1

Algebraic Number Theory

The first two sections of this introductory chapter provide a brief overview of several concepts and results from number theory. A detailed exposition of this material can be found in the books of Lang (1994) and Weil (1995) (cf. also Chapters 1–3 of [ANT]). It should be noted that, unlike Weil, we state the results here only for algebraic number fields, although the overwhelming majority of them also hold for global fields of positive characteristic, i.e., fields of algebraic functions over a finite field. In §1.3, we present results about group cohomology, including definitions and statements of the basic properties of noncommutative cohomology, that are necessary for understanding the rest of the book. Sections 1.4–1.5 contain basic results on simple algebras over local and global fields. Special attention is given to the investigation of the multiplicative structure of division algebras over such fields, particularly the triviality of the reduced Whitehead group. Moreover, in §1.5, we collect useful results on lattices in vector spaces and orders in semisimple algebras.

Throughout the book, we assume familiarity with field theory, particularly Galois theory (finite and infinite), as well as with elements of topological algebra, including the theory of profinite groups.

1.1 Algebraic Number Fields, Valuations, and Completions

1.1.1 Arithmetic of Algebraic Number Fields

Let K be an *algebraic number field*, i.e., a finite extension of the field $\mathbb{Q}$ of rational numbers, and let $\mathcal{O}_K$ be the ring of integers of K. The ring $\mathcal{O}_K$ is a classical object of interest in algebraic number theory. The analysis of its structural and arithmetic properties, which was initiated by Gauss, Dedekind, Dirichlet, and others in the nineteenth century, remains an active area of research.

From a purely algebraic point of view, the ring $\mathcal{O} = \mathcal{O}_K$ is easy to describe: if $[K\colon \mathbb{Q}] = n$, then $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank n. Furthermore, for any nonzero ideal $\mathfrak{a} \subset \mathcal{O}$, the quotient ring $\mathcal{O}/\mathfrak{a}$ is finite; in particular, any nonzero prime ideal is maximal. Rings with such properties (i.e., integral domains that are noetherian, integrally closed, and in which all nonzero prime ideals are maximal) are known as *Dedekind rings*. In such a ring, any nonzero ideal $\mathfrak{a} \subset \mathcal{O}$ can be written uniquely as the product of prime ideals: $\mathfrak{a} = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_r^{\alpha_r}$. This property generalizes the fundamental theorem of arithmetic on the uniqueness of factorization of any positive integer into a product of primes. Nevertheless, the analogy here is only partial: unique factorization of elements of $\mathcal{O}$ into prime elements, generally speaking, does not hold. This fact, which already suggests that the arithmetic of $\mathcal{O}$ can differ significantly from the arithmetic of $\mathbb{Z}$, has been crucial in shaping algebraic number theory.

The precise degree to which $\mathcal{O}$ fails to be a unique factorization domain is measured by the *ideal class group* of K, which is defined as follows. Recall that the fractional ideals of K are $\mathcal{O}$-submodules $\mathfrak{a}$ of K such that $x\mathfrak{a} \subset \mathcal{O}$ for a suitable nonzero x in $\mathcal{O}$. Define the product of two fractional ideals $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}$ to be the $\mathcal{O}$-submodule in K generated by the products xy for all $x \in \mathfrak{a}, y \in \mathfrak{b}$. Then, with respect to this operation, the set of fractional ideals becomes a group, called the *group of (fractional) ideals* of K, which we denote by $\mathrm{Id}(\mathcal{O})$. The principal fractional ideals, i.e., ideals $x\mathcal{O}$ where $x \in K^*$, form the subgroup $\mathrm{P}(\mathcal{O}) \subset \mathrm{Id}(\mathcal{O})$, and the quotient group $\mathrm{Cl}(\mathcal{O}) = \mathrm{Id}(\mathcal{O})/\mathrm{P}(\mathcal{O})$ is called the *ideal class group of* K. A classical result of algebraic number theory is that the group $\mathrm{Cl}(\mathcal{O})$ is always finite; its order, denoted by h_K, is the *class number* of K. Moreover, the factorization of elements of $\mathcal{O}$ into primes is unique if and only if $h_K = 1$. Another classical result (the Dirichlet Unit Theorem) states that the group of invertible elements $\mathcal{O}^*$ is finitely generated. These two facts are the starting point for the arithmetic theory of algebraic groups (cf. Preface to the Russian edition). However, in generalizing classical arithmetic to algebraic groups, we cannot appeal to ring-theoretic concepts, but rather need to develop such number-theoretic constructions as valuations and completions, as well as adeles, ideles, and others.

