q}$. The *Minkowski bound* B_K is the quantity

$$B_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|\operatorname{disc}(K)|^{1/2}.$$

Proposition 4.3.4 has the following interesting corollary

COROLLARY 4.3.6. *The discriminant of a number field K satisfies* $|\operatorname{disc}(K)|^{1/2} \geq \left(\frac{\pi}{4}\right)^{r_2}\frac{n^n}{n!}$.

PROOF. Take $\mathfrak{a} = \mathcal{O}_K$ in Proposition 4.3.4, and note that $|N_{K/\mathbb{Q}}(\alpha)| \geq 1$ for all $\alpha \in \mathcal{O}_K$. □

THEOREM 4.3.7 (Minkowski). *Let K be a number field of degree n over $\mathbb{Q}$. Then there exists a set of representatives for the ideal class group of K consisting of integral ideals $\mathfrak{a}$ with $N\mathfrak{a} \leq B_K$.*

PROOF. Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$. Let $d \in K^\times$ be such that $\mathfrak{b} = d\mathfrak{a}^{-1}$ is an integral ideal. By Proposition 4.3.4, there exists $\beta \in \mathfrak{b} - \{0\}$ with $|N_{K/\mathbb{Q}}(\beta)| \leq B_K \cdot N\mathfrak{b}$. Now, note that $(\beta) = \mathfrak{b}\mathfrak{c}$ for some ideal $\mathfrak{c}$ of $\mathcal{O}_K$, and the ideal class of $\mathfrak{c}$ is the ideal class of $\mathfrak{b}^{-1}$, which is the ideal class of $\mathfrak{a}$. Furthermore, we have that $|N_{K/\mathbb{Q}}(\beta)| = N\mathfrak{b}\cdot N\mathfrak{c}$, so $N\mathfrak{c} \leq B_K$, as desired. □

As a consequence, we have the following theorem.

THEOREM 4.3.8. *The class group of a number field is finite.*

PROOF. In fact, the set of nonzero integral ideals $\mathfrak{a}$ with $N\mathfrak{a} \leq B_K$ is finite. To see this, write $\mathfrak{a} = \mathfrak{p}_1^{r_1}\cdots\mathfrak{p}_k^{r_k}$ for distinct prime ideals $\mathfrak{p}_i$ and $r_i \geq 1$ for some $1 \leq i \leq k$. Then

$$N\mathfrak{a} = p_1^{r_1 f_1}\cdots p_k^{r_k f_k},$$

where $N\mathfrak{p}_i = p_i^{f_i}$ with p_i prime. Since there are only finitely many positive integers less than B_K, there are only finitely many primes that could divide $N\mathfrak{a}$, and the exponents of these primes are bounded (e.g., by $\log_2(B_K)$). Since each prime (p) of $\mathbb{Z}$ has only finitely many primes of $\mathcal{O}_K$ lying over it, we are done. □

DEFINITION 4.3.9. The *class number* h_K of a number field K is the order of the class group Cl_K.

The Minkowski bound allows us to actually give bounds on the class number of a number field and sometimes, to actually compute the class group.

EXAMPLE 4.3.10. Consider $K = \mathbb{Q}(\sqrt{-5})$. Note that $\mathrm{disc}(K) = -20$, so the Minkowski bound is

$$B_K = \frac{2}{\pi}\sqrt{20} < 3.$$

Since $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, it is not a PID, so $h_K \geq 2$. Since 2 ramifies in $\mathbb{Z}[\sqrt{-5}]$, the class of the prime over it in K is the only nontrivial element in Cl_K. We therefore have $h_K = 2$.

EXAMPLE 4.3.11. Consider $K = \mathbb{Q}(\sqrt{17})$. In this case $\mathrm{disc}(K) = 17$, and the Minkowski bound is

$$B_K = \frac{1}{2}\sqrt{17} < 3.$$

Set $\alpha = \frac{\sqrt{17}+1}{2}$ so that $\mathscr{O}_K = \mathbb{Z}[\alpha]$. Since the norm of any prime $\mathfrak{p}$ of $\mathbb{Z}[\alpha]$ is at least the prime p with $\mathfrak{p} \cap \mathbb{Z} = (p)$, there exists a set of representatives for Cl_K dividing 2. The minimal polynomial of α is $x^2 - x - 4$, which splits modulo 2. Therefore, the class group Cl_K is generated by the two primes over 2. Their classes are inverse to each other, so Cl_K is generated any one of them, which we denote $\mathfrak{p}$. For $\alpha \in \mathscr{O}_K$, we have $\mathfrak{p} = (\alpha)$ if and only if $N(\alpha) = \pm 2$. Note that

$$N_{K/\mathbb{Q}}\left(\frac{\sqrt{17}+5}{2}\right) = \frac{25-17}{4} = 2,$$

so $\mathfrak{p}$ is principal and K is a UFD.

4.4. Dirichlet's unit theorem

LEMMA 4.4.1. *Let $n, N \geq 1$. The set of algebraic integers α such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq n$ and $|\sigma(\alpha)| \leq N$ for all archimedean embeddings σ of $\mathbb{Q}(\alpha)$ is finite.*

PROOF. Let α be such an integer, and let $f = \sum_{i=0}^{n} a_i x^i$ be its minimal polynomial in $\mathbb{Z}[x]$. In $\mathbb{C}[x]$, we have $f = \prod_\sigma (x - \sigma(\alpha))$, the product being taken over the archimedean embeddings. Then $|a_i|$ is bounded: e.g., it satisfies $|a_i| \leq N^{n-i}\binom{n}{i}$ for all i. As each a_i is an integer, the number of minimal polynomials of elements in the stated set, and hence the order of the set, is finite. □

COROLLARY 4.4.2. *Let K be a number field. Then $\mu(K)$ is a finite group, equal to the set of all $\alpha \in \mathscr{O}_K$ such that $|\sigma(\alpha)| = 1$ for all archimedean embeddings σ of K.*

PROOF. If $\alpha \in \mathscr{O}_K$ satisfies $|\sigma(\alpha)| = 1$ for all σ, then so does α^n for all n. Since the set T of such α is finite by Lemma 4.4.1, the group $\langle \alpha \rangle$ is finite, and hence $\alpha \in \mu(K)$. In particular, since a root of unity has complex absolute value 1 under any archimedean embeddings, the set $\mu(K) = T$ is finite. □

DEFINITION 4.4.3. The *unit group* of a number field K is the group $\mathscr{O}_K^\times$ of units in $\mathscr{O}_K$.

DEFINITION 4.4.4. For a number field K, we let $\ell_K\colon K^\times \to \mathbb{R}^{r_1+r_2}$ be defined on $\alpha \in K^\times$ as

$$\ell_K(\alpha) = (\log|\sigma_1(\alpha)|,\dots,\log|\sigma_{r_1}(\alpha)|,\log|\tau_1(\alpha)|,\dots,\log|\tau_{r_2}(\alpha)|),$$

where $\sigma_1,\dots,\sigma_{r_1}$ are the real embeddings of K and $\tau_1,\dots,\tau_{r_2}$ are the complex embeddings of K.

PROPOSITION 4.4.5. *For a number field K, the set $\ell_K(\mathscr{O}_K^\times)$ is a lattice in $\mathbb{R}^{r_1+r_2}$ that sits in the hyperplane*

$$H = \left\{ (x_1,\dots,x_{r_1+r_2}) \;\middle|\; \sum_{i=1}^{r_1} x_i + 2\sum_{j=1}^{r_2} x_{j+r_1} = 0 \right\},$$

and $\ker \ell_K = \mu(K)$.

PROOF. That $\ker\ell_K = \mu(K)$ is just a rewording of Corollary 4.4.2. For $\alpha \in \mathscr{O}_K^\times$, we have that

$$\sum_{i=0}^{r_1} \log|\sigma_i(\alpha)| + 2\sum_{j=0}^{r_2} \log|\tau_j(\alpha)| = \log|N_{K/\mathbb{Q}}(\alpha)| = 0,$$

the latter equality by Corollary 2.5.18, so $\ell_K(\alpha) \in H$. For $N \geq 0$, consider the bounded subset

$$D_N = \{(x_1,\dots,x_{r_1+r_2}) \in H \mid |x_i| \leq N \text{ for all } i\}$$

of H. By Lemma 4.4.1, the set of elements of $\mathscr{O}_K^\times$ contained in D_N is finite, which means that there exists an open neighborhood U in $\mathbb{R}^{r_1+r_2}$ such that the intersection $U \cap \ell_K(\mathscr{O}_K^\times)$ is $\{0\}$. This implies that $\ell_K(\mathscr{O}_K^\times)$ is a discrete group: the set $\ell_K(\alpha)+U$ is also open and its intersection with $\ell_K(\mathscr{O}_K^\times)$ is $\{\ell_K(\alpha)\}$. Finally, recall that a discrete subgroup of $\mathbb{R}^{r_1+r_2}$ is a lattice. □

Proposition 4.4.5 implies that the sequence

$$1 \to \mu(K) \to \mathscr{O}_K^\times \xrightarrow{\ell_K} \ell_K(\mathscr{O}_K^\times) \to 0$$

is exact and that the set $\ell_K(\mathscr{O}_K^\times)$ is a free abelian group of finite rank. In particular, $\mathscr{O}_K^\times$ is a finitely generated abelian group of rank that of $\ell_K(\mathscr{O}_K^\times)$, and the sequence is split. If $\ell_K(\mathscr{O}_K^\times)$ is a complete lattice in H, then we know that the rank of $\mathscr{O}_K^\times$ is r_1+r_2-1. Dirichlet's unit theorem tells us that this is in fact the case. For this, we require the following lemma.

LEMMA 4.4.6. *Let $A = (a_{ij}) \in M_k(\mathbb{R})$ for some $k \geq 1$ satisfy $a_{ij} < 0$ for all $i \neq j$ and $\sum_{j=1}^k a_{ij} > 0$ for all i. Then A is invertible.*

PROOF. Suppose by way of contradication that $v = (v_1,\dots,v_k) \in \mathbb{R}^k$ is a solution to $Av = 0$, scaled so that $v_j = 1$ for some j and $|v_i| \leq 1$ for all $i \neq j$. Then

$$0 = \sum_{i=1}^k a_{ji}v_i = a_{jj} + \sum_{\substack{i=1\\ i\neq j}}^k a_{ji}v_i. \tag{4.4.1}$$

Note that $a_{ji}v_i \geq a_{ji}$ for $i \neq j$ since a_{ji} is negative and $v_i \leq 1$. Thus, the right-hand side of (4.4.1) is at least $\sum_{i=1}^{k} a_{ij} > 0$, which is the desired contradiction. □

For a number field K, let us use $\kappa_{\mathbb{R}}$ to identify $K \otimes_{\mathbb{Q}} \mathbb{R}$ and $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as rings. We can then make the following definition.

NOTATION 4.4.7. For a number field K, we let

$$[\cdot]\colon K \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{R}$$

denote the multiplicative function given by

$$[(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2})] = |x_1| \cdots |x_{r_1}||z_1|^2 \cdots |z_{r_2}|^2,$$

for $x_i \in \mathbb{R}$ with $1 \leq i \leq r_1$ and $z_j \in \mathbb{C}$ with $1 \leq j \leq r_2$.

The following rather complicated lemma is useful in showing the completeness of $\ell_K(\mathscr{O}_K^{\times})$ in H.

LEMMA 4.4.8. *Let K be a number field of degree n. Set*

$$D = \{v \in K \otimes_{\mathbb{Q}} \mathbb{R} \mid 1/2 \leq [v] \leq 1\}.$$

Let X be a bounded, convex subset of $K \otimes_{\mathbb{Q}} \mathbb{R}$ that is symmetric about the origin and has volume

$$\mu_V(X) > 2^{r_1+r_2} |\operatorname{disc}(K)|^{1/2}.$$

There exist $\alpha_1, \ldots, \alpha_s \in \mathscr{O}_K$ for some $s \geq 1$ such that for each $v \in D$, there exists some $\varepsilon \in \mathscr{O}_K^{\times}$ and $1 \leq i \leq s$ such that $v\iota_K(\varepsilon) \in \iota_K(\alpha_i^{-1})X$.

PROOF. For $w \in K \otimes_{\mathbb{Q}} \mathbb{R}$, the set

$$w \cdot \iota_K(\mathscr{O}_K) = \{w \cdot \iota_K(\alpha) \mid \alpha \in \mathscr{O}_K\}$$

is a complete lattice with volume $2^{-r_2}|\operatorname{disc}(K)|^{1/2} \cdot [w]$. Suppose $w \in D$. Since $[w] \leq 1$, we have

$$2^n \operatorname{Vol}(w \cdot \iota_K(\mathscr{O}_K)) \leq 2^n \operatorname{Vol}(\iota_K(\mathscr{O}_K)) = 2^{r_1+r_2}|\operatorname{disc}(K)|^{1/2},$$

the latter equality by Proposition 4.3.1. Minkowski's theorem then tells us that there exists $\alpha \in \mathscr{O}_K - \{0\}$ such that $w \cdot \iota_K(\alpha) \in X$.

Since X is bounded, there exists $M > 0$ such that $[x] \leq M$ for all $x \in X$. In particular, we have $[w \cdot \iota_K(\alpha)] \leq M$, which since $[w] \geq \frac{1}{2}$ forces $[\iota_K(\alpha)] \leq 2M$ and then $N(\alpha\mathscr{O}_K) \leq 2M$. As there are only finitely many ideals of absolute norm at most $2M$, there are only finitely many ideals $\alpha\mathscr{O}_K$ such that $w \cdot \iota_K(\alpha\mathscr{O}_K) \cap X \neq \{0\}$ for some $w \in D$. Let $\alpha_1\mathscr{O}_K, \ldots, \alpha_s\mathscr{O}_K$ be these ideals.

Finally, given $v \in D$, let $\beta \in \mathscr{O}_K - \{0\}$ have the property that $v \cdot \iota_K(\beta) \in X$. Then $\beta\mathscr{O}_K = \alpha_i\mathscr{O}_K$ for some $1 \leq i \leq s$, so $\varepsilon = \beta\alpha_i^{-1} \in \mathscr{O}_K^{\times}$ and $v \cdot \iota_K(\varepsilon) \in \iota_K(\alpha_i^{-1})X$. □

THEOREM 4.4.9 (Dirichlet's unit theorem). *Let K be a number field. Then we have an isomorphism*

$$\mathscr{O}_K^{\times} \cong \mathbb{Z}^{r_1(K)+r_2(K)-1} \times \mu(K).$$

PROOF. Let D, X, and $\alpha_1, \ldots, \alpha_s \in \mathscr{O}_K$ be as in Lemma 4.4.8. Set

$$Y = \bigcup_{i=1}^{s} \iota_K(\alpha_i^{-1})X.$$

Since Y is bounded, we may let N be such that if $(\lambda_1, \ldots, \lambda_{r_1+r_2}) \in Y$, then $|\lambda_i| \leq N$ for all $1 \leq i \leq r_1 + r_2$. For $1 \leq i \leq r_1 + r_2$, let

$$v^{(i)} = (v_1^{(i)}, \ldots, v_{r_1+r_2}^{(i)}) \in K \otimes_{\mathbb{Q}} \mathbb{R}$$

be an element such that $|v_j^{(i)}| > N$ for $j \neq i$ but $[v^{(i)}] = 1$. Then $v^{(i)} \in D$, so there exists $\varepsilon^{(i)} \in \mathscr{O}_K^\times$ such that $v^{(i)} \cdot \iota_K(\varepsilon^{(i)}) \in Y$. In particular, we must have

$$\iota_K(\varepsilon^{(i)}) = (\varepsilon_1^{(i)}, \ldots, \varepsilon_{r_1+r_2}^{(i)}) = (\sigma_1(\varepsilon^{(i)}), \ldots, \sigma_{r_1}(\varepsilon^{(i)}), \tau_1(\varepsilon^{(i)}), \ldots, \tau_{r_2}(\varepsilon^{(i)}))$$

with $|\varepsilon_j^{(i)}| < 1$ for all $j \neq i$. In other words, $\ell_K(\varepsilon^{(i)})$ has negative coordinates for $j \neq i$.

Assume without loss of generality that $r_1 + r_2 > 1$. Set

$$a_{i,j} = \begin{cases} \log|\sigma_j(\varepsilon^{(i)})| & \text{for } 1 \leq j \leq r_1 \\ 2\log|\tau_{j-r_1}(\varepsilon^{(i)})| & \text{for } r_1 + 1 \leq j \leq r_1 + r_2. \end{cases}$$

Consider the matrix $A = (a_{i,j})_{i,j} \in M_{r_1+r_2-1}(\mathbb{R})$. For $i < r_1 + r_2$, we have that the sum of the ith row is

$$\sum_{j=1}^{r_1+r_2-1} a_{i,j} = -a_{i,r_1+r_2} > 0$$

as $\ell_K(\varepsilon^{(i)}) \in H$ and $i \neq r_1 + r_2$. Lemma 4.4.6 then tells us that A is invertible, so the $\ell_K(\varepsilon^{(i)})$ for $1 \leq i < r_1 + r_2$ form a system of $r_1 + r_2 - 1$ linearly independent vectors in H. In other words, $\ell_K(\mathscr{O}_K^\times)$ is a complete lattice. □

EXAMPLE 4.4.10. Let $K = \mathbb{Q}(\sqrt{d})$ for some square-free integer $d \in \mathbb{Z}$, $d \neq 1$. If K is a real quadratic field, which is to say that $d > 0$, then $r_1(K) = 2$ and $r_2(K) = 0$. Since the complex conjugate of a root of unity ζ equals ζ if and only if $\zeta^2 = 1$, we have in this case that $\mu(K) = \{\pm 1\}$ and

$$\mathscr{O}_K^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

If K is an imaginary quadratic field, which is to say that $d < 0$, then $r_1(K) = 0$ and $r_2(K) = 1$. In this case, since $[K : \mathbb{Q}] = 2$, the field K cannot contain any roots of unity aside from 4th and 6th roots of 1. But $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$ for ω a primitive 3rd root of 1, so for $d < 0$, we have $\mathscr{O}_K^\times \cong \mathbb{Z}/2\mathbb{Z}$ unless $d = -1$ or $d = -3$, in which case $\mathscr{O}_K^\times \cong \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$, respectively.

EXAMPLE 4.4.11. Let $K = \mathbb{Q}(\sqrt{2})$. In this case, we know that $\mathscr{O}_K$ is generated by $\pm\varepsilon$ for some $\varepsilon \in \mathscr{O}_K^\times$ of infinite order. To find $a, b \in \mathbb{Z}$ such that $\varepsilon = a + b\sqrt{2}$, we note that $N_{K/\mathbb{Q}}(a + b\sqrt{2}) = a^2 - 2b^2 = \pm 1$. Suppose we choose ε with $a, b > 0$, which can be done since

$$\{\pm\varepsilon, \pm\varepsilon^{-1}\} = \{\pm a \pm b\sqrt{2}\}.$$

The ε is known as the fundamental unit for K.

If we consider $\varepsilon^n = a_n + b_n\sqrt{2}$ for $n > 1$, it is not hard to check that $a_n > a$ and $b_n > b$. Therefore, we must find a solution to $a^2 - 2b^2 = \pm 1$ with $a > 0$ or $b > 0$ minimal (and therefore both), e.g., $a = b = 1$. That is, $1 + \sqrt{2}$ is a fundamental unit for K.

EXAMPLE 4.4.12. Let $n \geq 3$ be a positive integer, and let m be n or $2n$ according to whether n is even or odd, respectively. We have

$$\mathbb{Z}[\mu_n]^\times \cong \mathbb{Z}^{\frac{\varphi(n)}{2}-1} \times \mu_m.$$

CHAPTER 5

Valuations and completions

5.1. Global fields

DEFINITION 5.1.1. A *global function field*, or a *function field in one variable over a finite field*, is a finite extension of $\mathbb{F}_p(t)$ for some prime p.

REMARK 5.1.2. A function field K in one variable over the finite field $\mathbb{F}_p$ is actually isomorphic to a finite separable extension of $\mathbb{F}_p(u)$ for some $u \in K$, so we always suppose that such a field is a separable extension of $\mathbb{F}_p(t)$ in what follows.

REMARK 5.1.3. In these notes, we will often refer to a function field in one variable over a finite field more simply as a function field.

DEFINITION 5.1.4. A field K is said to be a *global field* if it is either a number field or a function field in one variable over a finite field.

DEFINITION 5.1.5. The *ring of integers* $\mathcal{O}_K$ of a finite extension K of $\mathbb{F}_p(t)$ for a prime p is the integral closure of $\mathbb{F}_p[t]$ in K.

DEFINITION 5.1.6. Let $\mathfrak{p}$ be a nonzero prime ideal in the ring of integers of a global field K. Its ramification index (resp., residue degree) $e_\mathfrak{p}$ (resp., $f_\mathfrak{p}$) is its ramification index (resp., residue degree) over $\mathfrak{p} \cap \mathbb{Z}$ if K is a number field and over $\mathfrak{p} \cap \mathbb{F}_p[t]$ if K is a function field of characteristic p.

In the case of function fields, the choice of ring of integers is not really canonical. For instance, under the field isomorphism $\sigma\colon \mathbb{F}_p(t) \to \mathbb{F}_p(t)$ taking t to t^{-1}, the ring of integers $\mathbb{F}_p[t]$ is carried to $\mathbb{F}_p[t^{-1}]$. In particular, if we write $u = t^{-1}$, then σ restricts to an isomorphism

$$\sigma\colon \mathbb{F}_p[t,t^{-1}] \xrightarrow{\sim} \mathbb{F}_p[u,u^{-1}].$$

This gives a one-to-one correspondence between the nonzero prime ideals of $\mathbb{F}_p[t]$ aside from (t) and the nonzero prime ideals of $\mathbb{F}_p[t^{-1}]$ aside from (t^{-1}).

To phrase this in terms of algebraic geometry, one should view $\operatorname{Spec}\mathbb{F}_p[t]$ and $\operatorname{Spec}\mathbb{F}_p[t^{-1}]$ as two affine open neighborhoods of and covering the projective line $\mathbb{P}^1_{\mathbb{F}_p}$ over $\mathbb{F}_p$ that have intersection $\operatorname{Spec}\mathbb{F}_p[t,t^{-1}]$. The transition, or gluing map, between the two affine spaces along the intersection is that induced by σ. The point of $\mathbb{P}^1_{\mathbb{F}_p}$ that is not contained in $\operatorname{Spec}\mathbb{F}_p[t]$ is the prime ideal (t^{-1}) in $\operatorname{Spec}\mathbb{F}_p[t^{-1}]$, and this is known as the point ∞ at infinity.

DEFINITION 5.1.7. Let K be a global field of characteristic p. A *prime of K over ∞* is a prime ideal of the integral closure of $\mathbb{F}_p[t^{-1}]$ that lies over (t^{-1}).

DEFINITION 5.1.8. Let K be a global function field. The *primes* of K are the nonzero prime ideals of $\mathscr{O}_K$, which are called *finite primes*, and the primes above ∞ in K, which are also known as *infinite primes*.

We compare this with the case of number fields.

DEFINITION 5.1.9. Let K be a number field. The *finite primes* of K are the nonzero prime ideals in $\mathscr{O}_K$. The *infinite primes* of K are the archimedean primes of K. The *primes* of K are the finite and infinite primes of K.

The finite primes of a global field are exactly the nonzero prime ideals of its ring of integers. However, the infinite primes of number fields and function fields are quite different. In the next section, we shall see another classification of the primes that reflects this. For now, note the following.

Every finite prime in a global field K of characteristic p gives rise to a discrete valuation on K, as does every infinite prime, being a prime ideal in a Dedekind ring that is the integral closure of $\mathbb{F}_p[t^{-1}]$ in K.

EXAMPLE 5.1.10. The valuation attached to the prime ∞ of $\mathbb{F}_p(t)$ for a prime p takes a quotient $\frac{f}{g}$ of nonzero polynomials in $\mathbb{F}_p[t]$ to $\deg g - \deg f$ by definition, so it equals v_∞.

REMARK 5.1.11. As with nonzero prime ideals in $\mathscr{O}_K$, we can speak of the ramification index $e_\mathfrak{p}$ and residue degree $f_\mathfrak{p}$ of a prime $\mathfrak{p}$ of K over ∞. In fact, if R is the integral closure of $\mathbb{F}_p[t^{-1}]$ in K, then $\mathfrak{p}$ is a prime ideal of R lying over some prime ideal $(f) = \mathfrak{p} \cap \mathbb{F}_p[t^{-1}]$ of $\mathbb{F}_p[t^{-1}]$. The residue field of $\mathfrak{p}$ is $R/\mathfrak{p}$, and so we may speak of its residue degree over (f). Similarly, the ramification index is the highest power of $\mathfrak{p}$ dividing fR.

5.2. Valuations

DEFINITION 5.2.1. A *(multiplicative) valuation* (or *absolute value*) on a field K is a function $|\ \ |\colon K \to \mathbb{R}_{\geq 0}$ such that

i. $|a| = 0$ if and only if $a = 0$,

ii. $|ab| = |a||b|$, and

iii. $|a+b| \leq |a| + |b|$

for all $a, b \in K$.

REMARK 5.2.2. Every valuation $|\ \ |$ on a field K satisfies $|\zeta| = 1$ for all roots of unity $\zeta \in K^\times$.

DEFINITION 5.2.3. We say that a valuation $|\ \ |$ on a field K is *trivial* if $|a| = 1$ for all $a \in K^\times$, and nontrivial otherwise.

Valuations on fields give rise to metrics. That is, given a valuation $|\ \ |$ on a field K, it defines a distance function d on K by

$$d(a,b) = |a-b|$$

for $a,b \in K$. We can then give K the topology of the resulting metric space. For instance, the trivial valuation on a field gives rise to the discrete topology on K.

DEFINITION 5.2.4. We say that two multiplicative valuations on a field K are *equivalent* if they define the same topology on K.

PROPOSITION 5.2.5. *Let $|\ \ |_1$ and $|\ \ |_2$ be valuations on a field K. The following are equivalent:*

i. the valuations $|\ \ |_1$ and $|\ \ |_2$ are equivalent,

ii. any $a \in K$ satisfies $|a|_1 < 1$ if and only if $|a|_2 < 1$ as well,

iii. there exists $s > 0$ such that $|a|_2 = |a|_1^s$ for all $a \in K$.

PROOF. If $|\ \ |_1$ is nontrivial, then there exists $b \in K$ with $|b|_1 > 1$, and the sequence b^{-n} converges to 0, so the topology $|\ \ |_1$ induces on K is not discrete. Therefore, the trivial valuation is equivalent only to itself. By a check of conditions (ii) and (iii), we may assume that our two valuations are nontrivial.

If the two valuations are equivalent, then a sequence a^n converges to 0 in the common topology if and only if $|a^n|_i = |a|_i^n$ converges to 0, which is to say exactly that $|a|_i < 1$. Hence (i) implies (ii).

Suppose that (ii) holds. Let $b \in K$ be such that $|b|_1 > 1$, and set

$$s = \frac{\log |b|_2}{\log |b|_1} > 0$$

so that $|b|_2 = |b|_1^s$. Choose $a \in K^\times$, and let

$$t = \frac{\log |a|_1}{\log |b|_1} \in \mathbb{R}$$

so that $|a|_1 = |b|_1^t$. Let $m,n \in \mathbb{Z}$ with $n \neq 0$ be such that $t < q = \frac{m}{n}$. Then

$$|a|_1 = |b|_1^t < |b|_1^q,$$

so

$$\left|\frac{a^n}{b^m}\right|_1 < 1,$$

which implies $|a^n b^{-m}|_2 < 1$ and then $|a|_2 < |b|_2^q$ as well. Since this holds for all rational $q > t$, we have $|a|_2 \leq |b|_2^t$. On the other hand, if we assume instead that $q < t$, then we get $|a|_1 > |b|_1^q$, which implies in turn that $|a^{-n}b^m|_1 < 1$, that $|a^{-n}b^m|_2 < 1$, that $|a|_2 > |b|_2^q$, and finally that $|a|_2 \geq |b|_2^t$. We therefore have that

$$|a|_2 = |b|_2^t = |b|_1^{st} = |a|_1^s.$$

Hence, (ii) implies (iii).

For $i \in \{1,2\}$, consider the ball

$$B_i(a,\varepsilon) = \{b \in K \mid |a-b|_i < \varepsilon\}$$

of radius $\varepsilon > 0$ about $a \in K$. If s is as in (iii), then $B_1(a,\varepsilon) = B_2(a,\varepsilon^s)$, so the topologies defined by the two valuations are equivalent. That is, (iii) implies (i). □

REMARK 5.2.6. If $|\ |$ is a valuation and $s > 1$, then $|\ |^s$ need not be a valuation. For instance, let $|\ |$ be the usual absolute value on $\mathbb{R}$. Then $|\ |^2$ is not a valuation, as $2^2 > 1^2 + 1^2$.

DEFINITION 5.2.7. A *nonarchimedean valuation* $|\ |$ on a field K is a nontrivial multiplicative valuation such that

$$|a+b| \leq \max(|a|,|b|)$$

for all $a,b \in K$.

For our purposes, the following ad-hoc definition of an archimedean valuation will suffice.

NOTATION 5.2.8. An *archimedean valuation* on K is a nontrivial valuation on K that is not nonarchimedean.

REMARK 5.2.9. Every valuation in the equivalence class of a nonarchimedean valuation is also nonarchimedean.

The following is a useful equivalent condition for a valuation to be nonarchimedean.

LEMMA 5.2.10. *A nontrivial valuation $|\ |$ on a field K is nonarchimedean if and only if $|n \cdot 1| \leq 1$ for all integers $n \geq 2$.*

PROOF. We write $n \cdot 1 \in K$ more simply as n. If $|\ |$ is nonarchimedean, then

$$|n| \leq \max(|1|,\ldots,|1|) = 1$$

for $n \geq 2$. Conversely, suppose that $|n| \leq 1$ for $n \geq 2$ (and hence for all $n \in \mathbb{Z}$). Let $\alpha,\beta \in K$. For an integer $k \geq 1$, note that

$$|\alpha+\beta|^k \leq \sum_{i=0}^{k} \left| \binom{k}{i} \alpha^i \beta^{k-i} \right| \leq \sum_{i=0}^{k} \left| \binom{k}{i} \right| \max(|\alpha|,|\beta|)^k \leq (k+1)\max(|\alpha|,|\beta|)^k.$$

Taking kth roots, we obtain

$$|\alpha+\beta| \leq (1+k)^{\frac{1}{k}} \max(|\alpha|,|\beta|),$$

and taking the limit as k tends to infinity provides the result. □

As the integer multiples of 1 in a field of positive characteristic are units and 0, Lemma 5.2.10 yields the following.

COROLLARY 5.2.11. *Every nontrivial valuation on a field of positive characteristic is nonarchimedean.*

We also have the following notion, generalizing that of a discrete valuation.

DEFINITION 5.2.12. An *additive valuation* v on a field K is a function $v\colon K \to \mathbb{R}\cup\{\infty\}$ satisfying

i. $v(a) = \infty$ if and only $a = 0$,

ii. $v(ab) = v(a) + v(b)$, and

iii. $v(a+b) \geq \min(v(a), v(b))$

for all $a, b \in K$.

The following gives the comparison between additive valuations and nonarchimedean valuations.

LEMMA 5.2.13. *Let K be a field. Let $v\colon K \to \mathbb{R}\cup\{\infty\}$ and $|\ \ |\colon K \to \mathbb{R}_{\geq 0}$ be such that there exists a real number $c > 1$ such that $|a| = c^{-v(a)}$ for $a \in K$ (taking $c^{-\infty} = 0$). Then v is an additive valuation on K if and only if $|\ \ |$ is a nonarchimedean valuation on K.*

PROOF. Note that $f(x) = c^{-x}$ and $g(x) = -\log_c(x)$ are inverse functions between $\mathbb{R}\cup\{\infty\}$ and $\mathbb{R}_{\geq 0}$. So, $v(ab) = v(a) + v(b)$ if and only if

$$c^{-(v(a)+v(b))} = c^{-v(a)}c^{-v(b)},$$

so if and only if $|ab| = |a||b|$. Moreover,

$$v(a+b) \geq \min(v(a), v(b))$$

if and only if

$$c^{-v(a+b)} \leq c^{-\min(v(a),v(b))} = \max(c^{-v(a)}, c^{-v(b)}),$$

so if and only if $|a+b| \leq \max(|a| + |b|)$. Moreover, $a = \infty$ if and only if $c^{-a} = 0$, the property that $v(a) = \infty$ if and only if $a = 0$ holds if and only if the property that $|a| = 0$ holds if and only if $a = 0$. □

DEFINITION 5.2.14. The *value group* $|K^\times|$ of a valuation on a field K is the subgroup of $\mathbb{R}^\times$ consisting of elements $|a|$ for $a \in K^\times$.

DEFINITION 5.2.15. A valuation on a field K is *discrete* if and only if its value group is a discrete subset of $\mathbb{R}^\times$ (with respect to the subspace topology on $\mathbb{R}$).

REMARK 5.2.16. It is not so hard to show that any discrete valuation on a field is nonarchimedean.

REMARK 5.2.17. A nonarchimedean valuation $|\ \ |$ on a field K is discrete if and only if there exists $c \in \mathbb{R}_{>1}$ such that $v\colon K \to \mathbb{R}\cup\{\infty\}$ defined by $v(a) = \log_c(|a|)$ for $a \in K$ is discrete (i.e., has image $\mathbb{Z}\cup\{\infty\}$). In other words, a discrete (additive) valuation v corresponds to an equivalence class of discrete, nonarchimedean valuations on K.

REMARK 5.2.18. Since $\log_c\colon \mathbb{R}_{>0} \to \mathbb{R}$ is an isomorphism for any $c > 1$ and a subgroup of $\mathbb{R}$ is discrete if and only if it is a lattice, hence cyclic, a nonarchimedean valuation is discrete if and only if its value group is cyclic.

As with discrete valuations, nonarchimedean valuations give rise to a number of structures on a field.

LEMMA 5.2.19. *Let K be a field and $|\ |$ a nonarchimedean valuation on K. The set*

$$\mathscr{O} = \{a \in K \mid |a| \leq 1\}$$

is a subring of K that is local with maximal ideal $\mathfrak{m} = \{a \in K \mid |a| < 1\}$.

PROOF. If $a, b \in \mathscr{O}$, then $|ab| = |a| \cdot |b| \leq 1$ and $|a \pm b| \leq \max(|a|, |b|) \leq 1$, so $\mathscr{O}$ is a ring. Similarly, $\mathfrak{m}$ is an ideal. To see that it is maximal, note that if $a \in \mathscr{O} - \mathfrak{m}$, then $|a^{-1}| = |a|^{-1} = 1$, so $a^{-1} \in \mathscr{O}$. Thus a is a unit, so $\mathscr{O}$ is a local ring with maximal ideal $\mathfrak{m}$. □

DEFINITION 5.2.20. The *valuation ring of a nonarchimedean valuation* $|\ |$ on a field K is the subring $\mathscr{O}$ of K defined by

$$\mathscr{O} = \{a \in K \mid |a| \leq 1\}.$$

REMARK 5.2.21. Similarly, we can speak of the valuation ring of an additive valuation v of K. It is $\mathscr{O} = \{a \in K \mid v(a) \geq 0\}$, and its maximal ideal is $\mathfrak{m} = \{a \in K \mid v(a) > 0\}$.

LEMMA 5.2.22. *Let K be a field and $|\ |$ a nonarchimedean valuation on K. Then the valuation $|\ |$ is discrete if and only if its valuation ring $\mathscr{O}$ is a discrete valuation ring.*

PROOF. If $|\ |$ is discrete, then let $\pi \in \mathfrak{m}$ be an element for which $|\pi|$ is maximal. Then $|\pi|$ generates the value group of $|\ |$, so any $a \in \mathfrak{m}$ may be written as $a = \pi^k u$ for some $k \geq 1$ and $u \in \mathscr{O}^\times$. In particular, $\mathfrak{m} = (\pi)$, so $\mathscr{O}$ is a DVR.

Conversely, if $\mathscr{O}$ is a DVR, let $\pi \in \mathfrak{m}$ be a uniformizer. Then any $a \in K^\times$ may be written $a = \pi^k u$ for some $k \in \mathbb{Z}$ and $u \in \mathscr{O}^\times$, and we have $|a| = |\pi|^k$, so the value group $K^\times$ is cyclic, hence discrete. □

LEMMA 5.2.23. *Let K be a field and $|\ |$ a discrete valuation on K. Let $\mathfrak{m}$ be the maximal ideal of the valuation ring $\mathscr{O}$ of K. Then*

$$\mathfrak{m}^n = \{a \in K \mid |a| \leq r^n\},$$

for all $n \geq 1$, where r is the maximal value of $|\ |$ with $r < 1$.

PROOF. That $\mathfrak{m}$ is as stated follows Lemma 5.2.19 and the fact that $|\ |$ is discrete. Conversely, let $\pi \in \mathfrak{m}$ be a uniformizer. For any $a \in \mathscr{O}$, we have $a = \pi^k u$ for some $k \geq 0$ and $u \in \mathscr{O}^\times$, and $|a| = |\pi|^k$, so $r = |\pi|$, and $a \in \mathfrak{m}^n$ if and only if $|a| \leq r^n$. □

It is useful to pick a canonical, or normalized, multiplicative valuation attached to some of the discrete valuations we have studied. We define the $\mathfrak{p}$-adic absolute value for any nonzero finite prime $\mathfrak{p}$ of a global field.

DEFINITION 5.2.24. Let K be a global field, and let $\mathfrak{p}$ be a finite prime of K, or an infinite prime of K if K is a function field. Let p be the characteristic of the residue field of $\mathfrak{p}$, and let $f_\mathfrak{p}$ denote the residue degree of $\mathfrak{p}$. The $\mathfrak{p}$-*adic absolute value* on K is the unique multiplicative valuation on K that satisfies

$$|a|_\mathfrak{p} = p^{-f_\mathfrak{p} v_\mathfrak{p}(a)}$$

for $a \in K^\times$.

REMARK 5.2.25. If $\mathfrak{p}$ is a finite prime of a global field K that is a principal ideal (π) of $\mathscr{O}_K$, then we denote $|\ \ |_\mathfrak{p}$ by $|\ \ |_\pi$ as well.

EXAMPLE 5.2.26. The p-adic absolute value $|\ \ |_p$ on $\mathbb{Q}$ is defined by $|0|_p = 0$ and

$$|a|_p = p^{-v_p(a)}$$

for $a \in \mathbb{Q}^\times$. Note that it is discrete with valuation ring consisting of reduced fractions with denominator not divisible by p.

EXAMPLE 5.2.27. Let q be a prime power. The absolute value $|\ \ |_\infty$ at infinity on $\mathbb{F}_q(t)$ is defined by $|0|_\infty = 0$ and

$$\left|\frac{f}{g}\right|_\infty = q^{\deg f - \deg g}$$

for nonzero $f, g \in \mathbb{F}_q[t]$.

As for archimedean valuations, we have the following.

DEFINITION 5.2.28. Let K be a number field, and let $\sigma\colon K \hookrightarrow \mathbb{C}$ be an archimedean embedding of K. Then the *absolute value* with respect to σ is the multiplicative valuation $|\ \ |_\sigma\colon K \to \mathbb{R}_{\geq 0}$ defined by $|a|_\sigma = |\sigma(a)|$ (the complex absolute value of $\sigma(a)$) for $a \in K$.

In other words, archimedean primes give rise to archimedean valuations. We now make the following definition.

DEFINITION 5.2.29. A *place* of a global field K is an equivalence class of nontrivial valuations on K.

DEFINITION 5.2.30. A *finite place* (resp., *infinite place*) of a global field K is the equivalence class of the absolute value attached to a finite (resp., infinite) prime of K.

We will see that every place of a global field is either finite or infinite. At present, let us prove this for $\mathbb{Q}$.

THEOREM 5.2.31 (Ostrowski). *The places of $\mathbb{Q}$ are exactly the equivalence classes of the p-adic absolute values on $\mathbb{Q}$ for a prime number p and of the usual absolute value on $\mathbb{Q}$.*

PROOF. Let $|\ \ |$ be a nontrivial valuation on $\mathbb{Q}$. Let $m,n \geq 2$ be integers, and write m as

$$m = \sum_{i=0}^{k} a_i n^i$$

for some integers $0 \leq a_i < n$ for $0 \leq i \leq k$ and some $k \geq 0$, with $a_k \neq 0$. Note that $n^k \leq m$, so

$$k \leq \frac{\log m}{\log n}.$$

Let $N = \max(1,|n|)$. We also have $|1| = 1$, so $|a_i| < n$, and we have

$$|m| < \sum_{i=0}^{k} n|n|^i \leq (1+k)nN^k \leq \left(1 + \frac{\log m}{\log n}\right) nN^{\frac{\log m}{\log n}}.$$

Replacing m by m^t for some $t > 0$ and taking tth roots of both sides, we have

$$|m| < \left(1 + t\frac{\log m}{\log n}\right)^{\frac{1}{t}} n^{\frac{1}{t}} N^{\frac{\log m}{\log n}}.$$

As we let $t \to \infty$, we obtain

$$|m| \leq N^{\frac{\log m}{\log n}}. \tag{5.2.1}$$

If $|n| \leq 1$ for some integer $n \geq 2$, then $N = 1$, and (5.2.1) with this n implies that $|m| \leq 1$ for all $m \geq 2$, and hence for all $m \in \mathbb{Z}$. Since $|\ \ |$ is multiplicative and nontrivial, and $\mathbb{Z}$ is a unique factorization domain, we must then have $|p| < 1$ for some prime number p. Consider the set

$$\mathfrak{m} = \{a \in \mathbb{Z} \mid |a| < 1\}.$$

Since $|\ \ |$ is nonarchimedean by Lemma 5.2.10, the set $\mathfrak{m}$ is an ideal of $\mathbb{Z}$. Since it contains p and is not $\mathbb{Z}$, it must equal (p). Let $s > 0$ be such that $|p| = p^{-s}$. Any $q \in \mathbb{Q}$ can be expressed as $q = p^{v_p(q)}\frac{m}{n}$ for some $m,n \in \mathbb{Z}$ with $p \nmid mn$. We then have

$$|q| = |p|^{v_p(q)} = p^{-sv_p(q)} = |q|_p^s.$$

In other words, $|\ \ |$ is equivalent to $|\ \ |_p$, and moreover, it is not equivalent to $|\ \ |_\ell$ for any prime number $\ell \neq p$, since $\ell \notin \mathfrak{m}$, nor is it equivalent to $|\ \ |_\infty$, since $|2|_\infty = 2 > 1$.

If $|n| > 1$ for all integers $n \geq 2$, then (5.2.1) implies that

$$|m|^{\frac{1}{\log m}} \leq |n|^{\frac{1}{\log n}}$$

for all $m,n \geq 2$. Switching their roles of m and n gives the opposite inequality. In other words, $|n|^{\frac{1}{\log n}}$ is constant for $n \geq 2$, equal to some $s > 1$. We then have

$$|n| = s^{\log n} = n^{\log s}$$

for all $n \geq 2$, and multiplicativity then forces $|q| = |q|_\infty^{\log s}$ for all $q \in \mathbb{Q}$, where $|\ \ |_\infty$ denotes the usual absolute value on $\mathbb{Q}$. Proposition 5.2.5 implies that $|\ \ |$ is equivalent to $|\ \ |_\infty$. □

We also have the following, which we leave as an exercise.

PROPOSITION 5.2.32. *Let q be a prime power. The places of $\mathbb{F}_q(t)$ are exactly the equivalence classes of the f-adic absolute values, for f an irreducible polynomial in $\mathbb{F}_q[t]$, and the absolute value at ∞.*

REMARK 5.2.33. We often index the set V_K of places of a global field K by a subscript, such as v. Each place in V_K, as we have seen already for $K = \mathbb{Q}$ and stated for $K = \mathbb{F}_q(t)$, is represented by the multiplicative valuation attached to a unique prime (as in Definitions 5.2.24 and 5.2.28). We write $|\ \ |_v$ for for this valuation.

We note the following consequence of Theorem 5.2.31.

PROPOSITION 5.2.34. *For any $a \in \mathbb{Q}^\times$, we have $|a|_p = 1$ for all but finitely many prime numbers p, and we have*

$$\prod_{v \in V_\mathbb{Q}} |a|_v = 1.$$

PROOF. Since valuations are multiplicative, it suffices to prove this for -1 and every prime number p. But $|-1|_v = 1$ for all $v \in V_\mathbb{Q}$, and $|p|_\ell = 1$ for primes $\ell \neq p$, while $|p|_p = p^{-1}$ and $|p|_\infty = p$. □

We have a similar consequence of Proposition 5.2.32.

PROPOSITION 5.2.35. *Let q be a power of a prime number. Let $h \in \mathbb{F}_q(t)^\times$. Then $|h|_f = 1$ for all but finitely many irreducible polynomials $f \in \mathbb{F}_q[t]$, and we have*

$$\prod_{v \in V_{\mathbb{F}_q(t)}} |h|_v = 1.$$

We end the section with the weak approximation theorem, which is an analogue of the Chinese remainder theorem for valuations. This requires a lemma.

LEMMA 5.2.36. *Let $|\ \ |_1, |\ \ |_2, \ldots, |\ \ |_k$ be nontrivial, inequivalent valuations on a field K. Then there exists an element $a \in K$ such that $|a|_1 < 1$ and $|a|_j > 1$ for all $j \geq 2$.*

PROOF. In the case $k = 2$, note that Proposition 5.2.5 provides one with elements $\alpha, \beta \in K$ with $|\alpha|_1 < 1$, $|\alpha|_2 \geq 1$, $|\beta|_1 \geq 1$, and $|\beta|_2 < 1$. Then $c = \frac{\alpha}{\beta}$ satisfies $|c|_1 < 1$ and $|c|_2 > 1$.

For $k > 2$, suppose by induction that we have found an element α such that $|\alpha|_1 < 1$ and $|\alpha|_j > 1$ for all $2 \leq j \leq k-1$ and an element β such that $|\beta|_1 < 1$ and $|\beta|_k > 1$. If $|\alpha|_k > 1$, then we simply take $a = \alpha$. If $|\alpha|_k = 1$, then choose $s > 0$ sufficiently large so that $|\alpha|_j^s > |\beta|_j^{-1}$ for all $2 \leq j \leq k-1$ and $|\alpha|_1^s < |\beta|_1^{-1}$. Then $a = \alpha^s \beta$ works.

Finally, if $|\alpha|_k < 1$, let

$$c_m = \beta^{-1}(1+\alpha^m)^{-1}$$

for every integer $m \geq 1$. The sequence $(1+\alpha^m)^{-1}$ has a limit of 1 under the topology of $|\ \ |_i$ if $|\alpha|_i < 1$ and 0 if $|\alpha|_i > 1$. So, we have that $|c_m|_1 \to |\beta|_1^{-1}$, that $|c_m|_j \to 0$ for $2 \leq j \leq k-1$, and that $|c_m|_k \to |\beta|_k^{-1}$. We then take $a = c_m^{-1}$ for a sufficiently large value of m. □

THEOREM 5.2.37 (Weak Approximation). *Let $|\ \ |_1, |\ \ |_2, \ldots, |\ \ |_k$ be nontrivial, inequivalent valuations on a field K, and let $a_1, a_2 \ldots, a_k \in K$. For every $\varepsilon > 0$, there exists an element $b \in K$ such that $|a_i - b|_i < \varepsilon$ for all $1 \leq i \leq k$.*

PROOF. It follows from Lemma 5.2.36 that there exists for each i an element $\alpha_i \in K$ with $|\alpha_i|_i < 1$ and $|\alpha_i|_j > 1$ for all $j \neq i$. For each i and a chosen $\delta > 0$, let $\beta_i = \frac{1}{1+\alpha_i^m}$ for a value of m which is sufficiently large in order that $|\beta_i - 1|_i < \delta$ and $|\beta_i|_j < \delta$ for $j \neq i$. We then set

$$b = \sum_{j=1}^{k} a_j \beta_j,$$

which satisfies

$$|b - a_i|_i \leq |a_i|_i |\beta_i - 1|_i + \sum_{\substack{j=1 \\ j \neq i}}^{k} |a_j|_i |\beta_j|_i < \sum_{j=1}^{k} |a_j|_i \cdot \delta < \varepsilon$$

for a good choice of δ. □

5.3. Completions

DEFINITION 5.3.1. A pair consisting of a field K and a valuation $|\ \ |$ on K is called a *valued field*.

REMARK 5.3.2. When the valuation is understood, a valued field $(K, |\ \ |)$ is often simply denoted K.

DEFINITION 5.3.3. A *topological field K* is a field endowed with a topology with respect to which the binary operations of addition and multiplication are continuous, as are the maps that take an element to its additive inverse and a nonzero element to its multiplicative inverse, the latter with respect to the subspace topology on $K^\times$.

REMARK 5.3.4. A topological field is in particular a topological group with respect to addition, and its multiplicative group is a topological group with respect to multiplication. Moreover, multiplication is continuous on the entire field.

We leave the proof of the following to the reader.

PROPOSITION 5.3.5. *A valued field is a topological field with respect to the topology defined by its valuation.*

REMARK 5.3.6. A nonarchimedean valued field K has a valuation ring $\mathscr{O}$. Terminology is often abused between the two. For instance, the unit group of K would usually be taken to mean the unit group of $\mathscr{O}$. Or, if $\mathscr{O}$ is discrete, a uniformizer of K would mean a uniformizer of $\mathscr{O}$.

DEFINITION 5.3.7. A valued field K is said to be *complete* if it K is complete with respect to the topology defined by its valuation.

EXAMPLE 5.3.8. The fields $\mathbb{R}$ and $\mathbb{C}$ are complete with respect to their usual topologies.

DEFINITION 5.3.9. A field embedding $\iota\colon K \to K'$, where $(K, |\ |)$ and $(K', |\ |')$ are valued fields, is an *embedding of valued fields* if $|\iota(\alpha)|' = |\alpha|$ for all $\alpha \in K$. If $\iota\colon K \to K'$ is an embedding of valued fields, we say that ι *preserves the valuation* on K.

DEFINITION 5.3.10. An *isomorphism of valued fields* is a field isomorphism that is an embedding of valued fields.

We wish to study completions of a valued field K. The completion is a larger field that essentially consists of the limits of Cauchy sequences in K, with field operations determined by the fact that they should be continuous.

THEOREM 5.3.11. *Let $(K, |\ |)$ be a valued field. Then there exists a complete valued field $(\hat{K}, |\ |)$ and a embedding $\iota\colon K \to \hat{K}$ of valued fields such that the image $\iota(K)$ is dense in $\hat{K}$.*

PROOF. Let R be the set of Cauchy sequences on K. By definition, if $(a_n)_n \in R$, then for any $\varepsilon > 0$, there exists $N \geq 1$ such that $|a_n - a_m| < \varepsilon$ for all $n, m \geq N$. Thus, But $||a_n| - |a_m|| \leq |a_n - a_m|$, so $(|a_n|)_n$ is a Cauchy sequence in $\mathbb{R}$, which therefore converges. In other words, we may define a function $\|\ \|\colon R \to \mathbb{R}_{\geq 0}$ by

$$\|(a_n)_n\| = \lim_{n\to\infty} |a_n|.$$

Note that, in particular $(|a_n|)_n$ is bounded for any $(a_n)_n \in R$. It is easy to check that R is a ring: in particular, if $(a_n)_n$, $(b_n)_n \in R$, then

$$|a_n b_n - a_m b_m| \leq |a_n| \cdot |b_n - b_m| + |b_m||a_n - a_m|,$$

and if $|a_n| < M$ and $|b_n| < M$ for all n, then given $\varepsilon > 0$ we choose m, n sufficiently large so that $|a_n - a_m|, |b_n - b_m| < \frac{\varepsilon}{2M}$, and the right-hand side is less than ε.

Let $\mathfrak{M}$ be the set of (Cauchy) sequences on K that converge to 0. We check that $\mathfrak{M}$ is a maximal ideal of R. Clearly, the sum of any two sequences that converges to 0 does as well. If $(a_n)_n \in R$ and $(b_n)_n \in \mathfrak{M}$, then for any $\varepsilon > 0$, we have that

$$|a_n b_n| = |a_n| \cdot |b_n| < \varepsilon$$

for n large enough so that $|b_n| < \frac{\varepsilon}{M}$, where $|a_n| < M$ for all n. If $(a_n)_n \in R - \mathfrak{M}$, then $a_n \neq 0$ for n sufficiently large, so we can add an eventually 0 sequence (which necessarily lies in $\mathfrak{M}$) to it to make

$a_n \neq 0$ for all n. The sequence $(a_n^{-1})_n$ is then defined, and it is Cauchy, as $|a_n|$ is bounded below, and

$$|a_n^{-1} - a_m^{-1}| = \frac{|a_n - a_m|}{|a_n||a_m|}.$$

In other words, $R/\mathfrak{M}$ is a field.

Set $\hat{K} = R/\mathfrak{M}$. We have a natural field embedding $\iota : K \to \hat{K}$ that takes $a \in K$ to the coset of the constant sequence $(a)_n$.

For $(a_n)_n, (b_n)_n \in R$, note that

$$\|(a_n \cdot b_n)_n\| = \lim_{n\to\infty} |a_n b_n| = \lim_{n\to\infty} |a_n| \cdot |b_n| = \|(a_n)_n\| \cdot \|(b_n)_n\|$$

and

$$\|(a_n + b_n)_n\| = \lim_{n\to\infty} |a_n + b_n| \leq \lim_{n\to\infty} (|a_n| + |b_n|) = \|(a_n)_n\| + \|(b_n)_n\|.$$

Moreover, $\|(a_n)_n\| = 0$ if and only if $(a_n)_n \in \mathfrak{M}$. Thus, $\| \ \|$ induces a valuation $| \ |$ on $\hat{K}$, and it clearly preserves the valuation on K.

To see that $\hat{K}$ is complete with respect to $\| \ \|$, let $(c_m)_m$ with $c_m = (c_{m,n})_n$ be a Cauchy sequence in R. If it has a limit in R, its image in $\hat{K}$ has a limit as well. For $\varepsilon > 0$, there exists $N \geq 1$ such that for $m \geq k \geq N$, we have

$$\|c_m - c_k\| = \lim_{n\to\infty} |c_{m,n} - c_{k,n}| < \frac{\varepsilon}{2}.$$

There then exists $N_m \geq N$ such that for $k \leq m$, we have $|c_{m,n} - c_{k,n}| < \frac{\varepsilon}{2}$ for all $n \geq N_m$. On the other hand, since each c_m is Cauchy, there exist $l_m \geq \max(N_m, l_{m-1})$ (with $l_1 \geq N_1$) such that $|c_{m,n} - c_{m,n'}| < \frac{\varepsilon}{2}$ for $n, n' \geq l_m$. Consider the sequence $(a_n)_n$ of elements $a_n = c_{n,l_n}$ of K. For $m \geq k \geq N$, we have

$$|a_m - a_k| = |c_{m,l_m} - c_{k,l_k}| \leq |c_{m,l_m} - c_{k,l_m}| + |c_{k,l_m} - c_{k,l_k}| < \varepsilon$$

by our condition on ℓ_m, so $(a_n)_n \in R$. Moreover,

$$\|c_m - (a_n)_n\| = \lim_{n\to\infty} |c_{m,n} - c_{n,l_n}|,$$

and

$$|c_{m,n} - c_{n,l_n}| \leq |c_{m,n} - c_{m,l_m}| + |c_{m,l_m} - c_{n,l_n}| < \varepsilon$$

for $n \geq m \geq N$ and $n \geq l_m$, which means that $\|c_m - (a_n)_n\| \leq \varepsilon$ for $m \geq N'$. That is, the sequence $(c_m)_m$ of sequences converges to $(a_n)_n$ in R.

Finally, we show that the image of ι is dense. That is, let $(a_n)_n \in R$. For each $m \geq 1$, we have

$$\|(a_m)_n - (a_n)_n\| = \lim_{n\to\infty} |a_m - a_n|,$$

and we saw that $|a_m - a_n| < \varepsilon$ for $m, n \geq N$. But then

$$\|(a_m)_n - (a_n)_n\| \leq \varepsilon$$

so the sequence $(\iota(a_m))_m$ in $\hat{K}$ converges to the image of $(a_n)_n$. □

PROPOSITION 5.3.12. *Let K be a valued field and $\hat{K}$ a complete valued field for which there exists a dense embedding $\iota\colon K \to \hat{K}$ that preserves the valuation on K. If L is a complete valued field and $\sigma\colon K \to L$ is an embedding of valued fields, then there is a unique extension of σ to an embedding $\hat{\sigma}\colon \hat{K} \to L$ of valued fields.*

PROOF. Let $|\ \ |$ (resp., $|\ \ |'$) denote the valuation on K and $\hat{K}$ (resp., L). For any Cauchy sequence $(a_n)_n$ in K, the sequence $\sigma(a_n)_n$ is Cauchy as $|\sigma(a_n) - \sigma(a_m)|' = |a_n - a_m|$, and therefore it is convergent. Define $\hat{\sigma}\colon \hat{K} \to L$ by

$$\hat{\sigma}((a_n)_n) = \lim_{n\to\infty} \sigma(a_n).$$

This is clearly a nonzero ring homomorphism, hence a field embedding, and it extends σ. By definition, it preserves the valuation on $\hat{K}$. Moreover, if $\tau\colon \hat{K} \to L$ is any field embedding extending σ and preserving the valuation on $\hat{K}$, then for any $m \geq 1$, we have

$$|\tau((a_n)_n) - \sigma(a_m)|' = \lim_{n\to\infty} |a_n - a_m|,$$

which since $(a_n)_n$ is Cauchy implies that the sequence $(\sigma(a_m))_m$ converges to $\tau((a_n)_n)$ in L. On the other hand, this limit is by definition $\hat{\sigma}((a_n)_n)$, so $\tau = \hat{\sigma}$. □

This allows us to make the following definition.

DEFINITION 5.3.13. Let $(K, |\ \ |)$ be a valued field. Any complete valued field $(\hat{K}, |\ \ |)$ as in Theorem 5.3.11 is called the *completion* of K.

REMARK 5.3.14. The completion of a valued field is unique up to unique isomorphism fixing K by Theorem 5.3.11.

EXAMPLE 5.3.15. The completion of $\mathbb{Q}$ with respect to the usual absolute value is isomorphic to $\mathbb{R}$. To see this, define $\hat{\iota}\colon \hat{\mathbb{Q}} \to \mathbb{R}$ via the map that takes the class of a Cauchy sequence in $\mathbb{Q}$ to its limit. This is clearly a field embedding preserving the valuation, and it is surjective since, for every real number, there exists a sequence of rationals converging to it.

In fact, any complete archimedean valued field K is topologically isomorphic (i.e., isomorphic via fields via a map which is a homeomorphism) to $\mathbb{R}$ or $\mathbb{C}$. In other words, K is isomorphic as a valued field to $\mathbb{R}$ or $\mathbb{C}$ with valuation given by some power of the usual absolute value.

THEOREM 5.3.16 (Ostrowski). *Let K be a complete valued field with respect to an archimedean valuation. Then K is isomorphic as a valued field to either $(\mathbb{R}, |\ \ |^s)$ or $(\mathbb{C}, |\ \ |^s)$ for some $s \in (0, 1]$, where $|\ \ |$ denotes the usual absolute value on $\mathbb{R}$ or $\mathbb{C}$.*

PROOF. By Corollary 5.2.11, the field K must have characteristic zero. Let $|\ \ |$ denote the valuation on K, and in the proof let us use $|\ \ |_\infty$ to denote the absolute value on $\mathbb{C}$. By Ostrowski's theorem on $\mathbb{Q}$, the restriction of $|\ \ |$ to $\mathbb{Q}$ is equivalent to the usual absolute value. Note that $|\ \ |_\infty^s$ satisfies the

triangle inequality for a given $s \in \mathbb{R}_{>0}$ if and only $s \leq 1$. Let $s \in (0,1]$ be such that $|a| = |a|_\infty^s$ for all $a \in \mathbb{Q}$. As K is complete, it must then contain the completion $(\mathbb{R}, |\ |_\infty^s)$ of $\mathbb{Q}$ with respect to $|\ |$.

If $i = \sqrt{-1} \in K$, then for $\theta \in \mathbb{R}$, we have

$$|e^{2\pi i\theta}| \leq |\cos\theta| + |\sin\theta| \leq \sqrt{2},$$

but since this is true for all θ, we get $|e^{2\pi i\theta}|^n = |e^{2\pi in\theta}| \leq \sqrt{2}$ for all $n \in \mathbb{Z}$. Thus $|e^{2\pi i\theta}| = 1$. Since we can write $z \in \mathbb{C}$ as $z = re^{2\pi i\theta}$ with $r \geq 0$ and $\theta \in \mathbb{R}$, we have $|z| = |z|_\infty^s$ for all $z \in \mathbb{C} \subseteq K$.

In general, we can replace K by $K(i)$ and extend $|\ |$ to $K(i)$ by $|a+bi| = \sqrt{|a|^2 + |b|^2}$, so we may assume that in fact K contains $(\mathbb{C}, |\ |_\infty^s)$ as valued fields. Now let $\alpha \in K$, and let $w \in \mathbb{C}$ be such that $|\alpha - w|$ is minimal: this exists since the infimum t occurs as a limit in the closed ball of radius $|\alpha| + u$ about 0 in $\mathbb{C}$ for any $u > t$.

Now suppose $\alpha \notin \mathbb{C}$, which is to say that $t > 0$. Replacing α by $\alpha - w$, we may as well assume that $w = 0$. Then $t = |\alpha| \leq |\alpha - z|$ for all $z \in \mathbb{C}$. For $z \in \mathbb{C}$ and $n \geq 1$, note that

$$|z|^n + t^n \geq |\alpha^n - z^n| = \prod_{j=0}^{n-1} |\alpha - \zeta_n^j z| \geq t^{n-1}|\alpha - z|$$

where $\zeta_n = e^{2\pi i/n}$. We then have

$$|\alpha - z| \leq t\left(\frac{|z|^n}{t^n} + 1\right).$$

Thus, taking z such that $|z| < t$ and the limit as n tends to ∞, we obtain that $|\alpha - z| \leq t$. By minimality of t, this forces $|\alpha - z| = t$.

By the same argument with $\alpha - z$ replacing α, we see then that $|\alpha - z - w| = t$ for all $w \in \mathbb{C}$ with $|w| < t$. Recursively, we then see in particular that $|\alpha - mz| = t$ for all $m \geq 1$ and $z \in \mathbb{C}$ with $|z| \leq \alpha$. The set of all such mz being $\mathbb{C}$, we see that $|\alpha - z| = t$ for all $z \in \mathbb{C}$. But then $|z| \leq |z - \alpha| + |\alpha| = 2t$ for all $z \in \mathbb{C}$ which contradicts $|z| = |z|_\infty^s$ for any $z \in \mathbb{C}$ with sufficiently large $|z|_\infty$. In other words, α does not exist. □

LEMMA 5.3.17. *Let $(K, |\ |)$ be a nonarchimedean valued field, and let $(\hat{K}, |\ |)$ be its completion. Then $|\ |$ is a nonarchimedean valuation on $\hat{K}$ with the same value group as its restriction to K. If $\mathcal{O}$ (resp., $\hat{\mathcal{O}}$) denotes the valuation ring of K (resp., $\hat{K}$) and $\mathfrak{m}$ (resp., $\hat{\mathfrak{m}}$) denotes its the maximal ideal, then the canonical map*

$$\bar{\iota}\colon \mathcal{O}/\mathfrak{m} \to \hat{\mathcal{O}}/\hat{\mathfrak{m}}$$

is an isomorphism. Moreover, if $|\ |$ is discrete on K, then it is on $\hat{K}$ as well, and

$$\bar{\iota}_n\colon \mathcal{O}/\mathfrak{m}^n \to \hat{\mathcal{O}}/\hat{\mathfrak{m}}^n$$

is an isomorphism for every $n \geq 1$.

PROOF. That $\hat{K}$ is nonarchimedean is an immediate corollary of Lemma 5.2.10 (and can also be seen directly). If a is nonzero, then $|a_n - a| < |a|$ for all sufficiently large n, so $|a_n| = |(a_n - a) + a| = |a|$, and thus the value groups of $|\ \ |$ on K and $\hat{K}$ are equal.

Since the embedding $K \to \hat{K}$ preserves the valuation, we have $\mathfrak{m} = \mathscr{O} \cap \hat{\mathfrak{m}}$, so $\bar{\iota}$ is injective. If $a \in \hat{\mathscr{O}}$, then since K is dense in $\hat{K}$, there exists $b \in K$ with $|b - a| < 1$, so $b - a \in \hat{\mathfrak{m}}$, which in particular implies $b \in \hat{\mathscr{O}} \cap K = \mathscr{O}$ with $\bar{\iota}(b + \mathfrak{m}) = a + \hat{\mathfrak{m}}$. In other words, $\bar{\iota}$ is surjective.

If $|\ \ |$ is discrete on K, then any Cauchy sequence in K has valuation that is eventually constant or heads to 0. As a uniformizer π of K is also one of $\hat{K}$, it follows immediately that $\bar{\iota}_n$ is injective. We have

$$\mathfrak{m}^n = \{a \in K \mid |a| \leq |\pi|^n\},$$

and so if $a \in \hat{\mathfrak{m}}^n$ and we choose $b \in K$ with $|b - a| < |\pi|^n$, then $|b| \leq |\pi|^n$, so $b \in \mathfrak{m}^n$. That is, $\bar{\iota}_n$ is surjective. □

REMARK 5.3.18. A discrete additive valuation v on a field K extends to a discrete valuation on $\hat{K}$, usually denoted v as well.

DEFINITION 5.3.19. A valued field is said to be *discretely valued* if its valuation is discrete. A *complete discrete valuation field* is a complete discretely valued field.

PROPOSITION 5.3.20. *Let K be a complete discrete valuation field. Let $\mathscr{O}$ be its valuation ring, and $\mathfrak{m}$ the maximal ideal of $\mathscr{O}$. Let T be a set of representatives of $\mathscr{O}/\mathfrak{m}$ that includes 0, and let π be a uniformizer of $\mathscr{O}$. Every element $a \in K$ is a limit of a unique sequence of partial sums of the form*

$$a_n = \sum_{k=m}^{n} c_k \pi^k$$

for $m \in \mathbb{Z}$ and $c_k \in T$ for all $k \geq m$, with $c_m \neq 0$. Moreover, the additive valuation of such an element a is m.

PROOF. Since each a_n must have valuation m and the a_n must converge to a, we must have $m = v(a)$. So, we take $a_{m-1} = 0$ and, inductively, for any $n \geq m$, we write $a - a_{n-1} = b_n \pi^n$ for some $b_n \in \mathscr{O}$, and let $c_n \in T$ be the unique element such that $c_n \equiv b_n \bmod \mathfrak{m}$. (Note that $c_m \neq 0$.) Then

$$a - a_n = b_n \pi^n - c_n \pi^n \in \mathfrak{m}^{n+1},$$

and $c_n \in T$ is unique such that this holds. By definition, a is then the limit of the a_n, and the choice of each c_n is the only possibility for which this happens, as if $a \not\equiv a_n \bmod \mathfrak{m}^{n+1}$, then since $a \not\equiv a_k \bmod \mathfrak{m}^{n+1}$ for all $k > n$, the sequence $(a_n)_n$ would not converge to a. □

NOTATION 5.3.21. Let $(K, |\ \ |)$ be a complete discrete valuation field. The element

$$\sum_{k=m}^{\infty} c_k \pi^k \in \hat{K}$$

with $c_k \in \mathscr{O}$ is the limit of the corresponding sequence of partial sums.

EXAMPLE 5.3.22. By Proposition 5.3.20, the completion a field $K(t)$ with respect to the t-adic valuation on K is isomorphic to the field $K(\!(t)\!)$ of Laurent series in t. The valuation ring of $K(\!(t)\!)$ is the ring $K[\![t]\!]$ of power series in K.

DEFINITION 5.3.23. The field $\mathbb{Q}_p$ of *p-adic numbers* is the completion of $\mathbb{Q}$ with respect to its p-adic valuation. Its valuation ring $\mathbb{Z}_p$ is the ring of p-adic integers.

REMARK 5.3.24. An arbitrary element of $\mathbb{Q}_p$ has the unique form

$$\sum_{i=m}^{\infty} c_i p^i,$$

where $m \in \mathbb{Z}$ and $0 \leq c_i \leq p-1$ for each $i \geq m$, with $c_m \neq 0$. It is a p-adic integer (resp., unit) if and only if $m \geq 0$ (resp., $m = 0$).

EXAMPLE 5.3.25. The element $\alpha = 1 + p + p^2 + p^3 + \cdots \in \mathbb{Z}_p$ is $\frac{1}{1-p}$. To see this, note that

$$(1 + p + p^2 + \cdots + p^n)(1-p) = 1 - p^{n+1},$$

and the sequence $(1-p^{n+1})_n$ converges to 1. In particular,

$$-1 = \sum_{n=0}^{\infty} (p-1)p^n \in \mathbb{Z}_p.$$

Taking into account Lemma 5.3.17, the following gives an alternate description of the valuation ring of the completion of a discrete valuation field.

PROPOSITION 5.3.26. *Let K be a complete discrete valuation field, let $\mathscr{O}$ be its valuation ring, and let $\mathfrak{m}$ be the maximal ideal of $\mathscr{O}$. Then the map*

$$\phi : \mathscr{O} \to \varprojlim_n \mathscr{O}/\mathfrak{m}^n$$

that takes $a \in \mathscr{O}$ to the compatible sequence $(a + \mathfrak{m}^n)_n$ is an isomorphism of rings.

PROOF. This is actually a corollary of Proposition 5.3.20, in that $a_n + \mathfrak{m}^n$ for $a_n \in \mathscr{O}$ has a unique representative of the form

$$\sum_{k=0}^{n-1} c_k \pi^k$$

with $c_i \in T$, where T is a set of representatives of $\mathscr{O}/\mathfrak{m}$ and π is a fixed uniformizer of $\mathscr{O}$, and the c_i are independent of $n \geq i$. The element

$$a = \sum_{k=0}^{\infty} c_k \pi^k \in \mathscr{O}$$

is the unique element of $\mathscr{O}$ mapping to $(a_n + \mathfrak{m}^n)_n$. □

DEFINITION 5.3.27. Let A be a discrete valuation ring, and let $\mathfrak{p}$ be its maximal ideal. We say that A is *complete* if the canonical map

$$A \to \varprojlim_n A/\mathfrak{p}^n.$$

is an isomorphism.

The reader will verify the following.

LEMMA 5.3.28. *Let A be a DVR, and let K be its quotient field. Then K is complete with respect to the discrete valuation induced by the valuation on A if and only if A is complete.*

DEFINITION 5.3.29. Let K be a field, and let $f = \sum_{n=0}^{\infty} a_n x^n \in K[\![x]\!]$. For $k \geq 1$, the kth derivative of f is the power series $f^{(k)} \in K[\![x]\!]$ defined by

$$f^{(k)} = \sum_{n=0}^{\infty} (n+1)\cdots(n+k)a_{n+k}x^n.$$

THEOREM 5.3.30 (Hensel's Lemma). *Let K be a complete nonarchimedean valuation field with valuation ring $\mathscr{O}$ having maximal ideal $\mathfrak{m}$. Let $f \in \mathscr{O}[x]$, and let $\bar{f} \in \mathscr{O}/\mathfrak{m}[x]$ be the image of f. Suppose that $\bar{\alpha} \in \mathscr{O}/\mathfrak{m}$ is a simple root of $\bar{f}$. Then there exists a unique root α of f in $\mathscr{O}$ that reduces to $\bar{\alpha}$ modulo $\mathfrak{m}$.*

PROOF. Let $\alpha_0 \in \mathscr{O}$ be any lifting of $\bar{\alpha}$, and let $\pi = f(\alpha_0) \in \mathfrak{m}$. (If $\mathscr{O}$ is a DVR, we can instead take π to be a uniformizer.) Suppose by induction that we have found $\alpha_k \in \mathscr{O}$ for $0 \leq k \leq n$ such that $\alpha_n \equiv \alpha_k \bmod \pi^{2^k}$ for all such k and $f(\alpha_n) \equiv 0 \bmod \pi^{2^n}$. Writing $f = \sum_{i=0}^{\deg f} a_i x^i$ with $a_i \in \mathscr{O}$, we see that

$$f(\alpha_n + x) - (f(\alpha_n) + f'(\alpha_n)x) = \sum_{i=0}^{\deg f} a_i(\alpha_n + x)^i - \sum_{i=0}^{\deg f} a_i\alpha_n^i - \sum_{i=0}^{\deg f} i a_i \alpha_n^{i-1} x$$

is an element of (x^2) inside $\mathscr{O}[x]$. We therefore have that

$$f(\alpha_n + \beta\pi^{2^n}) \equiv f(\alpha_n) + f'(\alpha_n)\cdot\beta\pi^{2^n} \bmod \pi^{2^{n+1}}$$

for any $\beta \in \mathscr{O}$. Note that $f'(\alpha_n) \not\equiv 0 \bmod \pi$ (and in fact is a unit), since $\bar{\alpha}$ is a simple foot of f in $\mathscr{O}/\mathfrak{m}$. As $f'(\alpha_n)$ is invertible and π^{2^n} divides $f(\alpha_n)$, we may choose $\beta \in \mathscr{O}$ such that $f(\alpha_n + \beta\pi^{2^n}) \equiv 0 \bmod \pi^{2^{n+1}}$, and this choice is unique modulo π^{2^n}. We then set $\alpha_{n+1} = \alpha_n + \beta\pi^{2^n}$ so that $\alpha_{n+1} \equiv \alpha_n \bmod \pi^{2^n}$, and again we have $f(\alpha_{n+1}) \equiv 0 \bmod \pi^{2^{n+1}}$. Note that α_{n+1} is unique modulo $\pi^{2^{n+1}}$ with this property: in fact,

$$\alpha_{n+1} \equiv \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)} \bmod \pi^{2^{n+1}}. \tag{5.3.1}$$

Finally, letting

$$\alpha = \lim_{n\to\infty} \alpha_n,$$

we note that f defines a continuous function on $\mathscr{O}$, so

$$f(\alpha) = \lim_{n\to\infty} f(\alpha_n) = 0,$$

and α is by construction unique with this property among roots reducing to $\bar{\alpha}$. □

EXAMPLE 5.3.31. The polynomial $f = x^2 - 2$ has two simple roots in $\mathbb{F}_7$, which are 3 and 4. Hensel's Lemma tells us that it has two roots in $\mathbb{Z}_7$ as well. We may approximate such a root recursively using (5.3.1) in the proof of said result. For instance,

$$3 - \frac{3^2-2}{2\cdot 3} = 3 - \frac{1}{6}7 \equiv 10 \bmod 49$$

is a root of f modulo 49, and

$$10 - \frac{10^2-2}{2\cdot 10} = 10 - \frac{1}{10}7^2 \equiv 3 + 7 + 2\cdot 7^2 + 6\cdot 7^3 \equiv 2166 \bmod 7^4$$

is a root of f modulo 2401.

The following lemma provides another nice application of Hensel's Lemma.

LEMMA 5.3.32. *The group of roots of unity in $\mathbb{Q}_p$ has order $p-1$ for an odd prime p and 2 for $p = 2$.*

PROOF. The polynomial $x^{p-1} - 1$ splits completely into distinct linear factors $\mathbb{F}_p[x]$, since $\mathbb{F}_p^\times$ is cyclic of order $p-1$. By Hensel's Lemma, we see that each root of $x^{p-1} - 1$ in $\mathbb{F}_p$ lifts uniquely to a root of $x^{p-1} - 1$ in $\mathbb{Z}_p$. That is, $\mu_{p-1}(\mathbb{Q}_p)$ contains $p-1$ elements.

Suppose that ζ_n is a primitive nth root of unity ζ_n in $\mathbb{Q}_p$ (hence in $\mathbb{Z}_p$) for $n \geq 1$. Then ζ_n reduces to a root of unity in $\mathbb{F}_p$. If the order m of this root of unity is less than n, then ζ_n^m is trivial in $\mathbb{F}_p$, so $\zeta_n^m - 1 \in p\mathbb{Z}_p$. In particular, there exists a prime ℓ such that $\mathbb{Z}[\mu_\ell] \subseteq \mathbb{Z}_p$ and $\zeta_\ell - 1 \in p\mathbb{Z}_p$. Since $\zeta_\ell - 1$ divides ℓ, this would imply $\ell \in p\mathbb{Z}_p$, forcing $\ell = p$. On the other hand, if $\zeta_{2p} \in \mathbb{Z}_p$, then $\mathbb{Z}_p$ contains $\mathbb{Z}_p[\mu_{2p}]$, and so $p^{-1}(\zeta_{2p} - 1)^{\varphi(2p)} \in \mathbb{Z}_p^\times$ which contradicts the fact that p is a uniformizer in $\mathbb{Z}_p$. □

The following is a strong form of Hensel's lemma (without the uniqueness statement) that is sometimes also referred to as Hensel's lemma.

THEOREM 5.3.33 (Hensel). *Let K be a complete nonarchimedean valuation field with valuation ring $\mathscr{O}$ and maximal ideal $\mathfrak{m}$. If $f \in \mathscr{O}[x]$ is primitive and its image $\bar{f} \in \mathscr{O}/\mathfrak{m}[x]$ factors as $\bar{f} = \bar{g}\bar{h}$, where $\bar{g}$ and $\bar{h}$ are relatively prime, then f factors as $f = gh$ in $\mathscr{O}[x]$, where g and h reduce to $\bar{g}$ and $\bar{h}$, and $\deg g = \deg \bar{g}$.*

Moreover, if $g', h' \in \mathscr{O}[x]$ with $\deg g' = \deg \bar{g}$ satisfy $f \equiv g'h' \bmod \mathfrak{b}$ for some ideal $\mathfrak{b} \subseteq \mathfrak{m}$ and reduce to $\bar{g}$ and $\bar{h}$ respectively, then g and h can be chosen so that $g \equiv g' \bmod \mathfrak{b}$ and $h \equiv h' \bmod \mathfrak{b}$.

PROOF. Note that $f \in \mathscr{O}[x]$ is primitive if and only if $f \not\equiv 0 \bmod \mathfrak{m}$. Let k be the degree of $\deg \bar{g}$, and let d be the degree of f. Let $g_0, h_0 \in \mathscr{O}[x]$ be lifts of $\bar{g}$ and $\bar{h}$, respectively, such that $\deg g_0 = k$ and $\deg h_0 \leq d-k$, so

$$f \equiv g_0 h_0 \bmod \mathfrak{m}.$$

Since $\bar{g}$ and $\bar{h}$ are relatively prime, there exist $\bar{a}, \bar{b} \in \mathscr{O}/\mathfrak{m}[x]$ such that $\bar{a}\bar{g} + \bar{b}\bar{h} = 1$. Let $a, b \in \mathscr{O}[x]$ be lifts of $\bar{a}$ and $\bar{b}$, respectively, so we have

$$ag_0 + bh_0 \equiv 1 \bmod \mathfrak{m}.$$

Let $\mathfrak{a} \subseteq \mathfrak{m}$ be the ideal of $\mathscr{O}$ generated by the coefficients of $ag_0 + bh_0 - 1$, which will be generated by an element $\pi \in \mathfrak{a}$ that can be taken as the coefficient of maximal valuation. (We use $\mathfrak{a}$ in the argument below to deal with the possibility that the valuation on K is not discrete.)

Suppose by induction that for $n \geq 1$ and $m \leq n-1$, we have found polynomials g_m and h_m with $\deg(g_m - g_0) < k$ and and $\deg h_m \leq d-k$ such that

$$f \equiv g_m h_m \bmod \mathfrak{a}^{m+1},$$

for $m \leq n-1$ and both

$$g_{m+1} \equiv g_m \bmod \mathfrak{a}^{m+1} \quad \text{and} \quad h_{m+1} \equiv h_m \bmod \mathfrak{a}^{m+1}$$

for $m \leq n-2$. Let

$$f_n = \pi^{-n}(f - g_{n-1}h_{n-1}) \in \mathscr{O}[x].$$

Since g_0 is a lift of $\bar{g}$ with $\deg g_0 = k$, its leading coefficient is a unit. Hence, using the division algorithm, we may write

$$bf_n = q_n g_0 + r_n,$$

where $q_n, r_n \in \mathscr{O}[x]$ and $\deg r_n < k$. Then

$$(af_n + q_n h_0)g_0 + r_n h_0 = af_n g_0 + bf_n h_0 \equiv f_n \bmod \mathfrak{a}. \tag{5.3.2}$$

Let $s_n \in \mathscr{O}[x]$ be the polynomial with coefficients that agree with those coefficients of $af_n + q_n h_0$ that have nonzero reduction modulo $\mathfrak{a}$ and which are 0 otherwise. Then set

$$g_n = g_{n-1} + \pi^n r_n \quad \text{and} \quad h_n = h_{n-1} + \pi^n s_n.$$

Note that

$$\begin{aligned} g_n h_n &\equiv g_{n-1}h_{n-1} + \pi^n(r_n h_{n-1} + s_n g_{n-1}) \\ &\equiv g_{n-1}h_{n-1} + \pi^n(r_n h_0 + s_n g_0) \\ &\equiv g_{n-1}h_{n-1} + \pi^n f_n \\ &\equiv f \bmod \mathfrak{a}^{n+1}. \end{aligned}$$

Since $\deg(g_{n-1} - g_0) < k$ and $\deg r_n < k$, we have $\deg(g_n - g_0) < k$. Since $\deg(r_n h_0) < d$ and $\deg f_n \leq d$, we have by (5.3.2) that the reduction of $(af_n + q_n h_0)g_0$ modulo $\mathfrak{a}$ has degree at most d. Since

$\deg g_0 = k$, we therefore have that the reduction of $af_n + q_n h_0$ has degree at most $d-k$. As the nonzero coefficients of s_n, which is congruent to $a_n f_n + q_n h_0$ modulo $\mathfrak{a}$, are all units, we then have $\deg(s_n) \leq d-k$. Hence, we have completed the induction.

Now, since the degree of g_n is k, the degree of h_n is bounded by $d-k$, and $\bigcap_{n\geq 1} \mathfrak{a}^n = (0)$, it makes sense to consider the limits of these sequences of polynomials by taking the limits of their coefficients, with the resulting quantity an actual polynomial. Defining g and h to be the limits of the sequences $(g_n)_n$ and $(h_n)_n$ respectively, we obtain $f = gh$, as desired. The last statement follows easily from the above argument. □

REMARK 5.3.34. A valuation ring satisfying Hensel's lemma (without the uniqueness statement) is called a Henselian ring. One may check that any Henselian ring satisfies the strong form of Hensel's lemma as well.

5.4. Extension of valuations

In this section, we study the extension of a valuation on a (complete) field to a larger field.

DEFINITION 5.4.1. Let K be a field, and let $|\ \ |_K$ be a valuation on K. If L is a field extension of K, then an *extension* $|\ \ |_L$ of $|\ \ |_K$ to L is a valuation on L such that $|\alpha|_L = |\alpha|_K$ for all $\alpha \in K$.

In the case of global fields, we note the following.

REMARK 5.4.2. Let L/K be an extension of global fields, let $\mathfrak{p}$ be a nonarchimedean prime of K and $\mathfrak{P}$ a prime lying above it. The normalized $\mathfrak{P}$-adic valuation is equivalent, but not always equal to, an extension of the normalized $\mathfrak{p}$-adic valuation. That is, for $\alpha \in K$, we have

$$|\alpha|_{\mathfrak{P}} = p^{-f_{\mathfrak{P}} v_{\mathfrak{P}}(\alpha)} = p^{-f_{\mathfrak{P}} e_{\mathfrak{P}/\mathfrak{p}} v_{\mathfrak{p}}(\alpha)} = |\alpha|_{\mathfrak{p}}^{e_{\mathfrak{P}/\mathfrak{p}} f_{\mathfrak{P}/\mathfrak{p}}}.$$

In the case that the extension field is of finite degree, the following proposition restricts the possibilities for an extension of the valuation below to the extension field, up to equivalence.

PROPOSITION 5.4.3. *Let $(K, |\ \ |)$ be a complete valuation field, and let $(V, |\ \ |)$ be a finite-dimensional normed vector space over K such that $|\alpha v| = |\alpha||v|$ for all $\alpha \in K$ and $v \in V$. Then V is complete with respect to $|\ \ |$, and if $v_1, \ldots, v_n$ is an ordered basis of V, then the isomorphism $\phi : K^n \to V$ with*

$$\phi(a_1, \ldots, a_n) = \sum_{i=1}^{n} a_i v_i$$

is a homemorphism.

PROOF. The topology defined on K^n by the maximum norm

$$\|(a_1, \ldots, a_n)\| = \max(|a_1|, \ldots, |a_n|)$$

for $a_1, \ldots, a_n \in K$ agrees with the product topology. Via the map ϕ, this induces a norm

$$\|a_1 v_1 + \cdots + a_n v_n\| = \max(|a_1|, \ldots, |a_n|)$$

on V that we must show agrees with topology defined by the original norm $|\ \ |$ on V.

It suffices to show that there exists real numbers $c_1, c_2 > 0$ such that

$$c_1 \|v\| \leq |v| \leq c_2 \|v\|$$

for all $v \in V$. Take $c_2 = |v_1| + \cdots + |v_n|$. Then we have

$$|a_1 v_1 + \cdots + a_n v_n| \leq \sum_{i=1}^{n} |a_i||v_i| \leq \max(|a_1|, \ldots, |a_n|) \cdot \sum_{i=1}^{n} |v_i| = c_2 \|a_1 v_1 + \cdots + a_n v_n\|.$$

Suppose by the induction that we have the existence of c_1 for all vector spaces of dimension less than n. The case $n = 1$ is covered by taking $c_1 = |v_1|$. In general, let W_i be the K-span of $\{v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n\}$. Then each W_i is complete with respect to $|\ \ |$, hence is a closed subspace of V. Let B be an open ball of radius $\varepsilon > 0$ about $0 \in V$ such that $B \cap (v_i + W_i) = \varnothing$ for all $1 \leq i \leq n$. Let $v = \sum_{i=1}^{n} a_i v_i \in V$ with $v \neq 0$. For any $1 \leq j \leq n$ with $a_j \neq 0$, we have $a_j^{-1} v \in v_j + W_j$, so $|a_j^{-1} v| \geq \varepsilon$. In particular, we have $|v| \geq \varepsilon \|(a_1, \ldots, a_n)\| = \varepsilon \|v\|$, so we may take $c_1 = \varepsilon$. □

We will require the following lemma.

LEMMA 5.4.4. *Let $(K, |\ \ |)$ be a complete nonarchimedean valuation field. Let*

$$f = \sum_{i=0}^{n} a_i x^i \in K[x]$$

be irreducible with $a_n \neq 0$. Then either $|a_0|$ or $|a_n|$ is maximal among the values $|a_i|$ with $0 \leq i \leq n$.

PROOF. By multiplying f by an element of K, we may assume that $f \in \mathcal{O}[x]$, where $\mathcal{O}$ is the valuation ring of K, and at least one coefficient of f is a unit. Let j be minimal such that $a_j \in \mathcal{O}^\times$. If $\mathfrak{m}$ denotes the maximal ideal of $\mathcal{O}$, then

$$f \equiv (a_j + a_{j+1} x + \cdots + a_n x^{n-j}) x^j \bmod \mathfrak{m}.$$

Unless $j = 0$ or $j = n$, this contradicts Theorem 5.3.33, since f would be reducible in $\mathcal{O}[x]$. □

The following corollary of Lemma 5.4.4 is immediate.

COROLLARY 5.4.5. *Let $(K, |\ \ |)$ be a complete nonarchimedean valuation field. Let f be a monic, irreducible polynomial in $K[x]$ such that $f(0)$ lies in the valuation ring $\mathcal{O}$ of $|\ \ |$. Then $f \in \mathcal{O}[x]$.*

This in turn, has the following corollary.

COROLLARY 5.4.6. *Let $(K, |\ \ |)$ be a complete nonarchimedean valuation field. Let L be a finite extension of K. Let $\mathcal{O}$ be the valuation ring of K. Then the integral closure of $\mathcal{O}$ in L is equal to*

$$\{\beta \in L \mid N_{L/K}(\beta) \in \mathcal{O}\}.$$

PROOF. Let $n = [L : K]$. Let $\beta \in L^\times$, and let $f \in K[x]$ be its minimal polynomial. Lemma 1.3.14 tells us that $N_{L/K}(\beta) \in \mathscr{O}$ for every integral $\beta \in L$. On the other hand, we have

$$N_{L/K}(\beta) = (-1)^n f(0)^{n/d},$$

where $d = [K(\beta) : K]$. So, if $N_{L/K}(\beta) \in \mathscr{O}$, then $f(0) \in \mathscr{O}$, and Corollary 5.4.5 tells us that $f \in \mathscr{O}[x]$, which means that β is integral. □

We now prove that an extension of a valuation in an algebraic extension of a complete field exists and is unique.

THEOREM 5.4.7. *Let $(K, |\ |_K)$ be a complete valuation field, and let L be an algebraic extension of K. Then there is a unique extension of $|\ |_K$ to a valuation $|\ |_L$ on L. The valuation $|\ |_L$ is nonarchimedean if and only if $|\ |_K$ is. If L/K is finite, then L is complete with respect to $|\ |_L$, and this extension satisfies*

$$|\beta|_L = |N_{L/K}(\beta)|_K^{1/[L:K]}.$$

PROOF. If the valuation on K is archimedean, then by Theorem 5.3.16, we have that $(K, |\ |)$ is isomorphic to $(\mathbb{R}, |\ |^s)$ or $(\mathbb{C}, |\ |^s)$ with $s \in (0, 1]$, and the only extension of $|\ |^s$ on $\mathbb{R}$ to $\mathbb{C}$ is $|\ |^s$.

So, suppose that the valuation on K is nonarchimedean. First, we note that it suffices to assume that the degree of L/K is finite, as any algebraic extension is the union of its finite subextensions. Let $n = [L : K]$, and for $\beta \in L$, define

$$|\beta|_L = |N_{L/K}(\beta)|_K^{1/n}.$$

Clearly, $|\beta|_L = 0$ if and only if $\beta = 0$, and $|\alpha\beta|_L = |\alpha|_L|\beta|_L$ for $\alpha, \beta \in L$.

Let A be the valuation ring of K, and let B be the integral closure of A in L. Let $\alpha \in L$. We obviously have $\alpha \in B$ if and only if $\alpha + 1 \in B$. By Corollary 5.4.6, this tells us that $N_{L/K}(\alpha) \in A$ if and only if $N_{L/K}(\alpha + 1) \in A$, which says that by definition that $|\alpha|_L \leq 1$ if and only if $|\alpha + 1|_L \leq 1$. If $\beta \in L^\times$ with (without loss of generality), $|\alpha|_L \leq |\beta|_L$, then $|\alpha\beta^{-1}|_L \leq 1$, so

$$|\alpha + \beta|_L = |\beta|_L|\alpha\beta^{-1} + 1|_L \leq |\beta|_L = \max(|\alpha|_L, |\beta|_L).$$

Hence $|\ |_L$ is a nonarchimedean valuation, and it clearly extends $|\ |_K$. Moreover, L is complete with respect to this valuation by Proposition 5.4.3.

If $\|\ \|$ is any other valuation on L extending that on K, then let us let C be its valuation ring and $\mathfrak{n}$ be its maximal ideal. Note that the norm of any element of C lies in A, so $C \subseteq B$. Suppose that $\gamma \in B - C$. Let f be the minimal polynomial of γ over A, so $f \in A[x]$. Moreover, $\gamma^{-1} \in \mathfrak{n}$ since C is a valuation ring. But then $-1 = \gamma^{-\deg f} f(\gamma) - 1$ is an A-linear polynomial in γ^{-1} with no constant coefficient that therefore lies in $\mathfrak{n}$, a contradiction. That is, $B = C$. By Proposition 5.2.5, we have that $\|\ \|$ and $|\ |_L$ are equivalent. □

We have the following immediate corollary of the definition of the extended valuation in Theorem 5.4.7.