1.1.2 Valuations and Completions of Algebraic Number Fields

We define a *valuation* of a field K to be a function $|\ |_v\colon K \to \mathbb{R}$ satisfying the following conditions for all x, y in K:

(1) $|x|_v \geq 0$, with $|x|_v = 0$ if and only if $x = 0$;
(2) $|xy|_v = |x|_v|y|_v$;
(3) $|x + y|_v \leq |x|_v + |y|_v$.

If, instead of (3), the following stronger condition holds:

(3′) $|x+y|_v \leq \max\{|x|_v, |y|_v\}$,

the valuation is called *non-Archimedean*; otherwise, it is called *Archimedean*.

As an example of a valuation of an arbitrary field K, one can consider the *trivial* valuation, which is defined by setting $|x|_v = 1$ for all x in K^*, and $|0|_v = 0$. We next consider examples of nontrivial valuations of the field $K = \mathbb{Q}$. The ordinary absolute value $|\ |_\infty$ is obviously an archimedean valuation. Furthermore, to each prime p we can associate a non-Archimedean valuation $|\ |_p$ called the *p-adic* valuation. Namely, given any $\alpha \in \mathbb{Q}^*$, we write it in the form $\alpha = p^r \cdot \beta/\gamma$, where $r, \beta, \gamma \in \mathbb{Z}$ and β and γ are not divisible by p, and then set $|\alpha|_p = p^{-r}$; we also let $|0|_p = 0$. Sometimes, instead of the p-adic valuation $|\ |_p$, it is convenient to use the corresponding logarithmic valuation $v = v_p$, defined by the formula $v(\alpha) = r$ and $v(0) = +\infty$, so that $|\alpha|_p = p^{-v(\alpha)}$. Axiomatically v is given by the following conditions:

(1) $v(x)$ is an element of the additive group $\mathbb{Z}$ of integers (or more generally any ordered abelian group) for $x \neq 0$, and $v(0) = \infty$;
(2) $v(xy) = v(x) + v(y)$;
(3) $v(x+y) \geq \min\{v(x), v(y)\}$.

We shall use both ordinary valuations as well as the corresponding logarithmic valuations, and it should be clear from the context to which one we are referring.

It is worth noting that the examples given earlier actually exhaust all the nontrivial valuations of $\mathbb{Q}$.

Theorem 1.1 (OSTROWSKI) *Any nontrivial valuation of $\mathbb{Q}$ is equivalent either to the archimedean valuation $|\ |_\infty$ or to a p-adic valuation $|\ |_p$.*

(Recall that two valuations $|\ |_1$ and $|\ |_2$ on K are called *equivalent* if they induce the same topology on K; in this case we have $|\ |_1 = |\ |_2^\lambda$ for a suitable real $\lambda > 0$.)

Thus, restricting any nontrivial valuation $|\ |_v$ of an algebraic number field K to $\mathbb{Q}$, we obtain (up to equivalence) either an archimedean valuation $|\ |_\infty$ or a p-adic valuation (it can be shown that the restriction of a nontrivial valuation is always nontrivial). This means that any nontrivial valuation of K can be obtained by extending to K one of the (nontrivial) valuations of $\mathbb{Q}$. On the other hand, it is known that for any algebraic extension L/K, any valuation $|\ |_v$ of K can be extended to L, i.e., there exists a valuation $|\ |_w$ of L (denoted $w|v$)

such that $|x|_w = |x|_v$ for all x in K. In particular, starting with the valuations of $\mathbb{Q}$, we can obtain all valuations of an arbitrary number field K.