COROLLARY 5.4.8. *Let K be a complete discrete valuation field, and let L be an finite extension of K. Then the extension to L of the valuation on K is discrete.*

Let us consider the specific case of global fields.

PROPOSITION 5.4.9. *The places of a global field are exactly its finite and infinite places.*

PROOF. Let K be a global field. Theorem 5.3.16 tells us that any archimedean prime on L must arise from a real or complex embedding of L, so represents an infinite place. So, suppose $|\ \ |$ is a nonarchimedean valuation of K and note that its restriction to $\mathbb{Q}$ in the case that K has characterstic 0 or $\mathbb{F}_\ell(t)$ in the case that K has characteristic a prime ℓ must be equivalent to $|\ \ |_p$ for some prime p in the former case and to either $|\ \ |_f$ for some irreducible $f \in \mathbb{F}_\ell(t)$ or $|\ \ |_\infty$ in the latter case. So, if the latter restriction yields a finite place, coming from a finite prime $\mathfrak{p}$, consider $\mathfrak{P} = \{x \in \mathscr{O}_K \mid |x| < 1\}$, and otherwise consider $\mathfrak{P} = \{x \in A \mid |x| < 1\}$, where A is the integral closure of $\mathbb{F}_\ell[t^{-1}]$ in K. Then $\mathfrak{P}$ is a prime lying over $\mathfrak{p} = (p)$, (f), or (t^{-1}) in the respective cases. Note that the valuation $|\ \ |_\mathfrak{p}$ extends uniquely to the completion of $\mathbb{Q}$ or $\mathbb{F}_\ell(t)$ at $\mathfrak{p}$ by continuity and then to a valuation on $K_\mathfrak{P}$ that is equivalent to $|\ \ |_\mathfrak{P}$ by Theorem 5.4.7. But then the latter valuation is equivalent to $|\ \ |$ by uniqueness of the extension, as desired. □

We mention in passing the useful notion of a Newton polygon, as it relates to Lemma 5.4.4.

DEFINITION 5.4.10. Let K be a complete nonarchimedean valuation field with additive valuation v, and let $f = \sum_{i=0}^n a_i x^i \in K[x]$ with $a_n \neq 0$. The *Newton polygon* of f is the lower convex hull of the points $(i, v(a_i))$.

We omit the proof of the following.

PROPOSITION 5.4.11. *Let K be a complete nonarchimedean valuation field with additive valuation v, and let $f = \sum_{i=0}^n a_i x^i \in K[x]$ with $a_n \neq 0$. Let $-\infty \leq m_1 < m_2 < \ldots < m_r$ be the slopes of the line segments of the Newton polygon of f, and let $t_1, \ldots, t_r$ be their respective horizontal lengths. Then for each j with $1 \leq j \leq r$, the polynomial f has exactly t_j roots in an algebraic closure of K with valuation $-m_j$ under the extension of v.*

PROOF. Let $\mu_1 < \cdots < \mu_s$ be the valuations of the roots of f, and let k_i be the number of roots of valuation μ_i for $1 \leq i \leq s$. For such i, set $\ell_i = \sum_{t=1}^i k_t$, and set $\ell_0 = 0$.

Label the roots of f with multiplicity $\alpha_1, \ldots, \alpha_n$ in order of increasing valuation. Since a_{n-j} for $0 \leq j \leq n$ is, up to sign, the sum of all products of j distinct roots of f, its additive valuation is at least that of $\alpha_1 \cdots \alpha_j$. The latter valuation will be less than all other valuations of products of j distinct roots if and only if $j = \ell_i$ for some $1 \leq i \leq s$. In other words, if $\ell_{i-1} < j \leq \ell_i$, then

$$v(a_{n-j}) \geq \sum_{t=1}^{i-1} k_t \mu_t + (j - \ell_{i-1})\mu_i,$$

with equality guaranteed if $j = \ell_i$. It then follows that the lower convex hull of the Newton polygon consists of the line segments between the points $(n-\ell_{s-i}, \sum_{t=1}^{s-i} k_t\mu_t)$ for $0 \leq i \leq s$. It follows then that $r = s$, and the ith line segment has length

$$t_i = (n-\ell_{s-i-1}) - (n-\ell_{s-i}) = \ell_{s-i} - \ell_{s-i-1} = k_{s-i}$$

and slope

$$m_i = \frac{\sum_{t=1}^{s-i-1} k_t\mu_t - \sum_{t=1}^{s-i} k_t\mu_t}{t_i} = \frac{-k_{s-i}\mu_{s-i}}{k_{s-i}} = -\mu_{s-i}.$$

□

EXAMPLE 5.4.12. Consider the polynomial $f = 8x^4 + 30x^3 - 4x^2 + 7x - 2 \in \mathbb{Q}_2[x]$. Its Newton polygon is the lower convex hull of the points $(0,3)$, $(1,1)$, $(2,2)$, $(3,0)$, and $(4,1)$, which means the area above the piecewise linear function on $[0,4]$ consisting of the three line segments between the points $(0,3)$, $(1,1)$, $(3,0)$, and $(4,1)$. The line segments have lengths 1, 2, and 1 and slopes -2, $-\frac{1}{2}$, and 1, respectively, so f has one root of 2-adic valuation 2, two roots of valuation $\frac{1}{2}$, and one root of valuation -1.

EXAMPLE 5.4.13. For $n \geq 1$ and a prime number p, the function $x^n - p \in \mathbb{Q}_p[x]$ has a Newton polygon with lower boundary the single line segment from $(0,1)$ to $(n,0)$ of length n and slope $-\frac{1}{n}$. Thus, $x^n - p$ has n roots of p-adic valuation $\frac{1}{n}$ in an algebraic closure of $\mathbb{Q}_p$, and these are of course $\zeta_n^i \sqrt[n]{p}$ for $0 \leq i < n$, where ζ_n is a primitive nth root of unity.

We provide some useful corollaries.

COROLLARY 5.4.14. *In the notation of Proposition 5.4.11, the polynomial f factors as $f = f_1 \dots f_r$, where $f_i \in K[x]$ has degree t_i and the valuations of its roots are all $-m_i$.*

PROOF. By uniqueness of the extension v of the valuation on K to the splitting field field L of K, we have that $v \circ \sigma = v$ for any $\sigma \in \mathrm{Gal}(L/K)$. Therefore, any two roots of an irreducible factor of f must have the same valuation, hence the corollary. □

COROLLARY 5.4.15. *Suppose that K is a complete discrete valuation field with corresponding discrete additive valuation v. If $f \in K[x]$ is monic of degree n and has a Newton polygon with lower boundary a single line segment of slope $-\frac{c}{n}$, where $c \geq 1$ is relatively prime to n, then f is irreducible.*

PROOF. Let α be a root of f in an algebraic closure of K. Since n is the minimal integer such that $nv(\alpha) \in \mathbb{Z}$, we have that $\alpha^j \notin K$ for $1 \leq j < n$, and therefore L/K has degree n. □

This gives a less-standard proof of the following well-known result.

COROLLARY 5.4.16. *Let K be a global field, and let $f \in K[x]$ be an Eisenstein polynomial for a nonarchimedean prime $\mathfrak{p}$ of K. Then f is irreducible. Moreover, the prime $\mathfrak{p}$ is totally ramified in the extension of K generated by a root of f.*

PROOF. Suppose that f is Eisenstein for $\mathfrak{p}$, and consider the completion $K_\mathfrak{p}$ of K at $\mathfrak{p}$. Then f is still Eisenstein for the ideal generated by $\mathfrak{p}$ in the valuation ring of $K_\mathfrak{p}$, and therefore irreducible by the previous corollary. Since f is irreducible over $K_\mathfrak{p}$, it is irreducible in $K[x]$. The last statement follows as every root of f has valuation $\frac{1}{n}$, as in the proof of Corollary 5.4.15. □

5.5. Local fields

DEFINITION 5.5.1. A Hausdorff topological space X is *locally compact* if for every $x \in X$, there exists an open neighborhood U_x of x such that the closure of U_x is compact.

Let us make the following definition.

DEFINITION 5.5.2. A *local field* is a valuation field that is locally compact with respect to the topology defined by the valuation.

LEMMA 5.5.3. *Local fields are complete valuation fields.*

PROOF. Let $(K, |\ \ |)$ be a local field. Let $\varepsilon > 0$ be such that the closed ball of radius ε around 0 is compact, and note that by translation this applies to balls around every point. If $(a_n)_n$ is a Cauchy sequence in K, then of course there exists $N > 0$ such that $|a_n - a_N| < \varepsilon$ for all $n \geq N$. Therefore all a_n with $n \geq N$ lie in a compact set, and the Cauchy sequence $(a_n)_{n \geq N}$ has a limit. □

REMARK 5.5.4. If K is an archimedean local field, then being that it is complete, Theorem 5.3.16 tells us that K is isomorphic to $\mathbb{R}$ or $\mathbb{C}$, and the resulting valuation on $\mathbb{R}$ or $\mathbb{C}$ is equivalent to the standard absolute value.

REMARK 5.5.5. The term "local field" is often used to refer more specifically only to nonarchimedean local fields.

The definition we have given for a local field may not be that most familiar to algebraic number theorists, so let us work to classify such fields.

PROPOSITION 5.5.6. *Let K be a complete discrete valuation field with valuation ring $\mathscr{O}$ and maximal ideal $\mathfrak{m}$. The following are equivalent:*

i. K is a local field,

ii. $\mathscr{O}$ is compact, and

iii. $\mathscr{O}/\mathfrak{m}$ is finite.

PROOF. Let π be a unfiormizer of $\mathscr{O}$. If K is locally compact, then $\mathfrak{m}^n$, being an open and closed neighborhood of 0 in $\mathscr{O}$, must be compact for some $n \geq 0$. On the other hand, the map $\mathscr{O} \to \mathfrak{m}^n$ given by multiplication by π^n is a homeomorphism, since it is continuous with an apparent continuous inverse. So (i) implies (ii). Conversely, (ii) implies (i) since the neighborhood $a + \mathscr{O}$ of any $a \in K$ will be compact if $\mathscr{O}$ is.

If $\mathscr{O}$ is compact, then since $\mathscr{O}$ is the disjoint union of its open subsets $a+\mathfrak{m}$ for a in a set of coset representatives of $\mathscr{O}/\mathfrak{m}$, we have that the number of such representatives must be finite, so (ii) implies (iii). Conversely, if $\mathscr{O}/\mathfrak{m}$ is finite, then there exists a finite set T of coset representatives of it in $\mathscr{O}$. Suppose we have a sequence $(\alpha_n)_n$ in $\mathscr{O}$, which we write for each n as

$$\alpha_n = \sum_{i=0}^{\infty} a_{n,i}\pi^i$$

for some $a_{n,i} \in T$ for all $i \geq 0$. Among the coefficients $a_{n,0}$, some element of T must occur infinitely many times, so we may choose a subsequence $(\alpha_{k_{n,0}})_n$ of $(\alpha_n)_n$ such that the $a_{k_{n,0},0}$ are all constant. We then repeat, choosing a subsequence $(\alpha_{k_{n,1}})_n$ of $(\alpha_{k_{n,0}})_n$ such that the $a_{k_{n,1},1}$ are all constant, and so forth. Then the subsequence $(\alpha_{k_{n,n}})_n$ of α_n converges to

$$\sum_{i=0}^{\infty} a_{k_{i,i},i}\pi^i.$$

Therefore, $\mathscr{O}$ is a sequentially compact metric space, and so it is compact. □

PROPOSITION 5.5.7 (Krasner's Lemma). *Let K be a complete nonarchimedean valuation field. We use $|\ \ |$ denote the unique extension of the valuation on K to an algebraic closure $\overline{K}$ of K. Let $\alpha, \beta \in \overline{K}$. If α is separable over $K(\beta)$ and*

$$|\beta - \alpha| < |\sigma(\alpha) - \alpha|$$

for every embedding $\sigma\colon K(\alpha) \hookrightarrow \overline{K}$ fixing K but not α, then $K(\alpha) \subseteq K(\beta)$.

PROOF. We must show that $K(\alpha,\beta) = K(\beta)$. So let $\sigma\colon K(\alpha,\beta) \hookrightarrow \overline{K}$ be a field embedding fixing $K(\beta)$. We have

$$|\sigma(\alpha) - \beta| = |\sigma(\alpha) - \sigma(\beta)| = |\alpha - \beta|,$$

the latter equality by the uniqueness of the extension, so

$$|\sigma(\alpha) - \alpha| = |\sigma(\alpha) - \beta + \beta - \alpha| \leq \max(|\sigma(\alpha) - \beta|, |\beta - \alpha|) = |\beta - \alpha|.$$

By assumption, this forces σ to fix $K(\alpha)$, hence the result. □

We can derive the following from Krasner's lemma.

PROPOSITION 5.5.8. *Let K be a complete nonarchimedean valuation field with valuation ring $\mathscr{O}$. Let $f \in \mathscr{O}[x]$ be monic, irreducible, and separable of degree $n \geq 1$. There exists an ideal $\mathfrak{a}$ of $\mathscr{O}$ such that if $g \in \mathscr{O}[x]$ is monic of $\deg g = n$ and satisfies $f \equiv g \bmod \mathfrak{a}\mathscr{O}[x]$, and if β is a root of g in an algebraic closure $\overline{K}$ of K, then f has a root α in $\overline{K}$ such that $K(\alpha) = K(\beta)$. In particular, any such g is irreducible.*

PROOF. Write $f = \sum_{i=0}^{n} a_i x^i$ and $g = \sum_{i=0}^{n} b_i x^i$. Our assumption is that for some positive $\delta < 1$, we have $|a_i - b_i| \leq \delta$ for all $0 \leq i \leq n$, where $|\ \ |$ is the valuation on K (and its unique extension to $\overline{K}$). By choosing δ small enough, we may insure that either $|a_i| = |b_i|$ or $|b_i| \leq \delta$ (if $a_i = 0$ or $b_i = 0$) for each i. So, there exists $C > 0$ with $|b_i| \leq C$ independent of the choice of g. If β is a root of g, then

$$|\beta|^n \leq \max\{|b_i||\beta|^i \mid 0 \leq i < n\} \leq C\max\{1, |\beta|^{n-1}\},$$

so $|\beta|$ is bounded independent of g, say by D, which we take to be ≥ 1. We then have

$$|f(\beta)| = |f(\beta) - g(\beta)| \leq \max\{|a_i - b_i||\beta|^i \mid 0 \leq i < n\} \leq \delta \max\{1, |\beta|\}^{n-1} \leq \delta D^{n-1},$$

and so by choosing δ sufficiently small, we may make $|f(\beta)|$ arbitrarily small, independent of β, say less than ε^n for some $\varepsilon > 0$. Note that

$$|f(\beta)| = \prod_{i=1}^{n} |\beta - \alpha_i| < \varepsilon^n,$$

where $\alpha_1, \ldots, \alpha_n$ are the roots of f. One must then have $|\beta - \alpha_i| < \varepsilon$ for some i. If we take δ, and hence ε, small enough so that $\varepsilon < |\alpha_i - \alpha_j|$ for all $j \neq i$, and Krasner's lemma tells us that $K(\alpha_i) \subseteq K(\beta)$, which tells us that g is irreducible and $K(\alpha_i) = K(\beta)$. □

THEOREM 5.5.9. *The following are equivalent for a nonarchimedean valuation field K:*

i. K is a local field,

ii. K is complete, the valuation on K is discrete, and the residue field of K is finite,

iii. K is isomorphic to a completion of a global field, and

iv. K is isomorphic to a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p(\!(t)\!)$ for some prime p.

PROOF. That (ii) implies (i) is part of Proposition 5.5.6. That (iii) implies (ii) is a consequence of Proposition 5.3.12 and Lemma 5.3.17.

Suppose that (iv) holds. Suppose that K is a finite extension of $\mathbb{Q}_p$ for some prime p. Then $K = \mathbb{Q}_p(\alpha)$ for some $\alpha \in K$, and let f be its minimal polynomial. Choose $g \in \mathbb{Q}[x]$ monic of degree that of f and sufficiently close to f so that we may apply Proposition 5.5.8 to see that g is irreducible over $\mathbb{Q}_p$, so $\mathbb{Q}_p(\beta) = \mathbb{Q}_p(\alpha)$ for some root β of g. Since β is algebraic over $\mathbb{Q}$, we have that $K = \mathbb{Q}_p(\beta)$ is the completion of $\mathbb{Q}(\beta)$ in K. Similarly, if K is a finite extension of $\mathbb{F}_p(\!(t)\!)$, then it is a finite, separable extension of $\mathbb{F}_p(\!(t^{1/p^k})\!)$ for some $k \geq 1$, which is itself isomorphic to $\mathbb{F}_p(\!(t)\!)$. Hence, we may assume that $K = \mathbb{F}_p(\!(t)\!)(\alpha)$ for some $\alpha \in K$, and the above argument with $\mathbb{F}_p(\!(t)\!)$ replacing $\mathbb{Q}_p$ yields (iii).

To see that (i) implies (iv), suppose that K is a local field with residue field of characteristic a prime p. If K has characteristic 0, then the restriction of the valuation to $\mathbb{Q}$ cannot be trivial as it would otherwise extend to the trivial valuation on K by Theorem 6.1.4. It must therefore be a nonarchimedean valuation on $\mathbb{Q}$ with residue characteristic p, and Theorem 5.2.31 tells us that this valuation is equivalent to the p-adic valuation. But then the completion $\mathbb{Q}_p$ embeds canonically into

K, so K is an extension of $\mathbb{Q}_p$. If K has characteristic p, then it cannot be an algebraic extension of $\mathbb{F}_p$ since the valuation is nontrivial, so it must contain an element T that is transcendental over $\mathbb{F}_p$. We have that K is an extension of $\mathbb{F}_p(T)$, and by Proposition 5.2.32, the restriction of the valuation on K to $\mathbb{F}_p(T)$ is the f-adic valuation for some irreducible $f \in \mathbb{F}_p[T]$ or the ∞-adic valuation. The completion of $\mathbb{F}_p(T)$ with respect to this valuation is isomorphic to $\mathbb{F}_q(\!(t)\!)$ for some q and embeds in K, and the valuation on K is the unique extension of this valuation to K.

Next, suppose that K/F with $F = \mathbb{Q}_p$ or $\mathbb{F}_p(\!(t)\!)$ were an infinite extension. If K contains a transcendental element x over F, then since the residue field of K is finite, x is still transcendental over the largest extension E of F in K in which the valuation of F is unramified. By Theorem 2.5.11, the field extensions $E(x)/E(x^n)$ all have ramification index n at the unique prime of the valuation ring of $E(x)$. Let $h < 1$ be the valuation of a uniformizer of $E(x) \subseteq K$ under the unique extension of the valuation on F to $E(x)$. Then the valuation of a uniformizer of $E(x^n)$ is h^n. Since the valuation of a uniformizer of E is then less than h^n for all n, it must be 0, which is impossible (in fact, it is p^{-1}).

If K/F is algebraic, we can let $(K_n)_n$ be an infinite tower of distinct subfields of K with union equal to K. As K is a local field, its residue field is finite by Proposition 5.5.6. Therefore, the extension of residue fields for K_{n+1}/K_n is trivial for sufficiently large n. Since there is only one nonzero valuation on K_{n+1} extending that of K_n, the degree formula then tells us that the ramification degree of the prime of the valuation ring is $[K_{n+1} : K_n]$, and in particular nontrivial. Consider any sequence $(\pi_n)_n$, with $\pi_n \in K_n$ a uniformizer for each n. If $|\ \ |$ is the valuation on K, then we have that $|\pi_n - \pi_m| = |\pi_n|$ for $n > m$, with n sufficiently large (independent of the choice of m). But $|\pi_n|$ has a limit of 1 as n increases (as follows from Theorem 5.4.7), which means that the sequence $(\pi_n)_n$ has no convergent subsequence. Therefore K is not compact, and therefore the extension had to be finite. □

DEFINITION 5.5.10. A *p-adic field*, or *p-adic local field*, is a finite extension of $\mathbb{Q}_p$ for some prime p.

DEFINITION 5.5.11. A *Laurent series field* (over a finite field) is a finite extension of $\mathbb{F}_p(\!(t)\!)$.

REMARK 5.5.12. In fact, every finite extension K of $\mathbb{F}_p(\!(t)\!)$ is isomorphic to $\mathbb{F}_q(\!(y)\!)$ for some power q of p under a map that takes a uniformizer of K to y.

CHAPTER 6

Ramification theory

6.1. Semi-local theory

NOTATION 6.1.1. We often use a subscript v to denote a valuation $|\ \ |_v$ on a field K, even when that valuation is archimedean. When $|\ \ |_v$ is nonarchimedean, v also denotes an additive valuation corresponding to v, and when it is discrete, the additive valuation is chosen to have image $\mathbb{Z}\cup\{\infty\}$.

NOTATION 6.1.2. We let K_v denote the completion of K with respect to a valuation denoted $|\ \ |_v$.

REMARK 6.1.3. Let A be a Dedekind domain and $\mathfrak{p}$ a prime ideal of A. Let $|\ \ |_\mathfrak{p}$ be a valuation on the quotient field K of A such that $|a|_\mathfrak{p} = c^{-v_\mathfrak{p}(a)}$ for some $c \in \mathbb{R}_{>1}$ and all $a \in K^\times$. Then we may speak of the completion $K_\mathfrak{p}$ of K with respect to this valuation.

The following theorem explores extensions of valuations in the case that the ground field is not complete. In this case, uniqueness of the extension need not hold, but we can classify the distinct extensions.

THEOREM 6.1.4. *Let K be a field and v a valuation on K. Let $\bar{v}$ be an extension of v to a valuation on an algebraic closure $\overline{K_v}$ of K_v. Let L be an algebraic extension of K. For any extension of v to a valuation w on L, there exists an embedding $\tau\colon L \to \overline{K_v}$ fixing K such that $w = \bar{v}\circ\tau$, by which we mean that*

$$|\beta|_w = |\tau(\beta)|_{\bar{v}}$$

for all $\beta \in L$. If $\tau'\colon L \to \overline{K_v}$ is another embedding fixing K, then $w' = \bar{v}\circ\tau'$ is equal to w if and only if τ and τ' are conjugate over K_v: i.e., $\tau' = \sigma\circ\tau$ for some automorphism σ of $\overline{K_v}$ fixing K_v.

PROOF. The valuation that w induces on the completion L_w can only be the unique valuation extending the valuation that v induces on K_v. If $\tau\colon L_w \to \overline{K_v}$ is any field embedding fixing K_v, then $\bar{v}\circ\tau$ is a valuation on L_w that extends v on K_v, and hence it must be w.

For the second statement, suppose first that $\tau' = \sigma\circ\tau$ with $\sigma \in \mathrm{Aut}_{K_v}(\overline{K_v})$. Again, $\bar{v}$ is the unique valuation on $\overline{K_v}$ extending the valuation on K_v, so $\bar{v}\circ\sigma = \bar{v}$. But then we have $\bar{v}\circ\tau' = \bar{v}\circ\tau$, and restricting to L, this means that $w' = w$.

Conversely, suppose that $w' = w$. Note that $\tau'\circ\tau^{-1}\colon \tau(L) \to \tau'(L)$ is an isomorphism fixing K. Suppose that L/K is finite. As K is dense in K_v and $\tau(L)$ is also a finite extension of K, we have that $\tau(L)$ is dense in $\tau(L)\cdot K_v$ (and similarly for τ'). Define

$$\sigma\colon\ \tau(L)\cdot K_v \to \tau'(L)\cdot K_v$$

by

$$\sigma(\alpha) = \lim_{n\to\infty} \tau'(\alpha_n)$$

for $\alpha \in \tau(L)\cdot K_v$, choosing a sequence $(\alpha_n)_n$ of elements of L such that $(\tau(\alpha_n))_n$ converges to α. Note that this is independent of choice, as if α_n' is another such sequence, then the limits of $(\tau'(\alpha_n))_n$ and $(\tau'(\alpha_n'))_n$ are the same by continuity of τ'. But then $\tau' = \sigma\circ\tau$, and σ is the unique isomorphism fixing K_v with this property. We then extend σ to an element of $\mathrm{Aut}_{K_v}(\overline{K_v})$, obtaining the desired map.

In general, L is a union of finite extensions E of K. For each such E, we have defined a unique isomorphism $\sigma_E\colon \tau(E)K_v \to \tau'(E)K_v$ such that $\tau'|_E = \sigma_E\circ\tau|_E$. If E and E' are two finite extensions of K in L, then σ_E and $\sigma_{E'}$ agree on $\tau(E\cap E')K_v \subseteq \tau(E)K_v \cap \tau(E')K_v$ by uniqueness. Together, the collection of maps σ_E defines an embedding of the compositum of the fields $\tau(E)K_v$ into $\overline{K_v}$. We then extend this embedding to an automorphism of $\overline{K_v}$ fixing K_v, and by definition, it has the property that $\tau' = \sigma\circ\tau$. □

NOTATION 6.1.5. If L/K is an extension of fields, v is a valuation on K, and w is a valuation on L, then we write $w \mid v$ to denote that w is equivalent to an extension of v. The set of $w \mid v$ will mean a set of representatives of the equivalence classes of the extensions of v to L.

The following is in essence a consequence of Proposition 1.1.1.

PROPOSITION 6.1.6. *Let L/K be a finite separable extension of fields and v a valuation on K. Then there is an isomorphism*

$$\kappa\colon L\otimes_K K_v \xrightarrow{\sim} \prod_{w\mid v} L_w$$

such that $\kappa(\beta\otimes 1) = (\iota_w\beta)_w$ for all $\beta\in L$, where $\iota_w\colon L\to L_w$ is the canonical embedding of a field in its completion.

PROOF. As L/K is finite and separable, there exists an element $\theta\in L$ such that $L = K(\theta)$. Let f be the minimal polynomial of θ over K, and let $f = \prod_{i=1}^m f_i$ over K_v, where the f_i are irreducible (and necessarily distinct by separability of f). Choose a root θ_i of $f_i(x)$ for each i inside a fixed algebraic closure $\overline{K_v}$ of K. Proposition 1.1.1 provides an isomorphism

$$L\otimes_K K_v \xrightarrow{\sim} \prod_{i=1}^m K_v(\theta_i)$$

such that $\theta\otimes 1$ is sent to θ_i in the ith coordinate. By Theorem 5.4.7, the field $K_v(\theta_i)$ is necessarily complete with respect to a valuation w_i extending v. The embedding $\tau_i\colon L\to K_v(\theta_i)$ sending θ to θ_i and fixing K has dense image, so $K_v(\theta_i)$ is isomorphic to the completion of L with respect to w_i.

If w is any valuation on L extending v, then Theorem 6.1.4 yields an embedding τ of L into $\overline{K_v}$ such that $w = \bar{v}\circ\tau$, where $\bar{v}$ is the unique extension of v from K_v to $\overline{K_v}$. Then $\tau(\theta)$ is the root of f_i for some i, so there exists an automorphism σ over $\overline{K_v}$ fixing K_v such that $\tau = \sigma\circ\tau_i$ and therefore $w = \bar{v}\circ\sigma\circ\tau_i = \bar{v}\circ\tau_i = w_i$. □

COROLLARY 6.1.7. *Let L/K be a finite separable extension of fields and v a valuation on K. Then we have*

$$[L:K] = \sum_{w|v} [L_w : K_v].$$

We can get more out of Proposition 6.1.6, which we will use later.

DEFINITION 6.1.8. Let L/K be a finite separable extension of fields and v a valuation on K.

a. The *norm map* for L/K at v is the map

$$N_{L/K}^v \colon \prod_{w|v} L_w \to K_v$$

given by

$$N_{L/K}^v((\beta_w)_w) = \prod_{w|v} N_{L_w/K_v}(\beta_w).$$

b. The *trace map* for L/K at v is the map

$$\mathrm{Tr}_{L/K}^v \colon \prod_{w|v} L_w \to K_v$$

given by

$$\mathrm{Tr}_{L/K}^v((\beta_w)_w) = \sum_{w|v} \mathrm{Tr}_{L_w/K_v}(\beta_w).$$

When v is understood, these are denoted more simply by $N_{L/K}$ and $\mathrm{Tr}_{L/K}$.

We have the following, which says that $N_{L/K}^v$ and $N_{L/K}$ coincide on L (using its natural embedding in each L_w), and similarly for trace maps.

PROPOSITION 6.1.9. *Let L/K be a finite separable extension of fields, and let v be a valuation on K. For $\beta \in L$, we may view it as an element of L_w for each $w \mid v$, and as elements of K_v, we have*

$$N_{L/K}(\beta) = \prod_{w|v} N_{L_w/K_v}(\beta) \quad \text{and} \quad \mathrm{Tr}_{L/K}(\beta) = \sum_{w|v} \mathrm{Tr}_{L_w/K_v}(\beta).$$

PROOF. Let $m_\beta : L \to L$ be left multiplication. This indues a K_v-linear transformation $m_\beta \otimes \mathrm{id}_{K_v}$ on K_v, and the characteristic polynomials of m_β and $m_\beta \otimes \mathrm{id}_{K_v}$ agree. Noting that the isomorphism of Proposition 6.1.6 is one of L-vector spaces, the characteristic polynomial of $m_\beta \otimes \mathrm{id}_{K_v}$ coincides with the product of the characteristic polynomials of multiplication by β on the L_w for $w \mid v$. The result is then a consequence of Proposition 1.3.3. □

The following result on valuation rings will later be useful to us.

PROPOSITION 6.1.10. *Let L/K be a finite separable extension of fields and v a discrete valuation on K. Suppose that $(\beta_1, \ldots, \beta_n)$ is an ordered basis for L/K such that $|\beta_i|_w \leq 1$ for all $1 \leq i \leq n$ and*

places w of L lying over v, and $|\mathrm{D}(\beta_1,\dots,\beta_n)|_v = 1$. Then the isomorphism

$$\kappa\colon L\otimes_K K_v \xrightarrow{\sim} \prod_{w|v} L_w$$

of Proposition 6.1.6 restricts to an isomorphism

$$\kappa'\colon \bigoplus_{i=1}^{n} \mathscr{O}_v(\beta_i\otimes 1) \xrightarrow{\sim} \prod_{w|v} \mathscr{O}_w,$$

where $\mathscr{O}_v$ (resp., $\mathscr{O}_w$) denotes the valuation ring of K_v (resp., L_w).

PROOF. First, we note that both the domain and codomain of κ' are free $\mathscr{O}_v$-modules of rank $n = [L:K]$. Moreover, κ is injective, so it suffices to show that κ' is surjective. For this, note that the trace pairing $\psi\colon L\times L\to K$ given by

$$\psi(\alpha,\beta) = \mathrm{Tr}_{L/K}(\alpha\beta)$$

extends to a unique K_v-bilinear pairing

$$\psi_v\colon (L\otimes_K K_v)\times(L\otimes_K K_v)\to K_v,$$

which is given on simple tensors by the equation

$$\psi_v(\alpha\otimes a,\beta\otimes b) = ab\,\mathrm{Tr}_{L/K}(\alpha\beta).$$

Let $w_1,\dots,w_g$ be the places of L lying over v. Since $\mathscr{O}_v$ is a PID, each valuation ring $\mathscr{O}_{w_i}$ is a free $\mathscr{O}_v$-module of rank $n_i = [L_{w_i}:K_v]$. So, for $1\le i\le g$, let

$$m_i = \sum_{j=1}^{i-1} n_i,$$

and let $(\lambda_{m_i+1},\dots,\lambda_{m_{i+1}})$ be an ordered basis of $\mathscr{O}_{w_i}$ as a free $\mathscr{O}_v$-module. We view each λ_i as sitting in the product $\prod_{i=1}^g \mathscr{O}_{w_i}$ by taking the other coordinates to be zero. Let $A = (a_{i,j}) \in \mathrm{GL}_n(K_v)$ be the matrix such that

$$\lambda_i = \sum_{j=1}^{n} \kappa(\beta_j\otimes a_{i,j}), \tag{6.1.1}$$

for each $1\le i\le n$. We must show that A has entries in $\mathscr{O}_v$.

Via κ, the pairing ψ_v gives rise to a pairing

$$\tilde{\psi}\colon \prod_{i=1}^{g} L_{w_i}\times\prod_{i=1}^{g} L_{w_i}\to K_v$$

that is given on the basis $(\lambda_1, \dots, \lambda_n)$ by

$$\begin{aligned}\tilde{\psi}(\lambda_i, \lambda_j) &= \psi_v(\kappa^{-1}(\lambda_i), \kappa^{-1}(\lambda_j)) \\ &= \sum_{k=1}^{n} \sum_{l=1}^{n} \psi_v(\beta_k \otimes a_{i,k}, \beta_l \otimes a_{j,l}) \\ &= \sum_{k=1}^{n} a_{i,k} \sum_{l=1}^{n} a_{j,l} \operatorname{Tr}_{L/K}(\beta_k \beta_l) \\ &= \sum_{k=1}^{n} a_{i,k} \sum_{l=1}^{n} a_{j,l} \sum_{h=1}^{g} \operatorname{Tr}_{L_{w_h}/K_v}(\beta_k \beta_l) \\ &= \operatorname{Tr}^v_{L/K}(\lambda_i \lambda_j).\end{aligned}$$

Here, of course, we have applied Proposition 6.1.9.

Note that $\lambda_i \lambda_j$ has nontrivial component in L_{w_h} if and only if $m_h + 1 \leq i, j \leq m_{h+1}$. If this is the case, then

$$\tilde{\psi}(\lambda_i, \lambda_j) = \operatorname{Tr}_{L_{w_h}/K_v}(\lambda_i \lambda_j),$$

and otherwise $\tilde{\psi}(\lambda_i, \lambda_j) = 0$. It follows that the matrix $M = (\tilde{\psi}(\lambda_i, \lambda_j))$ is block-diagonal with determinant

$$\prod_{i=1}^{g} \mathrm{D}(\lambda_{m_i+1}, \dots, \lambda_{m_{i+1}}),$$

and this is exactly the discriminant of $\tilde{\psi}$ relative to the basis $(\lambda_1, \dots, \lambda_n)$.

On the other hand, the discriminant of $\tilde{\psi}$ relative to the basis $(\beta_1, \dots, \beta_n)$ is $\mathrm{D}(\beta_1, \dots, \beta_n)$ by definition, and we have by (6.1.1) and Lemma 1.4.6 that

$$\mathrm{D}(\beta_1, \dots, \beta_n) = \det(A)^2 \det(M) = \prod_{i=1}^{g} \mathrm{D}(\lambda_{m_i+1}, \dots, \lambda_{m_{i+1}}).$$

Since $\mathrm{D}(\lambda_{m_i+1}, \dots, \lambda_{m_{i+1}}) \in \mathscr{O}_v^\times$ for each i and $\mathrm{D}(\beta_1, \dots, \beta_n) \in \mathscr{O}_v^\times$ as well, we therefore have $\det(A) \in \mathscr{O}_v^\times$. Since the inverse of A has coefficients in $\mathscr{O}_v$, we therefore have that A does as well. □

Finally, let us treat the special case of valuations on global fields and prove a product formula that generalizes the cases of $\mathbb{Q}$ and $\mathbb{F}_p(t)$ for prime numbers p. The following modification of the complex absolute value is necessary to account for the fact that a complex embedding and its complex conjugate have the same valuation.

NOTATION 6.1.11. Let K be a global field and v a place K. We set

$$\| \ \|_v \colon K_v^\times \to \mathbb{R}_{\geq 0}$$

by $\| \ \|_v = | \ |_v$ if v is not complex, and $\| \ \|_v = | \ |_v^2$ if v is complex.

We have the following consequence of Proposition 6.1.9.

LEMMA 6.1.12. *Let L/K be a finite separable extension of global fields, and let v be a place of K. For $\beta \in L$, we have*

$$\|N_{L/K}(\beta)\|_v = \prod_{w|v} \| \beta\|_w.$$

PROOF. Remark 5.4.2 and the definition of $\| \ \|_v$ tell us that for a place w of L over v, we have

$$\|\alpha\|_w = \|\alpha\|_v^{[L_w:K_v]}$$

for all $\alpha \in K$. Noting Proposition 6.1.9, we then have

$$\|N_{L/K}(\beta)\|_v = \prod_{w|v} \|N_{L_w/K_v}(\beta)\|_v = \prod_{w|v} \|N_{L_w/K_v}(\beta)\|_w^{[L_w:K_v]^{-1}} = \prod_{w|v} \|\beta\|_w.$$

□

THEOREM 6.1.13 (Product formula). *Let K be a global field, and let $\alpha \in K^\times$. Then*

$$\prod_{v \in V_K} \|\alpha\|_v = 1.$$

PROOF. By Propositions 5.2.34 and 5.2.35, we have the result for $\mathbb{Q}$ and $\mathbb{F}_p(t)$ for all primes p. The field K is in the general case a finite extension of exactly one of these fields, which we denote by F. By Lemma 6.1.12, we have

$$\prod_{v \in V_K} \|\alpha\|_v = \prod_{u \in V_F} \prod_{v|u} \|\alpha\|_v = \prod_{u \in V_F} \|N_{K/F}(\alpha)\|_u = 1.$$

□

We make the following definitions.

DEFINITION 6.1.14. Suppose that L/K is a finite separable extension of complete discrete valuation fields.

a. The *ramification index* $e_{L/K}$ of L/K is the additive valuation on L of a uniformizer of K.

b. The *residue degree* $f_{L/K}$ of L/K is the degree of its residue field of L over the residue field of K.

REMARK 6.1.15. In the case that L/K is a finite separable extension of complete discrete valuation fields for which $K = \mathbb{Q}_p$ or $K = \mathbb{F}_p(\!(t)\!)$, we denote $e_{L/K}$ and $f_{L/K}$ by e_L and f_L, respectively.

REMARK 6.1.16. The latter definitions agree with those previously given. That is, let L/K be a finite extension of complete discrete valuation fields. Let $\mathfrak{m}_L$ be the maximal ideal of L and $\mathfrak{m}_K$ that of K. We then have $e_{L/K} = e_{\mathfrak{m}_L/\mathfrak{m}_K}$ and $f_{L/K} = f_{\mathfrak{m}_L/\mathfrak{m}_K}$.

For complete discrete valuation fields, the degree formula is rather simpler than before.

LEMMA 6.1.17. *Let L/K be a finite separable extension of complete discrete valuation fields. We have $[L:K] = e_{L/K} f_{L/K}$.*

PROOF. There is only one nonzero prime ideal in the valuation ring of L, and it lies over the maximal ideal of the valuation ring of K. Theorem 2.5.11 then yields the result. □

DEFINITION 6.1.18. We say that a finite separable extension L/K of complete discrete valuation fields is *unramified*, *ramified*, or *totally ramified* if the maximal ideal of the valuation ring of L/K is inert ($e_{L/K} = 1$), ramified ($e_{L/K} > 1$), or totally ramified ($e_{L/K} = [L:K]$) in the extension, respectively.

We compare these invariants with those defined previously.

PROPOSITION 6.1.19. *Let A be a Dedekind domain with quotient field K, and let B be the integral closure of A in a finite, separable extension L of K. Let $\mathfrak{p}$ be a nonzero prime ideal of A, and let $\mathfrak{P}$ be a prime ideal of B lying over $\mathfrak{p}$. Then $e_{\mathfrak{P}/\mathfrak{p}} = e_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ and $f_{\mathfrak{P}/\mathfrak{p}} = f_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$.*

PROOF. We know that the residue field of K for $\mathfrak{p}$ is isomorphic to the residue field of $K_{\mathfrak{p}}$, and similarly for L and $L_{\mathfrak{P}}$. Therefore, the second equality holds. As for the first, note that the valuation on $K_{\mathfrak{p}}$ (resp., $L_{\mathfrak{P}}$) is just the unique extension of that on K (resp., L). If π_K (resp., π_L) is a uniformizer of $K_{\mathfrak{p}}$ (resp., $L_{\mathfrak{P}}$), and $\mathscr{O}$ is the valuation ring of $L_{\mathfrak{P}}$ then we have

$$\pi_K \mathscr{O} = \mathfrak{p}\mathscr{O} = \mathfrak{P}^{e_{\mathfrak{P}/\mathfrak{p}}} \mathscr{O} = (\pi_L^{e_{\mathfrak{P}/\mathfrak{p}}}),$$

so the ramification index of $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is $v_{\mathfrak{P}}(\pi_K) = e_{\mathfrak{P}/\mathfrak{p}}$. □

DEFINITION 6.1.20. Let K be a field, let L be a Galois extension of K, and let w be a valuation on L. For $\sigma \in \mathrm{Gal}(L/K)$, the *conjugate valuation* $\sigma(w)$ is defined by

$$|\beta|_{\sigma(w)} = |\sigma^{-1}(\beta)|_w$$

for $\beta \in L$.

REMARK 6.1.21. Definition 6.1.20 provides an action of the Galois group of L/K on the set of valuations of L.

REMARK 6.1.22. Suppose that L/K is an extension of global fields. Let v be a valuation on K, and let w be a valuation on L lying over it (i.e., such that $|\ \ |_w$ extends $|\ \ |_v^{[L_w:K_v]}$).

a. If v is the $\mathfrak{p}$-adic valuation of a finite prime $\mathfrak{p}$, then w is the $\mathfrak{P}$-adic valuation of a prime $\mathfrak{P}$ lying over it, and $\sigma(w)$ is just the $\sigma(\mathfrak{P})$-adic valuation. If v is an infinite prime of a finite extension of $\mathbb{F}_p(t)$, then it arises as a prime ideal of the integral closure of $\mathbb{F}_p[t^{-1}]$ in K, and we have the analogous description.

b. If v is an archimedean prime, then v arises from a real or complex embedding τ_v of K, and w arises from an embedding τ_w extending it. We then have $|\beta|_{\sigma(w)} = |\tau_w \circ \sigma^{-1}(\beta)|$, and if τ_w is complex, the complex conjugate embedding $\overline{\tau}_w$ yields the same absolute value.

Given all this, we may speak of decomposition and inertia groups almost as before.

DEFINITION 6.1.23. Let L/K be a Galois extension of fields with Galois group G, and let w be a valuation on L.

a. The *decomposition group* G_w of w is the set of $\sigma \in G$ fixing w.

b. The *inertia group* I_w of w is the set of $\sigma \in G_w$ such that $|\sigma(\beta) - \beta|_w < 1$ for all $\beta \in L$ with $|\beta|_w \leq 1$ if w is nonarchimedean and the decomposition group if w is archimedean.

We leave the following simple check to the reader.

LEMMA 6.1.24. *Let L/K be a Galois extension of fields with Galois group G, and let w be a valuation on L. The inertia group I_w is a normal subgroup of the decomposition group G_w.*

The following is an immediate consequence of Proposition 2.6.14 in the case of discrete valuation fields, but note that the analogous proof goes through in general.

PROPOSITION 6.1.25. *If L/K is a Galois extension of complete nonarchimedean valuation fields, then the decomposition group of the prime of K is all of $G = \mathrm{Gal}(L/K)$, and we have an exact sequence*

$$1 \to I \to G \to \mathrm{Gal}(\kappa(L)/\kappa(K)) \to 1,$$

where I is the inertia group in G and $\kappa(L)$ (resp., $\kappa(K)$) is the residue field of L (resp., K).

For the valuations attached to nonzero prime ideals in Dedekind domains, the decomposition and inertia groups agree with Definitions 2.6.5 and 2.6.15, as seen from the following.

PROPOSITION 6.1.26. *Let L/K be a Galois extension of fields, and let w be a valuation on L extending a valuation v of K. Then the restriction map*

$$\mathrm{Gal}(L_w/K_v) \to \mathrm{Gal}(L/K), \qquad \sigma \mapsto \sigma|_L$$

is an injection with image the decomposition group of w. If w is nonarchimedean, the image of the inertia subgroup of $\mathrm{Gal}(L_w/K_v)$ under this map is the inertia group of w.

PROOF. Note that any $\sigma \in \mathrm{Gal}(L_w/K_v)$ acts continuously on L_w, since $w = \sigma(w)$, as there is a unique valuation on L_w extending the restriction of w to K_v. If $\sigma(\beta) = \beta$ for all $\beta \in L$, then continuity forces $\sigma(\beta) = \beta$ for all $\beta \in L_w$, since L is dense in L_w. So, the restriction map is injective, and its image is by definition contained in the decomposition group G_w of $G = \mathrm{Gal}(L/K)$. Any τ in the decomposition group of w in G satisfies $w = \tau(w)$ on L, so on L_w as well by continuity. Therefore, $\tau\colon L \to L$ is continuous, and its composite with the natural inclusion $L \hookrightarrow L_w$ extends to a unique element of $\mathrm{Gal}(L_w/K_v)$ by continuity, as in Proposition 5.3.12. That is, the image of restriction is G_w.

For w nonarchimedean, it remains to show that the image of the inertia group in $\mathrm{Gal}(L_w/K_v)$ is the inertia group I_w in G. By definition, the image is contained in this group. Let $\tau \in I_w$, and take $\beta \in \mathscr{O}_w$. As L_w is the completion of L, we have $|\beta - b|_w < 1$ for some $b \in L$ with $|b|_w \leq 1$. Set

$\beta' = \beta - b$. Since w is nonarchimedean and $|\tau(b) - b|_w < 1$, we have $|\tau(\beta) - \beta|_w < 1$ if and only if $|\tau(\beta') - \beta'|_w < 1$. But $|\tau(\beta') - \beta'|_w \leq |\beta'|_w < 1$ as $|\tau(\beta')|_w = |\beta'|_w$. Therefore, the extension of τ to an element of $\mathrm{Gal}(L_w/K_v)$ lies in the inertia subgroup. □

6.2. Differents and discriminants

LEMMA 6.2.1. *Let A be a integrally closed domain with quotient field K, let L be a finite separable extension of K, and let B be the integral closure of A in L. Let*

$$\mathfrak{C} = \{\alpha \in L \mid \mathrm{Tr}_{L/K}(\alpha\beta) \in A \text{ for all } \beta \in B\}.$$

Then $\mathfrak{C}$ is a fractional ideal of B.

PROOF. Let $\alpha_1, \ldots, \alpha_n$ be a basis of L as a K-vector space that consists of elements of B. Let $d = \mathrm{D}(\alpha_1, \ldots, \alpha_n)$. By Lemma 1.4.19, we have that $d\mathfrak{C} \subseteq B$, so $\mathfrak{C}$ is a fractional ideal of B. □

Lemma 6.2.1 allows us to make this following definition.

DEFINITION 6.2.2. Let A be a Dedekind domain with quotient field K, let L be a finite separable extension of K, and let B be the integral closure of A in L. The *different* $\mathfrak{D}_{B/A}$ of B over A is the inverse of the fractional ideal

$$\{\alpha \in L \mid \mathrm{Tr}_{L/K}(\alpha\beta) \in A \text{ for all } \beta \in B\}.$$

REMARK 6.2.3. Since L/K is finite separable in Definition 6.2.2, the trace pairing of Example 1.4.4 is nonnegenerate by Proposition 1.4.13. In particular, $\mathfrak{D}_{B/A}$ is well-defined since it is the inverse of a submodule of L.

REMARK 6.2.4. The inverse different $\mathfrak{D}_{B/A}$ of Definition 6.2.2 is the smallest nonzero ideal of B such that

$$\mathrm{Tr}_{L/K}(\mathfrak{D}_{B/A}^{-1}) \subseteq A,$$

and it is a nonzero ideal of B since $\mathfrak{D}_{B/A}^{-1}$ contains B by definition.

LEMMA 6.2.5. *Let A be a Dedekind domain with quotient field K. Let L/K and M/L be finite separable extensions, let B be the integral closure of A in L, and let C be the integral closure of A in M. We then have*

$$\mathfrak{D}_{C/A} = \mathfrak{D}_{C/B} \cdot \mathfrak{D}_{B/A}.$$

PROOF. We have

$$\mathrm{Tr}_{M/K}(\mathfrak{D}_{C/B}^{-1}\mathfrak{D}_{B/A}^{-1}) = \mathrm{Tr}_{L/K}(\mathfrak{D}_{B/A}^{-1}\mathrm{Tr}_{M/L}(\mathfrak{D}_{C/B}^{-1})) \subseteq \mathrm{Tr}_{L/K}(\mathfrak{D}_{B/A}^{-1}) \subseteq A,$$

which implies that $\mathfrak{D}_{C/A} \subseteq \mathfrak{D}_{C/B}\mathfrak{D}_{B/A}$. On the other hand, we may compute

$$\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\mathfrak{D}_{C/A}^{-1})) = \mathrm{Tr}_{M/K}(\mathfrak{D}_{C/A}^{-1}) \subseteq A,$$

so $\mathrm{Tr}_{M/L}(\mathfrak{D}_{C/A}^{-1}) \subset \mathfrak{D}_{B/A}^{-1}$. We therefore have that

$$\mathrm{Tr}_{M/L}(\mathfrak{D}_{B/A}\mathfrak{D}_{C/A}^{-1}) = \mathfrak{D}_{B/A}\,\mathrm{Tr}_{M/L}(\mathfrak{D}_{C/A}^{-1}) \subseteq B,$$

so $\mathfrak{D}_{C/B} \subseteq \mathfrak{D}_{B/A}^{-1}\mathfrak{D}_{C/A}$, which is to say that $\mathfrak{D}_{C/B}\mathfrak{D}_{B/A} \subseteq \mathfrak{D}_{C/A}$. □

LEMMA 6.2.6. *Let A be a Dedekind domain with quotient field K, let L be a finite separable extension of K, let B be the integral closure of A in L. For any multiplicatively closed subset S of A, one has*

$$\mathfrak{D}_{S^{-1}B/S^{-1}A} = S^{-1}\mathfrak{D}_{B/A}.$$

PROOF. Note that

$$\mathrm{Tr}_{L/K}(S^{-1}\mathfrak{D}_{B/A}^{-1}) = S^{-1}\,\mathrm{Tr}_{L/K}(\mathfrak{D}_{B/A}^{-1}) \subseteq S^{-1}B,$$

so $\mathfrak{D}_{S^{-1}B/S^{-1}A} \subseteq S^{-1}\mathfrak{D}_{B/A}$. On the other hand, we have

$$\mathrm{Tr}_{L/K}(\mathfrak{D}_{S^{-1}B/S^{-1}A}) \subseteq S^{-1}B,$$

so for each $\alpha \in \mathfrak{D}_{S^{-1}B/S^{-1}A}^{-1}$, there exists $s \in S$ such that $\mathrm{Tr}_{L/K}(s\alpha) = s\,\mathrm{Tr}_{L/K}(\alpha) \in B$, so $s\alpha \in \mathfrak{D}_{B/A}^{-1}$. Therefore, we have the other containment. □

Somewhat more involved is the following.

LEMMA 6.2.7. *Let A be a Dedekind domain with quotient field K, let L be a finite separable extension of K, let B be the integral closure of A in L. Let $\mathfrak{p}$ be a prime ideal of A, and let $\mathfrak{P}$ be a prime ideal of B lying over it. Let $\mathscr{O}_{\mathfrak{P}}$ (resp., $\mathscr{O}_{\mathfrak{p}}$) denote the valuation ring of $L_{\mathfrak{P}}$ (resp., $K_{\mathfrak{p}}$). Then*

$$\mathfrak{D}_{B/A}\mathscr{O}_{\mathfrak{P}} = \mathfrak{D}_{\mathscr{O}_{\mathfrak{P}}/\mathscr{O}_{\mathfrak{p}}}.$$

PROOF. Let $\alpha \in \mathfrak{D}_{B/A}^{-1}$, and let $\beta \in \mathscr{O}_{\mathfrak{P}}$. We claim that $\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha\beta) \in \mathscr{O}_{\mathfrak{p}}$. Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ be the prime ideals of B lying over $\mathfrak{p}$, taking $\mathfrak{P}_1 = \mathfrak{P}$. For this, let $(\beta_n)_n$ be a sequence in B with limit β in the $\mathfrak{P}$-adic topology and with limit 0 in the $\mathfrak{P}_i$-adic topology for $i \geq 2$, which exists by the Chinese remainder theorem. Since the trace map is continuous, we have

$$\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha\beta) = \lim_{n\to\infty} \mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha\beta_n).$$

Moreover, we have by Proposition 6.1.9 that

$$\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha\beta_n) = \mathrm{Tr}_{L/K}(\alpha\beta_n) - \sum_{i=2}^{g} \mathrm{Tr}_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(\alpha\beta_n).$$

Note that $\mathrm{Tr}_{L/K}(\alpha\beta_n) \in A$ and that, for $i \geq 2$, the sequence of elements $\mathrm{Tr}_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(\alpha\beta_n) \in K_{\mathfrak{p}}$ tends to 0 in the $\mathfrak{p}$-adic topology, again by continuity of the trace map. Therefore, for sufficiently large n, the element $\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha\beta_n)$ lies in $\mathscr{O}_{\mathfrak{p}}$, proving the claim. In particular, we have $\mathfrak{D}_{B/A}^{-1} \subseteq \mathfrak{D}_{\mathscr{O}_{\mathfrak{P}}/\mathscr{O}_{\mathfrak{p}}}^{-1}$.

On the other hand, if $\alpha \in \mathfrak{D}^{-1}_{\mathscr{O}_{\mathfrak{P}}/\mathscr{O}_{\mathfrak{p}}}$, then we may write α as the limit of a sequence $(\alpha_n)_n$ in L that has limit 0 in $L_{\mathfrak{P}_i}$ for $i \geq 2$. For $\beta \in B$, we have

$$\lim_{n\to\infty} \mathrm{Tr}_{L/K}(\alpha_n\beta) = \sum_{i=1}^{g} \lim_{n\to\infty} \mathrm{Tr}_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(\alpha_n\beta) = \mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha\beta) \in \mathscr{O}_{\mathfrak{p}}.$$

Since $K \cap \mathscr{O}_{\mathfrak{p}} = A_{\mathfrak{p}}$, we have that $\mathrm{Tr}_{L/K}(\alpha_n\beta) \in A_{\mathfrak{p}}$ for sufficiently large n. By Lemma 6.2.6, we therefore have $\alpha_n \in S^{-1}\mathfrak{D}^{-1}_{B/A}$ for all such n, where S is the complement of $\mathfrak{p}$ in A. But then $\alpha \in \mathfrak{D}^{-1}_{B/A}\mathscr{O}_{\mathfrak{P}}$ as the limit of these elements. We therefore have the reverse containment $\mathfrak{D}^{-1}_{\mathscr{O}_{\mathfrak{P}}/\mathscr{O}_{\mathfrak{p}}} \subseteq \mathfrak{D}^{-1}_{B/A}\mathscr{O}_{\mathfrak{P}}$ and therefore equality. Since the these fractional ideals in $\mathscr{O}_{\mathfrak{P}}$ agree, so do their inverses, proving the lemma. □

The following is an immediate corollary.

COROLLARY 6.2.8. *Let A be a Dedekind domain with quotient field K, let L be a finite separable extension of K, let B be the integral closure of A in L. For any prime ideal $\mathfrak{P}$ of B, we will use $\mathfrak{p}$ to denote $\mathfrak{P} \cap A$ and $\mathfrak{D}_{\mathfrak{P}/\mathfrak{p}}$ to denote the intersection with B of the local different $\mathfrak{D}_{\mathscr{O}_{\mathfrak{P}}/\mathscr{O}_{\mathfrak{p}}}$, where $\mathscr{O}_{\mathfrak{P}}$ (resp., $\mathscr{O}_{\mathfrak{p}}$) is the valuation ring of $L_{\mathfrak{P}}$ (resp., $K_{\mathfrak{p}}$). We then have*

$$\mathfrak{D}_{B/A} = \prod_{\mathfrak{P}} \mathfrak{D}_{\mathfrak{P}/\mathfrak{p}},$$

with the product taken over the nonzero prime ideals of B.

In the case that B/A is an extension Dedekind domains such that B is generated by a single element as an A-algebra, we have the following explicit recipe for the different.

PROPOSITION 6.2.9. *Let A be a Dedekind domain with quotient field K, let L be a finite separable extension of K. Let $\beta \in L$ be integral over A, let $f \in A[x]$ be the minimal polynomial of β, and let $f' \in A[x]$ be the formal derivative of f. Then $f'(\beta)^{-1}$ generates the $A[\beta]$-module*

$$\{\alpha \in L \mid \mathrm{Tr}_{L/K}(\alpha A[\beta]) \subseteq A\}.$$

PROOF. Write $f = \sum_{i=0}^{n} a_i x^i$ for some $a_i \in A$ with $a_n = 1$. Let $\beta_1, \ldots, \beta_n$ be the roots of f in an algebraic closure of L. We claim that for any nonnegative integer $k < n$, we have

$$\sum_{i=1}^{n} \frac{f}{x-\beta_i} \frac{\beta_i^k}{f'(\beta_i)} = x^k. \tag{6.2.1}$$

To see this, note that the two sides of (6.2.1) are equal upon evaluation at each β_i, yet both sides are polynomials of degree less than n, so their difference is identically zero.

We have

$$\frac{f}{x-\beta} = \sum_{j=0}^{n-1} b_j x^j$$

for some $b_j \in A[\beta]$, so

$$\sum_{j=0}^{n-1} \mathrm{Tr}_{L/K}\left(\beta^k \frac{b_j}{f'(\beta)}\right) x^j = x^k,$$

and therefore

$$\mathrm{Tr}_{L/K}\left(\beta^k \frac{b_j}{f'(\beta)}\right) = \delta_{j,k}.$$

Now, the elements $\frac{b_j}{f'(\beta)}$ span $\{\alpha \in L \mid \mathrm{Tr}_{L/K}(\alpha A[\beta]) \subseteq A\}$ as an A-module. We therefore need only show that the b_j span $A[\beta]$. For this, note that

$$(x-\beta)\sum_{i=0}^{n-1} b_i x^i = \sum_{i=0}^{n} a_i x^i,$$

so $b_{n-1} = 1$ and $b_j - \beta b_{j+1} = a_{j+1}$ for each $0 \leq j \leq n-1$. Solving for the b_j, we obtain

$$b_j = \sum_{i=0}^{n-j-1} a_{i+j+1}\beta^i,$$

for each j. Since the coefficients of the powers of β in the latter expression b_j form the columns of a unipotent matrix in A, each power β^i of β with $0 \leq i \leq n-1$ may be written as an A-linear combination of the b_j. Thus, the b_i span $A[\beta]$. □

COROLLARY 6.2.10. *Let A be a Dedekind domain with quotient field K, let L be a finite extension of K. Suppose that the integral closure of A in L equals $A[\beta]$ for some $\beta \in L$. Let $f \in A[x]$ be the minimal polynomial of β, and let $f' \in A[x]$ be the formal derivative of f. Then $\mathscr{D}_{B/A} = (f'(\beta))$.*

We will require the following.

LEMMA 6.2.11. *Let K be a complete discrete valuation field with valuation ring $\mathscr{O}_K$, and let L be a finite extension of K, with valuation ring $\mathscr{O}_L$. Suppose that the corresponding extension $\kappa(L)/\kappa(K)$ of residue fields is separable. Then there exists $\beta \in \mathscr{O}_L$ such that $\mathscr{O}_L = \mathscr{O}_K[\beta]$. Moreover, any $\beta' \in \mathscr{O}_L$ sufficiently close to β in the topology of L also satisfies $\mathscr{O}_L = \mathscr{O}_K[\beta']$.*

PROOF. Since $\kappa(L)/\kappa(K)$ is separable, there exists $\bar{\beta} \in \kappa(L)$ such that $\kappa(L) = \kappa(K)(\bar{\beta})$. Let $\bar{f} \in \kappa(K)[x]$ be the minimal polynomial of $\bar{\beta}$, and let $f \in \mathscr{O}_K[x]$ be any lift of $\bar{f}$. We claim that there exists a lift $\beta \in \mathscr{O}_L$ of $\bar{\beta}$ to an element with $f(\beta)$ a uniformizer of L. For any lift α, we must have at least that the valuation of $f(\alpha)$ is positive, since $\bar{f}(\bar{\beta}) = 0$. If it is not 1, then $\alpha + \pi_L$, where π_L is a uniformizer of L is another lift with

$$f(\alpha+\pi_L) \equiv f(\alpha) + f'(\alpha)\pi_L \bmod (\pi_L)^2.$$

Since $\bar{f}$ is separable, we have that $f'(\alpha) \in \mathscr{O}_L^\times$. Therefore, we $f(\alpha+\pi_L)$ does indeed have valuation 1.

Now, with β chosen, we set $\pi_L = f(\beta)$ and claim that the $\beta^i \pi_L^j = \beta^i f(\beta)^j$ with $0 \leq i \leq f_{L/K}-1$ and $0 \leq j \leq e_{L/K}-1$ form an $\mathscr{O}_K$-basis of $\mathscr{O}_L$, which will finish the proof, aside from the final

statement. Given a uniformizer π_K of K, it suffices to show that the elements $\beta^i \pi_L^j$ are a basis of $\mathscr{O}_L/\pi_K\mathscr{O}_L$ as an $\kappa(K)$-vector space. To see this, fix a set S_K of representatives of $\kappa(K)$ in $\mathscr{O}_K$, and note that the set S_L of elements

$$\sum_{i=0}^{f_{L/K}-1} c_i \beta^i$$

with $c_i \in S_K$ is a set of representatives of $\kappa(L)$. While $\pi_L^{e_{L/K}}$ is a multiple of π_K, the elements

$$\sum_{i=0}^{e_{L/K}-1} a_i \pi_L^i$$

with $a_i \in S_L$ clearly have distinct image in the quotient, which has dimension $e_{L/K} f_{L/K}$. Hence, we have the claim.

Finally, note that the proof that $\mathscr{O}_L = \mathscr{O}_K[\beta]$ depended only on the facts that β lifts $\bar{\beta}$ and that $f(\beta)$ is a uniformizer. Since this holds true for any element in the congruence class of β modulo π_L^2, we are done. □

The latter lemma helps to extend the recipe of Corollary 6.2.10 to the general case. We omit the proof of the following theorem.

THEOREM 6.2.12. *Let A be a Dedekind domain with quotient field K, let L be a finite separable extension of K, and let B be the integral closure of A in L. The $\mathfrak{D}_{B/A}$ is the ideal generated by the elements $f'(\beta)$ with $\beta \in B$ such that $L = K(\beta)$, for $f \in A[x]$ the minimal polynomial of β.*

We may now show that the different detects ramification of primes.

THEOREM 6.2.13. *Let A be a Dedekind domain with quotient field K, let L be a finite extension of K, and let B be the integral closure of A in L. Let $\mathfrak{P}$ be a nonzero prime ideal of B, let $\mathfrak{p} = A \cap \mathfrak{P}$, and suppose that the corresponding extension of residue fields is separable. Then $\mathfrak{P}$ is ramified over A if and only if it divides $\mathfrak{D}_{B/A}$.*

PROOF. By Lemma 6.2.7, we may replace B by its completion at $\mathfrak{P}$ and A by its completion at $\mathfrak{p}$. Therefore, we assume that A is a complete discrete valuation ring, as is B. By Lemma 6.2.11, we have that $B = A[\beta]$ for some $\beta \in B$. Let $f \in A[x]$ be the minimal polynomial of β. As $\mathfrak{D}_{B/A} = (f'(\beta))$, the prime $\mathfrak{P}$ does not divide $\mathfrak{D}_{B/A}$ if and only if $f'(\beta)$ is a unit, which is to say if and only if the image $\bar{\beta} \in B/\mathfrak{P}$ of β is a simple root of the image $\bar{f}$ of f in $(A/\mathfrak{p})[x]$.

If $\mathfrak{P}$ is unramified, then $B/\mathfrak{P} = (A/\mathfrak{p})[\bar{\beta}]$ is of degree $[L:K]$ over $A/\mathfrak{p}$, so $\bar{f}$ is irreducible. Since the extension of residue fields is separable, $\bar{f}$ is itself separable, so $f'(\beta)$ is a unit.

Conversely, suppose that $f'(\beta)$ is a unit. Then the minimal polynomial $\bar{g}$ of $\bar{\beta}$ is relatively prime to $\bar{f}\bar{g}^{-1}$. By Theorem 5.3.33, there is a lift $g \in A[x]$ of $\bar{g}$ that divides f and has the same degree as $\bar{g}$. As f is irreducible, this forces $\deg \bar{g} = [L:K]$, which means that $\bar{f} = \bar{g}$ is irreducible. Thus, $\mathfrak{P}$ is unramified. □

The different is closely is closely related to the discriminant, which we now define in greater generality than before, though with slightly less specificity in the already defined case that the ground ring is $\mathbb{Z}$, since the different we now consider is an ideal, not an integer.

DEFINITION 6.2.14. Let A be a Dedekind domain with quotient field K, let L be a finite separable extension of K, let B be the integral closure of A in L. The *discriminant* $\mathfrak{d}_{B/A}$ of B/A is the ideal of A generated by all discriminants $\mathrm{D}(\alpha_1,\dots,\alpha_n)$ of ordered bases $(\alpha_1,\dots,\alpha_n)$ of L over K that are contained in B.

PROPOSITION 6.2.15. *Let A be a Dedekind domain with quotient field K, let L be a finite separable extension of K, let B be the integral closure of A in L. Then*

$$\mathfrak{d}_{B/A} = N_{L/K}(\mathfrak{D}_{B/A}).$$

PROOF. Let $\mathfrak{p}$ be a prime ideal of A that divides $\mathfrak{d}_{B/A}$. (By Proposition 2.5.15, the ideals of A that ramify in B, hence lie below primes dividing $\mathfrak{D}_{B/A}$, divide $\mathfrak{d}_{B/A}$, so this suffices.) Let $S = A - \mathfrak{p}$, and consider the localizations $S^{-1}\mathfrak{D}_{B/A}$ and $S^{-1}\mathfrak{d}_{B/A}$. We know that $S^{-1}\mathfrak{D}_{B/A} = \mathfrak{D}_{S^{-1}B/S^{-1}A}$ and that $S^{-1}\mathfrak{d}_{B/A} = \mathfrak{d}_{S^{-1}B/S^{-1}A}$ follows directly from the definition of the discriminant (since S is contained in A and the discriminant function D is K-multilinear). Therefore, we may assume that A is a DVR, from which it follows that B is a PID (as a Dedekind domain with only finitely many nonzero prime ideals).

Since B is a torsion-free A-module of finite rank, it admits an A-basis $(\alpha_1,\dots,\alpha_n)$, and we have $\mathfrak{d}_{B/A} = \mathrm{D}(\alpha_1,\dots,\alpha_n)$. Let $(\beta_1,\dots,\beta_n) \in L^n$ be the dual basis to $(\alpha_1,\dots,\alpha_n)$ for which $\mathrm{Tr}_{L/K}(\alpha_i\beta_j) = \delta_{i,j}$ for $1 \le i,j \le n$. Then $(\beta_1,\dots,\beta_n)$ is a free A-module basis of $\mathfrak{D}_{B/A}^{-1}$. Let $\gamma \in B$ be such that $(\gamma) = \mathfrak{D}_{B/A}$, and note that $(\gamma^{-1}\alpha_1,\dots,\gamma^{-1}\alpha_n)$ is also an ordered basis of $\mathfrak{D}_{B/A}^{-1}$ as an A-module. We therefore have

$$(\mathrm{D}(\beta_1,\dots,\beta_n)) = (\mathrm{D}(\gamma^{-1}\alpha_1,\dots,\gamma^{-1}\alpha_n)) = (N_{L/K}(\gamma))^{-2}(\mathrm{D}(\alpha_1,\dots,\alpha_n)). \tag{6.2.2}$$

Let $\sigma_1,\dots,\sigma_n$ be the K-linear embeddings of L in an algebraic closure $\overline{K}$ of K. Note that the product of the transpose of the matrix $(\sigma_i\alpha_j)_{i,j}$ and the matrix $(\sigma_i\beta_j)_{i,j}$ has (i,j)-entry

$$\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\beta_j) = \mathrm{Tr}_{L/K}(\alpha_i\beta_j),$$

so is the identity matrix. Therefore, we have that

$$\mathrm{D}(\beta_1,\dots,\beta_n) = \pm\mathrm{D}(\alpha_1,\dots,\alpha_n)^{-1}.$$

Combining this with (6.2.2), we have

$$(\mathrm{D}(\alpha_1,\dots,\alpha_n))^2 = (N_{L/K}(\gamma))^2,$$

so we obtain $\mathfrak{d}_{B/A} = N_{L/K}(\mathfrak{D}_{B/A})$. □

We derive a few corollaries.

COROLLARY 6.2.16. *Let A be a Dedekind domain with quotient field K, let L be a finite separable extension of K, let B be the integral closure of A in L. A prime ideal of A ramifies in B if and only if it divides $\mathfrak{d}_{B/A}$.*

PROOF. This is immediate from Theorem 6.2.13 and Proposition 6.2.15. □

REMARK 6.2.17. Corollary 6.2.16 tells us that the ideal $p\mathbb{Z}$ generated by a prime p ramifies in $K/\mathbb{Q}$ for a number field K if and only if p divides $\mathrm{disc}(K)$.

COROLLARY 6.2.18. *Let A be a Dedekind domain with quotient field K. Let L/K and M/L be finite extensions, let B be the integral closure of K in L, and let C be the integral closure of K in M. We then have*

$$\mathfrak{d}_{C/A} = \mathfrak{d}_{B/A}^{[M:L]} N_{L/K}(\mathfrak{d}_{C/B}).$$

PROOF. By Lemma 6.2.5 and Proposition 6.2.15, we have

$$\mathfrak{d}_{C/A} = N_{M/K}(\mathfrak{D}_{C/A}) = N_{M/K}(\mathfrak{D}_{C/B}) N_{L/K}(\mathfrak{D}_{B/A})^{[M:L]} = N_{L/K}(\mathfrak{d}_{C/B}) \mathfrak{d}_{B/A}^{[M:L]},$$

as desired. □

COROLLARY 6.2.19. *Let A be a Dedekind domain with quotient field K, let L be a finite separable extension of K, let B be the integral closure of A in L. For any prime ideal $\mathfrak{P}$ of B, we will use $\mathfrak{p}$ to denote $\mathfrak{P} \cap A$ and $\mathfrak{d}_{\mathfrak{P}/\mathfrak{p}}$ to denote the intersection with A of the local discriminant $\mathfrak{d}_{\mathscr{O}_\mathfrak{P}/\mathscr{O}_\mathfrak{p}}$, where $\mathscr{O}_\mathfrak{P}$ (resp., $\mathscr{O}_\mathfrak{p}$) is the valuation ring of $L_\mathfrak{P}$ (resp., $K_\mathfrak{p}$). We then have*

$$\mathfrak{d}_{B/A} = \prod_{\mathfrak{P}} \mathfrak{d}_{\mathfrak{P}/\mathfrak{p}},$$

with the product taken over the nonzero prime ideals of B.

PROOF. By Lemma 6.1.9, Proposition 6.2.15, and Lemma 6.2.7, we have

$$\mathfrak{d}_{B/A}\mathscr{O}_\mathfrak{p} = N_{L/K}(\mathfrak{D}_{B/A})\mathscr{O}_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} N_{L_\mathfrak{P}/K_\mathfrak{p}}(\mathfrak{D}_{B/A}\mathscr{O}_\mathfrak{P}) = \prod_{\mathfrak{P}|\mathfrak{p}} N_{L_\mathfrak{P}/K_\mathfrak{p}}(\mathfrak{D}_{\mathscr{O}_\mathfrak{P}/\mathscr{O}_\mathfrak{p}}) = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{d}_{\mathscr{O}_\mathfrak{P}/\mathscr{O}_\mathfrak{p}},$$

hence the result by intersection with A. □

In the case of global or complete discrete valuation fields, which come equipped with canonical subrings, the ring of integers and valuation ring in the respective cases, we can use the field as the subscript in the definition of the different and discriminant, which we will typically do below.

DEFINITION 6.2.20.

a. The *different* $\mathfrak{D}_{L/K}$ (resp., *discriminant* $\mathfrak{d}_{L/K}$) of an extension L/K of global fields is the different (resp., discriminant) of the corresponding extension $\mathscr{O}_L/\mathscr{O}_K$ of rings of integers.

b. The *different* $\mathfrak{D}_{L/K}$ (resp., *discriminant* $\mathfrak{d}_{L/K}$) of an extension L/K of complete discrete valuation fields is the different (resp., discriminant) of the corresponding extension of valuation rings.

Combining the above results with Minkowski theory would allow us to derive the following fascinating result, which we state without proof.

THEOREM 6.2.21. *Let K be a number field and S a finite set of prime ideals of K. For each $n \geq 1$, there exist only finitely many extensions L/K of degree n in which the prime ideals of K that ramify in L are all contained in S.*

As a consequence of Theorem 6.2.21 and Corollary 4.3.6, one has the following.

THEOREM 6.2.22. *For any $N \geq 1$, there exist only finitely many number fields K with $|\operatorname{disc}(K)| \leq N$.*

DEFINITION 6.2.23. A separable algebraic extension L of a global field K is *unramified* if every place of K is unramified in L.

We have the following corollary of Theorem 4.3.6.

COROLLARY 6.2.24. *The field $\mathbb{Q}$ has no nontrivial extension that is unramified at all finite primes.*

PROOF. Corollary 4.3.6 tells us that if $[K : \mathbb{Q}] \geq 2$, then

$$|\operatorname{disc}(K)| \geq \frac{2^2}{2!} \cdot \left(\frac{\pi}{4}\right)^2 = \frac{\pi^2}{8} > 1,$$

so K is not unramified. □

6.3. Multiplicative groups of local fields

In this section, we study the structure of multiplicative groups of local fields. For the rest of this chapter, "local field" should be taken to mean "nonarchimedean local field". Let us make the following definition.

DEFINITION 6.3.1. Let K be a complete discrete valuation field with valuation ring $\mathscr{O}$ and maximal ideal $\mathfrak{m}$. Then the *ith unit group* $U_i = U_i(K)$ of K is defined by $U_0 = \mathscr{O}^\times$ for $i = 0$ and $U_i = 1 + \mathfrak{m}^i$ for $i \geq 1$.

NOTATION 6.3.2. In this section, we let K be a local field. We let p be the characteristic of its residue field, $\mathscr{O}$ its valuation ring, $\mathfrak{m}$ its maximal ideal, π a fixed uniformizer, κ the residue field, and q the order of κ. We let $e = e_K$ and $f = f_K$.

LEMMA 6.3.3. *The set of roots of unity of order prime to p in a local field K has order $q-1$, where q is the order of the residue field of K.*

PROOF. The polynomial $x^q - x$ splits completely over the residue field κ of K, so Hensel's Lemma tells us that $\mu_{q-1}(K)$ has order q and maps isomorphically onto $\kappa(K)^\times$. □

PROPOSITION 6.3.4. *Let K be a local field with residue field of order q. The canonical map*

$$\langle \pi \rangle \times \mu_{q-1}(K) \times U_1(K) \xrightarrow{\sim} K^\times$$

is an isomorphism.

PROOF. Since K is a discrete valuation field with valuation we denote v, we may write any $a \in K^\times$ uniquely as $a = \pi^{v(a)} b$ for some $b \in U_0$. By Lemma 6.3.3, each $b \in U_0$ may then be written uniquely as $b = \xi \cdot u$ with $\xi \in \mu_{q-1}$ and $u \in U_1$. □

LEMMA 6.3.5. *Let K be a local field. For $a \in \mathcal{O}$, let $\bar{a}$ denote its image in κ. We have isomorphisms of groups*

$$U_0/U_1 \xrightarrow{\sim} \kappa^\times, \qquad uU_1 \mapsto \bar{u},$$

and

$$U_i/U_{i+1} \xrightarrow{\sim} \kappa, \qquad (1+\pi^i a)U_{i+1} \mapsto \bar{a}$$

for $i \geq 1$.

PROOF. The first statement follows from Proposition 6.3.4. The bijectivity of the second map is clear, and that it is a homomorphism is simply that

$$(1+\pi^i a)(1+\pi^i b) \equiv 1 + \pi^i(a+b) \bmod \mathfrak{m}^{i+1}.$$

□

LEMMA 6.3.6. *Let K be a local field of residue characteristic p. We have an isomorphism of $\mathbb{Z}_p$-modules*

$$U_1 \xrightarrow{\sim} \varprojlim_i U_1/U_i$$

via the map induced by the universal property of the inverse limit.

PROOF. Since $\bigcap_i U_i = \{1\}$, the map in question is injective. Any sequence $(a_i)_i$ in U_1 with $a_{i+1}a_i^{-1} \in U_i$ for each $i \geq 1$ is the image of the limit of the sequence. □

Note also the following.

LEMMA 6.3.7. *Let K be a p-adic field. Let $e = v(p)$. For $i \geq 1$ and $a \in \mathcal{O}^\times$, we have*

$$(1+\pi^i a)^p \equiv 1 + p\pi^i a + \pi^{ip} a^p \bmod \mathfrak{m}^{2i+e}.$$

In particular, we have

$$(1+\pi^i a)^p \equiv \begin{cases} 1 + \pi^{ip} a^p \bmod \mathfrak{m}^{i+e} & \text{if } i < \frac{e}{p-1}, \\ 1 + p\pi^i a \bmod \mathfrak{m}^{i+e+1} & \text{if } i > \frac{e}{p-1}. \end{cases}$$

PROOF. The first statement is an easy consequence of the binomial expansion

$$(1+\pi^i a)^p = \sum_{k=0}^{p} \binom{p}{k} \pi^{ik} a^k,$$

since p exactly divides $\binom{p}{k}$ for $0 < k < p$. The second follows from the fact that $i > e/(p-1)$ if and only if

$$v(p\pi^i) = i + e < ip = v(\pi^{ip}).$$

□

LEMMA 6.3.8. *The pth power map is an isomorphism $U_i \xrightarrow{\sim} U_{i+e}$ for $i > \frac{e}{p-1}$.*

PROOF. For any $\alpha \in U_{i+e}$ and $k \geq 1$, suppose by induction that we have found $\beta_k \in U_i$ with

$$\beta_k^p \alpha^{-1} = 1 + p\pi^{i+k-1} a_k \bmod \mathfrak{m}^{i+e+k}$$

for some $a_k \in \mathscr{O}$. Set $\beta_{k+1} = \beta_k(1+\pi^{i+k-1}a_k)$ and

$$\beta = \lim_{k\to\infty} \beta_k.$$

Then $\beta \in U_i$ with $\beta^p = \alpha$, and the pth power map $U_i \to U_{i+e}$ is surjective.

Note that $p\mathbb{Z}_p[\mu_p] = (1-\zeta_p)^{p-1}$ for a primitive pth root of unity ζ_p by Lemma 3.1.13. So, if $\zeta_p \in K$, then $v(\zeta_p - 1) = e/(p-1)$. That is, $\zeta_p \notin U_{e/(p-1)+1}$, so the map is injective as well. □

As a pro-p group, $U_1(K)$ for K a local field of residue characteristic p is generated by any lift of a set of generators of U_1/U_1^p.

PROPOSITION 6.3.9. *Let K be a p-adic field, let q be the order of the residue field of K, let π_K be a uniformizer of K, and let p^n be the number of p-power roots of unity in K. Then we have an isomorphism*

$$U_1(K) \cong \mathbb{Z}_p^{[K:\mathbb{Q}_p]} \times \mathbb{Z}/p^n\mathbb{Z},$$

of finitely generated $\mathbb{Z}_p$-modules. In particular, there are isomorphisms of topological groups

$$K^\times \cong \langle \pi_K \rangle \times \mathscr{O}_K^\times \cong \langle \pi_K \rangle \times \mu_{q-1}(K) \times U_1(K) \cong \mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}_p^{[K:\mathbb{Q}_p]},$$

where $K^\times$ has the subspace topology from K, and the direct products are all given the product topology, with $\langle \pi_K \rangle$, $\mathbb{Z}$, and the finite groups involved given the discrete topology.

PROOF. Lemma 6.3.8 tells us that U_1/U_1^p is finite, so U_1 is a finitely generated $\mathbb{Z}_p$-module. Since the p-power torsion in U_1 is the group of p-power roots of unity in K, which is cyclic of order p^n, we have $U_1 \cong \mathbb{Z}_p^r \times \mathbb{Z}/p^n\mathbb{Z}$ for some $r \geq 0$, and this is a topological isomorphism.

No nontrivial p-power root of unity ζ lies in U_j for any integer $j > \frac{e}{p-1}$, where $e = v(p)$. Since U_j has finite index in U_1, we therefore have that $U_j \cong \mathbb{Z}_p^r$. By Lemma 6.3.8, we know that $U_j^p = U_{j+e}$, so

$$r = \dim_{\mathbb{F}_p} U_j/U_{j+e} = \sum_{k=j}^{j+e-1} \dim_{\mathbb{F}_p} U_k/U_{k+1} = ef = [K : \mathbb{Q}_p],$$

noting that $U_k/U_{k+1} \cong \mathbb{F}_{p^f}$ for all $k \geq 1$, where f is the residue degree of $K/\mathbb{Q}_p$.

Finally, note that the U_i form a basis of open neighborhoods of 1 in $K^\times$ under both the subspace topology and topology induced by the product topology in the isomorphism with $K^\times$ of the theorem. Therefore, these isomorphisms are of topological groups. □

Let us also mention the case of finite characteristic. We provide an outline of the proof.

PROPOSITION 6.3.10. *Let $K = \mathbb{F}_q(\!(t)\!)$. Then there exists a continuous $\mathbb{Z}_p$-linear isomorphism from $U_1(K)$ to a countable direct product of copies of $\mathbb{Z}_p$.*

PROOF. Let B be a basis of $\mathbb{F}_q$ as an $\mathbb{F}_p$-vector space. Let I be the countable set

$$I = \{(c,i) \mid c \in B, i \geq 1, p \nmid i\}.$$

Define a homomorphism

$$\kappa\colon \prod_{(c,i)\in I} \mathbb{Z}_p \to U_1(K)$$

by

$$\kappa((a_{c,i})_{(c,i)}) = \prod_{(c,i)\in I} (1 + ct^i)^{a_{c,i}}.$$

This is easily seen to be well-defined, and one may check that every element of U_1 has a unique expansion of this form.

The inverse image of U_j under κ contains the open neighborhood of 1 that is the direct product of $p^{n_i}\mathbb{Z}_p$ is the (c,i)-coordinate for each $(c,i) \in I$, where each $n_i \geq 0$ is minimal satisfying $p^{n_i} i > j$. On the other hand, the image of an open neighborhood

$$\prod_{c,i\in I} p^{n_{c,i}}\mathbb{Z}_p$$

with $n_{c,i} = 0$ for i sufficiently large contains U_j for j with

$$j = \max\{p^{n_{c,i}} i \mid (c,i) \in I, n_{c,i} \geq 1\},$$

which we leave to the reader to check. Therefore, κ is in fact a topological isomorphism. □

6.4. Tamely ramified extensions

Before studying the larger class of tamely ramified extensions of a local field, let us first consider unramified extensions.

LEMMA 6.4.1. *Let K be a local field. For each positive integer n, there exists a unique unramified extension of K of degree n, equal to $K(\mu_{q^n-1})$, where q is the order of the residue field of K.*

PROOF. Let L/K be an unramified extension of degree n. Then $\kappa(L)$ is a degree n extension of $\kappa(K)$ by the degree formula. That L contains $K(\mu_{q^n-1})$ is then simply Lemma 6.3.3. Moreover, $K(\mu_{q^n-1})$ is then by definition of degree n over K, so equals L. □

DEFINITION 6.4.2. We say that an algebraic extension L of a local field K is *unramified* if it is separable and every finite degree subextension of K in L is unramified.

Similarly, we have the following.

DEFINITION 6.4.3. We say that an algebraic extension L of a local field K is *totally ramified* if it is separable and every finite degree subextension of K in L is totally ramified.

DEFINITION 6.4.4. A *Frobenius automorphism* in a Galois extension L/K, with K a local field, is any lift of the Frobenius automorphism of the extension of residue fields to L.

REMARK 6.4.5. If L/K is unramified in Definition 6.4.4, then there is a unique Frobenius automorphism in $\mathrm{Gal}(L/K)$.

PROPOSITION 6.4.6. *Let L be an separable extension of a local field K. Then there is a unique maximal unramified extension E of K in L, and* $\mathrm{Gal}(E/K)$ *is topologically generated by its Frobenius automorphism.*

PROOF. It suffices to consider the case that L/K is finite. Let q be the order of the residue field of L. Set $E = K(\mu_{q-1})$, which is unramified over K. Any unramified extension of K in L is generated prime-to-p roots of unity, of which there are only q in L. □

The following definition makes sense as the union of all finite unramified extensions of a local field (in a fixed separable closure).

DEFINITION 6.4.7. The *maximal unramified extension* K^{ur} of a local field is the unique largest unramified extension of K inside a given separable closure of K.

PROPOSITION 6.4.8. *The maximal unramified extension K^{ur} of a local field K is given by adjoining all prime-to-p roots of unity in a separable closure of K. Its Galois group* $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ *is isomorphic to $\hat{\mathbb{Z}}$ via the map that takes the Frobenius automorphism to* 1.

PROOF. By definition, K^{ur} is the union of the finite unramified subextensions of K in K^{sep}, which is to say the fields $K_n = K(\mu_{q^n-1})$. Since any prime-to-p integer m divides $q^n - 1$ for some n, we have that K^{ur} is given by adjoining all prime-to-p roots of 1. Recall that $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/n\mathbb{Z}$ via the map that takes the Frobenius automorphism to 1. Therefore, the isomorphism in question is the composite of the canonical maps

$$\mathrm{Gal}(K^{\mathrm{ur}}/K) \cong \varprojlim_n \mathrm{Gal}(K_n/K) \cong \varprojlim_n \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} \cong \hat{\mathbb{Z}}.$$

□

DEFINITION 6.4.9. Let K be a local field and L a Galois extension of K. The *inertia subgroup* of $\mathrm{Gal}(L/K)$ is the subgroup of elements fixing the maximal unramified extension of K in L.

The following is analogous to Remark 6.1.25 and almost immediate from Proposition 6.4.8.

PROPOSITION 6.4.10. *Let K be a local field, and let I_K denote the inertia subgroup of G_K. Then there is an exact sequence*

$$1 \to I_K \to G_K \to G_{\kappa(K)} \to 1,$$

where $\kappa(K)$ is the residue field of K, and the map $G_K \to G_{\kappa(K)}$ is the composition of restriction $G_K \to \mathrm{Gal}(K^{\mathrm{ur}}/K)$ with the continuous isomorphism that takes a Frobenius element of $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ to the Frobenius element of $G_{\kappa(K)}$.

DEFINITION 6.4.11.

a. A separable extension L/K of local fields of residue characteristic p is *tamely ramified* if $p \nmid e_{L/K}$.

b. A separable extension L of a local field K is *tamely ramified* if every finite extension E of K in L is tamely ramified.

EXAMPLE 6.4.12. Let K be a local field, π a uniformizer, and e an integer not divisible by the residue characteristic p of K. Then $K(\pi^{1/e})/K$ is totally and tamely ramified, with ramification index e.

In fact, every tamely ramified extension is given in essentially this way.

PROPOSITION 6.4.13. *Let L/K be a tamely ramified extension of local fields of ramification index e. Then there exists a finite unramified extension E of K and a unifomizer λ of E such that $L = E(\mu)$ for an eth root μ of λ.*

PROOF. Let E be the maximal unramified subextension of K in L. Then L/E is a totally ramified extension of degree e. Let π_L be a uniformizer of L and π_K a uniformizer of K. A simple check of valuations tells us that $\pi_L^e = \pi_K \alpha$ for some $\alpha \in \mathscr{O}_L^\times$. In turn, Proposition 6.3.4 allows us to write $\alpha = \xi \cdot u$ with $\xi \in L$ a root of unity of order prime-to-p, where p is the residue characteristic of K,

and $u \in U_1(L)$. Since L/E is totally ramified, we actually have that $\xi \in E$. Since $p \nmid e$ and $U_1(L)$ is an abelian pro-p group, the element u has an eth root β in L. Set $\lambda = \pi_K \xi$, which is a uniformizer in E. We have $(\pi_L \beta^{-1})^e = \lambda$, so L contains an eth root μ of λ. Since the degree of $E(\mu)/E$ is e, we have $L = E(\mu)$. □

EXAMPLE 6.4.14. The extension $\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p$ is totally ramified of degree $p-1$, hence tamely ramified. In fact, we have that $\mathbb{Q}_p(\mu_p) = \mathbb{Q}_p((-p)^{\frac{1}{p-1}})$. To see this, note that

$$p = \prod_{i=1}^{p-1}(1-\zeta_p^i) = (1-\zeta_p)^{p-1}\prod_{i=1}^{p-1}(1+\zeta_p+\cdots+\zeta_p^{i-1}),$$

where ζ_p is a primitive pth root of 1. We have

$$\prod_{i=1}^{p-1}(1+\zeta_p+\cdots+\zeta_p^{i-1}) \equiv \prod_{i=1}^{p-1} i \equiv (p-1)! \equiv -1 \bmod (1-\zeta_p),$$

so $-p = (1-\zeta_p)^{p-1}u$ for some $u \in U_1(\mathbb{Q}_p(\mu_p))$. Since any such u is a $(p-1)$st power, we have the claim.

If a separable extension of a local field is not tamely ramified, we say it is wildly ramified.

DEFINITION 6.4.15. A separable extension L of a local field K of residue characteristic p is *wildly ramified* if p divides the ramification index of some finite extension E of K in L.

EXAMPLES 6.4.16. Let p be a prime number.

a. The extension $\mathbb{Q}_p(p^{1/p})/\mathbb{Q}_p$ is wildly ramified.

b. The extension $\mathbb{Q}_p(\mu_{p^2})/\mathbb{Q}_p$ is wildly ramified, since its ramification index is $p(p-1)$.

The compositum of any collection of tamely ramified extensions is tamely ramified, so we may speak of the maximal tamely ramified extension of a local field inside a separable algebraic closure.

REMARK 6.4.17. We can make sense of exponentiation on $\mathbb{Z}_p^\times$ by elements $\hat{\mathbb{Z}}$ as follows: if $u \in \mathbb{Z}_p$ and $a \in \hat{\mathbb{Z}}$, then we set

$$u^a = \lim_{n\to\infty} u^{a_n},$$

where $(a_n)_n$ is any sequence of integers with limit a. We leave it to the reader to check that the limit converges independently of the choice of sequence.

PROPOSITION 6.4.18. *The maximal tamely ramified extension L of a local field K of residue characteristic p is the Galois extension given by adjoining to K^{ur} the roots $\pi^{1/m}$ of a uniformizer π of K for all $m \geq 1$ with $p \nmid m$. The Galois group $\mathrm{Gal}(L/K^{\mathrm{ur}})$ is isomorphic to the direct product*

$$\hat{\mathbb{Z}}^{(p)} = \prod_{\ell \neq p} \mathbb{Z}_\ell,$$

where ℓ ranges over the prime numbers other than p. The Galois group $\mathrm{Gal}(L/K)$ *is the semi-direct product of* $\mathrm{Gal}(L/K^{\mathrm{ur}})$ *with* $\mathrm{Gal}(K^{\mathrm{ur}}/K) \cong \hat{\mathbb{Z}}$ *under the map* $\hat{\mathbb{Z}} \to \mathrm{Aut}(\hat{\mathbb{Z}}^{(p)})$ *taking* $a \in \hat{\mathbb{Z}}$ *to multiplication by* q^a *in each coordinate of* $\hat{\mathbb{Z}}^{(p)}$*, where* $q = |\kappa(K)|$.

REMARK 6.4.19. The Galois group of any Galois extension of the maximal tamely ramified extension of a local field is a pro-p group, where p is the residue characteristic. Any nontrivial such Galois extension is by necessity wildly ramified with no nontrivial tamely ramified subextension.

6.5. Ramification groups

Ramification groups provide a measure of the level of ramification in a Galois extension of a local field.

NOTATION 6.5.1. In this section, for a local field L, we use v_L to denote its valuation, $\mathscr{O}_L$ its valuation ring, and π_L a uniformizer. If $\mathfrak{a}$ is a fractional ideal of $\mathscr{O}_L$, it is generated by a power of π_L, and $v_L(\mathfrak{a})$ denotes that power.

DEFINITION 6.5.2. Let L/K be a Galois extension of local fields with Galois group G. For an integer $i \geq -1$, the ith *(higher) ramification group* of L/K is the subgroup of G given by

$$G_i = \{\tau \in G \mid v_L(\tau(\alpha) - \alpha) \geq i+1 \text{ for all } \alpha \in \mathscr{O}_L\}.$$

REMARK 6.5.3. We have by definition that $G_{-1} = G$ and G_0 is the inertia group of G. In particular, G/G_0 is the Galois group of the maximal unramified subextension of L/K.

REMARK 6.5.4. Let L/K be a Galois extension of local fields with Galois group G. By Lemma 6.2.11, we have that $\mathscr{O}_L = \mathscr{O}_K[\beta]$ for some $\beta \in \mathscr{O}_L$, so for any $i \geq -1$, we have

$$G_i = \{\tau \in G \mid v_L(\tau(\beta) - \beta) \geq i+1\}.$$

LEMMA 6.5.5. *Let L/K be a Galois extension of local fields with Galois group G. The ramification groups G_i are normal subgroups of G.*

PROOF. This is easy: let $\sigma \in G$ and $\tau \in G_i$. Then for any $\alpha \in \mathscr{O}_L$, we have

$$\tau(\sigma^{-1}(\alpha)) \equiv \sigma^{-1}(\alpha) \bmod \pi_L^{i+1},$$

so

$$\sigma\tau\sigma^{-1}(\alpha) \equiv \alpha \bmod \pi_L^{i+1}.$$

□

LEMMA 6.5.6. *Let L/K be a Galois extension of local fields with Galois group G. Let $\sigma \in G_0$. Then $\sigma \in G_i$ for $i \geq 0$ if and only if $\frac{\sigma(\pi_L)}{\pi_L} \in U_i(L)$.*

PROOF. First, we note that for $\sigma \in G_i$, we have $\sigma(\pi_L) \equiv \pi_L \bmod \pi_L^{i+1}$, so we have $\frac{\sigma(\pi_L)}{\pi_L} \in U_i(L)$. Conversely, if $\frac{\sigma(\pi_L)}{\pi_L} \in U_i(L)$, then for any $a \in \mathcal{O}_L$, we may write

$$a = \sum_{k=0}^{\infty} c_k \pi_L^k$$

for some $c_k \in \mu_{q-1}(L) \cup \{0\}$, where $q = |\kappa(L)|$. Since $\sigma \in G_0$, it fixes elements $\mu_{q-1}(L)$, so

$$\sigma(a) = \sum_{k=0}^{\infty} c_k \sigma(\pi_L)^k \equiv a \bmod \pi_L^{i+1},$$

the last step as $\sigma(\pi_L) \equiv \pi_L \bmod \pi_L^{i+1}$. That is, σ is an element of G_i. □

LEMMA 6.5.7. *Let L/K be a Galois extension of local fields with Galois group G. For each $i \geq 0$, we have an injection*

$$\rho_i \colon G_i/G_{i+1} \to U_i(L)/U_{i+1}(L)$$

given by

$$\rho_i(\sigma \cdot G_{i+1}) = \frac{\sigma(\pi_L)}{\pi_L} U_{i+1}(L).$$

PROOF. Lemma 6.5.6 tells us immediately that ρ_i is well-defined and sends only the coset G_{i+1} to the coset $U_{i+1}(L)$. Therefore, it remains only to see that ρ_i is a homomorphism. For this, let $\sigma, \tau \in G_i$, and note that

$$\frac{\sigma\tau(\pi_L)}{\pi_L} = \frac{\sigma(\pi_L)}{\pi_L} \cdot \sigma\Big(\frac{\tau(\pi_L)}{\pi_L}\Big) \equiv \frac{\sigma(\pi_L)}{\pi_L} \cdot \frac{\tau(\pi_L)}{\pi_L} \bmod \pi_L^{i+1},$$

the last step following from $\sigma \in G_0$ since $\tau(\pi_L)\pi_L^{-1} \in U_i(L)$. □

Since the quotients G_i/G_{i+1} are abelian for all $i \geq -1$, we have the following corollary.

COROLLARY 6.5.8. *The Galois group of any Galois extension of local fields is solvable.*

The following lemma is immediate from the definition of ramification groups.

LEMMA 6.5.9. *Let L/K be a Galois extension of local fields with Galois group G, and let H be a subgroup of G. Then $H_i = H \cap G_i$ for all $i \geq -1$.*

LEMMA 6.5.10. *Let L/K be a Galois extension of local fields with Galois group G. Then G/G_1 is the Galois group of the maximal tamely ramified subextension of L/K.*

PROOF. If L/K is tamely ramified, then each quotient G_i/G_{i+1} for $i \geq 1$ must be trivial. By Lemma 6.5.7, each quotient G_i/G_{i+1} for $i \geq 1$ is a p-group since since $U_i(L)/U_{i+1}(L)$ is one. Thus, $G_1 = \mathrm{Gal}(L/L^{G_1})$ is a p-group. As G_1 is contained in the inertia subgroup G_0 of G, the field L^{G_1} is totally ramified over L^{G_0} and contains the maximal tamely ramified subextension of L/K. On the other hand, G_0/G_1 injects into $U_0(L)/U_1(L)$, which has prime-to-p order, so L^{G_1}/L^{G_0} is in fact tamely ramified. As L^{G_0}/K is unramified, L^{G_1}/K is then tamely ramified. □

DEFINITION 6.5.11. Let L/K be a Galois extension of local fields with Galois group G. The subgroup of *wild inertia* for L/K is G_1.

PROPOSITION 6.5.12. *Let p be a prime and $n \geq 1$. Then*

$$\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)_i = \begin{cases} \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p) & \text{if } -1 \leq i \leq 0, \\ \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p(\mu_{p^k})) & \text{if } p^{k-1} \leq i \leq p^k - 1 \text{ with } 1 \leq k \leq n-1 \\ 1 & \text{if } i \geq p^{n-1}. \end{cases}$$

PROOF. Let $F_0 = \mathbb{Q}_p$ and $F_k = \mathbb{Q}_p(\mu_{p^k})$ for $k \geq 1$. Let $G = \mathrm{Gal}(F_n/\mathbb{Q}_p)$. Fix a primitive p^kth root of unity ζ_{p^k} for each $k \geq 1$ such that $\zeta_{p^{k+1}}^p = \zeta_{p^k}$ for each k. Let $\sigma \in G$ be nontrivial, let $i \in \mathbb{Z}$ be such that $\sigma(\zeta_{p^n}) = \zeta_{p^n}^i$, and let $k \geq 0$ be maximal such that $i \equiv 1 \bmod p^k$. Set $c = (i-1)/p^k$. We then have

$$\sigma(\zeta_{p^n}) - \zeta_{p^n} = \zeta_{p^n}^i - \zeta_{p^n} = \zeta_{p^n}^{1+cp^k} - \zeta_{p^n} = \zeta_{p^n}(\zeta_{p^{n-k}}^c - 1),$$

Since $p \nmid c$, this has valuation p^k in F_n. As the valuation ring of F_n is $\mathbb{Z}_p[\zeta_{p^n}]$, we then have that $\sigma \in G_{p^k-1} - G_{p^k}$. On the other hand, the fact that p^k exactly divides $i-1$ (for $k < n$) says that σ is an element of $\mathrm{Gal}(F_n/F_k)$ but not $\mathrm{Gal}(F_n/F_{k+1})$. The result follows. □

Ramification groups have the following interesting property, which we state without proof.

PROPOSITION 6.5.13. *Let L/K be a Galois extension of local fields with Galois group G, and let i and j be positive integers. For any $\sigma \in G_i$ and $\tau \in G_j$, the commutator $[\sigma,\tau] = \sigma\tau\sigma^{-1}\tau^{-1}$ is an element of G_{i+j+1}.*

Let us make the following useful definition.

DEFINITION 6.5.14. Let L/K be a Galois extension of local fields with Galois group G. Then we define a function $i_{L/K}\colon G \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ by

$$i_{L/K}(\sigma) = \min\{v_L(\sigma(\alpha) - \alpha) \mid \alpha \in \mathscr{O}_L\}$$

for $\sigma \in G$.

REMARK 6.5.15. In Definition 6.5.14, we have $\sigma \in G_i$ if and only if $i_{L/K}(\sigma) \geq i+1$.

We now show how the ramification filtration determines the different of a Galois extension of local fields.

PROPOSITION 6.5.16. *Let L/K be a Galois extension of local fields with Galois group G. Then we have*

$$v_L(\mathfrak{D}_{L/K}) = \sum_{\sigma \in G - \{1\}} i_{L/K}(\sigma) = \sum_{i=0}^{\infty} (|G_i| - 1).$$

PROOF. Let $\beta \in \mathscr{O}_L$ be such that $\mathscr{O}_L = \mathscr{O}_K[\beta]$. We let $f \in \mathscr{O}_K[x]$ be the minimal polynomial of β. Then

$$f'(\beta) = \prod_{\sigma \in G - \{1\}} (\beta - \sigma(\beta))$$

generates $\mathfrak{D}_{L/K}$ by Corollary 6.2.10, and so

$$v_L(f'(\beta)) = \sum_{\sigma \in G-\{1\}} i_{L/K}(\sigma) = \sum_{i=0}^{\infty} \sum_{\substack{\sigma \in G-\{1\} \\ i_{L/K}(\sigma)=i}} i = \sum_{i=0}^{\infty} i(|G_{i-1}| - |G_i|) = \sum_{i=0}^{\infty} (|G_i| - 1).$$

□

COROLLARY 6.5.17. *Let L/K be a Galois extension of local fields with Galois group G. Let H be a subgroup and $E = L^H$ its fixed field. Then*

$$v_E(\mathfrak{D}_{E/K}) = \frac{1}{e_{L/E}} \sum_{\sigma \in G-H} i_{L/K}(\sigma).$$

PROOF. Note first that

$$v_E(\mathfrak{D}_{E/K}) = \frac{1}{e_{L/E}} v_L(\mathfrak{D}_{E/K}).$$

By Lemma 6.2.5 and Proposition 6.5.16, we have

$$v_L(\mathfrak{D}_{E/K}) = v_L(\mathfrak{D}_{L/K}) - v_L(\mathfrak{D}_{L/E}) = \sum_{\sigma \in G-\{1\}} i_{L/K}(\sigma) - \sum_{\tau \in H-\{1\}} i_{L/E}(\tau) = \sum_{\sigma \in G-H} i_{L/K}(\sigma)$$

noting for the last step that $i_{L/E}(\tau) = i_{L/K}(\tau)$ for $\tau \in H$ by definition. □

Let us extend the definition of the lower ramification groups to all real numbers in the interval $[-1, \infty)$.

DEFINITION 6.5.18. Let L/K be a Galois extension of local fields with Galois group G. Let $t \in [-1, \infty)$. The tth *ramification group* G_t of L/K in the lower numbering is defined to be equal to the ramification group $G_{\lceil t \rceil}$, where $\lceil \cdot \rceil$ is the ceiling function.

We now define a function from $[-1, \infty)$ to $[-1, \infty)$ as follows.

DEFINITION 6.5.19. Let L/K be a Galois extension of local fields with Galois group G. We define

$$\phi_{L/K} \colon [-1, \infty) \to [-1, \infty)$$

by $\phi_{L/K}(t) = t$ for $t < 0$ and

$$\phi_{L/K}(t) = \int_0^t [G_0 : G_x]^{-1} dx$$

for $t \geq 0$.

REMARKS 6.5.20.

a. Definition 6.5.19 for an integer $k \geq -1$ may be written as

$$\phi_{L/K}(k) = \frac{1}{|G_0|} \sum_{i=1}^{k} |G_i|.$$

b. The function ϕ is continuous, piecewise linear, increasing, and concave down. Its slope between $k-1$ and k for an integer $k \geq 0$ is $|G_k|/|G_0|$, which is nonincreasing in k.

EXAMPLE 6.5.21. Let $F_n = \mathbb{Q}_p(\mu_{p^n})$ for a prime p and $n \geq 1$. By Proposition 6.5.12, we have

$$\phi_{F_n/\mathbb{Q}_p}(t) = \begin{cases} t & \text{if } -1 \leq i \leq 0, \\ \frac{t-p^{k-1}+1}{p^{k-1}(p-1)} + k - 1 & \text{if } p^{k-1}-1 \leq t \leq p^k - 1 \text{ with } 1 \leq k \leq n-1, \\ \frac{t-p^n+1}{p^{n-1}(p-1)} + n - 1 & \text{if } t \geq p^{n-1} - 1. \end{cases}$$

Note that $\phi_{F_n/\mathbb{Q}_p}(p^k - 1) = k$ for each $0 \leq k \leq n$.

We intend to show that $\phi_{L/K}$ behaves well under composition in towers of extension, and to investigate the behavior of ramification groups in quotients. For this, we first require several lemmas.

LEMMA 6.5.22. *Let L/K be a Galois extension of local fields with Galois group G, and let E/K be a normal subextension. Set $N = \mathrm{Gal}(L/E)$. For $\delta \in G/N$, we have*

$$i_{E/K}(\delta) = \frac{1}{e_{L/E}} \sum_{\substack{\sigma \in G \\ \sigma|_E = \delta}} i_{L/K}(\sigma).$$

PROOF. Write $\mathscr{O}_L = \mathscr{O}_K[\beta]$ for some $\beta \in \mathscr{O}_L$ and $\mathscr{O}_E = \mathscr{O}_K[\alpha]$ for some $\alpha \in \mathscr{O}_E$. Let $g \in \mathscr{O}_E[x]$ be the minimal polynomial of β over E. We have

$$g = \prod_{\tau \in N} (x - \tau(\beta)),$$

so letting $g^\sigma \in \mathscr{O}_E[x]$ denote the polynomial obtained by letting $\sigma \in G$ act on the coefficients of g, we have

$$g^\sigma = \prod_{\tau \in N} (x - \sigma\tau(\beta)).$$

Each coefficient of $g^\sigma - g$ is the difference of values of a symmetric polynomial in $|N|$-variables on the elements $\tau(\beta)$ and the elements $\sigma\tau(\beta)$. Since each coefficient of g lies in $\mathscr{O}_E$, it is a polynomial in α, and the coefficients of g^σ are the same polynomials in $\sigma(\alpha)$, so $\sigma(\alpha) - \alpha$ divides the coefficient of $g^\sigma - g$. In particular, $\sigma(\alpha) - \alpha$ divides $g^\sigma(\beta) - g(\beta) = g^\sigma(\beta)$.

Now, write $\alpha = f(\beta)$ for some $f \in \mathscr{O}_K[x]$. Note that $f(x) - \alpha$ has β as a root, so

$$f(x) - \alpha = g(x)h(x)$$

for some $h \in \mathscr{O}_E[x]$. Then

$$f(x) - \sigma(\alpha) = g^\sigma(x)h^\sigma(x).$$

Plugging in β, we obtain

$$\alpha - \sigma(\alpha) = g^\sigma(\beta) \cdot h^\sigma(\beta),$$

so $g^\sigma(\beta)$ divides $\sigma(\alpha) - \alpha$. In particular, they have the same valuation.

Now, let $\delta \in G/N$, which we may assume is not 1, since for $\delta = 1$ the result is obvious, with both sides of the equation in the statement being infinite. As we have seen, $\delta(\alpha) - \alpha$ and $g^\delta(\beta)$ have the same valuation. Thus, we have

$$e_{L/E} i_{E/K}(\delta) = v_L(\delta(\alpha) - \alpha) = v_L(g^\delta(\alpha)) = v_L\left(\prod_{\substack{\sigma \in G \\ \sigma|_E = \delta}} (\beta - \sigma(\beta)) \right) = \sum_{\substack{\sigma \in G \\ \sigma|_E = \delta}} i_{L/K}(\sigma).$$

□

LEMMA 6.5.23. *Let L/K be a Galois extension of local fields with Galois group G. For $t \geq -1$, we have*

$$\phi_{L/K}(t) + 1 = \frac{1}{|G_0|} \sum_{\sigma \in G} \min\{i_{L/K}(\sigma), t+1\}.$$

PROOF. Note that both sides of the equation in the statement are equal to 1 for $t = 0$. Also, both sides are piecewise linear and continuous, with slopes for any non-integral t equal to

$$\phi'_{L/K}(t) = [G_0 : G_{\lceil t \rceil}]^{-1} = \frac{|G_{\lceil t \rceil}|}{|G_0|}$$

and

$$\frac{1}{|G_0|} \sum_{\substack{\sigma \in G \\ i_{L/K}(\sigma) \geq \lceil t \rceil + 1}} 1 = \frac{|G_{\lceil t \rceil}|}{|G_0|}.$$

Hence, we have the result. □

LEMMA 6.5.24. *Let L/K be a Galois extension of fields with Galois group G, and let E/K be a Galois subextension. For every $t \geq -1$ and $\delta \in \mathrm{Gal}(E/K)$, we have*

$$i_{E/K}(\delta) - 1 = \max\{\phi_{L/E}(i_{L/K}(\sigma) - 1) \mid \sigma \in G, \sigma|_E = \delta\}.$$

PROOF. Let $N = \mathrm{Gal}(L/E)$. Let $\delta \in G/N$. Let $\sigma \in G$ with $\sigma|_E = \delta$ be such that $i = i_{L/K}(\sigma) - 1$ is maximal. Let $\beta \in \mathscr{O}_L$ be such that $\mathscr{O}_L = \mathscr{O}_K[\beta]$. For any $\tau \in N$, we have

$$i_{L/K}(\sigma\tau) = v_L(\sigma\tau(\beta) - \beta) \geq \min\{v_L(\sigma\tau(\beta) - \sigma(\beta)), v_L(\sigma(\beta) - \beta)\} = \min\{i_{L/K}(\tau), i_{L/K}(\sigma)\}$$

with equality if $i_{L/K}(\tau) \neq i_{L/K}(\sigma)$. In particular, if $\tau \notin N_i$, then $i_{L/K}(\sigma\tau) = i_{L/K}(\tau)$, and if $\tau \in N_i$, then $i_{L/K}(\sigma\tau) \geq i+1$ and then in fact equality so by maximality of i. We therefore have

$$i_{L/K}(\delta) = \frac{1}{|N_0|} \sum_{\tau \in N} i_{L/K}(\sigma\tau) = \frac{1}{|N_0|} \sum_{\tau \in N} \min\{i_{L/K}(\tau), i+1\} = \phi_{L/E}(i) + 1,$$

the first step by Lemma 6.5.22 and the last step by Lemma 6.5.23. □

The latter lemma has the following corollary.

THEOREM 6.5.25 (Herbrand's theorem). *Let L/K be a Galois extension of fields with Galois group G, let E/K be a Galois subextension, and set $N = \mathrm{Gal}(L/E)$. For any $t \geq -1$, one has*

$$(G/N)_{\phi_{L/E}(t)} = G_t N/N.$$

PROOF. Note that $\delta \in G/N$ lies in $(G/N)_{\phi_{L/E}(t)}$ if and only if $i_{E/K}(\delta) - 1 \geq \phi_{L/E}(t)$. This occurs by Lemma 6.5.24 if and only if there exists $\sigma \in G$ that restricts to δ such that

$$\phi_{L/E}(i_{L/K}(\sigma) - 1) \geq \phi_{L/E}(t)$$

and so if and only if $i_{L/K}(\sigma) - 1 \geq t$ for some such σ. In turn, this is exactly to say that $\sigma \in G_t$ for some lift $\sigma \in G$ of δ, or in other words that $\delta \in G_t N/N$. □

PROPOSITION 6.5.26. *Let L/K be a Galois extension of local fields and E a normal subextension of K in L. Then*

$$\phi_{L/K} = \phi_{E/K} \circ \phi_{L/E}.$$

PROOF. Note first that both sides agree at -1 and then that it suffices to consider the slope of both sides at non-integral values $t > -1$. Let $G = \mathrm{Gal}(L/K)$ and $N = \mathrm{Gal}(L/E)$. The derivative of the right-hand side at t is

$$\phi'_{E/K}(\phi_{L/E}(t)) \cdot \phi'_{L/E}(t) = [(G/N)_0 : (G/N)_{\phi_{L/E}(t)}]^{-1} [N_0 : N_t]^{-1}$$

and that of the left is $[G_0 : G_{\lceil t \rceil}]^{-1}$, so it suffices to note by Lemma 6.5.9 and Theorem 6.5.25 that

$$[G_s : N_s] = [G_s : G_s \cap N] = [G_s N : N] = |(G/N)_{\phi_{L/E}(s)}|$$

for $s = 0$ and $s = t$. □

Part 2

Class field theory

The goal of class field theory is to describe the structure of the Galois group of the maximal abelian extension of a field in terms of the arithmetic of the field itself.

REMARK 6.5.27. The term "class field theory" will at times be abbreviated "CFT".

CHAPTER 7

Global class field theory via ideals

In this chapter, we take the classical approach of comparing Galois groups of abelian extensions of a number field to generalizations of class groups of the field. We use zeta and L-functions in proving some of the key results.

7.1. Dedekind zeta functions

In this section, we shall be interested in the convergence of Dirichlet series.

DEFINITION 7.1.1. The *Dirichlet series* of a sequence $(a_n)_{n\geq 1}$ of complex numbers is the series

$$\sum_{n=1}^{\infty} a_n n^{-s},$$

where s is a complex variable.

The following trick can be proven by a simple induction.

LEMMA 7.1.2. *Let $(b_i)_{i\geq 1}$ and $(c_i)_{i\geq 1}$ be sequences of complex numbers. For $n \geq 1$, set $B_n = \sum_{i=1}^{n} b_i$. Then*

$$\sum_{i=1}^{n} b_i c_i = B_n c_n + \sum_{i=1}^{n-1} B_i (c_i - c_{i+1}).$$

In particular, for $n \geq m \geq 1$, we have

$$\sum_{i=m+1}^{n} b_i c_i = B_n c_n - B_m c_m + \sum_{i=m+1}^{n-1} B_i (c_i - c_{i+1})$$

PROOF. This is immediate for $n = 1$. Suppose it for n. Then the difference of the right-hand side of the above equation for $n+1$ and n is

$$B_{n+1} c_{n+1} + B_n (c_n - c_{n+1}) - B_n c_n = b_{n+1} c_{n+1},$$

as required. □

NOTATION 7.1.3. For $s_0 \in \mathbb{C}$, let $Z(s_0) = \{s \in \mathbb{C} \mid \mathrm{Re}(s) > \mathrm{Re}(s_0)\}$.

LEMMA 7.1.4. *Suppose that a Dirichlet series $\sum_{n=1}^{\infty} a_n n^{-s}$ converges at some $s_0 \in \mathbb{C}$. Then it converges for all $s \in Z(s_0)$, and it converges uniformly on every compact subset of $Z(s_0)$.*

PROOF. Let $t_0 = \mathrm{Re}(s_0)$ and $t = \mathrm{Re}(s)$ for $s \in Z(s_0)$, so $t > t_0$. For $m \geq 1$, let $D_m > 0$ be the maximum of all $|\sum_{k=1}^{n} a_k k^{-s_0}| \leq D_m$ with $n \leq m$. These are bounded by some $D > 0$ since the partial sums converge. Applying Lemma 7.1.2 to the sequences $(a_n n^{-s_0})_{n\geq 1}$ and $(n^{s_0-s})_{n\geq 1}$, we obtain

$$\left| \sum_{k=m+1}^{n} a_n n^{-s} \right| \leq D_n n^{t_0-t} + D_m m^{t_0-t} + \sum_{k=m+1}^{n-1} D_k |k^{s_0-s} - (k+1)^{s_0-s}|$$

Note that

$$|k^{s_0-s} - (k+1)^{s_0-s}| \leq |s-s_0| \int_k^{k+1} x^{t_0-t-1} dx,$$

from which it follows that

$$\sum_{k=m+1}^{n-1} D_k |k^{s_0-s} - (k+1)^{s_0-s}| \leq D_{n-1} |s-s_0| \int_{m+1}^{n-1} x^{t_0-t-1} dx$$

Taking the limit as $n \to \infty$, we obtain

$$\left| \sum_{k=m+1}^{\infty} a_n n^{-s} \right| \leq D m^{t_0-t} + |s-s_0| \int_{m+1}^{\infty} x^{t_0-t-1} dx \leq D m^{t_0-t} + \frac{|s-s_0|}{t-t_0} (m+1)^{t_0-t}.$$

Thus $\sum_{n=m+1}^{\infty} a_n n^{-s}$ approaches 0 uniformly as m increases for s in any fixed compact subset of $Z(s_0)$. □

LEMMA 7.1.5. *Let $(a_n)_{n\geq 1}$ be a sequence in $\mathbb{C}$, and suppose that $C > 0$ and $u \geq 0$ are such that $|\sum_{k=1}^{n} a_k| \leq C n^u$ for all $n \geq 1$. Then $\sum_{n=1}^{\infty} a_n n^{-s}$ converges absolutely uniformly on any compact subset of $Z(t)$.*

PROOF. For $t = \mathrm{Re}(s)$, the computation of Lemma 7.1.4 with $s_0 = 0$ and $D_n \leq C n^u$ gives

$$\left| \sum_{k=m+1}^{n} a_n n^{-s} \right| \leq C n^{u-t} + C m^{u-t} + C|s| \sum_{k=m+1}^{n-1} k^u \int_k^{k+1} x^{-t-1} dx \leq C n^{u-t} + C m^{u-t} + C|s| \int_{m+1}^{n} x^{u-t-1} dx.$$

Taking the limit as $n \to \infty$, we obtain

$$\left| \sum_{k=m+1}^{\infty} a_n n^{-s} \right| \leq C m^{u-t} + C \frac{|s|}{u-t} (m+1)^{u-t},$$

which again converges uniformly in any bounded subset of $Z(s)$. □

We give an application to the Riemann zeta function.

DEFINITION 7.1.6. The *Riemann zeta series* is the Dirichlet series

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}.$$

THEOREM 7.1.7. *The zeta series $\zeta(s)$ defines an analytic function on $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$, and it has a meromorphic continuation to $\mathrm{Re}(s) > 0$, in which region it is analytic aside from a simple pole at $s = 1$.*

PROOF. The first statement is an immediate consequence of Lemma 7.1.5, the condition of which holds for $C = 1$ and $t = 1$. Consider $\zeta_2(s) = \sum_{n=1}^{\infty}(-1)^{n-1}n^{-s}$. We can again apply Lemma 7.1.5 for $C = 1$ and $t = 0$ to see that the latter series converges uniformly and absolutely on $\mathrm{Re}(s) > 0$. Note that

$$\sum_{n=1}^{\infty}(-1)^{n-1}n^{-s} = \sum_{n=1}^{\infty}n^{-s} - 2\sum_{n=1}^{\infty}(-1)^{n-1}(2n)^{-s},$$

from which we see that $\zeta_2(s) = (1-2^{1-s})\zeta(s)$ for $s \in Z(0)$ aside from those with $2^{s-1} = 1$, i.e., those s of the form $1 + \frac{2\pi ni}{\log 2}$ for some $n \in \mathbb{Z}$. Similarly, the Dirichlet series $\zeta_3(s)$ attached to the sequence $(a_n)_{n\geq 1}$ with $a_{3k+1} = a_{3k+2} = 1$ and $a_{3k+3} = -2$ for all $k \geq 0$ converges for $\mathrm{Re}(s) > 0$ and satisfies $\zeta_3(s) = (1-3^{1-s})\zeta(s)$ on said region, aside from s with $3^{s-1} = 1$, those s of the form $1 + \frac{2\pi ni}{\log 3}$. Thus $\zeta(s)$ is analytic outside $s = 1$. Finally, we note that

$$\frac{1}{s-1} = \int_1^{\infty} x^{-s}dx \leq \sum_{n=1}^{\infty}n^{-s} \leq 1 + \int_1^{\infty} x^{-s}dx = \frac{s}{s-1}.$$

Thus, $\lim_{s\to 1}(s-1)\zeta(s) = 1$, so $\zeta(s)$ has a simple pole with residue 1 at $s = 1$. □

TERMINOLOGY 7.1.8. A product $\prod_{\mathfrak{p}}(1 - a_{\mathfrak{p}}N\mathfrak{p}^{-s})^{-1}$ over primes $\mathfrak{p}$ of a number field F for complex numbers $a_{\mathfrak{p}}$ is known as an *Euler product* for $s \in \mathbb{C}$ such that it converges. The individual term $(1 - a_{\mathfrak{p}}N\mathfrak{p}^{-s})^{-1}$ for a prime $\mathfrak{p}$ is known as an *Euler factor* at $\mathfrak{p}$.

PROPOSITION 7.1.9. *For any $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$, the Euler product $\prod_p(1-p^{-s})^{-1}$ over all primes p converges to $\zeta(s)$.*

PROOF. The logarithm of the Euler product is given by

$$\sum_{n=1}^{\infty}\sum_{p}\frac{1}{np^{ns}},$$

with the latter sum taken over all prime numbers p. For $t = \mathrm{Re}(s)$,we have

$$\sum_{n=2}^{\infty}\sum_{p}\frac{1}{np^{nt}} \leq \sum_{n=2}^{\infty}\sum_{p}p^{-nt} \leq \zeta(t),$$

so converges uniformly on an closed interval inside the interval $t > \frac{1}{2}$. In particular, the series $\sum_{n=1}^{\infty}\sum_p \frac{1}{np^{ns}}$ converges absolutely and uniformly on any compact subset of $Z(\frac{1}{2})$ on which $\sum_p p^{-s}$ does. In particular, the Euler product defines an analytic function on $Z(1)$.

We can then compare finite products and sums. Let S be a finite set of prime numbers and I_S be the semigroup they generate. Then

$$\prod_{p\in S}(1-p^{-s})^{-1} = \sum_{n\in I_S}n^{-s}.$$

We then have $\zeta(s) = \prod_p(1-p^{-s})^{-1}$ for $\mathrm{Re}(s) > 1$ by taking the limit over all S. □

NOTATION 7.1.10. For two meromorphic functions f and g on a neighborhood of $s = 1$ in $\mathbb{C}$, or which have meromorphic continuation to such a neighborhood, we write $f \sim g$ if they differ by a function analytic at 1.

We now turn to zeta functions of number fields.

DEFINITION 7.1.11. The *Dedekind zeta series* of a number field K is Dirichlet series

$$\zeta_K(s) = \sum_{\mathfrak{a} \subseteq \mathscr{O}_F} (N\mathfrak{a})^{-s},$$

where the sum runs over nonzero ideals $\mathfrak{a}$ of $\mathscr{O}_K$.

THEOREM 7.1.12. *For a number field K, the series $\zeta_K(s) = \sum_{\mathfrak{a} \subseteq \mathscr{O}_K} (N\mathfrak{a})^{-s}$ converges absolutely for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$. Moreover, for such s, we have*

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1},$$

where the product runs over all nonzero prime ideals $\mathfrak{p}$ of $\mathscr{O}_K$. It has a meromorphic continuation to $Z(1 - [K : \mathbb{Q}]^{-1})$ that is analytic outside of a simple pole at $s = 1$.

PROOF. We sketch part of the proof. Again, we consider the logarithm of the Euler product, noting that

$$\log \zeta_K(s) \sim \sum_{\mathfrak{p}} N\mathfrak{p}^{-s},$$

and the latter sum is at most $[K : \mathbb{Q}] \sum_p p^{-s} \sim [K : \mathbb{Q}] \log(s-1)^{-1}$, from which we obtain convergence of the Euler product on $Z(1)$ to an analytic function. We can then compare the Euler product over a finite sum of primes with the partial sum in the Dirichlet series over ideals divisible only by those primes to obtain equality in said region. We omit the argument regarding its meromorphic continuation and simple pole. □

From this, we obtain the following statement on the density of completely split primes.

DEFINITION 7.1.13. Let S be a set of prime ideals of a number field K. The *Dirichlet density* $\delta(S)$ of S, if it exists, is

$$\delta(S) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} N\mathfrak{p}^{-s}}{\sum_{\mathfrak{p}} N\mathfrak{p}^{-s}},$$

where the sum in the denominator is taken over all prime ideals of K. The *upper Dirichlet density* (resp., *lower Dirichlet density*) is obtained by replacing the limit in the definition of Dirichlet density with the lim inf (resp., lim sup).

THEOREM 7.1.14. *Let L/K be a Galois extension of number fields. Then the Dirichlet density of the set $S_{L/K}$ of primes of K that split completely in K is $\frac{1}{[L:K]}$.*

PROOF. As before, we have that $\log \zeta_L(s) \sim \sum_{\mathfrak{P}} N\mathfrak{P}^{-s}$. At the same time, the sum over primes that are not completely split is bounded absolutely by the finite sum over primes of degree ≥ 2 at $s = 1$, since $|N\mathfrak{P}^{-s}|$ is for such $\mathfrak{P}$ is at least p^2 for the prime p with $(p) = \mathfrak{P} \cap \mathbb{Z}$. Since each prime over K that is completely split in K has $[L : K]$ primes over it of the same absolute norm, we then have

$$\log \zeta_L(s) \sim [L : K] \sum_{\mathfrak{p} \in S_{L/K}} N\mathfrak{p}^{-s}$$

At the same time, since both $\zeta_L(s)$ and $\zeta_K(s)$ have a simple pole at $s = 1$, we have

$$\log \zeta_L(s) \sim \log(s-1)^{-1} \sim \log \zeta_K(s) \sim \sum_{\mathfrak{p}} N\mathfrak{p}^{-s},$$

and therefore $\delta(S_{L/K}) = [L : K]^{-1}$. □

We can attach a Dirichlet series to a finite-dimensional representation of a Galois extension L/K of number fields as follows.

DEFINITION 7.1.15. Let L/K be Galois, and let χ be a character of a finite-dimensional $\mathbb{C}$-representation of $\mathrm{Gal}(L/K)$. Then the *Artin L-function* of χ is Euler product expansion

$$L(\chi, s) = \prod_{\mathfrak{p}} \det(1 - x\varphi_{\mathfrak{p}} | V^{I_{\mathfrak{p}}})^{-1}|_{x = N\mathfrak{p}^{-s}}$$

on $Z(1)$, where $\varphi_{\mathfrak{p}}$ denotes a Frobenius in $\mathrm{Gal}(L/K)$ of some prime $\mathfrak{P}$ of L over $\mathfrak{p}$, and $I_{\mathfrak{p}}$ denotes the inertia group at $\mathfrak{P}$ in $\mathrm{Gal}(L/K)$.

PROPOSITION 7.1.16. *Let L/K be Galois, and let χ be a character of a finite-dimensional $\mathbb{C}$-representation of* $\mathrm{Gal}(L/K)$. *The Artin L-function $L(\chi, s)$ converges to an analytic function on* $\mathrm{Re}(s) > 1$. *In this range, we have*

$$\zeta_L(s) = \prod_{\chi} L(\chi, s)^{\chi(1)},$$

where the product is taken over the characters of irreducible representations of $\mathrm{Gal}(L/K)$.

NOTATION 7.1.17. If $\chi \colon \mathrm{Gal}(L/K) \to \mathbb{C}^\times$ is an abelian character, we view χ as the unique multiplicative function on the nonzero ideals of $\mathscr{O}_K$ such that $\chi(\mathfrak{p}) = 0$ for a prime ideal $\mathfrak{p}$ is 0 if $\mathfrak{p}$ ramifies in $L^{\ker \chi}/K$ and is $\chi(\varphi_{\mathfrak{p}})$ otherwise, where $\varphi_{\mathfrak{p}}$ is a Frobenius in $\mathrm{Gal}(L/K)$ at any prime over $\mathfrak{p}$.

PROPOSITION 7.1.18. *Let $\chi \colon \mathrm{Gal}(L/K) \to \mathbb{C}^\times$ be an abelian character of a Galois extension L/K of number fields. Then*

$$L(\chi, s) = \prod_{\mathfrak{p}} (1 - \chi(\mathfrak{p}) N\mathfrak{p}^{-s})^{-1} = \sum_{\mathfrak{a} \subseteq \mathscr{O}_K} \chi(\mathfrak{a}) N\mathfrak{a}^{-s}$$

for $\mathrm{Re}(s) > 1$.

For χ abelian, it is known that $L(\chi,s)$ is analytic on $\mathbb{C}$ (outside of a simple pole at $s=1$ if χ is trivial), but we require only something weaker. We provide a proof of the following result, assuming an input from the geometry of numbers.

PROPOSITION 7.1.19. *Let L/K be an abelian extension of number fields, let $m \geq 1$, and let χ be a nontrivial, irreducible character of* $\mathrm{Gal}(L/K)$. *Then $L(\chi,s)$ has a unique analytic extension to $Z(1-[K:\mathbb{Q}]^{-1})$, and $L(\chi,1)$ is nonzero.*

PROOF. Let $n \geq 2$ be the order of χ, fix an nth root of unity ζ, and let $d = [K:\mathbb{Q}]$. The geometry of numbers can be used to show that the number of ideals $\mathfrak{a}$ of $\mathscr{O}_K$ with $N\mathfrak{a} \leq N$ for $N \geq 1$ and $\chi(\mathfrak{a}) = \zeta$ is $CN + O(N^{1-d^{-1}})$, where C is a constant independent of ζ. Given this, we note that

$$\sum_{N\mathfrak{a} \leq N} \chi(\mathfrak{a}) = \sum_{\zeta \in \mu_n} |\{N\mathfrak{a} \leq N \mid \chi(\mathfrak{a}) = \zeta\}|\zeta = \sum_{\zeta \in \mu_n} \zeta \cdot CN + O(N^{1-d^{-1}}) = O(N^{1-d^{-1}}).$$

By Lemma 7.1.5, we therefore have that $\sum_{\mathfrak{a} \subset \mathscr{O}_K} \chi(\mathfrak{a}) N\mathfrak{a}^{-s}$ converges absolutely and uniformly on every compact subset of $Z(1-d^{-1})$.

For the nonvanishing, write $\log \zeta_L(t) = \sum_\chi \log L(\chi,t)$ and observe that, up to a bounded function as $t \to 1^+$, the latter sum has absolute value at least $(1 - \sum_\chi m_\chi)\log(t-1)^{-1}$, where m_χ is the order of vanishing of $L(\chi,s)$ at $s=1$. But if some $m_\chi \geq 1$, then $1 - \sum_\chi m_\chi \leq 0$, which is impossible since $\log \zeta_L(s) \sim \log(s-1)^{-1}$. □

7.2. Chebotarev density theorem

We prove Chebotarev's density theorem in something close to the original manner in which it was proven, roughly following an exposition of Stevenhagen and Lenstra.

PROPOSITION 7.2.1. *Let K be a number field, $m \geq 1$, and $G = \mathrm{Gal}(K(\mu_m)/K)$. For $\sigma \in G$, the Dirichlet density of primes $\mathfrak{p}$ of K with Frobenius σ in G is $\frac{1}{|G|}$.*

PROOF. From Proposition 7.1.16 and Proposition 7.1.19, it follows that

$$\zeta_L(s) = \prod_{\chi\colon G \to \mathbb{C}^\times} L(\chi,s)$$

for $\mathrm{Re}(s) > 1 - [L:\mathbb{Q}]^{-1}$. For a prime $\mathfrak{p}$ of K unramified in L, we have that $\varphi_\mathfrak{p}(\zeta_m) = \zeta_m^{N\mathfrak{p}}$ for a primitive mth root of unity ζ_m, and therefore $\chi(\varphi_\mathfrak{p})$ depends only on $N\mathfrak{p}$ modulo $\mathfrak{m}$.

Much as before, we have

$$\log L(\chi,s) \sim \sum_\mathfrak{p} \chi(\mathfrak{p}) N\mathfrak{p}^{-s}$$

for $\mathrm{Re}(s) > 1$. Given $\sigma \in \mathrm{Gal}(F(\mu_m)/F)$ with $\sigma(\zeta_m) = \zeta_m^a$ for some a prime to m, we have

$$\sum_{\chi\colon G \to \mathbb{C}^\times} \chi(\sigma)\chi(\mathfrak{p})^{-1} = \begin{cases} 0 & \text{if } a \not\equiv N\mathfrak{p} \bmod m, \\ |G| & \text{otherwise.} \end{cases}$$

Now, on the one hand we have

$$\sum_{\chi}\chi(\sigma)^{-1}\log L(\chi,s)\sim\sum_{\chi}\sum_{\mathfrak{p}}\chi(\sigma)^{-1}\chi(\mathfrak{p})N\mathfrak{p}^{-s}\sim|G|\sum_{N\mathfrak{p}\equiv a \bmod m}N\mathfrak{p}^{-s},$$

whereas on the other we have

$$\sum_{\chi}\chi(\sigma)^{-1}\log L(\chi,s)\sim\log\zeta_K(s)\sim\log(s-1)^{-1},$$

since we know that $L(\chi,1)\neq 0$ for all nontrivial χ. Comparing the two equations, we obtain that the Dirichlet density of $\mathfrak{p}$ with $\varphi_{\mathfrak{p}}=\sigma$ is $1/|G|$ □

THEOREM 7.2.2 (Chebotarev). *Let L/K be a Galois extension of number fields with Galois group G. Let C be a conjugacy class in G. The Dirichlet density of prime ideals $\mathfrak{p}$ of K such that the conjugacy class in G of a Frobenius of a prime over $\mathfrak{p}$ in L lies in C is $\frac{|C|}{|G|}$.*

PROOF. With Proposition 7.2.1 already in hand, we divide the remainder of the proof into two steps.

Step 1. First, we shall show that the theorem for L/K and C follows from the theorem for a cyclic subextension L/E, where E is the fixed field of an element of C. Let S be the set of prime ideals of K unramified in L with class C. Let $\sigma\in C$ and $E=K^{\langle\sigma\rangle}$ so that L/E is cyclic of degree $f=|\langle\sigma\rangle|$. Note that the latter order is independent of σ.

Let T_σ be the set of primes P of E unramified in L and over K with Frobenius φ_P at a prime of L over P equal to σ. If $P\in T_\sigma$, then $\varphi_P=\sigma$ fixes E, so P has degree one over F. As P is by definition inert in L, there are exactly $|G|/f$ primes of L over $P\cap K$. As the Frobenius elements of such primes are distributed evenly among the elements of the conjugacy class C of σ, exactly $|G|/f|C|$ of these have Frobenius σ.

We may then compute the Dirichlet density of S:

$$\delta(S)=\lim_{s\to1^+}\frac{\sum_{\mathfrak{p}\in S}N\mathfrak{p}^{-s}}{\sum_{\mathfrak{p}}N\mathfrak{p}^{-s}}=\frac{f|C|}{|G|}\lim_{s\to1^+}\frac{\sum_{P\in T_\sigma}NP^{-s}}{\sum_{\mathfrak{p}}N\mathfrak{p}^{-s}}=\frac{f|C|}{|G|}\delta(T_\sigma),$$

recalling once again that $\sum_{\mathfrak{p}}N\mathfrak{p}^{-s}\sim\sum_P NP^{-s}$. Supposing the theorem for K/E, we have $\delta(T_\sigma)=\frac{1}{f}$, and we therefore obtain $\delta(S)=\frac{|C|}{|G|}$, as desired.

Step 2. It remains to prove the theorem for cyclic extensions, and we shall actually make the weaker hypothesis that L/K is abelian. Choose $m\geq1$ not dividing the discriminant of L so that $H=\mathrm{Gal}(L(\mu_m)/L)$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$ via the mod m cyclotomic character, and $\mathrm{Gal}(L(\mu_m)/K)\cong G\times H$. For $\sigma\in G$ and $\tau\in H$, let S_σ be the set of primes of K unramified in L with Frobenius σ in G, and let $S_{\sigma,\tau}$ be the set of primes of K unramified in $L(\mu_m)$ with Frobenius $(\sigma,\tau)\in G\times H$. Then

$$\delta_{\inf}(S_\sigma)=\sum_{\tau\in H}\delta_{\inf}(S_{\sigma,\tau}).$$

Now suppose that $|G|$ divides the order of τ. Then $\langle(\sigma,\tau)\rangle \cap (G \times \{1\}) = 1$, which implies that $L(\mu_m)$ is given by adjoining μ_m to $F = K(\mu_m)^{\langle(\sigma,\tau)\rangle}$. Since we have previously shown the theorem for cyclotomic extensions such as $F(\mu_m)/F$, we have that the Dirichlet density of the set of unramified primes in this extension with Frobenius (σ,τ) is $\frac{1}{|\langle\tau\rangle|}$. From the argument of Step 1, we see that $\delta(S_{\sigma,\tau})$ exists and equals $\frac{1}{|G||H|}$.

Now let H_n be the set of elements $\tau \in H$ of order divisible by n. By summing over all $\tau \in H_n$, we see that $\delta_{\inf}(S_\sigma) \geq \frac{|H_n|}{|G||H|}$. Write $n = p_1^{k_1} \cdots p_r^{k_r}$ for distinct primes $p_1, \ldots, p_r$ and $k_1, \ldots, k_r \geq 1$. There exists a prime $m \equiv 1 \bmod n^j$, since the Dirichlet density of completely split primes in $\mathbb{Q}(\mu_{n^j})/\mathbb{Q}$ is positive. For such an m, let $j_i = v_{p_i}(m-1) \geq j$. We then have

$$\frac{|H_n|}{|H|} = \prod_{i=1}^{r} \left(1 - \frac{p_i^{k_i-1}}{p^{j_i k_i}}\right) \geq \prod_{i=1}^{r} \left(1 - \frac{1}{p^{(j-1)k_i+1}}\right).$$

so $\frac{|H_n|}{|H|}$ tends to 1 as j increases. It follows that $\delta_{\inf}(S_\sigma) \geq \frac{1}{|G|}$. Since the sum of these over all $\sigma \in G$ is then at least 1, it must equal 1. Thus, we have that $\delta(S_\sigma)$ exists and equals $\frac{1}{|G|}$. □

As a consequence, we obtain Dirichlet's theorem on primes in arithmetic progressions.

COROLLARY 7.2.3 (Dirichlet). *For $n \geq 1$ and $a \in \mathbb{Z}_{\geq 1}$ with $\gcd(a,n) = 1$, the set $\{a + kn \mid k \geq 0\}$ contains infinitely many prime numbers. In fact, the Dirichlet density of the set of such primes is $\frac{1}{\varphi(n)}$.*

PROOF. The prime numbers with Frobenius φ in $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ satisfying $\varphi(\zeta_n) = \zeta_n^a$ for a primitive nth root of unity ζ_n are exactly those in the arithmetic progression in question. Chebotarev's theorem then tells us that the Dirichlet density is the reciprocal of the degree $\varphi(n)$, as the extension is abelian. □

7.3. Ray class groups

Let us fix a number field K.

DEFINITION 7.3.1. A *modulus* $\mathfrak{m}$ for K is a formal product $\mathfrak{m} = \mathfrak{m}_f \mathfrak{m}_\infty$ consisting of a nonzero ideal $\mathfrak{m}_f$ of $\mathcal{O}_K$ and a formal product $\mathfrak{m}_\infty$ of distinct real places of K. We refer to $\mathfrak{m}_f$ and $\mathfrak{m}_\infty$ as the finite and infinite parts of $\mathfrak{m}$, respectively.

REMARK 7.3.2. A formal product of symbols is a tuple (or list) of symbols, written in product notation.

REMARK 7.3.3. In a modulus $\mathfrak{m}$, the product composing $\mathfrak{m}_\infty$ can be empty, in which case we simply write $\mathfrak{m} = \mathfrak{m}_f$.

We may define a notion of congruence modulo $\mathfrak{m}$.

DEFINITION 7.3.4. Let $\mathfrak{m}$ be a modulus for K. We say that $a, b \in K^\times$ are *congruent modulo* $\mathfrak{m}$, and write

$$a \equiv^* b \bmod \mathfrak{m}$$

if $a \equiv b \bmod \mathfrak{m}_f$ and the image of a/b is positive under the real embedding attached to any real place in the formal product $\mathfrak{m}_\infty$.

We may now define ray class groups.

DEFINITION 7.3.5. Let $\mathfrak{m} = \mathfrak{m}_f\mathfrak{m}_\infty$ be a modulus for a number field K.

a. The $\mathfrak{m}$-*ideal group* $I_K^\mathfrak{m}$ is the subgroup of the ideal group I_K generated by the nonzero prime ideals of $\mathscr{O}_K$ that do not divide $\mathfrak{m}_f$.

b. The *unit group* at $\mathfrak{m}$ in K is the subgroup $K_\mathfrak{m}$ of $K^\times$ defined by

$$K_\mathfrak{m} = \{a \in K^\times \mid v_\mathfrak{p}(a) = 0 \text{ for all primes } \mathfrak{p} \mid \mathfrak{m}_f\}.$$

c. The *ray modulo* $\mathfrak{m}$ in K is the subgroup $K_{\mathfrak{m},1}$ of $K^\times$ consisting of elements congruent to 1 modulo $\mathfrak{m}$: that is,

$$K_{\mathfrak{m},1} = \{a \in K^\times \mid a \equiv^* 1 \bmod \mathfrak{m}\}.$$

d. The *principal* $\mathfrak{m}$-*ideal group* $P_K^\mathfrak{m}$ is the subgroup of fractional ideals of $\mathscr{O}_K$ generated by elements of $K_{\mathfrak{m},1}$.

e. The *ray class group* $\mathrm{Cl}_K^\mathfrak{m}$ *of* K *of modulus* $\mathfrak{m}$ is the quotient group

$$\mathrm{Cl}_K^\mathfrak{m} = I_K^\mathfrak{m}/P_K^\mathfrak{m}.$$

f. The *ray class* $[\mathfrak{a}]_\mathfrak{m}$ for the modulus $\mathfrak{m}$ of a fractional ideal $\mathfrak{a} \in I_K^\mathfrak{m}$ is the image of $\mathfrak{a}$ in $\mathrm{Cl}_K^\mathfrak{m}$.

REMARK 7.3.6. The reason for the term "ray" is surely as follows. The ray $\mathbb{Q}_{\infty,1}$, where ∞ is the unique real prime of $\mathbb{Q}$, is equal to the set of positive rational numbers, which is dense in the ray $[0,\infty)$ in $\mathbb{R}$.

EXAMPLE 7.3.7. The class group of K is in fact the ray class group with modulus (1). That is, taking $\mathfrak{m} = (1)$, we have $I_K^\mathfrak{m} = I_K$ and $K_{\mathfrak{m},1} = K^\times$, so $P_K^\mathfrak{m} = P_K$ and $\mathrm{Cl}_K^\mathfrak{m} = \mathrm{Cl}_K$.

REMARK 7.3.8. For any modulus $\mathfrak{m}$, we have the map $I_K^\mathfrak{m} \to \mathrm{Cl}_K$ that takes an ideal to its class. Despite the fact that $I_K^\mathfrak{m}$ is not the full ideal group of K unless $\mathfrak{m}_f = (1)$, this map is still surjective, with kernel the principal fractional ideals in $I_K^\mathfrak{m}$. To see this, first note that any fractional ideal of $\mathscr{O}_K$ is a principal fractional ideal times an integral ideal $\mathfrak{a}$, and the Chinese remainder theorem tells us that we can find an element $a \in \mathscr{O}_K$ with exactly the same $\mathfrak{p}$-adic valuation as the maximal power of $\mathfrak{p}$ dividing $\mathfrak{a}$ for each $\mathfrak{p}$ dividing $\mathfrak{m}_f$. Then $\mathfrak{a}(a^{-1}) \in I_K^\mathfrak{m}$ has the same class of the original fractional ideal.

From now on, let us fix a modulus $\mathfrak{m}$ for K. The following is immediate from the definitions.

PROPOSITION 7.3.9. *We have an exact sequence*

$$1 \to \mathscr{O}_K^\times \cap K_{\mathfrak{m},1} \to K_{\mathfrak{m},1} \xrightarrow{\phi} I_K^{\mathfrak{m}} \to \mathrm{Cl}_K^{\mathfrak{m}} \to 0,$$

where $\phi\colon K^\times \to I_K$ *takes an element to the fractional ideal it generates. In particular, we have* $\phi(K_{\mathfrak{m},1}) = P_K^{\mathfrak{m}}$.

We also have an exact sequence as in the following proposition.

PROPOSITION 7.3.10. *There is an exact sequence*

$$1 \to \mathscr{O}_K^\times/(\mathscr{O}_K^\times \cap K_{\mathfrak{m},1}) \to K_{\mathfrak{m}}/K_{\mathfrak{m},1} \to \mathrm{Cl}_K^{\mathfrak{m}} \to \mathrm{Cl}_K \to 0,$$

where the first map is induced by the identity map on $K^\times$*, the second is induced by the map that takes an element to its* $\mathfrak{m}$*-ray ideal class, and the last is the quotient by* P_K.

PROOF. Since $\mathrm{Cl}_K^{\mathfrak{m}} = I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$. We saw in Remark 7.3.8 that the natural map $I_K^{\mathfrak{m}} \to \mathrm{Cl}_K$ is surjective with kernel $P_K \cap I_K^{\mathfrak{m}}$. Moreover, the natural map

$$K_{\mathfrak{m}} \to (P_K \cap I_K^{\mathfrak{m}})/P_K^{\mathfrak{m}},$$

is by definition surjective. Since the elements of $K_{\mathfrak{m}}$ that generate classes in $P_K^{\mathfrak{m}}$ are those in $\mathscr{O}_K^\times K_{\mathfrak{m},1}$, we have the result. □

We also have the following.

PROPOSITION 7.3.11. *The product of reduction modulo* $\mathfrak{m}_f$ *and the sign maps for each of the* r *real places dividing* $\mathfrak{m}_\infty$ *induces a canonical isomorphism*

$$K_{\mathfrak{m}}/K_{\mathfrak{m},1} \xrightarrow{\sim} (\mathscr{O}_K/\mathfrak{m}_f)^\times \times \prod_{i=1}^{r} \langle -1 \rangle.$$

PROOF. The kernel of the reduction modulo $\mathfrak{m}_f$ map on $K_{\mathfrak{m}}$ is $K_{\mathfrak{m}_f,1}$ and those elements of $K_{\mathfrak{m}_f,1}$ with trivial sign at all real places dividing $\mathfrak{m}_\infty$ constitute $K_{\mathfrak{m},1}$. Therefore, we have an injective map as in the statement. That this map is surjective is an immediate corollary of weak approximation. □

The following is immediate from the exact sequence in Proposition 7.3.10, noting the finiteness of the class group and the finiteness of $K_{\mathfrak{m}}/K_{\mathfrak{m},1}$ implied by Proposition 7.3.11.

COROLLARY 7.3.12. *The ray class group* $\mathrm{Cl}_K^{\mathfrak{m}}$ *is finite.*

EXAMPLE 7.3.13. Let us consider the ray class groups of $\mathbb{Q}$. Recall that $\mathrm{Cl}_{\mathbb{Q}} = (1)$ and that $\mathbb{Z}^\times = \langle -1 \rangle$. We will consider two cases for an $f \geq 1$: (i) $\mathfrak{m} = (f)$ and (ii) $\mathfrak{m} = (f)\infty$.

i. We have

$$\mathbb{Q}_{(f)}/\mathbb{Q}_{(f),1} \cong (\mathbb{Z}/f\mathbb{Z})^\times,$$

and if $f \geq 3$ so that this group is nontrivial, then $-1 \notin \mathbb{Q}_{(f),1}$. Propositions 7.3.10 and 7.3.11 then tell us for any f that we have an isomorphism

$$\phi'_f \colon \mathrm{Cl}_{\mathbb{Q}}^{(f)} \xrightarrow{\sim} (\mathbb{Z}/f\mathbb{Z})^\times/\langle -1\rangle.$$

with $\phi'_f([(a)]_{(f)})$ the image of a for any $a \in \mathbb{Z}$ relatively prime to f.

ii. We have

$$\mathbb{Q}_{(f)\infty}/\mathbb{Q}_{(f)\infty,1} \cong (\mathbb{Z}/f\mathbb{Z})^\times \times \langle -1\rangle,$$

and $-1 \notin \mathbb{Q}_{(f)\infty,1}$. Again by Propositions 7.3.10 and 7.3.11, we then have an exact sequence

$$0 \to \langle -1\rangle \to (\mathbb{Z}/f\mathbb{Z})^\times \times \langle -1\rangle \to \mathrm{Cl}_{\mathbb{Q}}^{(f)\infty} \to 0,$$

where the first map takes -1 to $(-1,-1)$. It follows that we have an isomorphism

$$\phi_f \colon \mathrm{Cl}_{\mathbb{Q}}^{(f)\infty} \xrightarrow{\sim} (\mathbb{Z}/f\mathbb{Z})^\times$$

with $\phi_f([(a)]_{(f)\infty}) = a \bmod f$ for $a \in \mathbb{Z}$ relatively prime to f.

We next show that norm maps descend to ray class groups.

LEMMA 7.3.14. *Let L/K be a finite extension of number fields and $\mathfrak{m}$ a modulus for K. Then*

$$N_{L/K}(L_{\mathfrak{m},1}) \subseteq K_{\mathfrak{m},1}.$$

PROOF. Let $\alpha \in L_{\mathfrak{m},1}$. We have that $N_{L/K}(\alpha)$ is the product of the $\tau(\alpha)$ over all embeddings τ of L fixing K in our fixed algebraic closure of K. Since the ideal $\mathfrak{m}_f$ of $\mathscr{O}_K$ is fixed under these embeddings, we have $N_{L/K}\alpha \equiv 1 \bmod \mathfrak{m}_f$.

As for the infinite part, if $\sigma \colon K \to \mathbb{R}$ corresponds to a place dividing $\mathfrak{m}_\infty$ and S is the set of embeddings $\tau \colon L \to \mathbb{C}$ extending σ, then

$$\sigma(N_{L/K}\alpha) = \prod_{\tau \in S} \tau(\alpha).$$

If $\tau \in S$ is real, then $\alpha \in L_{\mathfrak{m},1}$ tells us that $\tau(\alpha) > 0$. If $\tau \in S$ is complex, then the complex conjugate embedding $\bar{\tau}$ is also in S, and

$$\tau(\alpha)\bar{\tau}(\alpha) = |\tau(\alpha)|^2 > 0.$$

As a product of positive numbers, $\sigma(N_{L/K}\alpha)$ is positive. □

DEFINITION 7.3.15. Let L/K be a finite extension of number fields and $\mathfrak{m}$ a modulus for K. The *norm map* $N_{L/K} \colon \mathrm{Cl}_L^{\mathfrak{m}} \to \mathrm{Cl}_K^{\mathfrak{m}}$ is the map defined on $\mathfrak{a} \in I_K^{\mathfrak{m}}$ by

$$N_{L/K}([\mathfrak{a}]_{\mathfrak{m}}) = [N_{L/K}(\mathfrak{a})]_{\mathfrak{m}},$$

where $N_{L/K}(\mathfrak{a})$ is the norm from L to K of $\mathfrak{a}$.

Let us prove what is known as the first fundamental inequality of global class field theory.

PROPOSITION 7.3.16. *Let L/K be a finite abelian extension of number fields. For any modulus $\mathfrak{m}$ of K divisible by the primes that ramify in L/K, we have*

$$[\mathrm{Cl}_K^{\mathfrak{m}} : N_{L/K}\mathrm{Cl}_L^{\mathfrak{m}}] \leq [L:K].$$

PROOF. Let $H = I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}N_{L/K}I_L^{\mathfrak{m}}$, and let Let $\chi\colon H \to \mathbb{C}^\times$ be a nontrivial character. Much as with nontrivial characters of $\mathrm{Gal}(L/K)$, we can define an L-function

$$L_{\mathfrak{m}}(\chi,s) = \prod_{\mathfrak{p}\nmid\mathfrak{m}}(1-\chi(\mathfrak{p})N\mathfrak{p}^{-s})^{-1} = \sum_{\substack{\mathfrak{a}\subseteq\mathscr{O}_K \\ \mathfrak{a}+\mathfrak{m}=\mathscr{O}_K}} \chi(\mathfrak{a})N\mathfrak{a}^{-s}$$

which converges to an analytic function on $Z(1-[K:\mathbb{Q}]^{-1})$. Let m_χ be its order of vanishing at $s=1$. On the one hand, we have

$$\log\zeta_K(s) + \sum_{\chi\neq 1}\log L_{\mathfrak{m}}(\chi,s) \sim \left(1-\sum_{\chi} m_\chi\right)\log(s-1)^{-1},$$

while on the other hand, we have

$$\log\zeta_K(s) + \sum_{\chi\neq 1}\log L_{\mathfrak{m}}(\chi,s) \sim \sum_{\chi}\sum_{A\in H}\chi(A)\sum_{\mathfrak{p}\in A}N\mathfrak{p}^{-s} \sim |H|\sum_{\mathfrak{p}\in P_K^{\mathfrak{m}}N_{L/K}I_L^{\mathfrak{m}}}N\mathfrak{p}^{-s}.$$

As the primes $\mathfrak{p}$ which are norms from L/K and unramified are the completely split primes $S_{L/K}$, the latter sum is, up to a constant (the sum of the reciprocals of the ramified primes), at least

$$|H|\sum_{\mathfrak{p}\in S_{L/K}}N\mathfrak{p}^{-s} = \frac{|H|}{[L:K]}\log(s-1)^{-1},$$

employing Theorem 7.1.14. We therefore have that every m_χ is zero and $1 \geq \frac{|H|}{[L:K]}$, which is what we aimed to show. □

As we shall see later, the first fundamental inequality is actually an equality.

7.4. Statements

DEFINITION 7.4.1. Let K be a number field and $\mathfrak{m}$ a modulus for K. Let L be a finite abelian extension of K such that every place of K that ramifies in L/K divides $\mathfrak{m}$. The *Artin map* for L/K with modulus $\mathfrak{m}$ is the unique homomorphism

$$\Psi_{L/K}^{\mathfrak{m}}\colon I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$$

such that $\Psi_{L/K}^{\mathfrak{m}}(\mathfrak{p})$ is the unique Frobenius element at $\mathfrak{p}$ in $\mathrm{Gal}(L/K)$ for every nonzero prime ideal $\mathfrak{p}$ of $\mathscr{O}_K$ that does not divide $\mathfrak{m}_f$.

REMARKS 7.4.2.

a. The Artin map $\Psi^{\mathfrak{m}}_{L/K}$ is well-defined. To see this, note that $I^{\mathfrak{m}}_K$ is freely generated by the prime ideals of $\mathscr{O}_K$ not dividing $\mathfrak{m}_f$, so it suffices to define it on these primes. Moreover, L/K is abelian and unramified at any such prime $\mathfrak{p}$, so there is a unqiue Frobenius element in $\mathrm{Gal}(L/K)$ at $\mathfrak{p}$. This Frobenius element is often written $(\mathfrak{p}, L/K)$.

b. For any two moduli $\mathfrak{m}$ and $\mathfrak{m}'$ for K such that every prime that ramifies in L divide both $\mathfrak{m}_f$ and $\mathfrak{m}'_f$, the Artin maps $\Psi^{\mathfrak{m}}_{L/K}$ and $\Psi^{\mathfrak{m}'}_{L/K}$ agree on the fractional ideals on which they are both defined.

NOTATION 7.4.3. Given a modulus $\mathfrak{m}$ for K and a finite extension K'/K, we use $\mathfrak{m}$ also to denote the modulus $\mathfrak{m}'$ for K' with $\mathfrak{m}'_f = \mathfrak{m}_f \mathscr{O}_{K'}$ and $\mathfrak{m}'_\infty$ the product of the real places of K' lying over those of K that divide $\mathfrak{m}_\infty$.

Artin maps satisfy the following compatibilities, analogous to the case of the local reciprocity map.

PROPOSITION 7.4.4. *Let K be a number field, and let K'/K be a finite extension. Let $\mathfrak{m}$ be a modulus for K. Let L' be a finite abelian extension of K' such that every place of K' that ramifies in L'/K' divides $\mathfrak{m}$, and set $L = L' \cap K^{\mathrm{ab}}$. Then we have the following commutative diagrams:*

a.

$$\begin{array}{ccc} I^{\mathfrak{m}}_{K'} & \xrightarrow{\Psi^{\mathfrak{m}}_{L'/K'}} & \mathrm{Gal}(L'/K') \\ {\scriptstyle N_{K'/K}}\downarrow & & \downarrow{\scriptstyle R_{L/K}} \\ I^{\mathfrak{m}}_K & \xrightarrow{\Psi^{\mathfrak{m}}_{L/K}} & \mathrm{Gal}(L/K), \end{array}$$

where $R_{L/K}$ denotes the restriction map on Galois groups,

b.

$$\begin{array}{ccc} I^{\mathfrak{m}}_K & \xrightarrow{\Psi^{\mathfrak{m}}_{L/K}} & \mathrm{Gal}(L/K) \\ \downarrow & & \downarrow{\scriptstyle V_{K'/K}} \\ I^{\mathfrak{m}}_{K'} & \xrightarrow{\Psi^{\mathfrak{m}}_{L'/K'}} & \mathrm{Gal}(L'/K') \end{array}$$

if L'/K is Galois, where the map $I^{\mathfrak{m}}_K \hookrightarrow I^{\mathfrak{m}}_{K'}$ is the natural injection and $V_{K'/K}\colon \mathrm{Gal}(L/K) \to \mathrm{Gal}(L'/K')$ is the transfer map, and

c.

$$\begin{array}{ccc} I^{\mathfrak{m}}_K & \xrightarrow{\Psi^{\mathfrak{m}}_{L/K}} & \mathrm{Gal}(L/K) \\ {\scriptstyle \sigma}\downarrow & & \downarrow{\scriptstyle \sigma^*} \\ I^{\sigma(\mathfrak{m})}_{\sigma(K)} & \xrightarrow{\Psi^{\sigma(\mathfrak{m})}_{\sigma(L)/\sigma(K)}} & \mathrm{Gal}(\sigma(L)/\sigma(K)), \end{array}$$

where σ is an automorphism of the separable closure of K and σ^* is the map $\sigma^*(\tau) = \sigma|_L \circ \tau \circ \sigma^{-1}|_{\sigma(L)}$, and where $\sigma(\mathfrak{m})$ is the modulus for $\sigma(K)$ given by $\sigma(\mathfrak{m})_f = \sigma(\mathfrak{m}_f)$ and $\sigma(\mathfrak{m}_\infty)$ is the product of the applications of σ to the real places dividing $\mathfrak{m}_\infty$.

PROOF. We verify only part (a). It suffices to check commutativity on a prime ideal $\mathfrak{P}$ of $\mathscr{O}_{K'}$ that does not divide $\mathfrak{m}$. In this case, $\Psi^{\mathfrak{m}}_{L'/K'}(\mathfrak{P})$ is the Frobenius $(\mathfrak{P}, L'/K')$ and $\mathfrak{P}$, and its restriction to $\mathrm{Gal}(L/K)$ is $(\mathfrak{p}, L/K)^{f_{\mathfrak{P}/\mathfrak{p}}}$, where $\mathfrak{p} = \mathfrak{P} \cap \mathscr{O}_K$. On the other hand,

$$N_{K'/K}\mathfrak{P} = \mathfrak{p}^{f_{\mathfrak{P}/\mathfrak{p}}},$$

and $\Psi^{\mathfrak{m}}_{L/K}$ sends this to $(\mathfrak{p}, L/K)^{f_{\mathfrak{P}/\mathfrak{p}}}$, so we are done. □

Note the following corollary.

COROLLARY 7.4.5. *Let K be a number field, and let L/K be a finite abelian extension. Let $\mathfrak{m}$ be modulus for K that is divisible by every place of K that ramifies in L/K. Then* $\ker \Psi^{\mathfrak{m}}_{L/K}$ *contains* $N_{L/K} I^{\mathfrak{m}}_L$.

PROOF. Take $K' = L' = L$ in Proposition 7.4.4. Then the commutativity of the diagram in part (a) therein forces $\Psi^{\mathfrak{m}}_{L/K} \circ N_{L/K} = 0$ on $I^{\mathfrak{m}}_L$. □

REMARK 7.4.6. Let K be a number field. We may speak of a formal product of places dividing another such formal product in the obvious manner. Therefore, we say that a modulus $\mathfrak{m}$ for K divides a modulus $\mathfrak{n}$ for K if the divisibility occurs as formal products of places.

DEFINITION 7.4.7. Let L/K be an abelian extension of number fields. A *defining modulus* for L/K is a modulus for K that is divisible by the ramified places in L/K and is such that $P^{\mathfrak{m}}_K \subseteq \ker \Psi^{\mathfrak{m}}_{L/K}$.

Given a modulus $\mathfrak{m}$ for an extension L/K of number fields, the reciprocity map induces a reciprocity map on the ray class group.

DEFINITION 7.4.8. Let L/K be an abelian extension of number fields and $\mathfrak{m}$ a defining modulus for L/K. Then the map

$$\psi^{\mathfrak{m}}_{L/K} \colon \mathrm{Cl}^{\mathfrak{m}}_K \to \mathrm{Gal}(L/K)$$

induced by $\Psi^{\mathfrak{m}}_{L/K}$ in the sense that

$$\psi^{\mathfrak{m}}_{L/K}([\mathfrak{a}]_{\mathfrak{m}}) = \Psi^{\mathfrak{m}}_{L/K}(\mathfrak{a})$$

for every $\mathfrak{a} \in I^{\mathfrak{m}}_K$ is also referred to as the *the Artin reciprocity map* for L/K (on $\mathrm{Cl}^{\mathfrak{m}}_K$) with modulus $\mathfrak{m}$.

REMARK 7.4.9. When the defining modulus $\mathfrak{m}$ for L/K is understood, we may at times denote $\psi^{\mathfrak{m}}_{L/K}$ more simply by $\psi_{L/K}$.

REMARK 7.4.10. If L/K is a finite abelian extension with defining modulus $\mathfrak{m}$ and E is a subextension, then $\mathfrak{m}$ is a defining modulus for E as well.

Let us state the main theorems of global class field theory. The first is due to Emil Artin.

THEOREM 7.4.11 (Artin reciprocity). *Every abelian extension L/K of number fields has a defining modulus $\mathfrak{m}$ divisible exactly by the places of K that ramify in L. Moreover, $\psi_{L/K}^{\mathfrak{m}}$ is surjective with kernel $N_{L/K}(\mathrm{Cl}_L^{\mathfrak{m}})$, so induces an isomorphism*

$$\mathrm{Cl}_K^{\mathfrak{m}}/N_{L/K}(\mathrm{Cl}_L^{\mathfrak{m}}) \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

The following is due to Teiji Takagi, building on work of Heinrich Weber.

THEOREM 7.4.12 (Existence theorem of global CFT). *Let K be a number field, let $\mathfrak{m}$ be a modulus for K, and let H be a subgroup of $\mathrm{Cl}_K^{\mathfrak{m}}$. Then there exists a (unique) finite abelian extension L of K with defining modulus $\mathfrak{m}$ such that $H = N_{L/K}\mathrm{Cl}_L^{\mathfrak{m}}$.*

In other words, every subgroup of $\mathrm{Cl}_K^{\mathfrak{m}}$ for a number field K and modulus $\mathfrak{m}$ is the norm group $N_{L/K}\mathrm{Cl}_L^{\mathfrak{m}}$ from a single finite abelian extension L of K. We have written "unique" in parentheses in the theorem, as it is sometimes excluded from the statement of the existence theorem.

PROPOSITION 7.4.13. *Let K be a number field and $\mathfrak{m}$ a modulus for K. For finite abelian extensions L and M of K for which $\mathfrak{m}$ is a defining modulus, we have the following:*

a. $N_{L/K}\mathrm{Cl}_L^{\mathfrak{m}} \cap N_{M/K}\mathrm{Cl}_M^{\mathfrak{m}} = N_{LM/K}\mathrm{Cl}_{LM}^{\mathfrak{m}}$ *(and $\mathfrak{m}$ is a defining modulus for LM),*

b. $N_{L/K}\mathrm{Cl}_L^{\mathfrak{m}} \cdot N_{M/K}\mathrm{Cl}_M^{\mathfrak{m}} = N_{(L\cap M)/K}\mathrm{Cl}_{L\cap M}^{\mathfrak{m}}$, *and*

c. $N_{M/K}\mathrm{Cl}_M^{\mathfrak{m}} \subseteq N_{L/K}\mathrm{Cl}_L^{\mathfrak{m}}$ *if and only if $L \subseteq M$.*

DEFINITION 7.4.14. Let K be a number field and $\mathfrak{m}$ a modulus for K. The *ray class field* for K with modulus $\mathfrak{m}$ is the unique finite abelian extension L of K with modulus $\mathfrak{m}$ such that $\mathfrak{m}$ is a defining modulus for L/K and the Artin map $\psi_{L/K}^{\mathfrak{m}}$ is an isomorphism.

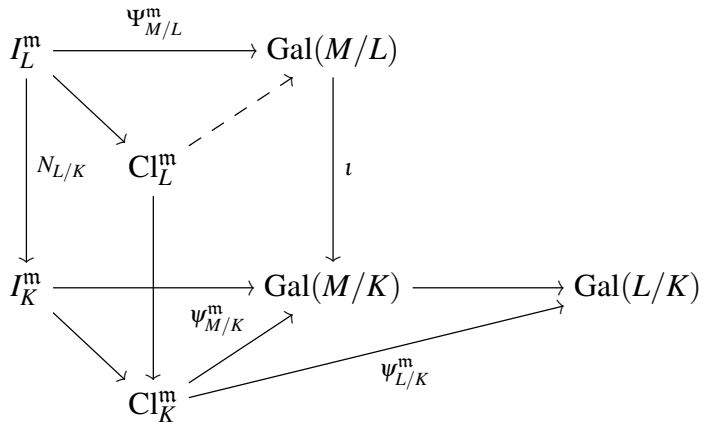
That is, the ray class field L of K for $\mathfrak{m}$ is the unique finite abelian extension of K with defining modulus $\mathfrak{m}$ such that $N_{L/K}\mathrm{Cl}_L^{\mathfrak{m}} = 1$.

REMARK 7.4.15. As a consequence of Proposition 7.4.13c, every finite abelian extension L of K for which a modulus $\mathfrak{m}$ for K is a defining modulus is contained in the ray class field of K with modulus $\mathfrak{m}$.

Using the existence theorem, Proposition 7.4.13, and the surjectivity of $\Psi_{L/K}^{\mathfrak{m}}$ we may now demonstrate a part of Artin reciprocity.

PROOF THAT $\psi_{L/K}^{\mathfrak{m}}$ HAS KERNEL $N_{L/K}(\mathrm{Cl}_L^{\mathfrak{m}})$. Let M be the ray class field of K with modulus $\mathfrak{m}$. Then $N_{M/K}\mathrm{Cl}_M^{\mathfrak{m}} = 1$ by Artin reciprocity. It follows from Proposition 7.4.13c that $L \subseteq M$. Consider

the diagram



By Proposition 7.4.4a, the diagram commutes. As $\mathrm{Gal}(M/L)$ is a subgroup of $\mathrm{Gal}(M/K)$ and $\psi_{M/K}^{\mathfrak{m}}$ is an isomorphism, an element of $I_L^{\mathfrak{m}}$ lies in the kernel of $\Psi_{M/L}^{\mathfrak{m}}$ if and only if its image in $\mathrm{Cl}_L^{\mathfrak{m}}$ has trivial norm in $\mathrm{Cl}_K^{\mathfrak{m}}$. In particular, we have $P_L^{\mathfrak{m}} \subseteq \ker \Psi_{M/L}^{\mathfrak{m}}$, so $\mathfrak{m}$ is a defining modulus for M/L, and the dotted map in the diagram exists and is $\psi_{M/L}^{\mathfrak{m}}$.

Now, the kernel of $\psi_{L/K}^{\mathfrak{m}}$ consists of exactly those elements of $\mathrm{Cl}_K^{\mathfrak{m}}$ with image in $\mathrm{Gal}(M/L)$ under $\psi_{M/K}^{\mathfrak{m}}$. Since $\Psi_{M/L}^{\mathfrak{m}}$ is assumed surjective, we have that $\psi_{M/L}^{\mathfrak{m}}$ is as well. Therefore, the composition

$$N_{L/K} = (\psi_{M/K}^{\mathfrak{m}})^{-1} \circ \iota \circ \psi_{M/L}^{\mathfrak{m}} \colon \mathrm{Cl}_L^{\mathfrak{m}} \to \mathrm{Cl}_K^{\mathfrak{m}}$$

has image $\ker \psi_{L/K}^{\mathfrak{m}}$, finishing the proof. □

Alternatively, we could have used the entire Artin reciprocity law and the existence theorem to prove Proposition 7.4.13 and the uniqueness of ray class fields, much as in the spirit of the case of local class field theory.

EXAMPLE 7.4.16. We claim that the ray class field L of $\mathbb{Q}(i)$ with modulus (3) is $\mathbb{Q}(\mu_{12})$. Note that only the primes over 3 ramify in $\mathbb{Q}(\mu_{12})/\mathbb{Q}(i)$. To see the claim, suppose first that $p \equiv 3 \bmod 4$ with $p \neq 3$. Then (p) is inert in $\mathbb{Q}(i)/\mathbb{Q}$. Since the Frobenius at p over $\mathbb{Q}(i)$ will fix $\mathbb{Q}(\mu_{12})$ if and only if it fixes μ_{12}, we have $(p, \mathbb{Q}(\mu_{12})/\mathbb{Q}(i)) = 1$ if and only if $p^2 \equiv 1 \bmod 12$. But the latter congruence holds for all $p \neq 3$. Since $(p) = (-p)$, we actually have $(p) \in P_K^{(3)}$ for all $p \neq 3$ as well.

If $p \equiv 1 \bmod 4$, then p splits in $\mathbb{Q}(i)$. In fact, $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ and

$$p\mathbb{Z}[i] = (a+bi)(a-bi).$$

We have $(a+bi, \mathbb{Q}(\mu_{12})/\mathbb{Q}(i)) = 1$ if and only if

$$p = N_{L/K}(a+bi) \equiv 1 \bmod 12.$$

This will occur if and only if exactly one of a and b is nonzero modulo 3. For such a prime p, by multiplying $a+bi$ by i if needed, we may assume that $3 \mid b$, and by multiplying $a+bi$ by -1 if needed, we may then assume that $a \equiv 1 \bmod 3$. Conversely, a pair (a,b) with $a \equiv 1 \bmod 3$ and $3 \mid b$ yields a

prime $p \equiv 1 \bmod 12$. In other words, $(a+bi) \in P_K^{(3)}$ for $p \equiv 1 \bmod 4$ with $p = a^2+b^2$ if and only if $(a+bi) \in \ker \Psi_{\mathbb{Q}(\mu_{12})/\mathbb{Q}(i)}$. It follows by multiplicativity that the kernel of $\Psi_{\mathbb{Q}(\mu_{12})/\mathbb{Q}(i)}$ is exactly $P^{(3)}_{\mathbb{Q}(i)}$. Therefore, we have $L = \mathbb{Q}(\mu_{12})$ by the uniqueness of ray class fields.

We now show that there is a defining modulus for any abelian extension that is minimal in a particular sense.

PROPOSITION 7.4.17. *Every abelian extension L/K of number fields has a defining modulus that divides all other defining moduli for L/K.*

PROOF. If $\{\mathfrak{m}_i \mid i \in I\}$ is a nonempty set of moduli for a number field K, where I is some indexing set, then we define a modulus

$$\mathfrak{M} = \sum_{i \in I} \mathfrak{m}_i$$

such that $\mathfrak{M}_f$ is the sum of the finite ideals $(\mathfrak{m}_i)_f$ over $i \in I$ and $\mathfrak{M}_\infty$ equal to the product of all real primes dividing every $(\mathfrak{m}_i)_\infty$. We then see from the definition that

$$K_{\mathfrak{M},1} = \prod_{i \in I} K_{\mathfrak{m}_i,1},$$

and so $P_K^{\mathfrak{M}}$ is also the sum of the $P_K^{\mathfrak{m}_i}$.

Given an abelian extension L/K of number fields, we consider the set of moduli $\mathfrak{m}$ that are divisible by all places of K that ramify in L and for which $P_K^{\mathfrak{m}}$ lies in the kernel of $\Psi^{\mathfrak{m}}_{L/K}$. By Artin reciprocity, this set is nonempty. The sum of these moduli is by construction the unique modulus that is divisible by all places that ramify in L and is contained in $\ker \Psi^{\mathfrak{M}}_{L/K}$. □

DEFINITION 7.4.18. The *conductor* $\mathfrak{f}_{L/K}$ of an abelian extension L/K of number fields is the unique defining modulus for L/K that divides all other defining moduli for L/K.

REMARK 7.4.19. It is possible for two distinct finite abelian extensions of a number field K to have the same conductor. On the other hand, not all moduli for K need be conductors of finite abelian extensions of K. In particular, the ray class field of K with modulus $\mathfrak{m}$ is only guaranteed to have conductor dividing $\mathfrak{m}$, and if this conductor does not equal the modulus, then that modulus is not the conductor of any finite abelian extension of K with defining modulus $\mathfrak{m}$, since any such field is contained in the ray class field.

EXAMPLE 7.4.20. The conductor of the ray class field $\mathbb{Q}(\mu_{12})$ of $\mathbb{Q}(i)$ with modulus (3) is (3), since (3) ramifies in $\mathbb{Q}(\mu_{12})/\mathbb{Q}(i)$.

The following gives the comparison between the conductor of an extension of global fields and the conductors of the local extensions given by completion at a finite prime of the extension field.

PROPOSITION 7.4.21. *Let L/K be a finite abelian extension of number fields. Then*

$$\mathfrak{f}_{L/K,f} = \prod_{\mathfrak{p}} (\mathfrak{f}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} \cap \mathscr{O}_K),$$

where the product runs over all nonzero prime ideals $\mathfrak{p}$ of $\mathscr{O}_K$ and for each such $\mathfrak{p}$, we choose a prime ideal $\mathfrak{P}$ of $\mathscr{O}_L$ lying over it.

7.5. Class field theory over $\mathbb{Q}$

DEFINITION 7.5.1.

i. A number field is said to be *totally real* if all of its archimedean embeddings are real.

ii. A number field is said to be *purely imaginary* if all of its archimedean embeddings are complex.

REMARK 7.5.2. A Galois extension of $\mathbb{Q}$ is either totally real or purely imaginary. On the other hand, by way of example, $\mathbb{Q}(\sqrt[3]{2})$ has one real embedding and a pair of complex conjugate complex embeddings.

EXAMPLE 7.5.3. For any $n \geq 1$, the field $\mathbb{Q}(\mu_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ for a primitive nth root of unity ζ_n is a totally real field. In fact, it is the largest totally real subfield of the field $\mathbb{Q}(\mu_n)$, which is purely imaginary if $n \geq 3$.

We consider the ray class fields of $\mathbb{Q}$.

EXAMPLE 7.5.4. Let $f \geq 1$. Let ζ_f be a primitive fth root of unity.

i. We claim that the ray class field for $\mathbb{Q}$ with modulus $(f)\infty$ is $\mathbb{Q}(\mu_f)$. To see this, note that only the places dividing $(f)\infty$ ramify in $\mathbb{Q}(\mu_f)$. Let a denote a positive integer relatively prime to f, and let $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\mu_f)/\mathbb{Q})$ be such that $\sigma_a(\zeta_f) = \zeta_f^a$. We then have that

$$\Psi^{(f)\infty}_{\mathbb{Q}(\mu_f)/\mathbb{Q}}((a)) = \sigma_a,$$

which is immediately seen by writing out the factorization of a and noting that $\sigma_p = (p, \mathbb{Q}(\mu_f)/\mathbb{Q})$ for any prime p not dividing f. In particular, we see that

$$P_{\mathbb{Q}}^{(f)\infty} \subseteq \Psi^{(f)\infty}_{\mathbb{Q}(\mu_f)/\mathbb{Q}},$$

so $(f)\infty$ is a defining modulus for $\mathbb{Q}(\mu_f)/\mathbb{Q}$.

Next, note that the cyclotomic character χ_f provides an isomorphism

$$\chi_f \colon \mathrm{Gal}(\mathbb{Q}(\mu_f)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/f\mathbb{Z})^\times$$

with $\chi_f(\sigma_a) = a$. Recall also the isomorphism from Example 7.3.13(ii)

$$\phi_f \colon \mathrm{Cl}_{\mathbb{Q}}^{(f)\infty} \xrightarrow{\sim} (\mathbb{Z}/f\mathbb{Z})^\times$$

such that $\phi_f([(a)]_{(f)\infty}) = a \bmod f$. The composition

$$(\mathbb{Z}/f\mathbb{Z})^\times \xrightarrow{\phi_f^{-1}} \mathrm{Cl}_{\mathbb{Q}}^{(f)\infty} \xrightarrow{\psi^{(f)\infty}_{\mathbb{Q}(\mu_f)/\mathbb{Q}}} \mathrm{Gal}(\mathbb{Q}(\mu_f)/\mathbb{Q}) \xrightarrow{\chi_f} (\mathbb{Z}/f\mathbb{Z})^\times$$

is then the identity map. That is, we have

$$\chi_f \circ \psi_{\mathbb{Q}(\mu_f)/\mathbb{Q}} \circ \phi_f^{-1}(a) = \chi_f \circ \psi^{(f)\infty}_{\mathbb{Q}(\mu_f)/\mathbb{Q}}([(a)]_{(f)\infty}) = \chi_f(\sigma_a) = a.$$

ii. We next claim that the ray class field for $\mathbb{Q}$ with modulus (f) is

$$\mathbb{Q}(\mu_f)^+ = \mathbb{Q}(\zeta_f + \zeta_f^{-1}).$$

Note that the image of the cyclotomic character χ on $\mathrm{Gal}(\mathbb{Q}(\mu_f)/\mathbb{Q}(\mu_f)^+)$ is $\langle \pm 1 \rangle$, so χ induces an isomorphism

$$\chi'_f \colon \mathrm{Gal}(\mathbb{Q}(\mu_f)^+/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/f\mathbb{Z})^\times/\langle \pm 1 \rangle$$

Recall also that Example 7.3.13(i) sets up an isomorphism

$$\phi'_f \colon \mathrm{Cl}_{\mathbb{Q}}^{(f)} \xrightarrow{\sim} (\mathbb{Z}/f\mathbb{Z})^\times/\langle \pm 1 \rangle.$$

Since the maps in question are all induced by those in part a, the composition

$$(\mathbb{Z}/f\mathbb{Z})^\times/\langle -1 \rangle \xrightarrow{(\phi'_f)^{-1}} \mathrm{Cl}_{\mathbb{Q}}^{(f)} \xrightarrow{\psi^{(f)}_{\mathbb{Q}(\mu_f)/\mathbb{Q}}} \mathrm{Gal}(\mathbb{Q}(\mu_f)^+/\mathbb{Q}) \xrightarrow{\chi'_f} (\mathbb{Z}/f\mathbb{Z})^\times/\langle -1 \rangle$$

is the identity.

As a corollary of Example 7.5.4 and Artin reciprocity, we see that every abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field. In other words, we have $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\mu_\infty)$. However, we can also see this directly from the local Kronecker-Weber theorem, as we now show.

THEOREM 7.5.5 (Kronecker-Weber). *Every finite abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\mu_n)$ for some $n \geq 1$.*

PROOF. Let F be a finite abelian extension of $\mathbb{Q}$. For $k \geq 0$, let $p_1, \ldots, p_k$ be the distinct primes that ramify in $F/\mathbb{Q}$, and choose primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ of F such that $\mathfrak{p}_i$ lies over p_i for each $1 \leq i \leq k$. By the local Kronecker-Weber theorem, we have for each i that $F_{\mathfrak{p}_i} \subseteq \mathbb{Q}_{p_i}(\mu_{n_i})$ for some $n_i \geq 1$, and let us let $r_i \geq 0$ be maximal such that p^{r_i} divides n_i. Set $n = p_1^{r_1} \cdots p_k^{r_k}$, and let $K = F(\mu_n)$, an abelian extension of $\mathbb{Q}$. We claim that $K = \mathbb{Q}(\mu_n)$, which will finish the proof.

Set $G = \mathrm{Gal}(K/\mathbb{Q})$, and let I_{p_i} be the inertia group at p_i in G. The completion of K at a prime $\mathfrak{P}_i$ over $\mathfrak{p}_i$ is

$$K_{\mathfrak{P}_i} = F_{\mathfrak{p}_i}(\mu_n) = \mathbb{Q}_{p_i}(\mu_{\mathrm{lcm}(n,n_i)}).$$

Since $p_i^{r_i}$ exactly divides $m = \mathrm{lcm}(n, n_i)$ by definition, we have

$$I_{p_i} \cong \mathrm{Gal}(\mathbb{Q}_{p_i}(\mu_m)/\mathbb{Q}_{p_i}(\mu_{m/p_i^{r_i}})) \cong \mathrm{Gal}(\mathbb{Q}_{p_i}(\mu_{p_i^{r_i}})/\mathbb{Q}_{p_i}).$$

Let I be the subgroup of G generated by all its inertia subgroups: that is, $I = I_{p_1} \cdots I_{p_k}$. The order of I is

$$|I| \leq \prod_{i=1}^{k} |I_{p_i}| = \prod_{i=1}^{k} \varphi(p_i^{r_i}) = \varphi(n) = [\mathbb{Q}(\mu_n) : \mathbb{Q}].$$

However, since there is no nontrivial extension of $\mathbb{Q}$ that is unramified at all primes in $\mathbb{Z}$, the inertia groups in G must generate G, so we have that $I = G$. Since $\mathbb{Q}(\mu_n) \subseteq K$, this forces $K = \mathbb{Q}(\mu_n)$. □

EXAMPLE 7.5.6. Let K be a finite abelian extension of $\mathbb{Q}$, and let n be minimal such that $K \subseteq \mathbb{Q}(\mu_n)$. Note that $\mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_{n/2})$ if n is exactly divisible by 2, so the minimality of n forces n to be odd or divisible by 4. Then the smallest ray class field in which K is contained is either $\mathbb{Q}(\mu_n)^+$, the ray class field of modulus (n), or $\mathbb{Q}(\mu_n)$, the ray class field of modulus $(n)\infty$. Note that $\mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_n)^+$ only for $n = 1$. Thus, if K is totally real, its conductor $\mathfrak{f}_{K/\mathbb{Q}}$ is (n). If K is purely imaginary, then the conductor is $(n)\infty$. Note that $(2m)$ and $(2m)\infty$ for m odd, as well as (∞), never occur as conductors of abelian extensions of $\mathbb{Q}$.

7.6. The Hilbert class field

The most fundamental example of a ray class field is that with modulus (1), which was originally considered by Hilbert.

DEFINITION 7.6.1. The *Hilbert class field* of a number field K is the maximal abelian extension of K that is unramified at all places of K.

REMARK 7.6.2. To see that the Hilbert class field of a number field K is the ray class field of K with conductor (1), note that the reciprocity law says that if L/K is finite abelian and unramified, then (1) is a defining modulus, and the converse holds by definition. The ray class field with conductor (1) is the largest field with defining modulus (1), hence is the Hilbert class field.

The following is immediate by Artin reciprocity.

PROPOSITION 7.6.3. *Let E be the Hilbert class field of a number field K. By the Artin reciprocity law, the Artin map*

$$\psi_{E/K} \colon \mathrm{Cl}_K \to \mathrm{Gal}(E/K)$$

is an isomorphism.

We have the following interesting corollary.