Let us analyze the extension procedure in greater detail. To begin with, it is helpful to introduce the completion K_v of K with respect to a valuation $|\ |_v$. If we consider K as a metric space with respect to the metric arising from $|\ |_v$, then its completion K_v is a metric space that, at the same time, is a field under the natural operations, and is complete with respect to the corresponding extension of $|\ |_v$, for which we will use the same notation. It is well known that if L is an algebraic extension of K_v (and, in general, of any field that is complete with respect to a valuation $|\ |_v$), then $|\ |_v$ has a unique extension $|\ |_w$ to L. Using this, we can derive an explicit formula for $|\ |_w$, which can be taken as the definition of $|\ |_w$. Indeed, since $|\ |_v$ extends uniquely to a valuation of the algebraic closure $\bar{K}_v$, it follows that $|\sigma(x)|_w = |x|_w$ for any x in $\bar{K}_v$ and any σ in $\mathrm{Gal}(\bar{K}_v/K_v)$. Now let L/K_v be a finite extension of degree n, and let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings of L into $\bar{K}_v$ over K_v. Then for the norm $N_{L/K}(a)$ of an element $a \in L$, we have

$$|N_{L/K}(a)|_v = \left|\prod_{i=1}^{n} \sigma_i(a)\right|_v = \prod_{i=1}^{n} |\sigma_i(a)|_w = |a|_w^n.$$

As a result, we obtain the following explicit description of the extension $|\ |_w$:

$$|a|_w = |N_{L/K}(a)|_v^{1/n} \quad \text{for any } a \text{ in } L. \tag{1.1}$$

Now let us discuss the procedure of extending valuations to a finite extension L/K for a number field K. Let $|\ |_v$ be a valuation of K and $|\ |_w$ its unique extension to the algebraic closure $\bar{K}_v$ of K_v. Then for any embedding $\tau\colon L \to \bar{K}_v$ over K (and in fact we have $n = [L\colon K]$ such embeddings), we can define a valuation u on L by $|x|_u = |\tau(x)|_w$, which clearly extends the original valuation $|\ |_v$ of K. In this case, the completion L_u can be identified with the compositum $\tau(L)K_v$. Moreover, any extension may be obtained in this way, and two embeddings $\tau_1, \tau_2\colon L \to \bar{K}_v$ give the same extension if they are conjugate over K_v, i.e., if there exists λ in $\mathrm{Gal}(\bar{K}_v/K_v)$ with $\tau_2 = \lambda\tau_1$. In other words, if $L = K(\alpha)$ and $f(t)$ is the irreducible polynomial of α over K, then the extensions $|\ |_{u_1}, \ldots, |\ |_{u_r}$ of $|\ |_v$ over L are in one-to-one correspondence with the irreducible factors of f over K_v, viz. $|\ |_{u_i}$ corresponds to the embedding $\tau_i\colon L \to \bar{K}_v$ that sends α to a root of f_i. Further, the completion L_{u_i} is the finite extension of K_v generated by a root of f_i. It follows that

$$L \bigotimes_K K_v \simeq \prod_{i=1}^{r} L_{u_i}; \tag{1.2}$$

in particular, the degree $[L\colon K]$ equals the sum of the local degrees $[L_{u_i}\colon K_v]$.

Moreover, one has the following formulas for the norm and the trace of an element α in L:

$$N_{L/K}(a) = \prod_{u|v} N_{L_u/K_v}(a), \qquad \mathrm{Tr}_{L/K}(a) = \sum_{u|v} \mathrm{Tr}_{L_u/K_v}(a). \tag{1.3}$$

Thus, the set V^K of all pairwise inequivalent valuations of K (or, to put it more precisely, of the equivalence classes of valuations of K) is the union of the finite set V_∞^K of the archimedean valuations, which are the extensions to K of the ordinary absolute value $|\ |_\infty$ on $\mathbb{Q}$, and the set V_f^K of non-Archimedean valuations, obtained as extensions of the p-adic valuation $|\ |_p$ of $\mathbb{Q}$, for each prime number p. The archimedean valuations correspond to the embeddings of K into either $\mathbb{R}$ or $\mathbb{C}$, in which case they are respectively called *real* or *complex valuations* and the corresponding completions can be identified with $\mathbb{R}$ or $\mathbb{C}$. If $v \in V_\infty^K$ is a real valuation, then an element α in K is said to be *positive* with respect to v if its image under v is a positive number. Let s (respectively t) denote the number of real (respectively pairwise nonconjugate complex) embeddings of K. Then $s + 2t = n$ is the degree of L over K.