COROLLARY 7.6.4. *Let E be the Hilbert class field of a number field K. Then a nonzero prime ideal of $\mathcal{O}_K$ is principal if and only if it splits completely in E/K.*

PROOF. To say that a nonzero prime $\mathfrak{p}$ in $\mathcal{O}_K$ is principal is exactly to say its class $[\mathfrak{p}]$ in Cl_K is trivial, which is exactly to say that $\psi_{E/K}([\mathfrak{p}]) = 1$. In turn, this just says that the Frobenius $(\mathfrak{p}, E/K)$ is trivial, which means that the decomposition group at $\mathfrak{p}$ in $\mathrm{Gal}(E/K)$ is trivial, which is to say that $\mathfrak{p}$ splits completely in the abelian extension E/K. □

EXAMPLE 7.6.5. Let $K = \mathbb{Q}(\sqrt{-5})$. Then Cl_K has order 2 and is generated by the class of $\mathfrak{p} = (2, 1+\sqrt{-5})$. The Hilbert class field E therefore has degree 2 over K. In fact, $E = K(i)$. For this, note that $\mathbb{Q}(i)/\mathbb{Q}$ ramifies only at 2, so the extension $K(i)/K$ can ramify only at the unique prime $\mathfrak{p}$ over 2 in $\mathscr{O}_K$. Note that $\alpha = \frac{1+\sqrt{5}}{2}$ has minimal polynomial $x^2 - x - 1$ over K, so $\alpha \in \mathscr{O}_{K(i)}$. Since $x^2 - x - 1$ is irreducible over $\mathscr{O}_{K(i)}/\mathfrak{p} \cong \mathbb{F}_2$, the extension of this residue field in $K(i)$ is of degree 2, so $\mathfrak{p}$ is inert in $K(i)/K$. That is $K(i)/K$ is unramified, and it clearly has degree 2, so we must have $E = K(i)$.

Every nonzero ideal in the ring of integers of a number field generates a trivial ideal in the ring of integers of the Hilbert class field, as we will show. Key to this is the following lemma, which we state without proof.

LEMMA 7.6.6. *Let G be a group with commutator subgroup $[G,G]$ of finite index in G. Then the transfer map $V\colon G^{\mathrm{ab}} \to [G,G]^{\mathrm{ab}}$ is trivial.*

We now prove the Hauptidealsatz of Emil Artin.

THEOREM 7.6.7 (Principal ideal theorem). *Let K be a number field and E its Hilbert class field. For every $\mathfrak{a} \in I_K$, the fractional ideal $\mathfrak{a}\mathscr{O}_E$ is principal.*

PROOF. Let M be the Hilbert class field of E, and note that

$$\mathrm{Gal}(M/E) = [\mathrm{Gal}(M/K), \mathrm{Gal}(M/K)]$$

and $\mathrm{Gal}(E/K) = \mathrm{Gal}(M/K)^{\mathrm{ab}}$. By Lemma 7.6.6, the Verlagerung map

$$V_{E/K}\colon \mathrm{Gal}(E/K) \to \mathrm{Gal}(M/E)$$

is trivial. The commutative diagram of Proposition 7.4.4(ii) then reads

$$\begin{array}{ccc} \mathrm{Cl}_K & \xrightarrow{\psi_{E/K}} & \mathrm{Gal}(E/K) \\ {\scriptstyle \iota_{E/K}}\downarrow & & \downarrow{\scriptstyle V_{E/K}=0} \\ \mathrm{Cl}_E & \xrightarrow{\psi_{M/E}} & \mathrm{Gal}(M/E), \end{array}$$

which forces $\iota_{E/K} = 0$, as $\psi_{M/E}$ is an isomorphism. □

CHAPTER 8

Class formations

8.1. Reciprocity maps

DEFINITION 8.1.1. Let K be a field. A *class formation* (A, inv) for K is a discrete G_K-module A such that for each finite separable extension L of K, we have $H^1(G_L, A) = 0$ and an isomorphism

$$\mathrm{inv}_L \colon H^2(G_L, A) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

such that for any intermediate field E, we have

$$\mathrm{inv}_L \circ \mathrm{Res}_{L/E} = [L : E]\, \mathrm{inv}_E,$$

where $\mathrm{Res}_{L/E}$ is the restriction map $H^2(G_E, A) \to H^2(G_L, A)$.

For the rest of this section, fix a field K and a class formation (A, inv) a class formation for K.

REMARK 8.1.2. A class formation over K gives rise to a class formation over all finite separable extensions of K. Thus, in several results below, we use K as the base field where it may be replaced by a finite separable extension without actual loss of generality.

NOTATION 8.1.3. For a finite separable extension L of K, we set $A_L = A^{G_L}$. If E is an intermediate extension, we let $\mathrm{Cor}_{L/E}$ and $\mathrm{Res}_{L/E}$ denote restriction and corestriction between G_L and G_E. We write the corestriction map $A_L \to A_E$ more simply by $N_{L/E}$.

REMARK 8.1.4. For a Galois extension L/K, we have $H^1(\mathrm{Gal}(L/K), A_L) = 0$ and an isomorphism

$$\mathrm{inv}_{L/K} \colon H^2(\mathrm{Gal}(L/K), A_L) \xrightarrow{\sim} \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

induced by the commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^2(\mathrm{Gal}(L/K), A_L) & \xrightarrow{\mathrm{Inf}} & H^2(G_K, A) & \xrightarrow{\mathrm{Res}} & H^2(G_L, A) \\
 & & \downarrow{\scriptstyle \mathrm{inv}_{L/K}} & & \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\
0 & \longrightarrow & \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:K]} & \mathbb{Q}/\mathbb{Z}.
\end{array}$$

REMARK 8.1.5. For all purposes below, we may weaken the statement that inv_L is an isomorphism in the definition of a class formation to being an injection, so long as $\mathrm{inv}_{M/L}$ is supposed to be an isomorphism for all finite separable extensions M/L.

DEFINITION 8.1.6. The unique element $\alpha_{L/E} \in H^2(\mathrm{Gal}(L/E), A_L)$ with $\mathrm{inv}_{L/E}(\alpha_{L/E}) = \frac{1}{[L:E]}$ is called the *fundamental class* for L/E.

As a consequence of Remark 8.1.4, we may apply Tate's theorem to obtain the following result.

PROPOSITION 8.1.7. *For any finite Galois extension L of K, there is an canonical isomorphism* $\mathrm{Gal}(L/K)^{\mathrm{ab}} \xrightarrow{\sim} A_K/N_{L/K}(A_L)$ *given by cup product with the fundamental class $\alpha_{L/K}$:*

$$\theta_{L/K} \colon \hat{H}^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) \to \hat{H}^0(\mathrm{Gal}(L/K), A_L), \quad \theta_{L/K}(\beta) = \alpha_{L/K} \cup \beta.$$

DEFINITION 8.1.8. Let L be a finite Galois extension of K. The *reciprocity map* for L/K with respect to the class formation (A, inv) for K is the map

$$\rho_{L/K} \colon A_K \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$$

that factors through the inverse $A_K/N_{L/K}A_L \to \mathrm{Gal}(L/K)$ of the isomorphism $\theta_{L/K}$ of Proposition 8.1.7.

LEMMA 8.1.9. *Let G be a finite group, let $\sigma \in G$ with image $\bar{\sigma} \in G^{\mathrm{ab}}$, and let $\chi \colon G \to \mathbb{Q}/\mathbb{Z}$ be a homomorphism. Viewing $\bar{\sigma}$ as an element of $\hat{H}^{-2}(G, \mathbb{Z})$ and $\chi \in H^1(G, \mathbb{Q}/\mathbb{Z})$, we have*

$$\bar{\sigma} \cup \chi = \chi(\sigma) \in \mathbb{Q}/\mathbb{Z},$$

noting that $\hat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z}) \cong \frac{1}{|G|}\mathbb{Z}/\mathbb{Z}$.

PROOF. Consider the connecting homomorphisms δ and $\delta^\vee$ for the sequence

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

and its $\mathbb{Q}/\mathbb{Z}$-dual

$$0 \to \mathbb{Q}/\mathbb{Z} \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(I_G, \mathbb{Q}/\mathbb{Z}) \to 0.$$

The image of $\bar{\sigma}$ in $\hat{H}^{-1}(G, I_G)$ is the image of $\sigma - 1$ in I_G/I_G^2, and the inverse image of χ in $\hat{H}^0(G, \mathrm{Hom}(I_G, \mathbb{Q}/\mathbb{Z}))$ is class of the homomorphism f that takes $\tau - 1$ for $\tau \in G$ to $\chi(\tau)$. We then have

$$\bar{\sigma} \cup \chi = \delta(\bar{\sigma}) \cup (\delta^\vee)^{-1}(\chi) = f(\sigma - 1) = \chi(\sigma).$$

□

PROPOSITION 8.1.10. *Let L be a finite Galois extension of K, and let δ denote the connecting homomorphism for the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ of $\mathrm{Gal}(L/K)$-modules. For any homomorphism $\chi \colon \mathrm{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z}$, we have*

$$\mathrm{inv}_{L/K}(a \cup \delta(\chi)) = \chi(\rho_{L/K}(a))$$

for all $a \in A_K$.

PROOF. Note that $\alpha_{L/K} \cup \rho_{L/K}(a) = \bar{a}$ by definition of $\rho_{L/K}$, viewing its image as the group $\hat{H}^{-2}(\mathrm{Gal}(L/K), \mathbb{Z})$, where $\bar{a}$ denotes the image of a in $A_K/N_{L/K}A_L$. By the associativity of cup products and property (iii) of their definition, we have

$$\alpha_{L/K} \cup \delta(\rho_{L/K}(a) \cup \chi) = \alpha_{L/K} \cup \rho_{L/K}(a) \cup \delta(\chi) = \bar{a} \cup \delta(\chi).$$

The composition of the canonical maps

$$\tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \xrightarrow{\sim} \hat{H}^{-1}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \hat{H}^{0}(\mathrm{Gal}(L/K), \mathbb{Z}) \xrightarrow{\sim} \mathbb{Z}/[L:K]\mathbb{Z}$$

is the isomorphism induced by multiplication by $[L:K]$ (since the norm for $\mathrm{Gal}(L/K)$ acts as multiplication by $[L:K]$ on $\mathbb{Q}$). By definition of $\alpha_{L/K}$ and the latter fact, we have

$$\mathrm{inv}_{L/K}(\alpha_{L/K} \cup \delta(\rho_{L/K}(a) \cup \chi)) = \delta(\rho_{L/K}(a) \cup \chi)\,\mathrm{inv}_{L/K}(\alpha_{L/K}) = \rho_{L/K}(a) \cup \chi = \chi(\rho_{L/K}(a)),$$

the final step from Lemma 8.1.9. □

COROLLARY 8.1.11. *Let $L \subseteq M$ be finite Galois extensions of K. Then*

$$\rho_{M/K}(a)|_L = \rho_{L/K}(a)$$

for all $a \in A_K$.

PROOF. Let $\chi\colon \mathrm{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z}$ be a homomorphism, which we may view as a homomorphism on $\mathrm{Gal}(M/K)$ (and its abelianization) as well. It suffices to show that for any such χ, we have $\chi(\rho_{M/K}(a)) = \chi(\rho_{L/K}(a))$. For this, it sufficient by Proposition 8.1.10 to show that

$$\mathrm{inv}_{M/K}(a \cup \delta(\chi)) = \mathrm{inv}_{L/K}(a \cup \delta(\chi)),$$

where abusing notation. Since $\mathrm{inv}_{L/K} = \mathrm{inv}_{M/K} \circ \mathrm{Inf}$, where

$$\mathrm{Inf}\colon H^i(\mathrm{Gal}(L/K), A_L) \to H^i(\mathrm{Gal}(M/K), A_M)$$

is inflation, this is clear from the compatibility of cup products with inflation. □

We may now define the reciprocity map.

DEFINITION 8.1.12. The *reciprocity map* for K with respect to the class formation (A, inv) for K is the map

$$\rho_K\colon A_K \to G_K^{\mathrm{ab}}$$

defined as the inverse limit of the reciprocity maps $\rho_{E/K}\colon A_K \to \mathrm{Gal}(E/K)^{\mathrm{ab}}$ over finite Galois extensions of E in a separable closure of K.

The following theorem, which is immediate from the definitions, is called a reciprocity law.

THEOREM 8.1.13 (Reciprocity law for class formations). *Let K be a field and (A, inv) a class formation for K, and let $\rho_K\colon K^\times \to G_K^{\mathrm{ab}}$. For any finite Galois extension L/K, the composition of ρ_K with restriction induces a surjective map $\rho_{L/K}\colon K^\times \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$ with kernel $N_{L/K}L^\times$.*

REMARK 8.1.14. A class formation for K gives rise to a class formation for any finite separable extension L of K, with the same module A and with the subcollection of invariant maps for finite separable extensions of L. Therefore, we obtain reciprocity maps $\rho_L : A_L \to G_L^{\mathrm{ab}}$ for all finite separable L/K from a class formation for K.

We next turn to properties of the reciprocity map. First, we need to describe a certain abstract group homomorphism.

LEMMA 8.1.15. *Let G be a group and H a subgroup of finite index n. Let $X = \{x_1, x_2, \ldots, x_n\}$ be a set of left H-coset representatives in G. Given $g \in G$ and $x_i \in X$, let $1 \leq g(i) \leq n$ and $t_i(g) \in H$ be such that*

$$gx_i = x_{g(i)} t_i(g).$$

Then the element $V(g)$ of H^{ab} that is represented by the element $t_1(g)t_2(g)\cdots t_n(g)$ is independent of all choices, and this induces a homomorphism $V : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$.

PROOF. Note that G acts on the set of left H-cosets by left multiplication. If we replace a single x_i by $x_i h$ for some $h \in H$, then $gx_i h = x_j t_i(g) h$, so $t_i(g)$ is replaced by $h^{-1} t_i(g) h$ if $g(i) = i$ and $t_i(g)h$ if $g(i) \neq i$. In the latter case, $gx_{g^{-1}(i)} = x_i t_{g^{-1}(i)}(g)$, and then $t_{g^{-1}(i)}(g)$ is replaced by $h^{-1} t_{g^{-1}(i)}(g)$. For all other j, the quantity $t_j(g)$ is unchanged. As the product $t_1(g)t_2(g)\cdots t_n(g)$ is taken in H^{ab}, it is unchanged since the overall effect of the change is multiplication by $h \cdot h^{-1}$. Similarly, if the ordering of the x_i is changed, then the order of the $t_i(g)$ is likewise changed, but this does not matter in H^{ab}. Thus $V(g)$ is well-defined.

To see that V is a homomorphism, we merely note that

$$gg' x_i = g x_{g'(i)} t_i(g') = x_{gg'(i)} t_i(g) t_i(g')$$

and again that multiplication is commutative in H^{ab}. □

DEFINITION 8.1.16. Let G be a group and H be a subgroup of finite index. The homomorphism $V : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ constructed in Lemma 8.1.15 is known as the *transfer map* (or *Verlagerung*) between G and H.

LEMMA 8.1.17. *Let G be a group and H a subgroup of finite index. We have a commutative diagram*

$$\begin{array}{ccc} H_1(G,\mathbb{Z}) & \xrightarrow{\mathrm{Res}} & H_1(H,\mathbb{Z}) \\ \downarrow \wr & & \downarrow \wr \\ G^{\mathrm{ab}} & \xrightarrow{V} & H^{\mathrm{ab}}, \end{array}$$

where the vertical maps are the canonical isomorphisms and V is the transfer map and a commutative diagram

$$\begin{array}{ccc} H_1(H,\mathbb{Z}) & \xrightarrow{\text{Cor}} & H_1(G,\mathbb{Z}) \\ \downarrow\wr & & \downarrow\wr \\ H^{\text{ab}} & \longrightarrow & G^{\text{ab}}, \end{array}$$

where the lower horizontal map is induced by the inclusion map.

PROOF. Recall that the vertical isomorphism is given by the series of canonical isomorphisms

$$H_1(G,\mathbb{Z}) \cong H_0(G,I_G) \cong I_G/I_G^2 \cong G^{\text{ab}}.$$

As restriction is a δ-functor, we have a commutative diagram

$$\begin{array}{ccccc} H_1(G,\mathbb{Z}) & \xrightarrow{\text{Res}} & H_1(H,\mathbb{Z}) & = & H_1(H,\mathbb{Z}) \\ \downarrow\wr & & \downarrow & & \downarrow\wr \\ H_0(G,I_G) & \xrightarrow{\text{Res}} & H_0(H,I_G) & \longleftarrow & H_0(H,I_H). \end{array}$$

That is, our restriction map factors through I_G/I_GI_H. By the definition of restriction on 0th cohomology groups, we have

$$\text{Res}(g^{-1}-1) = \sum_{i=1}^{n} x_i^{-1}(g^{-1}-1) = \sum_{i=1}^{n}((gx_i)^{-1}-x_i^{-1})$$

where $\{x_1,x_2,\ldots,x_n\}$ is a set of left H-coset representatives in G. For $t_i(g)$ as in the definition of the transfer, this equals

$$\sum_{i=1}^{n} t_i(g)^{-1}x_{g(i)}^{-1} - \sum_{i=1}^{n} x_i^{-1} = \sum_{i=1}^{n}(t_i(g)^{-1}-1)x_{g(i)}^{-1} \equiv \sum_{i=1}^{n}(t_i(g)^{-1}-1) \equiv V_i(g)^{-1}-1 \bmod I_GI_H.$$

Thus, the restriction map and the transfer agree.

The second statement follows easily from the commutative diagram

$$\begin{array}{ccccc} H_1(H,\mathbb{Z}) & = & H_1(H,\mathbb{Z}) & \xrightarrow{\text{Cor}} & H_1(G,\mathbb{Z}) \\ \downarrow\wr & & \downarrow & & \downarrow\wr \\ H_0(H,I_H) & \longrightarrow & H_0(H,I_G) & \xrightarrow{\text{Cor}} & H_0(G,I_G). \end{array}$$

□

The reciprocity maps attached to a class formation satisfy the following compatibilities.

PROPOSITION 8.1.18. *Let (A,inv) be a class formation for K, and let L be a finite separable extension of K. Then we have the following commutative diagrams:*

a.

$$\begin{array}{ccc} A_L & \xrightarrow{\rho_L} & G_L^{\mathrm{ab}} \\ \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle R_{L/K}} \\ A_K & \xrightarrow{\rho_K} & G_K^{\mathrm{ab}}, \end{array}$$

where $R_{L/K}$ denotes the restriction map on Galois groups,

b.

$$\begin{array}{ccc} A_K & \xrightarrow{\rho_K} & G_K^{\mathrm{ab}} \\ \downarrow & & \downarrow{\scriptstyle V_{L/K}} \\ A_L & \xrightarrow{\rho_L} & G_L^{\mathrm{ab}}, \end{array}$$

where the map $A_K \to A_L$ is the natural injection and $V_{L/K}\colon G_K^{\mathrm{ab}} \to G_L^{\mathrm{ab}}$ is the transfer map, and

c.

$$\begin{array}{ccc} A_L & \xrightarrow{\rho_L} & G_L^{\mathrm{ab}} \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma^*} \\ A_{\sigma(L)} & \xrightarrow{\rho_{\sigma(L)}} & G_{\sigma(L)}^{\mathrm{ab}}, \end{array}$$

for each embedding $\sigma\colon L \hookrightarrow K^{\mathrm{sep}}$, where σ^* denotes the map induced by conjugation $\tau \mapsto \sigma\tau\sigma^{-1}$ for $\tau \in G_L$.

PROOF. Fix a Galois extension M of K containing L. The norm $N_{L/K}\colon A_L \to A_K$ induces corestriction from $\mathrm{Gal}(M/L)$ to $\mathrm{Gal}(M/K)$ on zeroth Tate cohomology groups, and

$$R_{L/K}\colon \mathrm{Gal}(M/L)^{\mathrm{ab}} \to \mathrm{Gal}(M/K)^{\mathrm{ab}}$$

coincides with corestriction on Tate cohomology groups of $\mathbb{Z}$ in degree -2 by Lemma 8.1.17. Part a then follows from Proposition A.9.10c, which tells us that

$$\mathrm{Cor}(\alpha_{M/L} \cup \beta) = \alpha_{M/K} \cup \mathrm{Cor}(\beta)$$

for $\beta \in \hat{H}^0(\mathrm{Gal}(M/L), A_M)$, since $\mathrm{Res}(\alpha_{M/K}) = \alpha_{M/L}$.

The injection $A_K \to A_L$ induces restriction on $\hat{H}^0(\mathrm{Gal}(M/K), A_L)$, and the transfer map $V_{L/K}$ coincides with restriction on $\hat{H}^{-2}(\mathrm{Gal}(M/K), \mathbb{Z})$, again by Lemma 8.1.17. Part b then follows from Proposition A.9.10a, which tells us that

$$\mathrm{Res}(\alpha_{M/K} \cup \beta) = \alpha_{L/K} \cup \mathrm{Res}(\beta)$$

for $\beta \in \hat{H}^0(\mathrm{Gal}(M/K), A_M)$.

We leave part c as an exercise for the reader. □

8.2. Norm groups

Let us fix a field K and a class formation (A, inv) for K.

DEFINITION 8.2.1. A subgroup $\mathscr{N}$ of A is called a *norm group* for the class formation (A, inv) if there exists a finite separable extension L of K with $\mathscr{N} = N_{L/K}A_L$.

NOTATION 8.2.2. For a finite extension L of K, let us set $\mathscr{N}_L = N_{L/K}A_L$.

LEMMA 8.2.3. *Let M and L be finite separable extensions of K with $L \subseteq M$. Then $\mathscr{N}_M \subset \mathscr{N}_L$.*

PROOF. This is the following straightforward calculation using Proposition 1.3.6:

$$\mathscr{N}_M = N_{M/K}A_L = N_{M/L}(N_{L/K}A_L) \subset N_{M/L}A_K = \mathscr{N}_K.$$

□

LEMMA 8.2.4. *Let L be a finite separable extension of K, and let E be the maximal abelian extension of K in L. Then $\mathscr{N}_L = \mathscr{N}_E$.*

PROOF. It suffices to show that any $a \in \mathscr{N}_E$ is contained in $\mathscr{N}_L$. Let M be a finite Galois extension of K containing L. Set $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$. By definition, we have $\rho_{E/K}(a) = 1$, so $\tau = \rho_{M/K}(a) \in G^{\mathrm{ab}}$ maps trivially to $\mathrm{Gal}(E/K) = G/([G,G]H)$ by Corollary 8.1.11. In other words τ is the image of some element σ in H^{ab}. By the surjectivity of the reciprocity map $\rho_{M/L}\colon A_L \to H^{\mathrm{ab}}$ and there exists $b \in A_L$ such that $\rho_{M/L}(b) = \sigma$. By Proposition 8.1.18a, we then have

$$\rho_{M/K}(N_{L/K}(b)) = \rho_{M/K}(a),$$

so $a - N_{L/K}(b) = N_{M/K}(c)$ for some $c \in A_M$. It follows that $a = N_{L/K}(b - N_{M/L}(c))$, as desired. □

The following corollary is essentially immediate.

COROLLARY 8.2.5. *Every norm group $\mathscr{N}$ of (A, inv) has finite index in A_K, with $[A_K : \mathscr{N}] \leq [L : K]$ for $\mathscr{N} = \mathscr{N}_L$, with equality if and only if L/K is abelian.*

We next show that the map that takes a finite extension L of K to $N_{L/K}A_L$ is an inclusion-reversing bijection from finite abelian extensions of K to norm groups.

PROPOSITION 8.2.6. *For any finite abelian extensions L and M of K, we have the following:*

a. $\mathscr{N}_L \cap \mathscr{N}_M = \mathscr{N}_{LM}$,

b. $\mathscr{N}_L + \mathscr{N}_M = \mathscr{N}_{L \cap M}$,

c. $\mathscr{N}_M \subseteq \mathscr{N}_L$ *if and only if* $L \subseteq M$,

d. for any subgroup $\mathscr{A}$ of A_K containing $\mathscr{N}_L$, there exists an intermediate field E in L/K with $\mathscr{A} = \mathscr{N}_E$.

PROOF.

a. Let $a \in A_K$. We have $a \in \mathscr{N}_{LM}$ if and only if $\rho_K(a)|_{LM}$ is trivial, which occurs if and only if $\rho_K(a)|_L$ and $\rho_K(a)|_M$ are both trivial, and so if and only if $a \in \mathscr{N}_L$ and $a \in \mathscr{N}_M$.

c. By Lemma 8.2.3, if $L \subseteq M$, then $\mathscr{N}_M \subseteq \mathscr{N}_L$. On the other hand, if $\mathscr{N}_M \subseteq \mathscr{N}_L$, then by part (a) we have

$$\mathscr{N}_{LM} = \mathscr{N}_L \cap \mathscr{N}_M = \mathscr{N}_M.$$

By Corollary 8.2.5, this implies that $[LM : K] = [M : K]$, so $LM = M$, and therefore $L \subseteq M$.

d. Let $E = L^{\rho_{L/K}(\mathscr{A})}$. Then $\rho_{L/K}$ induces an injective homomorphism

$$\mathscr{A}/\mathscr{N}_L \to \mathrm{Gal}(L/E)$$

that must be an isomorphism as $\rho_{L/K}(\mathscr{A})$ does not fix any larger subfield of L than E. The kernel of $\rho_{E/K}$, being that $\rho_{E/K}$ is the composite of $\rho_{L/K}$ with restriction, is then $\rho_{L/K}^{-1}(\mathrm{Gal}(L/E)) = \mathscr{A}$. But we know from the reciprocity law that the kernel is $\mathscr{N}_E$.

b. By part (d), the group $\mathscr{A} = \mathscr{N}_L + \mathscr{N}_M$ is equal to $\mathscr{N}_E$ for some finite abelian E/K which by part (c) is contained in both L and M. On the other hand, we clearly have that $\mathscr{A}$ is contained in $\mathscr{N}_{L\cap M}$, so again by (c), the field E contains $L \cap M$ as well.

□

The following corollary is nearly immediate from part (c) of Proposition 9.2.8.

COROLLARY 8.2.7 (Uniqueness theorem). *For a norm subgroup $\mathscr{N}$ of A_K, there exists a unique finite abelian extension L/K such that $\mathscr{N} = \mathscr{N}_L$.*

NOTATION 8.2.8. For a finite separable extension L of K, we set $D_L = \ker \rho_L$.

LEMMA 8.2.9. *For any finite extension L of K in a fixed separable closure K^{sep}, we have*

$$D_L = \bigcap_{M \in \mathscr{E}_L} N_{M/L} A_M,$$

where $\mathscr{E}_L$ is the set of finite abelian (or separable) extensions of L in K^{sep}.

PROOF. We have $a \in \ker \rho_L$ if and only if $\rho_{M/L}(a) = \rho_L(a)|_M = 1$ for all finite abelian M over L, and $\ker \rho_{M/L} = N_{M/L} A_M$. □

DEFINITION 8.2.10. We say that a class formation (A, inv) for K is *topological* if A is given an additional Hausdorff topology under which it becomes a topological G_K-module with the following properties:

i. the norm map $N_{M/L} : A_M \to A_L$ has closed image and compact kernel for each finite extension M/L of finite separable extensions of K,

ii. for each prime p, there exists a finite separable extension K_p over K such that for all finite separable extensions L of K_p, the kernel of $\phi_p\colon A_L \to A_L$ by $\phi_p(a) = pa$ for $a \in A_L$ is compact and the image of ϕ_p contains D_L, and

iii. for each finite separable extension L of K, there exists a compact subgroup U_L of A_L such that every closed subgroup of finite index in A_L that contains U_L is a norm group.

REMARK 8.2.11. The norm map $N_{M/L}\colon A_M \to A_L$ for a finite extension of finite separable extensions is continuous if A is a topological G_K-module, since it is a sum of continuous maps induced by field embeddings of M in its Galois closure over L.

The following proposition uses only the property (i) of a topological class formation.

PROPOSITION 8.2.12. *Let (A, inv) be a topological class formation for K. For any finite separable extension L of K, we have $N_{L/K}D_L = D_K$.*

PROOF. Let $\mathscr{E}_L$ be the set of finite abelian (or separable) extensions of L in K^{sep} (and likewise with K). We have

$$N_{L/K}\left(\bigcap_{M\in\mathscr{E}_L} N_{M/L}A_M\right) \subseteq \bigcap_{M\in\mathscr{E}_L} N_{M/K}A_M = \bigcap_{M\in\mathscr{E}_K} N_{M/K}A_M,$$

the last step noting Lemma 8.2.3, and thus $N_{L/K}D_L \subseteq D_K$.

Fix $a \in D_K$. For any finite separable M/L, the set

$$Y_M = N_{M/L}A_M \cap N_{L/K}^{-1}(a)$$

is compact since $N_{M/K}A_M$ is closed and $N_{L/K}^{-1}(a)$ is compact by Definition 8.2.10(i). Since $a \in D_K$, there exists $b \in A_M$ with $N_{M/K}(b) = a$, and then $N_{M/L}(b) \in Y_M$. Thus Y_M is nonempty. Note that if M'/M is finite separable, then $Y_{M'} \subseteq Y_M$, and so the Y_M form a collection of subsets of the compact space Y_L that satisfy the finite intersection property. We therefore have that the intersection of all Y_M is nonempty, so contains an element b. Then $N_{L/K}(b) = a$, and $b \in D_L$ as it lies in every $N_{M/L}A_M$. Thus, we have $N_{L/K}(D_L) = D_K$. □

The next proposition uses properties (i) and (ii) of a topological class formation.

PROPOSITION 8.2.13. *Let (A, inv) be a topological class formation for K. Then D_K is divisible, equal to $\bigcap_{n=1}^{\infty} nA_K$.*

PROOF. To see that D_K is divisible, it suffices to show that $D_K = pD_K$ for all primes p. Fix $a \in D_K$. Let L be a finite separable extension of K containing K_p. Set

$$X_L = \mathscr{N}_L \cap \phi_p^{-1}(a),$$

where $\phi_p\colon A_L \to A_L$ is the multiplication-by-p map. By (i) of Definition 8.2.10, the set $\mathscr{N}_L$ is closed, and by (ii), the set $\phi_p^{-1}(a)$ is compact, so X_L is compact. By Proposition 8.2.12, there exists $x \in D_L$

with $a = N_{L/K}x$. By Definition 8.2.10(ii), there exists $y \in D_L$ with $py = x$, and we set $b = N_{L/K}y$. Then $b \in X_L$, so X_L is nonempty. Again, if M/L is finite separable, then $X_M \subseteq X_L$. It follows as in the proof of Proposition 8.2.12 that the intersection of all X_L as L varies is nonempty, so contains some element c. By definition, we have $c \in D_K$ and $pc = b$. Thus $D_K = pD_K$.

Since $D_K \subset A_K$, we have

$$D_K = \bigcap_{n=1}^{\infty} nD_K \subseteq \bigcap_{n=1}^{\infty} nA_K.$$

Suppose, on the other hand, that $a \in \bigcap_{n=1}^{\infty} nA_K$. Let $b \in A_K$ with $nb = a$ for $n \geq 1$. Take any finite separable extension L/K, and set $n = [L : K]$ Then $N_{L/K}(b) = nb = a$, so $a \in N_{L/K}A_L$. Since L was arbitrary, we have $a \in D_L$. □

We are now ready to prove the existence theorem for topological class formations, which tells us that given a closed subgroup $\mathscr{N}$ of finite index in A_K, there exists a finite separable extension L/K with $\mathscr{N} = \mathscr{N}_L$. Since a topological class formation for K gives rise to a topological class formation for any finite extension of K (in that the existence of U_L in condition (iii) is assumed for all finite separable L/K, and not just for K), this result for norm groups of K implies the analogous result for norm groups over finite separable extensions.

THEOREM 8.2.14 (Existence theorem). *Let (A, inv) be a topological class formation for K. A subgroup of A_K is a norm group if and only if it is closed of finite index in A_K.*

PROOF. If a subgroup is a norm group, then it is of finite index by the reciprocity law and is closed in A_K by Definition 8.2.10(i).

Conversely, if $\mathscr{N}$ is a closed subgroup of A_K of finite index, set $n = [A_K : \mathscr{N}]$. Then $nA_K \subseteq \mathscr{N}$, so $D_K \subseteq \mathscr{N}$ by Proposition 8.2.13. Let U_K be as in Definition 8.2.10(iii). Then for any norm subgroup $\mathscr{M}$ of A_K, the sets $\mathscr{M} \cap U_K$ are compact. The intersection of the $\mathscr{M} \cap U_K$ over all norm groups $\mathscr{M}$ is equal to $D_K \cap U_K$, so is contained in the open set $\mathscr{N}$. Since the intersection of all $\mathscr{M} \cap U_K$ with $A_K - \mathscr{N}$ would be nonempty if each intersection were, there exists a norm group $\mathscr{M}$ with $\mathscr{M} \cap U_K \subseteq \mathscr{N}$.

Let $a \in \mathscr{M} \cap (U_K + \mathscr{M} \cap \mathscr{N})$, and write $a = u + v$ with $u \in U_K$ and $v \in \mathscr{M} \cap \mathscr{N}$. Then $u = a - v \in \mathscr{M}$, so $u \in U_K \cap \mathscr{M}$, so $u \in \mathscr{N}$, and thus $a \in \mathscr{N}$. Thus, we have

$$\mathscr{M} \cap (U_K + \mathscr{M} \cap \mathscr{N}) \subseteq \mathscr{N}.$$

Since $\mathscr{M} \cap \mathscr{N}$ is closed of finite index, so is $U_K + \mathscr{M} \cap \mathscr{N}$, and thus it is a norm group by Definition 8.2.10(iii). Then $\mathscr{M} \cap (U_K + \mathscr{M} \cap \mathscr{N})$ is a norm group by Proposition 9.2.8a, and $\mathscr{N}$ is a norm group by Proposition 9.2.8d. □

PROPOSITION 8.2.15. *Let (A, inv) be a topological class formation for K. Then the reciprocity map*

$$\rho_K : A_K \to G_K^{\mathrm{ab}}$$

is continuous with dense image.

PROOF. To see that ρ_K is continuous, we need only note that the inverse image $\mathscr{N}_L$ of the open neighborhood $\mathrm{Gal}(K^{\mathrm{ab}}/L)$ of 1, for L/K finite abelian, is open by property (i) of Definition 8.2.10.

The closure of the image of ρ_K is obviously a closed subgroup of $G_K^{\mathrm{ab}} \cong \varprojlim_L \mathrm{Gal}(L/K)$, so equal to $\mathrm{Gal}(K^{\mathrm{ab}}/M)$ for some M/K abelian. As it also surjects onto each of the finite quotients $\mathrm{Gal}(L/K)$ since each $\rho_{L/K}$ is surjective, we must have $M = K$. Thus, ρ_K has dense image. □

8.3. Class field theory over finite fields

Class field theory for finite fields is rather simple, the reciprocity map being injection of $\mathbb{Z}$ into the absolute Galois group of the field that takes 1 to the Frobenius automorphism. However, it allows us to give a toy example of a class formation that illustrates the theory we have developed.

PROPOSITION 8.3.1. *For any prime p and all powers q of p, there are canonical isomorphisms* $\mathrm{inv}\colon H^2(G_{\mathbb{F}_q},\mathbb{Z}) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ *for all powers q of p such that $(\mathbb{Z},\mathrm{inv})$ is a class formation for $\mathbb{F}_p$.*

PROOF. For positive n, we have

$$H^1(G_{\mathbb{F}_{q^n}},\mathbb{Z}) = \mathrm{Hom}_{\mathrm{cts}}(G_{\mathbb{F}_{q^n}},\mathbb{Z}),$$

and the latter group is zero since the image of any continuous homomorphism of a compact Hausdorff group with values in a discrete group is finite, and the only finite subgroup of $\mathbb{Z}$ is trivial.

Consider the exact sequence

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

For $i \geq 1$, we have

$$H^i(G_{\mathbb{F}_{q^n}},\mathbb{Q}) = \varinjlim_m H^i(\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_{q^n}),\mathbb{Q}) = 0,$$

where the direct limit is taken over multiples of n, since $H^i(\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_{q^n}),\mathbb{Q})$ has exponent dividing $\frac{m}{n}$ but is also a $\mathbb{Q}$-vector space. Thus, we have isomorphisms

$$H^2(G_{\mathbb{F}_{q^n}},\mathbb{Z}) \xleftarrow{\sim} H^1(G_{\mathbb{F}_{q^n}},\mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_{\mathrm{cts}}(G_{\mathbb{F}_{q^n}},\mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cts}}(\hat{\mathbb{Z}},\mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}, \tag{8.3.1}$$

the latter map being given by evaluation at 1, and through these we obtain a map

$$\mathrm{inv}_{\mathbb{F}_{q^n}} : H^2(G_{\mathbb{F}_{q^n}},\mathbb{Z}) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}.$$

For $n \mid m$, we have a commutative diagram

$$\begin{array}{ccc}
H^2(G_{\mathbb{F}_{q^n}},\mathbb{Z}) & \xrightarrow{\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_{q^n}}} & H^2(G_{\mathbb{F}_{q^m}},\mathbb{Z}) \\
\wr\downarrow & & \wr\downarrow \\
H^1(G_{\mathbb{F}_{q^n}},\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_{q^n}}} & H^2(G_{\mathbb{F}_{q^m}},\mathbb{Q}/\mathbb{Z}) \\
\wr\downarrow \mathrm{inv}_{\mathbb{F}_{q^n}} & & \wr\downarrow \mathrm{inv}_{\mathbb{F}_{q^m}} \\
\mathbb{Q}/\mathbb{Z} & \xrightarrow{\frac{m}{n}} & \mathbb{Q}/\mathbb{Z}.
\end{array}$$

To see the commutativity of the lower square, note that the homomorphism that sends the Frobenius element φ_n in $G_{\mathbb{F}_{q^n}}$ to 1 restricts to a homomorphism sending the Frobenius $\varphi_m = \varphi_n^{m/n}$ to $\frac{m}{n}$, and the invariant map for n (resp., m) sends the homomorphism that takes φ_n (resp., φ_m) to 1 to the element $1 \in \mathbb{Q}/\mathbb{Z}$. Thus, $(\mathbb{Z}, \mathrm{inv})$ is a class formation for $\mathbb{F}_q$. □

Let us fix the class formation $(\mathbb{Z}, \mathrm{inv})$ of Proposition 8.3.1 each prime p in order to discuss reciprocity maps and norm groups.

PROPOSITION 8.3.2. *For a prime power q, the reciprocity map*

$$\rho_{\mathbb{F}_q} \colon \mathbb{Z} \to G_{\mathbb{F}_q}$$

satisfies $\rho_{\mathbb{F}_q}(1) = \varphi$, where φ is the Frobenius element in $G_{\mathbb{F}_q}$.

PROOF. Let $n \geq 1$, and consider the homomorphism $\chi \colon \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \to \mathbb{Q}/\mathbb{Z}$ that takes (the restriction of) φ to $\frac{1}{n}$. Let δ denote the connecting homomorphism arising from the sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. By Proposition 8.1.10, as required, we have

$$\chi(\rho_{\mathbb{F}_{q^n}/\mathbb{F}_q}(1)) = \mathrm{inv}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(1 \cup \delta(\chi)) = \mathrm{inv}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\delta(\chi)) = \frac{1}{n},$$

the last equality following from the construction of the invariant map in (8.3.1). □

The following should already be clear.

PROPOSITION 8.3.3. *Let q be a prime power.*

a. For any $n \geq 1$, the reciprocity map

$$\rho_{\mathbb{F}_{q^n}/\mathbb{F}_q} \colon \mathbb{Z} \to \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$$

is a surjection with kernel $n\mathbb{Z}$.

b. The map $\rho_{\mathbb{F}_q}$ is injective with dense image. With respect to the discrete topology on $\mathbb{Z}$, it is continuous.

c. The map that takes $n\mathbb{Z}$, for $n \geq 1$, to $\mathbb{F}_{q^n}$ is a bijection between (closed) subgroups of $\mathbb{Z}$ (under the discrete topology) and finite (abelian) extensions of $\mathbb{F}_q$ in an algebraic closure of $\mathbb{F}_q$.

The third part of Proposition 8.3.3 does not provide such a great example of the theory of norm groups, in that the discrete topology makes the class formation $(\mathbb{Z}, \mathrm{inv})$ topological, with $D_{\mathbb{F}_q}$ and $U_{\mathbb{F}_q}$ in Definition 8.2.10 both the zero group.

CHAPTER 9

Local class field theory

9.1. The Brauer group of a local field

Fix a local field K and a separable closure K^{sep} of K. All separable extensions of K will be supposed to lie in K^{sep}. In this section, we construct invariant maps $\mathrm{inv}_L\colon \mathrm{Br}(L) \to \mathbb{Q}/\mathbb{Z}$ for finite separable extensions L/K such that $((K^{\mathrm{sep}})^\times, \mathrm{inv})$ forms a class formation for K.

NOTATION 9.1.1. For a Galois extension E/F of fields, we set

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

We construct inv_K by first defining it on the subgroup $\mathrm{Br}(K^{\mathrm{ur}}/K)$ of $\mathrm{Br}(K)$ corresponding to the maximal unramified extension K^{ur} of K. For this, note that the unique extension $w_K\colon (K^{\mathrm{ur}})^\times \to \mathbb{Z}$ of the additive valuation on K to K^{ur} is a map of $\mathrm{Gal}(K^{\mathrm{ur}}/K)$-modules, hence induces a map

$$w_K^*\colon \mathrm{Br}(K^{\mathrm{ur}}/K) \to H^2(\mathrm{Gal}(K^{\mathrm{ur}}/K), \mathbb{Z}),$$

where we identify $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ with $\hat{\mathbb{Z}}$ via the isomorphism taking the Frobenius element to 1.

DEFINITION 9.1.2. The invariant map $\mathrm{inv}_{K^{\mathrm{ur}}/K}\colon \mathrm{Br}(K^{\mathrm{ur}}/K) \to \mathbb{Q}/\mathbb{Z}$ is the composition

$$\mathrm{Br}(K^{\mathrm{ur}}/K) \xrightarrow{w_K^*} H^2(\mathrm{Gal}(K^{\mathrm{ur}}/K), \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(\mathrm{Gal}(K^{\mathrm{ur}}/K), \mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{ev}_{\varphi_K}} \mathbb{Q}/\mathbb{Z},$$

where δ is the connecting homomorphism arising from $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$, and ev_{φ_K} is evaluation at the Frobenius φ_K in $\mathrm{Gal}(K^{\mathrm{ur}}/K)$.

We will show that $\mathrm{inv}_{K^{\mathrm{ur}}/K}$ is an isomorphism, which amounts to showing that w_K^* is an isomorphism. We require a preliminary lemma.

LEMMA 9.1.3. *Let G be a finite group, and let M be a G-module such that there exists a decreasing sequence $(M_n)_{n\geq 0}$ with $M_0 = M$ of G-submodules of M for which*

$$M = \varprojlim_n M/M_n.$$

Let $i \geq 0$, and suppose that $H^i(G, M_n/M_{n+1}) = 0$ for all $n \geq 0$. Then $H^i(G, M) = 0$ as well.

PROOF. Let $f \in Z^i(G,M)$. Suppose that we have inductively defined $f_n \in Z^i(G,M_n)$ and $h_j \in C^{i-1}(G,M_j)$ for $0 \leq j \leq n-1$ such that

$$f = f_n + \sum_{j=0}^{n-1} d^{i-1}(h_j).$$

(Note that we take $C^{-1}(G,M_j) = 0$.) The image of f_n in $Z^i(G,M_n/M_{n+1})$ is a coboundary by assumption, say of $\bar{h}_n \in C^{i-1}(G,M_n/M_{n+1})$. Lifting $\bar{h}_n$ to any $h_n \in C^{i-1}(G,M_n)$, we then set $f_{n+1} = f_n - d^{i-1}(h_i)$. Since $M = \varprojlim_n M/M_n$, the sequence of partial sums $\sum_{j=1}^n h_j$ converges to an element of $C^{i-1}(G,M)$ with coboundary f. □

PROPOSITION 9.1.4. *Let L be a finite Galois extension of K. Then there exists an open* $\mathrm{Gal}(L/K)$*-submodule V of $\mathscr{O}_L^\times$ that is cohomologically trivial.*

PROOF. Let $G = \mathrm{Gal}(L/K)$. By the normal basis theorem, there exists $\alpha \in L$ such that $\{\sigma(\alpha) \mid \sigma \in G\}$ forms a K-basis of L. By multiplying by an element $K^\times$, we may suppose that $\alpha \in \mathscr{O}_L$. Let Λ' be the $\mathscr{O}_K$-lattice in L spanned by the $\sigma(\alpha)$. Let π be a uniformizer in $\mathscr{O}_K$. Then $[\mathscr{O}_L : \Lambda']$ is finite, so $\pi^n \mathscr{O}_L \subseteq \Lambda'$ for n sufficiently large. Set $\Lambda = \pi^{n+1}\Lambda'$. Then

$$\Lambda \cdot \Lambda = \pi^{2(n+1)}\Lambda' \subseteq \pi^{2(n+1)}\mathscr{O}_L \subseteq \pi^{n+2}\mathscr{O}_L \subseteq \pi\Lambda.$$

Then $V = 1 + \Lambda$ is a G-submodule of $\mathscr{O}_L^\times$, and V in turn has a decreasing filtration $V_i = 1 + \pi^i\Lambda$ for $i \geq 0$ of G-submodules. We have isomorphisms

$$V_i/V_{i+1} \xrightarrow{\sim} \Lambda/\pi\Lambda, \qquad (1+\pi^i\lambda)V_{i+1} \mapsto \lambda + \pi\Lambda.$$

Since $\Lambda/\pi\Lambda$ is a free $\mathbb{F}_p[G]$-module, it is induced, so cohomologically trivial. Lemma 9.1.3 then tells us, in particular, that $H^i(G_p,V) = 0$ for all $i \geq 1$ for each Sylow subgroup G_p of G, and the cohomological triviality then follows from Theorem A.11.11. □

We use Proposition 9.1.4 first to study the case of cyclic, and then more specifically, unramified extensions.

COROLLARY 9.1.5. *Let L be a finite cyclic extension of K. Then the Herbrand quotient of $\mathscr{O}_L^\times$ with respect to group* $\mathrm{Gal}(L/K)$ *is* 1.

PROOF. Let V be as in Proposition 9.1.4. The exact sequence

$$1 \to V \to \mathscr{O}_L^\times \to \mathscr{O}_L^\times/V \to 1$$

gives rise to the identity of Herbrand quotients

$$h(\mathscr{O}_L^\times) = h(V)h(\mathscr{O}_L^\times/V) = 1$$

since $\mathscr{O}_L^\times/V$ is finite as V is open. □

COROLLARY 9.1.6. *Let L/K be a finite unramified extension. Then $\mathscr{O}_L^\times$ is a cohomologically trivial* $\mathrm{Gal}(L/K)$*-module.*

PROOF. It clearly suffices to show that $\hat{H}^i(G,\mathscr{O}_L^\times) = 0$ for $G = \mathrm{Gal}(L/K)$ and all i, since any subgroup of G is the Galois group of an unramified extension of local fields. The additive valuation v_L on $\mathscr{O}_L$ restricts to the valuation v_K on $\mathscr{O}_L$ since L/K is unramified. The short exact sequence

$$1 \to \mathscr{O}_L^\times \to L^\times \xrightarrow{v_L} \mathbb{Z} \to 0$$

then gives rise to a long exact sequence starting

$$1 \to \mathscr{O}_K^\times \to K^\times \xrightarrow{v_K} \mathbb{Z} \to H^1(G,\mathscr{O}_L^\times) \to H^1(G,L^\times),$$

with the last group zero by Hilbert's Theorem 90 and the map v_K surjective. Thus $H^1(G,\mathscr{O}_L^\times) = 0$, and since L/K is cyclic, the result follows from the triviality of the Herbrand quotient and the periodicity of Tate cohomology. □

PROPOSITION 9.1.7. *The invariant map* $\mathrm{inv}_{K^{\mathrm{ur}}/K}\colon \mathrm{Br}(K^{\mathrm{ur}}/K) \to \mathbb{Q}/\mathbb{Z}$ *is an isomorphism.*

PROOF. For any $i \geq 1$, Proposition 9.1.6 implies that

$$H^i(\mathrm{Gal}(K^{\mathrm{ur}}/K),\mathscr{O}_{K^{\mathrm{ur}}}^\times) \cong \varinjlim_n H^i(\mathrm{Gal}(K_n/K),\mathscr{O}_{K_n}^\times) = 0$$

where K_n is the unique unramified extension of K (in K^{sep}) of degree n. The valuation map yields an exact sequence

$$1 \to \mathscr{O}_{K^{\mathrm{ur}}}^\times \to (K^{\mathrm{ur}})^\times \xrightarrow{w_K} \mathbb{Z} \to 0,$$

we therefore have that

$$w_K^*\colon \mathrm{Br}(K^{\mathrm{ur}}/K) \to H^2(\mathrm{Gal}(K^{\mathrm{ur}}/K),\mathbb{Z})$$

is an isomorphism. The other maps in the definition of $\mathrm{inv}_{K^{\mathrm{ur}}/K}$ are clearly isomorphisms, so the result holds. □

NOTATION 9.1.8. For a finite separable extension L of K, we use $\mathrm{Res}_{L/K}$ to denote the map

$$\mathrm{Res}_{L/K}\colon \mathrm{Br}(K^{\mathrm{ur}}/K) \to \mathrm{Br}(L^{\mathrm{ur}}/L)$$

defined by the compatible pair consisting of restriction $\mathrm{Gal}(L^{\mathrm{ur}}/L) \to \mathrm{Gal}(K^{\mathrm{ur}}/K)$ and the inclusion $(K^{\mathrm{ur}})^\times \to (L^{\mathrm{ur}})^\times$.

REMARK 9.1.9. For L/K finite separable, the map $\mathrm{Res}_{L/K}$ fits into a commutative diagram

$$\begin{array}{ccc} \mathrm{Br}(K^{\mathrm{ur}}/K) & \xrightarrow{\mathrm{Res}_{L/K}} & \mathrm{Br}(L^{\mathrm{ur}}/L) \\ \downarrow \mathrm{Inf} & & \downarrow \mathrm{Inf} \\ \mathrm{Br}(K) & \xrightarrow{\mathrm{Res}_{L/K}} & \mathrm{Br}(L). \end{array}$$

The following describes how our invariant map behaves after finite extension of the base field.

PROPOSITION 9.1.10. *Let L be a finite separable extension of K. Then*

$$\mathrm{inv}_{L^{\mathrm{ur}}/L} \circ \mathrm{Res}_{L/K} = [L:K]\,\mathrm{inv}_{K^{\mathrm{ur}}/K}.$$

PROOF. We claim that the diagram

$$\begin{array}{ccccccc}
\mathrm{Br}(K^{\mathrm{ur}}/K) & \xrightarrow{w_K^*} & H^2(\mathrm{Gal}(K^{\mathrm{ur}}/K),\mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(\mathrm{Gal}(K^{\mathrm{ur}}/K),\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\mathrm{ev}_{\varphi_K}} & \mathbb{Q}/\mathbb{Z} \\
\downarrow{\scriptstyle \mathrm{Res}_{L/K}} & & \downarrow{\scriptstyle e_{L/K}\mathrm{Res}_{L/K}} & & \downarrow{\scriptstyle e_{L/K}\mathrm{Res}_{L/K}} & & \downarrow{\scriptstyle [L:K]} \\
\mathrm{Br}(L^{\mathrm{ur}}/L) & \xrightarrow{w_L^*} & H^2(\mathrm{Gal}(L^{\mathrm{ur}}/L),\mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(\mathrm{Gal}(L^{\mathrm{ur}}/K),\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\mathrm{ev}_{\varphi_L}} & \mathbb{Q}/\mathbb{Z}
\end{array}$$

commutes (where $\mathrm{Res}_{L/K}$ in the middle two arrows denotes the corresponding composition of restriction and inflation), from which the result follows. The commutativity of the middle square is straightforward. Since the restriction of w_L to $(K^{\mathrm{ur}})^\times$ is $e_{L/K}w_K$, the leftmost square commutes. Since the restriction of φ_L to K^{ur} is the $f_{L/K}$-power of φ_K, the rightmost square commutes. □

Having defined the invariant map on $\mathrm{Br}(K^{\mathrm{ur}}/K)$ and shown that it satisfied the desired property with respect to change of base field, our next goal is to show that the inflation map

$$\mathrm{Inf}\colon\ \mathrm{Br}(K^{\mathrm{ur}}/K) \to \mathrm{Br}(K)$$

is an isomorphism. At the finite level, we note the following.

COROLLARY 9.1.11. *Let L/K be a finite Galois extension of local fields, and set*

$$\mathrm{Br}(L/K)^{\mathrm{ur}} = \mathrm{Br}(K^{\mathrm{ur}}/K) \cap \mathrm{Br}(L/K) \leq \mathrm{Br}(K).$$

Then $\mathrm{Br}(L/K)^{\mathrm{ur}}$ is cyclic of order $[L:K]$.

PROOF. By the inflation-restriction sequence for Brauer groups, we have

$$\mathrm{Br}(L/K)^{\mathrm{ur}} = \{\alpha \in \mathrm{Br}(K^{\mathrm{ur}}/K) \mid \mathrm{Res}_{L/K}(\alpha) = 0\}.$$

By Proposition 9.1.10, this coincides with the kernel of $[L:K]$ on $\mathrm{Br}(K^{\mathrm{ur}}/K)$, which is cyclic of order n. □

We require a special case of the following cohomological lemma.

LEMMA 9.1.12. *Let G be a finite group, let A be a G-module, and let $i, r \geq 0$. Suppose that for all subgroups H of G, we have that $\hat{H}^j(H,A) = 0$ for all $1 \leq j \leq i-1$ and that the order $\hat{H}^i(H/K, A^K)$ divides $[H:K]^r$ for all normal subgroups K of H of prime index. Then the order of $\hat{H}^i(G,A)$ divides $|G|^r$.*

PROOF. If we replace G by a Sylow p-subgroup for a prime p, then the conditions of the lemma are still satisfied. By Corollary A.8.24, we see that $|H^i(G,A)|$ divides $\prod_p |H^i(G_p,A)|$, which if we prove the lemma for each G_p will divide $\prod_p |G_p|^r = |G|^r$.

Thus, we can and do assume that G is a p-group. Let H be a normal subgroup of G of index p. By hypothesis, we have that $|\hat{H}^i(G/H,A^H)|$ divides p^r, and we may suppose by induction on the order of G that $|\hat{H}^i(H,A)|$ divides $|H|^r$. If $i \geq 1$, then by the triviality of $H^j(H,A)$ for $1 \leq j \leq i-1$, we have an exact inflation-restriction sequence

$$0 \to H^i(G/H,A^H) \to H^i(G,A) \to H^i(H,A),$$

so the order of $H^i(G,A)$ divides $|G|^r = (p|H|)^r$. For $i = 0$, we merely replace the inflation-restriction sequence with the exact sequence

$$\hat{H}^0(H,A) \xrightarrow{\text{Cor}} \hat{H}^0(G,A) \to \hat{H}^0(G/H,A^H),$$

where we recall that corestriction in degree 0 coincides with the sum over left coset representatives of G/H. □

THEOREM 9.1.13. *The inflation map* $\text{Inf}\colon \text{Br}(K^{\text{ur}}/K) \to \text{Br}(K)$ *is an isomorphism.*

PROOF. It suffices to see that $\text{Br}(L/K)^{\text{ur}} = \text{Br}(L/K)$ for every finite Galois extension L/K, since the union under (injective) inflation maps of the groups $\text{Br}(L/K)^{\text{ur}}$ is $\text{Br}(K^{\text{ur}}/K)$ and the union under inflation maps of the groups $\text{Br}(L/K)$ is $\text{Br}(K)$. For this, it suffices by Corollary 9.1.11 to show that $\text{Br}(L/K)$ has order dividing $n = [L:K]$.

First, suppose that L/K is cyclic. We consider Herbrand quotients for $G = \text{Gal}(L/K)$. The exact sequence defined by the valuation on L yields

$$h(L^\times) = h(\mathscr{O}_L^\times)h(\mathbb{Z}).$$

We have $h(\mathscr{O}_L^\times) = 1$ by Lemma 9.1.5, while $h(\mathbb{Z}) = n$ since $\hat{H}^0(G,\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$ and $\hat{H}^{-1}(G,\mathbb{Z}) = 0$. Since $h_1(L^\times) = 1$ by Hilbert's Theorem 90, we have $|\text{Br}(L/K)| = h_0(L^\times) = n$.

Now take L/K to be any finite Galois extension. With $G = \text{Gal}(L/K)$ and $A = L^\times$, the hypotheses of Lemma 9.1.12 are satisfied with $i = 2$ and $r = 1$ by Hilbert's Theorem 90 and the case of cyclic extensions. Consequently, $\text{Br}(L/K)$ has order dividing n, as we aimed to show. □

By Theorem 9.1.13, we may make the following definition of the invariant map for K (and hence for any local field).

DEFINITION 9.1.14. The *invariant map* $\text{inv}_K\colon \text{Br}(K) \to \mathbb{Q}/\mathbb{Z}$ for a local field K is the composition

$$\text{inv}_K\colon \text{Br}(K) \xrightarrow{\text{Inf}^{-1}} \text{Br}(K^{\text{ur}}/K) \xrightarrow{\text{inv}_{K^{\text{ur}}/K}} \mathbb{Q}/\mathbb{Z}.$$

THEOREM 9.1.15. *The pair* $((K^{\text{sep}})^\times, \text{inv})$ *is a class formation for* K.

PROOF. For L/K finite separable, we have $H^1(G_L,(K^{\mathrm{sep}})^\times)=0$ by Hilbert's Theorem 90. The invariant map inv_L is an isomorphism by Theorem 9.1.13 and Proposition 9.1.7. Moreover, we have

$$\mathrm{inv}_L\circ\mathrm{Res}_{L/K}=[L:K]\,\mathrm{inv}_K$$

as a consequence of Proposition 9.1.10, noting Remark 9.1.9. Thus, the axioms of a class formation are satisfied. □

9.2. Local reciprocity

We continue to let K denote a local field and K^{sep} a separable closure of K.

DEFINITION 9.2.1. The *(local) reciprocity map* for K is the reciprocity map $\rho_K\colon K^\times\to G_K^{\mathrm{ab}}$ attached to the class formation $((K^{\mathrm{sep}})^\times,\mathrm{inv})$ of Theorem 9.1.15.

Let us proceed directly to the statement of the main theorem.

THEOREM 9.2.2 (Local reciprocity). *Let K be a nonarchimedean local field. Then the local reciprocity map*

$$\rho_K\colon K^\times\to G_K^{\mathrm{ab}}$$

satisfies

i. for each uniformizer π of K, the element $\rho_K(\pi)$ is a Frobenius element in G_K^{ab}, and

ii. for any finite abelian extension L of K, the map

$$\rho_{L/K}\colon K^\times\to\mathrm{Gal}(L/K)$$

defined by $\rho_{L/K}(a)=\rho_K(a)|_L$ for all $a\in K^\times$ is surjective with kernel $N_{L/K}L^\times$.

PROOF. By Theorem 8.1.13, the reciprocity map ρ_K satisfies (ii). We show that it satisfies (i). For this, take any finite unramified extension L/K, and let $G=\mathrm{Gal}(L/K)$. Let φ denote the Frobenius element in G. Let $\chi\colon G\to\mathbb{Q}/\mathbb{Z}$ be an injective homomorphism. It suffices to show that $\chi(\rho_{L/K}(\pi))=\chi(\varphi)$. By Proposition 8.1.10, we have

$$\chi(\rho_{L/K}(\pi))=\mathrm{inv}_{L/K}(\pi\cup\delta(\chi)),$$

where δ is the connnecting homomorphisms for $0\to\mathbb{Z}\to\mathbb{Q}\to\mathbb{Q}/\mathbb{Z}\to 0$. For the valuation v_L on L, we have

$$v_L^*(\pi\cup\delta(\chi))=v_L(\pi)\cup\delta(\chi)=\delta(\chi).$$

Since $\mathrm{inv}_{L/K}=\mathrm{ev}_\varphi\circ\delta^{-1}\circ v_L^*$ by definition, we have

$$\mathrm{inv}_{L/K}(\pi\cup\delta(\chi))=\mathrm{ev}_\varphi(\chi)=\chi(\varphi).$$

□

REMARK 9.2.3. Theorem 9.2.2 is also referred to as the local reciprocity law.

We can quickly see a connection with class field theory over a finite field.

PROPOSITION 9.2.4. *Let K be a nonarchimedean local field and π a uniformizer of K. Let*

$$\iota_\pi \colon \mathbb{Z} \to \langle \pi \rangle$$

denote the isomorphism that sends 1 *to* π*. Let*

$$\mathrm{Res} \colon G_K^{\mathrm{ab}} \to G_{\kappa(K)}$$

be induced by the restriction map to $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ *and its natural isomorphism with* $G_{\kappa(K)}$*, as in Proposition 6.4.10. Then*

$$\mathrm{Res} \circ \rho_K \circ \iota_\pi \colon \mathbb{Z} \to G_{\kappa(K)}$$

is the reciprocity map $\rho_{\kappa(K)}$ *for the finite field* $\kappa(K)$*.*

REMARK 9.2.5. Given a nonarchimedean local field K and a finite abelian extension L of K, we at times also denote by $\rho_{L/K}$ the induced isomorphism

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

and refer to it also as the local reciprocity map for L/K.

REMARK 9.2.6. In the case K is $\mathbb{R}$ or $\mathbb{C}$, we can also define a reciprocity map. In the case of $\mathbb{C}$, the group $G_{\mathbb{C}}$ is trivial, so the reciprocity map is trivial $\rho_{\mathbb{C}} \colon \mathbb{C}^\times \to 1$. In the case of $\mathbb{R}$, it is the unique homomorphism

$$\rho_{\mathbb{R}} \colon \mathbb{R}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{R})$$

with kernel the positive reals $\mathbb{R}_{>0}$.

We remark that the following compatibilities among local reciprocity maps follow immediately from Proposition 8.1.18.

PROPOSITION 9.2.7. *Let K be a local field, and let L/K be a finite separable extension. Then we have commutative diagrams*

$$\begin{array}{ccc} L^\times & \xrightarrow{\rho_L} & G_L^{\mathrm{ab}} \\ \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle R_{L/K}} \\ K^\times & \xrightarrow{\rho_K} & G_K^{\mathrm{ab}} \end{array} \qquad \begin{array}{ccc} K^\times & \xrightarrow{\rho_K} & G_K^{\mathrm{ab}} \\ \downarrow{\scriptstyle i_{L/K}} & & \downarrow{\scriptstyle V_{L/K}} \\ L^\times & \xrightarrow{\rho_L} & G_L^{\mathrm{ab}} \end{array} \qquad \begin{array}{ccc} L^\times & \xrightarrow{\rho_L} & G_L^{\mathrm{ab}} \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma^*} \\ \sigma(L)^\times & \xrightarrow{\rho_{\sigma(L)}} & G_{\sigma(L)}^{\mathrm{ab}}, \end{array}$$

where $R_{L/K}$ denotes the restriction map, $i_{L/K}$ is the inclusion map, $V_{L/K}$ is the transfer map, and for any embedding $\sigma \colon L \hookrightarrow K^{\mathrm{sep}}$, the map σ^* is induced by conjugation $\tau \mapsto \sigma\tau\sigma^{-1}$ for $\tau \in G_L$.

It follows immediately from Theorem 9.2.2(ii), or Corollary 8.2.5, that we have

$$[L:K] = [K^\times : N_{L/K}L^\times] \tag{9.2.1}$$

for any finite abelian extension L of K in K^{sep}. Moreover, in the present context, Proposition 8.2.6 says the following.

PROPOSITION 9.2.8. *Let K be a local field, and let L and M finite abelian extensions of K. Then we have the following:*

a. $N_{L/K}L^\times \cap N_{M/K}M^\times = N_{LM/K}(LM)^\times$,

b. $N_{L/K}L^\times \cdot N_{M/K}M^\times = N_{(L\cap M)/K}(L\cap M)^\times$,

c. $N_{M/K}M^\times \subseteq N_{L/K}L^\times$ *if and only if* $L \subseteq M$,

d. for any subgroup A of $K^\times$ containing $N_{L/K}L^\times$, there exists an intermediate field E in L/K with $A = N_{E/K}E^\times$.

REMARK 9.2.9. The equality of degrees and the statements of Proposition 9.2.8 quite obviously hold for archimedean local fields as well. The extension $\mathbb{C}/\mathbb{R}$ is of course the only nontrivial extension in that setting, with norm group $N_{\mathbb{C}/\mathbb{R}}\mathbb{C}^\times = \mathbb{R}^\times_{>0}$ of index 2 in $\mathbb{R}^\times$.

9.3. Norm residue symbols

NOTATION 9.3.1. In this section, we fix an integer $n \geq 1$ and suppose that K is a local field of characteristic not dividing n such that K contains μ_n, the nth roots of unity in a separable closure K^{sep} of K.

DEFINITION 9.3.2. The nth *norm residue symbol* (or *Hilbert symbol*, or *Hilbert norm residue symbol*) for the field K is the pairing

$$(\ ,\ )_{n,K} \colon K^\times \times K^\times \to \mu_n$$

defined on $a, b \in K^\times$ by

$$(a,b)_{n,K} = \frac{\rho_K(b)(a^{1/n})}{a^{1/n}},$$

where $a^{1/n}$ is an nth root of α in K^{ab}.

REMARK 9.3.3. Since K contains μ_n, the nth roots of a lie in K^{ab}, and every element of G_K^{ab} acts trivially on μ_n, so the quantity $\sigma(a^{1/n})a^{-1/n}$ for $\sigma \in G_K^{\mathrm{ab}}$ is independent of the choice of nth root $a^{1/n}$ of a.

PROPOSITION 9.3.4. *The nth norm residue symbol for K has the following properties:*

a. it is bimultiplicative: i.e., for all $a, b, a', b' \in K^\times$, we have

$$(aa', b)_{n,K} = (a,b)_{n,K}(a',b)_{n,K} \quad \text{and} \quad (a, bb')_{n,K} = (a,b)_{n,K}(a,b')_{n,K},$$

b. $(a,b)_{n,K} = 1$ *for* $a,b \in K^\times$ *if and only if* $b \in N_{K(a^{1/n})/K}K(a^{1/n})^\times$,

c. $(a,1-a)_{n,K} = 1$ *for all* $a \in K - \{0,1\}$,

d. $(a,-a)_{n,K} = 1$ *for all* $a \in K^\times$,

e. it is skew-symmetric: i.e., $(a,b)_{n,K} = (b,a)_{n,K}^{-1}$ *for all* $a,b \in K^\times$,

f. it induces a perfect pairing on $K^\times/K^{\times n}$*: i.e.,* $(a,b)_{n,K} = 1$ *for a fixed* $a \in K^\times$ *(resp.,* $b \in K^\times$*) for all* $b \in K^\times$ *(resp.,* $a \in K^\times$*) if and only if* $a \in K^{\times n}$ *(resp.,* $b \in K^{\times n}$*).*

PROOF.

a. Note that we may choose $(aa')^{1/n}$ to equal $a^{1/n}(a')^{1/n}$. Since $\rho_K(b)$ is a homomorphism, we have

$$(aa',b)_{n,K} = \frac{\rho_K(b)((aa')^{1/n})}{(aa')^{1/n}} = \frac{\rho_K(b)(a^{1/n})}{a^{1/n}}\frac{\rho_K(b)((a')^{1/n})}{(a')^{1/n}} = (a,b)_{n,K}(a',b)_{n,K},$$

and since ρ_K is a homomorphism and $\rho_K(b) \in G_K^{\mathrm{ab}}$ acts trivially on μ_n, we have

$$(a,bb')_{n,K} = \frac{\rho_K(bb')(a^{1/n})}{a^{1/n}} = \frac{\rho_K(b)(a^{1/n})}{a^{1/n}} \cdot \rho_K(b)\left(\frac{\rho_K(b')(a^{1/n})}{a^{1/n}}\right) = (a,b)_{n,K}(a,b')_{n,K}.$$

b. Note that $(a,b)_{n,K} = 1$ if and only if $\rho_K(b)(a^{1/n}) = a^{1/n}$, so if and only if $\rho_K(b)$ fixes $K(a^{1/n})$, and so if and only if $\rho_{K(a^{1/n})/K}(b) = 1$. But this occurs if and only if b is a norm from $K(a^{1/n})$ by local reciprocity.

c. For any $c \in K^\times$ and a primitive nth root ζ_n of 1 in K, we may write

$$c^n - a = \prod_{i=0}^{n-1}(c - \zeta_n^i a^{1/n}) = N_{K(a^{1/n})/K}(c - a^{1/n}).$$

We then take $c = 1$ and apply (b).

d. Take $c = 0$ in the proof of (c) and again apply (b).

e. By (d) and (a), we have

$$1 = (ab,-ab)_{n,K} = (a,-a)_{n,K}(a,b)_{n,K}(b,a)_{n,K}(b,-b)_{n,K} = (a,b)_{n,K}(b,a)_{n,K}.$$

f. If $a \in K^{\times n}$, then write $a = c^n$ with $c \in K^\times$, and note that $(a,b)_{n,K} = (c,b)_{n,K}^n = 1$. On the other hand, if $(a,b)_{n,K} = 1$ for all $b \in K^\times$, then $\rho_{K(a^{1/n})/K}$ is the trivial homomorphism by the argument of (a). Local reciprocity then tells us that $K(a^{1/n}) = K$, so $a \in K^{\times n}$. The analogous statement switching the variables now follows immediately from (e).

□

REMARK 9.3.5. Part (b) of the Proposition 9.3.4, says that $(a,b)_{n,K} = 1$ for $a,b \in K^\times$ if and only if b is a norm from $K(a^{1/n})$. It is this property for which the norm residue symbol is named. Much

less obvious from the definition is the fact then obtained using the skew-symmetry of the symbol in part (e) of said proposition: that is, we also have $(a,b)_{n,K} = 1$ if and only if a is a norm from $K(b^{1/n})$. So, a is a norm from $K(b^{1/n})$ if and only if b is a norm from $K(a^{1/n})$.

Let us compute the norm residue symbol for $n = 2$, when $p = 2$, which is sometimes simply referred to as the Hilbert symbol.

PROPOSITION 9.3.6. *Let $a,b \in \mathbb{Z}_2^\times$. Then $(2,2)_{2,\mathbb{Q}_2} = 1$,*

$$(a,b)_{2,\mathbb{Q}_2} = (-1)^{(a-1)(b-1)/4} \quad \text{and} \quad (2,b)_{2,\mathbb{Q}_2} = (-1)^{(b^2-1)/8}.$$

PROOF. Note first that the expression $f(a,b) = (a-1)(b-1) \bmod 8$ for $a,b \in \mathbb{Z}_2^\times$ satisfies

$$f(aa',b) \equiv (a'(a-1)+a'-1)(b-1) \equiv f(a,b)+f(a',b) \bmod 8$$

and the expression $g(b) = b^2 - 1 \bmod 16$ satisfies

$$g(bb') \equiv (bb')^2 - 1 \equiv (b')^2(b^2-1) + ((b')^2-1) \equiv g(b)+g(b') \bmod 16,$$

so the right-hand sides of the equations of interest are multiplicative in the variables a and b. Since they are also continuous, it suffices to verify the formulas on a set of topological generators.

Recall that $\mathbb{Q}_2^\times$ is topologically generated by -1, 2, and 5. First, we claim that -1 is not a norm from $\mathbb{Q}_2(i)$, which is to say an element of the form a^2+b^2 with $a,b \in \mathbb{Q}_2^\times$. For this, note that it suffices to consider $a,b \in \mathbb{Z}_2^\times$ and then congruence modulo 4 eliminates the possibility. We therefore have $(-1,-1)_{2,\mathbb{Q}_2} = -1$. Since 2 and 5 are norms from $\mathbb{Q}_2(i)$, we have $(2,-1)_{2,\mathbb{Q}_2} = 1$ and $(5,-1)_{2,\mathbb{Q}_2} = 1$. We then have (noting (d) of Proposition 9.3.4) that

$$(2,2)_{2,\mathbb{Q}_2} = (2,-2)_{2,\mathbb{Q}_2}(2,-1)_{2,\mathbb{Q}_2} = 1$$

and similarly $(5,5)_{2,\mathbb{Q}_2} = 1$. Finally we calculate $(2,5)_{2,\mathbb{Q}_2}$. The question becomes whether $5 = a^2 - 2b^2$ for some $a,b \in \mathbb{Z}_2^\times$, but a^2, b^2 lie in $\{0,1,4\}$ modulo 8, and a quick check shows that the equality cannot hold modulo 8 and therefore $(2,5)_{2,\mathbb{Q}_2} = -1$. These values all agree with the stated values, as needed. □

In the case that n and the residue characteristic of K are coprime, the norm residue symbol is also not too difficult to compute. Note that in this case, the extensions $K(a^{1/n})$ with $a \in K^\times$ are tamely ramified.

DEFINITION 9.3.7. Suppose that n is relatively prime to the residue characteristic of K. Then $(\ ,\ )_{n,K}$ is called a *tame symbol*.

THEOREM 9.3.8. *Suppose that n is not divisible by the residue characteristic of K. Let q denote the order of the residue field κ of K, and note that n divides $q-1$ since K is assumed to contain μ_n. For $a,b \in K^\times$, let $[a,b]_K \in \kappa^\times$ be defined by*

$$[a,b]_K = (-1)^{v_K(a)v_K(b)} \frac{a^{v_K(b)}}{b^{v_K(a)}} \bmod \pi_K,$$

where π_K is a uniformizer of K. We then have

$$(a,b)_{n,K} = [a,b]_K^{(q-1)/n} \in \mu_n,$$

identifying elements of $\mu_n(\kappa)$ with their unique lifts to nth roots of unity in K.

PROOF. Let us first compute $(a,\pi_K)_{n,K}$ for a unit $a \in \mathscr{O}_K^\times$. Let $L = K(a^{1/n})$, and note that L/K is unramified. Therefore, $\rho_{L/K}(\pi_K)$ is the unique Frobenius element in $\mathrm{Gal}(L/K)$. In particular, we have

$$\rho_K(\pi_K)(a^{1/n}) \equiv (a^{1/n})^q \bmod \pi_K \mathscr{O}_L,$$

so

$$(a,\pi_K)_{n,K} \equiv a^{(q-1)/n} \bmod \pi_K,$$

as desired. Note that if $b \in \mathscr{O}_K^\times$ as well, then $\rho_{L/K}(b)$ is trivial since L/K is unramified, so $(a,b)_{n,K} = 1$.

In general, take $a,b \in K^\times$, and write $a = \pi_K^{v(a)}\alpha$ and $b = \pi_K^{v(b)}\beta$ with $\alpha,\beta \in \mathscr{O}_K^\times$. Writing $v = v_K$ for short, the properties of the norm residue symbol and the cases already computed yield

$$\begin{aligned}(a,b)_{n,K} &= (\pi_K,\pi_K)_{n,K}^{v(a)v(b)}(\alpha,\pi_K)^{v(b)}(\beta,\pi_K)^{-v(a)} \\ &= (\pi_K,-1)^{v(a)v(b)}\alpha^{v(b)(q-1)/n}\beta^{-v(a)(q-1)/n} = ((-1)^{v(a)v(b)}a^{v(b)}b^{-v(a)})^{(q-1)/n},\end{aligned}$$

as originally asserted. □

REMARK 9.3.9. We may also speak of the 2nd norm residue symbol for $\mathbb{R}$, which is defined in the same manner as for nonarchimedean local fields. It satisfies

$$(a,b)_{2,\mathbb{R}} = \begin{cases} -1 & \text{if } a,b<0, \\ 1 & \text{if } a,b>0, \end{cases}$$

since -1 is not a norm from $\mathbb{C}$ to $\mathbb{R}$. We can also speak of nth norm residue symbols for $\mathbb{C}$ for any n, but they are all of course trivial.

We end with a more cohomological description of norm residue symbols which can be useful. From now on, let us identify $\mathbb{Z}/n\mathbb{Z}$ with $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ via the inverse of multiplication by n. We denote the resulting injection $\mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z}$ by ι.

LEMMA 9.3.10. *The invariant map on* $\mathrm{Br}(K)$ *induces a canonical isomorphism*

$$H^2(G_K, \mu_n \otimes_{\mathbb{Z}} \mu_n) \xrightarrow{\sim} \mu_n.$$

PROOF. First, note that μ_n is a trivial G_K-module since μ_n is contained in K. Set $\mu_n^{\otimes 2} = \mu_n \otimes_{\mathbb{Z}} \mu_n$. First, there is a canonical isomorphism

$$H^i(G_K,\mu_n) \otimes_{\mathbb{Z}} \mu_n \to H^i(G_K,\mu_n^{\otimes 2})$$

for all $i \in \mathbb{Z}$ that is induced by the map of complexes

$$C^{\cdot}(G_K, \mu_n) \otimes_{\mathbb{Z}} \mu_n \to C^{\cdot}(G_K, \mu_n^{\otimes 2})$$

that takes an $f \otimes \zeta$, where $f \in C^i(G_K, \mu_n)$ and $\zeta \in \mu_n$ to the cochain with value on $x \in G^i$ given by $f(x) \otimes \zeta$.

Secondly, recall from Proposition B.5.4 that $H^2(G_K, \mu_n) \cong \mathrm{Br}(K)[n]$, and the invariant map induces an isomorphism $\mathrm{Br}(K)[n] \xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \xrightarrow{\iota^{-1}} \mathbb{Z}/n\mathbb{Z}$. In total, we have

$$H^i(G_K, \mu_n^{\otimes 2}) \cong \mu_n \otimes \mathbb{Z}/n\mathbb{Z} \cong \mu_n,$$

hence the result. □

Recall that Kummer theory provides an isomorphism $K^\times/K^{\times n} \xrightarrow{\sim} H^1(G_K, \mu_n)$, hence a canonical surjection from $K^\times$ to the latter group.

PROPOSITION 9.3.11. *The pairing* $(\ ,\ )$ *defined by the cup product through the composition*

$$(\ ,\ ) \colon K^\times \times K^\times \twoheadrightarrow H^1(G_K, \mu_n) \times H^1(G_K, \mu_n) \xrightarrow{\cup} H^2(G_K, \mu_n \otimes_{\mathbb{Z}} \mu_n) \xrightarrow{\sim} \mu_n$$

is equal to the norm residue symbol for K.

PROOF. Let $a, b \in K^\times$. Let $\chi_a \colon G_K \to \mu_n$ be the Kummer character attached to a. Fix a primitive nth root of unity ζ_n, let $\tilde{\chi} \colon G_K \to \mathbb{Z}/n\mathbb{Z}$ be defined by $\chi_a(\sigma) = \zeta_n^{\tilde{\chi}(\sigma)}$, and let $\chi = \iota \circ \tilde{\chi} \colon G_K \to \mathbb{Q}/\mathbb{Z}$. By definition and Proposition 8.1.10, we have

$$(a,b)_{n,K} = \chi_a(\rho_K(b)) = \zeta_n^{\iota^{-1}(\mathrm{inv}_K(b \cup \delta(\chi)))},$$

where δ is again the connecting homomorphism for $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. On the other hand,

$$\chi_a \cup \chi_b = (\tilde{\chi} \cup \chi_b) \otimes \zeta_n,$$

and we see that

$$(a,b) = \zeta_n^{\iota^{-1}(\mathrm{inv}_K(\tilde{\chi} \cup \chi_b))}$$

by construction of the isomorphism in Lemma 9.3.10.

It thus suffices to see that $b \cup \delta(\chi) = \tilde{\chi} \cup \chi_b$ in $\mathrm{Br}(K)[n]$. We compare 2-cocycles representing these classes, noting the antisymmetry

$$\tilde{\chi} \cup \chi_b = -(\chi_b \cup \tilde{\chi}).$$

Lift $\tilde{\chi}$ to a map $\chi \colon G_K \to \mathbb{Z}$, and choose an nth root β of b. Let $\sigma, \tau \in G_K$. By construction of δ, we have

$$\delta(\chi)(\sigma, \tau) = \frac{1}{n}(\psi(\sigma) + \psi(\tau) - \psi(\sigma\tau)) \in \mathbb{Z},$$

from which it follows that

$$(b \cup \delta(\chi))(\sigma, \tau) = b^{\delta(\chi)(\sigma,\tau)} = \beta^{\psi(\sigma)+\psi(\tau)-\psi(\sigma\tau)}$$

while, via the identification $\mu_n \otimes \mathbb{Z}/n\mathbb{Z} = \mu_n$, we have

$$(\chi_b \cup \tilde{\chi})(\sigma,\tau) = \chi_b(\sigma) \otimes \tilde{\chi}(\tau) = \left(\frac{\sigma(\beta)}{\beta}\right)^{\psi(\tau)} \in \mu_n.$$

The product of these 2-cocycles in $Z^2(G_K, (K^{\mathrm{sep}})^\times)$ is

$$\beta^{\psi(\sigma)}\beta^{-\psi(\sigma\tau)}\sigma(\beta)^{\psi(\tau)},$$

which is the value on (σ,τ) of the coboundary of the 1-cochain

$$\sigma \mapsto \beta^{\psi(\sigma)}.$$

□

9.4. The existence theorem

Let K be a local field. We give its separable closure K^{sep} the topology defined by the unique extension of the valuation on K to K^{sep} and then endow $(K^{\mathrm{sep}})^\times$ with the subspace topology. We will show that $((K^{\mathrm{sep}})^\times, \mathrm{inv})$ is a topological class formation. Note that the Galois group G_K acts continuously on $(K^{\mathrm{sep}})^\times$ since it its action preserves the valuation of elements.

PROPOSITION 9.4.1. *For any finite separable extension L of K, the norm map $N_{L/K}\colon L^\times \to K^\times$ has closed image and compact kernel.*

PROOF. Recall from Proposition 5.5.6 that $\mathscr{O}_L^\times$ is compact. Since $v_K \circ N_{L/K} = f_{L/K} v_L$, the kernel of the continuous map $N_{L/K}$ is a closed subgroup of $\mathscr{O}_L^\times$, hence is compact.

Since $\mathscr{O}_L^\times$ is compact, $N_{L/K}(\mathscr{O}_L^\times)$ is a closed subset of $\mathscr{O}_K^\times$. Note that

$$N_{L/K}\mathscr{O}_L^\times = \mathscr{O}_K^\times \cap N_{L/K}L^\times,$$

so

$$[\mathscr{O}_K^\times : N_{L/K}\mathscr{O}_L^\times] \leq [K^\times : N_{L/K}L^\times] = [L:K]$$

is finite. Being of finite index in $\mathscr{O}_K^\times$, the closed subgroup $N_{L/K}(\mathscr{O}_L^\times)$ is open in $\mathscr{O}_K^\times$. Since $\mathscr{O}_K^\times$ is open in $K^\times$, the group $N_{L/K}(\mathscr{O}_L^\times)$ is open in $K^\times$ as well. Finally, as a union of $N_{L/K}(\mathscr{O}_L^\times)$-cosets, the subgroup $N_{L/K}L^\times$ is open in $K^\times$, hence closed. □

PROPOSITION 9.4.2. *Let p be a prime, and suppose that the characteristic of K is not p. For any finite separable extension L of $K(\mu_p)$, the pth power map on $L^\times$ has finite kernel μ_p and image $L^{\times p}$ containing $D_L = \ker \rho_L$.*

PROOF. The first statement is obvious. If $a \in \ker\rho_L$, then $a \in N_{M/L}M^\times$ for every finite abelian extension M of L. In particular, for all $b \in L^\times$, we have that $a \in N_{L(b^{1/p})/L}L(b^{1/p})^\times$, so $(a,b)_{p,L} = 1$. Proposition 9.3.4f then implies that $a \in L^{\times p}$. □

PROPOSITION 9.4.3. *Every closed subgroup of $K^\times$ of finite index that contains $\mathscr{O}_K^\times$ is a norm group.*

PROOF. Note that $K^\times/\mathscr{O}_K^\times \cong \mathbb{Z}$ via the valuation map, which is in fact a homeomorphism if we give the left-hand side the quotient topology and the right-hand side the discrete topology. The closed subgroups of finite index in $\mathbb{Z}$ are the nontrivial subgroups, so the closed subgroups of finite index in $K^\times$ that contain $\mathscr{O}_K^\times$ are those of the form $\mathscr{N}_n = \langle \pi^n \rangle \mathscr{O}_K^\times$ for some $n \geq 1$ and a fixed uniformizer π. If K_n is the unramified extension of K of degree n, then every element of $K_n^\times$ has the form for some $i \in \mathbb{Z}$ and $u \in \mathscr{O}_{K_n}^\times$, and we have

$$N_{K_n/K}(\pi^i u) = \pi^{ni} N_{K_n/K}(u) \in \mathscr{N}_n.$$

The indices of the two subgroups $N_{K_n/K}K_n^\times \leq \mathscr{N}_n$ of $\mathscr{O}_K^\times$ are both n, the former being the consequence (9.2.1) of local reciprocity, so they must be equal. □

THEOREM 9.4.4 (Existence theorem of local CFT). *The closed subgroups of $K^\times$ of finite index are exactly the norm subgroups $N_{L/K}L^\times$ with L a finite abelian extension of K.*

We omit the proof of Theorem 9.4.4 for Laurent series fields and focus on the characteristic zero setting.

PROOF FOR p-ADIC FIELDS. The three properties of Definition 8.2.10 are satisfied by Propositions 9.4.1, 9.4.2, 9.4.3, so the result follows from Theorem 8.2.14. □

We also have the following, which is actually immediate from part (c) of Proposition 9.2.8.

THEOREM 9.4.5 (Uniqueness theorem of local CFT). *Let L and M be distinct finite abelian extensions of K. Then $N_{L/K}L^\times \neq N_{M/K}M^\times$.*

REMARK 9.4.6. Taken together, the existence and uniqueness theorems that there is a one-to-one correspondence between finite abelian extensions L of K and open subgroups of finite index in $K^\times$ given by taking L to $N_{L/K}L^\times$. In part for historical reasons, we have stated them separately. We have seen additional properties of this (inclusion-reversing) correspondence in parts (a) and (b) of Proposition 9.2.8.

Next, we see that local reciprocity and the existence theorem imply the following.

THEOREM 9.4.7. *Let K be a nonarchimedean local field.*

a. The reciprocity map ρ_K is continuous and injective with dense image.

b. The restriction of ρ_K to $\mathscr{O}_K^\times$ provides a topological isomorphism between $\mathscr{O}_K^\times$ and the inertia subgroup of G_K^{ab}.

PROOF. That ρ_K is continuous with dense image follows from Proposition 8.2.15. Recall that, by definition, the groups $U_i(K)$ with $i \geq 1$ form a basis of open neighborhoods of 1 in the topology on

K. They are not, however, of finite index in $K^\times$. However, the subgroups $\langle \pi^n \rangle \times U_i(K)$ with $i,n \geq 1$ are, and are clearly open. Moreover, their intersection is $\{1\}$. By the existence theorem, there exists a finite abelian extension $L_{n,i}/K$ such that $N_{L_{n,i}/K} L_{n,i}^\times = \langle \pi^n \rangle U_i(K)$. For $a \in K^\times$ with $a \neq 1$, we may then choose n and i large enough so that $a \notin N_{L_{n,i}/K} L_{n,i}^\times$, and therefore local reciprocity tells us that $\rho_{L_{n,i}/K}(a)$ is nontrivial, so $\rho_K(a)$ is nontrivial. That is, ρ_K is injective. This proves (a).

That ρ_K maps $\mathscr{O}_K^\times$ into the inertia group in G_K^{ab} is as follows. Every element $u \in \mathscr{O}_K^\times$ may be written as a quotient of two uniformizers π and π' by taking $\pi' = u\pi$ for any uniformizer π. By property (i) in the local reciprocity law, we have

$$\rho_K(u)|_{K^{\mathrm{ur}}} = \rho_K(\pi')|_{K^{\mathrm{ur}}} (\rho_K(\pi)|_{K^{\mathrm{ur}}})^{-1} = \varphi_K \varphi_K^{-1} = 1,$$

where φ_K is the Frobenius element of $\mathrm{Gal}(K^{\mathrm{ur}}/K)$. Hence, $\rho_K(u)$ lies in the inertia subgroup, and for the same reason, this occurs only when u is a unit. As for surjectivity onto inertia, the element $\rho_K(\pi)$ gives a choice of Frobenius, hence a splitting of the surjection $G_K^{\mathrm{ab}} \to \mathrm{Gal}(K^{\mathrm{ur}}/K)$. Via this splitting, the reciprocity map is the direct product of the continuous maps from $\mathscr{O}_K^\times$ to inertia and the group generated by π to $\mathrm{Gal}(K^{\mathrm{ur}}/K)$. Since ρ_K has dense image, the image of $\mathscr{O}_K^\times$ in inertia is therefore dense as well, and it suffices to see that $\rho_K(\mathscr{O}_K^\times)$ is closed. But ρ_K is continuous and $\mathscr{O}_K^\times$ is compact Hausdorff, so indeed this is the case, proving (b). □

We leave the following remark to the reader as an exercise.

LEMMA 9.4.8. *Let K be a nonarchimedean local field, and let π be a uniformizer of K. Let K_π denote the fixed field of $\rho_K(\pi)$ in K^{ab}. Then $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{ur}}$. Moreover, K_π is a maximal totally ramified extension of K in K^{ab}.*

We next prove the uniqueness of the local reciprocity map to complete the proof of the local reciprocity law.

THEOREM 9.4.9 (Uniqueness of the local reciprocity map). *The reciprocity map ρ_K is the unique map satisfying properties (i) and (ii) of Theorem 9.2.2.*

PROOF. We prove that if a homomorphism $\phi : K^\times \to G_K^{\mathrm{ab}}$ satisfies properties (i) and (ii) of Theorem 9.2.2 with ρ_K replaced by ϕ, then it is ρ_K. Consider the open subgroup $A_n = \langle \pi \rangle U_n(K)$ of finite index in $K^\times$. By the existence theorem, there exists a finite abelian extension L_n of K with norm group equal to A_n. The union of the fields L_n is the field K_π of Lemma 9.4.8. Being that $\pi \in A_n$ for all n, we have that by property (ii) of the local reciprocity law that $\phi(\pi)|_{K_\pi} = 1$,. On the other hand, by property (i), we have that $\phi(\pi)|_{K^{\mathrm{ur}}}$ is the Frobenius element of $\mathrm{Gal}(K^{\mathrm{ur}}/K)$. On the other hand, $\rho_K(\pi)$ also has both of these properties and $K^{\mathrm{ab}} = K_\pi \cdot K$, so $\rho_K(\pi) = \phi(\pi)$. Since this holds for every uniformizer of K and any $a \in K^\times$ can be written as $a = \pi^{v_K(a)-1} \cdot \pi'$ where π' is a uniformizer defined by this equality, the two maps ρ_K and ϕ are equal. □

We end with a few remarks on the topology of $K^\times$.

PROPOSITION 9.4.10. *Let K be a p-adic field. Then every subgroup of $K^\times$ of finite index is open.*

PROOF. Since A be a subgroup of finite index in $K^\times$, and let m be the exponent of $K^\times/A$. Then $K^{\times m} \subseteq A$, and Proposition 6.3.9 tells us that $K^\times/K^{\times m}$ is a finite abelian group (in fact, isomorphic to a subgroup of $(\mathbb{Z}/m\mathbb{Z})^{[K:\mathbb{Q}_p]+2}$). Thus $K^{\times m}$ has finite index in $K^\times$. As the mth power map is continuous and $\mathscr{O}_K^\times$ is compact, $\mathscr{O}_K^{\times m}$ is closed in $\mathscr{O}_K^\times$. Letting π_K denote a uniformizer for K, we then have that $K^{\times m} = \mathscr{O}_K^{\times m}\langle \pi_K^m \rangle$ is closed in $K^\times$, therefore open. As A is a union $K^\times$-cosets, it is open as well. □

COROLLARY 9.4.11. *Let K be a p-adic field. Then ρ_K induces a topological isomoprhism*

$$\widehat{K^\times} \xrightarrow{\sim} G_K^{\mathrm{ab}},$$

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

PROOF. By definition G_K^{ab} is isomorphic to the inverse limit of the system of groups $\mathrm{Gal}(L/K)$ for L/K finite abelian with respect to restriction maps. On the other hand, local reciprocity provides a series of isomorphisms

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

that are compatible with the natural quotient maps on the left and restriction maps on the right. In other words, local reciprocity sets up an isomorphism

$$\varprojlim_L K^\times/N_{L/K}L^\times \to G_K^{\mathrm{ab}}, \tag{9.4.1}$$

but as L runs over the finite abelian extensions, Proposition 9.4.10 tells us that the groups $N_{L/K}L^\times$ run over all subgroups of finite index in $K^\times$. Therefore, the inverse limit in (9.4.1) is just the profinite completion of $K^\times$. □

REMARKS 9.4.12.

a. The converse to Proposition 9.4.10 is false: for instance, $\mathscr{O}_K^\times$ is open in $K^\times$ but not of finite index.

b. If K is a Laurent series field, then its multiplicative group has subgroups of finite index that are not closed. To see this, recall that K is isomorphic to $\mathbb{F}_q(\!(t)\!)$ for some q. Recall from Proposition 6.3.10 that $U_1(K)$ and $\prod_{i=1}^\infty \mathbb{Z}_p$ are topologically isomorphic. Note that $\bigoplus_{i=1}^\infty \mathbb{Z}_p$ is dense in $\prod_{i=1}^\infty \mathbb{Z}_p$ but not closed. Any subgroup of finite index in the latter group containing the former group will therefore not be closed. Choose such a group U, and consider $\langle t \rangle U$. (We leave it as an exercise to apply Zorn's lemma to see that U exists.) This is a subgroup of finite index in $K^\times$ that is not closed.

c. For a Laurent series field K, the isomorphism (9.4.1) still holds, but the inverse limit of the multiplicative group modulo norm groups, while a profinite group, is no longer isomorphic to the profinite completion of $K^\times$.

9.5. Class field theory over $\mathbb{Q}_p$

In this section, we will determine the abelian extensions of $\mathbb{Q}_p$ and make explicit the reciprocity law for $\mathbb{Q}_p$. We shall not assume the results of the previous section.

LEMMA 9.5.1. *Let p be a prime, and let K be a field of characteristic not equal to p. Let $a \in K(\mu_p)^\times$. For a generator δ of $\mathrm{Gal}(K(\mu_p)/K)$, let $c \in \mathbb{Z}$ be such that $\delta(\zeta_p) = \zeta_p^c$ for any generator ζ_p of μ_p. Then $M = K(\mu_p, a^{1/p})$ is abelian over K if and only if*

$$\delta(a)a^{-c} \in K(\mu_p)^{\times p}.$$

PROOF. We may suppose without loss of generality that $a \notin K(\mu_p)^{\times p}$. Let $\tau \in \mathrm{Gal}(M/K(\mu_p))$ be a generator such that $\tau(a^{1/p}) = \zeta_p a^{1/p}$.

Suppose first that M/K is abelian. Lift δ to a generator of $\mathrm{Gal}(M/L)$, where L is the unique abelian subextension in M/K of degree p over K, and denote this also by δ. We have

$$\tau(\delta(a^{1/p})) = \delta(\tau(a^{1/p})) = \delta(\zeta)\delta(a^{1/p}) = \zeta_p^c \delta(a^{1/p}).$$

In terms of Kummer duality, this says that the Kummer pairing of τ and $\delta(a)$ is ζ_p^c. Since $M/K(\mu_p)$ is generated by a pth root of a and τ pairs with a^c to ζ_p^c as well, we have by the nondegeneracy of the Kummer pairing that $\delta(a)a^{-c} \in K(\mu_p)^{\times p}$.

Now, suppose that $\delta(a)a^{-c} = x^p$ for some $x \in K(\mu_p)^\times$. Extend δ to an embedding of M in $\overline{K}$. Note that $\delta(a^{1/p})$ is a pth root of $a^c x^p$, hence of the form $\zeta_p^j (a^{1/p})^c x$ for some $j \in \mathbb{Z}$, and this is an element of M. It follows that M/K is Galois. Moreover, we have

$$\tau(\delta(a^{1/p})) = \tau(\zeta_p^j a^{c/p} x) = \zeta_p^{j+c} a^{c/p} x = \zeta_p^c \delta(a^{1/p}) = \delta(\zeta a^{1/p}) = \delta(\tau(a^{1/p}))$$

and

$$\tau(\delta(\zeta_p)) = \zeta_p^c = \delta(\tau(\zeta_p))$$

since τ fixes μ_p. Thus, the generators δ and τ of $\mathrm{Gal}(M/K)$ commute, and so M/K is abelian. □

The following is a straightforward exercise using Lemma 6.3.7.

LEMMA 9.5.2. *For any prime p, we have*

$$U_1(\mathbb{Q}_p(\mu_p)) \cap \mathbb{Q}_p(\mu_p)^{\times p} = U_{p+1}(\mathbb{Q}_p(\mu_p)).$$

We also have the following.

LEMMA 9.5.3. *Let p be an odd prime. Let δ be a generator of $\mathrm{Gal}(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p)$, and let $c \in \mathbb{Z}$ be such that $\delta(\zeta_p) = \zeta_p^c$ for ζ_p generating μ_p. For any positive integer $i \leq p$ and $a \in U_i(\mathbb{Q}_p(\mu_p)) - U_{i+1}(\mathbb{Q}_p(\mu_p))$, one has*

$$\delta(a) \equiv a^{c^i} \bmod (1-\zeta_p)^{i+1}.$$

PROOF. Set $\lambda = 1 - \zeta_p$. Note first that for any $k \geq 1$, one has

$$1 - \zeta_p^k = \lambda \sum_{j=0}^{k-1} \zeta_p^j \equiv k\lambda \bmod \lambda^2.$$

In particular, we have $\delta(\lambda) \equiv c\lambda \bmod \lambda^2$. It follows from the binomial theorem that

$$\delta(\lambda)^i \equiv (c\lambda + (\delta(\lambda) - c\lambda))^i \equiv (c\lambda)^i \bmod \lambda^{i+1}.$$

Write $a = 1 + u\lambda^i$ for some $u \in \mathbb{Z}[\mu_p]^\times$. One then has

$$\delta(a) \equiv \delta(1 + u\lambda^i) \equiv 1 + u\delta(\lambda)^i \equiv 1 + uc^i\lambda^i \equiv (1 + u\lambda^i)^{c^i} \equiv a^{c^i} \bmod \lambda^{i+1}.$$

□

PROPOSITION 9.5.4.

a. Let p be an odd prime. The maximal abelian extension of $\mathbb{Q}_p$ of exponent p has Galois group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$.

b. The maximal abelian extension of $\mathbb{Q}_2$ of exponent 4 has Galois group isomorphic to $(\mathbb{Z}/4\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z}$.

PROOF. Let p be a prime and L be the maximal abelian extension of $\mathbb{Q}_p$ of exponent p. The restriction map

$$\mathrm{Gal}(L(\mu_p)/\mathbb{Q}_p(\mu_p)) \to \mathrm{Gal}(L/\mathbb{Q}_p) \tag{9.5.1}$$

is an isomorphism since $[\mathbb{Q}_p(\mu_p) : \mathbb{Q}_p]$ and $[L : \mathbb{Q}_p]$ are relatively prime,. By Kummer theory, there exists a unique subgroup Δ of $L(\mu_p)^\times$ containing $L(\mu_p)^{\times p}$ such that $L(\mu_p) = \mathbb{Q}_p(\mu_p, \sqrt[p]{\Delta})$. By Lemma 9.5.1, we have

$$\Delta = \{a \in \mathbb{Q}_p(\mu_p)^\times \mid \delta(a)a^{-c} \in \mathbb{Q}_p(\mu_p)^{\times p}\}.$$

Now suppose that p is odd. Let us set $U_i = U_i(\mathbb{Q}_p(\mu_p))$ for each $i \geq 1$. Note first that since the valuation of an element is unchanged by application of δ, any element of Δ must lie in $\langle\lambda^p\rangle\mathbb{Z}_p[\mu_p]^\times$. Moreover, every element of $\mu_{p-1}(\mathbb{Q}_p)$ is a pth power, so

$$\Delta = \mathbb{Q}_p(\mu_p)^{\times p} \cdot (U_1 \cap \Delta). \tag{9.5.2}$$

Now, it follows from Lemmas 9.5.1, 9.5.2, and 9.5.3, any non pth power in $U_1 \cap \Delta$ lies either in $U_1 - U_2$ or $U_p - U_{p+1}$. We know that $\mu_p \subseteq \Delta$, in that the group μ_{p^2} generates an abelian extension of $\mathbb{Q}_p$. If any other element x of $U_1 - U_2$ were in Δ, then there would exist a pth root of unity ξ such that $x\xi^{-1} \in U_2 \cap \Delta$, which would imply $x\xi^{-1} \in U_p$. Moreover, since $U_{p+1} \leq \mathbb{Q}_p(\mu_p)^{\times p}$, we have that U_p itself is contained in Δ. It follows that $U_1 \cap \Delta = \mu_p U_p$. Recall that $U_p/U_{p+1} \cong \mathbb{Z}/p\mathbb{Z}$. Applying (9.5.2), we see that

$$\Delta/\mathbb{Q}_p(\mu_p)^{\times p} \cong (\mathbb{Z}/p\mathbb{Z})^2.$$

Kummer theory tells us that

$$\mathrm{Gal}(L(\mu_p)/\mathbb{Q}_p(\mu_p)) \cong \mathrm{Hom}(\Delta/\mathbb{Q}_p(\mu_p)^{\times p}, \mu_p) \cong \mathrm{Hom}((\mathbb{Z}/p\mathbb{Z})^2, \mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^2.$$

Recalling (9.5.1), this implies the result.

If $p = 2$, then we note that $\Delta = \mathbb{Q}_2^\times$ has a minimal set of topological generators consisting of -1, 2, and 3. Otherwise, we omit the proof of part b. □

We now turn to the local Kronecker-Weber theorem.

THEOREM 9.5.5 (Local Kronecker-Weber). *Let p be a prime number. Then every finite abelian extension of $\mathbb{Q}_p$ is contained in $\mathbb{Q}_p(\mu_n)$ for some $n \geq 1$.*

PROOF. Since any finite abelian extension of $\mathbb{Q}_p$ will be a compositum of such a finite abelian extension of p-power and a finite abelian extension of prime-to-p power degree, it suffices to consider such fields separately. We recall that finite abelian extensions of $\mathbb{Q}_p$ of degree prime to p are tamely ramified. The maximal tamely ramified abelian extension of $\mathbb{Q}_p$ is equal to $\mathbb{Q}_p^{\mathrm{ur}}((-p)^{1/(p-1)})$, since $-p$ is a uniformizer of $\mathbb{Q}_p$, and we know that $\mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\mu_p)$ while $\mathbb{Q}_p^{\mathrm{ur}}$ is the field given by adjoining to $\mathbb{Q}_p$ all prime-to-p roots of unity. Hence, we have the result for such fields.

So, let L be an abelian extension of $\mathbb{Q}_p$ of exponent p^r for some $r \geq 1$, and set $G = \mathrm{Gal}(L/\mathbb{Q}_p)$. First consider odd p. By Proposition 9.5.4a, the group G/G^p is a quotient of $(\mathbb{Z}/p\mathbb{Z})^2$. By the structure theorem for finite abelian groups, G is then isomorphic to a quotient of $(\mathbb{Z}/p^r\mathbb{Z})^2$. On the other hand, $\mathbb{Q}_p(\mu_{p^{r+1}})$ is a totally ramified abelian extension of $\mathbb{Q}_p$ with Galois group

$$\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^{r+1}})/\mathbb{Q}_p) \cong \mathbb{Z}/p^r\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times,$$

and the field $\mathbb{Q}_p(\mu_{p^{p^r}-1})$ is an unramified abelian extension of $\mathbb{Q}_p$ with Galois group isomorphic to $\mathbb{Z}/p^r\mathbb{Z}$. It follows that $\mathbb{Q}_p(\mu_{p^{r+1}(p^{p^r}-1)})$ has a subfield with Galois group $(\mathbb{Z}/p^r\mathbb{Z})^2$ over $\mathbb{Q}_p$, and so said field is L. The result follows for odd p.

In the case that $p = 2$, Proposition 9.5.4b tells us that $G/G^4 \cong (\mathbb{Z}/4\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z}$. It follows that G is isomorphic to a quotient of $(\mathbb{Z}/2^r\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z}$. Now, we know that

$$\mathrm{Gal}(\mathbb{Q}_2(\mu_{2^{r+2}})/\mathbb{Q}_2) \cong \mathbb{Z}/2^r\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

As with p odd, we have an unramified cyclotomic extension of $\mathbb{Q}_2$, linearly disjoint from the totally ramified $\mathbb{Q}_2(\mu_{2^{r+2}})$ over $\mathbb{Q}_2$, with Galois group $\mathbb{Z}/2^r\mathbb{Z}$. So, there exists a cyclotomic extension of $\mathbb{Q}_2$ with Galois group $(\mathbb{Z}/2^r\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z}$, which must then be L. □

COROLLARY 9.5.6. *For any prime p, the maximal abelian extension of $\mathbb{Q}_p$ is given by adjoining all roots of unity in $\overline{\mathbb{Q}_p}$. That is, we have*

$$\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p(\mu_\infty),$$

where μ_∞ is the group of all roots of unity in $\overline{\mathbb{Q}_p}$.

With the knowledge of the maximal abelian extension of $\mathbb{Q}_p$ in hand, we are now prepared to give an explicit construction of the reciprocity map for $\mathbb{Q}_p$.

REMARK 9.5.7. If ζ is a p^kth root of unity in $\overline{\mathbb{Q}_p}$ for some prime p and $k \geq 1$, then ζ^a for any $a \in \mathbb{Z}_p$ is the well-defined root of unity equal to ζ^b for any $b \in \mathbb{Z}$ with $b \equiv a \bmod p^k$.

PROPOSITION 9.5.8. *For each $n \geq 1$, let ζ_n denote a primitive nth root of unity in $\mathbb{Q}_p^{\mathrm{ab}}$. There exists a unique homomorphism $\rho\colon \mathbb{Q}_p^\times \to G_{\mathbb{Q}_p}^{\mathrm{ab}}$ which, for $m \geq 1$ prime to p and $k \geq 1$, satisfies*

i. $\rho(p)(\zeta_{p^k}) = \zeta_{p^k}$ and $\rho(p)(\zeta_m) = \zeta_m^p$, and

ii. $\rho(u)(\zeta_{p^k}) = \zeta_{p^k}^{u^{-1}}$ and $\rho(u)(\zeta_m) = \zeta_m$ for every $u \in \mathbb{Z}_p^\times$.

The map ρ takes uniformizers in $\mathbb{Q}_p$ to Frobenius elements, and its restriction to $\mathbb{Z}_p^\times$ is an isomorphism onto the inertia subgroup of $G_{\mathbb{Q}_p}^{\mathrm{ab}}$.

PROOF. Recall that $\mathbb{Q}_p^{\mathrm{ur}}$ is given by adjoining all prime-to-p roots of unity in $\overline{\mathbb{Q}_p}$. Corollary 9.5.6 then tells us that

$$\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p^{\mathrm{ur}}(\mu_{p^\infty}) = \mathbb{Q}_p^{\mathrm{ur}} \cdot \mathbb{Q}_p(\mu_{p^\infty}),$$

where μ_{p^∞} is the group of p-power roots of unity in $\overline{\mathbb{Q}_p}$. Since $\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p$ is totally ramified, we have

$$\mathbb{Q}_p^{\mathrm{ur}} \cap \mathbb{Q}_p(\mu_{p^\infty}) = \mathbb{Q}_p,$$

and so

$$\begin{aligned} G_{\mathbb{Q}_p}^{\mathrm{ab}} = \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) &\cong \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p^{\mathrm{ur}}) \times \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p(\mu_{p^\infty})) \\ &\cong \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p), \end{aligned} \tag{9.5.3}$$

the latter isomorphism being the product of restriction maps.

We claim the automorphisms $\rho(p)$ and $\rho(u)$ for $u \in \mathbb{Z}_p^\times$ of μ_∞ specified in the statement of the theorem are actually restrictions of elements of $G_{\mathbb{Q}_p}^{\mathrm{ab}}$. Given this, since every root of unity is the product of roots of unity of prime-to-p and p-power order and $\mathbb{Q}_p^\times \cong \langle p \rangle \times \mathbb{Z}_p^\times$, it follows that ρ is indeed a homomorphism to $G_{\mathbb{Q}_p}^{\mathrm{ab}}$, and it is uniquely specified by the given conditions.

For the claim, it suffices by (9.5.3) to see that these automorphisms define automorphisms of the prime-to-p and p-power roots of unity that are the restrictions of Galois elements in $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p)$ and $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$, respectively. First, we note that $\rho(p)$ has the same action as the trivial element on p-power roots of unity and as the Frobenius element on prime-to-p roots of unity. In particular, $\rho(p)$ does extend to a Frobenius element of $G_{\mathbb{Q}_p}^{\mathrm{ab}}$.

On the other hand, $\rho(u)$ acts trivially on p-power roots of unity, so we need only see that its action on p-power roots of unity is the restriction of a Galois element. Note that the cyclotomic character The cyclotomic character

$$\chi\colon \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p) \to \varprojlim_k (\mathbb{Z}/p^k\mathbb{Z})^\times \cong \mathbb{Z}_p^\times, \qquad \chi(\sigma)(\zeta_{p^k}) = \zeta_{p^k}^{\chi(\sigma)}$$

for $\mathbb{Q}_p$ is an isomorphism in that $[\mathbb{Q}_p(\mu_{p^k}) : \mathbb{Q}_p] = p^{k-1}(p-1)$ for each k. Thus, we have that there exists $\sigma_u \in \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$ with $\chi(\sigma_u) = u$. We then have that $\rho(u)$ as defined is indeed the restriction of σ_u^{-1} on μ_{p^∞}. That is $\rho(u)$ does extend to a well-defined element of $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$. with $\rho(u)|_{\mathbb{Q}_p(\mu_{p^\infty})} = \sigma_u^{-1}$. Moreover, as ρ on $\mathbb{Z}_p^\times$ followed by restriction to $\mathbb{Q}_p(\mu_{p^\infty})$ is the inverse map to the map taking σ to $\chi(\sigma)^{-1}$, we have that $\rho|_{\mathbb{Z}_p^\times}$ is an isomorphism to inertia in $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$.

Finally note that $\rho(p)$ is by definition a Frobenius element and $\rho(u)$ for $u \in \mathbb{Z}_p^\times$ has image in inertia, so $\rho(pu)$ is a Frobenius element as well. Since u was arbitrary, ρ takes uniformizers to Frobenius elements. □

Though we omit the proof, it is possible to show using the uniqueness in Theorem 9.2.2 (after computations of norm groups of abelian extensions of $\mathbb{Q}_p$) that the map ρ of Proposition 9.5.8 must indeed be the local reciprocity map for $\mathbb{Q}_p$.

THEOREM 9.5.9. *The map ρ constructed in Proposition 9.5.8 is the local reciprocity map $\rho_{\mathbb{Q}_p}$.*

9.6. Ramification groups and the unit filtration

DEFINITION 9.6.1. Let L/K be a Galois extension of local fields with Galois group G. Then $\psi_{L/K} \colon [-1,\infty) \to [-1,\infty)$ be defined to be the inverse of the function $\phi_{L/K}$ of Definition 6.5.19.

This allows us to define ramification groups in the upper numbering.

DEFINITION 9.6.2. Let L/K be a Galois extension of local fields with Galois group G. For any real number $s \geq -1$, we define the sth ramification group G^s of L/K in the *upper numbering* (or *upper ramification group*) by $G^s = G_{\psi_{L/K}(s)}$.

REMARKS 9.6.3. Suppose that L/K is a Galois extension of local fields with Galois group G.

a. Since $\phi_{L/K} = \psi_{L/K}^{-1}$, we have $G_t = G^{\phi_{L/K}(t)}$ for all $t \geq -1$.

b. For the same reason, we have

$$\psi_{L/K}(s) = \int_0^s [G^0 : G^y]dy$$

for any $s \geq 0$.

EXAMPLE 9.6.4. Let $F_n = \mathbb{Q}_p(\mu_{p^n})$ for a prime p and $n \geq 1$. As a consequence of Example 6.5.21, we have

$$\psi_{F_n/\mathbb{Q}_p}(s) = \begin{cases} s & \text{if } -1 \leq s \leq 0, \\ p^{k-1}(1+(p-1)(s-k+1))-1 & \text{if } k-1 \leq s \leq k \text{ with } 1 \leq k \leq n-1, \\ p^{n-1}(1+(p-1)(s-n+1))-1 & \text{if } s \geq n-1 \end{cases}$$

for all $s \geq -1$.

The following property of the ψ-function is immediate from Proposition 6.5.26.

LEMMA 9.6.5. *Let L/K be a Galois extension of local fields and E a normal subextension of K in L. Then*

$$\psi_{L/K} = \psi_{L/E} \circ \psi_{E/K}.$$

We also see that ramification groups in the upper numbering are compatible with quotients.

PROPOSITION 9.6.6. *Let L/K be a Galois extension of fields with Galois group G, let E/K be a Galois subextension, and set $N = \mathrm{Gal}(L/E)$. For any $s \geq -1$, one has*

$$(G/N)^s = G^s N/N.$$

PROOF. By definition of the upper numbering and the function $\psi_{L/E}$, Herbrand's theorem, and Lemma 9.6.5, we have

$$(G/N)^s = (G/N)_{\psi_{E/K}(s)} = G_{\psi_{L/E}(\psi_{E/K}(s))}N/N = G_{\psi_{L/K}(s)}N/N = G^s N/N.$$

□

We therefore have the following example.

PROPOSITION 9.6.7. *Let p be a prime and $n \geq 1$. Then for any $s \geq -1$, we have*

$$\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)^s = \begin{cases} \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p) & \text{if } -1 \leq s \leq 0, \\ \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p(\mu_{p^k})) & \text{if } k-1 < s \leq k \text{ with } 1 \leq k \leq n-1 \\ 1 & \text{if } s > n-1. \end{cases}$$

PROOF. This is quickly calculated using Proposition 6.5.12 and Example 9.6.4. □

DEFINITION 9.6.8. Let L/K be a Galois extension of local fields with Galois group G. A real number $s \in [-1, \infty)$ is said to be a *jump in the ramification filtration* of L/K (in the upper numbering) if $G^s \neq G^{s+\varepsilon}$ for all $\varepsilon > 0$.

EXAMPLE 9.6.9. The jumps in the ramification filtration of $\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p$ are $0, 1, 2, \ldots, n-1$.

Note that the jumps in the ramification filtration of $\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p$ for a prime p and $n \geq 1$ are always integers, though there may seem to be no a priori reason for them to be so. In fact, the jumps in the ramification filtration of an abelian extension of local fields are always integers. The following related result is known as the Hasse-Arf theorem: in the form stated it is actually due to Hasse. We state it without proof.

THEOREM 9.6.10 (Hasse). *Let K be a local field and L be a finite abelian extension of K with Galois group G. Then the jumps in the ramification filtration of G (in the upper numbering) are all integers.*

We next state, also without proof, the following remarkable connection between the reciprocity map and ramification groups in the upper numbering.

THEOREM 9.6.11. *Let K be a local field and L be a finite abelian extension of K with Galois group G. Then $\rho_{L/K}(U_i(K)) = G^i$ for all $i \geq 0$.*

We have the following immediate corollary.

COROLLARY 9.6.12. *Let L/K be a finite abelian extension of local fields with Galois group G. Then G^i is trivial for some $i \geq 1$ if and only if*

$$U_i(K) \subseteq N_{L/K}L^\times.$$

We make the following definition.

DEFINITION 9.6.13. Let L/K be a finite abelian extension of local fields. The conductor $\mathfrak{f}_{L/K}$ of the extension L/K is the ideal $\mathfrak{m}_K^r$, where $\mathfrak{m}_K$ is the maximal ideal of the valuation ring of K and r is the smallest positive integer such that $U_r(K) \subseteq N_{L/K}L^\times$.

REMARK 9.6.14. By Corollary 9.6.12, the conductor of a finite abelian extension L/K of local fields is $\mathfrak{m}_K^r$, where r is the smallest integer such that the upper ramification group $\mathrm{Gal}(L/K)^r$ is trivial. This r is one more than the last jump in the ramification filtration of $\mathrm{Gal}(L/K)$, recalling the integrality of the jumps that is the Hasse-Arf theorem.

We leave as an exercise to the reader the computation of the conductor of an arbitrary finite abelian extension of $\mathbb{Q}_p$ using local Kronecker-Weber and the computation of the upper ramification groups of $\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p$. The result is as follows.

EXAMPLE 9.6.15. The conductor of a finite abelian extension L of $\mathbb{Q}_p$ is (p^n), where n is maximal such that L is contained in an unramified extension of $\mathbb{Q}_p(\mu_{p^n})$.

Let us consider one nontrivial example.

PROPOSITION 9.6.16. *Let p be an odd prime and $K = \mathbb{Q}_p(\mu_p)$. Set $L = K((1-p)^{1/p})$. The conductor of the extension L/K is $(1-\zeta_p)^2$.*

PROOF. Note that $L/\mathbb{Q}_p$ is totally ramified of degree $p(p-1)$. Let ζ_p be a primitive pth root of unity in K. We have that

$$p = N_{\mathbb{Q}_p((1-p)^{1/p})/\mathbb{Q}_p}(1-(1-p)^{1/p}),$$

so $\pi = 1-(1-p)^{1/p}$ is a uniformizer of $\mathbb{Q}_p((1-p)^{1/p})$. It follows that $v_L(\pi) = p-1$ and then, since $v_L(1-\zeta_p) = p$, that $\lambda = (1-\zeta_p)/\pi$ is a uniformizer of L.

For $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma((1-p)^{1/p}) = \zeta_p(1-p)^{1/p}$, we have

$$\frac{\sigma(\lambda)}{\lambda} = \frac{\pi}{\sigma(\pi)}.$$

and

$$\sigma(\pi) = 1-\zeta_p(1-p)^{1/p} = \pi + (1-\zeta_p)(1-p)^{1/p}.$$

Thus, noting that $v_L(1-\zeta_p) = p$, we have

$$v_L\Big(\frac{\sigma\lambda}{\lambda} - 1\Big) = 1.$$

It follows that the first (and last) jump in the upper numbering in the ramification filtration of $\mathrm{Gal}(L/K)$ is at 1, and therefore by Remark 7.4.19, we have $\mathfrak{f}_{L/K} = (1-\zeta_p)^2$, as asserted. □

9.7. Lubin-Tate formal groups

Let R denote a commutative ring.

REMARK 9.7.1. Consider the power series ring $A = R[\![x_1,\dots,x_n]\!]$ in n variables over R. The composition $f \circ g$ of $f, g \in A$ is well-defined in A so long as g has zero constant term, i.e., $g \in (x_1,\dots,x_n)$.

LEMMA 9.7.2. *The following are equivalent for a power series $f \in xR[\![x]\!]$:*

i. f has a left inverse under composition,

ii. f has a right inverse under composition,

iii. $f \equiv ux \bmod (x^2)$ with $u \in R^\times$.

Moreover, if f has an inverse, then it is unique.

PROOF. Suppose that $f \equiv ux \bmod (x^2)$ with $u \in R^\times$. Let $g_1 = u^{-1}x$, and suppose we have found $g_n \in R[x]$ of degree at most n such that $f \circ g_n$ and $g_n \circ f$ are both x in $R[x]/(x^{n+1})$. Write $f \circ g_n = x + ax^{n+1} \bmod (x^{n+2})$ for some $a \in R$. We then set $g_{n+1} = g_n - u^{-1}ax^{n+1}$ and note that

$$f \circ g_{n+1} = f \circ (g_n - u^{-1}ax^{n+1}) \equiv f \circ g_n - ax^{n+1} \equiv x \bmod (x^{n+2})$$

in that $(g_n - u^{-1}ax^{n+1})^k \equiv g_n^k \bmod (x^{n+2})$ for any $k \geq 2$. Let $g = \lim_{n\to\infty} g_n \in R[\![X]\!]$ so that $f \circ g = x$. Now, g also has some right inverse h, and so $x = g \circ h = g \circ f \circ g \circ h = g \circ f$. Moreover, note that g_n specified recursively as above is unique with the property that $f \circ g_n \equiv x \bmod (x^{n+1})$.

Finally, suppose that $f, g \in xR[\![x]\!]$. If $f \equiv ax \bmod (x^2)$ and $g \equiv bx \bmod x^2$, then $f \circ g \equiv abx \bmod x^2$, so if $f \circ g = x$, then a and b must both be units in R. □

DEFINITION 9.7.3. A (commutative) *formal group law* over R is a polynomial $F \in R[\![x,y]\!]$ such that

i. $F(x,y) \equiv x + y \bmod (x,y)^2$,

ii. $F(F(x,y),z) = F(x,F(y,z))$ in $R[\![x,y,z]\!]$, and

iii. $F(x,y) = F(y,x)$.

LEMMA 9.7.4. *Let $F \in R[\![x,y]\!]$ be a formal group law. Then*

a. $F(x,y) \equiv x + y \bmod (xy)$, and

b. there exists a unique $\iota_F(x) \in R[\![x]\!]$ *such that* $F(x, \iota_F(x)) = 0$.

PROOF. For part (a), set $f = F(x,0)$, so $f \equiv x \bmod (x^2)$. We also have $F(F(x,0),0) = F(x,0)$, so $f \circ f = f$, which forces $f = x$. For part (b), we leave it to the reader to check recursively that for any $F \in R[\![x,y]\!]$ having the form in part (a), there exists a unique $\iota_F(x) \equiv -x \bmod (x^2)$ with the desired property. □

EXAMPLES 9.7.5.

a. We have the *additive formal group law* $F(x,y) = x+y$. Here, we have $\iota_F(x) = -x$.

b. We have the *multiplicative formal group law* $G(x,y) = x+y+xy$. Note that $\iota_G = (x+1)^{-1} - 1$, as $G(x,y) = (x+1)(y+1) - 1$.

DEFINITION 9.7.6. A *homomorphism* $f\colon F \to G$ *of formal group laws* F and G is a power series $f \in xR[\![x]\!]$ such that $f(F(x,y)) = G(f(x), f(y))$. We write $f \circ F = G \circ f$ for to denote that f is such a homomorphism.

We can compose homomorphisms of formal group laws by composing the power series which define them, and we can add them as well.

DEFINITION 9.7.7. Let F and G be formal groups over R.

a. The *group of homomorphisms* from F to G is the set $\mathrm{Hom}(F,G)$ of homomorphisms from F to G with the operation of addition of power series.

b. The *ring of endomorphisms* of F is the set $\mathrm{End}(F)$ of endomorphisms of F with the operations of addition and composition of power series.

REMARK 9.7.8. An isomorphism of formal group laws $f\colon F \xrightarrow{\sim} G$ is a homomorphism given by a power series with an inverse f^{-1} under composition.

If R is a complete local ring with maximal ideal $\mathfrak{m}$, any power series in $R[\![x]\!]$ converges on $\mathfrak{m}$. Given the existence of the inverse power series of Lemma 9.7.4(b), a commutative formal group law then defines the structure of an abelian group on $\mathfrak{m}$.

DEFINITION 9.7.9. For a complete local ring R with maximal ideal $\mathfrak{m}$, a *formal group* is $\mathfrak{m}$ together with the group law $a +_F b = F(a,b)$ for $a, b \in \mathfrak{m}$, where $F \in R[\![x,y]\!]$ is a formal group law.

NOTATION 9.7.10.

a. The *additive formal group*, with formal group law $x+y$. is denoted $\mathbb{G}_a$.

b. The *multiplicative formal group*, with formal group law $x+y+xy$, is denoted $\mathbb{G}_m$.

Our interest is in a class of formal groups particularly useful for studying abelian extensions of local fields. Let K denote a local field with valuation ring $\mathscr{O}$, and maximal ideal $\mathfrak{m}$. Let q denote the order of the residue field $\kappa = \mathscr{O}/\mathfrak{m}$.

DEFINITION 9.7.11. A *Lubin-Tate power series* for K is a power series $f \in \mathscr{O}[\![x]\!]$ such that $f(x) \equiv x^q \bmod \pi$ and $f(x) \equiv \pi x \bmod (x^2)$, where π is a uniformizer of K.

NOTATION 9.7.12. For a uniformizer π of K, we let $\mathfrak{F}_\pi$ denote the set of Lubin-Tate power series over K with $f(x) \equiv \pi x \bmod (x^2)$.

Let us fix a uniformizer π of K. We omit, for now, the proof of the following key result.

PROPOSITION 9.7.13. *Let $f, g \in \mathscr{F}_\pi$. Let $\ell = \sum_{i=1}^n a_i x_i$ with $a_i \in \mathscr{O}$ for $1 \leq i \leq n$, and where the x_i are indeterminates. Then there exists a unique $F \in \mathscr{O}[\![x_1, \ldots, x_n]\!]$ such that $F \equiv \ell \bmod (x_1, \ldots, x_n)^2$ and $f(F(x_1, \ldots, x_n)) = F(g(x_1), \ldots, g(x_n))$.*

PROOF. Let $I = (x_1, \ldots, x_n)$. Set $\ell_1 = \ell$ and $F_0 = 0$, and suppose we have constructed $F_k = F_{k-1} + \ell_k$ for some k, where $\ell_k \in \mathscr{O}[x_1, \ldots, x_n]$ is homogeneous of degree k, such that

$$f \circ F_k \equiv F_k \circ g \bmod \pi I^{k+1}.$$

Let $H \equiv 0 \bmod \pi$ be the homogeneous of degree $k+1$ part of $f \circ F_k = F_k \circ g$, and set $\ell_{k+1} = -(\pi - \pi^{k+1})^{-1} H \in \mathscr{O}[x]$. Set $F_{k+1} = F_k + \ell_{k+1}$. Then

$$f \circ F_{k+1} \equiv f \circ F_k + \pi \ell_{k+1} \bmod I^{k+2},$$

while

$$F_{k+1} \circ g \equiv F_k \circ g + \pi^{k+1} \ell_{k+1} \bmod I^{k+2}$$

so subtracting the two equations, we have

$$f \circ F_{k+1} - F_{k+1} \circ g \equiv H + (\pi - \pi^{k+1}) \ell_{k+1} \equiv 0 \bmod I^{k+2}.$$

Since $f, g \equiv x^q \bmod \pi$, we also have

$$f \circ F_{k+1} - F_{k+1} \circ g \equiv (F_{k+1})^q - F_{k+1}(x^q) \equiv 0 \bmod \pi,$$

where $(F_{k+1})^q$ denotes qth power in the power series ring. Thus, the difference lies in πI^{k+1}, and we may continue the recursion. Setting $F = \sum_{k=1}^\infty \ell_k$, the uniqueness is clear from the uniqueness of H at each step. □

DEFINITION 9.7.14. A *Lubin-Tate formal group law* associated to $f \in \mathscr{F}_\pi$ is a formal group law $F_f \in \mathscr{O}[\![x, y]\!]$, where $f \in \mathscr{O}[x]$ is a Lubin-Tate power series which is an endomorphism for F_f, which is to say $f \circ F_f = F_f \circ f$.

Taking the linear form in Proposition 9.7.13 to be $x + y$, we see that F_f is uniquely specified by f.

COROLLARY 9.7.15. *Given $f \in \mathscr{F}_\pi$, there exists a unique Lubin-Tate formal group law associated to f.*

PROOF. The proposition provides a power series $F_f \in \mathscr{O}[\![x,y]\!]$ with $F_f \equiv x+y \bmod (x,y)^2$ such that f is an endomorphism of F_f. That $F_f(x,y) = F_f(y,x)$ follows by the uniqueness therein, since $x+y = x+y$. Similarly, that $F_f(x,F_f(y,z)) = F_f(F_f(x,y),z)$ follows as both commute with f and have linear terms $x+y+z$. □

We also have the following.

COROLLARY 9.7.16. *Let $f \in \mathscr{F}_\pi$. For any $a \in \mathscr{O}$, there exists a unique power series $[a]_f \in \mathscr{O}[\![x]\!]$ with $[a]_f \equiv ax \bmod (x^2)$ and which commutes with f under composition. In particular, $[\pi]_f = f$. Moreover, $[a]_f$ is an endomorphism of F_f, and the resulting map $[\ ]_f \colon \mathscr{O} \to \mathrm{End}(\mathscr{F}_\pi)$ is an injective ring homomorphism.*

PROOF. We take $n = 1$, $\ell(x) = ax$, and $g = f$ in Proposition 9.7.13 to define $[a]_f$. To see that $[a]_f$ is an endomorphism of F_f, note that $F_f \circ [a]_f$ and $[a]_f \circ F_f$ both have linear terms $ax+ay$ and commute with f, so we can again use uniqueness in the proposition. The rest follows similarly by uniqueness of the power series $[a]_f$, aside from the injectivity of the ring homomorphism they determine, which follows as $[a]_f \equiv ax \bmod x^2$, and $ax \equiv bx \bmod x^2$ if and only if $a = b$. □

COROLLARY 9.7.17. *Let $f,g \in \mathscr{F}_\pi$ be Lubin-Tate power series for K. Then F_f and F_g are isomorphic.*

PROOF. Suppose $f \in \mathscr{F}_\pi$ and $g \in \mathscr{F}_\pi$. Apply Proposition 9.7.13 with $\ell = x$ to get a power series $h \in \mathscr{O}[\![x]\!]$ with $f \circ h = h \circ g$. Then $F_f \circ h$ and $h \circ F_g$ both have linear terms $x+y$. Since $f \circ (F_f \circ h) = F_f \circ (f \circ h) = (F_f \circ h) \circ g$ and similarly with $h \circ F_g$, uniqueness gives that $F_f \circ h = h \circ F_g$. As h is invertible, we have that h provides the isomorphism. □

EXAMPLE 9.7.18. For $K = \mathbb{Q}_p$, set $f(x) = (x+1)^p - 1 \in \mathscr{F}_p$. Then the multiplicative formal group law $G = (x+1)(y+1)-1$ satisfies $f \circ F = (x+1)^p(y+1)^p - 1 = F \circ f$, so $G = F_f$. That is, the associated Lubin-Tate formal group to f is $\mathbb{G}_m$. We have $[a]_f = (x+1)^a - 1 \in \mathbb{Z}_p[\![x]\!]$ for $a \in \mathbb{Z}_p$.

The power series $[u]_f$ associated to a unit $u \in \mathscr{O}^\times$ is an isomorphism of F_f, so it can have no zeros in the maximal ideal of the valuation ring of the completion of an algebraic closure of K. On the other hand, $[\pi]_f$ certainly can and does.

DEFINITION 9.7.19. For $n \geq 0$, the *π^n-torsion in the formal group associated to f* is the kernel $W_{f,n}$ of $[\pi^n]_f$ on the maximal ideal in the completion of an algebraic closure of K. We refer to $W_{f,n} - W_{f,n-1}$ for $n \geq 1$ as the *primitive π^n-torsion*. The *torsion in the formal group of f* is $W_f = \bigcup_{n=1}^\infty W_{f,n}$.

THEOREM 9.7.20. *For $n \geq 1$ and $f \in \mathscr{F}_\pi$, we have the following.*

a. The field extension $K_{\pi,n} = K(W_{f,n})$ is a totally ramified Galois extension of K, independent of f.

b. Any primitive n-torsion element $\varpi_n \in W_f^n$ is a uniformizer in K_n.

c. The group W_f^n is a free $(\mathscr{O}/\mathfrak{m}^n)$-module of rank 1 for the action of $\mathscr{O}$ via $[\ ]_f$.

d. There is an isomorphism of groups $\chi_{f,n}\colon \mathrm{Gal}(K_n/K) \to (\mathscr{O}/\mathfrak{m}^n)^\times$ with inverse taking the image of $a \in \mathscr{O}^\times$ to the Galois element σ such that $[a]_f(\varpi_n) = \sigma(\varpi_n)$.

PROOF. Suppose that $f = \pi x + x^q$, which is x times an Eisenstein polynomial. In general, we see that $[\pi^n]_f = f \circ f \circ \cdots \circ f$ is $[\pi^{n-1}]_f$ times an Eisenstein polynomial of degree $q^{n-1}(q-1)$ which has as its roots the primitive π^n-torsion of F_f. Setting $K_n = K(W_{f,n})$, this forces K_n/K to be not just algebraic, but Galois and totally ramified of degree $q^{n-1}(q-1)$, having any $\varpi_n \in W_f^n - W_f^{n-1}$ as a uniformizer. As $[a]_f(\varpi_n) \equiv a\varpi_n \bmod \varpi_n^2$ for $a \in \mathscr{O}^\times$, we see that $W_f^n - W_f^{n-1}$ is free of rank 1 over $(\mathscr{O}/\mathfrak{m}^n)^\times$ under the action of $[\ ]_f$. It follows that $\sigma(\varpi_n) \in W_f^n$ equals $[a]_f(\varpi_n)$ for some $a \in \mathscr{O}^\times$, unique modulo $\mathfrak{m}^n$. It is then clear that $\chi_{f,n}$ defines an isomorphism.

In general, let $g \in \mathscr{F}_\pi$, and suppose that h is an isomorphism from F_f to F_g so that $h \circ f = g \circ h$. Then $[\pi^n]_g(h(\varpi_n)) = 0$, and it follows h defines an $\mathscr{O}$-module isomorphism between $W_{f,n}$ and $W_{g,n}$. Since $h \in \mathscr{O}[\![x]\!]$ with $h \equiv x \bmod x^2$, we have that $h(\varpi_n) \in W_{g,n} - W_{g,n-1}$ converges to a uniformizer in $K(W_{f,n})$, and therefore $K_n = K(W_{g,n})$. For $\sigma \in \mathrm{Gal}(K_n/K)$, we have $\sigma(h(\varpi_n)) = h(\sigma(\varpi_n))$, and if $\chi_{f,n}(\sigma) = a \bmod \mathfrak{m}^n$, then $[a]_g(h(\varpi_n)) = h([a]_f(\varpi_n)) \equiv h(\sigma(\varpi_n)) \equiv \sigma(h(\varpi_n)) \bmod \mathfrak{m}^n$. Thus, the proposition holds for g as it holds for f. □

Observing that $\mathscr{O}^\times \cong \varprojlim_n (\mathscr{O}/\mathfrak{m}^n)^\times$, we have the following.

COROLLARY 9.7.21. *The field $K_{\pi,\infty} = K(W_{f,\infty})$ is a totally ramified Galois extension of K with, independent of $f \in \mathscr{F}_\pi$, with Galois group isomorphic to $\mathscr{O}^\times$.*

We omit the proof of the following lemma.

LEMMA 9.7.22. *Let $h = \sum_{i=0}^n a_i x^i \in \mathbb{F}_q[x]$ be monic of degree $n \geq 1$ with $\gcd(q,n) = 1$. Then there exists $k \geq 1$ and $r \in \mathbb{F}_q[x]$ with $\deg r \leq k$ and $r(0) = 1$ such that $g = x^k h + r$ has no multiple zeros.*

PROOF. Let $m \geq 1$ be such that $q^m > n$ and $\mathbb{F}_{q^m}$ contains the roots of h'. Then set $k = q^{m+1}$ and $r = -x^q h + 1$. We then have $g = (x^{q^{m+1}} - x^q)h + 1$ and $g' = (x^{q^{m+1}} - x^q)h'$. If α is a root of $x^{q^{m+1}} - x^q$, then $g(\alpha) = 1$. If α is a root of h', then it lies in $\mathbb{F}_{q^m}$, so $g(\alpha) = (\alpha^q - \alpha^q)h(\alpha) + 1 = 1$ as well. □

PROPOSITION 9.7.23. *For $n \geq 1$, we have $N_{K_{\pi,n}/K} K_{\pi,n}^\times = \langle \pi \rangle U_n(K)$.*

PROOF. We know that $K_{\pi,n} = K(W_f^n)$ with $f = \pi x + x^q$. Moreover, $[\pi^n]_f = [\pi^{n-1}]_f \cdot h_n$, where h_n is $\pi + [\pi^{n-1}]_f^{q-1}$. This has leading coefficient π, and its roots are the primitive π^n-torsion elements for F_f. In particular, $\pi = N_{K_{\pi,n}/K}(\varpi_n)$ if $K_{\pi,n}/K$ is nontrivial (i.e., other than the case that q even and $n = 1$).

It is now enough to show that the norms of units from $K_{\pi,n}$ are contained in $U_n(K)$ since local reciprocity implies that $q^{n-1}(q-1) = [K^\times : N_{K_{\pi,n}/K} K_{\pi,n}^\times]$. The norms of elements of μ_{q-1} are clearly trivial, so it suffices to consider norms of 1-units.

Let $u = 1 + \sum_{i=1}^{\infty} a_i \varpi_n^i \in U_1(K_{\pi,n})$ with $a_i \in \mathscr{O}_K$, and set $a_0 = 1$. Let $p = \sum_{i=0}^{m-1} a_{n-i} x^i$, where $m = q^{n-1}(q-1)n$. Apply Lemma 9.7.22 to the reduction of p modulo π, and then lift the result back to $\mathscr{O}_K$, obtaining $P = x^k p + r$ for some $r \in \mathscr{O}_K$ with $r(0) = 1$ and $k \geq \deg r$. Since P has no multiple zeros modulo π, its roots lie in K^{ur}. Write $P = \prod_{i=1}^{s}(x - \alpha_i)$, where $s = m + k - 1$.

Now, note that

$$\prod_{i=1}^{s}(1 - \alpha_i \varpi_n) = \varpi_n^s P(\varpi_n^{-1}) \equiv 1 + \sum_{i=1}^{\infty} a_i \varpi_n^i \equiv u \bmod \varpi_n^m,$$

so there exists $v \in U_m(K_{\pi,n}^{\mathrm{ur}})$ with $\prod_{i=1}^{s}(1 - \alpha_i \varpi_n)v = u$. Since $N_{K_{\pi,n}^{\mathrm{ur}}/K^{\mathrm{ur}}}(v) \in U_n(K^{\mathrm{ur}})$, it suffices to check that $\prod_{i=1}^{s} N_{K_{\pi,n}^{\mathrm{ur}}/K^{\mathrm{ur}}}(1 - \alpha_i \varpi_n) \in U_n(K^{\mathrm{ur}})$. Note that

$$N_{K_{\pi,n}^{\mathrm{ur}}/K^{\mathrm{ur}}}(1 - \alpha_i \varpi_n) = \alpha_i^{q^{n-1}(q-1)} \frac{[\pi^n]_f(\alpha_i^{-1})}{[\pi^{n-1}]_f(\alpha_i^{-1})}.$$

As $P(0) = 1$, we then have

$$\prod_{i=1}^{s} N_{K_{\pi,n}^{\mathrm{ur}}/K^{\mathrm{ur}}}(1 - \alpha_i \varpi_n) = \prod_{i=1}^{s} \frac{[\pi^n]_f(\alpha_i^{-1})}{[\pi^{n-1}]_f(\alpha_i^{-1})}.$$

As $[\pi^{n-1}]_f(x) \equiv x^{q^{n-1}} \bmod \pi$, each $[\pi^{n-1}]_f(\alpha_i^{-1})$ is a unit, so it suffices to show that

$$\prod_{i=1}^{s} [\pi^n]_f(\alpha_i^{-1}) \equiv \prod_{i=1}^{s} [\pi^{n-1}]_f(\alpha_i^{-1}) \bmod \pi^n \mathscr{O}_{K^{\mathrm{ur}}}.$$

Note that in fact, both sides are contained in $\mathscr{O}$, as the set of α_i is a union of Frobenius conjugacy classes, and we have $f(\alpha_i^{-1}) \equiv \alpha_i^{-q} \equiv \alpha_j^{-1} \bmod \pi \mathscr{O}_{K^{\mathrm{ur}}}$ for some $1 \leq j \leq s$. Thus,

$$\prod_{i=1}^{s} f(\alpha_i^{-1}) \equiv \prod_{i=1}^{s} \alpha_i^{-1} \bmod \pi.$$

We then see that f applied to both sides gives a congruence modulo π^2, and recursively we have the desired congruence. □

We then have that the intersection of the norm groups for the $K_{\pi,n}$ is $\langle \pi \rangle$. The following is then an easy consequence.

THEOREM 9.7.24. *The maximal abelian extension of K is equal to $K^{\mathrm{ur}} K_{\pi,\infty}$ for any uniformizer π of K.*

THEOREM 9.7.25. *Let π be a uniformizer of K and $f \in \mathscr{F}_\pi$. The local reciprocity map ρ_K for K is the unique map such that*

i. the value $\rho_K(\pi)$ is the Frobenius element in $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ fixing K_π,

ii. for $u \in \mathscr{O}^\times$, the value $\rho_K(u)$ is the unique element of $\mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}})$ such that $\rho_K(u)(\varpi) = [u^{-1}]_f(\varpi)$ for all $\varpi \in W_{f,\infty}$.

CHAPTER 10

Global class field theory via idèles

10.1. Restricted topological products

We begin by defining the notion of a restricted topological product.

DEFINITION 10.1.1. Let I be an indexing set. For each $i \in I$, let X_i be a topological space and A_i be an open subset. The *restricted topological product* of the spaces X_i relative to the open subsets A_i is the set

$$\prod_{i\in I}(X_i,A_i) = \left\{ (x_i)_{i\in I} \in \prod_{i\in I} X_i \mid x_i \in A_i \text{ for all but finitely many } i \in I \right\},$$

endowed with the topology which has as a (standard) basis the open sets of the form

$$\{(x_i)_{i\in I} \mid x_i \in U_i \text{ for } i \in J \text{ and } x_i \in A_i \text{ for } i \in I - J\},$$

where $J \subseteq I$ is finite and U_j is an open subset of X_j for each $j \in J$. This topology on the set $\prod_{i\in I}(X_i,A_i)$ is referred to as the restricted product topology.

REMARK 10.1.2. The standard basic open sets of a restricted topological product $\prod_{i\in I}(X_i,A_i)$ have the form

$$\prod_{j\in J} U_j \times \prod_{i\in I-J} A_i$$

with $J \subset I$ finite and U_j open in X_j for each $j \in J$. The subspace topology on these open sets is exactly the product topology for the subspace topology from the X_i on the sets that form its product.

REMARK 10.1.3. The restricted topological product $\prod_{i\in I}(X_i,A_i)$ does not in general have the subspace topology of the product topology on $\prod_{i\in I} X_i$. That is, a standard basic open neighborhood of $\prod_{i\in I} X_i$ has the form

$$\prod_{k\in K} V_k \times \prod_{i\in I-K} X_i$$

with $K \subset I$ finite and V_k open in X_k for each $k \in K$. Any such set contains a basic open neighborhood in the restricted product topology on $\prod_{i\in I}(X_i,A_i)$. On the other hand, no such set will have its intersection with $\prod_{i\in I}(X_i,A_i)$ contained in any set of the form

$$\prod_{j\in J} U_j \times \prod_{i\in I-J} A_i$$

with $J \subset I$ finite and U_j open in X_j for each $j \in J$ so long as there are infinitely many $i \in I$ for which $A_i \neq X_i$. In other words, the restricted product topology on $\prod_{i\in I}(X_i, A_i)$ is finer and can be strictly finer than the subspace topology for the product topology.

The following simple lemma is quite useful.

LEMMA 10.1.4. *Let I be an indexing set, and for each $i \in I$, let X_i and Y_i be topological spaces, let A_i be an open subset of X_i, let B_i be an open subset of Y_i, and let $f_i \colon X_i \to Y_i$ be a continuous function. Suppose that $f_i(A_i) \subseteq B_i$ for all but finitely many $i \in I$. Then the product of the maps f_i restricts to a continuous function*

$$\prod_{i\in I}(X_i, A_i) \to \prod_{i\in I}(Y_i, B_i).$$

PROOF. For $x = (x_i)_{i\in I} \in X$, we have that $x_i \in A_i$ for almost all i, so $f_i(x_i) \in A_i$ for almost all i, and therefore $\prod_i f_i(x) \in \prod_{i\in I}(Y_i, B_i)$. Thus, it makes sense to let f denote the restriction of $\prod_i f_i$ to a map between the restricted topological products.

Consider a finite subset J of I and open subsets V_j of Y_j for each $j \in J$, and suppose $f(x) \in \prod_{j\in J} V_j \times \prod_{i\in I-J} Y_i$. For each $j \in J$, there exists an open neighborhood U_j of x_j in X such that $f_j(U_j) \subseteq V_j$, as f_j is continuous. Consequently, we have that $f(\prod_{j\in J} U_j \times \prod_{i\in I-J} X_i)$ is contained in $\prod_{j\in J} V_j \times \prod_{i\in I-J} Y_i$. Thus, f is continuous. □

LEMMA 10.1.5. *Let I be an indexing set. For each $i \in I$, let X_i be a Hausdorff topological space, and let A_i be an open subset of X_i. Then the restricted topological product $\prod_{i\in I}(X_i, A_i)$ is Hausdorff.*

PROOF. This is a consequence of either the discussion of Remark 10.1.3 or Lemma 10.1.5 applied to the case that $Y_i = B_i = X_i$. The product $\prod_{i\in I} X_i$ is Hausdorff, and if distinct $x, y \in \prod_{i\in I}(X_i, A_i)$ are contained in disjoint open neighborhoods in $\prod_{i\in I} X_i$, then the intersection of these neighborhoods with $\prod_{i\in I}(X_i, A_i)$ are disjoint open neighborhoods of x and y in the latter space. □

We are often interested in the case that our sets are topological groups or rings. In the proof, we treat only the case of groups, the case of rings being analogous.

LEMMA 10.1.6. *Let I be an indexing set, and for each $i \in I$, let G_i be a locally compact, Hausdorff topological group (resp., ring), and let K_i an open subgroup (subring) of G_i that is compact for almost all i. Then the restricted topological product $\prod_{i\in I}(G_i, K_i)$ is a locally compact, Hausdorff topological group (resp., ring).*

PROOF. That $\mathscr{G} = \prod_{i\in I}(G_i, K_i)$ is a group is straightforward. That is, clearly $1 = (1)_i \in G$, and if $a = (a_i)_i$ and $b = (b_i)_i$ are elements of $\mathscr{G}$, then $a_i, b_i \in K_i$ for all but finitely many $i \in I$, so $ab \in \mathscr{G}$. Similarly, $a^{-1} \in \mathscr{G}$ since $a_i^{-1} \in K_i$ if $a_i \in K_i$. It is then a topological group by applying Lemma 10.1.4 to the multiplication and inverse maps on $\mathscr{G}$.

That $\mathscr{G}$ is Hausdorff is Lemma 10.1.5. Let J be a finite subset of I such that K_i is compact for $i \in I - J$, and let U_j be a compact neighborhood of 1 in G_j for $j \in J$. Then $\prod_{j\in J} U_j \times \prod_{i\in I-J} K_i$ is an compact neighborhood of 1 in $\mathscr{G}$ by Tychonoff's theorem, so $\mathscr{G}$ is locally compact. □

10.2. Adeles

We now define the ring of adeles of a global field K.

DEFINITION 10.2.1. Let K be a global field. The *ring of adeles* (or *adele ring*) $\mathbb{A}_K$ of K is the restricted topological product

$$\mathbb{A}_K = \prod_{v\in V_K} (K_v, \mathscr{O}_v),$$

where V_K is the set of all places of K, where K_v is the completion of K at the place v, and where $\mathscr{O}_v$ is the valuation ring of K_v, which we take to be K_v if v is archimedean. An element of $\mathbb{A}_K$ is referred to as an adele.

REMARK 10.2.2. Let α be an adele in a global field K. Then α_v for some $v \in V_K$ shall denote the v-coordinate of α.

LEMMA 10.2.3. *Let $a \in K$. Then $a \in \mathscr{O}_v$ for all but finitely many places v of K.*

PROOF. It suffices to check this on the cofinite subset of finite places of K in V_K. Only those finitely many finite primes $\mathfrak{p}$ occur in the factorization of $a\mathscr{O}_K$, so only finitely many have negative valuation $v_\mathfrak{p}(a)$. The result follows. □

As an immediate consequence of Lemma 10.2.3, we see that every element of a global field gives rise to an element of its adele ring (since units are in particular integers).

DEFINITION 10.2.4. The *diagonal embedding* $\delta_K \colon K \to \mathbb{A}_K$ is the homomorphism $\delta_K(a) = (a)_{v\in V_K}$.

We note also that we have embeddings of adele rings into adele rings of extension fields.

DEFINITION 10.2.5. For L/K finite, the *canonical embedding* of $\mathbb{A}_K$ in $\mathbb{A}_L$ is the map $\iota_{L/K} \colon \mathbb{A}_K \to \mathbb{A}_L$ given by $\iota_{L/K}(\alpha)_w = \alpha_v$ for every place w of L and the place v of w lying below it.

We will show that the diagonal embedding has discrete image. This is rather straightforward for $K = \mathbb{Q}$, for example, so we proceed by reduction to this case, using the following result. Note that the diagonal embedding provides $\mathbb{A}_K$ with the structure of a K-vector space.

PROPOSITION 10.2.6. *Let L/K be a finite, separable extension of global fields. Then there is a canonical isomorphism of topological L-algebras*

$$\kappa \colon L \otimes_K \mathbb{A}_K \xrightarrow{\sim} \mathbb{A}_L$$

given on simple tensors of $b \in L$ and $\alpha \in \mathbb{A}_K$ by

$$\kappa(b \otimes \alpha) = \delta_L(b)\iota_{L/K}(\alpha) = (b\alpha_v)_w,$$

where v is used to denote the place of K lying below a place w of L. Here, a choice of K-basis of L provides an isomorphism $\mathbb{A}_K \otimes_K L \cong \mathbb{A}_K^{[L:K]}$ of $\mathbb{A}_K$-modules, and we give $\mathbb{A}_K \otimes_K L$ the topology induced via this isomorphism from the product topology on $\mathbb{A}_K^{[L:K]}$.

PROOF. Recall that Proposition 6.1.6 says that there is, for each place v of K, an isomorphism

$$\kappa_v \colon L \otimes_K K_v \xrightarrow{\sim} \prod_{w|v} L_w,$$

and the map κ as defined is the restriction of the product of these to $L \otimes_K \mathbb{A}_K$, which has image in $\mathbb{A}_L$ since both δ_L and $\iota_{L/K}$ do.

Since the product of the maps κ_v is an isomorphism, the map κ is an injection that we claim is surjective. For this, let $b_1, \dots, b_n$ be a K-basis for L. For all but finitely many finite primes v of K, we have for all places w of L over v both that $b_i \in \mathscr{O}_w$ for $1 \leq i \leq n$ and that $w(\mathrm{D}(b_1, \dots, b_n)) = 0$. For any such v, the map κ_v restricts to a map

$$\kappa_v' \colon \bigoplus_{i=1}^{n} (1 \otimes \mathscr{O}_v)(b_i \otimes 1) \to \prod_{w|v} \mathscr{O}_w$$

of free $\mathscr{O}_v$-modules of rank n, which by Proposition 6.1.10 is an isomorphism.

Given this, choose a finite set S of places of K containing the infinite places and those finite places v with $b_i \notin \mathscr{O}_w$ for some i or $w(\mathrm{D}(b_1, \dots, b_n)) \neq 0$ for some w dividing v, and let T be the finite set of places of L above it. Since κ_v is surjective for all $v \in S$ and κ_v' is surjective for all $v \notin S$, the image of κ contains

$$\prod_{w \in T} L_w \times \prod_{w \in V_L - T} \mathscr{O}_w.$$

Since any arbitrary finite set of places of L is contained in some such set T, it follows that κ is surjective.

For continuity of κ, note that each $f_i \colon \mathbb{A}_K \to \mathbb{A}_L$ defined by $f_i(\alpha) = \delta_L(b_i)\iota_{L/K}(\alpha)$ is continuous, noting that $\iota_{L/K}$ is continuous by Lemma 10.1.4. Then κ viewed as a map

$$\mathbb{A}_K^{[L:K]} \to \mathbb{A}_L$$

using this basis is continuous as a sum of the continuous maps f_i, since $\mathbb{A}_L$ is a topological group under addition. □

We next show that K sits discretely in its adele ring.

PROPOSITION 10.2.7. *The diagonal embedding $\delta_K \colon K \to \mathbb{A}_K$ has discrete image.*

PROOF. If K is a number field, Proposition 10.2.6 for the extension $K/\mathbb{Q}$ identifies $\kappa^{-1} \circ \delta_K$ for the map κ therein with the map

$$\mathrm{id}_K \otimes \delta_{\mathbb{Q}} \colon K \otimes_{\mathbb{Q}} \mathbb{Q} \to K \otimes_{\mathbb{Q}} \mathbb{A}_{\mathbb{Q}}.$$

Therefore, it suffices to show that $\delta_{\mathbb{Q}}$ has discrete image. (Similarly, for function fields of characteristic p, it suffices to consider $\iota_{\mathbb{F}_p(t)}$, for which we omit the proof.)

We identify $\mathbb{Q}$ with its image in $\mathbb{A}_{\mathbb{Q}}$ under $\delta_{\mathbb{Q}}$ and endow it with the subspace topology. The intersection of the open neighborhood

$$\prod_{p \text{ prime}} \mathbb{Z}_p \times \{a \in \mathbb{R} \mid |a| < 1\}$$

of 0 in $\mathbb{A}_{\mathbb{Q}}$ with $\mathbb{Q}$ consists of elements with nonnegative valuation at p for every p, which to say integers, that also have absolute value less than 1. In other words, the intersection is $\{0\}$. Since $\mathbb{A}_{\mathbb{Q}}$ is a topological ring and $\mathbb{Q}$ is a subring, we have by translation that $\mathbb{Q}$ has discrete image. □

NOTATION 10.2.8. We use the diagonal embedding δ_K to identify a global field K with a subring of $\mathbb{A}_K$, denoted also by K.

We also have the following.

PROPOSITION 10.2.9. *Let K be a global field. Then there exists a finite set S of places of K including the archimedean places and positive real numbers ε_v for each $v \in S$ such that*

$$X = \prod_{v \in V_K - S} \mathscr{O}_v \times \prod_{v \in S} \{a \in K_v \mid |a| \leq \varepsilon_v\}. \tag{10.2.1}$$

satisfies $\mathbb{A}_K = K + X$.

PROOF. First consider the case $K = \mathbb{Q}$. In this case, we claim that the set

$$Y = \prod_{p \text{ prime}} \mathbb{Z}_p \times \{a \in \mathbb{R} \mid |a| \leq \tfrac{1}{2}\}$$

satisfies $\mathbb{A}_{\mathbb{Q}} = \mathbb{Q} + Y$. Let $\alpha \in \mathbb{A}_{\mathbb{Q}}$. Let $p_1, \ldots, p_n$ be the finite list of prime numbers p such that $\alpha_p \notin \mathbb{Z}_p$. Let $k_i = -v_{p_i}(\alpha_{p_i})$ for each i with $1 \leq i \leq n$. Let $b = p_1^{k_1} \cdots p_n^{k_n}$. Let $a \in \mathbb{Z}$ be the unique integer such that

$$-\tfrac{b}{2} < a - b\alpha_\infty \leq \tfrac{b}{2}$$

and

$$a \equiv b\alpha_{p_i} \bmod p_i^{k_i}\mathbb{Z}_{p_i}$$

for each i. Then $\alpha - \frac{a}{b} \in Y$, as desired.

For an arbitrary number field, choose a basis $b_1, \ldots, b_n$ of K as a $\mathbb{Q}$-vector space, and note that Proposition 10.2.6 tells us that every element $\beta \in \mathbb{A}_K$ has the form

$$\beta = \sum_{i=1}^{n} b_i \iota_{K/\mathbb{Q}}(\alpha_i)$$

for some $\alpha_1, \ldots, \alpha_n \in \mathbb{A}_{\mathbb{Q}}$. In turn, each α_i may be written as $\alpha_i = y_i + c_i$ with $y_i \in Y$ and $c_i \in \mathbb{Q}$. We then have

$$\beta \in K + \sum_{i=1}^{n} b_i \iota_{K/\mathbb{Q}}(Y),$$

and we let X' denote the latter sum. We let S be the set consisting of the archimedean places of K and the nonarchimedean places of K such that $b_i \notin \mathscr{O}_v$ for some i, and we note that every element $\alpha \in X'$ satisfies $\alpha_v \in \mathscr{O}_v$ for all $v \notin S$. For each nonarchimedean (resp., archimedean) $v \in S$, let ε_v be such that $|b_i|_v \leq \varepsilon_v$ (resp., $|b_i|_v \leq 2\varepsilon_v$) for all $1 \leq i \leq n$. Then X as defined by (10.2.1) contains X' and satisfies $\mathbb{A}_K = K + X$.

The case of a function field is similarly derived from the case $K = \mathbb{F}_p(t)$, and the proof is left to the reader. □

COROLLARY 10.2.10. *Let K be a global field. Then the quotient K-vector space $\mathbb{A}_K/K$ is compact Hausdorff.*

PROOF. The compact (Hausdorff) set X of Proposition 10.2.9 maps onto the quotient $\mathbb{A}_K/K$ under the continuous projection map from $\mathbb{A}_K$. The space $\mathbb{A}_K/K$ is Hausdorff as K is closed in $\mathbb{A}_K$, so $\mathbb{A}_K/K$ is compact as well. □

Since an adele necessarily has valuation less than or equal to 1 in all but finitely many places, the infinite product in the following definition converges.

DEFINITION 10.2.11. Let K be a global field. Let $\alpha \in \mathbb{A}_K$. The *content* $c_K(\alpha)$ of α is defined to be

$$c_K(\alpha) = \prod_{v \in V_K} \|\alpha_v\|_v,$$

where we recall that $\|\alpha_v\|_v = |\alpha_v|_v$ unless v is complex, in which case $\|\alpha_v\|_v = |\alpha_v|_v^2$.

LEMMA 10.2.12. *Let K be a global field. Then there exists a positive real number C such that for every $\alpha \in \mathbb{A}_K$ with $c_K(\alpha) > C$, there exists an element $a \in K^\times$ with $|a|_v \leq |\alpha_v|_v$ for all places v of K.*

SKETCH OF PROOF. Since $\mathbb{A}_K$ is a locally compact abelian group, it has an invariant Haar measure. Letting S denote the set of archimedean places of K, we set

$$Z = \prod_{v \in V_K - S} \mathscr{O}_v \times \prod_{v \in S} \bar{B}_{1/2}(0)$$

where $B_{1/2}(0)$ denotes the closed ball of radius $1/2$ around 0 under the usual absolute value corresponding to v. We normalize our Haar measure so that Z has volume 1. As $\mathbb{A}_K/K$ is compact, it has finite quotient measure, and we take C to be this measure.

Now let α be as in the statement. The set αZ has measure $c_K(\alpha) > C$ (which we leave to the reader to verify, using uniqueness of Haar measure and noting that local Haar measures will scale by the multiplicative valuation used in defining the content), so it follows that there exist two distinct elements β, β' of αZ with the same image in $\mathbb{A}_K/K$, which is to say that the difference $a = \beta - \beta'$ lies in K. For each $v \in V_K$, we clearly have $|\beta - \beta'|_v \leq |\alpha|_v$ by choice of Z, so the result holds. □

The lemma has the following corollary.

COROLLARY 10.2.13. *Let K be a global field and u be a place of K. Let S be a finite set of places of K not including u, and choose a real number $\varepsilon_v > 0$ for each $v \in S$. Then there exists an element $a \in K^\times$ such that $|a|_v \leq \varepsilon_v$ for all $v \in S$ and $|a|_v \leq 1$ for all $v \notin S$ with $v \neq u$.*

PROOF. Let C be as in Lemma 10.2.12. Choose elements $\alpha_v \in K_v$ for each v with $|\alpha_v|_v \leq \varepsilon_v$ for each $v \in S$ and $|\alpha_v|_v = 1$ for all other places $v \neq u$ of K. Let $\alpha_u \in K_u$ be such that

$$\|\alpha_u\|_u > C \prod_{v \in S} \|\alpha_v\|_v^{-1}.$$

Setting $\alpha = (\alpha_v)_v \in \mathbb{A}_K$, we then have $c_K(\alpha) > C$, so there exists an element $a \in K^\times$ with $|a|_v \leq |\alpha_v|_v$ for all v and therefore $|a|_v \leq \varepsilon_v$ for all $v \in S$ and $|a_v|_v \leq 1$ for $v \notin S \cup \{u\}$. □

While any global field K sits discretely in $\mathbb{A}_K$, if we exclude one prime from $\mathbb{A}_K$, the result is very different.

THEOREM 10.2.14 (Strong Approximation). *Let K be a global field, and let u be a place of K. Set*

$$\mathbb{A}_K^{\neq u} = \prod_{v \in V_K - \{u\}} (K_v, \mathscr{O}_v).$$

Then K is embedded diagonally as a dense subset of $\mathbb{A}_K^{\neq u}$.

PROOF. Let $\alpha \in \mathbb{A}_K^{\neq u}$, let $\delta > 0$, and let T be a finite subset of $V_k - \{u\}$ that includes its archimedean places and places with $\alpha_v \notin \mathscr{O}_v$. We claim that there exists $a \in K$ such that $|a - \alpha_v|_v \leq \delta$ for all $v \in T$ and $|a|_v \leq 1$ for all $v \notin T$, which will prove the result.

By Proposition 10.2.9, we have a set X of the form in (10.2.1) such that $\mathbb{A}_K = K + X$. We use the notation S and ε_v for $v \in S$ found therein. Setting $\varepsilon_v = 1$ for $v \notin S$, there exists by Corollary 10.2.13 an element $b \in K^\times$ with

$$|b|_v \leq \begin{cases} \varepsilon_v^{-1}\delta & \text{if } v \in T, \\ \varepsilon_v^{-1} & \text{if } v \notin T \cup \{u\}. \end{cases}$$

Note that

$$\mathbb{A}_K = b\mathbb{A}_K = bX + K.$$

Write $\alpha = bx + a$ for some $x \in X$ and $a \in K$. Since $|bx_v|_v \leq \delta$ for all $v \in T$ and $|bx_v|_v \leq 1$ for all $v \notin T \cup \{u\}$, the element $a = \alpha_v - bx_v$ for any $v \neq u$ has the desired properties. □

Let us record the rephrasing of the strong approximation theorem found in its proof. The statement is more clearly a direct generalization of weak approximation.

COROLLARY 10.2.15. *Let K be a global field, and let u be a place of K. Let $\alpha_v \in K_v$ for each place $v \neq u$ of K and suppose that $\alpha_v \in \mathscr{O}_v$ for all but finitely many such v. Then for every $\varepsilon > 0$ and finite set of primes S of K with $u \notin S$, there exists $a \in K$ such that $|a - \alpha_v|_v < \varepsilon$ for all $v \in S$ and $|a|_v \leq 1$ for all finite places $v \notin S$ with $v \neq u$.*

We next investigate how adele rings behave in extensions. For a finite extension of L of K, we identify $\mathbb{A}_K$ with a closed subgroup of $\mathbb{A}_L$ via the canonical embedding.

LEMMA 10.2.16. *Let L/K be a finite Galois extension of global fields. Then $\mathbb{A}_L^{\mathrm{Gal}(L/K)} = \mathbb{A}_K$.*

PROOF. The Galois group $G = \mathrm{Gal}(L/K)$ permutes the places of L lying over a place v of K. Let

$$(\alpha_w)_w \in \prod_{\substack{w \in V_L \\ w|v}} L_w$$

be G-invariant. Since the decomposition group G_w at $w \mid v$ preserves the w-coordinate, it fixes α_w. Thus, $\alpha_w \in K_v$, and this holds for all $w \mid v$. Moreover, G acts on $\prod_{w|v} K_v$ by permuting the coordinates, and the action of G on the set of places is transitive, so all of the α_w must be equal. That is, $(\alpha_w)_w$ is in the image of some $a \in K_v$ in the product $\prod_{w|v} L_w$. If, moreover, $(\alpha_w)_w \in \prod_{w|v} \mathscr{O}_w$, then clearly $a \in \mathscr{O}_v$.

With respect to inclusion maps, we have

$$\mathbb{A}_K = \varinjlim_{S \subset V_K} \left(\prod_{v \in S} K_v \times \prod_{v \in V_K - S} \mathscr{O}_v \right),$$

where S runs over the finite sets of places of K. For such a set S, let S_L be the subset of V_L of places lying over places in S. Every finite set of places of L is contained in some S_L, so

$$\mathbb{A}_L^G = \varinjlim_{S \subset V_K} \left(\prod_{w \in S_L} L_w \times \prod_{w \in V_L - S_L} \mathscr{O}_w \right)^G = \varinjlim_{S \subset V_K} \left(\prod_{v \in S} \left(\prod_{\substack{w \in V_L \\ w|v}} L_w \right)^G \times \prod_{v \in V_K - S} \left(\prod_{\substack{w \in V_L \\ w|v}} \mathscr{O}_w \right)^G \right) = \mathbb{A}_K.$$

□

Let us consider norm and trace maps on adeles.

DEFINITION 10.2.17. Let L/K be an extension of global fields.

a. The *norm map* $N_{L/K} \colon \mathbb{A}_L \to \mathbb{A}_K$ is the multiplicative function defined by

$$N_{L/K}(\beta) = \left(\prod_{w|v} N_{L/K}(\beta_w) \right)_v$$

on $\beta \in \mathbb{A}_L$.

b. The *trace map* $\mathrm{Tr}_{L/K} \colon \mathbb{A}_L \to \mathbb{A}_K$ is the homomorphism

$$\mathrm{Tr}_{L/K}(\beta) = \left(\sum_{w|v} \mathrm{Tr}_{L/K}(\beta_w) \right)_v.$$

on $\beta \in \mathbb{A}_L$.

REMARKS 10.2.18. Let L/K be a finite extension of global fields.

a. That the norm and trace for L/K on adeles have images inside the adeles follows from the fact that $\beta \in \mathbb{A}_L$ has β_w in the valuation ring of L_w for all but finitely many w, and hence for all w dividing v for all but finitely many places v of K, and therefore $N_{L/K}(\beta_w)$ and $\mathrm{Tr}_{L/K}(\beta_w)$ lie in the valuation ring of K_v for all w dividing v for all but finitely many v.

b. In the notation of Definition 6.1.8, the norm and trace maps on adeles have v-coordinates on $\beta \in \mathbb{A}_L$ given by

$$N_{L/K}(\beta)_v = N^v_{L/K}((\beta_w)_w) \quad \text{and} \quad \mathrm{Tr}_{L/K}(\beta)_v = \mathrm{Tr}^v_{L/K}((\beta_w)_w),$$

where w runs over the places dividing v.

c. It follows form Lemma 10.1.4 that $N_{L/K}$ and $\mathrm{Tr}_{L/K}$ are continuous maps on adeles.

10.3. Idèles

In this section, we define the idèles, the elements of which are the units in the adeles. We continue to let K denote a global field.

DEFINITION 10.3.1. Let K be a global field. The *group of idèles* (or *idèle group*) $\mathbb{I}_K$ of K is the restricted topological product

$$\mathbb{I}_K = \prod_{v \in V_K} (K_v^\times, \mathscr{O}_v^\times),$$

where V_K is the set of all places of K, where K_v is the completion of K at the place v, and where $\mathscr{O}_v$ is the valuation ring of K_v, for which we set $\mathscr{O}_v^\times = K_v^\times$ if v is archimedean. An element of $\mathbb{I}_K$ is referred to as an idèle.

REMARK 10.3.2. Note that $\mathbb{I}_K = \mathbb{A}_K^\times$ as sets, but $\mathbb{I}_K$ does not have the subspace topology from $\mathbb{A}_K$. For each finite prime v, fix a uniformizer π_v in K_v, and let α_v be the adele that is π_v in its v-coordinate and 1 in every other coordinate. Then every open neighborhood of 1 in $\mathbb{A}_K$ contains all but finitely many α_v. On the other hand, the basic open neighborhood

$$\prod_{v \in V_K} \mathscr{O}_v^\times$$

of 1 in $\mathbb{I}_K$ contains not a single α_v. On the other hand, the intersection of a basic open neighborhood of $\mathbb{A}_K$ with $\mathbb{I}_K$ is an open neighborhood of $\mathbb{I}_K$, so the topology on $\mathbb{I}_K$ is strictly finer than the subspace topology from $\mathbb{A}_K$.

We leave it to the reader to check the following.

LEMMA 10.3.3. *The restricted product topology on the idèle group $\mathbb{I}_K$ of a global field agrees with the subspace topology induced by the injection*

$$\mathbb{I}_K \to \mathbb{A}_K \times \mathbb{A}_K, \qquad \alpha \mapsto (\alpha, \alpha^{-1}).$$

REMARK 10.3.4. Note that the content $c_K(\alpha)$ of an idèle α is a positive real number, as all but finitely many coordinates of α will have multiplicative valuation 1 and the valuations of the other coordinates will be nonzero. In fact, the property that of having nonzero content characterizes the idèles as a subset of the adeles, as the reader may quickly check.

We may then make the following definition.

DEFINITION 10.3.5. Let K be a global field. The *content homomorphism* $c_K\colon \mathbb{I}_K \to \mathbb{R}_{>0}$ is the function that takes an idèle α to its content

$$c_K(\alpha) = \prod_{v\in V_K} \|\alpha_v\|_v.$$

Let $\mathbb{I}_K^1$ denote the kernel of c_K.

PROPOSITION 10.3.6. *Let K be a global field. Then the content homomorphism $c_K\colon \mathbb{I}_K \to \mathbb{R}_{>0}$ is continuous.*

PROOF. We leave it to the reader to verify the following simple claim, which implies the statement. For any $\varepsilon > 0$, there exists a sufficiently small $\delta > 0$ such that $c_K^{-1}((1-\varepsilon, 1+\varepsilon))$ contains $\prod_{v\in V_K - S} \mathscr{O}_v^\times \times \prod_{v\in S} B_\delta(1)$, where S is the set of archimedean places of K and $B_\delta(1) \subset K_v^\times$ is a ball of radius δ about 1. □

COROLLARY 10.3.7. *The group $\mathbb{I}_K^1$ of idèles of content 1 is a closed subgroup of $\mathbb{I}_K$*

We have the following result on the kernel of the content homomorphism.

LEMMA 10.3.8. *The topology on $\mathbb{I}_K^1$ from $\mathbb{I}_K$ agrees with its subspace topology from $\mathbb{A}_K$.*

PROOF. By Remark 10.3.2, the subspace topology on $\mathbb{I}_K^1$ from $\mathbb{I}_K$ is finer than the subspace topology from $\mathbb{A}_K$, so we need only show that the intersection of a basic open neighborhood of 1 in $\mathbb{I}_K$ with $\mathbb{I}_K^1$ contains the intersection of an open neighborhood of 1 in $\mathbb{A}_K$ with $\mathbb{I}_K^1$.

Let S be a finite set of places of K containing the archimedean places, and for each $v \in S$, let U_v be an open subset of $K_v^\times$ containing 1. Then

$$U = \prod_{v\in S} U_v \times \prod_{v\in V_K - S} \mathscr{O}_v^\times$$

is a basic open in $\mathbb{I}_K$ containing 1. We may suppose that the sets U_v are chosen to be balls of sufficiently small radius such that the products of the (modified) valuations of any elements in $\prod_{v\in S} U_v$ is less than 2. Since every element $\mathscr{O}_v - \mathscr{O}_v^\times$ has valuation at most $\frac{1}{2}$, we then have

$$U \cap \mathbb{I}_K^1 = (\prod_{v\in S} U_v \times \prod_{v\in V_K - S} \mathscr{O}_v) \cap \mathbb{I}_K^1,$$

and $\prod_{v\in S} U_v \times \prod_{v\in V_K - S} \mathscr{O}_v$ is a basic open neighborhood of 1 in $\mathbb{A}_K$. □

Note that we may think of $K^\times$ as a subgroup of $\mathbb{I}_K$ via the diagonal embedding. By the product formula for valuations on global fields, every element of $K^\times$ lies in $\mathbb{I}_K^1$.

PROPOSITION 10.3.9. *The image of $K^\times$ in $\mathbb{I}_K^1$ is discrete, and $\mathbb{I}_K^1/K^\times$ is compact Hausdorff.*

PROOF. The first statement follows from Corollary 10.2.10, since Lemma 10.3.8 tells us that $\mathbb{I}_K^1$ has the subspace topology from $\mathbb{A}_K$. For the second statement, let $\alpha \in \mathbb{A}_K$ be an adele with $c_K(\alpha) > C$, where C is as in the statement of Lemma 10.2.12. We define a compact subset of $\mathbb{A}_K$ by

$$X = \{\beta \in \mathbb{I}_K^1 \mid |\beta_v|_v \leq |\alpha_v|_v \text{ for all } v \in V_K\},$$

where here we use the fact that $\mathbb{I}_K^1$ is closed in $\mathbb{A}_K$. For an arbitrary $\gamma \in \mathbb{I}_K^1$, Lemma 10.2.12 tells us that there exists $a \in K^\times$ with $|a|_v \leq |\gamma_v^{-1}\alpha_v|_v$ for all places v of K. We then have $\gamma a \in X$, so X surjects onto the Hausdorff space $\mathbb{I}_K^1/K^\times$, and therefore the latter quotient is compact. □

DEFINITION 10.3.10. The *principal idèles* of a global field K are the elements of $\mathbb{I}_K$ that lie in $K^\times$ (under its diagonal embedding).

DEFINITION 10.3.11. Let K be a global field. Then the *idèle class group* $\mathbb{C}_K$ of K is the quotient topological group $\mathbb{I}_K/K^\times$. The image $[\alpha]$ of $\alpha \in \mathbb{I}_K$ in $\mathbb{C}_K$ is the idèle class of α.

NOTATION 10.3.12. For a global field K, we shall use $V_{K,f}$ to denote its set of finite places.

DEFINITION 10.3.13. Let K be a global field. The fractional ideal of $\mathscr{O}_K$ defined by an idèle α of K is the finite product

$$\prod_{v \in V_{K,f}} \mathfrak{p}_v^{v(\alpha)},$$

where $\mathfrak{p}_v$ denotes the prime corresponding to a finite place v of K.

PROPOSITION 10.3.14. *Let K be a number field. Let $\pi_K \colon \mathbb{I}_K \to I_K$ be the homomorphism that takes an idèle to the fractional ideal it defines. Then $\pi_K(\mathbb{I}_K^1) = I_K$, and π_K is continuous if we endow I_K with the discrete topology.*

PROOF. For the first statement, we need only show that every nonzero prime $\mathfrak{p}$ is the image of an element of $\mathbb{I}_K^1$. We may take an idèle α of content 1 that is a uniformizer $\pi_\mathfrak{p}$ in the coordinate corresponding to $\mathfrak{p}$, that in a fixed archimedean place w satisfies $\|\alpha_w\|_w = |\pi_\mathfrak{p}|_\mathfrak{p}^{-1}$, and which is 1 in all other coordinates.

For the second statement, we need only note that

$$\pi_K^{-1}(\{(1)\}) = \prod_{v \in V_K} \mathscr{O}_v^\times$$

is open in $\mathbb{I}_K$. □

REMARK 10.3.15. Proposition 10.3.14 enables us to give a second proof that Cl_K is finite. That is, since π_K in the proposition takes $K^\times$ onto P_K, we have an induced continuous, surjective map $\mathbb{I}_K^1/K^\times \to \mathrm{Cl}_K$. It follows that Cl_K is both compact as the continuous image of a compact space and discrete as a quotient of I_K, and therefore Cl_K is finite.

NOTATION 10.3.16. For a finite extension L/K of global fields, we use $\imath_{L/K}\colon \mathbb{C}_K \to \mathbb{C}_L$ also to denote the map induced by the canonical embedding $\imath_{L/K}\colon \mathbb{I}_K \to \mathbb{I}_L$.

LEMMA 10.3.17. *For a finite extension L/K of global fields, the map $\imath_{L/K}\colon \mathbb{C}_K \to \mathbb{C}_L$ is injective.*

PROOF. Identifying $\mathbb{I}_K$ and $L^\times$ with their images in $\mathbb{I}_L$, we need only see that $\mathbb{I}_K \cap L^\times = K^\times$. Let M be a finite Galois extension of K containing L. We claim that $\mathbb{I}_K \cap M^\times = K^\times$, which will prove the result. But Lemma 10.2.16 gives us the first equality in

$$\mathbb{I}_K \cap M^\times = \mathbb{I}_M^{\mathrm{Gal}(M/K)} \cap M^\times = (M^\times)^{\mathrm{Gal}(M/K)} = K^\times,$$

the second equality following from the compatibility of the Galois action on $M^\times$ and $\mathbb{I}_M$ under the diagonal embedding. □

NOTATION 10.3.18. We identify $\mathbb{C}_K$ with a (closed) subgroup of $\mathbb{C}_L$ via the embedding $\imath_{L/K}$, noting Lemma 10.3.17.

As a consequence of Lemma 10.2.16, we have that $\mathbb{I}_L^{\mathrm{Gal}(L/K)} = \mathbb{I}_K$ for any finite Galois extension L/K. We claim that the same holds for idèle class groups.

LEMMA 10.3.19. *Let L/K be a finite Galois extension of global fields. Then $\mathbb{C}_L^{\mathrm{Gal}(L/K)} = \mathbb{C}_K$.*

PROOF. We have an exact sequence of modules for $G = \mathrm{Gal}(L/K)$ given by

$$0 \to L^\times \to \mathbb{I}_L \to \mathbb{C}_L \to 0,$$

and this gives rise to a long exact sequence starting

$$0 \to K^\times \to \mathbb{I}_K \to \mathbb{C}_L^G \to H^1(G, L^\times).$$

Since the latter group is zero by Hilbert's Theorem 90, the resulting short exact sequence yields the result. □

Since the idèles are the units in the adele ring, the norm map on adele ring is immediately seen to define a norm map on the idèle group. Continuity of the norm follows from Lemma 10.1.4, as with adeles.

DEFINITION 10.3.20. Let L/K be an extension of global fields. The *norm map* $N_{L/K}\colon \mathbb{I}_L \to \mathbb{I}_K$ is the homomorphism that is the restriction of $N_{L/K}\colon \mathbb{A}_L \to \mathbb{A}_K$.

Since the norms of principal idèles are principal, we may make the following definition.

DEFINITION 10.3.21. The *norm map* $N_{L/K}\colon \mathbb{C}_L \to \mathbb{C}_K$ is the map induced on quotient groups by the corresponding norm map on idèle groups.

REMARK 10.3.22. The norm map is continuous on idèle groups and idèle class groups.

10.4. Statements

The reciprocity map in the idèle-theoretic approach to global class field theory is constructed out of the local reciprocity maps of the completions of the global fields in question. We provide the preliminary results to its construction.

LEMMA 10.4.1. *Let K be a global field, let L be a finite abelian extension of K, and let $\alpha \in \mathbb{I}_K$. Then $\rho_{L_w/K_v}(\alpha_v) = 1$ for all places w lying over v for all but finitely many places v of K.*

PROOF. All but finitely many v are unramified in L/K and for all but finitely many v, the valuation v is nonarchimedean and α_v is a unit in its valuation ring $\mathscr{O}_v$. Since $\rho_{L_w/K_v}(\mathscr{O}_v^\times)$ is contained in the inertia subgroup of $\mathrm{Gal}(L_w/K_v)$ for any v and this inertia subgroup is trivial in an unramified extension, we have the result. □

REMARK 10.4.2. Suppose we start with a global field K and a place v of K. Consider the canonical map from $G_{K_v}^{\mathrm{ab}}$ to a decomposition group D_v in G_K^{ab} at a place w over v. (Note that, while the map $G_{K_v} \hookrightarrow G_K$ identifying G_{K_v} with the decomposition group at a place of K^{sep} is injective, the map $G_{K_v}^{\mathrm{ab}} \to G_K^{\mathrm{ab}}$ it induces may not be.) The resulting map $G_{K_v}^{\mathrm{ab}} \to G_K^{\mathrm{ab}}$ is independent of the choice of w since conjugation by an element of G_K^{ab} is a trivial automorphism of G_K^{ab}. We may then view the local reciprocity map as producing global elements via the composition

$$K_v^\times \xrightarrow{\rho_{K_v}} G_{K_v}^{\mathrm{ab}} \xrightarrow{\sim} D_v \hookrightarrow G_K^{\mathrm{ab}}$$

that takes $\alpha \in K_v^\times$ to $\rho_{K_v}(\alpha)|_{K^{\mathrm{ab}}}$, and since all of the maps in the composition are independent of w, this map is as well.

The following lemma is now an immediate consequence of Remark 10.4.2.

LEMMA 10.4.3. *Let L/K be a finite abelian extension of global fields, let v be a place of K, and let $\alpha \in K_v^\times$. The quantity*

$$\rho_{L_w/K_v}(\alpha)|_L \in \mathrm{Gal}(L/K)$$

for a place w of L lying over v is independent of w.

Lemmas 10.4.1 and 10.4.3 allow us to define the reciprocity map for a finite abelian extension of global fields.

DEFINITION 10.4.4. Let L/K be a finite abelian extension of global fields. The *(global) reciprocity map* for L/K is the homomorphism $\Phi_{L/K}\colon \mathbb{I}_K \to \mathrm{Gal}(L/K)$ defined by

$$\Phi_{L/K}(\alpha) = \prod_{v \in V_K} \rho_{L_w/K_v}(\alpha_v)|_L,$$

where for each valuation v of K, we have chosen a valuation w of L lying over v.

We note the following compatibility among the global reciprocity maps.

LEMMA 10.4.5. *Let K be a global field, and let L and M be finite abelian extensions of K with $L \subseteq M$. For every $\alpha \in \mathbb{I}_K$, we have $\Phi_{L/K}(\alpha) = \Phi_{M/K}(\alpha)|_L$.*

PROOF. For each $v \in V_K$, we choose $w \in V_L$ lying over v and $u \in P_M$ lying over w. By property (ii) of local reciprocity, we have

$$\rho_{L_w/K_v}(\alpha_v) = \rho_{M_u/K_v}(\alpha_v)|_{L_w},$$

and the result is then an immediate consequence of the definition of the global reciprocity map. □

COROLLARY 10.4.6. *Let K be a global field. Then for each $\alpha \in \mathbb{I}_K$, the quantity*

$$\varprojlim_L \Phi_{L/K}(\alpha),$$

with the inverse limit taken over finite abelian extensions L of K with respect to restriction maps, is well-defined.

We may therefore make the following definition.

DEFINITION 10.4.7. Let K be a global field. The *(global) reciprocity map* for K is the homomorphism $\Phi_K\colon \mathbb{I}_K \to G_K^{\mathrm{ab}}$ given by

$$\Phi_K = \varprojlim_L \Phi_{L/K},$$

where the inverse limit is taken over finite abelian extensions L of K with respect to restriction maps.

REMARK 10.4.8. For $\alpha \in \mathbb{I}_K$, we have

$$\Phi_K(\alpha) = \varprojlim_L \Phi_{L/K}(\alpha) = \varprojlim_L \prod_{v \in V_K} \rho_{L_w/K_v}(\alpha_v)|_L = \prod_{v \in V_K} \Big(\varprojlim_{L_w} \rho_{L_w/K_v}(\alpha_v) \Big)|_{K^{\mathrm{ab}}} = \prod_{v \in V_K} \rho_{K_v}(\alpha_v)|_{K^{\mathrm{ab}}},$$

where the first two inverse limits run over the finite abelian extensions of K and the third runs over the completions of the finite abelian extensions of K at a fixed prime of K^{ab} over v.

Our key result is now a reworking of Artin reciprocity.

THEOREM 10.4.9 (Global reciprocity). *Let K be a global field.*

a. We have $\Phi_K(a) = 1$ for all $a \in K^\times$.

b. For every finite abelian extension L of K, the reciprocity map $\Phi_{L/K}$ is surjective with kernel $K^\times N_{L/K}(\mathbb{I}_L)$.

In other words, the global reciprocity map factors through the idèle class group.