Non-Archimedean valuations lead to more complicated completions. More specifically, if $v \in V_f^K$ is an extension of a p-adic valuation, then the completion K_v is a finite extension of the field $\mathbb{Q}_p$ of p-adic numbers. Since $\mathbb{Q}_p$ is a locally compact field, it follows that K_v is locally compact (with respect to the topology determined by the valuation).[1] The closure of the ring of integers $\mathcal{O}$ in K_v is the *valuation ring*

$$\mathcal{O}_v = \{a \in K_v \colon |a|_v \leq 1\},$$

sometimes called the ring of v-adic integers. Then $\mathcal{O}_v$ is a local ring with maximal ideal $\mathfrak{p}_v = \{a \in K_v \colon |a|_v < 1\}$, called the *valuation ideal*, and group of invertible elements

$$U_v = \mathcal{O}_v \setminus \mathfrak{p}_v = \{a \in K_v \colon |a|_v = 1\}.$$

It is easy to see that the valuation ring of $\mathbb{Q}_p$ is the ring of p-adic integers $\mathbb{Z}_p$, and the corresponding valuation ideal is $p\mathbb{Z}_p$. In general, $\mathcal{O}_v$ is a free module over $\mathbb{Z}_p$, whose rank equals the degree $[K_v \colon \mathbb{Q}_p]$, making $\mathcal{O}_v$ an open compact subring of K_v. Moreover, the powers $\mathfrak{p}_v^i$ of $\mathfrak{p}_v$ form a fundamental system of

[1] Henceforth, completions of a number field with respect to nontrivial valuations are called *local fields*. It can be shown that the class of local fields thus defined coincides with the class of nondiscrete locally compact fields of characteristic zero. We note also that we shall use the term local field primarily in connection with non-Archimedean completions, and to emphasize this we will use the term *non-Archimedean local field*.

neighborhoods of zero in $\mathcal{O}_v$. The quotient ring $k_v = \mathcal{O}_v/\mathfrak{p}_v$ is a finite field and is called the *residue field* of v. The ideal $\mathfrak{p}_v \subset \mathcal{O}_v$ is principal; any of its generators π is called a *uniformizer* and is characterized by the property that $v(\pi)$ is the (positive) generator of the value group $\Gamma = v(K_v^*) \simeq \mathbb{Z}$. Once we have fixed a uniformizer π, we can write any a in K_v^* as $a = \pi^r u$, for a suitable $u \in U_v$; this yields a continuous isomorphism $K_v^* \simeq \mathbb{Z} \times U_v$, given by $a \mapsto (r, u)$, where $\mathbb{Z}$ is endowed with the discrete topology. Thus, to determine the structure of K_v^*, we need only describe U_v. It can be shown quite easily that U_v is a compact group, locally isomorphic to $\mathcal{O}_v$. It follows that $U_v \simeq F \times \mathbb{Z}_p^n$, where $n = [K_v\colon \mathbb{Q}_p]$, and F is the group of all roots of unity in K_v. Thus $K_v^* \simeq \mathbb{Z} \times F \times \mathbb{Z}_p^n$.

Two important concepts associated with field extensions are the ramification index and the residual degree. We introduce these concepts first for the local case. Let L_w/K_v be a finite extension of degree n. Then the value group $\Gamma_v = v(K_v^*)$ has finite index in $\Gamma_w = w(L_w^*)$, and the corresponding index $e(w|v) = [\Gamma_w\colon \Gamma_v]$ is called the *ramification index*. The residue field $\ell_w = \mathcal{O}_{L_w}/\mathfrak{P}_{L_w}$ for L_w is a finite extension of the residue field k_v, and $f(w|v) = [\ell_w\colon k_v]$ is the *residual degree*. Moreover, $e(w|v)f(w|v) = n$. An extension for which $e(w|v) = 1$ is called *unramified*, while an extension for which $f(w|v) = 1$ is called *totally ramified*.