DEFINITION 10.4.10. Let K be a global field.

a. The *global reciprocity map* $\phi_K\colon \mathbb{C}_K \to G_K^{\mathrm{ab}}$ is the homomorphism induced on the quotient $\mathbb{C}_K$ of $\mathbb{I}_K$ by the global reciprocity map Φ_K on idèles.

b. The *global reciprocity map* $\phi_{L/K}\colon \mathbb{C}_K \to \mathrm{Gal}(L/K)$ for L/K is the composition of ϕ_K with restriction to $\mathrm{Gal}(L/K)$.

The following is then just a rewording of global reciprocity.

THEOREM 10.4.11. *Let L/K be a finite abelian extension of global fields. The global reciprocity map $\phi_{L/K}$ induces an isomorphism*

$$\mathbb{C}_K/N_{L/K}\mathbb{C}_L \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

REMARK 10.4.12. For a number field K, the reciprocity map ϕ_K is surjective, and its kernel is the connected component $\mathbb{C}_K^\circ$ of 1 in $\mathbb{C}_K$. This connected component is the closure of the image of the subgroup of $\mathbb{I}_K$ consisting of idèles that are zero in all nonarchimedean coordinates and positive in all real coordinates.

We have the following compatibilities between reciprocity maps, which are quickly derived from the analogous result in local reciprocity.

PROPOSITION 10.4.13. *Let K be a global field, and let L/K be a finite separable extension. Then we have the following commutative diagrams:*

a.

$$\begin{array}{ccc} \mathbb{C}_L & \xrightarrow{\phi_L} & G_L^{\mathrm{ab}} \\ \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle R_{L/K}} \\ \mathbb{C}_K & \xrightarrow{\phi_K} & G_K^{\mathrm{ab}}, \end{array}$$

where $R_{L/K}$ is the restriction map on Galois groups,

b.

$$\begin{array}{ccc} \mathbb{C}_K & \xrightarrow{\phi_K} & G_K^{\mathrm{ab}} \\ \downarrow{\scriptstyle \iota_{L/K}} & & \downarrow{\scriptstyle V_{L/K}} \\ \mathbb{C}_L & \xrightarrow{\phi_L} & G_L^{\mathrm{ab}}, \end{array}$$

where the map $\iota_{L/K}$ is induced by the natural injection map $\mathbb{I}_K \to \mathbb{I}_L$, and

c. for any embedding $\sigma\colon L \hookrightarrow K^{\mathrm{sep}}$,

$$\begin{array}{ccc} \mathbb{C}_L & \xrightarrow{\phi_L} & G_L^{\mathrm{ab}} \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma^*} \\ \mathbb{C}_{\sigma(L)} & \xrightarrow{\phi_{\sigma(L)}} & G_{\sigma(L)}^{\mathrm{ab}}, \end{array}$$

where the map σ^* *is induced by conjugation by* σ.

PROOF. We prove only part a, in that parts b and c is similar. For $\beta \in \mathbb{C}_L$, we have

$$\begin{aligned} \phi_L(\beta)|_{K^{\mathrm{ab}}} = \prod_{w\in V_L} \rho_{L_w}(\beta_w)|_{K^{\mathrm{ab}}} = \prod_{v\in V_K}\prod_{w|v} \rho_{L_w}(\beta_w)|_{K^{\mathrm{ab}}} = \prod_{v\in V_K}\prod_{w|v} \rho_{K_v}(N_{L_w/K_v}\beta_w)|_{K^{\mathrm{ab}}} \\ = \prod_{v\in V_K} \rho_{K_v}(N^v_{L/K}((\beta_w)_{w|v}))|_{K^{\mathrm{ab}}} = \phi_K(N_{L/K}\beta), \end{aligned}$$

where Remark 10.4.8 is used in the first and last equality and Proposition 9.2.7 is used in the third equality. □

Much as in the case of local class field theory, we have a one-to-one correspondence between norm subgroups of $\mathbb{C}_K$ and finite abelian extensions of K. That norm subgroups are open follows by the same arguments as in the case of local fields.

THEOREM 10.4.14 (Existence theorem of global CFT). *The open subgroups of* $\mathbb{C}_K$ *of finite index are exactly the norm subgroups* $N_{L/K}\mathbb{C}_L$ *with* L *a finite abelian extension of* K.

The following consequences of the global reciprocity law and existence theorem can then be obtained much as before.

PROPOSITION 10.4.15. *Let* K *be a global field. For finite abelian extensions* L *and* M *of* K*, we have the following:*

a. $N_{L/K}\mathbb{C}_L \cap N_{M/K}\mathbb{C}_M = N_{LM/K}\mathbb{C}_{LM}$,

b. $N_{L/K}\mathbb{C}_L \cdot N_{M/K}\mathbb{C}_M = N_{(L\cap M)/K}\mathbb{C}_{L\cap M}$, *and*

c. $N_{M/K}\mathbb{C}_M \subseteq N_{L/K}\mathbb{C}_L$ *if and only if* $L \subseteq M$.

THEOREM 10.4.16 (Uniqueness theorem of global CFT). *Let* L *and* M *be distinct finite abelian extensions of a global field* K. *Then* $N_{L/K}\mathbb{C}_L \neq N_{M/K}\mathbb{C}_M$.

10.5. Comparison of the approaches

In this section, we compare the ideal-theoretic and idèle-theoretic approaches to global class field theory for number fields. For this, we begin by comparing ideal groups with groups of idèles. This requires a good deal of notation.

NOTATION 10.5.1. Let K be a number field, and let $\mathfrak{m}$ be a modulus for K. For a finite place v such that the associated prime ideal $\mathfrak{p}$ divides $\mathfrak{m}_f$, set $m_v = v(\mathfrak{m}_f)$. For a real place v such that the associated absolute value divides $\mathfrak{m}_\infty$, set $m_v = 1$, and let $U_1(K_v)$ denote the positive real numbers in $K_v = \mathbb{R}$. For exactly those v of either sort, we say that v divides $\mathfrak{m}$ and write $v \mid \mathfrak{m}$.

DEFINITION 10.5.2. Let K be a number field and $\mathfrak{m}$ a modulus for K.

a. The $\mathfrak{m}$-*idèle group* is the open subgroup $\mathbb{I}_K^{\mathfrak{m}}$ of $\mathbb{I}_K$ given by

$$\mathbb{I}_K^{\mathfrak{m}} = \{\alpha \in \mathbb{I}_K \mid \alpha_v \in U_{m_v}(K_v) \text{ for all } v \mid \mathfrak{m}\}.$$

b. The *congruence subgroup* of $\mathbb{I}_K^{\mathfrak{m}}$ with modulus $\mathfrak{m}$ is the open subgroup

$$W_{\mathfrak{m}} = \prod_{\substack{v \in V_K \\ v \mid \mathfrak{m}}} U_{m_v}(K_v) \times \prod_{\substack{v \in V_K \\ v \nmid \mathfrak{m}}} \mathscr{O}_v^\times.$$

PROPOSITION 10.5.3. *Let K be a number field and $\mathfrak{m}$ be a modulus for K.*

a. The homomorphism $\pi_K^{\mathfrak{m}} \colon \mathbb{I}_K^{\mathfrak{m}} \to I_K^{\mathfrak{m}}$ given by

$$\pi_K^{\mathfrak{m}}(\alpha) = \prod_{\substack{v \in V_{K,f} \\ v \nmid \mathfrak{m}}} \mathfrak{p}_v^{v(\alpha_v)}.$$

is surjective with kernel $W_{\mathfrak{m}}$.

b. The inclusion of $\mathbb{I}_K^{\mathfrak{m}}$ in $\mathbb{I}_K$ induces an isomorphism

$$\iota_K^{\mathfrak{m}} \colon \mathbb{I}_K^{\mathfrak{m}} / K_{\mathfrak{m},1} \xrightarrow{\sim} \mathbb{C}_K.$$

PROOF. That $\pi_K^{\mathfrak{m}}$ is surjective is immediate from the definitions, since elements of $\mathbb{I}_K^{\mathfrak{m}}$ have arbitrary coodinates (with all but finitely many unit coordinates) for $v \nmid \mathfrak{m}$. The kernel is also clearly $W_{\mathfrak{m}}$, as the requirement that an element of $\mathbb{I}_K^{\mathfrak{m}}$ lie in the kernel is exactly that it be a unit in all finite v not dividing $\mathfrak{m}$. This proves part a.

As for part b, note that $K^\times \cap \mathbb{I}_K^{\mathfrak{m}} = K_{\mathfrak{m},1}$, since the condition that $a \in K^\times$ lie in $\mathbb{I}_K^{\mathfrak{m}}$ is exactly that it lie in each $U_{m_v}(K_v)$ for $v \mid \mathfrak{m}$, which is to say that it lies in $K_{\mathfrak{m},1}$. For $\alpha \in \mathbb{I}_K$, we may choose $b \in K^\times$ such that $\alpha_v b^{-1} \in U_{m_v}(K_v)$ for all v dividing $\mathfrak{m}$ by weak approximation. It follows that $\alpha b^{-1} \in \mathbb{I}_K^{\mathfrak{m}}$ and therefore that $\alpha \in \mathbb{I}_K^{\mathfrak{m}} K^\times$. Since this tells us that $\mathbb{I}_K = \mathbb{I}_K^{\mathfrak{m}} K^\times$, the map $\iota_K^{\mathfrak{m}}$ is onto. □

NOTATION 10.5.4. Let us use $\eta_K^{\mathfrak{m}}$ to denote the composition

$$\eta_K^{\mathfrak{m}} = \bar{\pi}_K^{\mathfrak{m}} \circ (\iota_K^{\mathfrak{m}})^{-1} \colon \mathbb{C}_K \to \mathrm{Cl}_K^{\mathfrak{m}},$$

where $\bar{\pi}_K^{\mathfrak{m}} \colon \mathbb{I}_K^{\mathfrak{m}} / K_{\mathfrak{m},1} \to \mathrm{Cl}_K^{\mathfrak{m}}$ is the surjection induced by $\pi_K^{\mathfrak{m}}$, and where $\pi_K^{\mathfrak{m}}$ and $\iota_K^{\mathfrak{m}}$ are as in Proposition 10.5.3.

The following now gives the comparison between the Artin map $\psi_{L/K}^{\mathfrak{m}} \colon \mathrm{Cl}_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ for an abelian extension L/K with defining modulus $\mathfrak{m}$ and the global reciprocity map $\phi_{L/K} \colon \mathbb{C}_K \to \mathrm{Gal}(L/K)$.

THEOREM 10.5.5. *Let L/K be a finite abelian extension of number fields and $\mathfrak{m}$ a defining modulus for L/K. Then*

$$\phi_{L/K} = \psi_{L/K}^{\mathfrak{m}} \circ \eta_K^{\mathfrak{m}}$$

as maps from $\mathbb{C}_K$ to $\mathrm{Gal}(L/K)$.

PROOF. Choose an idèle class in $\mathbb{C}_K$, let $\alpha \in \mathbb{I}_K^{\mathfrak{m}}$ represent it, and let $\mathfrak{a} \in I_K^{\mathfrak{m}}$ be the product

$$\mathfrak{a} = \prod_{\substack{v \in V_{K,f} \\ v \nmid \mathfrak{m}}} \mathfrak{p}_v^{v(\alpha_v)},$$

which implies that $[\mathfrak{a}]_{\mathfrak{m}} = \eta_K^{\mathfrak{m}}([\alpha])$. We have

$$\psi_{L/K}^{\mathfrak{m}}([\mathfrak{a}]_{\mathfrak{m}}) = \prod_{\substack{v \in V_{K,f} \\ v \nmid \mathfrak{m}}} \psi_{L/K}^{\mathfrak{m}}([\mathfrak{p}_v]_{\mathfrak{m}})^{v(\alpha_v)} = \prod_{\substack{v \in V_{K,f} \\ v \nmid \mathfrak{m}}} (\mathfrak{p}_v, L/K)^{v(\alpha_v)} = \prod_{\substack{v \in V_{K,f} \\ v \nmid \mathfrak{m}}} \rho_{L_w/K_v}(\alpha_v). \tag{10.5.1}$$

Now, note that the conductor $\mathfrak{f}_{L/K}$ divides $\mathfrak{m}$ and that, by Proposition 7.4.21, we have $\mathfrak{f}_{L/K,f}\mathscr{O}_v = \mathfrak{f}_{L_w/K_v}$. Since for any finite v dividing $\mathfrak{m}$ and w a place of v lying over it we have by choice of α that $\alpha_v \equiv 1 \bmod \mathfrak{f}_{L_w/K_v}$, the definition of the local conductor tells us that $\rho_{L_w/K_v}(\alpha_v) = 1$. Moreover, if τ is a real embedding such that $|\ \ |_\tau$ divides $\mathfrak{m}$, we have that $\tau(\alpha_v) > 0$, so $\rho_{L_w/K_v}(\alpha_v) = 1$ as well. Therefore, we have

$$\prod_{\substack{v \in V_{K,f} \\ v \nmid \mathfrak{m}}} \rho_{L_w/K_v}(\alpha_v) = \prod_{v \in V_K} \rho_{L_w/K_v}(\alpha_v) = \Phi_{L/K}(\alpha),$$

and this together with (10.5.1) yields the result. □

REMARK 10.5.6. The global reciprocity map is defined a product of local reciprocity maps and computes the Artin maps for all finite abelian extensions. The Artin maps avoid much of the difficulty of ramification, as they arise from ideal groups that exclude ramified primes. The connection with local reciprocity is then much weaker, as one only sees the local maps for unramified extensions, whereby any uniformizer is taken to the unique Frobenius in the Galois group of the local extension. In that sense, the Artin maps then miss much of the complexity of the maps of local class field theory, which on the other hand is seen in the idèlic viewpoint.

Let us end this section by examining the case of class field theory over $\mathbb{Q}$.

EXAMPLE 10.5.7. Let us verify the global reciprocity law for $\mathbb{Q}$ via our computation of the local reciprocity map over $\mathbb{Q}_p$. The computation is given in Proposition 9.5.8, and we use it repeatedly.

Let p be a prime and $k \geq 1$. By the Kronecker-Weber theorem, it suffices to demonstrate that each $\Phi_{\mathbb{Q}}$ carries -1 and each prime number ℓ to Galois elements that act trivially on a primitive p^kth root of unity ζ_{p^k}.

For all primes $q \notin \{p, \ell\}$, we have that $\rho_{\mathbb{Q}_q}(\ell)$ fixes ζ_{p^k}. Also, since $\ell > 0$, we have $\rho_{\mathbb{R}}(\ell) = 1$. If $\ell = p$, then we have

$$\Phi_{\mathbb{Q}}(\ell)(\zeta_{p^k}) = \rho_{\mathbb{Q}_\ell}(\ell)(\zeta_{p^k}) = \zeta_{p^k}.$$

On the other hand, if $\ell \neq p$, then we have

$$\Phi_{\mathbb{Q}}(\ell)(\zeta_{p^k}) = \rho_{\mathbb{Q}_\ell}(\ell) \cdot \rho_{\mathbb{Q}_p}(\ell)(\zeta_{p^k}) = \rho_{\mathbb{Q}_\ell}(\ell)(\zeta_{p^k}^{\ell^{-1}}) = \zeta_{p^k},$$

As for -1, we have that $\rho_{\mathbb{Q}_q}(-1)$ fixes ζ_{p^k} for all $q \neq p$, that $\rho_{\mathbb{Q}_p}(-1)$ inverts ζ_{p^k}, and that $\rho_{\mathbb{R}}(-1)$ is complex conjugation, so

$$\Phi_{\mathbb{Q}}(-1)(\zeta_{p^k}) = \rho_{\mathbb{R}}(-1) \cdot \rho_{\mathbb{Q}_p}(-1)(\zeta_{p^k}) = \rho_{\mathbb{R}}(-1)(\zeta_{p^k}^{-1}) = \zeta_{p^k}.$$

REMARK 10.5.8. Recall that we did not actually prove Theorem 9.5.9 that the map constructed in Proposition 9.5.8 equals the local reciprocity map $\rho_{\mathbb{Q}_p}$. Via the argument of the last lemma, noting that local reciprocity maps for unramified extensions will be trivial on units and take uniformizers to the Frobenius element, we can actually use the global reciprocity law to give a short proof of this theorem.

EXAMPLE 10.5.9. We refer to the subspace

$$\mathbb{I}_{\mathbb{Q}}^f = \prod_{p \text{ prime}} (\mathbb{Q}_p^\times, \mathbb{Z}_p^\times)$$

of $\mathbb{I}_{\mathbb{Q}}$ as the group of finite idèles. Note that

$$\mathbb{I}_{\mathbb{Q}} = \mathbb{I}_{\mathbb{Q}}^f \times \mathbb{R}^\times.$$

Since $\mathbb{R}_{>0}$ is the kernel of $\rho_{\mathbb{R}}$, the map $\Phi_{\mathbb{Q}}$ factors through $\mathbb{I}_{\mathbb{Q}}^f \times \{\pm 1\}$. We have

$$\mathbb{I}_{\mathbb{Q}}/\mathbb{Q}^\times \mathbb{R}_{>0} \cong (\mathbb{I}_{\mathbb{Q}}^f \times \{\pm 1\})/\mathbb{Q}^\times \cong \mathbb{I}_{\mathbb{Q}}^f/\mathbb{Q}_{>0}.$$

Now, consider the map $\mathbb{I}_{\mathbb{Q}}^f \to \mathbb{Q}_{>0}$ that takes a finite idèle to the unique positive generator of the ideal to which it gives rise: that is, α is taken to $\prod_p p^{v_p(\alpha_p)}$. This is surjective with kernel

$$\hat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$$

and splits the natural inclusion $\mathbb{Q}_{>0} \to \mathbb{I}_{\mathbb{Q}}^f$. In other words, we have an identification

$$\mathbb{I}_{\mathbb{Q}}/\mathbb{Q}^\times \mathbb{R}_{>0} \cong \hat{\mathbb{Z}}^\times,$$

and the global reciprocity map $\phi_{\mathbb{Q}} \colon \mathbb{C}_{\mathbb{Q}} \to G_{\mathbb{Q}}^{\mathrm{ab}}$ factors through $\hat{\mathbb{Z}}^\times$.

The resulting map $\phi \colon \hat{\mathbb{Z}}^\times \to G_{\mathbb{Q}}^{\mathrm{ab}}$ is the inversion of the inverse map to the cyclotomic character $\chi \colon G_{\mathbb{Q}}^{\mathrm{ab}} \to \hat{\mathbb{Z}}^\times$. That is, we have

$$\phi(a)(\zeta) = \zeta^{a^{-1}}$$

for all $a = (a_p)_p \in \hat{\mathbb{Z}}^\times$ and roots of unity ζ. To see this, note that if ζ_{p^k} is a primitive p^kth root of unity for some prime p and $k \geq 1$, then Theorem 9.5.9 and our definition of ϕ imply that

$$\phi(a)(\zeta_{p^k}) = \rho_{\mathbb{Q}_p}(a_p)(\zeta_{p^k}) = \zeta_{p^k}^{a_k^{-1}},$$

where we may make sense of a^{-1} modulo p^k. In particular, ϕ is an isomorphism, so the image of $\mathbb{R}_{>0}$ is the kernel of $\phi_{\mathbb{Q}}$.

10.6. Cohomology of the idèles

Let L/K be a finite Galois extension of global fields with Galois group G. For a place w of L, let G_w denote the decomposition group of w in G.

LEMMA 10.6.1. *Let v be a place of K and u denote a fixed place of L lying over it. We have isomorphisms of G-modules*

$$\operatorname{Ind}_{G_u}^{G}(L_u^\times) \cong \prod_{w|v} L_w^\times \quad \text{and} \quad \operatorname{Ind}_{G_u}^{G}(\mathscr{O}_u^\times) \cong \prod_{w|v} \mathscr{O}_w^\times.$$

PROOF. The elements $\sigma \in G$ induce isomorphisms $\sigma\colon L_u \to L_{\sigma(u)}$ of K-algebras that in particular preserve valuations. The maps are then the restriction of the map

$$\operatorname{Ind}_{G_u}^{G}(L_u) = \mathbb{Z}[G] \otimes_{\mathbb{Z}[G_u]} L_u \to \prod_{w|v} L_w$$

induced by the biadditive map taking (σ, β) for $\sigma \in G$ and $\beta \in L_u$ to $\sigma(\beta) \in L_{\sigma(u)}$. That this is well-defined follows from the fact that if $\sigma = \sigma'\tau$ for some $\tau \in G_u$, then (σ, β) and $(\sigma', \tau(\beta))$ map to the same element. It is then easily seen to be an isomorphism of G-modules, and then the restrictions are isomorphisms as well. □

By Lemma 10.6.1 and Shapiro's lemma, we have isomorphisms

$$\hat{H}^i(G_u, L_u^\times) \cong \hat{H}^i\Big(G, \prod_{w|v} L_w^\times\Big) \quad \text{and} \quad \hat{H}^i(G_u, \mathscr{O}_u^\times) \cong \hat{H}^i\Big(G, \prod_{w|v} \mathscr{O}_w^\times\Big)$$

for all $i \in \mathbb{Z}$. Together, these enable us to describe the Tate cohomology groups of the idèle group $\mathbb{I}_L$.

NOTATION 10.6.2. For a finite set of places S of K, we set

$$\mathbb{I}_{L,S} = \prod_{v \in S} \prod_{w|v} L_w^\times \times \prod_{v \notin S} \prod_{w|v} \mathscr{O}_w^\times.$$

REMARK 10.6.3. We have $\mathbb{I}_L = \varinjlim_S \mathbb{I}_{L,S}$, where S runs over all finite subsets of V_K, with the injective maps induced by inclusions of sets of places. We can of course use any cofinal set of finite sets of places here.

PROPOSITION 10.6.4. *Let S be a finite set of places of K containing the archimedean places and those places that ramify in L/K. We have isomorphisms*

$$\hat{H}^i(G, \mathbb{I}_{L,S}) \cong \bigoplus_{v \in S} \hat{H}^i(G_w, L_w^\times)$$

for all $i \in Z$, where w denotes a choice of place over $v \in S$.

PROOF. As Tate cohomology commutes with products by construction, we have

$$\begin{aligned}\hat{H}^i(G,\mathbb{I}_{L,S}) &\cong \prod_{v\in S}\hat{H}^i\Big(G,\prod_{w|v}L_w^\times\Big)\times\prod_{v\notin S}\hat{H}^i\Big(G,\prod_{w|v}\mathscr{O}_w^\times\Big)\\ &\cong \prod_{v\in S}\hat{H}^i(G_w,L_w^\times)\times\prod_{v\notin S}\hat{H}^i(G_w,\mathscr{O}_w^\times),\end{aligned}$$

where in the latter step we have fixed a place w over each place $v\in V_K$. Since each $v\notin S$ is unramified in L, we have $\hat{H}^i(G_w,\mathscr{O}_w^\times)=0$ for all $i\in\mathbb{Z}$ by Lemma 9.1.6. The result follows. □

By (9.2.1), Hilbert's Theorem 90 and via the isomorphisms given by the local invariant maps, we have the following.

COROLLARY 10.6.5. *Let S be a finite set of places of K containing the archimedean places and those places that ramify in L/K. We have $|\hat{H}^0(G,\mathbb{I}_{L,S})|=\prod_{v\in S}|G_w|$, the group $H^1(G,\mathbb{I}_{L,S})$ is trivial, and*

$$H^2(G,\mathbb{I}_{L,S})=\bigoplus_{v\in S}\frac{1}{|G_w|}\mathbb{Z}/\mathbb{Z}$$

for any choice w of place of L over $v\in S$.

PROPOSITION 10.6.6. *We have*

$$\hat{H}^i(G,\mathbb{I}_L)\cong\bigoplus_{v\in V_K}\hat{H}^i(G_w,L_w^\times)$$

for all $i\in\mathbb{Z}$, where w denotes a choice of place over $v\in V_K$.

PROOF. It follows from Remark 10.6.3 that

$$\hat{H}^i(G,\mathbb{I}_L)\cong\varinjlim_S\hat{H}^i(G,\mathbb{I}_{L,S}),$$

where S runs over the finite sets of places of K containing the archimedean places of K and those places that ramify in L/K. By Proposition 10.6.4, we then have

$$\hat{H}^i(G,\mathbb{I}_L)\cong\varinjlim_S\prod_{v\in S}\hat{H}^i(G_w,L_w^\times)\cong\bigoplus_{v\in V_K}\hat{H}^i(G_w,L_w^\times).$$

□

Again, we have the following.

COROLLARY 10.6.7. *We have $H^1(G,\mathbb{I}_L)=0$ and*

$$H^2(G,\mathbb{I}_L)\cong\bigoplus_{v\in V_K}\frac{1}{|G_w|}\mathbb{Z}/\mathbb{Z}.$$

10.7. The first inequality

We will restrict our proofs of the reciprocity laws of global class field theory to number fields. We remark that the proofs we give carry over with little-to-no change to the function field setting for extensions of degree prime to the characteristic, but the proof of the second inequality in the case of equal characteristic requires some additional work.

So, we now let L/K be a finite Galois extension of number fields, still with Galois group G. Our interest is in the G-cohomology of $\mathbb{C}_L$, in that we would like to define invariant maps that make it into a class formation. Recall that we have a surjection $\mathbb{I}_L \to I_L$ taking an idèle to the fractional ideal it defines, and this map induces a surjection $\mathbb{C}_L \to \mathrm{Cl}_L$.

We will use S to denote a finite set of places of K, which we consistently suppose contains the archimedean places of K. (In the function field setting, S should be taken to be nonempty and the class group considered below should be replaced by a certain divisor class group.)

LEMMA 10.7.1. *Suppose that S contains a set of finite places generating the ideal class group of $\mathscr{O}_L$. Then $\mathbb{I}_K = \mathbb{I}_{K,S}K^\times$.*

PROOF. The kernel of the surjection $\mathbb{I}_K \to I_K$ is generated by the product of the local units at finite places and local multiplicative groups at infinite places, so the kernel of $\mathbb{C}_K \to \mathrm{Cl}_K$ is as well. We then note that the class group is generated by the classes of the chosen set of finite representatives $\mathfrak{p}$, and these are the images of idèles in $\mathbb{I}_{K,S}$ that are 1 in places but that for $\mathfrak{p}$ and the uniformizer at the prime. Thus $\mathbb{I}_K/\mathbb{I}_{K,S}K^\times = 0$. (Since we take $\mathscr{O}_w^\times = L_w^\times$ for archimedean places w, it is not strictly necessary to include these places in our set.) □

DEFINITION 10.7.2. The *ring of S-integers* $\mathscr{O}_{K,S}$ of K is the set of elements of K that lie in the valuation ring at all nonarchimedean places of K not in S. The *S-unit group* of K is $\mathscr{O}_{K,S}^\times$.

REMARK 10.7.3. We have $\mathbb{I}_{K,S} \cap K^\times = \mathscr{O}_{K,S}^\times$.

NOTATION 10.7.4. We use $\mathscr{O}_{L,S}$ to denote the S_L-integer ring of $\mathscr{O}_L$, where S_L denotes the set of places of L lying over those in S.

We have the following extension of Dirichlet's unit theorem. It also holds for function fields, though we restrict to the case of number fields.

PROPOSITION 10.7.5. *For a finite set S of places of a number field K containing its archimedean places, we have*

$$\mathrm{rank}_{\mathbb{Z}} \mathscr{O}_{K,S}^\times = |S| - 1.$$

PROOF. By Dirichlet's unit theorem, we know that $\mathrm{rank}_{\mathbb{Z}} \mathscr{O}_K = r_1(K) + r_2(K) - 1$, one less than the number of archimedean places of K. We have an exact sequence

$$1 \to \mathscr{O}_K^\times \to \mathscr{O}_{K,S}^\times \xrightarrow{\Sigma_{v \in S_f} v} \bigoplus_{v \in S_f} \mathbb{Z},$$

where S_f denotes the set of finite places in S. It then suffices to exhibit an S-unit with nonzero additive valuation at a given $v \in S_f$ and trivial valuation at all other finite places of K. For this, note that some power of the prime $\mathfrak{p}$ corresponding to v is principal, and any generator is then an S-unit with the desired property. □

As with local class field theory, much can be gained from the study of cyclic extensions.

THEOREM 10.7.6. *If L/K is cyclic, then $h(\mathbb{C}_L) = [L:K]$, for $G = \mathrm{Gal}(L/K)$.*

PROOF. Let S contain the ramified places in L/K and a set of finite places lying below primes generating the ideal class group of $\mathscr{O}_L$. We have $\mathbb{C}_L \cong \mathbb{I}_{L,S}/\mathscr{O}_{L,S}^\times$ by Lemma 10.7.1. Thus, we have

$$h(\mathbb{C}_L) = \frac{h(\mathbb{I}_{L,S})}{h(\mathscr{O}_{L,S}^\times)}.$$

Now, consider the $\mathbb{R}$-vector space V with basis the elements of the set S_L of places of L over those in S. Let G act on V by its canonical permutation of the standard basis. Consider its $\mathbb{Z}[G]$-submodule A generated over $\mathbb{Z}$ by the standard basis of V. We have $A \cong \bigoplus_{v\in S} \mathrm{Ind}_{G_w}^G(\mathbb{Z})$, where w is again used to denote a place over v. Then

$$h(A) \cong \prod_{v\in S} h(G_w, \mathbb{Z}) = \prod_{v\in S} n_v,$$

where n_v denotes the local degree of L/K at a prime over v.

We define a second lattice as follows. We have the homomorphism $\ell_{L,S}\colon \mathscr{O}_{L,S}^\times \to V$ given by

$$\ell_{L,S}(\beta) = (\log \|\beta\|_w)_{w\in S_L}.$$

By Corollary 4.4.2, we have that $\ker \ell_{L,S}$ is finite and, by the product formula, the image B^0 of $\ell_{L,S}$ is contained in the hyperplane V^0 of elements that sum to zero. The $\mathscr{O}_{L,S}^\times$ is the rank of $\mathscr{O}_L^\times$ plus the number of finite places in S, as some power of any finite prime is principal, and from this and Theorem 10.7.5, we see that B^0 must be a complete lattice in the hyperplane V^0.

Let $x = (1)_{w\in S_L} \in V^G$, and set

$$B = \mathbb{Z}x + B^0,$$

which is a complete lattice in V. We have an exact sequence of G-modules

$$0 \to B^0 \to B \to \mathbb{Z}x \to 0,$$

so $h(B) = h(B^0)h(\mathbb{Z}) = nh(\mathscr{O}_{L,S}^\times)$. On the other hand, any two complete lattices in a finite-dimensional $\mathbb{R}$-vector space are isomorphic upon tensor product with $\mathbb{Q}$, from which one can see that their Herbrand quotients are equal. Thus we have $h(A) = h(B)$, which tells us upon application of Corollary 10.6.5 that

$$h(\mathscr{O}_{L,S}^\times) = \frac{1}{n}h(A) = \frac{1}{n}\prod_{v\in S} n_v.$$

Combining this with our computation of $h(\mathbb{I}_{L,S})$ yields the theorem. □

As a corollary of this, we obtain what is known as the first inequality of global class field theory.

COROLLARY 10.7.7 (The first inequality). *For any finite cyclic extension L/K, we have $[\mathbb{C}_K : N_{L/K}\mathbb{C}_L] \geq [L:K]$.*

PROOF. The quantity on the left-hand side of the inequality is the order of $\hat{H}^0(G,\mathbb{C}_L)$, which is a multiple of the Herbrand quotient. □

The following is a simple consequence of the much stronger Čebotarev density theorem. We prove it using the first inequality.

COROLLARY 10.7.8. *Let L/K be finite abelian and S be a finite set of places of K containing the archimedean places and the ramified places in L/K. Then G is generated by the Frobenius elements in G of places not in S.*

PROOF. We may by enlarging S suppose that it contains a set of representatives of the class group of K. Let E be the fixed field of the subgroup of G generated by the Frobenius elements of nonarchimedean places not in S. Then for any $v \notin S$ and place w lying over v in G, we have that the local extension E_w/K_v is trivial, and in particular that $N_{E_w/K_v}E_w^\times = K_v^\times$. Thus, we have that $N_{E/K}\mathbb{I}_{E,S} = \mathbb{I}_{K,S}$, and by Lemma 10.7.1 we have that $K^\times\mathbb{I}_{K,S} = \mathbb{I}_K$, so $N_{E/K}\mathbb{C}_E = \mathbb{C}_K$. This implies the same equality with E replaced by any cyclic subextension, and then by the first inequality, such an extension must be trivial, so $E = K$. □

We leave it to the reader to prove the following additional consequences in a similar fashion, using Corollary 10.7.8.

COROLLARY 10.7.9. *Let L/K be cyclic of prime power degree. Then there exist infinitely many primes of K that remain inert in L/K.*

COROLLARY 10.7.10. *Let $L_1,\dots,L_t$ be cyclic extensions of K of prime degree p such that each L_i is disjoint from the compositum of the L_j for $j \neq i$. Then there are infinitely many primes of K that are inert in L_1 and split completely in L_i for $i \geq 2$.*

10.8. The second inequality

We turn to the opposite inequality, known as the second inequality, for general Galois extensions of number fields, beginning with Kummer extensions of prime exponent.

For now, let us fix $n \geq 1$. For a subset T of S, we set

$$\mathscr{I}_T = \prod_{v\in S-T} K_v^\times \times \prod_{v\in T} K_v^{\times n} \times \prod_{v\notin S} \mathscr{O}_v^\times.$$

LEMMA 10.8.1. *Suppose that $\mu_n \subset K$ and S contains the primes dividing n. Let T be a finite subset of S, and set $\Delta = K^\times \cap \mathscr{I}_T$ and $L = K(\Delta^{1/n})$. Then L/K is unramified outside of the places in $S-T$ and completely split at the places in T.*

PROOF. It suffices to see that for all $a \in \Delta$, the extension $K_v(a^{1/n})/K_v$ is unramified if $v \in S-T$ and trivial if $v \in T$. If $v \notin S$, then $a \in \mathscr{O}_v^\times$, so $K_v(a^{1/n})/K_v$ is tamely ramified, being of prime-to-p degree. Its is moreover unramified as the group $\langle a \rangle K_v^{\times n}$ contains no mth power of a uniformizer of K_v for m properly dividing n. If $v \in T$, then $a \in K_v^{\times n}$, so clearly $K_v(a^{1/n}) = K_v$. □

The following simple group-theoretic lemma will be of use to us shortly.

LEMMA 10.8.2. *For subgroups A, B, and C of a group with $A \leq B$ of finite index, we have*

$$[A : B] = [AC : BC][A \cap C : B \cap C].$$

PROOF. By the second and third isomorphism theorems and the fact that $A \leq B$, we have

$$\frac{AC}{BC} \cong \frac{AC/C}{BC/C} \cong \frac{A/(A \cap C)}{(A \cap BC)/(A \cap C)} \cong \frac{A}{(A \cap C)B} \cong \frac{A/B}{(A \cap C)B/B},$$

and $(A \cap C)B/B \cong (A \cap C)/(B \cap C)$. □

LEMMA 10.8.3. *Suppose that $\mu_n \subset K$ and S contains the primes over n and a set of representatives for Cl_K. Let S_1 be a subset of S and $S_2 = S - S_1$. Let $\Delta_i = K^\times \cap \mathscr{I}_{S_i}$ and $L_i = L(\Delta_i^{1/n})$ for $i \in \{1,2\}$. Then*

a. $\mathscr{I}_{S_1} \subseteq N_{L_2/K}\mathbb{I}_{L_2}$ and $\mathscr{I}_{S_2} \subseteq N_{L_1/K}\mathbb{I}_{L_1}$, and

b. $[\mathbb{C}_K : K^\times \mathscr{I}_{S_1}][\mathbb{C}_K : K^\times \mathscr{I}_{S_2}] = [L_1 : K][L_2 : K]$.

PROOF. For part a, let $\alpha = (\alpha_v)_v \in \mathscr{I}_{S_i}$ with $i \in \{1,2\}$. Let j be such that $\{i,j\} = \{1,2\}$, and let $E = L_j$ for brevity. For $v \in S_i$, we have $\alpha_v \in K_v^{\times n}$. By the the local reciprocity law, the quotient of $K_v^\times$ by the norm group $N_{E_w/K_v}E_w^\times$ for $w \mid v$ has exponent dividing n, so therefore α_v lies in it. Any $v \in S_j$ splits completely in E/K, so α_v is automatically a local norm for all places $w \mid v$. For all $v \notin S$, the extension E/K is unramified at v, and $\alpha_v \in \mathscr{O}_v^\times$. Since the local extension is unramified, its norm group contains $\mathscr{O}_v^\times$ (and in fact is generated by it and the uniformizer of K_v to the power of the residue degree of the extension). Thus, $\alpha \in N_{E/K}\mathbb{I}_E$. That is, we have $\mathscr{I}_{S_i} \subseteq N_{E/K}\mathbb{I}_E$.

As for part b, by Lemma 10.7.1 and the group-theoretic equality of indices that is Lemma 10.8.2, we have

$$[\mathbb{I}_K : K^\times \mathscr{I}_{S_1}] = [K^\times \mathbb{I}_{K,S} : K^\times \mathscr{I}_{S_1}] = \frac{[\mathbb{I}_{K,S} : \mathscr{I}_{S_1}]}{[K^\times \cap \mathbb{I}_{K,S} : K^\times \cap \mathscr{I}_{S_1}]} = \frac{[\mathbb{I}_{K,S} : \mathscr{I}_{S_1}]}{[\mathscr{O}_{K,S}^\times : \Delta_1]}.$$

Note that

$$\mathbb{I}_{K,S}/\mathscr{I}_{S_1} \cong \prod_{v \in S_1} K_v^\times / K_v^{\times n},$$

For a place v over p we have

$$[K_v^\times : K_v^{\times n}] = n^2 \cdot \|n\|_v^{-1},$$

since $K_v^\times \cong \mathbb{Z} \times \mu(K_v) \times \mathbb{Z}_p^{[K_v:\mathbb{Q}_p]}$ by Propositions 6.3.4 and 6.3.9 and $\mu_n \subseteq \mu(K_v)$. In fact, for any place v, we have we still have the equality, noting that the only archimedean places for $n \geq 3$ are complex. Letting $s = |S|$, we then have

$$[\mathbb{I}_{K,S} : \mathscr{I}_{S_1}][\mathbb{I}_{K,S} : \mathscr{I}_{S_2}] = n^{2s} \prod_{v \in S} \|n\|_v^{-1} = n^{2s} \prod_{v \notin S} \|n\|_v = n^{2s}$$

by the product formula and the fact that every place that divides n and all archimedean places lie in S.

We also have $[\mathscr{O}_{K,S} : \mathscr{O}_{K,S}^{\times n}] = n^s$ by Proposition 10.7.5 (which says that $\mathscr{O}_{K,S}^\times \cong \mathbb{Z}^{s-1} \times \mu(K)$), and $[\Delta_1 : \mathscr{O}_{K,S}^{\times n}] = [L_1 : K]$ by Kummer theory. Thus,

$$[\mathscr{O}_{K,S}^\times : \Delta_1][\mathscr{O}_{K,S}^\times : \Delta_2] = n^{2s}([L_1 : K][L_2 : K])^{-1},$$

and we then have

$$[\mathbb{I}_K : K^\times \mathscr{I}_{S_1}][\mathbb{I}_K : K^\times \mathscr{I}_{S_2}] = \frac{[\mathbb{I}_{K,S} : \mathscr{I}_{S_1}][\mathbb{I}_{K,S} : \mathscr{I}_{S_2}]}{[\mathscr{O}_{K,S}^\times : \Delta_1][\mathscr{O}_{K,S}^\times : \Delta_2]} = [L_1 : K][L_2 : K],$$

as claimed. □

We now specialize to the case that n equals a prime p.

PROPOSITION 10.8.4. *Let K be a number field that contains the pth roots of unity for a prime p. Let L/K be finite abelian of exponent p. Then $[\mathbb{C}_K : N_{L/K}\mathbb{C}_L]$ divides $[L : K]$.*

PROOF. Let k be such that $[L : K] = p^k$, and let $a_1, \ldots, a_k \in K^\times$ be such that $L = K(a_1^{1/p}, \ldots, a_k^{1/p})$. We aim to construct finite disjoint sets S_1 and S_2 of primes such that $S = S_1 \cup S_2$ satisfies the conditions of Lemma 10.8.3 with $K^\times \mathscr{I}_{S_2} = \mathbb{I}_K$ and $L_2 = L$. We will then have $[\mathbb{C}_K : N_{L_1/K}\mathbb{C}_{L_1}] = 1$, which by the first inequality forces $L_1 = K$, and Lemma 10.8.3 then implies the desired divisibility.

To start, choose S_1 to consist of the archimedean places, the primes over p, a set of representatives of Cl_K, and every finite place v such that $v(a_i) \neq 0$ for $1 \leq i \leq k$. Then $K^\times \mathbb{I}_{K,S_1} = \mathbb{I}_K$ by Lemma 10.7.1, and $a_i \in \mathscr{O}_{K,S_1}^\times$ for $1 \leq i \leq k$. Let $b_1, \ldots, b_t \in \mathscr{O}_{K,S_1}^\times$ be such that the images of $a_1, \ldots, a_k, b_1, \ldots, b_t$ form a basis of $\mathscr{O}_{K,S_1}^\times / \mathscr{O}_{K,S_1}^{\times p}$. Now, by Corollary 10.7.10, we may choose $S_2 = \{v_1, \ldots, v_t\}$, where for each v_i splits completely in L/K, remains inert in $K(b_i^{1/p})/K$, and splits completely in $K(b_j^{1/p})/K$ for $j \neq i$.

Recalling that we have set $n = p$, we have

$$\mathbb{I}_{K,S_1} \cap \mathscr{I}_{S_2} = \prod_{v \in S_1} K_v^\times \times \prod_{v \in S_2} \mathscr{O}_v^{\times p} \times \prod_{v \notin S} \mathscr{O}_v^\times.$$

We then have

$$\mathbb{I}_{K,S_1} / (\mathbb{I}_{K,S_1} \cap \mathscr{I}_{S_2}) \cong \prod_{i=1}^t \mathscr{O}_{v_i}^\times / \mathscr{O}_{v_i}^{\times p},$$

and since the residue characteristic of K_{v_i} is not p and $\mu_p \subset K_{v_i}^\times$, we have $\mathscr{O}_{v_i}^\times / \mathscr{O}_{v_i}^{\times p} \cong \mathbb{Z}/p\mathbb{Z}$. Note that $b_i \in \mathbb{I}_{K,S_1}$, and for $1 \leq i, j \leq t$, we have $b_i \notin \mathscr{O}_{v_j}^{\times p}$ if and only if $i = j$. Thus, the images of the

b_i generate $\mathbb{I}_{K,S_1}/(\mathbb{I}_{K,S_1} \cap \mathscr{I}_{S_2})$. Since the b_i lie in K, this tells us that $K^\times \mathscr{I}_{S_2} = K^\times \mathbb{I}_{K,S_1} = \mathbb{I}_K$, as desired.

Next, note that

$$\mathscr{I}_{S_2} \subseteq \mathbb{I}_{K,S_1} \mathbb{I}_K^p = \mathbb{I}_{K,S_1} (K^\times \mathbb{I}_{K,S_1})^p = \mathbb{I}_{K,S_1} K^{\times p}$$

by what we have just shown. In particular,

$$\Delta_2 = \mathscr{I}_{S_2} \cap K^\times \subseteq \mathscr{O}_{K,S_1}^\times K^{\times p},$$

and $\Delta_2 K^{\times p}/K^{\times p}$ is generated by the S_1-units that are locally pth powers at all $v \in S_2$. Recall that $\mathscr{O}_{K,S_1}^\times K^{\times p}/K^{\times p}$ is generated by the images of $a_1, \ldots, a_k, b_1, \ldots, b_t$. Since each v_j splits completely in the subfield $K(a_i^{1/p})$ of L, we have that $a_i \in \mathscr{O}_{v_j}^{\times p}$, so $a_i \in \Delta_2$ for $1 \leq i \leq k$. On the other hand, any non-pth-power in $\langle b_1, \ldots, b_t \rangle$ has nontrivial image in $\mathscr{O}_{v_j}^\times / \mathscr{O}_{v_j}^{\times p}$ for some j, so does not lie in $\Delta_2 K^{\times p}$. Thus, the images of the a_i generate $\Delta_2 K^{\times p}/K^{\times p}$, which is to say that $L_2 = L$. □

We now turn to more general extensions, no longer supposing $\mu_n \subset K$.

LEMMA 10.8.5. *For any finite extension L/K, the index $[\mathbb{C}_K : N_{L/K}\mathbb{C}_L]$ is finite and divisible only by primes dividing $[L:K]$.*

PROOF. Once we have finiteness, the divisibility statement follows from the fact that for any $\alpha \in \mathbb{C}_K$, we have $\alpha^{[L:K]} \in N_{L/K}\mathbb{C}_L$. For finiteness, we may suppose that L/K is Galois, since the norms of idèle classes from the Galois closure of L to K will also be norms from L. By Lemma 10.7.1, we may find a finite set of primes S of K containing the primes that ramify in L such that $\mathbb{I}_L = \mathbb{I}_{L,S} L^\times$ and $\mathbb{I}_K = \mathbb{I}_{K,S} K^\times$. Then

$$[\mathbb{C}_K : N_{L/K}\mathbb{C}_L] = [\mathbb{I}_K : K^\times N_{L/K}\mathbb{I}_L] = [K^\times \mathbb{I}_{K,S} : K^\times N_{L/K}\mathbb{I}_{L,S}] \leq [\mathbb{I}_{K,S} : N_{L/K}\mathbb{I}_{L,S}] = \prod_{v \in S} [L_w : K_v],$$

where w is any place of L over v, with the last equality by Proposition 10.6.5. □

For brevity, for a finite extension E/F of number fields, we let $n_{E/F} = [\mathbb{C}_F : N_{E/F}\mathbb{C}_E]$.

LEMMA 10.8.6. *Let M/K be a finite Galois extension and L an intermediate field. Then $n_{M/K}$ divides $n_{M/L} n_{L/K}$.*

PROOF. Note that

$$n_{M/K} = [N_{L/K}\mathbb{C}_L : N_{M/K}\mathbb{C}_M] n_{L/K}.$$

The map $N_{L/K}$ induces a surjective map

$$\mathbb{C}_L / N_{M/L}\mathbb{C}_M \to N_{L/K}\mathbb{C}_L / N_{M/K}\mathbb{C}_M$$

so $[N_{L/K}\mathbb{C}_L : N_{M/K}\mathbb{C}_M]$ divides $n_{M/L}$. □

The following is then immediate from the multiplicativity of degrees of field extensions.

COROLLARY 10.8.7. *Let M/K be a finite Galois extension and L an intermediate field. If $n_{M/L} \mid [M:L]$ and $n_{L/K} \mid [L:K]$, then $n_{M/K} \mid [M:K]$.*

THEOREM 10.8.8. *Let L/K be a finite Galois extension of number fields with Galois group G. Then $\hat{H}^0(G,\mathbb{C}_L)$ and $H^2(G,\mathbb{C}_L)$ have order dividing $[L:K]$, and $H^1(G,\mathbb{C}_L) = 0$.*

PROOF. By Lemma 9.1.12 applied in the cases $(i,r) = (0,1),(1,0),(2,1)$ in that order, the result follows for arbitrary Galois extensions from the case of cyclic extensions of prime degree. So, suppose that L/K is cyclic of degree a prime p. If we can show that $n_{L/K} = |\hat{H}^0(G,\mathbb{C}_L)|$ divides p, then the 2-periodicity of Tate cohomology and Theorem 10.7.6 give the result.

By Lemma 8.2.3, we have that $n_{L/K} \mid n_{L(\mu_p)/K}$, and by Lemma 10.8.6, we have that

$$n_{L(\mu_p)/K} \mid n_{L(\mu_p)/K(\mu_p)} n_{K(\mu_p)/K}.$$

Since $n_{K(\mu_p)/K}$ is prime to p and $n_{L/K}$ is a power of p by Lemma 10.8.5, we have that $n_{L/K}$ divides $n_{L(\mu_p)/K(\mu_p)}$, which is p by Proposition 10.8.4.

□

COROLLARY 10.8.9 (The second inequality). *For any finite Galois extension L/K, we have*

$$[\mathbb{C}_K : N_{L/K}\mathbb{C}_L] \leq [L:K].$$

From the fact that $H^1(G,\mathbb{C}_L) = 0$, we obtain the interesting consequence that in cyclic extensions, global elements that are local norms everywhere are global norms.

COROLLARY 10.8.10. *Suppose that L/K is cyclic. If $a \in K^\times$ and $a \in N_{L_w/K_v} L_w^\times$ for some $w \mid v$ for all places $v \in V_K$, then $a \in N_{L/K} L^\times$.*

PROOF. Since $H^1(G,\mathbb{C}_L) = 0$, the map

$$H^2(G,L^\times) \to H^2(G,\mathbb{I}_L)$$

is an injection. Since G is cyclic, we have that the corresponding map on 0th Tate cohomology groups is injective as well. In other words, the map

$$K^\times/N_{L/K}L^\times \to \bigoplus_{v\in V_K} K^\times/N_{L_w/K_v}L_w^\times$$

is injective, noting that the norm group for L_w/K_v is independent of the choice of $w \mid v$ (as L/K is Galois). This is exactly what was claimed. □

10.9. The reciprocity law

We continue to let K denote a number field and S a finite set of places of K containing the archimedean places. In this section, we use L to denote a finite abelian extension of K with Galois group G.

As noted in the proof of the Corollary 10.8.10, the triviality of $H^1(G,\mathbb{C}_L)$ implies that the map

$$\mathrm{Br}(L/K) = H^2(G,L^\times) \to H^2(G,\mathbb{I}_L) \cong \bigoplus_{v\in S} \mathrm{Br}(L_w/K_v)$$

is injective. In the direct limit over all Galois extensions L of K, we obtain an injective map

$$\mathrm{Br}(K) \hookrightarrow \bigoplus_{v\in V_K} \mathrm{Br}(K_v).$$

Let us use $\mathrm{inv}_v\colon \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$ to denote the composition of the map $\mathrm{Br}(K) \to \mathrm{Br}(K_v)$ with the local invariant map inv_{K_v}. (Here, $\mathrm{inv}_{\mathbb{R}}$ is the unique injection of the group $\mathrm{Br}(\mathbb{R})$ of order 2 in $\mathbb{Q}/\mathbb{Z}$.) We see from the fact that $\mathrm{Br}(K)$ maps to the direct sum that

$$\sum_{v\in V_K} \mathrm{inv}_v\colon \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$$

is well-defined. We will show that this map is zero.

In the following, we also use the notation inv_v to denote the composition

$$\mathrm{inv}_v\colon H^2(G,\mathbb{I}_L) \to \mathrm{Br}(K_v) \xrightarrow{\mathrm{inv}_{K_v}} \mathbb{Q}/\mathbb{Z}.$$

LEMMA 10.9.1. *For $\alpha \in \mathbb{I}_K$ and $\chi \in \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$, we have*

$$\sum_{v\in V_K} \mathrm{inv}_v(\bar{\alpha}\cup\delta\chi) = \chi(\Phi_{L/K}(\alpha)),$$

where $\delta\colon H^1(G,\mathbb{Q}/\mathbb{Z}) \to H^2(G,\mathbb{Z})$ is the connecting homomorphism for $0\to\mathbb{Z}\to\mathbb{Q}\to\mathbb{Q}/\mathbb{Z}\to 0$, and $\bar{\alpha}$ denotes the class of α in $\hat{H}^0(G,\mathbb{I}_L)$.

PROOF. By definition and the compatibility of cup products with restriction, we have

$$\mathrm{inv}_v(\bar{\alpha}\cup\delta\chi) = \mathrm{inv}_{K_v}(\overline{\alpha_v}\cup\delta\chi_v),$$

where $\overline{\alpha_v}$ denotes the image of α_v in $\hat{H}^0(G_v,L_w^\times)$ for a place w over v, where $\chi_v \in H^1(G_v,\mathbb{Q}/\mathbb{Z})$ is the restriction of χ to the decomposition group G_w, and where δ continues to denote the corresponding connecting homomorphism. By Proposition 8.1.10, we have that

$$\mathrm{inv}_{K_v}(\overline{\alpha_v}\cup\delta\chi_v) = \chi_v(\rho_{L_w/K_v}(\alpha_v)).$$

By definition of $\Phi_{L/K}$ and the fact that χ is a homomorphism, we have that

$$\chi(\Phi_{L/K}(\alpha)) = \sum_{v\in V_K} \chi_v(\rho_{L_w/K_v}(\alpha_v)),$$

hence the result. □

From the global recirpocity law for $\mathbb{Q}$, we may easily prove the global reciprocity law for cyclotomic extensions.

LEMMA 10.9.2. *Let L be an extension of K contained in $K(\mu_N)$ for some $N\geq 1$. Then $\Phi_{L/K}(a) = 1$ for all $a\in K^\times$.*

PROOF. For $E = \mathbb{Q}(\mu_N)$, we have $\Phi_{L/K}(a)|_E = \Phi_{E/\mathbb{Q}}(N_{K/\mathbb{Q}}(a))$ by part a of Proposition 10.4.13. Since the restriction map $G \to \mathrm{Gal}(E/\mathbb{Q})$ is injective, we are reduced to the already proven reciprocity law for $\mathbb{Q}$. □

LEMMA 10.9.3. *For any $n \geq 1$, let S denote the set of places of K dividing n and all real places. Then there exists a cyclic extension L of K contained in $K(\mu_N)$ for some $N \geq 1$ such that the local degree of L/K is divisible by n for all $v \in S_f$ and is equal to 2 for all real places of K.*

PROOF. Without loss of generality, we may suppose that 2 divides n. Let $n = p_1^{r_1} \cdots p_k^{r_k}$ be the prime factorization of n. If p_i is odd, let L_i be the maximal pro-p subextension of the field given by adjoining to K all p_i-power roots of unity. Otherwise, let L_i be the extension of K given by adjoining $\zeta - \zeta^{-1}$ for all 2-power roots of unity ζ. The unique degree 2 subextension of the latter field has no real places. For each i, the completions of the fields L_i at places $v \in S_f$ are infinite pro-p_i procyclic extensions. In particular, the compositum L of the fields L_i is a procyclic extension of K that contains a finite degree extension that is the desired subfield. □

We require the following simple cohomological lemma, the proof of which is left to the reader.

LEMMA 10.9.4. *Let G be a finite cyclic group of order n and $\chi\colon G \to \mathbb{Q}/\mathbb{Z}$ be an injective character. Let δ be the connecting map for $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. Let g be a generator of G, and let $u_g \in \hat{H}^{-2}(G,\mathbb{Z})$ be as in Proposition A.10.3. Viewing $\hat{H}^0(G,\mathbb{Z})$ and $\mathbb{Z}/n\mathbb{Z}$, and letting $\tilde{\chi}\colon G \to \mathbb{Z}/n\mathbb{Z}$ be the isomorphism obtained from χ by multiplication by n, we have*

$$u_g \cup \delta\chi = \tilde{\chi}(g) \in \mathbb{Z}/n\mathbb{Z}.$$

In other words, we have the following, the map being inverse to cup product with u_g for a generator $g \in G$ with $\chi(g) = \frac{1}{n}$.

COROLLARY 10.9.5. *Let G be a finite cyclic group of order n and $\chi\colon G \to \mathbb{Q}/\mathbb{Z}$ be an injective character. Let δ be the connecting map for $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. For any G-module A and and $i \in \mathbb{Z}$, the map*

$$\hat{H}^i(G,A) \to \hat{H}^{i+2}(G,A), \qquad c \mapsto \delta\chi \cup c$$

is an isomorphism.

PROPOSITION 10.9.6. *The map $\sum_{v \in V_K} \mathrm{inv}_v\colon \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$ is trivial.*

PROOF. Let $\beta \in \mathrm{Br}(K)$, and let n be the least common multiple of the orders of the elements $\mathrm{inv}_v(\beta)$ for $v \in V_K$. Let S contain the places where $\mathrm{inv}_v(\beta)$ is nonzero, and let L be as in Lemma 10.9.3. Then for each $v \in S$, the group $\mathrm{Br}(L_w/K_v)$ sits in $\mathrm{Br}(K_v)$ as as a cyclic subgroup of order a multiple of n, and hence it contains the image of β. It follows that $\beta \in \mathrm{Br}(L/K)$. Since L/K is cyclic, we have

an injective character $\chi\colon G \to \mathbb{Q}/\mathbb{Z}$. Corollary 10.9.5 then tells us that there exists $b \in K^\times$ such that such that $b \cup \delta\chi = \beta$. By Lemma 10.9.1, we have

$$\sum_{v \in V_K} \mathrm{inv}_v(\beta) = \chi(\Phi_{L/K}(b)),$$

and $\Phi_{L/K}(b) = 0$ by Lemma 10.9.2. □

We can now prove that the global reciprocity map factors through $\mathbb{C}_K$.

COROLLARY 10.9.7. *We have $\Phi_K(a) = 1$ for all $a \in K^\times$.*

PROOF. It suffices to show that $\Phi_{L/K}(a) = 1$ for all finite abelian extensions L/K, and for this, it suffices to show that $\chi(\Phi_{L/K}(a)) = 0$ for all characters $\chi\colon G \to \mathbb{Q}/\mathbb{Z}$ for all such L. By Lemma 10.9.1, the latter quantity equals $\sum_{v \in V_K} \mathrm{inv}_v(\bar{a} \cup \delta\chi)$, but this is zero by Proposition 10.9.6. □

Note that for any finite extension L of K, we have an injection $\mathbb{C}_K \hookrightarrow \mathbb{C}_L$ by Lemma 10.3.17. We aim to construct an invariant map $\mathrm{inv}\colon H^2(G_K, \mathbb{C}_{K^{\mathrm{sep}}}) \to \mathbb{Q}/\mathbb{Z}$ to show that $\mathbb{C}_{K^{\mathrm{sep}}} = \varinjlim_L \mathbb{C}_L$ together with the invariant maps associated for finite separable extensions of K forms a class formation.

Since since $H^1(G, \mathbb{C}_L) = 0$ and

$$H^2(G, \mathbb{I}_L) \cong \bigoplus_{v \in V_K} \mathrm{Br}(L_w/K_v),$$

the latter by Proposition 10.6.6, we have an exact sequence

$$0 \to \mathrm{Br}(L/K) \to \bigoplus_{v \in V_K} \mathrm{Br}(L_w/K_v) \to H^2(G, \mathbb{C}_L).$$

Recall that we have an isomorphism

$$\mathrm{inv}_{L_w/K_v}\colon \mathrm{Br}(L_w/K_v) \xrightarrow{\sim} \frac{1}{|G_w|}\mathbb{Z}/\mathbb{Z},$$

where G_w is the decomposition group at any $w \mid v$. The sum of these local invariant maps

$$\sum_{v \in V_K} \mathrm{inv}_{L_w/K_v}\colon \bigoplus_{v \in S} \mathrm{Br}(L_w/K_v) \to \frac{1}{|G|}\mathbb{Z}/\mathbb{Z}$$

is surjective due to the existence of an inert prime w over some $v \in V_K$. Let

$$\widetilde{\mathrm{inv}}_{L/K}\colon H^2(G, \mathbb{I}_L) \twoheadrightarrow \frac{1}{|G|}\mathbb{Z}/\mathbb{Z}$$

denote the composite map. By Proposition 10.9.6, we have that $\mathrm{Br}(L/K)$ is contained in the kernel of $\widetilde{\mathrm{inv}}_{L/K}$. That is, $\widetilde{\mathrm{inv}}_{L/K}$ factors through a surjective global invariant map

$$\mathrm{inv}_{L/K}\colon B_{L/K} \twoheadrightarrow \frac{1}{|G|}\mathbb{Z}/\mathbb{Z}$$

from the image $B_{L/K}$ of $H^2(G, \mathbb{I}_L) \to H^2(G, \mathbb{C}_L)$. We aim to show that $H^2(G, \mathbb{I}_L) \to H^2(G, \mathbb{C}_L)$ is surjective so $B_{L/K} = H^2(G, \mathbb{C}_K)$, and $\mathrm{inv}_{L/K}$ is an injective. We start with cyclic extensions.

LEMMA 10.9.8. *Let L/K be finite cyclic. Then $H^2(G,\mathbb{I}_L) \to H^2(G,\mathbb{C}_L)$ is surjective, and the invariant map*

$$\mathrm{inv}_{L/K}\colon H^2(G,\mathbb{C}_L) \xrightarrow{\sim} \frac{1}{|G|}\mathbb{Z}/\mathbb{Z}$$

is an isomorphism.

PROOF. We have $H^3(G,L^\times) \cong H^1(G,L^\times) = 0$ by the periodicty of Tate cohomology, so $B_{L/K} = H^2(G,\mathbb{C}_L)$. Since $H^2(G,\mathbb{C}_L)$ has order $|G|$ by the first and second inequalities, the result follows. □

The next lemma shows that global invariant maps behave as expected under restriction.

LEMMA 10.9.9. *Let E be a finite extension of K contained in L, and set $H = \mathrm{Gal}(L/E)$. The diagram*

$$\begin{array}{ccc} H^2(G,\mathbb{I}_L) & \xrightarrow{\widetilde{\mathrm{inv}}_{L/K}} & \frac{1}{|G|}\mathbb{Z}/\mathbb{Z} \\ \big\downarrow \mathrm{Res} & & \big\downarrow [E:K] \\ H^2(H,\mathbb{I}_L) & \xrightarrow{\widetilde{\mathrm{inv}}_{L/E}} & \frac{1}{|H|}\mathbb{Z}/\mathbb{Z} \end{array}$$

commutes.

PROOF. Since the global invariant maps are sums of local invariant maps, this reduces to the commutativity of the diagram

$$\begin{array}{ccc} H^2(G,\prod_{w|v} L_w^\times) & \xrightarrow{\sum_{w|v}\mathrm{inv}_{L_w/K_v}} & \frac{1}{|G|}\mathbb{Z}/\mathbb{Z} \\ \big\downarrow \mathrm{Res} & & \big\downarrow [E:K] \\ H^2(H,\prod_{w|v} L_w^\times) & \xrightarrow{\sum_{w|v}\mathrm{inv}_{L_w/K_v}} & \frac{1}{|H|}\mathbb{Z}/\mathbb{Z} \end{array}$$

where $v \in V_K$ and w denotes a place of L over v. By Lemma 10.6.1 and Shapiro's lemma, this reduces to the commutativity of

$$\begin{array}{ccc} \mathrm{Br}(L_{w_0}/K_v) & \xrightarrow{\mathrm{inv}_{L_{w_0}/K_v}} & \frac{1}{|G|}\mathbb{Z}/\mathbb{Z} \\ \big\downarrow \mathrm{Res} & & \big\downarrow [E:K] \\ \bigoplus_{u|v}\mathrm{Br}(L_w/E_u) & \xrightarrow{\sum_{u|v}\mathrm{inv}_{L_w/E_u}} & \frac{1}{|H|}\mathbb{Z}/\mathbb{Z}, \end{array}$$

where u runs over the places over v in E, we use w to denote a place over u, and w_0 denotes a fixed place of L over v. Here, each w is conjugate to w_0 over K, and the u-coordinate fo the restriction map Res is induced by conjugation by $\sigma \in G$ with $\sigma(w_0) = w$ followed by restriction. We remark that $\mathrm{inv}_{L_w/K_v} \circ \sigma^* = \mathrm{inv}_{L_{w_0}/K_v}$ by definition. The local invariant maps have the property that

$$\mathrm{inv}_{L_w/E_u} \circ \mathrm{Res}_{E_u/K_v} = [E_u : K_v]\,\mathrm{inv}_{L_w/K_v},$$

so we have

$$\left(\sum_{u|v} \mathrm{inv}_{L_w/E_u}\right) \circ \mathrm{Res}_{E_u/K_v} = \sum_{u|v} [E_u : K_v] \, \mathrm{inv}_{L_w/K_v} = [E : K] \, \mathrm{inv}_{L_w/K_v},$$

the latter step as the sum of local degrees is the global degree. □

We next treat the general case.

PROPOSITION 10.9.10. *The map $H^2(G, \mathbb{I}_L) \to H^2(G, \mathbb{C}_L)$ is surjective, and the invariant map*

$$\mathrm{inv}_{L/K} \colon H^2(G, \mathbb{C}_L) \xrightarrow{\sim} \frac{1}{|G|}\mathbb{Z}/\mathbb{Z}$$

is an isomorphism.

PROOF. Since $H^1(G, A_L) = 0$, where $A_L \in \{L^\times, \mathbb{I}_L, \mathbb{C}_L\}$, the inflation maps

$$\mathrm{Inf} \colon H^2(G, A_L) \to H^2(G_K, A_{K^{\mathrm{sep}}})$$

are injective, being part of the inflation-restriction sequences. The direct limit of the maps $\widetilde{\mathrm{inv}}_{L/K}$ over Galois extensions L/K provide a surjective map

$$\widetilde{\mathrm{inv}}_K \colon H^2(G_K, \mathbb{I}_{K^{\mathrm{sep}}}) \to \mathbb{Q}/\mathbb{Z}.$$

which factors through a surjective map

$$\mathrm{inv}_K \colon B_K \to \mathbb{Q}/\mathbb{Z},$$

where $B_K = \varinjlim_L B_{L/K}$. By Lemma 10.9.3,

$$H^2(G_K, \mathbb{I}_{K^{\mathrm{sep}}}) \cong \bigoplus_{v \in V_K} \mathrm{Br}(K_v)$$

is the union of its subgroups $H^2(\mathrm{Gal}(F/K), \mathbb{I}_F)$, where F runs over the set $\mathscr{E}$ of cyclic cyclotomic extensions of K. From the map of exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \bigcup_{F\in\mathscr{E}} \mathrm{Br}(F/K) & \longrightarrow & \bigcup_{F\in\mathscr{E}} H^2(\mathrm{Gal}(F/K), \mathbb{I}_F) & \longrightarrow & \bigcup_{F\in\mathscr{E}} H^2(\mathrm{Gal}(F/K), \mathbb{C}_F) & \longrightarrow & 0 \\
 & & \big\downarrow & & \big\downarrow \wr & & \big\downarrow & & \\
0 & \longrightarrow & \mathrm{Br}(K) & \longrightarrow & H^2(G_K, \mathbb{I}_{K^{\mathrm{sep}}}) & \longrightarrow & H^2(G_K, \mathbb{C}_{K^{\mathrm{sep}}}), & &
\end{array}$$

we see that $\mathrm{Br}(K) = \bigcup_{F\in\mathscr{E}} \mathrm{Br}(F/K)$ is the kernel of $\tilde{\mathrm{inv}}_K$ and $B_K = \bigcup_{F\in\mathscr{E}} H^2(G, \mathbb{C}_F)$. In particular, we have an induced isomorphism $\mathrm{inv}_K \colon B_K \to \mathbb{Q}/\mathbb{Z}$.

Since $B_{L/K}$ injects into $B_K \cong \mathbb{Q}/\mathbb{Z}$ with image $\frac{1}{|G|}\mathbb{Z}/\mathbb{Z}$, we see that $B_{L/K}$ has order $[L : K]$. On the other hand, $B_{L/K}$ divides the order of $H^2(G, \mathbb{C}_L)$, which divides $[L : K]$ by Theorem 10.8.8. So $B_{L/K} = H^2(G, \mathbb{C}_L)$ is mapped isomorphically to $\frac{1}{|G|}\mathbb{Z}/\mathbb{Z}$ by $\mathrm{inv}_{L/K}$, as asserted. □

We have now constructed our global class formation.

THEOREM 10.9.11. *Given a number field K, the pair $(\mathbb{C}_{K^{\mathrm{sep}}}, \mathrm{inv})$, where* inv *is the collection of invariant maps*

$$\mathrm{inv}_E \colon H^2(G_E, \mathbb{C}_{K^{\mathrm{sep}}}) \to \mathbb{Q}/\mathbb{Z}$$

for finite separable extensions E of K in K^{sep} forms a class formation for K. Moreover, the reciprocity map defined by this class formation is the map $\phi_K \colon \mathbb{C}_K \to G_K^{\mathrm{ab}}$ induced by the product Φ_K of local reciprocity maps on the idèles.

PROOF. That we have a global class formation is an immediate corollary of Proposition 10.9.9 and Lemma 10.9.10. Let $\phi_{L/K}$ be the resulting reciprocity map. We know by Proposition 8.1.10 that

$$\mathrm{inv}_{L/K}(\bar{a} \cup \delta(\chi)) = \chi(\phi_{L/K}(a))$$

for all $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ and $a \in \mathbb{C}_K$. On the other hand, we showed in Lemma 10.9.1 that

$$\widetilde{\mathrm{inv}}_{L/K}(\bar{\alpha} \cup \delta\chi) = \chi(\Phi_{L/K}(\alpha)),$$

for all such χ and $\alpha \in \mathbb{I}_K$. Since $\phi_{L/K}$ and $\Phi_{L/K}$ are completely determined by their compositions with characters of G, we must have that $\Phi_{L/K}$ factors through $\mathbb{C}_K$ and induces $\phi_{L/K}$ on the quotient. □

10.10. Power reciprocity laws

In this section, we consider higher reciprocity laws that generalize quadratic reciprocity. For this, we introduce the notion of an nth power residue symbol for a number field.

NOTATION 10.10.1. In this section, n will denote a positive integer, and K will denote a number field that contains the full group μ_n of nth roots of unity.

DEFINITION 10.10.2. The nth *power residue symbol* for K is a function with values

$$\left(\frac{a}{\mathfrak{b}}\right)_{n,K} \in \mu_n$$

defined on pairs $(a, \mathfrak{b})$ consisting of a nonzero element a of $\mathscr{O}_K$ and a nonzero ideal $\mathfrak{b}$ of $\mathscr{O}_K$ such that $\mathfrak{b}$ is relatively prime to (na) defined as follows. For a prime $\mathfrak{p}$ not dividing (na), its value is the unique nth root of unity in $K^\times$ satisfying the congruence

$$\left(\frac{a}{\mathfrak{p}}\right)_{n,K} \equiv a^{(N\mathfrak{p}-1)/n} \bmod \mathfrak{p},$$

and for an arbitrary $\mathfrak{b}$ with prime factorization $\mathfrak{b} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$, its value is given by

$$\left(\frac{a}{\mathfrak{b}}\right)_{n,K} = \prod_{i=1}^{k} \left(\frac{a}{\mathfrak{p}_i}\right)_{n,K}^{r_i}.$$

NOTATION 10.10.3. If a and b are nonzero elements of $\mathscr{O}_K$ such that (b) is relatively prime to (na), then we set

$$\left(\frac{a}{b}\right)_{n,K} = \left(\frac{a}{(b)}\right)_{n,K}.$$

REMARK 10.10.4. The 2nd power residue symbol for $\mathbb{Q}$ is none other than the Jacobi symbol, since $N(p) = p$ for a prime (p) of $\mathbb{Z}$.

We will derive an nth power reciprocity law for the power residue symbols, generalizing quadratic reciprocity. To begin with, we have the following.

LEMMA 10.10.5. *Suppose that $\mathfrak{p}$ is a nonzero prime of K not dividing n and that $a \in \mathscr{O}_K$ with $v_\mathfrak{p}(a) = 0$. Let $\pi_\mathfrak{p}$ be a unifomizer of $K_\mathfrak{p}$. Then*

$$\left(\frac{a}{\mathfrak{p}}\right)_{n,K} = (a, \pi_\mathfrak{p})_{n,K_\mathfrak{p}}.$$

PROOF. Since $N\mathfrak{p}$ is the order of the residue field of $K_\mathfrak{p}$ and a is a unit in the valuation ring of $K_\mathfrak{p}$, that the two sides are equal are an immediate consequence of our formula for the tame symbol. □

COROLLARY 10.10.6. *Let $a, b \in \mathscr{O}_K$ be nonzero, and suppose that (b) is relatively prime to (na). Then*

$$\left(\frac{a}{b}\right)_{n,K} = \prod_{\mathfrak{p}|(b)} (a,b)_{n,K_\mathfrak{p}},$$

where the product is over nonzero primes of $\mathscr{O}_K$ dividing (b).

PROOF. Write $(b) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$ for distinct primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ and positive integers r_i for some $k \geq 0$. Letting $\pi_{\mathfrak{p}_i}$ denote a uniformizer for $K_{\mathfrak{p}_i}$, we have by Lemma 10.10.5 that

$$\left(\frac{a}{b}\right)_{n,K} = \prod_{i=1}^{k} \left(\frac{a}{\mathfrak{p}_i}\right)_{n,K}^{r_i} = \prod_{i=1}^{k} (a, \pi_{\mathfrak{p}_i}^{r_i})_{n,K_{\mathfrak{p}_i}}.$$

Since b is $\pi_{\mathfrak{p}_i}^{r_i}$ times a unit in the valuation ring of $K_{\mathfrak{p}_i}$, we have (for instance by the formula for the tame symbol) that

$$(a, \pi_{\mathfrak{p}_i}^{r_i})_{n,K_{\mathfrak{p}_i}} = (a,b)_{n,K_{\mathfrak{p}_i}}$$

for each i, and the result follows. □

Note also that global reciprocity gives us the following product formula for norm residue symbols.

LEMMA 10.10.7. *For every $a, b \in K^\times$, we have*

$$\prod_{v \in V_K} (a,b)_{n,K_v} = 1.$$

PROOF. We have $\rho_{K_v(a^{1/n})/K_v}(b) = 1$ outside of a finite set $S = \{v_1, \ldots, v_t\}$ of places of K, so the product is finite, and global reciprocity then says that

$$\prod_{v \in S} \rho_{K_v(a^{1/n})/K_v}(b) = 1.$$

It follows that

$$\prod_{v\in V_K}(a,b)_{n,K_v}=\prod_{v\in S}(a,b)_{n,K_v}=\prod_{v\in S}\frac{\rho_{K_v}(b)(a^{1/n})}{a^{1/n}}$$
$$=\prod_{i=1}^{t}\rho_{K_{v_1}}(b)\cdots\rho_{K_{v_{i-1}}}(b)\left(\frac{\rho_{K_{v_i}}(b)(a^{1/n})}{a^{1/n}}\right)=\frac{\left(\prod_{v\in S}\rho_{K_v(a^{1/n})/K_v}(b)\right)(a^{1/n})}{a^{1/n}}=1.$$

□

We are now in a position to prove the nth power reciprocity law for K.

THEOREM 10.10.8 (Higher reciprocity law). *Let K be a number field containing the group μ_n of nth roots of unity. Let $a,b\in\mathscr{O}_K$ elements relatively prime to each other and to n. We then have*

$$\left(\frac{a}{b}\right)_{n,K}\left(\frac{b}{a}\right)_{n,K}^{-1}=\prod_{v|n\infty}(b,a)_{n,K_v},$$

where the product is over the places of K extending a prime dividing n or the real infinite place of $\mathbb{Q}$. Moreover, if $c\in\mathscr{O}_K$ is relatively prime to a and divisible only by primes dividing n, then

$$\left(\frac{c}{b}\right)_{n,K}=\prod_{v|n\infty}(b,c)_{n,K_v}.$$

PROOF. Corollary 10.10.6 tells us that

$$\left(\frac{a}{b}\right)_{n,K}\left(\frac{b}{a}\right)_{n,K}^{-1}=\prod_{\mathfrak{p}|(b)}(a,b)_{n,K_\mathfrak{p}}\cdot\prod_{\mathfrak{p}|(a)}(b,a)_{n,K_\mathfrak{p}}^{-1}=\prod_{\mathfrak{p}|(ab)}(a,b)_{n,K_\mathfrak{p}}.$$

Note that $(a,b)_{n,K_\mathfrak{p}}=1$ unless the prime $\mathfrak{p}$ of $\mathscr{O}_K$ divides one of a, b, or n, since otherwise the extension $K_\mathfrak{p}(a^{1/n})/K_\mathfrak{p}$ is unramified and b is a unit in $K_\mathfrak{p}$. Applying Lemma 10.10.7, we then have

$$\prod_{\mathfrak{p}|(ab)}(a,b)_{n,K_\mathfrak{p}}=\left(\prod_{v|n\infty}(a,b)_{n,K_v}\right)^{-1}=\prod_{v|n\infty}(b,a)_{n,K_v},$$

finishing the proof in this case. In the remaining case, the same argument, but now noting that $(a,b)_{n,K_\mathfrak{p}}=1$ unless $\mathfrak{p}$ divides b or n, we have

$$\left(\frac{c}{b}\right)_{n,K}=\prod_{\mathfrak{p}|(b)}(c,b)_{n,K_\mathfrak{p}}=\prod_{v|n\infty}(b,c)_{n,K_\mathfrak{p}}.$$

□

EXAMPLE 10.10.9. Take the case that $K=\mathbb{Q}$ and $n=2$. Let a and b be positive, odd integers. Then Theorem 10.10.8 implies that

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=(b,a)_{2,\mathbb{Q}_p}(b,a)_{2,\mathbb{R}}.$$

The first symbol is $(-1)^{(a-1)(b-1)/4}$ by Proposition 9.3.6, and the second symbol is trivial by Remark 9.3.9. Similarly, we have

$$\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2} \quad \text{and} \quad \left(\frac{2}{b}\right) = (-1)^{(p^2-1)/8}.$$

Thus, the power reciprocity law for $K = \mathbb{Q}$ and $n = 2$ is simply quadratic reciprocity.

The following special case of a result of the author serves as an entertaining example of the use of higher reciprocity laws.

PROPOSITION 10.10.10. *Let p be an odd prime number, and let m be an integer. Suppose that $\ell = \Phi_p(pm)$ is a prime number. Then every divisor of m is a pth power residue modulo ℓ.*

PROOF. Let a be a divisor of m. Note that

$$\ell = N_{\mathbb{Q}(\mu_p)/\mathbb{Q}}(1 - pm\zeta_p)$$

and can only be prime if m is nonzero. The definition of the pth power residue symbol says that

$$\left(\frac{a}{1-pm\zeta_p}\right)_{p,\mathbb{Q}(\mu_p)} \equiv a^{(\ell-1)/p} \bmod (1 - pm\zeta_p), \tag{10.10.1}$$

Since a is an integer, this implies that the symbol in (10.10.1) is the unique pth root of unity congruent to $a^{(\ell-1)/p}$ modulo ℓ. Thus, it will be trivial if and only if a is a pth power residue modulo ℓ.

So, we compute the symbol. We have

$$\left(\frac{a}{1-pm\zeta_p}\right)_{p,\mathbb{Q}(\mu_p)} = \left(\frac{1-pm\zeta_p}{a}\right)_{p,\mathbb{Q}(\mu_p)} (1 - pm\zeta_p, a)_{p,\mathbb{Q}_p(\mu_p)} = (1 - pm\zeta_p, a)_{p,\mathbb{Q}_p(\mu_p)}.$$

If p divides m, then $1 - pm\zeta_p$ is a pth power in $\mathbb{Q}_p(\mu_p)$, and we are done. If a is a pth power in $\mathbb{Z}_p^\times$, we are done as well. So, we may assume that a is not a pth power in $\mathbb{Z}_p^\times$. Then $\mathbb{Q}_p(\zeta_p, a^{1/p}) = \mathbb{Q}_p(\zeta_p, (1-p)^{1/p})$, and the conductor of the latter extension of $\mathbb{Q}_p(\mu_p)$ is $(1-\zeta_p)^2$ by Proposition 9.6.16. Since $1 - pm\zeta_p \in U_{p-1}(\mathbb{Q}_p(\mu_p))$ and $p - 1 \geq 2$, we then have that $(1 - pm\zeta_p, a)_{p,\mathbb{Q}_p(\mu_p)} = 1$, which completes the proof. □

APPENDIX A

Group cohomology

A.1. Group rings

Let G be a group.

DEFINITION A.1.1. The *group ring* (or, more specifically, $\mathbb{Z}$-group ring) $\mathbb{Z}[G]$ of a group G consists of the set of finite formal sums of group elements with coefficients in $\mathbb{Z}$

$$\left\{ \sum_{g\in G} a_g g \mid a_g \in \mathbb{Z} \text{ for all } g \in G, \text{ almost all } a_g = 0 \right\}.$$

with addition given by addition of coefficients and multiplication induced by the group law on G and $\mathbb{Z}$-linearity. (Here, "almost all" means all but finitely many.)

In other words, the operations are

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g$$

and

$$\left(\sum_{g\in G} a_g g \right) \left(\sum_{g\in G} b_g g \right) = \sum_{g\in G} (\sum_{k\in G} a_k b_{k^{-1}g}) g.$$

REMARK A.1.2. In the above, we may replace $\mathbb{Z}$ by any ring R, resulting in the R-group ring $R[G]$ of G. However, we shall need here only the case that $R = \mathbb{Z}$.

DEFINITION A.1.3.

i. The *augmentation map* is the homomorphism $\varepsilon\colon \mathbb{Z}[G] \to \mathbb{Z}$ given by

$$\varepsilon \left(\sum_{g\in G} a_g g \right) = \sum_{g\in G} a_g.$$

ii. The *augmentation ideal* I_G is the kernel of the augmentation map ε.

LEMMA A.1.4. *The augmentation ideal I_G is equal to the ideal of $\mathbb{Z}[G]$ generated by the set $\{g-1 \mid g \in G\}$.*

PROOF. Clearly $g - 1 \in \ker \varepsilon$ for all $g \in G$. On the other hand, if $\sum_{g\in G} a_g = 0$, then

$$\sum_{g\in G} a_g g = \sum_{g\in G} a_g (g-1).$$

□

DEFINITION A.1.5. If G is a finite group, we then define the *norm element* of $\mathbb{Z}[G]$ by $N_G = \sum_{g\in G} g$.

REMARK A.1.6.

a. We may speak, of course, of modules over the group ring $\mathbb{Z}[G]$. We will refer here to such $\mathbb{Z}[G]$-modules more simply as *G-modules*. To give a G-module is equivalent to giving an abelian group A together with a G-action on A that is compatible with the structure of A as an abelian group, i.e., a map

$$G \times A \to A, \qquad (g,a) \mapsto g \cdot a$$

satisfying the following properties:

(i) $1 \cdot a = a$ for all $a \in A$,

(ii) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $a \in A$ and $g_1, g_2 \in G$, and

(iii) $g \cdot (a_1 + a_2) = g \cdot a_1 + g \cdot a_2$ for all $a_1, a_2 \in A$ and $g \in G$.

b. A homomorphism $\kappa\colon A \to B$ of G-modules is just a homomorphism of abelian groups that satisfies $\kappa(ga) = g\kappa(a)$ for all $a \in A$ and $g \in G$. The group of such homomorphisms is denoted by $\mathrm{Hom}_{\mathbb{Z}[G]}(A,B)$.

DEFINITION A.1.7. We say that a G-module A is a *trivial* if $g \cdot a = a$ for all $g \in G$ and $a \in A$.

DEFINITION A.1.8. Let A be a G-module.

i. The group of *G-invariants* A^G of A is given by

$$A^G = \{a \in A \mid g \cdot a = a \text{ for all } g \in G, a \in A\},$$

which is to say the largest submodule of A fixed by G.

ii. The group of *G-coinvariants* A_G of A is given by

$$A_G = A/I_G A,$$

which is to say (noting Lemma A.1.4) the largest quotient of A fixed by G.

EXAMPLE A.1.9.

a. If A is a trivial G-module, then $A^G = A$ and $A_G \cong A$.

b. One has $\mathbb{Z}[G]_G \cong \mathbb{Z}$. We have $\mathbb{Z}[G]^G = (N_G)$ if G is finite and $\mathbb{Z}[G]^G = (0)$ otherwise.

A.2. Group cohomology via cochains

The simplest way to define the ith cohomology group $H^i(G,A)$ of a group G with coefficients in a G-module A would be to let $H^i(G,A)$ be the ith derived functor on A of the functor of G-invariants. However, not wishing to assume homological algebra at this point, we take a different tack.

DEFINITION A.2.1. Let A be a G-module, and let $i \geq 0$.

i. The group of *i-cochains* of G with coefficients in A is the set of functions from G^i to A:

$$C^i(G,A) = \{f\colon G^i \to A\}.$$

ii. The ith *differential* $d^i = d^i_A\colon C^i(G,A) \to C^{i+1}(G,A)$ is the map

$$d^i(f)(g_0,g_1,\ldots,g_i) = g_0 \cdot f(g_1,\ldots g_i) + \sum_{j=1}^{i} (-1)^j f(g_0,\ldots,g_{j-2},g_{j-1}g_j,g_{j+1},\ldots,g_i) + (-1)^{i+1} f(g_0,\ldots,g_{i-1}).$$

We will continue to let A denote a G-module throughout the section. We remark that $C^0(G,A)$ is taken simply to be A, as G^0 is a singleton set. The proof of the following is left to the reader.

LEMMA A.2.2. *For any $i \geq 0$, one has $d^{i+1} \circ d^i = 0$.*

REMARK A.2.3. Lemma A.2.2 shows that $C^{\cdot}(G,A) = (C^i(G,A), d^i)$ is a cochain complex.

We consider the cohomology groups of $C^{\cdot}(G,A)$.

DEFINITION A.2.4. Let $i \geq 0$.

i. We set $Z^i(G,A) = \ker d^i$, the group of *i-cocycles* of G with coefficients in A.

ii. We set $B^0(G,A) = 0$ and $B^i(G,A) = \operatorname{im} d^{i-1}$ for $i \geq 1$. We refer to $B^i(G,A)$ as the group of *i-coboundaries* of G with coefficients in A.

We remark that, since $d^i \circ d^{i-1} = 0$ for all $i \geq 1$, we have $B^i(G,A) \subseteq Z^i(G,A)$ for all $i \geq 0$. Hence, we may make the following definition.

DEFINITION A.2.5. We define the *ith cohomology group* of G with coefficients in A to be

$$H^i(G,A) = Z^i(G,A)/B^i(G,A).$$

The cohomology groups measure how far the cochain complex $C^{\cdot}(G,A)$ is from being exact. We give some examples of cohomology groups in low degree.

LEMMA A.2.6.

a. The group $H^0(G,A)$ is equal to A^G, the group of G-invariants of A.

b. We have

$$Z^1(G,A) = \{f\colon G \to A \mid f(gh) = gf(h) + f(g) \text{ for all } g,h \in G\}$$

and $B^1(G,A)$ is the subgroup of $f\colon G \to A$ for which there exists $a \in A$ such that $f(g) = ga - a$ for all $g \in G$.

c. If A is a trivial G-module, then $H^1(G,A) = \operatorname{Hom}(G,A)$.

PROOF. Let $a \in A$. Then $d^0(a)(g) = ga - a$ for $g \in G$, so $\ker d^0 = A^G$. That proves part a, and part b is simply a rewriting of the definitions. Part c follows immediately, as the definition of $Z^1(G,A)$ reduces to $\mathrm{Hom}(G,A)$, and $B^1(G,A)$ is clearly (0), in this case. □

We remark that, as A is abelian, we have $\mathrm{Hom}(G,A) = \mathrm{Hom}(G^{\mathrm{ab}},A)$, where G^{ab} is the maximal abelian quotient of G (i.e., its abelianization). We turn briefly to an even more interesting example.

DEFINITION A.2.7. A *group extension* of G by a G-module A is a short exact sequence of groups

$$0 \to A \xrightarrow{\iota} \mathscr{E} \xrightarrow{\pi} G \to 1$$

such that, choosing any section $s\colon G \to \mathscr{E}$ of π, one has

$$s(g)as(g)^{-1} = g \cdot a$$

for all $g \in G$, $a \in A$. Two such extensions $\mathscr{E} \to \mathscr{E}'$ are said to be equivalent if there is an isomorphism $\theta\colon \mathscr{E} \xrightarrow{\sim} \mathscr{E}'$ fitting into a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & \mathscr{E} & \longrightarrow & G & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle\theta} & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & \mathscr{E}' & \longrightarrow & G & \longrightarrow & 0, \end{array}$$

We denote the set of equivalence classes of such extensions by $\mathscr{E}(G,A)$.

We omit the proof of the following result, as it is not used in the remainder of these notes. We also leave it as an exercise to the reader to define the structure of an abelian group on $\mathscr{E}(G,A)$ which makes the following identification an isomorphism of groups.

THEOREM A.2.8. *The group $H^2(G,A)$ is in canonical bijection with $\mathscr{E}(G,A)$ via the map induced by that taking a 2-cocycle $f\colon G^2 \to A$ to the extension $\mathscr{E}_f = A \times G$ with multiplication given by*

$$(a,g) \cdot (b,h) = (a + gb + f(g,h), gh)$$

This identification takes the identity to the semi-direct product $A \ltimes G$ determined by the action of G on A.

One of the most important uses of cohomology is that it converts short exact sequences of G-modules to long exact sequences of abelian groups. For this, in homological language, we need the fact that $C^i(G,A)$ provides an exact functor in the module A.

LEMMA A.2.9. *If $\alpha\colon A \to B$ is a G-module homomorphism, then for each $i \geq 0$, there is an induced homomorphism of groups*

$$\alpha^i\colon C^i(G,A) \to C^i(G,B)$$

taking f to $\alpha \circ f$ and compatible with the differentials in the sense that

$$d_B^i \circ \alpha^i = \alpha^{i+1} \circ d_A^i.$$

PROOF. We need only check the compatibility. For this, note that

$$d^i(\alpha\circ f)(g_0,g_1,\dots,g_i) = g_0\alpha\circ f(g_1,\dots g_i) + \sum_{j=i}^{i}(-1)^j\alpha\circ f(g_0,\dots,g_{j-2},g_{j-1}g_j,g_{j+1},\dots,g_i)+(-1)^{i+1}\alpha\circ f(g_0,\dots,g_{i-1}) = \alpha(d^i(f)(g_0,g_1,\dots,g_i)),$$

as α is a G-module homomorphism (the fact of which we use only to deal with the first term). □

In other words, α induces a morphism of complexes $\alpha^{\cdot}: C^{\cdot}(G,A)\to C^{\cdot}(G,B)$. As a consequence, one sees easily the following

NOTATION A.2.10. If not helpful for clarity, we will omit the superscripts from the notation in the morphisms of cochain complexes. Similarly, we will consistently omit them in the resulting maps on cohomology, described below.

COROLLARY A.2.11. *A G-module homomorphism $\alpha: A\to B$ induces maps*

$$\alpha^*: H^i(G,A)\to H^i(G,B)$$

on cohomology.

The key fact that we need about the morphism on cochain complexes is the following.

LEMMA A.2.12. *Suppose that*

$$0\to A\xrightarrow{\iota} B\xrightarrow{\pi} C\to 0$$

is a short exact sequence of G-modules. Then the resulting sequence

$$0\to C^i(G,A)\xrightarrow{\iota} C^i(G,B)\xrightarrow{\pi} C^i(G,C)\to 0$$

is exact.

PROOF. Let $f\in C^i(G,A)$, and suppose $\iota\circ f=0$. As ι is injective, this clearly implies that $f=0$, so the map ι^i is injective. As $\pi\circ\iota=0$, the same is true for the maps on cochains. Next, suppose that $f'\in C^i(G,B)$ is such that $\pi\circ f'=0$. Define $f\in C^i(G,A)$ by letting $f(g_1,\dots,g_i)\in A$ be the unique element such that

$$\iota(f(g_1,\dots,g_i)) = f'(g_1,\dots,g_i),$$

which we can do since $\operatorname{im}\iota=\ker\pi$. Thus, $\operatorname{im}\iota^i=\ker\pi^i$. Finally, let $f''\in C^i(G,C)$. As π is surjective, we may define $f'\in C^i(G,B)$ by taking $f'(g_1,\dots,g_i)$ to be any element with

$$\pi(f'(g_1,\dots,g_i)) = f''(g_1,\dots,g_i).$$

We therefore have that π^i is surjective. □

We now prove the main theorem of the section.

THEOREM A.2.13. *Suppose that*

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

is a short exact sequence of G-modules. Then there is a long exact sequence of abelian groups

$$0 \to H^0(G,A) \xrightarrow{\iota^*} H^0(G,B) \xrightarrow{\pi^*} H^0(G,C) \xrightarrow{\delta^0} H^1(G,A) \to \cdots.$$

Moreover, this construction is natural in the short exact sequence in the sense that any morphism

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\iota} & B & \xrightarrow{\pi} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{\iota'} & B' & \xrightarrow{\pi'} & C' & \longrightarrow & 0, \end{array}$$

gives rise to a morphism of long exact sequences, and in particular, a commutative diagram

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & H^i(G,A) & \xrightarrow{\iota^*} & H^i(G,B) & \xrightarrow{\pi^*} & H^i(G,C) & \xrightarrow{\delta^i} & H^{i+1}(G,A) & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle \alpha^*} & & \downarrow{\scriptstyle \beta^*} & & \downarrow{\scriptstyle \gamma^*} & & \downarrow{\scriptstyle \alpha^*} & & \\ \cdots & \longrightarrow & H^i(G,A') & \xrightarrow{(\iota')^*} & H^i(G,B') & \xrightarrow{(\pi')^*} & H^i(G,C') & \xrightarrow{\delta^i} & H^{i+1}(G,A') & \longrightarrow & \cdots. \end{array}$$

PROOF. First consider the diagrams

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C^j(G,A) & \xrightarrow{\iota} & C^j(G,B) & \xrightarrow{\pi} & C^j(G,C) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_A^j} & & \downarrow{\scriptstyle d_B^j} & & \downarrow{\scriptstyle d_C^j} & & \\ 0 & \longrightarrow & C^{j+1}(G,A) & \xrightarrow{\iota} & C^{j+1}(G,B) & \xrightarrow{\pi} & C^{j+1}(G,C) & \longrightarrow & 0 \end{array}$$

for $j \geq 0$. Noting Lemma A.2.12, the exact sequences of cokernels (for $j = i-1$) and kernels (for $j = i+1$) can be placed in a second diagram

$$\begin{array}{ccccccccc} & & \frac{C^i(G,A)}{B^i(G,A)} & \xrightarrow{\iota} & \frac{C^i(G,B)}{B^i(G,B)} & \xrightarrow{\pi} & \frac{C^i(G,C)}{B^i(G,C)} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_A^i} & & \downarrow{\scriptstyle d_B^i} & & \downarrow{\scriptstyle d_C^i} & & \\ 0 & \longrightarrow & Z^{i+1}(G,A) & \xrightarrow{\iota} & Z^{i+1}(G,B) & \xrightarrow{\pi} & Z^{i+1}(G,C) & & \end{array}$$

(recalling that $B^0(G,A) = 0$ for the case $i = 0$), and the snake lemma now provides the exact sequence

$$H^i(G,A) \xrightarrow{\alpha^*} H^i(G,B) \xrightarrow{\beta^*} H^i(G,C) \xrightarrow{\delta^i} H^{i+1}(G,A) \xrightarrow{\alpha^*} H^{i+1}(G,B) \xrightarrow{\beta^*} H^{i+1}(G,C).$$

Splicing these together gives the long exact sequence in cohomology, exactness of

$$0 \to H^0(G,A) \to H^0(G,B)$$

being obvious. We leave naturality of the long exact sequence as an exercise. □

REMARK A.2.14. The maps $\delta^i\colon H^i(G,C) \to H^{i+1}(G,A)$ defined in the proof of theorem A.2.13 are known as *connecting homomorphisms*. Again, we will often omit superscripts and simply refer to δ.

REMARK A.2.15. A sequence of functors that take short exact sequences to long exact sequences (i.e., which also give rise to connecting homomorphisms) and is natural in the sense that every morphism of short exact sequences gives rise to a morphism of long exact sequences is known as a δ-functor. Group cohomology forms a (cohomological) δ-functor that is universal in a sense we omit a discussion of here.

A.3. Group cohomology via projective resolutions

In this section, we assume a bit of homological algebra, and redefine the G-cohomology of A in terms of projective resolutions.

For $i \geq 0$, let G^{i+1} denote the direct product of $i+1$ copies of G. We view $\mathbb{Z}[G^{i+1}]$ as a G-module via the left action

$$g \cdot (g_0, g_1, \ldots, g_i) = (gg_0, gg_1, \ldots, gg_i).$$

We first introduce the standard resolution.

DEFINITION A.3.1. The *(augmented) standard resolution* of $\mathbb{Z}$ by G-modules is the sequence of G-module homomorphisms

$$\cdots \to \mathbb{Z}[G^{i+1}] \xrightarrow{d_i} \mathbb{Z}[G^i] \to \cdots \to \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z},$$

where

$$d_i(g_0, \ldots, g_i) = \sum_{j=0}^{i} (-1)^j (g_0, \ldots, g_{j-1}, g_{j+1}, \ldots, g_i)$$

for each $i \geq 1$, and ε is the augmentation map.

At times, we may use $(g_0, \ldots, \widehat{g_j}, \ldots, g_i) \in G^i$ to denote the i-tuple excluding g_j. To see that this definition is actually reasonable, we need the following lemma.

PROPOSITION A.3.2. *The augmented standard resolution is exact.*

PROOF. In this proof, take $d_0 = \varepsilon$. For each $i \geq 0$, compute

$$d_i \circ d_{i+1}(g_0, \ldots, g_{i+1}) = \sum_{j=0}^{i+1} \sum_{\substack{k=0 \\ k \neq j}}^{i+1} (-1)^{j+k-s(j,k)} (g_0, \ldots, \widehat{g_j}, \ldots, \widehat{g_k}, \ldots, g_{i+1}),$$

where $s(j,k)$ is 0 if $k < j$ and 1 if $k > j$. Each possible $(i-1)$-tuple appears twice in the sum, with opposite sign. Therefore, we have $d_i \circ d_{i+1} = 0$.

Next, define $\theta_i\colon \mathbb{Z}[G^i] \to \mathbb{Z}[G^{i+1}]$ by

$$\theta_i(g_1, \ldots, g_i) = (1, g_1, \ldots, g_i).$$

Then

$$\begin{aligned} d_i \circ \theta_i(g_0,\dots,g_i) &= (g_0,\dots,g_i) - \sum_{j=0}^{i} (-1)^j (1,g_0,\dots,\widehat{g_j},\dots,g_i) \\ &= (g_0,\dots,g_i) - \theta_{i-1} \circ d_{i-1}(g_0,\dots,g_i), \end{aligned}$$

which is to say that

$$d_i \circ \theta_i + \theta_{i-1} \circ d_{i-1} = \mathrm{id}_{\mathbb{Z}[G^i]}.$$

If $\alpha \in \ker d_{i-1}$ for $i \geq 1$, it then follows that $d_i(\theta_i(\alpha)) = \alpha$, so $\alpha \in \mathrm{im}\, d_i$. □

For a G-module A, we wish to consider the following complex

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],A) \to \cdots \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}],A) \xrightarrow{D^i} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+2}],A) \to \cdots. \tag{A.3.1}$$

Here, we define $D^i = D^i_A$ by $D^i(\varphi) = \varphi \circ d_{i+1}$. We compare this with the complex of cochains for G.

THEOREM A.3.3. *The maps*

$$\psi^i \colon \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}],A) \to C^i(G,A)$$

defined by

$$\psi^i(\varphi)(g_1,\dots,g_i) = \varphi(1,g_1,g_1g_2,\dots,g_1g_2\cdots g_i)$$

are isomorphisms for all $i \geq 0$. This provides isomorphisms of complexes in the sense that $\psi^{i+1} \circ D^i = d^i \circ \psi^i$ for all $i \geq 0$. Moreover, these isomorphisms are natural in the G-module A.

PROOF. If $\psi^i(\varphi) = 0$, then $\varphi(1,g_1,g_1g_2,\dots,g_1g_2\cdots g_i) = 0$ for all $g_1,\dots,g_i \in G$. Let $h_0,\dots,h_i \in G$, and define $g_j = h_{j-1}^{-1}h_j$ for all $1 \leq j \leq i$. We then have

$$\varphi(h_0,h_1,\dots,h_i) = h_0\varphi(1,h_0^{-1}h_1,\dots,h_0^{-1}h_i) = h_0\varphi(1,g_1,\dots,g_1\cdots g_i) = 0.$$

Therefore, ψ^i is injective. On the other hand, if $f \in C^i(G,A)$, then defining

$$\varphi(h_0,h_1,\dots,h_i) = h_0 f(h_0^{-1}h_1,\dots,h_{i-1}^{-1}h_i),$$

we have

$$\varphi(gh_0,gh_1,\dots,gh_i) = gh_0 f((gh_0)^{-1}gh_1,\dots,(gh_{i-1})^{-1}gh_i) = g\varphi(h_0,h_1,\dots,h_i)$$

and $\psi^i(\varphi) = f$. Therefore, ψ^i is an isomorphism of groups.

That $\psi^{\cdot}$ forms a map of complexes is shown in the following computation:

$$\begin{aligned} \psi^{i+1}(D^i(\varphi))(g_1,\dots,g_{i+1}) &= D^i(\varphi)(1,g_1,\dots,g_1\cdots g_{i+1}) \\ &= \varphi \circ d_{i+1}(1,g_1,\dots,g_1\cdots g_{i+1}) \\ &= \sum_{j=0}^{i+1} (-1)^j \varphi(1,g_1,\dots,\widehat{g_1\cdots g_j},\dots,g_1\cdots g_{i+1}). \end{aligned}$$

The latter term equals

$$g_1\psi^i(\varphi)(g_2,\dots,g_{i+1})+\sum_{j=1}^{i}(-1)^j\psi^i(\varphi)(g_1,\dots,g_{j-1},g_jg_{j+1},g_{j+2},\dots,g_{i+1})$$
$$+(-1)^{i+1}\psi^i(\varphi)(g_1,\dots,g_i),$$

which is $d^i(\psi^i(\varphi))$.

Finally, suppose that $\alpha\colon A\to B$ is a G-module homomorphism. We then have

$$\alpha\circ\psi^i(\varphi)(g_1,\dots,g_i)=\alpha\circ\varphi(1,g_1,\dots,g_1\cdots g_i)=\psi^i(\alpha\circ\varphi)(g_1,\dots,g_i),$$

hence the desired naturality. □

COROLLARY A.3.4. *The ith cohomology group of the complex* $(\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}],A),D_A^i)$ *is naturally isomorphic to* $H^i(G,A)$.

In fact, the standard resolution is a projective resolution of $\mathbb{Z}$, as is a consequence of the following lemma and the fact that every free module is projective.

LEMMA A.3.5. *The G-module* $\mathbb{Z}[G^{i+1}]$ *is free.*

PROOF. In fact, we have

$$\mathbb{Z}[G^{i+1}]\cong\bigoplus_{(g_1,\dots,g_i)\in G^i}\mathbb{Z}[G](1,g_1,\dots,g_i),$$

and the submodule generated by $(1,g_1,\dots,g_i)$ is clearly free. □

REMARKS A.3.6.

a. Lemma A.3.5 implies that the standard resolution provides a projective resolution of $\mathbb{Z}$. It follows that

$$H^i(G,A)\cong\mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z},A)$$

for any G-module A. Moreover, if $P_\cdot\to\mathbb{Z}\to 0$ is any projective resolution of $\mathbb{Z}$ by G-modules, we have that $H^i(G,A)$ is the ith cohomology group of the complex $\mathrm{Hom}_{\mathbb{Z}[G]}(P_\cdot,A)$.

b. By definition, $\mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z},A)$ is the ith right derived functor of the functor that takes the value $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z},A)$ on A. Note that $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z},A)\cong A^G$, the module of G-invariants. Therefore, if $0\to A\to I^\cdot$ is any injective $\mathbb{Z}[G]$-resolution of A, then $H^i(G,A)$ is the ith cohomology group in the sequence

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

A.4. Homology of groups

In this section, we consider a close relative of group cohomology, known as group homology. Note first that $\mathbb{Z}[G^{i+1}]$ is also a right module over $\mathbb{Z}[G]$ by the diagonal right multiplication by an element of G. Up to isomorphism of G-modules, this is the same as taking the diagonal left multiplication of $\mathbb{Z}[G^{i+1}]$ by the inverse of an element of G.

DEFINITION A.4.1. The ith *homology group* $H_i(G,A)$ of a group G with coefficients in a G-module A is defined to be the ith homology group $H_i(G,A) = \ker d_i / \operatorname{im} d_{i+1}$ in the complex

$$\cdots \to \mathbb{Z}[G^3] \otimes_{\mathbb{Z}[G]} A \xrightarrow{d_2} \mathbb{Z}[G^2] \otimes_{\mathbb{Z}[G]} A \xrightarrow{d_1} \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \xrightarrow{d_0} 0$$

induced by the standard resolution.

We note that if $f : A \to B$ is a G-module homomorphism, then there are induced maps $f_* : H_i(G,A) \to H_i(G,B)$ for each $i \geq 0$.

REMARK A.4.2. It follows from Definition A.4.1 that $H_i(G,A) \cong \operatorname{Tor}^i_{\mathbb{Z}[G]}(\mathbb{Z},A)$ for every $i \geq 0$, and that $H_i(G,A)$ may be calculated by taking the homology of $P_\cdot \otimes_{\mathbb{Z}[G]} A$, where $P_\cdot$ is any projective $\mathbb{Z}[G]$-resolution of $\mathbb{Z}$. Here, we view P_i as a right G-module via the action $x \cdot g = g^{-1}x$ for $g \in G$ and $x \in X$.

As a first example, we have

LEMMA A.4.3. *We have natural isomorphisms $H_0(G,A) \cong A_G$ for every G-module A.*

PROOF. Note first that $\mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \cong A$, and the map d_1 under this identification is given by

$$d_1((g_0,g_1) \otimes a) = (g_0 - g_1)a.$$

Hence, the image of d_1 is $I_G A$, and the result follows. □

As $A_G \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$, we have in particular that $H_i(G,A)$ is the ith left derived functor of A_G. As with cohomology, we therefore have in particular that homology carries short exact sequences to long exact sequences, as we now spell out.

THEOREM A.4.4. *Suppose that*

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

is a short exact sequence of G-modules. Then there are connecting homomorphisms $\delta_* : H_i(G,C) \to H_{i-1}(G,A)$ and a long exact sequence of abelian groups

$$\cdots \to H_1(G,C) \xrightarrow{\delta} H_0(G,A) \xrightarrow{\iota_*} H_0(G,B) \xrightarrow{\pi_*} H_0(G,C) \to 0.$$

Moreover, this construction is natural in the short exact sequence in the sense that any morphism of short exact sequences gives rise to a morphism of long exact sequences.

The following result computes the homology group $H_1(G,\mathbb{Z})$, where $\mathbb{Z}$ has the trivial G-action.

PROPOSITION A.4.5. *There are canonical isomorphisms $H_1(G,\mathbb{Z}) \cong I_G/I_G^2 \cong G^{\mathrm{ab}}$, where G^{ab} denotes the abelianization of G, the latter taking the coset of $g-1$ to the coset of $g \in G$.*

PROOF. Since $\mathbb{Z}[G]$ is $\mathbb{Z}[G]$-projective, we have $H_1(G,\mathbb{Z}[G]) = 0$, and hence our long exact sequence in homology has the form

$$0 \to H_1(G,\mathbb{Z}) \to H_0(G,I_G) \to H_0(G,\mathbb{Z}[G]) \to H_0(G,\mathbb{Z}) \to 0.$$

Note that $H_0(G,I_G) \cong I_G/I_G^2$ and $H_0(G,\mathbb{Z}[G]) \cong \mathbb{Z}[G]/I_G \cong \mathbb{Z}$ via the augmentation map. Since $H_0(G,\mathbb{Z}) \cong \mathbb{Z}$ and any surjective map $\mathbb{Z} \to \mathbb{Z}$ (in this case the identity) is an isomorphism, we obtain the first isomorphism of the proposition.

For the second isomorphism, let us define maps $\phi\colon G^{\mathrm{ab}} \to I_G/I_G^2$ and $\psi\colon I_G/I_G^2 \to G^{\mathrm{ab}}$. For $g \in G$, we set

$$\phi(g[G,G]) = (g-1) + I_G^2,$$

where $[G,G]$ denotes the commutator subgroup of G. To see that this is a homomorphism on G, hence on G^{ab}, note that

$$(gh-1) + I_G^2 = (g-1) + (h-1) + (g-1)(h-1) + I_G^2 = (g-1) + (h-1) + I_G^2$$

for $g,h \in G$.

Next, define ψ on $\alpha = \sum_{g\in G} a_g g \in I_G$ by

$$\psi(\alpha + I_G^2) = \prod_{g\in G} g^{a_g}[G,G].$$

The order of the product doesn't matter as G^{ab} is abelian, and ψ is then a homomorphism if well-defined. It suffices for the latter to check that the recipe defining ψ takes the generators $(g-1)(h-1)$ of I_G^2 for $g,h \in G$ to the trivial coset, but this follows as $(g-1)(h-1) = gh - g - h + 1$, and for instance, we have

$$gh \cdot g^{-1} \cdot h^{-1} \in [G,G].$$

Finally, we check that the two homomorphisms are inverse to each other. We have

$$\phi(\psi(\alpha + I_G^2)) = \sum_{g\in G} a_g(g-1) + I_G^2 = \alpha + I_G^2$$

since $\alpha \in I_G$ implies $\sum_{g\in G} a_g = 0$, and

$$\psi(\phi(g[G,G])) = \phi((g-1) + I_G^2) = g[G,G].$$

□

A.5. Induced modules

DEFINITION A.5.1. Let H be a subgroup of G, and suppose that B is a $\mathbb{Z}[H]$-module. We set

$$\mathrm{Ind}_H^G(B) = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} B \quad \text{and} \quad \mathrm{CoInd}_H^G(B) = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], B).$$

We give these G-actions by

$$g \cdot (\alpha \otimes b) = (g\alpha) \otimes b \quad \text{and} \quad (g \cdot \varphi)(\alpha) = \varphi(\alpha \cdot g).$$

We say that the resulting modules are *induced* and *coinduced*, respectively, from H to G.

REMARK A.5.2. What we refer to as a "coinduced" module is often actually referred to as an "induced" module.

We may use these modules to interpret H-cohomology groups as G-cohomology groups.

THEOREM A.5.3 (Shapiro's Lemma). *For each $i \geq 0$, we have canonical isomorphisms*

$$H_i(G, \mathrm{Ind}_H^G(B)) \cong H_i(H, B) \quad \text{and} \quad H^i(G, \mathrm{CoInd}_H^G(B)) \cong H^i(H, B)$$

that provide natural isomorphisms of δ-functors.

PROOF. Let $P_\cdot$ be the standard resolution of $\mathbb{Z}$ by G-modules. Define

$$\psi_i \colon \mathrm{Hom}_{\mathbb{Z}[G]}(P_i, \mathrm{CoInd}_H^G(B)) \to \mathrm{Hom}_{\mathbb{Z}[H]}(P_i, B)$$

by $\psi_i(\theta)(x) = \theta(x)(1)$. If $\theta \in \ker \psi_i$, then

$$\theta(x)(g) = (g \cdot \theta(x))(1) = \theta(gx)(1) = 0.$$

for all $x \in P_i$ and $g \in G$, so $\theta = 0$. Conversely, if $\varphi \in \mathrm{Hom}_{\mathbb{Z}[H]}(P_i, B)$, then define θ by $\theta(x)(g) = \varphi(gx)$, and we have $\psi_i(\theta) = \varphi$.

As for the induced case, note that associativity of tensor products yields

$$P_i \otimes_{\mathbb{Z}[G]} (\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} B) \cong P_i \otimes_{\mathbb{Z}[H]} B,$$

and $P_i = \mathbb{Z}[G^{i+1}]$ is free as a left H-module, hence projective. (We leave it to the reader to check that usual $\otimes$-Hom adjunction can be similarly used to give a shorter proof of the result for cohomology.) □

In fact, if H is of finite index in G, the notions of induced and coinduced from H to G coincide.

PROPOSITION A.5.4. *Suppose that H is a subgroup of finite index in G and B is a H-module. Then we have a canonical isomorphism of G-modules*

$$\chi \colon \mathrm{CoInd}_H^G(B) \xrightarrow{\sim} \mathrm{Ind}_H^G(B), \qquad \chi(\varphi) = \sum_{\bar{g} \in H\backslash G} g^{-1} \otimes \varphi(g),$$

where for each $\bar{g} \in H\backslash G$, the element $g \in G$ is an arbitrary choice of representative of $\bar{g}$.

PROOF. First, we note that χ is a well-defined map, as

$$(hg)^{-1} \otimes \varphi(hg) = g^{-1}h^{-1} \otimes h\varphi(g) = g \otimes \varphi(g)$$

for $\varphi \in \mathrm{CoInd}_H^G(B)$, $h \in H$, and $g \in G$. Next, we see that χ is a G-module homomorphism, as

$$\chi(g'\varphi) = \sum_{\bar{g} \in H\backslash G} g^{-1} \otimes \varphi(gg') = g' \sum_{\bar{g} \in H\backslash G} (gg')^{-1} \otimes \varphi(gg') = g'\chi(\varphi)$$

for $g' \in G$. As the coset representatives form a basis for $\mathbb{Z}[G]$ as a free $\mathbb{Z}[H]$-module, we may define an inverse to χ that maps

$$\sum_{\bar{g} \in H\backslash G} g^{-1} \otimes b_g \in \mathrm{Ind}_H^G(B)$$

to the unique $\mathbb{Z}[H]$-linear map φ that takes the value b_g on g for the chosen representative of $\bar{g} \in H\backslash G$. □

In the special case of the trivial subgroup, we make the following definition.

DEFINITION A.5.5. We say that G-modules of the form

$$\mathrm{Ind}^G(X) = \mathbb{Z}[G] \otimes_{\mathbb{Z}} X \quad \text{and} \quad \mathrm{CoInd}^G(X) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X),$$

where X is an abelian group, are *induced* and *coinduced* G-modules, respectively.

REMARK A.5.6. Note that Proposition A.5.4 implies that the notions of induced and coinduced modules coincide for finite groups G. On the other hand, for infinite groups, $\mathrm{CoInd}^G(X)$ will never be finitely generated over $\mathbb{Z}[G]$ for nontrivial X, while $\mathrm{Ind}^G(X)$ will be for any finitely generated abelian group X.

THEOREM A.5.7. *Suppose that A is an induced (resp., coinduced) G-module. Then we have $H_i(G,A) = 0$ (resp., $H^i(G,A) = 0$) for all $i \geq 1$.*

PROOF. Let X be an abelian group. By Shapiro's Lemma, we have

$$H_i(G, \mathrm{Ind}^G(X)) = H_i(\{1\}, X)$$

for $i \geq 1$. Since $\mathbb{Z}$ has a projective $\mathbb{Z}$-resolution by itself, the latter groups are 0. The proof for cohomology is essentially identical. □

DEFINITION A.5.8. A G-module A such that $H^i(G,A) = 0$ for all $i \geq 1$ is called *G-acyclic*.

We show that we may construct induced and coinduced G-modules starting from abelian groups that are already equipped with a G-action.

REMARK A.5.9. Suppose that A and B are G-modules. We give $\mathrm{Hom}_{\mathbb{Z}}(A,B)$ and $A \otimes_{\mathbb{Z}} B$ actions of G by

$$(g \cdot \varphi)(a) = g\varphi(g^{-1}a) \quad \text{and} \quad g \cdot (a \otimes b) = ga \otimes gb,$$

respectively.

LEMMA A.5.10. *Let A be a G-module, and let A° be its underlying abelian group. Then*

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G],A) \cong \mathrm{CoInd}^G(A^\circ) \quad \text{and} \quad \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \cong \mathrm{Ind}^G(A^\circ).$$

PROOF. We define

$$\kappa\colon \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G],A) \to \mathrm{CoInd}^G(A^\circ), \qquad \kappa(\varphi)(g) = g \cdot \varphi(g^{-1}).$$

For $g,k \in G$, we then have

$$(k \cdot \kappa(\varphi))(g) = \kappa(\varphi)(gk) = gk \cdot \varphi(k^{-1}g^{-1}) = g \cdot (k \cdot \varphi)(g^{-1}) = \kappa(k \cdot \varphi)(g),$$

so κ is a G-module homomorphism. Note that κ is also self-inverse on the underlying set of both groups, so is an isomorphism. In the induced case, we define

$$\nu\colon \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \to \mathrm{Ind}^G(A^\circ), \qquad \nu(g \otimes a) = g \otimes g^{-1}a.$$

For $g,k \in G$, we now have

$$k \cdot \nu(g \otimes a) = (kg) \otimes g^{-1}a = \nu(kg \otimes ka) = \nu(k \cdot (g \otimes a)),$$

so ν is a G-module isomorphism with inverse $\nu^{-1}(g \otimes a) = g \otimes ga$. □

REMARK A.5.11. Noting the lemma, we will simply refer to $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G],A)$ as $\mathrm{CoInd}^G(A)$ and $\mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ as $\mathrm{Ind}^G(A)$.

A.6. Tate cohomology

We suppose in this section that G is a finite group. In this case, recall that we have the norm element $N_G \in \mathbb{Z}[G]$, which defines by left multiplication a map $N_G\colon A \to A$ on any G-module A. Its image $N_G A$ is the *group of G-norms* of A.

LEMMA A.6.1. *The norm element induces a map $\bar{N}_G\colon A_G \to A^G$.*

PROOF. We have $N_G((g-1)a) = 0$ for any $g \in G$ and $a \in A$, so the map factors through A_G, and clearly $\mathrm{im} N_G \subseteq A^G$. □

DEFINITION A.6.2. We let $\hat{H}^0(G,A)$ (resp., $\hat{H}_0(G,A)$) denote the cokernel (resp., kernel) of the map in Lemma A.6.1. In other words,

$$\hat{H}^0(G,A) = A^G/N_G A \quad \text{and} \quad \hat{H}_0(G,A) = {}_N A/I_G A,$$

where ${}_N A$ denotes the kernel of the left multiplication by N_G on A.

EXAMPLE A.6.3. Consider the case that $A = \mathbb{Z}$, where $\mathbb{Z}$ is endowed with a trivial action of G. Since $N_G\colon \mathbb{Z} \to \mathbb{Z}$ is just the multiplication by $|G|$ map, we have that $\hat{H}^0(G,\mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$ and $\hat{H}_0(G,\mathbb{Z}) = 0$.

REMARK A.6.4. In general, when we take cohomology with coefficients in a group, like $\mathbb{Z}$ or $\mathbb{Q}$, with no specified action of the group G, the action is taken to be trivial.

The Tate cohomology groups are an amalgamation of the homology groups and cohomology groups of G, with the homology groups placed in negative degrees.

DEFINITION A.6.5. Let G be a finite group and A a G-module. For any $i \in \mathbb{Z}$, we define the *ith Tate cohomology group* by

$$\hat{H}^i(G,A) = \begin{cases} H_{-i-1}(G,A) & \text{if } i \leq -2 \\ \hat{H}_0(G,A) & \text{if } i = -1 \\ \hat{H}^0(G,A) & \text{if } i = 0 \\ H^i(G,A) & \text{if } i \geq 1. \end{cases}$$

We have modified the zeroth homology and cohomology groups in defining Tate cohomology so that we obtain long exact sequences from short exact sequences as before, but extending infinitely in both directions, as we shall now see.

THEOREM A.6.6 (Tate). *Suppose that*

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

is a short exact sequence of G-modules. Then there is a long exact sequence of abelian groups

$$\cdots \to \hat{H}^i(G,A) \xrightarrow{\iota} \hat{H}^i(G,B) \xrightarrow{\pi} \hat{H}^i(G,C) \xrightarrow{\delta} \hat{H}^{i+1}(G,A) \to \cdots.$$

Moreover, this construction is natural in the short exact sequence in the sense that any morphism of short exact sequences gives rise to a morphism of long exact sequences.

PROOF. The first part follows immediately from applying the snake lemma to the following diagram, which in particular defines the map δ on $\hat{H}^{-1}(G,C)$:

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & H_1(G,C) & \xrightarrow{\delta} & H_0(G,A) & \xrightarrow{\iota_*} & H_0(G,B) & \xrightarrow{\pi_*} & H_0(G,C) & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \bar{N}_G} & & \downarrow{\scriptstyle \bar{N}_G} & & \downarrow{\scriptstyle \bar{N}_G} & & \\ & & 0 & \longrightarrow & H^0(G,A) & \xrightarrow{\iota_*} & H^0(G,B) & \xrightarrow{\pi_*} & H^0(G,C) & \xrightarrow{\delta} & H^1(G,A) \longrightarrow \cdots, \end{array}$$

and the second part is easily checked. □

Tate cohomology groups have the interesting property that they vanish entirely on induced modules.

PROPOSITION A.6.7. *Suppose that A is an induced G-module. Then $\hat{H}^i(G,A) = 0$ for all $i \in \mathbb{Z}$.*

PROOF. By Theorem A.5.7 and Proposition A.5.4, it suffices to check this for $i = -1$ and $i = 0$. Let X be an abelian group. Since $\mathbb{Z}[G]^G = N_G\mathbb{Z}[G]$, we have

$$H^0(G, \mathrm{Ind}^G(X)) = N_G\mathbb{Z}[G] \otimes_{\mathbb{Z}} X,$$

so $\hat{H}^0(G, \mathrm{Ind}^G(X)) = 0$ by definition. We also have that

$$H_0(G, \mathrm{Ind}^G(X)) = (\mathbb{Z}[G] \otimes_{\mathbb{Z}} X)_G \cong \mathbb{Z} \otimes_{\mathbb{Z}} X \cong X. \tag{A.6.1}$$

Let $\alpha = \sum_{g\in G}(g \otimes x_g)$ be an element of $\mathrm{Ind}^G(X)$. Then

$$N_G\alpha = N_G \otimes \sum_{g\in G} x_g$$

is trivial if and only if $\sum_{g\in G} x_g = 0$, which by the identification in (A.6.1) is to say that α has trivial image in $H_0(G, \mathrm{Ind}^G(X))$. Hence $\hat{H}_0(G, \mathrm{Ind}^G(X)) = 0$ as well. □

The Tate cohomology groups can also be computed via a doubly infinite resolution of G-modules. The proof of this is rather involved and requires some preparation.

LEMMA A.6.8. *Let X be a G-module that is free of finite rank over $\mathbb{Z}$, and let A be any G-module. Then the map*

$$\nu\colon X \otimes_{\mathbb{Z}} A \to \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}), A), \qquad \nu(x \otimes a)(\varphi) = \varphi(x)a$$

is an isomorphism of G-modules.

PROOF. We note that

$$\nu(g \cdot (x \otimes a))(\varphi) = \varphi(gx)ga,$$

while

$$(g \cdot \nu(x \otimes a))(\varphi) = g\nu(x \otimes a)(g^{-1}\varphi) = (g^{-1}\varphi)(x)ga = \varphi(gx)ga,$$

so ν is a homomorphism of G-modules.

Let $x_1, \ldots, x_m$ be any $\mathbb{Z}$-basis of X, and let $x_1^*, \ldots, x_m^*$ be the dual basis of $\mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z})$ such that $x_i^*(x_j) = \delta_{ij}$ for $1 \le i, j \le m$. We define

$$\omega\colon \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}), A) \to X \otimes_{\mathbb{Z}} A, \qquad \omega(\psi) = \sum_{i=1}^{m} x_i \otimes \psi(x_i^*).$$

Then

$$(\nu \circ \omega)(\psi)(\varphi) = \nu\left(\sum_{i=1}^{m} x_i \otimes \psi(x_i^*)\right)(\varphi) = \sum_{i=1}^{m} \varphi(x_i)\psi(x_i^*) = \psi\left(\sum_{i=1}^{m} \varphi(x_i)x_i^*\right) = \psi(\varphi).$$

On the other hand,

$$(\omega \circ \nu)(x \otimes a) = \sum_{i=1}^{m} x_i \otimes x_i^*(x)a = \sum_{i=1}^{m} x_i^*(x)x_i \otimes a = x \otimes a.$$

Hence, ν is an isomorphism. □

LEMMA A.6.9. *Let X and A be G-modules, and endow X with a right G-action by $x \cdot g = g^{-1}x$. Then we have a canonical isomorphism*

$$X \otimes_{\mathbb{Z}[G]} A \xrightarrow{\sim} (X \otimes_{\mathbb{Z}} A)_G$$

induced by the identity on $X \otimes_{\mathbb{Z}} A$.

PROOF. First, note that $X \otimes_{\mathbb{Z}[G]} A$ is a quotient of the G-module $X \otimes_{\mathbb{Z}} A$, which is endowed the diagonal left G-action. By definition of the tensor product over $\mathbb{Z}[G]$, we have

$$g^{-1}x \otimes a = x \cdot g \otimes a = x \otimes ga,$$

so G acts trivially on $X \otimes_{\mathbb{Z}[G]} A$, and hence the latter group is a quotient of $(X \otimes_{\mathbb{Z}} A)_G$. On the other hand, the $\mathbb{Z}$-bilinear map

$$X \times A \to (X \otimes_{\mathbb{Z}} A)_G, \qquad (x,a) \mapsto x \otimes a$$

is $\mathbb{Z}[G]$-balanced, hence induces a map on the tensor product inverse to the above-described quotient map. □

We are now ready to prove the theorem.

THEOREM A.6.10. *Let $P_\cdot \xrightarrow{\alpha} \mathbb{Z}$ be a projective resolution by G-modules of finite $\mathbb{Z}$-rank, and consider the $\mathbb{Z}$-dual $\mathbb{Z} \xrightarrow{\hat{\alpha}} P_*^\cdot$, where $P_*^i = \mathrm{Hom}_{\mathbb{Z}}(P_i, \mathbb{Z})$ for $i \geq 0$ and G acts on P_*^i by $(g \cdot \varphi)(x) = \varphi(g^{-1}x)$. Let $Q_\cdot$ be the exact chain complex*

$$\cdots \to P_1 \to P_0 \xrightarrow{\hat{\alpha} \circ \alpha} P_*^0 \to P_*^1 \to \cdots,$$

where P_0 occurs in degree 0. (That is, we set $Q_i = P_i$ for $i \geq 0$ and $Q_i = P_*^{-1-i}$ for $i < 0$.) For any G-module A, the Tate cohomology group $\hat{H}^i(G,A)$ is the ith cohomology group of the cochain complex $C^\cdot = \mathrm{Hom}_{\mathbb{Z}[G]}(Q_\cdot, A)$.

PROOF. As P_i is projective over $\mathbb{Z}[G]$, it is in particular $\mathbb{Z}$-free, so the $\mathbb{Z}$-dual sequence $\mathbb{Z} \to P_*^\cdot$ is still exact. Let us denote the ith differential on P_i by d_i and its $\mathbb{Z}$-dual by $\hat{d}^i$. We check exactness at Q_0 and Q_{-1}. Let $\beta = \hat{\alpha} \circ \alpha$. By definition, $\mathrm{im}\, d_1 = \ker \alpha$, and as $\hat{\alpha}$ is injective, we have $\mathrm{im}\, d_1 = \ker \beta$. Similarly, we have $\ker \hat{d}^0 = \mathrm{im}\, \hat{\alpha}$, and as α is surjective, we have $\ker \hat{d}^0 = \mathrm{im}\, \beta$. Therefore, $Q_\cdot$ is exact.

That $\mathrm{Hom}_{\mathbb{Z}[G]}(Q_\cdot, A)$ computes the Tate cohomology groups $\hat{H}^i(G,A)$ follows immediately from the definition for $i \geq 1$. By Lemma A.6.9, we have an isomorphism

$$P_i \otimes_{\mathbb{Z}[G]} A \xrightarrow{\sim} (P_i \otimes_{\mathbb{Z}} A)_G.$$

By Proposition A.6.7 and Lemma A.5.10, we have that

$$(P_i \otimes_{\mathbb{Z}} A)_G \xrightarrow{\bar{N}_G} (P_i \otimes_{\mathbb{Z}} A)^G$$

is an isomorphism as well, and following this by the restriction

$$(P_i \otimes_{\mathbb{Z}} A)^G \to \mathrm{Hom}_{\mathbb{Z}}(P^i_*, A)^G = \mathrm{Hom}_{\mathbb{Z}[G]}(P^i_*, A)$$

of the map ν of Lemma A.6.8, we obtain in summary an isomorphism

$$\chi_i \colon P_i \otimes_{\mathbb{Z}[G]} A \to \mathrm{Hom}_{\mathbb{Z}[G]}(P^i_*, A).$$

Next, we check that the maps ν of Lemma A.6.8 commute with the differentials on the complexes $P_\cdot \otimes_{\mathbb{Z}} A$ and $\mathrm{Hom}_{\mathbb{Z}}(P^\cdot_*, A)$, the former of which are just the tensor products of the differentials d_i on the P_i with the identity (then also denoted d_i), and the latter of which are double duals $\tilde{d}_i$ of the d_i, i.e., which satisfy

$$\tilde{d}_i(\psi)(\varphi) = \psi(\varphi \circ d_i),$$

for $\psi \in \mathrm{Hom}_{\mathbb{Z}}(P^i_*, A)$ and $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(P_{i-1}, \mathbb{Z})$. We have

$$(\nu \circ d_i)(x \otimes a)(\varphi) = \nu(d_i(x) \otimes a)(\varphi) = \varphi(d_i(x))a.$$

On the other hand, we have

$$(\tilde{d}_i \circ \nu)(x \otimes a)(\varphi) = \tilde{d}_i(\nu(x \otimes a))(\varphi) = \nu(x \otimes a)(\varphi \circ d_i) = \varphi(d_i(x))a,$$

as desired. Moreover, the d_i commute with $\bar{N}_G$ on $(P_i \otimes_{\mathbb{Z}} A)_G$, being that they are G-module maps. Hence, the maps χ_i for all i together provide an isomorphism of complexes. In particular, the ith cohomology group of $\mathrm{Hom}_{\mathbb{Z}[G]}(Q_\cdot, A)$ is $\hat{H}^i(G, A)$ for all $i \leq -2$, and we already knew this for all $i \geq 1$.

It remains to consider the cases $i = 0, -1$. We need to compute the cohomology of

$$P_1 \otimes_{\mathbb{Z}[G]} A \to P_0 \otimes_{\mathbb{Z}[G]} A \xrightarrow{\tau} \mathrm{Hom}_{\mathbb{Z}[G]}(P_0, A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, A) \tag{A.6.2}$$

in the middle two degrees, and

$$\tau(x \otimes a)(y) = (\chi_0(x \otimes a) \circ \hat{\alpha} \circ \alpha)(y) = \sum_{g \in G} (\hat{\alpha} \circ \alpha)(y)(gx)ga = \sum_{g \in G} \alpha(y)\alpha(x)ga,$$

noting that $\alpha(gx) = \alpha(x)$ for every $g \in G$ and $\hat{\alpha}(n)(x) = n\alpha(x)$ for every $n \in \mathbb{Z}$. On the other hand, viewing α and $\hat{\alpha}$ as inducing maps

$$\lambda \colon P_0 \otimes_{\mathbb{Z}[G]} A \to A_G \quad \text{and} \quad \hat{\lambda} \colon A^G \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_0, A),$$

respectively, we have

$$\begin{aligned}(\hat{\lambda} \circ \bar{N}_G \circ \lambda)(x \otimes a)(y) = \hat{\lambda}(\bar{N}_G(\alpha(x)a))(y) = \hat{\lambda}\Big(\sum_{g \in G} \alpha(x)ga\Big)(y) \\ = \sum_{g \in G} \hat{\alpha}(\alpha(x))(y)ga = \sum_{g \in G} \alpha(x)\alpha(y)ga.\end{aligned}$$

In other words, we have $\tau = \hat{\lambda} \circ \bar{N}_G \circ \lambda$. As the cokernel of the first map in (A.6.2) is $H_0(G, A) = A_G$ and the kernel of the last is $H^0(G, A) = A^G$, with these identifications given by the maps λ and

$\hat{\lambda}$ respectively, we have that the complex given by $A_G \xrightarrow{\bar{N}_G} A^G$ in degrees -1 and 0 computes the cohomology groups in question, as desired. □

As what is in essence a corollary, we have the following version of Shapiro's lemma.

THEOREM A.6.11. *Let G be a finite group, let H be a subgroup, and let B be an H-module. Then for every $i \in \mathbb{Z}$, we have canonical isomorphisms*

$$\hat{H}^i(G, \mathrm{CoInd}_H^G(B)) \cong \hat{H}^i(H, B)$$

that together provide natural isomorphisms of δ-functors.

PROOF. The proof is nearly identical to that of Shapiro's lemma for cohomology groups. That is, we may simply use the isomorphisms induced by

$$\psi_i \colon \mathrm{Hom}_{\mathbb{Z}[G]}(Q_i, \mathrm{CoInd}_H^G(B)) \to \mathrm{Hom}_{\mathbb{Z}[H]}(Q_i, B)$$

by $\psi_i(\theta)(x) = \theta(x)(1)$, for $Q_\cdot$ the doubly infinite resolution of $\mathbb{Z}$ for G of Theorem A.6.10. □

A.7. Dimension shifting

One useful technique in group cohomology is that of dimension shifting. The key idea here is to use the acyclicity of coinduced modules to obtain isomorphisms among cohomology groups.

To describe this technique, note that we have a short exact sequence

$$0 \to A \xrightarrow{\iota} \mathrm{CoInd}^G(A) \to A^* \to 0, \tag{A.7.1}$$

where ι is defined by $\iota(a)(g) = a$ for $a \in A$ and $g \in G$, and A^* is defined to be the cokernel of ι. We also have a short exact sequence

$$0 \to A_* \to \mathrm{Ind}^G(A) \xrightarrow{\pi} A \to 0, \tag{A.7.2}$$

where π is defined by $\pi(g \otimes a) = a$ for $a \in A$ and $g \in G$, and A_* is defined to be the kernel of π.

REMARK A.7.1. If we view A as $\mathbb{Z} \otimes_{\mathbb{Z}} A$, we see by the freeness of $\mathbb{Z}$ as a $\mathbb{Z}$-module and the definition of $\mathrm{Ind}^G(A)$ that $A_* \cong I_G \otimes_{\mathbb{Z}} A$ with a diagonal action of G. Moreover, viewing A as $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A)$, we see that $A^* \cong \mathrm{Hom}_{\mathbb{Z}}(I_G, A)$.

PROPOSITION A.7.2. *With the notation as above, we have*

$$H^{i+1}(G, A) \cong H^i(G, A^*) \quad \text{and} \quad H_{i+1}(G, A) \cong H_i(G, A_*)$$

for all $i \geq 1$.

PROOF. By Lemma A.5.10, we know that $\mathrm{CoInd}^G(A)$ (resp., $\mathrm{Ind}^G(A)$) is coinduced (resp., induced). The result then follows easily by Theorem A.5.7 and the long exact sequences of Theorems A.2.13 and A.4.4. □

For Tate cohomology groups, we have an even cleaner result.

THEOREM A.7.3 (Dimension shifting). *Suppose that G is finite. With the above notation, we have*

$$\hat{H}^{i+1}(G,A) \cong \hat{H}^i(G,A^*) \quad \text{and} \quad \hat{H}^{i-1}(G,A) \cong \hat{H}^i(G,A_*)$$

for all $i \in \mathbb{Z}$.

PROOF. Again noting Lemma A.5.10, it follows from Theorem A.5.4 and Proposition A.6.7 that the long exact sequences associated by Theorem A.6.6 to the short exact sequences in (A.7.1) and (A.7.2) reduce to the isomorphisms in question. □

This result allows us to transfer questions about cohomology groups in a certain degree to analogous questions regarding cohomology groups in other degrees. Let us give a first application.

PROPOSITION A.7.4. *Suppose that G is a finite group and A is a G-module. Then the groups $\hat{H}^i(G,A)$ have exponent dividing $|G|$ for every $i \in \mathbb{Z}$.*

PROOF. By Theorem A.7.3, the problem immediately reduces to proving the claim for $i = 0$ and every module A. But for any $a \in A^G$, we have $|G|a = N_G a$, so $\hat{H}^0(G,A)$ has exponent dividing $|G|$. □

This has the following important corollary.

COROLLARY A.7.5. *Suppose that G is a finite group and A is a G-module that is finitely generated as an abelian group. Then $\hat{H}^i(G,A)$ is finite for every $i \in \mathbb{Z}$.*

PROOF. We know that $\hat{H}^i(G,A)$ is a subquotient of the finitely generated abelian group $Q_i \otimes_{\mathbb{Z}[G]} A$ of Theorem A.6.10, hence is itself finitely generated. As it has finite exponent, it is therefore finite. □

We also have the following.

COROLLARY A.7.6. *Suppose that G is finite. Suppose that A is a G-module on which multiplication by $|G|$ is an isomorphism. Then $\hat{H}^i(G,A) = 0$ for $i \in \mathbb{Z}$.*

PROOF. Multiplication by $|G|$ on A induces multiplication by $|G|$ on Tate cohomology, which is then an isomorphism. Since by Proposition A.7.4, multiplication by $|G|$ is also the zero map on Tate cohomology, the Tate cohomology groups must be 0. □

A.8. Comparing cohomology groups

DEFINITION A.8.1. Let G and G' be groups, A a G-module and A' a G'-module. We say that a pair (ρ, λ) with $\rho\colon G' \to G$ and $\lambda : A \to A'$ group homomorphisms is *compatible* if

$$\lambda(\rho(g')a) = g'\lambda(a)$$

for all $g' \in G'$ and $a \in A$.

Compatible pairs are used to provide maps among cohomology groups.

PROPOSITION A.8.2. *Suppose that $\rho\colon G' \to G$ and $\lambda\colon A \to A'$ form a compatible pair. Then the maps*

$$C^i(G,A) \to C^i(G',A'), \qquad f \mapsto \lambda \circ f \circ (\rho \times \cdots \times \rho)$$

induce maps on cohomology $H^i(G,A) \to H^i(G',A')$ for all $i \geq 0$.

PROOF. One need only check that this is compatible with differentials, but this is easily done using compatibility of the pair. That is, if f' is the image of f, then to show that

$$d^i f'(g'_0,\ldots,g'_i) = \lambda(d^i f(\rho(g'_0),\ldots,\rho(g'_i))),$$

immediately reduces to showing that the first terms on both sides arising from the expression for the definition of the differential are equal. Since the pair is compatible, we have

$$g'_0 f'(g'_1,\ldots g'_i) = g'_0\lambda(f(\rho(g'_1),\ldots,\rho(g'_i))) = \lambda(\rho(g'_0)f(\rho(g'_1),\ldots,\rho(g'_i))),$$

as desired. □

REMARK A.8.3. Using the standard resolution, we have a homomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}],A) \to \mathrm{Hom}_{\mathbb{Z}[G']}(\mathbb{Z}[(G')^{i+1}],A'), \qquad \psi \mapsto \lambda \circ \psi \circ (\rho \times \cdots \times \rho)$$

attached to a compatible pair (ρ,λ) that is compatible with the map on cochains.

REMARK A.8.4. Given a third group G'', a G''-module A'', and compatible pair (ρ',λ') with $\rho'\colon G'' \to G'$ and $\lambda'\colon A' \to A''$, we may speak of the composition $(\rho\circ\rho',\lambda'\circ\lambda)$, which will be a compatible pair that induces the morphism on complexes that is the composition of the morphisms arising from the pairs (ρ,λ) and (ρ',λ').

EXAMPLE A.8.5. In Shapiro's Lemma, the inclusion map $H \hookrightarrow G$ and the evaluation at 1 map $\mathrm{CoInd}_H^G(B) \to B$ form a compatible pair inducing the isomorphisms in its statement.

We consider two of the most important examples of compatible pairs, and the maps on cohomology arising from them.

DEFINITION A.8.6. Let H be a subgroup of G. Let A be a G-module.

a. Let $e\colon H \hookrightarrow G$ be the natural inclusion map. Then the maps

$$\mathrm{Res}\colon H^i(G,A) \to H^i(H,A)$$

induced by the compatible pair (e,id_A) on cohomology are known as *restriction maps*.

b. Suppose that H is normal in G. Let $q\colon G \to G/H$ be the quotient map, and let $\iota\colon A^H \to A$ be the inclusion map. Then the maps

$$\mathrm{Inf}\colon H^i(G/H,A^H) \to H^i(G,A)$$

induced by the compatible pair (q,ι) are known as *inflation maps*.

REMARK A.8.7. Restriction of an i-cocycle is just simply that, it is the restriction of the map $f\colon G^i \to A$ to a map $\mathrm{Res}(f)\colon H^i \to A$ given by $\mathrm{Res}(f)(h) = f(h)$ for $h \in H^i$. Inflation of an i-cocycle is just as simple: $\mathrm{Inf}(f)(g) = f(\bar{g})$, for $g \in G^i$ and $\bar{g}$ its image in $(G/H)^i$.

EXAMPLE A.8.8. In degree 0, the restriction map $\mathrm{Res}\colon A^G \to A^H$ is simply inclusion, and the inflation map $\mathrm{Inf}\colon (A^H)^{G/H} \to A^G$ is the identity.

REMARKS A.8.9.

a. Restriction provides a morphism of δ-functors. That is, it provides a sequence of natural transformations between the functors $H^i(G,\cdot)$ and $H^i(H,\cdot)$ on G-modules (which is to say that restriction commutes with G-module homomorphisms) such that for any short exact sequence of G-modules, the maps induced by the natural transformations commute with the connecting homomorphisms in the two resulting long exact sequences.

b. We could merely have defined restriction for $i = 0$ and used dimension shifting to define it for all $i \geq 1$, as follows from the previous remark.

THEOREM A.8.10 (Inflation-Restriction Sequence). *Let G be a group and N a normal subgroup. Let A be a G-module. Then the sequence*

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

is exact.

PROOF. The injectivity of inflation on cocycles obvious from Remark A.8.7. Let f be a cocycle in $Z^1(G/N, A^N)$. If $f(\bar{g}) = (g-1)a$ for some $a \in A$ and all $g \in G$, then $a \in A^N$ as $f(\bar{1}) = 0$, so Inf is injective. Also, note that $\mathrm{Res} \circ \mathrm{Inf}(f)(n) = f(\bar{n}) = 0$ for all $n \in N$.

Let $f' \in Z^1(G,A)$ and suppose $\mathrm{Res}(f') = 0$. Then there exists $a \in A$ such that $f'(n) = (n-1)a$ for all $n \in N$. Define $k \in Z^1(G,A)$ by $k(g) = f'(g) - (g-1)a$. Then $k(n) = 0$ for all $n \in N$. We then have

$$k(gn) = gk(n) + k(g) = k(g)$$

for all $g \in G$ and $n \in N$, so k factors through G/N. Also,

$$k(g) = k(g \cdot g^{-1}ng) = k(ng) = nk(g) + k(n) = nk(g),$$

so k has image in A^N. Therefore, k is the inflation of a cocycle in $Z^1(G/N, A^N)$, proving exactness. □

In fact, under certain conditions, we have an inflation-restriction sequence on the higher cohomology groups.

PROPOSITION A.8.11. *Let G be a group and N a normal subgroup. Let A be a G-module. Let $i \geq 1$, and suppose that $H^j(N,A) = 0$ for all $1 \leq j \leq i-1$. Then the sequence*

$$0 \to H^i(G/N, A^N) \xrightarrow{\mathrm{Inf}} H^i(G,A) \xrightarrow{\mathrm{Res}} H^i(N,A)$$

is exact.

PROOF. Let A^* be as in (A.7.1). By Theorem A.8.10, we may assume that $i \geq 2$. Since $H^1(N,A) = 0$, we have an exact sequence

$$0 \to A^N \to \mathrm{CoInd}^G(A)^N \to (A^*)^N \to 0 \tag{A.8.1}$$

in N-cohomology. Moreover, noting Lemma A.5.10, we have that

$$\mathrm{CoInd}^G(A)^N \cong \mathrm{Hom}_{\mathbb{Z}[N]}(\mathbb{Z}[G],A^\circ) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/N],A^\circ) \cong \mathrm{CoInd}^{G/N}(A),$$

where A° is the abelian group A with a trivial G-action. Thus, the connecting homomorphism

$$\delta^{i-1}\colon H^{i-1}(G/N,(A^*)^N) \xrightarrow{\sim} H^i(G/N,A^N)$$

in the G/N-cohomology of (A.8.1) is an isomorphism for $i \geq 2$.

Consider the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^{i-1}(G/N,(A^*)^N) & \xrightarrow{\mathrm{Inf}} & H^{i-1}(G,A^*) & \xrightarrow{\mathrm{Res}} & H^{i-1}(N,A^*) \\ & & \downarrow{\scriptstyle \delta^{i-1}} & & \downarrow{\scriptstyle \delta^{i-1}} & & \downarrow{\scriptstyle \delta^{i-1}} \\ 0 & \longrightarrow & H^i(G/N,A^N) & \xrightarrow{\mathrm{Inf}} & H^i(G,A) & \xrightarrow{\mathrm{Res}} & H^i(N,A). \end{array} \tag{A.8.2}$$

We have already seen that the leftmost vertical map in (A.8.2) is an isomorphism, and since $\mathrm{CoInd}^G(A)$ is an coinduced G-module, the central vertical map in (A.8.2) is an isomorphism. Moreover, as a coinduced G-module, $\mathrm{CoInd}^G(A)$ is also coinduced as an N-module, and therefore the rightmost vertical map in (A.8.2) is also an isomorphism. Therefore, the lower row of (A.8.2) will be exact if the top row is. But the top row is exact by Theorem A.8.10 if $i = 2$, and by induction if $i > 2$, noting that

$$H^{j-1}(N,A^*) \cong H^j(N,A) = 0$$

for all $j < i$. □

We consider one other sort of compatible pair, which is conjugation.

PROPOSITION A.8.12. *Let A be a G-module.*

a. Let H be a subgroup of G. Let $g \in G$, and define $\rho_g\colon gHg^{-1} \to H$ by $\rho_g(k) = g^{-1}kg$ for $k \in gHg^{-1}$. Define $\lambda_g\colon A \to A$ by $\lambda_g(a) = ga$. Then (ρ_g,λ_g) forms a compatible pair, and we denote by g^* the resulting map

$$g^*\colon H^i(H,A) \to H^i(gHg^{-1},A).$$

We have $g_1^* \circ g_2^* = (g_1 \circ g_2)^*$ for all $g_1, g_2 \in G$.

b. Suppose that N is normal in G. Then $H^i(N,A)$ is a G-module, where $g \in G$ acts as g^*. We refer to the above action as the conjugation action of G. The conjugation action factors through the quotient G/N and turns N-cohomology into a δ-functor from the category of G-modules to the category of (G/N)-modules.

c. The action of conjugation commutes with restriction maps among subgroups of G, which is to say that if $K \leq H \leq G$ and $g \in G$, then the diagram

$$\begin{array}{ccc} H^i(H,A) & \xrightarrow{\text{Res}} & H^i(K,A) \\ \downarrow{\scriptstyle g^*} & & \downarrow{\scriptstyle g^*} \\ H^i(gHg^{-1},A) & \xrightarrow{\text{Res}} & H^i(gKg^{-1},A) \end{array}$$

commutes.

PROOF.

a. First, we need check compatibility:

$$\lambda_g(\rho_g(h)a) = g \cdot g^{-1}hga = hga = h\lambda_g(a).$$

Next, we have

$$\lambda_{g_1g_2} = \lambda_{g_1} \circ \lambda_{g_2} \quad \text{and} \quad \rho_{g_1g_2} = \rho_{g_2} \circ \rho_{g_1},$$

so by Remark A.8.4, composition is as stated.

b. Suppose that $\kappa\colon A \to B$ is a G-module homomorphism. If $\alpha \in H^i(N,A)$ is the class of $f \in Z^i(N,A)$, then $\kappa^* \circ g^*(\alpha)$ is the class of

$$(n_1,\ldots,n_i) \mapsto \kappa(gf(g^{-1}n_1g,\ldots,g^{-1}n_ig)) = g\kappa(f(g^{-1}n_1g,\ldots,g^{-1}n_ig)),$$

and so has class $g^* \circ \kappa^*(\alpha)$.

Moreover, if

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

is an exact sequence of G-modules, then let

$$\delta\colon H^i(N,C) \to H^{i+1}(N,A)$$

Let $\gamma \in H^i(N,C)$. We must show that $\delta \circ g^*(\gamma) = g^* \circ \delta(\gamma)$. Since ι and π are G-module maps, by what we showed above, we need only show that the differential on $C^i(N,B)$ commutes with the map $g^{\cdot}$ induced by g on cochains. Let $z \in C^i(N,B)$. Then

$$\begin{aligned} g^{\cdot} \circ d^i(z)(n_0,\ldots,n_i) &= gd^i(z)(g^{-1}n_0g,\ldots,g^{-1}n_ig) \\ &= n_0gz(g^{-1}n_0g,\ldots,g^{-1}n_ig) + \sum_{j=1}^{i}(-1)^j f(g^{-1}n_0g,\ldots,g^{-1}n_{j-1}n_jg,\ldots,g^{-1}n_ig) \\ &\qquad + (-1)^{i+1}f(g^{-1}n_0g,\ldots,g^{-1}n_{i-1}g) = d^i(g^*(z))(n_0,\ldots,n_i). \end{aligned}$$

It only remains to show that the restriction of the action of G on Tate cohomology to N is trivial. This is easily computed on H^0: for $a \in A^N$ and $n \in N$, we have $n^*(a) = na = a$. In general, let A^* be as in (A.7.1) for the group G. The diagram

$$\begin{array}{ccc} H^i(N,A^*) & \xrightarrow{\delta} & H^{i+1}(N,A) \\ \downarrow{\scriptstyle n^*} & & \downarrow{\scriptstyle n^*} \\ H^i(N,A^*) & \xrightarrow{\delta} & H^{i+1}(N,A), \end{array}$$

which commutes what we have already shown. Assuming that n^* is the identity on $H^i(N,B)$ for every G-module B by induction (and in particular for $B = A^*$), we then have that n^* is the identity on $H^{i+1}(N,A)$ as well.

c. Noting Remark A.8.4, it suffices to check that the compositions of the compatible pairs in question are equal, which is immediate from the definitions.

□

We note the following corollary.

COROLLARY A.8.13. *The conjugation action of G on $H^i(G,A)$ is trivial for all i: that is,*

$$g^* \colon H^i(G,A) \to H^i(G,A)$$

is just the identity for all $g \in G$ and $i \geq 0$.

On homology, the analogous notion of a compatible pair is a pair (ρ,λ) where $\rho \colon G \to G'$ and $\lambda : A \to A'$ are group homomorphisms satisfying

$$\lambda(ga) = \rho(g)\lambda(a) \tag{A.8.3}$$

for all $g \in G$ and $a \in A$. These then provide morphisms

$$\tilde{\rho} \otimes \lambda : \mathbb{Z}[G^{i+1}] \otimes_{\mathbb{Z}[G]} A \to \mathbb{Z}[(G')^{i+1}] \otimes_{\mathbb{Z}[G']} A',$$

where $\tilde{\rho}$ is the induced map $\mathbb{Z}[G^{i+1}] \to \mathbb{Z}[(G')^{i+1}]$. By the homological compatibility of (A.8.3), these are seen to be compatible with the differentials, providing maps

$$H_i(G,A) \to H_i(G',A')$$

for all $i \geq 0$. As a consequence, we may make the following definition.

DEFINITION A.8.14. For $i \geq 0$ and a subgroup H of G, the *corestriction maps*

$$\mathrm{Cor} \colon H_i(H,A) \to H_i(G,A)$$

are defined to be the maps induced by the compatible pair (e, id_A), where $e \colon H \to G$ is the natural inclusion map.

EXAMPLE A.8.15. In degree 0, corestriction $\mathrm{Cor}\colon A_H \to A_G$ is just the quotient map.

DEFINITION A.8.16. For $i \geq 0$ and a normal subgroup H of G, the *coinflation maps*

$$\mathrm{CoInf}\colon H_i(G,A) \to H_i(G/H, A_H)$$

are defined to be the maps induces by the compatible pair (q,π), where $q\colon G \to G/H$ and $\pi\colon A \to A_H$ are the quotient maps.

REMARK A.8.17. For a G-module A and any normal subgroup H of G, the sequence

$$H_1(H,A) \xrightarrow{\mathrm{Cor}} H_1(G,A) \xrightarrow{\mathrm{CoInf}} H_1(G/H, A_H) \to 0.$$

is exact.

REMARK A.8.18. For a subgroup H of G, the pair (ρ_g^{-1}, λ_g) is a compatible pair for H-homology, inducing conjugation maps

$$g_*\colon H_i(H,A) \to H_i(gHg^{-1}, A).$$

If H is a normal subgroup, then these again provide a (G/H)-action on $H_i(H,A)$ and turn H-homology into a δ-functor. Conjugation commutes with corestriction on subgroups of G.

If H is of finite index in G, then we may define restriction maps on homology and corestriction maps on cohomology as well. If G is finite, then we obtain restriction and corestriction maps on all Tate cohomology groups as well. Let us first explain this latter case, as it is a bit simpler. Take, for instance, restriction. We have

$$\mathrm{Res}\colon H^i(G,A) \to H^i(H,A)$$

for all $i \geq 0$, so maps on Tate cohomology groups for $i \geq 1$. By Proposition A.7.3, we have

$$\hat{H}^{i-1}(G,A) \cong \hat{H}^i(G, A_*),$$

and the same holds for H-cohomology, as $\mathrm{Ind}^G(A)$ is also an induced H-module. We define

$$\mathrm{Res}\colon \hat{H}^{i-1}(G,A) \to \hat{H}^{i-1}(H,A)$$

to make the diagram

$$\begin{array}{ccc} \hat{H}^{i-1}(G,A) & \xrightarrow{\sim} & \hat{H}^i(G,A_*) \\ \big\downarrow \mathrm{Res} & & \big\downarrow \mathrm{Res} \\ \hat{H}^{i-1}(H,A) & \xrightarrow{\sim} & \hat{H}^i(H,A_*) \end{array}$$

commute.

If we wish to define restriction on homology groups when G is not finite, we need to provide first a definition of restriction on $H_0(G,A)$, so that we can use dimension shifting to define it for $H_i(G,A)$ with $i \geq 1$. Similarly, we need a description of corestriction on $H^0(G,A)$.

DEFINITION A.8.19. Suppose that H is a finite index subgroup of a group G and A is a G-module.

i. Define

$$\mathrm{Res}\colon H_0(G,A) \to H_0(H,A), \qquad x \mapsto \sum_{\bar{g}\in H\backslash G} g\cdot\tilde{x},$$

where $x \in A_G$ and $\tilde{x} \in A_H$ is any lift of it, and where g denotes any coset representative of $\bar{g} \in H\backslash G$.

ii. Define

$$\mathrm{Cor}\colon H^0(H,A) \to H^0(G,A), \qquad a \mapsto \sum_{\bar{g}\in G/H} g\cdot a$$

where $a \in A^H$ and g is as above.

PROPOSITION A.8.20. *Let G be a group and H a subgroup of finite index. Then there are maps*

$$\mathrm{Res}\colon H_i(G,A) \to H_i(H,A) \quad \textit{and} \quad \mathrm{Cor}\colon H^i(H,A) \to H^i(G,A)$$

for all $i \geq 0$ that coincide with the maps of Definition A.8.19 for $i = 0$ and that provide morphisms of δ-functors.

PROOF. Again, we consider the case of restriction, that of corestriction being analogous. We have a commutative diagram with exact rows

$$\begin{array}{ccccccc}
0 & \longrightarrow & H_1(G,A) & \longrightarrow & H_0(G,A_*) & \longrightarrow & H_0(G,\mathrm{Ind}^G(A)) \\
 & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} \\
0 & \longrightarrow & H_1(H,A) & \longrightarrow & H_0(H,A_*) & \longrightarrow & H_0(H,\mathrm{Ind}^G(A)),
\end{array}$$

which allows us to define restriction as the induced maps on kernels. For any $i \geq 2$, we proceed as described above in the case of Tate cohomology to define restriction maps on the ith homology groups.

That Res gives of morphism of δ-functors can be proven by induction using dimension shifting and a straightforward diagram chase and is left to the reader. □

REMARK A.8.21. Corestriction commutes with conjugation on the cohomology groups of subgroups of G with coefficients in G-modules. In the same vein, restriction commutes with conjugation on the homology of subgroups of G with G-module coefficients.

COROLLARY A.8.22. *Let G be finite and H a subgroup. The maps* Res *and* Cor *defined on both homology and cohomology above induce maps*

$$\mathrm{Res}\colon \hat{H}^i(G,A) \to \hat{H}^i(H,A) \quad \textit{and} \quad \mathrm{Cor}\colon \hat{H}^i(H,A) \to \hat{H}^i(G,A)$$

for all $i \in \mathbb{Z}$, and these provide morphisms of δ-functors.

PROOF. The reader may check that Res and Cor defined in homological and cohomological degree 0, respectively, induce morphisms on the corresponding Tate cohomology groups. We then have left only to check the commutativity of one diagram in each case.

Suppose that

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

is an exact sequence of G-modules. For restriction, we want to check that

$$\begin{array}{ccc} \hat{H}^{-1}(G,C) & \xrightarrow{\delta} & \hat{H}^0(G,A) \\ \downarrow \text{Res} & & \downarrow \text{Res} \\ \hat{H}^{-1}(H,C) & \xrightarrow{\delta} & \hat{H}^0(H,A) \end{array}$$

commutes. Let c be in the kernel of N_G on C, and denote its image in $\hat{H}^{-1}(G,C)$ by $\bar{c}$. Choose $b \in B$ with $\pi(b) = c$ and considering $N_G b \in B^G$, which is $\iota(a)$ for some $a \in A^G$. Then $\delta(c)$ is the image of a in $\hat{H}^0(G,A)$. Then $\text{Res}(\delta(\bar{c}))$ is just the image of a in $\hat{H}^0(H,A)$. On the other hand,

$$\text{Res}(\bar{c}) = \sum_{\bar{g} \in H\backslash G} g\tilde{c},$$

where $\tilde{c}$ is the image of c in $\hat{H}^{-1}(H,C)$. We may lift the latter element to $\sum_{\bar{g}} gc$ in the kernel of N_H on C and then to $\sum_{\bar{g}} gb \in B$. Taking N_H of this element gives us $N_G b$, which is $\iota(a)$, and so $\delta(\text{Res}(\bar{c}))$ is once again the image of a in $\hat{H}^0(H,A)$.

The case of corestriction is very similar, and hence omitted. □

The following describes an important relationship between restriction and corestriction.

PROPOSITION A.8.23. *Let G be a group and H a subgroup of finite index. Then the maps* $\text{Cor} \circ \text{Res}$ *on homology, cohomology, and, when G is finite, Tate cohomology, are just the multiplication by $[G:H]$ maps.*

PROOF. It suffices to prove this on the zeroth homology and cohomology groups. The result then follows by dimension shifting. On cohomology we have the composite map

$$A^G \xrightarrow{\text{Res}} A^H \xrightarrow{\text{Cor}} A^G,$$

where Res is the natural inclusion and Cor the map of Definition A.8.19. For $a \in A^G$, we have

$$\sum_{g \in G/H} ga = [G:H]a,$$

as desired.

On homology, we have maps

$$A_G \xrightarrow{\text{Res}} A_H \xrightarrow{\text{Cor}} A_G,$$

where Res is as in Definition A.8.19 and Cor is the natural quotient map. For $x \in A_G$ and $\tilde{x} \in A_H$ lifting it, the element

$$\sum_{g \in H \backslash G} g\tilde{x}$$

has image $[G:H]x$ in A_G, again as desired. □

Here is a useful corollary.

COROLLARY A.8.24. *Let G_p be a Sylow p-subgroup of a finite group G, for a prime p. Then the kernel of*

$$\mathrm{Res}\colon \hat{H}^i(G,A) \to \hat{H}^i(G_p,A)$$

has no elements of order p.

PROOF. Let $\alpha \in \hat{H}^i(G,A)$ with $p^n\alpha = 0$ for some $n \geq 0$. Then $\mathrm{Cor}(\mathrm{Res}(\alpha)) = [G:G_p]\alpha$, but $[G:G_p]$ is prime to p, hence $\mathrm{Cor}(\mathrm{Res}(\alpha))$ is nonzero if $\alpha \neq 0$, and therefore $\mathrm{Res}(\alpha)$ cannot be 0 unless $\alpha = 0$. □

We then obtain the following.

COROLLARY A.8.25. *Let G be a finite group. For each prime p, fix a Sylow p-subgroup G_p of G. Fix $i \in \mathbb{Z}$, and suppose that*

$$\mathrm{Res}\colon \hat{H}^i(G,A) \to \hat{H}^i(G_p,A)$$

is trivial for all primes p. Then $\hat{H}^i(G,A) = 0$.

PROOF. The intersection of the kernels of the restriction maps over all p contains no elements of p-power order for any p by Corollary A.8.24. So, if all of the restriction maps are trivial, the group $\hat{H}^i(G,A)$ must be trivial. □

Finally, we remark that we have conjugation Tate cohomology, as in the cases of homology and cohomology.

REMARK A.8.26. Suppose that G is finite and H is a subgroup of G. The conjugation maps on $H^0(H,A)$ and $H_0(H,A)$ induce maps on $\hat{H}^0(H,A)$ and $\hat{H}_0(H,A)$, respectively, and so we use the conjugation maps on homology and cohomology to define maps

$$g^*\colon \hat{H}^i(H,A) \to \hat{H}^i(gHg^{-1},A).$$

for all i. Again, these turn Tate cohomology for H into a δ-functor from G-modules to (G/H)-modules when H is normal in G. Conjugation commutes with restriction and corestriction on subgroups of G.

A.9. Cup products

We consider the following maps on the standard complex $P_\cdot$:

$$\kappa_{i,j}\colon P_{i+j} \to P_i \otimes_{\mathbb{Z}} P_j, \qquad \kappa_{i,j}(g_0,\dots,g_{i+j}) = (g_0,\dots,g_i)\otimes(g_i,\dots,g_{i+j}).$$

That is, there is a natural map

$$\operatorname{Hom}_{\mathbb{Z}[G]}(P_i,A)\otimes_{\mathbb{Z}}\operatorname{Hom}_{\mathbb{Z}[G]}(P_j,B) \to \operatorname{Hom}_{\mathbb{Z}[G]}(P_i\otimes_{\mathbb{Z}} P_j, A\otimes_{\mathbb{Z}} B)$$

defined by

$$\varphi\otimes\varphi' \mapsto (\alpha\otimes\beta \mapsto \varphi(\alpha)\otimes\varphi'(\beta)).$$

Composing this with the map induced by precomposition with $\kappa_{i,j}$ gives rise to a map

$$\operatorname{Hom}_{\mathbb{Z}[G]}(P_i,A)\otimes_{\mathbb{Z}}\operatorname{Hom}_{\mathbb{Z}[G]}(P_j,B) \xrightarrow{\cup} \operatorname{Hom}_{\mathbb{Z}[G]}(P_{i+j}, A\otimes_{\mathbb{Z}} B),$$

and we denote the image of $\varphi\otimes\varphi'$ under this map by $\varphi\cup\varphi'$. Let us summarize this.

DEFINITION A.9.1. Let $\varphi\in\operatorname{Hom}_{\mathbb{Z}[G]}(P_i,A)$ and $\varphi'\in\operatorname{Hom}_{\mathbb{Z}[G]}(P_j,B)$. The *cup product* $\varphi\cup\varphi'\in\operatorname{Hom}_{\mathbb{Z}[G]}(P_{i+j},A\otimes_{\mathbb{Z}}B)$ is defined by

$$(\varphi\cup\varphi')(g_0,\dots,g_{i+j}) = \varphi(g_0,\dots,g_i)\otimes\varphi'(g_i,\dots,g_{i+j}).$$

LEMMA A.9.2. *Let $\varphi\in\operatorname{Hom}_{\mathbb{Z}[G]}(P_i,A)$ and $\varphi'\in\operatorname{Hom}_{\mathbb{Z}[G]}(P_j,B)$. Then*

$$D^{i+j}_{A\otimes B}(\varphi\cup\varphi') = D^i_A(\varphi)\cup\varphi' + (-1)^i\varphi\cup D^j_B(\varphi'),$$

where the differentials D^i are as in (A.3.1).

PROOF. We compute the terms. We have

$$D^{i+j}_{A\otimes B}(\varphi\cup\varphi')(g_0,\dots,g_{i+j+1}) = \sum_{k=0}^{i}(-1)^k\varphi(g_0,\dots,\widehat{g_k},\dots,g_{i+1})\otimes\varphi'(g_{i+1},\dots,g_{i+j+1}) + \sum_{k=i+1}^{i+j+1}(-1)^k\varphi(g_0,\dots,g_i)\otimes\varphi'(g_i,\dots,\widehat{g_k},\dots,g_{i+j+1}),$$

while

$$(D^i_A(\varphi)\cup\varphi')(g_0,\dots,g_{i+j+1}) = \sum_{k=0}^{i+1}(-1)^k\varphi(g_0,\dots,\widehat{g_k},\dots,g_{i+1})\otimes\varphi'(g_{i+1},\dots,g_{i+j+1}) \tag{A.9.1}$$

and

$$(\varphi\cup D^j_B(\varphi'))(g_0,\dots,g_{i+j+1}) = \sum_{k=i}^{j+i+1}(-1)^{k-i}\varphi(g_0,\dots,g_i)\otimes\varphi'(g_i,\dots,\widehat{g_j},\dots,g_{i+j+1}). \tag{A.9.2}$$

As $(-1)^{i+1}+(-1)^i=0$, the last term in (A.9.1) cancels with the $(-1)^i$ times the first term in (A.9.2). The equality of the two sides follows. □

REMARK A.9.3. On cochains, we can define cup products

$$C^i(G,A)\otimes_{\mathbb{Z}} C^j(G,B)\xrightarrow{\cup} C^{i+j}(G,A\otimes_{\mathbb{Z}} B)$$

of $f\in C^i(G,A)$ and $f'\in C^j(G,B)$ by

$$(f\cup f')(g_1,g_2,\dots g_{i+j}) = f(g_1,\dots,g_i)\otimes g_1g_2\dots g_i f'(g_{i+1},\dots,g_{i+j}).$$

To see that these match up with the previous definition, note that if we define φ and φ' by

$$\varphi(1,g_1,\dots,g_1\cdots g_i) = f(g_1,\dots,g_i) \quad \text{and} \quad \varphi'(1,g_1,\dots,g_1\cdots g_j) = f'(g_1,\dots,g_j),$$

then

$$\begin{aligned}(f\cup f')(g_1,\dots,g_{i+j}) &= \varphi(1,g_1,\dots,g_1\cdots g_i)\cup g_1g_2\dots g_i\varphi(1,g_{i+1},\dots,g_{i+1}\cdots g_{i+j+1})\\ &= \varphi(1,g_1,\dots,g_1\cdots g_i)\cup \varphi(g_1\cdots g_i,g_1\cdots g_{i+1},\dots,g_1\cdots g_{i+j+1})\\ &= (\varphi\cup\varphi')(1,g_1,\dots,g_1\cdots g_{i+j+1}),\end{aligned}$$

so the definitions agree under the identifications of Theorem A.3.3. As a consequence of Lemma A.9.2, the cup products on cochains satisfy

$$d^{i+j}_{A\otimes B}(f\cup f') = d^i_A(f)\cup f' + (-1)^i f\cup d^j_B(f'). \tag{A.9.3}$$

LEMMA A.9.4. *The sequences*

$$0\to A\otimes_{\mathbb{Z}} B\to \mathrm{CoInd}^G(A)\otimes_{\mathbb{Z}} B\to A^*\otimes_{\mathbb{Z}} B\to 0 \tag{A.9.4}$$

$$0\to A_*\otimes_{\mathbb{Z}} B\to \mathrm{Ind}^G(A)\otimes_{\mathbb{Z}} B\to A\otimes_{\mathbb{Z}} B\to 0 \tag{A.9.5}$$

are exact for any G-modules A and B.

PROOF. Since the augmentation map ε is split over $\mathbb{Z}$, it follows using Remark A.7.1 that the sequences (A.7.1) and (A.7.2) are split as well. It follows that the sequences in the lemma are exact. □

THEOREM A.9.5. *The cup products of Definition A.9.1 induce maps, also called cup products,*

$$H^i(G,A)\otimes_{\mathbb{Z}} H^j(G,B)\xrightarrow{\cup} H^{i+j}(G,A\otimes_{\mathbb{Z}} B)$$

that are natural in A and B and satisfy the following properties:

(i) For $i=j=0$, one has that the cup product

$$A^G\otimes_{\mathbb{Z}} B^G\to (A\otimes_{\mathbb{Z}} B)^G$$

is induced by the identity on $A\otimes_{\mathbb{Z}} B$.

(ii) If

$$0 \to A_1 \to A \to A_2 \to 0$$

is an exact sequence of G-modules such that

$$0 \to A_1 \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B \to A_2 \otimes_{\mathbb{Z}} B \to 0$$

is exact as well, then

$$\delta(\alpha_2 \cup \beta) = (\delta\alpha_2) \cup \beta \in H^{i+j+1}(G, A_1 \otimes_{\mathbb{Z}} B)$$

for all $\alpha_2 \in H^i(G,A_2)$ and $\beta \in H^j(G,B)$. (In other words, cup product on the right with a cohomology class provides a morphism of δ-functors.)

(iii) If

$$0 \to B_1 \to B \to B_2 \to 0$$

is an exact sequence of G-modules such that

$$0 \to A \otimes_{\mathbb{Z}} B_1 \to A \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B_2 \to 0$$

is exact as well, then

$$\delta(\alpha \cup \beta_2) = (-1)^i \alpha \cup (\delta\beta_2) \in H^{i+j+1}(G, A \otimes_{\mathbb{Z}} B_1)$$

for all $\alpha \in H^i(G,A)$ and $\beta_2 \in H^j(G,B_2)$.

Moreover, the cup products on cohomology are the unique collection of such maps natural in A and B and satisfying properties (i), (ii), and (iii).

PROOF. Let $f \in C^i(G,A)$ and $f' \in C^j(G,B)$. By (A.9.3), it is easy to see that the cup product of two cocycles is a cocycle and that the cup product of a cocycle and a coboundary is a coboundary. Thus, the cup product on cochains induces cup products on cohomology. The naturality in A and B follows directly from the definition. Property (i) is immediate from the definition as well. Property (ii) can be seen by tracing through the definition of the connecting homomorphism. Let f_2 represent α_2. Then $\delta(\alpha_2)$ is obtained by lifting f_2 to a cochain $f \in C^i(G,A)$, taking its boundary $df \in C^{i+1}(G,A)$, and then noting that df is the image of some cocycle $z_1 \in Z^{i+1}(G,A_1)$. Let $f' \in Z^j(G,B)$ represent β. By (A.9.3), we have $df \cup f' = d(f \cup f')$. Note that $z_1 \cup f'$ has class $\delta(\alpha_2) \cup \beta$ and image $df \cup f'$ in $C^{i+j+1}(G, A \otimes_{\mathbb{Z}} B)$. On the other hand, $d(f \cup f')$ is the image of a cocycle representing $\delta(\alpha_2 \cup \beta)$, as $f \cup f'$ is a cocycle lifting $f_2 \cup f'$. Since the map

$$C^{i+j+1}(G, A_1 \otimes_{\mathbb{Z}} B) \to C^{i+j+1}(G, A \otimes_{\mathbb{Z}} B)$$

is injective, we have (ii). Property (iii) follows similarly, the sign appearing in the computation arising from (A.9.3).

The uniqueness of the maps with these properties follows from the fact that given a collection of such maps, property (i) specifies them uniquely for $i = j = 0$, while properties (ii) and (iii) specify

them uniquely for all other $i, j \geq 0$ by dimension shifting. For instance, by (ii) and Lemma A.9.4, we have a commutative square

$$\begin{array}{ccc} H^i(G,A^*) \otimes_{\mathbb{Z}} H^j(G,B) & \xrightarrow{\cup} & H^{i+j}(G,A^* \otimes_{\mathbb{Z}} B) \\ \downarrow\!\!\downarrow & & \downarrow \\ H^{i+1}(G,A) \otimes_{\mathbb{Z}} H^j(G,B) & \xrightarrow{\cup} & H^{i+j+1}(G,A \otimes_{\mathbb{Z}} B) \end{array}$$

in which the lefthand vertical arrow is a surjection for all i (and an isomorphism for $i \geq 1$). Thus, the cup products in degrees (i, j) for $i \geq 1$ and $j \geq 0$ specify by the cup products in degrees $(i+1, j)$. Similarly, using (iii), we see that the cup products in degrees (i, j) specify the cup products in degrees $(i, j+1)$. □

REMARK A.9.6. Associativity of tensor products and Lemma A.5.10 tell us that

$$\mathrm{Ind}^G(A \otimes_{\mathbb{Z}} B) \cong \mathrm{Ind}^G(A) \otimes_{\mathbb{Z}} B,$$

so in particular the latter modules is induced. This also implies that we have isomorphisms

$$(A \otimes_{\mathbb{Z}} B)_* \cong A_* \otimes_{\mathbb{Z}} B.$$

If G is finite, Proposition A.5.4 tells us that we have

$$\mathrm{CoInd}^G(A \otimes_{\mathbb{Z}} B) \cong \mathrm{CoInd}^G(A) \otimes_{\mathbb{Z}} B \quad \text{and} \quad (A \otimes_{\mathbb{Z}} B)^* \cong A^* \otimes_{\mathbb{Z}} B$$

as well.

COROLLARY A.9.7. *Consider the natural isomorphism*

$$s_{AB} \colon A \otimes_{\mathbb{Z}} B \to B \otimes_{\mathbb{Z}} A$$

given by $a \otimes b \mapsto b \otimes a$, and the maps that it induces on cohomology. For all $\alpha \in H^i(G,A)$ and $\beta \in H^j(G,B)$, one has that

$$s_{AB}^*(\alpha \cup \beta) = (-1)^{ij}(\beta \cup \alpha).$$

PROOF. We first verify the result in the case $i = j = 0$. For $a \in A^G$ and $b \in B^G$, we have

$$s_{AB}^*(a \cup b) = s_{AB}(a \otimes b) = b \otimes a = b \cup a.$$

Suppose that we know the result for a given pair $(i-1, j)$. Let $\alpha \in H^i(G,A)$ and $\beta \in H^j(G,B)$. Recall that the maps $H^{i-1}(G,A^*) \to H^i(G,A)$ are surjective for all $i \geq 1$ (and isomorphisms for $i \geq 2$), and write $\alpha = \delta(\alpha^*)$ for some $\alpha^* \in H^{i-1}(G,A^*)$. Since (A.9.4) is exact, we have by Theorem A.9.5 that

$$\begin{aligned} s_{AB}^*(\alpha \cup \beta) = s_{AB}^*(\delta(\alpha^*) \cup \beta) = s_{AB}^*(\delta(\alpha^* \cup \beta)) = \delta(s_{AB}^*(\alpha^* \cup \beta)) \\ = (-1)^{(i-1)j}\delta(\beta \cup \alpha^*) = (-1)^{(i-1)j}(-1)^j \beta \cup \delta(\alpha^*) = (-1)^{ij}\beta \cup \alpha. \end{aligned}$$

Suppose next that we know the result for a given pair $(i, j-1)$. Let $\alpha \in H^i(G,A)$ and $\beta \in H^{j-1}(G,B)$, and write $\beta = \delta(\beta^*)$ for some $\beta^* \in H^j(G,B^*)$. Since (A.9.4) is exact, we have by Theorem A.9.5 that

$$\begin{aligned} s^*_{AB}(\alpha \cup \beta) = s^*_{AB}(\alpha \cup \delta(\beta^*)) = (-1)^i s^*_{AB}(\delta(\alpha \cup \beta^*)) = \delta(s^*_{AB}(\alpha \cup \beta^*)) \\ = (-1)^i(-1)^{i(j-1)}\delta(\beta^* \cup \alpha) = (-1)^{ij}\delta(\beta^*) \cup \alpha = (-1)^{ij}\beta \cup \alpha. \end{aligned}$$

The result now follows by induction on i and j. □

Cup products also have an associative property, which can be checked directly on cochains.

PROPOSITION A.9.8. *Let A, B, and C be G-modules, and let $\alpha \in H^i(G,A)$, $\beta \in H^j(G,B)$, and $\gamma \in H^k(G,C)$. Then*

$$(\alpha \cup \beta) \cup \gamma = \alpha \cup (\beta \cup \gamma) \in H^{i+j+k}(G, A \otimes_{\mathbb{Z}} B \otimes_{\mathbb{Z}} C).$$

Often, when we speak of cup products, we apply an auxiliary map from the tensor product of A and B to a third module before taking the result. For instance, if $A = B = \mathbb{Z}$, then one will typically make the identification $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}$. We codify this in the following definition.

DEFINITION A.9.9. Suppose that A, B, and C are G-modules and $\theta\colon A \otimes_{\mathbb{Z}} B \to C$ is a G-module homomorphism. Then the maps

$$H^i(G,A) \otimes_{\mathbb{Z}} H^j(G,B) \to H^{i+j}(G,C), \qquad \alpha \otimes \beta \mapsto \theta(\alpha \cup \beta)$$

are also referred to as cup products. When θ is understood, we denote $\theta(\alpha \cup \beta)$ more simply by $\alpha \cup \beta$.

Cup products behave nicely with respect to restriction, corestriction, and inflation.

PROPOSITION A.9.10. *Let A and B be G-modules. We then have the following compatibilities.*

a. Let H be a subgroup of G. For $\alpha \in H^i(G,A)$ and $\beta \in H^j(G,B)$, one has

$$\mathrm{Res}(\alpha \cup \beta) = \mathrm{Res}(\alpha) \cup \mathrm{Res}(\beta) \in H^{i+j}(H, A \otimes_{\mathbb{Z}} B),$$

where Res *denotes restriction from G to H.*

b. Let N be a normal subgroup of G. For $\alpha \in H^i(G/N, A^N)$ and $\beta \in H^j(G/N, B^N)$, one has

$$\mathrm{Inf}(\alpha \cup \beta) = \mathrm{Inf}(\alpha) \cup \mathrm{Inf}(\beta) \in H^{i+j}(G, A \otimes_{\mathbb{Z}} B),$$

where Inf *denotes inflation from G/N to G. (Here, we implicitly use the canonical map $A^N \otimes_{\mathbb{Z}} B^N \to (A \otimes_{\mathbb{Z}} B)^N$ prior to taking inflation on the left.)*

c. Let H be a subgroup of finite index in G. For $\alpha \in H^i(H,A)$ and $\beta \in H^j(G,B)$, one has

$$\mathrm{Cor}(\alpha) \cup \beta = \mathrm{Cor}(\alpha \cup \mathrm{Res}(\beta)) \in H^{i+j}(G, A \otimes_{\mathbb{Z}} B),$$

where Res *denotes restriction from G to H and* Cor *denotes corestriction from H to G.*

PROOF. We can prove part a by direct computation on cocycles. That is, for $f \in Z^i(G,A)$, $f' \in Z^i(G,B)$, and $h_1,\dots,h_{i+j} \in H$, we have

$$\begin{aligned}\mathrm{Res}(f\cup f')(h_1,\dots,h_{i+j}) &= (f\cup f')(h_1,\dots,h_{i+j}) = f(h_1,\dots,h_i)\otimes h_1\cdots h_i f'(h_{i+1},\dots,h_{i+j})\\ &= \mathrm{Res}(f)(h_1\dots,h_i)\otimes h_1\cdots h_i\,\mathrm{Res}(f')(h_{i+1},\dots,h_{i+j}) = (\mathrm{Res}(f)\cup\mathrm{Res}(f'))(h_1,\dots,h_{i+j}).\end{aligned}$$

Part b is similarly computed.

We now prove part c. Consider the case that $i=j=0$. Then $a\in A^H$ and $b\in B^G$. By property (i) in Theorem A.9.5 and the definition of corestriction on H^0, we have

$$\mathrm{Cor}(a)\cup b = \sum_{\bar g\in G/H}(ga)\otimes b = \sum_{\bar g\in G/H}(ga\otimes gb) = \sum_{\bar g\in G/H} g(a\otimes b) = \mathrm{Cor}(a\cup\mathrm{Res}(b)).$$

As corestriction and restriction commute with connecting homomorphisms, and as cup products behave well with respect to connecting homomorphisms on either side, we can use dimension shifting to prove the result for all i and j. That is, suppose we know the result for a fixed pair $(i-1,j)$. We prove it for (i,j). Letting δ the connecting homomorphism induced by (A.7.1) for A, and choose $\alpha^*\in H^{i-1}(G,A^*)$ such that $\delta(\alpha^*)=\alpha$. We then have

$$\begin{aligned}\mathrm{Cor}(\alpha)\cup\beta = \delta(\mathrm{Cor}(\alpha^*))\cup\beta &= \delta(\mathrm{Cor}(\alpha^*)\cup\beta)\\ &= \delta(\mathrm{Cor}(\alpha^*\cup\mathrm{Res}(\beta)) = \mathrm{Cor}(\delta(\alpha^*\cup\mathrm{Res}(\beta))) = \mathrm{Cor}(\alpha\cup\mathrm{Res}(\beta)).\end{aligned}$$

Similarly, take δ for the sequence analogous to (A.7.1) for the module B and assume the result for $(i,j-1)$. Choosing $\beta^*\in H^{j-1}(G,B^*)$ with $\delta(\beta^*)=\beta$, we have

$$\begin{aligned}\mathrm{Cor}(\alpha)\cup\beta = \mathrm{Cor}(\alpha)\cup\delta(\beta^*) = (-1)^i\delta(\mathrm{Cor}(\alpha)\cup\beta^*) &= (-1)^i\delta(\mathrm{Cor}(\alpha\cup\mathrm{Res}(\beta^*)))\\ &= (-1)^i\mathrm{Cor}(\delta(\alpha\cup\mathrm{Res}(\beta^*))) = \mathrm{Cor}(\alpha\cup\delta(\mathrm{Res}(\beta^*))) = \mathrm{Cor}(\alpha\cup\mathrm{Res}(\beta)).\end{aligned}$$

□

NOTATION A.9.11. We may express the statement of Proposition A.9.10a as saying that the diagram

$$\begin{array}{ccc} H^i(G,A)\otimes_{\mathbb{Z}} H^j(G,B) & \xrightarrow{\cup} & H^i(G,A\otimes_{\mathbb{Z}} B)\\ \big\downarrow \mathrm{Res} \quad \big\downarrow \mathrm{Res} & & \big\downarrow \mathrm{Res}\\ H^i(H,A)\otimes_{\mathbb{Z}} H^j(H,B) & \xrightarrow{\cup} & H^i(H,A\otimes_{\mathbb{Z}} B)\end{array}$$

commutes (with a similar diagram for part b) and the statement of Proposition A.9.10c as saying that the diagram

$$\begin{array}{ccc} H^i(G,A)\otimes_{\mathbb{Z}} H^j(G,B) & \xrightarrow{\cup} & H^i(G,A\otimes_{\mathbb{Z}} B)\\ \big\uparrow \mathrm{Cor} \quad \big\downarrow \mathrm{Res} & & \big\uparrow \mathrm{Cor}\\ H^i(H,A)\otimes_{\mathbb{Z}} H^j(H,B) & \xrightarrow{\cup} & H^i(H,A\otimes_{\mathbb{Z}} B)\end{array}$$

commutes.

For finite groups, we have cup products on Tate cohomology as well.

THEOREM A.9.12. *Let G be finite. There exists a unique family of maps*

$$\hat{H}^i(G,A) \otimes_{\mathbb{Z}} \hat{H}^j(G,B) \xrightarrow{\cup} \hat{H}^{i+j}(G, A \otimes_{\mathbb{Z}} B)$$

with $i, j \in \mathbb{Z}$ that are natural in the G-modules A and B and which satisfy the following properties:

(i) The diagram

$$\begin{array}{ccc} H^0(G,A) \otimes_{\mathbb{Z}} H^0(G,B) & \xrightarrow{\cup} & H^0(G, A \otimes_{\mathbb{Z}} B) \\ \downarrow & & \downarrow \\ \hat{H}^0(G,A) \otimes_{\mathbb{Z}} \hat{H}^0(G,B) & \xrightarrow{\cup} & \hat{H}^0(G, A \otimes_{\mathbb{Z}} B) \end{array}$$

commutes.

(ii) If

$$0 \to A_1 \to A \to A_2 \to 0$$

is an exact sequence of G-modules such that

$$0 \to A_1 \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B \to A_2 \otimes_{\mathbb{Z}} B \to 0$$

is exact as well, then

$$\delta(\alpha_2 \cup \beta) = (\delta \alpha_2) \cup \beta \in \hat{H}^{i+j+1}(G, A_1 \otimes_{\mathbb{Z}} B)$$

for all $\alpha_2 \in \hat{H}^i(G,A_2)$ and $\beta \in \hat{H}^j(G,B)$.

(iii) If

$$0 \to B_1 \to B \to B_2 \to 0$$

is an exact sequence of G-modules such that

$$0 \to A \otimes_{\mathbb{Z}} B_1 \to A \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B_2 \to 0$$

is exact as well, then

$$\delta(\alpha \cup \beta_2) = (-1)^i \alpha \cup (\delta \beta_2) \in \hat{H}^{i+j+1}(G, A \otimes_{\mathbb{Z}} B_1)$$

for all $\alpha \in \hat{H}^i(G,A)$ and $\beta_2 \in \hat{H}^j(G,B_2)$.

PROOF. Consider the complex $Q_\cdot$ of Theorem A.6.10, obtained from the standard resolution $P_\cdot$. The proof goes through as in Theorem A.9.5 once we define maps $Q_{i+j} \to Q_i \otimes_{\mathbb{Z}} Q_j$ satisfying the formula of Lemma A.9.2. There are six cases to consider (the case $i, j \geq 0$ being as before), and these are omitted. □

REMARK A.9.13. Corollary A.9.7, Proposition A.9.8, and Proposition A.9.10 all hold for cup products on Tate cohomology as well. We can also compose cup products with G-module maps from the tensor product, and we again denote them using the same symbol, as in Definition A.9.9.

A.10. Tate cohomology of cyclic groups

In this section, let G be a cyclic group of finite order. We prove that the Tate cohomology groups with coefficients in a module A are periodic in the degree of period 2, up to isomorphisms determined by a choice of generator g of G.

The first thing that we will observe is that for such a group G, there is an even nicer projective resolution of $\mathbb{Z}$ than the standard one: i.e., consider the sequence

$$\cdots \to \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0, \tag{A.10.1}$$

where the boundary maps are multiplication N_G in even degree and by $g-1$ in odd degree. We can splice this together with its dual as in Theorem A.6.10.

PROPOSITION A.10.1. *The G-cohomology groups of A are the cohomology groups of the complex*

$$\cdots \to A \xrightarrow{g-1} A \xrightarrow{N_G} A \xrightarrow{g-1} A \to \cdots,$$

with a map $g-1$ following the term in degree 0.

PROOF. Note first that for $i \in \{-1,0\}$, the group $\hat{H}^i(G,A)$ is by definition isomorphic to the ith cohomology group of the complex in question. Let $C_\cdot$ denote the projective resolution of $\mathbb{Z}$ given by (A.10.1). The complex $C_\cdot \otimes_{\mathbb{Z}[G]} A$ that ends

$$\cdots \to A \xrightarrow{g-1} A \xrightarrow{N_G} A \xrightarrow{g-1} A \to 0$$

computes $H_i(G,A)$, yielding the result for $i \leq -2$.

Multiplication by g induces the endomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],A), \qquad \varphi \mapsto (x \mapsto \varphi(gx) = g\varphi(x)).$$

Via the isomorphism of G-modules $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],A) \xrightarrow{\sim} A$ given by evaluation at 1, the latter endomorphism is identified with multiplication by g on A. The complex $\mathrm{Hom}_{\mathbb{Z}[G]}(C_\cdot,A)$ that computes $H^i(G,A)$ is therefore isomorphic to

$$0 \to A \xrightarrow{g-1} A \xrightarrow{N_G} A \xrightarrow{g-1} A \to \cdots,$$

providing the result for $i \geq 1$. □

COROLLARY A.10.2. *For any $i \in \mathbb{Z}$, we have*

$$\hat{H}^i(G,A) \cong \begin{cases} \hat{H}^0(G,A) & i \text{ even} \\ \hat{H}^{-1}(G,A) & i \text{ odd.} \end{cases}$$

We show that, in fact, these isomorphisms can be realized by means of a cup product. As usual, consider $\mathbb{Z}$ as having a trivial G-action. We remark that

$$\hat{H}^{-2}(G,\mathbb{Z}) \cong H_1(G,\mathbb{Z}) \cong G^{\mathrm{ab}} \cong G$$

by Proposition A.4.5. Any choice of generator g of G is now a generator u_g of this Tate cohomology group. Note that $\mathbb{Z}\otimes_{\mathbb{Z}} A \cong A$ for any G-module A via multiplication. Here then is the result.

PROPOSITION A.10.3. *Let G be cyclic with generator g, and let A be a G-module. Then the map*

$$\hat{H}^i(G,A) \to \hat{H}^{i-2}(G,A), \qquad c \mapsto u_g \cup c$$

is an isomorphism for any $i \in \mathbb{Z}$.

PROOF. Consider the two exact sequences of G-modules:

$$0 \to I_G \to \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0 \quad \text{and} \quad 0 \to \mathbb{Z} \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g-1} I_G \to 0.$$

As $\hat{H}^i(G,\mathbb{Z}[G]) = 0$ for all $i \in \mathbb{Z}$, we then have two isomorphisms

$$\hat{H}^{-2}(G,\mathbb{Z}) \xrightarrow{\delta} \hat{H}^{-1}(G,I_G) \xrightarrow{\delta} \hat{H}^0(G,\mathbb{Z}).$$

(In fact, tracing it through, one sees that the image of u_g under this composition is 1 modulo $|G|$. This is not needed for the proof.)

Since we have

$$\delta(\delta(u_g)) \cup c = \delta(\delta(u_g \cup c))$$

by property (ii) of Theorem A.9.12, it suffices to show that cup product with the image of 1 in $\hat{H}^0(G,\mathbb{Z})$ is an isomorphism. For this, using property (iii) of Theorem A.9.12 to dimension shift, the problem reduces to the case that $i = 0$. In this case, we know that the cup product is induced on $\hat{H}^0$ by the multiplication map on H^0's:

$$\mathbb{Z}\otimes_{\mathbb{Z}} A^G \to A^G, \qquad m \otimes a \mapsto ma.$$

However, $1 \cdot a = a$, so the map $\hat{H}^0(G,A) \to \hat{H}^0(G,A)$ induced by taking cup product with the image of 1 is an isomorphism. □

Given the 2-periodicity of the Tate cohomology groups of a finite cyclic group, we can make the following definition.

DEFINITION A.10.4. Let G be a finite cyclic group and A a G-module. Set $h_0(A) = |\hat{H}^0(G,A)|$ and $h_1(A) = |\hat{H}^1(G,A)|$, taking them to be infinite when the orders of the Tate cohomology groups are infinite. If both $h_0(A)$ and $h_1(A)$ are finite, we then define the *Herbrand quotient* $h(A)$ by

$$h(A) = \frac{h_0(A)}{h_1(A)}.$$

Clearly, if A is finitely generated, then $h(A)$ will be defined. The following explains how Herbrand quotients behave with respect to modules in short exact sequences.

THEOREM A.10.5. *Let*

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

be an exact sequence of G-modules. Suppose that any two of $h(A)$, $h(B)$, and $h(C)$ are defined. Then the third is as well, and

$$h(B) = h(A) \cdot h(C).$$

PROOF. It follows immediately from Proposition A.10.3 that we have an exact hexagon

$$\begin{array}{ccccc} & & \hat{H}^0(G,A) & \longrightarrow & \hat{H}^0(G,B) & & \\ & \nearrow & & & & \searrow & \\ \hat{H}^1(G,C) & & & & & & \hat{H}^0(G,C) \\ & \nwarrow & & & & \swarrow & \\ & & \hat{H}^1(G,B) & \longleftarrow & \hat{H}^1(G,A) & & \end{array} .$$

Note that the order of any group in the hexagon is the product of the orders of the image of the map from the previous group and the order of the image of the map to the next group. Therefore, that any two of $h(A)$, $h(B)$, and $h(C)$ are finite implies the third is. When all three are finite, an Euler characteristic argument then tells us that

$$\frac{h_0(A) \cdot h_0(C) \cdot h_1(B)}{h_0(B) \cdot h_1(A) \cdot h_1(C)} = 1, \tag{A.10.2}$$

hence the result. More specifically, the order of each cohomology group is the product of the orders of the images of two adjacent maps in the hexagon, and the order of the image of each such map then appears once in each of the numerator and denominator of the left-hand side of (A.10.2). □

As an immediate consequence of Theorem A.10.5, we have the following.

COROLLARY A.10.6. *Suppose that*

$$0 \to A_1 \to A_2 \to \cdots \to A_n \to 0$$

is an exact sequence of G-modules with $h(A_k)$ finite for at least one of each consecutive pair of subscripts k, including at least one of A_n and A_1. Then all $h(A_k)$ are finite and

$$\prod_{k=1}^{n} h(A_k)^{(-1)^k} = 1.$$

Next, we show that the Herbrand quotients of finite modules are trivial.

PROPOSITION A.10.7. *Suppose that A is a finite G-module. Then $h(A) = 1$.*

PROOF. Let g be a generator of G, and note that the sequence

$$0 \to A^G \to A \xrightarrow{g-1} A \to A_G \to 0$$

is exact. As A is finite and any alternating product of orders of finite groups in exact sequences of finite length is 1, we therefore have $|A^G| = |A_G|$. On the other hand, we have the exact sequence

$$0 \to \hat{H}^{-1}(G,A) \to A_G \xrightarrow{\tilde{N}_G} A^G \to \hat{H}^0(G,A) \to 0$$

defining $\hat{H}^i(G,A)$ for $i = 0,-1$. As $h_1(A) = |\hat{H}^{-1}(G,A)|$, we therefore have $h(A) = 1$. □

We therefore have the following.

PROPOSITION A.10.8. *Let $f\colon A \to B$ be a G-module homomorphism with finite kernel and cokernel. Then $h(A) = h(B)$ if either one is defined.*

PROOF. This follows immediately from the exact sequence

$$0 \to \ker f \to A \to B \to \operatorname{coker} f \to 0,$$

Corollary A.10.6, and Proposition A.10.7. □

A.11. Cohomological triviality

In this section, we suppose that G is a finite group.

DEFINITION A.11.1. A G-module A is said to be *cohomologically trivial* if $\hat{H}^i(H,A) = 0$ for all subgroups H of G and all $i \in \mathbb{Z}$.

In this section, we will give conditions for a G-module to be cohomologically trivial.

REMARK A.11.2. Every free G-module is also a free H-module for every subgroup H of G and any group G, not necessarily finite. In particular, $\mathbb{Z}[G]$ is free over $\mathbb{Z}[H]$ on any set of cosets representatives of $H\backslash G$.

We remark that it follows from this that induced G-modules are induced H-modules, as direct sums commute with tensor products. We then have the following examples of cohomologically trivial modules.

EXAMPLES A.11.3.

a. Induced G-modules are cohomologically trivial by Proposition A.6.7.

b. Projective G-modules are cohomologically trivial. To see this, suppose that P and Q are projective G-modules with $P \oplus Q$ free over $\mathbb{Z}[G]$, hence over $\mathbb{Z}[H]$. Then

$$\hat{H}^i(H,P) \hookrightarrow \hat{H}^i(H,P) \oplus \hat{H}^i(H,Q) \cong \hat{H}^i(H,P \oplus Q) = 0$$

for all $i \in \mathbb{Z}$.

We need some preliminary lemmas. Fix a prime p.

LEMMA A.11.4. *Suppose that G is a p-group and that A is a G-module of exponent dividing p. Then $A = 0$ if and only if $A_G = 0$ and if and only if $A^G = 0$.*

PROOF. Suppose $A^G = 0$, and let $a \in A$. The submodule B of A generated by a is finite, and $B^G = 0$. The latter fact implies that the G-orbits in B are either $\{0\}$ or have order a multiple of p. Since B has p-power order, this forces the order to be 1, so $B = 0$. Since a was arbitrary, $A = 0$. On the other hand, if $A_G = 0$, then $X = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{F}_p)$ satisfies $pX = 0$ and

$$X^G = \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathbb{F}_p) = \mathrm{Hom}_{\mathbb{Z}[G]}(A_G, \mathbb{F}_p) = 0.$$

By the invariants case just proven, we know $X = 0$, so $A = 0$. □

LEMMA A.11.5. *Suppose that G is a p-group and that A is a G-module of exponent dividing p. If $H_1(G,A) = 0$, then A is free as an $\mathbb{F}_p[G]$-module.*

PROOF. Lift an $\mathbb{F}_p$-basis of A_G to a subset Σ of A. For the G-submodule B of A generated by Σ, the quotient A/B has trivial G-coinvariant group, hence is trivial by Lemma A.11.4. That is, Σ generates A as an $\mathbb{F}_p[G]$-module. Letting F be the free $\mathbb{F}_p[G]$-module generated by Σ, we then have a canonical surjection $\pi\colon F \to A$, and we let R be the kernel. Consider the exact sequence

$$0 \to R_G \to F_G \xrightarrow{\bar{\pi}} A_G \to 0$$

that exists since $H_1(G,A) = 0$. We have by definition that the map $\bar{\pi}$ induced by π is an isomorphism, so we must have $R_G = 0$. As $pR = 0$, we have by Lemma A.11.4 that $R = 0$, and so π is an isomorphism. □

We are now ready to give a module-theoretic characterization of cohomologically trivial modules that are killed by p.

PROPOSITION A.11.6. *Suppose that G is a p-group and that A is a G-module of exponent dividing p. The following are equivalent:*

(i) A is cohomologically trivial

(ii) A is a free $\mathbb{F}_p[G]$-module.

(iii) There exists $i \in \mathbb{Z}$ such that $\hat{H}^i(G,A) = 0$.

PROOF.

(i) $\Rightarrow$ (iii) Immediate.

(i) $\Rightarrow$ (ii) This is a special case of Lemma A.11.5, since $H_1(G,A) \cong \hat{H}^{-2}(G,A)$.

(ii) $\Rightarrow$ (i) Suppose A is free over $\mathbb{F}_p[G]$ on a generating set I. Then

$$A \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} \bigoplus_{i \in I} \mathbb{F}_p,$$

so A is induced, hence cohomologically trivial.

(iii) $\Rightarrow$ (ii) We note that the modules A_* and A^* that we use to dimension shift, as in (A.7.2) and (A.7.1) are killed by p since A is. In particular, it follows by dimension shifting that there exists a G-module B such that $pB = 0$ and

$$\hat{H}^{j-2}(H,B) \cong \hat{H}^{j+i}(H,A)$$

for all $H \leq G$ and $j \in \mathbb{Z}$. In particular, $H_1(G,B) = \hat{H}^{-2}(G,B)$ is trivial. By Lemma A.11.5, B is $\mathbb{F}_p[G]$-free. However, we have just shown that this implies that B is cohomologically trivial, and therefore so is A.

□

We next consider the case that A has no elements of order p.

PROPOSITION A.11.7. *Suppose that G is a p-group and A is a G-module with no elements of order p. The following are equivalent:*

(i) A is cohomologically trivial.

(ii) There exists $i \in \mathbb{Z}$ such that $\hat{H}^i(G,A) = \hat{H}^{i+1}(G,A) = 0$.

(iii) A/pA is free over $\mathbb{F}_p[G]$.

PROOF.

(i) $\Rightarrow$ (ii) Immediate.

(ii) $\Rightarrow$ (iii) Since A has no p-torsion,

$$0 \to A \xrightarrow{p} A \to A/pA \to 0$$

is exact. By (ii) and the long exact sequence in Tate cohomology, we have $\hat{H}^i(G,A/pA) = 0$. By Proposition A.11.6, we have therefore that A/pA is free over $\mathbb{F}_p[G]$.

(iii) $\Rightarrow$ (i) By Proposition A.11.6, we have that A/pA is cohomologically trivial, and therefore multiplication by p is an isomorphism on each $\hat{H}^i(H,A)$ for each subgroup H of G and every $i \in \mathbb{Z}$. However, the latter cohomology groups are annihilated by the order of H, so must be trivial since H is a p-group.

□

We next wish to generalize to arbitrary finite groups.

PROPOSITION A.11.8. *Let G be a finite group and, for each p, choose a Sylow p-subgroup G_p of G. Let A be a G-module. Then A is cohomologically trivial if and only if A is cohomologically trivial as a G_p-module for each p.*

PROOF. Suppose that A is cohomologically trivial for all G_p. Let H be a subgroup of G. Any Sylow p-subgroup H_p of H is contained in a conjugate of G_p, say gG_pg^{-1}. By the cohomological

triviality of G_p, we have that $\hat{H}^i(g^{-1}H_pg,A) = 0$. As g^* is an isomorphism, we have that $\hat{H}^i(H_p,A) = 0$. Therefore, we see that the restriction map $\mathrm{Res}\colon \hat{H}^i(H,A) \to \hat{H}^i(H_p,A)$ is 0. Since this holds for each p, Corollary A.8.25 implies that $\hat{H}^i(H,A) = 0$. □

In order to give a characterization of cohomologically trivial modules in terms of projective modules, we require the following lemma.

LEMMA A.11.9. *Suppose that G is a p-group and A is a G-module that is free as an abelian group and cohomologically trivial. For any G-module B which is p-torsion free, we have that* $\mathrm{Hom}_{\mathbb{Z}}(A,B)$ *is cohomologically trivial.*

PROOF. Since B has no p-torsion and A is free over $\mathbb{Z}$, we have that

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(A,B) \xrightarrow{p} \mathrm{Hom}_{\mathbb{Z}}(A,B) \to \mathrm{Hom}_{\mathbb{Z}}(A,B/pB) \to 0$$

is exact. In particular, $\mathrm{Hom}_{\mathbb{Z}}(A,B)$ has no p-torsion, and

$$\mathrm{Hom}_{\mathbb{Z}}(A/pA,B/pB) \cong \mathrm{Hom}_{\mathbb{Z}}(A,B/pB) \cong \mathrm{Hom}_{\mathbb{Z}}(A,B)/p\,\mathrm{Hom}_{\mathbb{Z}}(A,B).$$

Since A/pA is free over $\mathbb{F}_p[G]$ with some indexing set that we shall call I, we have

$$\mathrm{Hom}_{\mathbb{Z}}(A/pA,B/pB) \cong \prod_{i\in I}\mathrm{Hom}_{\mathbb{Z}}(\mathbb{F}_p[G],B/pB) \cong \mathrm{Hom}_{\mathbb{Z}}\Big(\mathbb{Z}[G],\prod_{i\in I}B/pB\Big),$$

so $\mathrm{Hom}_{\mathbb{Z}}(A,B/pB)$ is coinduced, and therefore $\mathbb{F}_p[G]$-free. By Proposition A.11.7, we have that $\mathrm{Hom}_{\mathbb{Z}}(A,B)$ is cohomologically trivial. □

PROPOSITION A.11.10. *Let G be a finite group and A a G-module that is free as an abelian group. Then A is cohomologically trivial if and only if A is a projective G-module.*

PROOF. We have already seen that projective implies cohomologically trivial. Suppose that A is cohomologically trivial as a G-module. Since A is $\mathbb{Z}$-free, it follows that $\mathrm{Ind}^G(A)$ is a free G-module, and the sequence

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(A,A_*) \to \mathrm{Hom}_{\mathbb{Z}}(A,\mathrm{Ind}^G(A)) \to \mathrm{Hom}_{\mathbb{Z}}(A,A) \to 0 \tag{A.11.1}$$

is exact. Moreover, A_* is rather clearly $\mathbb{Z}$-free since A is, so it follows from Lemma A.11.9 that the module $\mathrm{Hom}_{\mathbb{Z}}(A,A_*)$ is cohomologically trivial. In particular, by the long exact sequence in cohomology attached to (A.11.1), we see that

$$\mathrm{Hom}_{\mathbb{Z}[G]}(A,\mathrm{Ind}^G(A)) \to \mathrm{Hom}_{\mathbb{Z}[G]}(A,A)$$

is surjective. In particular, the identity map lifts to a homomorphism $A \to \mathrm{Ind}^G(A)$, which is a splitting of the natural surjection $\mathrm{Ind}^G(A) \to A$. It follows that A is projective as a G-module. □

Finally, we consider the general case.

THEOREM A.11.11. *Let G be a finite group and A a G-module. The following are equivalent.*

(i) A is cohomologically trivial.

(ii) For each prime p, there exists some $i \in \mathbb{Z}$ such that $\hat{H}^i(G_p, A) = \hat{H}^{i+1}(G_p, A) = 0$.

(iii) There is an exact sequence of G-modules

$$0 \to P_1 \to P_0 \to A \to 0$$

in which P_0 and P_1 are projective.

PROOF.

(i) $\Rightarrow$ (ii) This follows from the definition of cohomologically trivial.

(ii) $\Rightarrow$ (iii) Let F be a free G-module that surjects onto A, and let R be the kernel. As F is cohomologically trivial, we have $\hat{H}^{j-1}(G_p, A) \cong \hat{H}^j(G_p, R)$ for every $j \in \mathbb{Z}$. It follows that $\hat{H}^j(G_p, R)$ vanishes for two consecutive values of j. Since R is $\mathbb{Z}$-free, being a subgroup of F, we have by Propositions A.11.7, A.11.8, and A.11.10 that R is projective.

(iii) $\Rightarrow$ (i) This follows from the fact that projective modules are cohomologically trivial and the long exact sequence in Tate cohomology.

□

A.12. Tate's theorem

We continue to assume that G is a finite group, and we choose a Sylow p-subgroup G_p of G for each prime p. We begin with a consequence of our characterization of cohomologically trivial modules to maps on cohomology.

PROPOSITION A.12.1. *Let $\kappa\colon A \to B$ be a G-module homomorphism. Viewed as a G_p-module homomorphism, let us denote it by κ_p. Suppose that, for each prime p, there exists a $j \in \mathbb{Z}$ such that*

$$\kappa_p^*\colon \hat{H}^i(G_p, A) \to \hat{H}^i(G_p, B)$$

is surjective for $i = j-1$, an isomorphism for $i = j$, and injective for $i = j+1$. Then

$$\kappa^*\colon \hat{H}^i(H, A) \to \hat{H}^i(H, B)$$

is an isomorphism for all $i \in \mathbb{Z}$ and subgroups H of G.

PROOF. Consider the canonical injection of G-modules

$$\kappa \oplus \iota\colon A \to B \oplus \mathrm{CoInd}^G(A),$$

and let C be its cokernel. As $\mathrm{CoInd}^G(A)$ is H-cohomologically trivial for all $H \leq G$, we have

$$\hat{H}^i(H, B \oplus \mathrm{CoInd}^G(A)) \cong \hat{H}^i(H, B)$$

for all $i \in \mathbb{Z}$. The long exact sequence in G_p-cohomology then reads

$$\cdots \to \hat{H}^i(G_p,A) \xrightarrow{\kappa_p^*} \hat{H}^i(G_p,B) \to \hat{H}^i(G_p,C) \xrightarrow{\delta} \hat{H}^{i+1}(G_p,A) \xrightarrow{\kappa_p^*} \hat{H}^{i+1}(G_p,B) \to \cdots.$$

Consider the case $i = j-1$. The map κ_p^* being surjective on $\hat{H}^{j-1}$ and injective on $\hat{H}^j$ implies that $\hat{H}^{j-1}(G_p,C) = 0$. Similarly, for $i = j$, the map κ_p^* being surjective on $\hat{H}^j$ and injective on $\hat{H}^{j+1}$ implies that $\hat{H}^j(G_p,C) = 0$. Therefore, C is cohomologically trivial by Theorem A.11.11, and so each map $\kappa^*\colon \hat{H}^i(H,A) \to \hat{H}^i(H,B)$ in question must be an isomorphism by the long exact sequence in Tate cohomology. □

We now prove the main theorem of Tate and Nakayama.

THEOREM A.12.2. *Suppose that A, B, and C are G-modules and*

$$\theta\colon A \otimes_{\mathbb{Z}} B \to C$$

is a G-module map. Let $k \in \mathbb{Z}$ and $\alpha \in \hat{H}^k(G,A)$. For each subgroup H of G, define

$$\Theta^i_{H,\alpha}\colon \hat{H}^i(H,B) \to \hat{H}^{i+k}(H,C), \qquad \Theta^i_{H,\alpha}(\beta) = \theta^*(\mathrm{Res}(\alpha) \cup \beta).$$

For each prime p, suppose that there exists $j \in \mathbb{Z}$ such that the map $\Theta^i_{G_p,\alpha}$ is surjective for $i = j-1$, an isomorphism for $i = j$, and injective for $i = j+1$. Then for every subgroup H of G and $i \in \mathbb{Z}$, one has that $\Theta^i_{H,\alpha}$ is an isomorphism.

PROOF. First consider the case that $k = 0$. Then the map $\psi\colon B \to C$ given by $\psi(b) = \theta(a \otimes b)$, where $a \in A^G$ represents α, is a map of G-modules, since

$$\psi(gb) = \theta(a \otimes gb) = \theta(ga \otimes gb) = g\theta(a \otimes b) = g\psi(b).$$

We claim that the induced maps on cohomology

$$\psi^*\colon \hat{H}^i(H,B) \to \hat{H}^i(H,C)$$

agree with the maps given by left cup product with $\mathrm{Res}(\alpha)$. Given this, we have by Proposition A.12.1 that the latter maps are all isomorphisms in the case $k = 0$.

To see the claim, consider first the case that $i = 0$, in which the map ψ^* is induced by $\psi\colon B^H \to C^H$. For $b \in B^H$, we have $\psi(b) = \theta(a \otimes b)$, and the class of the latter term is $\theta^*(\mathrm{Res}(a) \cup b)$ by (i) of Theorem A.9.12. For the case of arbitrary i, we consider the commutative diagram

(A.12.1)
$$\begin{array}{ccccccccc}
0 & \longrightarrow & (A \otimes_{\mathbb{Z}} B)_* & \longrightarrow & \mathrm{Ind}^G(A \otimes_{\mathbb{Z}} B) & \longrightarrow & A \otimes_{\mathbb{Z}} B & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \tilde{\theta}} & & \downarrow{\scriptstyle \mathrm{Ind}^G(\theta)} & & \downarrow{\scriptstyle \theta} & & \\
0 & \longrightarrow & C_* & \longrightarrow & \mathrm{Ind}^G(C) & \longrightarrow & C & \longrightarrow & 0,
\end{array}$$

where $\mathrm{Ind}^G(\theta) = \mathrm{id}_{\mathbb{Z}[G]} \otimes \theta$, and where $\tilde{\theta}$ is both the map making the diagram commute and $\mathrm{id}_{I_G} \otimes \theta$, noting Remark A.7.1. In fact, by Remark A.9.6, we have an exact sequence isomorphic to the top row of (A.12.1), given by

$$0 \to A \otimes_{\mathbb{Z}} B_* \to A \otimes_{\mathbb{Z}} \mathrm{Ind}^G(B) \to A \otimes_{\mathbb{Z}} B \to 0$$

and then a map $\tilde{\psi}\colon B_* \to C_*$ given by $\tilde{\psi}(b') = \tilde{\theta}(a \otimes b')$ for $b' \in B_*$. We then have two commutative diagrams

$$\begin{array}{ccc} \hat{H}^{i-1}(H,B) & \xrightarrow[\sim]{\delta} & \hat{H}^i(H,B_*) \\ \downarrow & & \downarrow \\ \hat{H}^{i-1}(H,C) & \xrightarrow[\sim]{\delta} & \hat{H}^i(H,C_*). \end{array}$$

In the first, the left vertical arrow is $\Theta^{i-1}_{H,\alpha}$ and the right vertical arrow is the map $\tilde{\Theta}^i_{H,\alpha}$ given on $\beta' \in \hat{H}^i(H,B_*)$ by

$$\tilde{\Theta}^i_{H,\alpha}(\beta') = \tilde{\theta}^*(\mathrm{Res}(\alpha) \cup \beta').$$

In the second, the left vertical arrow is ψ^* and the right is $\tilde{\psi}^*$. Supposing our claim for i, we have $\tilde{\psi}^* = \tilde{\Theta}^i_{H,\alpha}$. As the connecting homomorphisms in the diagrams are isomorphisms, we then have that $\psi^* = \Theta^i_{H,\alpha}$. I.e., if the claim holds for i, it holds for $i-1$. The analogous argument using coinduced modules allows us to shift from i to $i+1$, proving the claim for all $i \in \mathbb{Z}$, hence the theorem for $k = 0$.

For any $k \in \mathbb{Z}$, the result is again proven by dimension shifting, this time for A. Fix $\alpha \in \hat{H}^{k-1}(H,A)$, and let $\alpha' = \delta(\alpha) \in \hat{H}^k(H,A_*)$. We note that the top row of (A.12.1) is also isomorphic to

$$0 \to A_* \otimes_{\mathbb{Z}} B \to \mathrm{Ind}^G(A) \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B \to 0.$$

Much as before, define $\Theta^i_{H,\alpha'}\colon \hat{H}^i(H,B) \to \hat{H}^{i+k}(H,C_*)$ by $\Theta^i_{H,\alpha'}(\beta) = \tilde{\theta}^*(\mathrm{Res}(\alpha') \cup \beta)$, where $\tilde{\theta}\colon A_* \otimes_{\mathbb{Z}} B \to C_*$ is the map determined by θ. The diagram

$$\begin{array}{ccc} \hat{H}^i(H,B) & = & \hat{H}^i(H,B) \\ \downarrow{\scriptstyle \Theta^i_{H,\alpha}} & & \downarrow{\scriptstyle \Theta^i_{H,\alpha'}} \\ \hat{H}^{i+k-1}(H,C) & \xrightarrow[\sim]{\delta} & \hat{H}^{i+k}(H,C_*) \end{array}$$

then commutes as

$$\delta \circ \Theta^i_{H,\alpha}(\beta) = \delta \circ \theta^*(\mathrm{Res}(\alpha) \cup \beta) = \tilde{\theta}^* \delta(\mathrm{Res}(\alpha) \cup \beta) = \tilde{\theta}^*(\mathrm{Res}(\alpha') \cup \beta) = \Theta^i_{H,\alpha'}(\beta).$$

There exists by assumption $j \in \mathbb{Z}$ such that the map $\Theta^i_{G_p,\alpha}$ is surjective for $i = j-1$, an isomorphism for $i = j$, and injective for $i = j+1$. By the commutativity of the diagram, the same holds for $\Theta^i_{G_p,\alpha'}$. Assuming the theorem for k, we then have that all of the maps $\Theta^i_{H,\alpha'}$ are isomorphisms, and therefore again by commutativity that so are the maps $\Theta^i_{H,\alpha}$. Thus, the theorem for a given k implies the

theorem for $k-1$. By the analogous argument using coinduced modules, the theorem for k implies the theorem for $k+1$ as well. □

The following special case was first due to Tate.

THEOREM A.12.3 (Tate). *Let A be a G-module, and let $\alpha \in H^2(G,A)$. Suppose that, for every p, the group $H^1(G_p,A)$ is trivial and $H^2(G_p,A)$ is a cyclic group of order $|G_p|$ generated by the restriction of α. Then the maps*

$$\hat{H}^i(H,\mathbb{Z}) \to \hat{H}^{i+2}(H,A), \qquad \beta \mapsto \mathrm{Res}(\alpha) \cup \beta$$

are isomorphisms for every $i \in \mathbb{Z}$ and subgroup H of G.

PROOF. For $H = G_p$, the maps in question are surjective for $i = -1$, as $H^1(G_p,A) = 0$, and injective for $i = 1$, as

$$H^1(G_p,\mathbb{Z}) = \mathrm{Hom}(G_p,\mathbb{Z}) = 0.$$

For $i = 0$, we have

$$\hat{H}^0(G_p,\mathbb{Z}) \cong \mathbb{Z}/|G_p|\mathbb{Z},$$

and the map takes the image of $n \in \mathbb{Z}$ to $n\mathrm{Res}(\alpha)$ (which is straightforward enough to see by dimension shifting, starting with the known case of cup products of degree zero classes), hence is an isomorphism by the assumption on $H^2(G_p,A)$. □

APPENDIX B

Galois cohomology

B.1. Profinite groups

DEFINITION B.1.1. A *topological group* G is a group endowed with a topology with respect to which both the multiplication map $G \times G \to G$ and the inversion map $G \to G$ that takes an element to its inverse are continuous.

EXAMPLES B.1.2.

a. The groups $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^\times$, and $\mathbb{C}^\times$ are continuous with respect to the topologies defined by their absolute values.

b. Any group can be made a topological group by endowing it with the discrete topology.

REMARK B.1.3. We may consider the category of topological groups, in which the maps are continuous homomorphisms between topological groups.

DEFINITION B.1.4. A homomorphism $\phi\colon G \to G'$ between topological groups G and G' is a *topological isomorphism* if it is both an isomorphism and a homeomorphism.

The following lemma is almost immediate, since elements of a group are invertible.

LEMMA B.1.5. *Let G be a topological group and $g \in G$. Then the map $m_g\colon G \to G$ with $m_g(a) = ga$ for all $a \in G$ is a homeomorphism.*

We also have the following.

LEMMA B.1.6. *A group homomorphism $\phi\colon G \to G'$ between topological groups is continuous if and only if, for each open neighborhood U of 1 in G' with $1 \in U$, the set $\phi^{-1}(U)$ contains an open neighborhood of 1.*

PROOF. We consider the non-obvious direction. Let V be an open set in G', and suppose that $g \in G$ is such that $h = \phi(g) \in V$. Then $h^{-1}V$ is open in G' as well, by Lemma B.1.5. By assumption, there exists an open neighborhood W of 1 in G contained in $\phi^{-1}(h^{-1}V)$, and so gW is an open neighborhood of g in G such that $\phi(gW) \subseteq V$. Hence, ϕ is continuous. □

LEMMA B.1.7. *Let G be a topological group.*

a. Any open subgroup of G is closed.

b. Any closed subgroup of finite index in G is open.

PROOF. If H is an open (resp., closed) subgroup of G, then its cosets are open (resp., closed) as well. Moreover, $G-H$ is the union of the nontrivial cosets of H. Therefore, $G-H$ is open if G is open and closed if G is closed of finite index, so that there are only finitely many cosets of H. □

LEMMA B.1.8. *Every open subgroup of a compact group G is of finite index in G.*

PROOF. Let H be a open subgroup of G. Note that G is the union of its distinct H-cosets, which are open and disjoint. Since G is compact, there can therefore only be finitely many cosets, which is to say that H is of finite index in G. □

We leave it to the reader to verify the following.

LEMMA B.1.9.

a. A subgroup of a topological group is a topological group with respect to the subspace topology.

b. The quotient of a topological group G by a normal subgroup N is a topological group with respect to the quotient topology, and it is Hausdorff if N is closed.

c. A direct product of topological groups is a topological group with respect to the product topology.

Recall the definitions of a directed set, inverse system, and the inverse limit.

DEFINITION B.1.10. A *directed set* $I=(I,\geq)$ is a partially ordered set such that for every $i,j\in I$, there exists $k\in I$ with $k\geq i$ and $k\geq j$.

DEFINITION B.1.11. Let I be a directed set. An *inverse system* $(G_i,\phi_{i,j})$ of groups over the indexing set I is a set

$$\{G_i \mid i\in I\}$$

of groups and a set

$$\{\phi_{i,j}\colon G_i\to G_j \mid i,j\in I, i\geq j\}$$

of group homomrphisms.

DEFINITION B.1.12. An *inverse limit*

$$G=\varprojlim_i G_i$$

of an inverse system of groups $(G_i,\phi_{i,j})$ over a directed indexing set I is a pair $G=(G,\{\pi_i \mid i\in I\})$ consisting of a group G and homomorphisms $\pi_i\colon G\to G_i$ such that $\phi_{i,j}\circ\pi_i=\pi_j$ for all $i,j\in I$ with $i\geq j$ that satisfy the following universal property: Given a group G' and maps $\pi_i'\colon G'\to G_i$ for $i\in I$ such that $\phi_{i,j}\circ\pi_i'=\pi_j'$ for all $i\geq j$, there exists a unique map $\psi\colon G'\to G$ such that $\pi_i'=\pi_i\circ\psi$ for all $i\in I$.

By the universal property, any two inverse limits of an inverse system of groups are canonically isomorphic (via compatible maps).

REMARK B.1.13. We may make the latter definition more generally with any category $\mathscr{C}$ replacing the category of groups. The groups are replaced with objects in $\mathscr{C}$ and the group homomorphisms with morphisms in $\mathscr{C}$. Moreover, we may view the system of groups as a covariant functor to the category $\mathscr{C}$ from the category that has the elements of I as its objects and morphisms $i \to j$ for each $i, j \in I$ with $i \geq j$.

We may give a direct construction of an inverse limit of an inverse system of groups as follows. The proof is left to the reader.

PROPOSITION B.1.14. *Let $(G_i, \phi_{i,j})$ be an inverse system of groups over an indexing set I. Then the an inverse limit of the system is given explicitly by the group*

$$G = \left\{ (g_i)_i \in \prod_{i \in I} G_i \mid \phi_{i,j}(g_i) = g_j \right\}$$

and the maps $\pi_i \colon G \to G_i$ for $i \in I$ that are the compositions of the $G \to \prod_{i \in I} G_i \to G_i$ of inclusion followed by projection.

We may endow an inverse limit of groups with a topology as follows.

DEFINITION B.1.15. Let $(G_i, \phi_{i,j})$ be an inverse system of topological groups over an indexing set I, with continuous maps. Then the *inverse limit topology* on the inverse limit G of Proposition B.1.14 is the subspace topology for the product topology on $\prod_{i \in I} G_i$.

LEMMA B.1.16. *The inverse limit of an inverse system $(G_i, \phi_{i,j})$ of topological groups (over a directed indexing set I) is a topological group under the inverse limit topology.*

PROOF. The maps

$$\prod_{i \in I} G_i \times \prod_{i \in I} G_i \to \prod_{i \in I} G_i \quad \text{and} \quad \prod_{i \in I} G_i \to \prod_{i \in I} G_i$$

given by componentwise multiplication and inversion are clearly continuous, and this continuity is preserved under the subspace topology on the inverse limit. □

REMARK B.1.17. In fact, the inverse limit of an inverse system of topological groups and continuous maps, when endowed with the product topology, is an inverse limit in the category of topological groups.

When we wish to view it as a topological group, we typically endow a finite group with the discrete topology.

DEFINITION B.1.18. A *profinite group* is an inverse limit of a system of finite groups, endowed with the inverse limit topology for the discrete topology on the finite groups.

Recall the following definition.

DEFINITION B.1.19. A topological space is *totally disconnected* if and only if every point is a connected component.

We leave the following as difficult exercises.

PROPOSITION B.1.20. *A compact Hausdorff space is totally disconnected if and only if it has a basis of open neighborhoods that are also closed.*

PROPOSITION B.1.21. *A compact Hausdorff group that is totally disconnected has a basis of neighborhoods of* 1 *consisting of open normal subgroups (of finite index).*

We may now give a topological characterization of profinite groups.

THEOREM B.1.22. *A profinite topological group G is compact, Hausdorff, and totally disconnected.*

PROOF. First, suppose that G is profinite, equal to an inverse limit of a system $(G_i, \phi_{i,j})$ of finite groups over an indexing set I. The direct product $\prod_{i\in I} G_i$ of finite (discrete) groups G_i is compact Hausdorff (compactness being Tychonoff's theorem). As a subset of the direct product, G is Hausdorff, and to see it is compact, we show that G is closed. Suppose that

$$(g_i)_i \in \prod_{i\in I} G_i$$

with $(g_i)_i \notin G$, and choose $i, j \in I$ with $i > j$ and $\phi_{i,j}(g_i) \neq g_j$. The open subset

$$\left\{ (h_k)_k \in \prod_{k\in I} G_k \mid h_i = g_i, h_j = g_j \right\}$$

of the direct product contains $(g_i)_i$ and has trivial intersection with G. In that the complement of G is open, G itself is closed. Finally, note that any open set $\prod_{i\in I} U_i$ with each U_i open in G_i (i.e., an arbitrary subset) and $U_i = G_i$ for all but finitely many i is also closed. That is, its complement is the intersection

$$\bigcap_{j\in I} \left((G_j - U_j) \times \prod_{i\in I-\{j\}} U_i \right)$$

of open sets, which is actually equal to the finite intersection over $j \in I$ with $U_i \neq G_i$. It is therefore open, and by Proposition B.1.20, the group G is totally disconnected. □

REMARK B.1.23. We leave it to the reader to check that the converse to Theorem B.1.22 also holds. They key is found in the proof of part a of the following proposition.

PROPOSITION B.1.24. *Let G be a profinite group, and let $\mathscr{U}$ be the set of all open normal subgroups of G. Then the following canonical homomorphisms are homeomorphisms:*

a. $G \to \varprojlim_{N\in\mathscr{U}} G/N$,

b. $H \to \varprojlim_{N\in\mathscr{U}} H/(H\cap N)$, *for H a closed subgroup of G, and*

c. $G/K \to \varprojlim_{N\in\mathscr{U}} G/NK$, *for K a closed normal subgroup of G.*

PROOF. We prove part *a*. The continuous map ϕ from G to the inverse limit Q of its quotients has closed image, and ϕ is injective since $\mathscr{U}$ is a basis of 1 in G as in Proposition B.1.21. Suppose that $(g_N N)_{N\in\mathscr{U}}$ is not in the image of ϕ, which is exactly to say that the intersection of the closed sets $g_N N$ is empty. Since G is compact this implies that some finite subset of the $\{g_N N \mid N \in \mathscr{U}\}$ is empty, and letting M be the intersection of the N in this subset, we see that $g_M M = \varnothing$, which is a contradiction. In other words, ϕ is surjective. □

The following is a consequence of Proposition B.1.24a. We leave the proof to the reader.

COROLLARY B.1.25. *Let G be a profinite group and $\mathscr{V}$ a set of open normal subgroups of G that forms a basis of open neighborhoods of* 1. *Then the homomorphism*

$$G \to \varprojlim_{N\in\mathscr{V}} G/N$$

is a homeomorphism.

The following lemma will be useful later.

LEMMA B.1.26. *The closed subgroups of a profinite group are exactly those that may be written as intersections of open subgroups.*

PROOF. In a topological group, an open subgroup is also closed, an arbitrary intersection of closed sets is closed, and an arbitrary intersection of subgroups is a subgroup, so an intersection of open subgroups is a closed subgroup. Let $\mathscr{U}$ denote the set of open subgroups of a profinite group G. Let H be a closed subgroup of G. It follows from Proposition B.1.24b and the second isomorphism theorem that the set of subgroups of the form NH with N open normal in G has intersection H. Note that each NH is open as a union of open subgroups, so it is open. □

We may also speak of pro-p groups.

DEFINITION B.1.27. A *pro-p group*, for a prime p, is an inverse limit of a system of finite p-groups.

We may also speak of profinite and pro-p completions of groups.

DEFINITION B.1.28. Let G be a group.

a. The *profinite completion* $\hat{G}$ of G is the inverse limit of its finite quotients G/N, for N a normal subgroup of finite index in G, together with the natural quotient maps $G/N \to G/N'$ for $N \leq N'$.

b. The *pro-p completion* $G^{(p)}$ of G, for a prime p, is the inverse limit of the finite quotients of G of p-power order, i.e., of the G/N for $N \trianglelefteq G$ with $[G:N]$ a power of p, together with the natural quotient maps.

REMARK B.1.29. A group G is endowed with a canonical homomorphism to its profinite completion $\hat{G}$ by the universal property of the inverse limit.

REMARK B.1.30. We may also speak of topological rings and fields, where multiplication, addition, and the additive inverse map are continuous, and in the case of a topological field, the multiplicative inverse map on the multiplicative group is continuous as well. We may speak of profinite rings as inverse limits by quotients by two-sided ideals of finite index (or for pro-p rings, of p-power index).

The next proposition shows that $\mathbb{Z}_p$ is the pro-p completion of $\mathbb{Z}$.

PROPOSITION B.1.31. *Let p be a prime. We have an isomorphism of rings*

$$\psi\colon \mathbb{Z}_p \xrightarrow{\sim} \varprojlim_{k\geq 1} \mathbb{Z}/p^k\mathbb{Z}, \qquad \sum_{i=0}^{\infty} a_i p^i \mapsto \left(\sum_{i=0}^{k-1} a_i p^i\right)_k,$$

where the maps $\mathbb{Z}/p^{k+1}\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ in the system are the natural quotient maps. Moreover, ψ is a homeomorphism.

PROOF. The canonical quotient map $\psi_k\colon \mathbb{Z}_p \to \mathbb{Z}/p^k\mathbb{Z}$ is the kth coordinate of ψ, which is then a ring homomorphism by the universal property of the inverse limit. The kernel ψ is the intersection of the kernels of the maps ψ_k, which is exactly

$$\bigcap_k p^k\mathbb{Z}_p = 0.$$

Moreover, any sequence of partial sums modulo increasing powers of p has a limit in $\mathbb{Z}_p$, which maps to the sequence under ψ. The open neighborhood $p^n\mathbb{Z}_p$ of 0 in the p-adic topology is sent to the intersection

$$\left(\prod_{k=1}^{n}\{0\} \times \prod_{k=n+1}^{\infty} \mathbb{Z}_p/p^k\mathbb{Z}_p\right) \cap \left(\varprojlim_{k\geq 1} \mathbb{Z}/p^k\mathbb{Z}\right),$$

which is open in the product topology. On the other hand, the inverse image of a basis open neighborhood

$$\left(\prod_{k=1}^{n} U_k \times \prod_{k=n+1}^{\infty} \mathbb{Z}_p/p^k\mathbb{Z}_p\right) \cap \left(\varprojlim_{k\geq 1} \mathbb{Z}/p^k\mathbb{Z}\right)$$

with $0 \in U_k$ for all $1 \leq k \leq n$ under ψ clearly contains $p^n\mathbb{Z}_p$. It then follows from Lemma B.1.6 that ψ is a homeomorphism. □

DEFINITION B.1.32. The *Prüfer ring* $\hat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$. That is, we have

$$\mathbb{Z} \cong \varprojlim_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$$

with respect to the quotient maps $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ for $m \mid n$.

Since $\mathbb{Z}/n\mathbb{Z}$ may be written as a direct product of the $\mathbb{Z}/p^k\mathbb{Z}$ for primes p with p^k exactly dividing n, we have the following.

LEMMA B.1.33. *We have an isomorphism of topological rings*

$$\hat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p.$$

EXAMPLE B.1.34. The free profinite (or pro-p) group on a generating set S is the profinite (resp., pro-p) completion of the free group on S.

REMARK B.1.35. As with free groups, closed subgroups of free profinite (or pro-p) groups are free profinite (or pro-p) groups. Moreover, every profinite (resp., pro-p) group is a topological quotient of the free group on a set of its generators, so we may present such groups via generators and relations much as before.

DEFINITION B.1.36. A subset S of a topological group G is said to be a *topological generating set* of G if G is the closure of the subgroup generated by S.

DEFINITION B.1.37. We say that a topological group is *(topologically) finitely generated* if it has a finite set of topological generators.

REMARK B.1.38. If G is a free profinite (or pro-p) group on a set S, then it is topologically generated by S.

We leave a proof of the following to the reader.

LEMMA B.1.39. *Let G be a topological group, and let H be a (normal) subgroup. Then the closure $\overline{H}$ of H is also a (normal) subgroup of G.*

DEFINITION B.1.40. The Frattini subgroup $\Phi(G)$ of a pro-p group G, where p is a prime, is smallest closed normal subgroup containing the commutator subgroup $[G,G]$ and the pth powers in G.

The following lemma is a consequence of the well-known case of finite p-groups.

LEMMA B.1.41. *Let G be a pro-p group for a prime p. Then $\Phi(G)$ is normal in G, and a subset S of G generates G if and only if its image in $G/\Phi(G)$ generates $G/\Phi(G)$.*

REMARK B.1.42. In the case that G is an abelian pro-p group, the Frattini subgroup $\Phi(G)$ in Lemma B.1.41 is G^p.

Finally, we state without proof the structure theorem for (topologically) finitely generated abelian pro-p groups. In fact, this is an immediate consequence of the structure theorem for finitely generated modules over a PID.

THEOREM B.1.43. *Let A be a topologically finitely generated abelian pro-p group. Then there exist $r,k \geq 0$ and $n_1 \geq n_2 \geq \cdots \geq n_k \geq 1$ such that we have an isomorphism*

$$A \cong \mathbb{Z}_p^r \oplus \mathbb{Z}/p^{n_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{n_k}\mathbb{Z}$$

of topological groups.

B.2. Cohomology of profinite groups

In this section, G will denote a topological group.

DEFINITION B.2.1. A *topological G-module A* is an abelian topological group such that the map $G \times A \to A$ defining the action of G on A is continuous.

DEFINITION B.2.2. A G-module A is *discrete* if it is a topological G-module for the discrete topology on A.

PROPOSITION B.2.3. *Let G be a profinite group, and let A be a G-module. The following are equivalent:*

i. A is discrete,

ii. $A = \bigcup_{N \in \mathscr{U}} A^N$, where $\mathscr{U}$ is the set of open normal subgroups of G, and

iii. the stabilizer of each $a \in A$ is open in G.

PROOF. Let $\pi\colon G \times A \to A$ be the map defining the G-action on A. For $a \in A$, let G_a denote the stabilizer of a. If A is discrete, then $\pi^{-1}(a) \cap (G \times \{a\})$ is open and equal to $G_a \times \{a\}$, so G_a is open as well. Thus, (i) implies (iii). Conversely, suppose that (iii) holds. To see (i), it suffices to check that for any $a, b \in A$, then set $X_{a,b} = \{g \in G | ga = b\}$ is open. If $X_{a,b}$ is nonempty, then for any $g \in X_{a,b}$, we clearly have $X_{a,b} = G_b g$, which is open by the continuity of the multiplication on G. Thus, (iii) implies (i).

If G_a is open for a given $a \in A$, then as $\mathscr{U}$ is a base of open neighborhoods of 1 in G, there exists $N \in \mathscr{U}$ with $N \subseteq G_a$. In other words, $a \in A^N$. Thus (iii) implies (ii). Conversely, suppose that (ii) holds. Take $a \in A$ and let $N \in \mathscr{U}$ be such that $a \in A^N$. Since N has finite index in G, the stabilizer G_a is a finite union of N-cosets, so G_a is open as well. Thus (ii) implies (iii). □

REMARK B.2.4. Note that our notion of a discrete G-module A says only that the G-action on A is continuous with respect to the discrete topology, so A can be thought of as a topological module when endowed with said topology. It is possible that the discrete topology is not the unique topology that makes A a topological G-module. For instance, $\mathbb{Z}/2\mathbb{Z}$ acts on $\mathbb{R}$ by $x \mapsto -x$, and this is continuous with respect to both the discrete and the usual topology on $\mathbb{R}$.

EXAMPLES B.2.5.

a. Every trivial G-module is a discrete G-module.

b. If G is finite (with the discrete topology), then every G-module is discrete.

c. If G is profinite, then every finite G-module is necessarily discrete.

d. The action of $\mathbb{C}^\times$ on $\mathbb{C}$ by left multiplication gives $\mathbb{C}$ the structure of a $\mathbb{C}^\times$-module that is not discrete.

e. The action of $\hat{\mathbb{Z}}^\times$ on the group of roots of unity in $\mathbb{C}$ by $u\cdot\zeta = \zeta^u$, for $u \in \hat{\mathbb{Z}}^\times$ and ζ a root of unity, is discrete. Here, ζ^u is ζ raised to the power of any integer that is congruent to u modulo the order of ζ.

DEFINITION B.2.6. We say that a topological G-module A is *discrete* if its topology is the discrete topology.

DEFINITION B.2.7. For a topological G-module A and $i \in \mathbb{Z}$, the group of continuous i-cochains of G with A-coefficients is

$$C^i_{\text{cts}}(G,A) = \{f\colon G^i \to A \mid f \text{ continuous}\}.$$

LEMMA B.2.8. *Let A be a topological G-module. The usual differential d^i_A on $C^i(G,A)$ restricts to a map $d^i_A\colon C^i_{\text{cts}}(G,A) \to C^{i+1}_{\text{cts}}(G,A)$. Thus, $(C^{\cdot}_{\text{cts}}(G,A), d^{\cdot}_A)$ is a cochain complex.*

PROOF. Set $X = G^{i+1}$. Since $f \in C^i_{\text{cts}}(G,A)$ and the multiplication maps $G\times G \to G$ and $G\times A \to A$ are continuous, so are the $i+2$ maps $X \to A$ taking $(g_1,\dots,g_{i+1})$ to $g_1 f(g_2,\dots,g_{i+1})$, to $f(g_1,\dots,g_jg_{j+1},\dots,g_i)$ for some $1 \le j \le i$, and to $f(g_1,\dots,g_i)$. The alternating sum defining $d^i_A(f)$ from these $i+2$ maps is the composition of the diagonal map $X \to X^{i+2}$, the direct product $X^{i+2} \to A^{i+2}$ of the maps in question, and the alternating sum map $A^{i+2} \to A$. Since all of these maps are continuous, so is $d^i_A(f)$. □

REMARK B.2.9. In general, $C^{\cdot}(G,\ \cdot\ )$ is a left exact functor from the category of topological G-modules with continuous G-module homomorphisms to the category of abelian groups. However, it need not be exact.

PROPOSITION B.2.10. *Let G be a topological group. If*

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

is an exact sequence of discrete G-modules, then endowing A, B, and C with the discrete topology, the sequence

$$0 \to C^i_{\text{cts}}(G,A) \xrightarrow{\iota^i} C^i_{\text{cts}}(G,B) \xrightarrow{\pi^i} C^i_{\text{cts}}(G,C) \to 0$$

is exact for each i.

PROOF. We need only show right-exactness. Choose a set-theoretic splitting of $s\colon C \to B$ of π. In that B and C are discrete, s is necessarily continuous. For any continuous $f\colon G^i \to C$, the map $s \circ f\colon G^i \to B$ is therefore continuous, and $\pi^i(s \circ f) = f$. □

DEFINITION B.2.11. Let G be a profinite group and A a discrete G-module. The ith profinite cohomology group of G with coefficients in A is $H^i(G,A) = H^i(C^{\cdot}_{\mathrm{cts}}(G,A))$, where A is endowed with the discrete topology.

NOTATION B.2.12. If $f\colon A \to B$ is a G-module homomorphism between discrete G-modules A and B, where G is profinite, then the induced maps on cohomology are denoted $f^*\colon H^i(G,A) \to H^i(G,B)$.

As a corollary of Proposition B.2.10, any short exact sequence of discrete G-modules gives rise to a long exact sequence of profinite cohomology groups.

THEOREM B.2.13. *Suppose that*

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

is a short exact sequence of discrete G-modules. Then there is a long exact sequence of abelian groups

$$0 \to H^0(G,A) \xrightarrow{\iota^*} H^0(G,B) \xrightarrow{\pi^*} H^0(G,C) \xrightarrow{\delta^0} H^1(G,A) \to \cdots.$$

Moreover, this construction is natural in the short exact sequence in the sense of Theorem A.2.13.

REMARK B.2.14. If G is a profinite group and A is a discrete G-module, then $H^i(G,A)$ in the sense of Definition B.2.11 need not be the same as $H^i(G,A)$ in the sense of (abstract) group cohomology. They do, however, agree in the case that G is finite, since in that case G is a discrete group, and every cochain $G^i \to A$ is continuous. Whenever G is a profinite group and A is discrete, we take $H^i(G,A)$ to be the profinite cohomology group.

EXAMPLE B.2.15. For a pro-p group G, the first cohomology group $H^1(G,\mathbb{F}_p)$ consists of the continuous homomorphisms from G to $\mathbb{F}_p$. It is then canonically isomorphic to the $\mathbb{F}_p$-dual of $G/\Phi(G)$, with $\Phi(G)$ the Frattini subgroup. It follows from Lemma B.1.41 that the $\mathbb{F}_p$-dimension of $H^1(G,\mathbb{F}_p)$ is equal to the order of the smallest (topological) generating set of G.

The following proposition shows that profinite cohomology groups are direct limits of usual cohomology groups of finite groups under inflation maps.

PROPOSITION B.2.16. *Let G be a profinite group, and let $\mathscr{U}$ be the set of open normal subgroups of G. For each discrete G-module A, we have an isomorphism*

$$H^i(G,A) \cong \varinjlim_{N \in \mathscr{U}} H^i(G/N, A^N),$$

where the direct limit is taken with respect to inflation maps, and these isomorphisms are natural in A.

PROOF. It suffices to check that we have natural isomorphisms

$$C^i_{\text{cts}}(G,A) \cong \varinjlim_{N\in\mathscr{U}} C^i(G/N,A^N)$$

commuting with connecting homomorphisms. We verify the isomorphism, which then clearly has the other properties. Let $f\colon G^i \to A$ be continuous. Since G is compact and A is discrete, the image of f is finite. For each $a \in \operatorname{im} f$, let $M_a \in \mathscr{U}$ be such that $a \in A^{M_a}$. Then $M = \bigcap_{a\in\operatorname{im} f} M_a \in \mathscr{U}$, and $\operatorname{im} f \subset A^M$.

We next check that f factors through $(G/H)^i$ for an open subgroup $H \in \mathscr{U}$. For this, note that the continuity of f forces it to be constant on an open neighborhood of any $x \in G^i$, and inside such a neighborhood is a neighborhood of the form $x\prod_{j=1}^i H_j(x)$ with H_j an open normal subgroup of G. Take $H(x) = \bigcap_{j=1}^i H_j(x)$, which again is an open normal subgroup, so f is constant on $xH(x)^i$. Now G^i is covered by the $xH(x)^i$ for $x \in G^i$. Compactness of G^i tells us that is a finite subcover corresponding to some $x_1,\dots,x_n \in G^i$. The intersection $H = \bigcap_{k=1}^n H(x_k)$ is then such that f factors through $(G/H)^i$, since for any $y \in G^i$, we have $y \in x_kH(x_k)^i$ for some k, and therefore f is constant on $yH \subseteq x_iH(x_i)^i$. Thus f factors through $(G/H)^i$.

We have shown that f is the inflation of a map $(G/H)^i \to A^M$. If we take $N = H \cap M$, then f factors through a map $(G/N)^i \to A^N$, proving the result. □

The notion of a compatible pair passes to profinite group cohomology if we merely suppose that our map of profinite groups is continuous.

DEFINITION B.2.17. Let G and G' be profinite groups, A a discrete G-module and A' a G'-module. We say that a pair (ρ,λ) with $\rho\colon G' \to G$ a continuous group homomorphism and $\lambda : A \to A'$ a group homomorphism is *compatible* if

$$\lambda(\rho(g')a) = g'\lambda(a)$$

for all $a \in A$ and $g' \in G'$.

Consequently, we have inflation, restriction, and conjugation maps as in Definition A.8.6 and Proposition A.8.12 so long as the subgroup is taken to be closed, which ensures that it is a profinite group. By Proposition B.2.16 and exactness of the direct limit, it is easy to see that these maps are just direct limits of the analogous maps for usual group cohomology under inflation, as holds for any map on profinite cohomology induced by a compatible pair. In fact, we also have corestriction, defined simply as the direct limit of corestriction maps at finite level. Moreover, the inflation-restriction sequence is still exact, and this works for any closed normal subgroup. We state the higher degree version of this result for later use.

PROPOSITION B.2.18. *Let G be a profinite group, let N be a closed normal subgroup of G, and let A be a discrete G-module. Let $i \geq 1$, and suppose that $H^j(N,A) = 0$ for all $j \leq i-1$. Then the sequence*

$$0 \to H^i(G/N, A^N) \xrightarrow{\text{Inf}} H^i(G,A) \xrightarrow{\text{Res}} H^i(N,A)$$

is exact.

B.3. Galois theory of infinite extensions

Recall that an algebraic extension of fields L/K is Galois if it is normal, so that every polynomial in $K[x]$ that has a root in L splits completely, and separable, so that no irreducible polynomial in $K[x]$ has a double root in L. The Galois group $\mathrm{Gal}(L/K)$ of such an extension is the group of automorphisms of L that fix K.

In the setting of finite Galois extensions L/K, the subfields E of L containing K are in one-to-one correspondence with the subgroups H of $\mathrm{Gal}(L/K)$. In fact, the maps $E \mapsto \mathrm{Gal}(L/E)$ and $H \mapsto L^H$ give inverse bijections between these sets. This is not so in the setting of infinite Galois extensions, where there are rather more subgroups than there are subfields. To fix this issue, we place a topology on $\mathrm{Gal}(L/K)$ and consider only the closed subgroups under this topology. The above-described correspondences then work exactly as before.

PROPOSITION B.3.1. *Let L/K be a Galois extension of fields. Let $\mathscr{E}$ denote the set of finite Galois extensions of K contained in L, ordered by inclusion. This is a directed set. Let ρ be the map*

$$\rho\colon \mathrm{Gal}(L/K) \to \varprojlim_{E \in \mathscr{E}} \mathrm{Gal}(E/K)$$

defined by the universal property of the inverse limit, with the maps $\mathrm{Gal}(E'/K) \to \mathrm{Gal}(E/K)$ for $E, E' \in \mathscr{E}$ with $E \subseteq E'$ and the maps $\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$ for $E \in \mathscr{E}$ being restriction maps. Then ρ is an isomorphism.

PROOF. Let $\sigma \in \mathrm{Gal}(L/K)$. If $\sigma|_E = 1$ for all $E \in \mathscr{E}$, then since

$$L = \bigcup_{E \in \mathscr{E}} E,$$

we have that $\sigma = 1$. On the other hand, if elements $\sigma_E \in \mathrm{Gal}(E/K)$ for each $E \in \mathscr{E}$ are compatible under restriction, then define $\sigma \in \mathrm{Gal}(L/K)$ by $\sigma(\alpha) = \sigma_E(\alpha)$ if $\alpha \in E$. Then, if $\alpha \in E'$ for some $E' \in \mathscr{E}$ as well, then

$$\sigma_{E'}(\alpha) = \sigma_{E \cap E'}(\alpha) = \sigma_E(\alpha),$$

noting that $E \cap E' \in \mathscr{E}$. Therefore, σ is well-defined, and so ρ is bijective. □

Proposition B.3.1 gives us an obvious topology to place on the Galois group of a Galois extension.

DEFINITION B.3.2. Let L/K be a Galois extension of fields. The *Krull topology* on $\mathrm{Gal}(L/K)$ is the unique topology under which the set of $\mathrm{Gal}(L/E)$ for E/K finite Galois with $E \subseteq L$ forms a basis of open neighborhoods of 1.

REMARK B.3.3. The Krull topology agrees with the inverse limit topology induced by the isomorphism of Proposition B.3.1, since

$$1 \to \mathrm{Gal}(L/E) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K) \to 1$$

is exact. Therefore, if L/K is Galois, then $\mathrm{Gal}(L/K)$ is a topological group under the Krull topology.

LEMMA B.3.4. *Let L/K be a Galois extension of fields. The open subgroups in* $\mathrm{Gal}(L/K)$ *are exactly those subgroups of the form* $\mathrm{Gal}(L/E)$ *with E an intermediate field in L/K of finite degree over K.*

PROOF. First, let E be an intermediate field in L/K of finite degree. Let E' be the Galois closure of E in L, which is of finite degree over K. Then $\mathrm{Gal}(L/E')$ is an open normal subgroup under the Krull topology, contained in $\mathrm{Gal}(L/E)$. Since $\mathrm{Gal}(L/E)$ is then a union of left $\mathrm{Gal}(L/E')$-cosets, which are open, we have that $\mathrm{Gal}(L/E)$ is open.

Conversely, let H be an open subgroup in $\mathrm{Gal}(L/K)$. Then H contains $\mathrm{Gal}(L/E)$ for some finite Galois extension E/K in L. Any $\alpha \in L^H$, where L^H is the fixed field of H in L, is contained in $M^{\mathrm{Gal}(L/E)}$, where M is the Galois closure of $E(\alpha)$. Since the restriction map $\mathrm{Gal}(L/E) \to \mathrm{Gal}(M/E)$ is surjective, we then have $\alpha \in M^{\mathrm{Gal}(M/E)}$. But M/K is finite, so $M^{\mathrm{Gal}(M/E)} = E$ by the fundamental theorem of Galois theory. Thus $L^H \subseteq E$.

Let $\bar{H}$ be the image of H under the restriction map $\pi\colon \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$. As $\mathrm{Gal}(L/E) \leq H$, we have that $\pi^{-1}(\bar{H}) = H$. We remark that $\bar{H} = \mathrm{Gal}(E/L^H)$, since $\bar{H} = \mathrm{Gal}(E/E^{\bar{H}})$ by the fundamental theorem of Galois theory for finite extensions and $L^H = E^H = E^{\bar{H}}$. But $\pi^{-1}(\bar{H})$ is then $\mathrm{Gal}(L/L^H)$ as well. □

From this, we may derive the following.

LEMMA B.3.5. *Let L/K be a Galois extension of fields. The closed subgroups of* $\mathrm{Gal}(L/K)$ *are exactly those of the form* $\mathrm{Gal}(L/E)$ *for some intermediate field E in the extension L/K.*

PROOF. Under the Krull topology on $\mathrm{Gal}(L/K)$, the open subgroups are those of the form $\mathrm{Gal}(L/E)$ with E/K finite. By Lemma B.1.26, we have therefore that the closed subgroups are those that are intersections of $\mathrm{Gal}(L/E)$ over a set S of finite degree over K intermediate fields E. Any such intersection necessarily fixes the compositum $E' = \prod_{E \in S} E$, while if an element of $\mathrm{Gal}(L/K)$ fixes E', then it fixes every $E \in S$, so lies in the intersection. That is, any closed subgroup has the form

$$\mathrm{Gal}(L/E') = \bigcap_{E \in S} \mathrm{Gal}(L/E).$$

□

THEOREM B.3.6 (Fundamental theorem of Galois theory). *Let L/K be a Galois extension. Then there are inverse one-to-one, inclusion reversing correspondences*

$$\{\text{intermediate extensions in } L/K\} \underset{\theta}{\overset{\psi}{\rightleftarrows}} \{\text{closed subgroups of } \mathrm{Gal}(L/K)\}$$

given by $\psi(E) = \mathrm{Gal}(L/E)$ for any intermediate extension E in L/K and $\theta(H) = L^H$ for any closed subgroup H of $\mathrm{Gal}(L/K)$. These correspondences restrict to bijections between the normal extensions of K in L and the closed normal subgroups of $\mathrm{Gal}(L/K)$, as well as to bijections between the finite degree (normal) extensions of K in L and the open (normal) subgroups of $\mathrm{Gal}(L/K)$. Moreover, if E is normal over K (resp., $H \trianglelefteq \mathrm{Gal}(L/K)$ is closed), then restriction induces a topological isomorphism

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/E) \xrightarrow{\sim} \mathrm{Gal}(E/K)$$

(*resp.,* $\mathrm{Gal}(L/K)/H \xrightarrow{\sim} \mathrm{Gal}(L^H/K)$).

PROOF. We will derive this from the fundamental theorem of Galois theory for finite Galois extensions. Let E be an intermediate extension in L/K. Then $E \subseteq L^{\mathrm{Gal}(L/E)}$ by definition. Let $x \in L^{\mathrm{Gal}(L/E)}$. The Galois closure M of $E(x)$ in L is of finite degree over E. But every element of $\mathrm{Gal}(M/E)$ extends to an element of $\mathrm{Gal}(L/E)$, which fixes x. So $x \in M^{\mathrm{Gal}(M/E)}$, which equals E by fundamental theorem of Galois theory for finite Galois extensions. Since x was arbitrary, we have $E = L^{\mathrm{Gal}(L/E)}$. In other words, $\theta(\psi(E)) = E$.

Let H be a closed subgroup of $\mathrm{Gal}(L/K)$. In Lemma B.3.5, we saw that $H = \mathrm{Gal}(L/E)$ for some intermediate E in L/K. Since $E = L^{\mathrm{Gal}(L/E)} = L^H$ from what we have shown, we have that $H = \mathrm{Gal}(L/L^H)$. Therefore, $\psi(\theta(H)) = H$. It follows that we have the desired inclusion-reserving one-to-one correspondences. The other claims are then easily checked and are left to the reader. □

DEFINITION B.3.7. A *separable closure* of a field L is any field that contains all roots of all separable polynomials in L.

NOTATION B.3.8. We typically denote a separable closure of L by L^{sep}.

REMARK B.3.9. If one fixes an algebraically closed field Ω containing L, then there is a unique separable closure of L in Ω, being the subfield generated by the roots of all separable polynomials in $L[x]$.

DEFINITION B.3.10. The *absolute Galois group* of a field K is the Galois group

$$G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K),$$

where K^{sep} is a separable closure of K.

REMARK B.3.11. The absolute Galois group, despite the word "the", is not unique, but rather depends on the choice of separable closure. An isomorphism of separable closures gives rise to a canonical isomorphism of absolute Galois groups, however.

EXAMPLE B.3.12. Let q be a power of a prime number. Then there is a unique topological isomorphism $G_{\mathbb{F}_q} \xrightarrow{\sim} \hat{\mathbb{Z}}$ sending the Frobenius automorphism $\varphi_q\colon x \mapsto x^q$ to 1. To see this, note that $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \to \mathbb{Z}/n\mathbb{Z}$ given by sending φ_q to 1 is an isomorphism, and these give rise to compatible isomorphisms in the inverse limit

$$G_{\mathbb{F}_q} \xrightarrow{\sim} \varprojlim_n \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \xrightarrow{\sim} \varprojlim_n \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \hat{\mathbb{Z}}.$$

EXAMPLE B.3.13. Let $\mathbb{Q}(\mu_{p^\infty})$ denote the field given by adjoining all p-power roots of unity to $\mathbb{Q}$. Then

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \cong \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_p^\times$$

the middle isomorphisms arising from the p^nth cyclotomic characters.

TERMINOLOGY B.3.14. The isomorphism $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \to \mathbb{Z}_p^\times$ of Example B.3.13 called the *p-adic cyclotomic character*.

Since the compositum of two abelian extensions of a field inside a fixed algebraic closure is abelian, the following makes sense.

NOTATION B.3.15. Let K be a field. The *maximal abelian extension* of K inside an algebraic closure of K is denoted K^{ab}.

REMARK B.3.16. The abelianization G_K^{ab} of the absolute Galois group G_K of a field K canonically isomorphic to $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ via the map induced by restriction on G_K.

B.4. Galois cohomology

DEFINITION B.4.1. Let L/K be a Galois extension of fields, and let A be a discrete $\mathrm{Gal}(L/K)$-module with respect to the Krull topology on $\mathrm{Gal}(L/K)$. For $i \geq 0$, the *ith Galois cohomology group* of L/K with coefficients in A is the profinite cohomology group $H^i(\mathrm{Gal}(L/K), A)$.

EXAMPLE B.4.2. Let L/K be a Galois extension with Galois group G. Then the additive and multiplicative groups of L are discrete G-modules. That is, L is the union of the finite Galois subextensions E of K in L, and $E = L^{\mathrm{Gal}(L/E)}$ by the fundamental theorem of infinite Galois theory.

Hilbert's Theorem 90 admits the following generalization to Galois cohomology.

THEOREM B.4.3. *Let L/K be a Galois extension of fields. Then $H^1(\mathrm{Gal}(L/K), L^\times) = 0$.*

PROOF. Let $\mathscr{E}$ denote the set of finite Galois extensions of K in L. Then

$$H^1(\mathrm{Gal}(L/K), L^\times) = \varinjlim_{E \in \mathscr{E}} H^1(\mathrm{Gal}(E/K), E^\times),$$

which reduces us to the case that L/K is finite Galois. Let $G = \mathrm{Gal}(L/K)$, and let $f\colon G \to L^\times$ be a 1-cocycle. We may view the elements $\sigma \in G$ as abelian characters $L^\times \to L^\times$. As distinct characters

of $L^\times$, these characters form a linearly independent set. The sum $\sum_{\sigma\in G} f(\sigma)\sigma$ is therefore a nonzero map $L^\times \to L$. Let $\alpha \in L^\times$ be such that $z = \sum_{\sigma\in G} f(\sigma)\sigma(\alpha) \neq 0$. For any $\tau \in G$, we have

$$\begin{aligned}\tau^{-1}(z) &= \sum_{\sigma\in G} \tau^{-1}(f(\sigma))\cdot\tau^{-1}\sigma(\alpha) = \sum_{\sigma\in G} \tau^{-1}(f(\tau\sigma))\sigma(\alpha)\\ &= \sum_{\sigma\in G} \tau^{-1}(f(\tau)\cdot\tau f(\sigma))\sigma(\alpha) = \tau^{-1}(f(\tau))\sum_{\sigma\in G} f(\sigma)\sigma(\alpha) = \tau^{-1}(f(\tau))z.\end{aligned}$$

Thus,

$$f(\tau) = \frac{z}{\tau(z)},$$

so f is the 1-coboundary of z^{-1}. □

This has the usual statement of Hilbert's Theorem 90 as a corollary.

COROLLARY B.4.4. *Let L/K be a finite cyclic extension of fields, and let $N_{L/K}\colon L^\times \to K^\times$ be the norm map. Then*

$$\ker N_{L/K} = \left\{\alpha \in L^\times \mid \alpha = \tfrac{\sigma(\beta)}{\beta} \text{ for some } \beta \in L^\times\right\},$$

where σ is a generator of $\mathrm{Gal}(L/K)$.

PROOF. Since σ generates $G = \mathrm{Gal}(L/K)$, the element $\sigma - 1 \in \mathbb{Z}[G]$ generates I_G, and so the statement at hand is $\ker N_{L/K} = I_G L^\times$, which is to say $\hat{H}^{-1}(G, L^\times) = 0$. Since G is cyclic, we have $\hat{H}^{-1}(G, L^\times) \cong H^1(G, L^\times)$. Thus, the result follows from Theorem B.4.3. □

For the additive group, we have the following much stronger generalization of the additive version of Hilbert's Theorem 90.

THEOREM B.4.5. *Let L/K be a Galois extension of fields. Then $H^i(\mathrm{Gal}(L/K), L) = 0$ for all $i \geq 1$.*

PROOF. As in the proof of Theorem B.4.3, this reduces quickly to the case that L/K is finite, which we therefore suppose. As a $K[G]$-module, L is free on a single generator by the normal basis theorem, and therefore it is isomorphic to

$$Z[G] \otimes_{\mathbb{Z}} K \cong \mathrm{Ind}^G(K) \cong \mathrm{CoInd}^G(K).$$

So, the result follows from the acyclicity of coinduced modules. □

NOTATION B.4.6. For a field K, we let K^{sep} denote a fixed separable closure and G_K denote its absolute Galois group.

DEFINITION B.4.7. The Brauer group $\mathrm{Br}(K)$ of a field K is $H^2(G_K, (K^{\mathrm{sep}})^\times)$.

We have the following inflation-restriction theorem for Brauer groups.

PROPOSITION B.4.8. *For any Galois extension L/K, there is an exact sequence*

$$0 \to H^2(\mathrm{Gal}(L/K), L^\times) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(L)$$

of abelian groups.

PROOF. Let K^{sep} be a separable closure of K containing L. Note that $((K^{\mathrm{sep}})^\times)^{G_L} = L^\times$ by the fundamental theorem of Galois theory, and we have $H^1(G_L, (K^{\mathrm{sep}})^\times) = 0$ by Theorem B.4.3. The sequence is then just the inflation-restriction sequence of Proposition B.2.18 for $i = 2$, $G = G_K$, $N = G_L$, and $A = (K^{\mathrm{sep}})^\times$. □

EXAMPLE B.4.9. Consider the finite field $\mathbb{F}_q$ for a prime power q. For $n \geq 1$, we know that $\mathbb{F}_{q^n}/\mathbb{F}_q$ is cyclic of degree n, so we have an isomorphism

$$H^2(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q), \mathbb{F}_{q^n}^\times) \cong \hat{H}^0(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q), \mathbb{F}_{q^n}^\times) \cong \mathbb{F}_q^\times / N_{\mathbb{F}_{q^n}/\mathbb{F}_q} \mathbb{F}_{q^n}^\times.$$

Now, the norm of any primitive $(q^n - 1)$th root of unity ξ is

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\xi) = \prod_{i=0}^{n-1} \xi^{q^i} = \xi^{\frac{q^n-1}{q-1}},$$

which is a primitive $(q-1)$th root of unity. In other words, the norm map is surjective, so

$$\mathrm{Br}(\mathbb{F}_q) = \varinjlim_n H^2(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q), \mathbb{F}_{q^n}^\times) = 0.$$

B.5. Kummer theory

NOTATION B.5.1. For a field K of characteristic not dividing $n \geq 1$, we use μ_n to denote the group of nth roots of unity in K^{sep}.

NOTATION B.5.2. For an abelian group A and $n \geq 1$, let $A[n]$ denote the elements of exponent dividing n in A.

EXAMPLE B.5.3. We have $K^{\mathrm{sep}}[n] = \mu_n$ for any $n \geq 1$ not divisible by $\mathrm{char}(K)$.

PROPOSITION B.5.4. *Let K be a field of characteristic not dividing $n \geq 1$, and let μ_n be the group of roots of unity in a separable closure K^{sep} of K. Let $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ be the absolute Galois group. Then there are canonical isomorphisms*

$$K^\times / K^{\times n} \xrightarrow{\sim} H^1(G_K, \mu_n) \quad \text{and} \quad H^2(G_K, \mu_n) \xrightarrow{\sim} \mathrm{Br}_K[n].$$

PROOF. Since K^{sep} is separably closed, we have an exact sequence

$$1 \to \mu_n \to (K^{\mathrm{sep}})^\times \xrightarrow{n} (K^{\mathrm{sep}})^\times \to 1 \tag{B.5.1}$$

of discrete G_K-modules. By Hilbert's Theorem 90, the long exact sequence attached to (B.5.1) breaks into exact sequences

$$K^\times \xrightarrow{n} K^\times \to H^1(G_K, \mu_n) \to 0 \quad \text{and} \quad 0 \to H^2(G_K, \mu_n) \to \mathrm{Br}(K) \xrightarrow{n} \mathrm{Br}(K).$$

□

TERMINOLOGY B.5.5. The sequence in (B.5.1) is often called a *Kummer sequence*.

DEFINITION B.5.6. Let K be a field of characteristic not dividing $n \geq 1$, let $a \in K^\times$, and choose an nth root $\alpha \in (K^{\mathrm{sep}})^\times$ of a. The *Kummer cocycle* $\chi_a \colon G_K \to \mu_n$ attached to a (or more precisely, α) is the 1-cocycle defined on $\sigma \in G_K$ by

$$\chi_a(\sigma) = \frac{\sigma(\alpha)}{\alpha}.$$

REMARKS B.5.7. We maintain the notation of Definition B.5.6.

a. If $\mu_n \subset K$, then χ_a is independent of the choice of α and is in fact a group homomorphism, since G_K acts trivially on μ_n. In this case, we refer to χ_a as the *Kummer character* attached to a.

b. The class of χ_a in $H^1(G_K, \mu_n)$ is independent of the choice of α, as the difference between two such choices is the 1-coboundary of an nth root of unity.

LEMMA B.5.8. *Let K be a field of characteristic not dividing $n \geq 1$. Then the isomorphism $K^\times/K^{\times n} \xrightarrow{\sim} H^1(G_K, \mu_n)$ of Proposition B.5.4 takes the image of $a \in K^\times$ to χ_a.*

PROOF. The connecting homomorphism yielding the map is the snake lemma map in the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_n & \longrightarrow & (K^{\mathrm{sep}})^\times & \xrightarrow{n} & (K^{\mathrm{sep}})^\times & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle d^0} & & \downarrow{\scriptstyle d^0} & & \downarrow{\scriptstyle d^0} & & \\
0 & \longrightarrow & Z^1(G_K, \mu_n) & \longrightarrow & Z^1(G_K, (K^{\mathrm{sep}})^\times) & \xrightarrow{n} & Z^1(G_K, (K^{\mathrm{sep}})^\times) & \longrightarrow & 0,
\end{array}$$

so given on $a \in K^\times$ by picking $\alpha \in (K^{\mathrm{sep}})^\times$ with $\alpha^n = a$, taking $d^0(\alpha) \in Z^1(G_K, K^\times)$ and noting that it takes values in μ_n. Since $d^0(\alpha) = \chi_a$ by definition, we are done. □

TERMINOLOGY B.5.9. The isomorphism $K^\times/K^{\times n} \xrightarrow{\sim} H^1(G_K, \mu_n)$ of Lemma B.5.8 is called the *Kummer isomorphism*.

PROPOSITION B.5.10. *Let L/K be a Galois extension of fields of characteristic not dividing $n \geq 1$, and suppose that μ_n is contained in L. Then the Kummer isomorphism restricts to an isomorphism*

$$(K^\times \cap L^{\times n})/K^{\times n} \xrightarrow{\sim} H^1(\mathrm{Gal}(L/K), \mu_n).$$

PROOF. This is a simple consequence of the inflation-restriction sequence combined with the Kummer isomorphisms for K and L. These yield a left exact sequence

$$0 \to H^1(\mathrm{Gal}(L/K), \mu_n) \to K^\times/K^{\times n} \to L^\times/L^{\times n}$$

that provides the isomorphism. □

PROPOSITION B.5.11. *Let K be a field of characteristic not dividing $n \geq 1$, and suppose that K contains the nth roots of unity. Let L/K be a cyclic extension of degree n. Then $L = K(\sqrt[n]{a})$ for some $a \in K^\times$.*

PROOF. Let ζ be a primitive nth root of unity in K. Note that $N_{L/K}(\zeta) = \zeta^n = 1$, so Hilbert's Theorem 90 tells us that there exists $\alpha \in L$ and a generator σ of $\mathrm{Gal}(L/K)$ with $\frac{\sigma(\alpha)}{\alpha} = \zeta$. Note that

$$N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma^i \alpha = \prod_{i=1}^{n} \zeta^i \alpha = \zeta^{n(n-1)/2} \alpha^n = (-1)^{n-1} \alpha^n,$$

so setting $a = -N_{L/K}(-\alpha)$, we have $\alpha^n = a$. Since α has n distinct conjugates in L, we have that $L = K(\alpha)$. □

NOTATION B.5.12. Let Δ be a subset of a field K, and let $n \geq 1$ be such that K contains the nth roots of unity in $\overline{K}$. Then the field $K(\sqrt[n]{\Delta})$ is the field given by adjoining an nth root of each element of Δ to K.

THEOREM B.5.13 (Kummer duality). *Let K be a field of characteristic not dividing $n \geq 1$, and suppose that K contains the nth roots of unity. Let L be an abelian extension of K of exponent dividing n, and set $\Delta = L^{\times n} \cap K^\times$. Then $L = K(\sqrt[n]{\Delta})$, and there is a perfect bimultiplicative pairing*

$$\langle\ ,\ \rangle \colon \mathrm{Gal}(L/K) \times \Delta/K^{\times n} \to \mu_n$$

given by $\langle \sigma, a \rangle = \chi_a(\sigma)$ for $\sigma \in \mathrm{Gal}(L/K)$ and $a \in \Delta$.

PROOF. Since $\mu_n \subset K$, Proposition B.5.10 tells us that the map taking $a \in \Delta$ to its Kummer cocycle χ_a yields

$$\Delta/K^{\times n} \cong \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n).$$

This isomorphism gives rise to the bimultiplicative pairing $\langle\ ,\ \rangle$, and it implies that any $a \in \Delta/K^{\times n}$ of order d dividing n pairs with some element of $\mathrm{Gal}(L/K)$ to a dth root of unity. It remains to show that the pairing also induces an isomorphism

$$\mathrm{Hom}(\Delta/K^{\times n}, \mu_n) \cong \mathrm{Gal}(L/K).$$

Clearly, $K(\sqrt[n]{\Delta})$ is contained in L. On the other hand, L/K is a compositum of cyclic extensions of exponent dividing n, we have by Proposition B.5.11 that $L = K(\sqrt[n]{\Gamma})$ for some subset Γ of $K^\times$, which then can be taken to be Δ. So, let $\sigma \in \mathrm{Gal}(L/K)$ be of order d dividing n. Since $L = K(\sqrt[n]{\Delta})$, we have that there exists $a \in \Delta$ such that $\sigma(\alpha)/\alpha$ for $\alpha \in L$ with $\alpha^n = a$ is a primitive dth root of unity times α. Hence, the pairing is perfect. □

REMARK B.5.14. One may replace Δ in Theorem B.5.13 by any $\Gamma \subseteq \Delta$ with $\Delta = \Gamma K^{\times n}$. Then $\Delta/K^{\times n}$ should be replaced by the isomorphic $\Gamma/(\Gamma \cap K^{\times n})$.

REMARK B.5.15. The pairing of Proposition B.5.13 is perfect with respect to the Krull topology on $\mathrm{Gal}(L/K)$ and the discrete topology on Δ.

TERMINOLOGY B.5.16. We say that $\mathrm{Gal}(L/K)$ and $\Delta/K^{\times n}$ in Proposition B.5.13 are *Kummer dual* to each other.

COROLLARY B.5.17. *Let K be a field of characteristic not dividing $n \geq 1$, and suppose that K contains the nth roots of unity. The Galois group of the maximal abelian extension of K of exponent n is Kummer dual to $K^\times/K^{\times n}$.*

REMARK B.5.18. Suppose that K contains μ_n, where n is not divisible by the residue characteristic of K. Let L/K be abelian of exponent n and $G = \mathrm{Gal}(L/K)$. Write $L = K(\sqrt[n]{\Delta})$ for some $\Delta \leq K^\times$. Then $L_d = K(\sqrt[d]{\Delta})$ is the maximal subextension of exponent dividing d, and $G_d = \mathrm{Gal}(L_d/K) \cong G/G^d$. Moreover, we have a commutative diagram of pairings

$$\begin{array}{ccc} G \times \Delta/(\Delta \cap K^{\times n}) & \xrightarrow{\langle\ ,\ \rangle} & \mu_n \\ \downarrow & & \downarrow \\ G_d \times \Delta/(\Delta \cap K^{\times d}) & \xrightarrow{\langle\ ,\ \rangle_d} & \mu_d, \end{array}$$

where the left vertical map is the direct product of the restriction (or the quotient map) with the map induced by the identity and the map $\mu_n \to \mu_d$ is the n/d-power map. That is, we have

$$\langle \sigma, a \rangle_d = \frac{\sigma(\sqrt[d]{a})}{\sqrt[d]{a}} = \left(\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} \right)^{n/d} = \langle \sigma, a \rangle^{n/d},$$

where σ denotes both an element of G and its image in G_d and a denotes the image of an element of Δ. In particular, the composition

$$G \to \mathrm{Hom}(\Delta, \mu_n) \to \mathrm{Hom}(\Delta, \mu_d)$$

in which the first map is given by $\langle\ ,\ \rangle$ and the second by the (n/d)-power map agrees with the map $G \to \mathrm{Hom}(\Delta, \mu_d)$ given by $\langle\ ,\ \rangle_d$.

REMARK B.5.19. By Kummer duality, if K has characteristic 0 and contains all roots of unity, then

$$G_K^{\mathrm{ab}} \cong \varprojlim_n G_K^{\mathrm{ab}}/(G_K^{\mathrm{ab}})^n \cong \varprojlim_n \mathrm{Hom}(K^\times, \mu_n) \cong \varprojlim_n \mathrm{Hom}_{\mathrm{cts}}(\widehat{K^\times}, \mu_n) \cong \mathrm{Hom}_{\mathrm{cts}}\left(\widehat{K^\times}, \varprojlim_n \mu_n\right),$$

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

EXAMPLE B.5.20. Let K be a field of characteristic not p containing the group μ_{p^∞} of all p-power roots of unity, and let $a \in K^\times$ with $a \notin K^{\times p}$. Then the field $L = K(\sqrt[p^\infty]{a})$ given by adjoining all p-power roots of a to K is the union of the fields $L_n = K(\sqrt[p^n]{a})$, each of which has degree p^n over K by Theorem B.5.13 since a has order p^n in $K^\times/K^{\times p^n}$. Let $\Delta = \langle a \rangle$. Then

$$\mathrm{Gal}(L/K) \cong \varprojlim \mathrm{Gal}(L_n/K) \cong \varprojlim_n \mathrm{Hom}(\Delta, \mu_{p^n}) \cong \varprojlim_n \mu_{p^n} \cong \mathbb{Z}_p,$$

since a homomorphism from Δ is determined by where it sends a.

DEFINITION B.5.21. Let K be a field of characteristic p. The *Tate module* $\mathbb{Z}_p(1)$ is the topological G_K-module that is $\mathbb{Z}_p$ as a topological group together with the action of the G_K given by

$$\sigma \cdot a = \chi(\sigma)a$$

for $a \in \mathbb{Z}_p$, where $\chi\colon G_K \to \mathbb{Z}_p^\times$ is the p-adic cyclotomic character.

REMARK B.5.22. Let K be a field of characteristic not p, set $G = \mathrm{Gal}(K(\mu_{p^\infty})/K)$. The group

$$T_p = \varprojlim_n \mu_{p^n}$$

is a Galois module also referred to as the Tate module, the action of G given by multiplication by the p-adic cyclotomic character $\chi\colon G \to \mathbb{Z}_p^\times$ (which factors through G) in the sense that

$$\sigma((\xi_n)_n) = (\xi_n^{\chi(\sigma)})_n$$

for all $(\xi_n)_n \in T_p$. The group T_p is noncanonically topologically isomorphic to the Tate module $\mathbb{Z}_p(1)$, with the isomorphism given by choice of a compatible sequence $(\zeta_{p^n})_n$ of primitive p^nth roots of unity, which is taken to 1.

EXAMPLE B.5.23. Let K be a field of characteristic not p and $a \in K^\times - K^{\times p}$. Set $L = K(\mu_{p^\infty})$ and $M = L(\sqrt[p^\infty]{a})$. By Example B.5.20, we know that $\mathrm{Gal}(M/L) \cong \mathbb{Z}_p$ as topological groups. But note that M/K is Galois. In fact, take $\sigma \in \mathrm{Gal}(L/K)$ and lift it to an embedding δ of M into a separable closure of M. Then

$$\tilde{\sigma}(\sqrt[p^n]{a})^{p^n} = a,$$

so $\tilde{\sigma}(\sqrt[p^n]{a}) = \xi \sqrt[p^n]{a}$ for some p^nth root of unity ξ, which is in M by definition. To determine the Galois group, take $\tau \in \mathrm{Gal}(M/L)$, and let ζ be the p^nth root of unity such that $\tau(\sqrt[p^n]{a}) = \zeta \sqrt[p^n]{a}$. For $n \geq 1$, we then have

$$\tilde{\sigma}\tau\tilde{\sigma}^{-1}(\sqrt[p^n]{a}) = \tilde{\sigma}(\tau(\tilde{\sigma}^{-1}(\xi^{-1})\sqrt[p^n]{a})) = \tilde{\sigma}(\sigma^{-1}(\xi^{-1})\zeta\sqrt[p^n]{a}) = \sigma(\zeta)\sqrt[p^n]{a} = \zeta^{\chi(\sigma)}\sqrt[p^n]{a},$$

where χ is the p-adic cyclotomic character. In other words, we have

$$\mathrm{Gal}(M/L) \cong \mathrm{Gal}(M/L) \rtimes \mathrm{Gal}(L/K) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times,$$

where through the conjugation action of $\mathrm{Gal}(L/K)$ on $\mathrm{Gal}(M/L)$, the latter module is isomorphic to the Tate module $\mathbb{Z}_p(1)$.