Now let L/K be an extension of degree n of number fields. Then for any valuation v in V_f^K and any extension w to L, the ramification index $e(w|v)$ and residual degree $f(w|v)$ are defined respectively as the ramification index and residual degree for the extension of the completions L_w/K_v. (One can also give an intrinsic definition based on the value groups $\tilde{\Gamma}_v = v(K^*)$, $\tilde{\Gamma}_w = w(L^*)$, and the residue fields

$$\tilde{k}_w = \mathcal{O}_K(v)/\mathfrak{p}_K(v), \qquad \tilde{\ell}_w = \mathcal{O}_L(w)/\mathfrak{P}_L(w),$$

where $\mathcal{O}_K(v), \mathcal{O}_L(w)$ are the valuation rings of v and w in K and L, and $\mathfrak{p}_K(v), \mathfrak{P}_L(w)$ are the respective valuation ideals, but in fact $\tilde{\Gamma}_v = \Gamma_v, \tilde{\Gamma}_w = \Gamma_w, \tilde{k}_v = k_v$, and $\tilde{\ell}_w = \ell_w$.) As earlier, $[L_w\colon K_v] = e(w|v)f(w|v)$. Thus, if $w_1, \dots, w_r$ are all the extensions of v to L, then

$$\sum_{i=1}^{r} e(w_i|v)f(w_i|v) = \sum_{i=1}^{r} [L_{w_i}\colon K_v] = n.$$

Generally speaking, $e(w_i|v)$ and $f(w_i|v)$ do not have to be equal for different i, but in the important case of a Galois extension L/K, they are indeed the same for all i. To see this, we let $\mathcal{G}$ denote the Galois group of L/K. Then all extensions $w_1, \dots, w_r$ of v to L are conjugate under $\mathcal{G}$, i.e., for any $i = 1, \dots, r$, there exists σ_i in $\mathcal{G}$ such that $w_i(x) = w_1(\sigma_i(x))$ for all x in L. It follows that

$e(w_i|v)$ and $f(w_i|v)$ are independent of i (we will denote them simply by e and f); moreover, the number of different extensions r is the index $[\mathcal{G}\colon \mathcal{G}(w_1)]$ of the *decomposition group* $\mathcal{G}(w_1) = \{\sigma \in \mathcal{G}\colon w_1(\sigma x) = w_1(x) \text{ for all } x \text{ in } L\}$. Consequently, $efr = n$, and $\mathcal{G}(w_1)$ is the Galois group of the corresponding extension L_{w_1}/K_v of the completions.

1.1.3 Unramified and Totally Ramified Field Extensions

Let $v \in V_f^K$ and assume that the corresponding residue field k_v is the finite field $\mathbb{F}_q$ with q elements.

Proposition 1.2 *For any integer $n \geq 1$, there exists a unique unramified extension L/K_v of degree n. It is generated over K_v by all the $(q^n - 1)$-roots of unity, and therefore is a Galois extension. The correspondence that sends $\sigma \in Gal(L/K_v)$ to its reduction $\bar{\sigma} \in Gal(\ell/k_v)$, where $\ell \simeq \mathbb{F}_{q^n}$ is the residue field of L, yields an isomorphism of Galois groups $Gal(L/K_v) \simeq Gal(\ell/k_v)$.*

In order to define the reduction $\bar{\sigma}$ of a given automorphism $\sigma \in \mathrm{Gal}(L/K_v)$, we note that the valuation ring $\mathcal{O}_L$ and its valuation ideal $\mathfrak{P}_L$ are invariant under σ. So, σ induces an automorphism of the residue field $\ell = \mathcal{O}_L/\mathfrak{P}_L$ which we call $\bar{\sigma}$. Furthermore, we observe that $\mathrm{Gal}(\ell/k_v)$ is a cyclic group generated by the Frobenius automorphism $\varphi(x) = x^q$ for all x in ℓ; the corresponding element of $\mathrm{Gal}(L/K_v)$ will also be called the Frobenius automorphism (of the extension L/K_v) and will be denoted by $\mathrm{Fr}(L/K_v)$.

The following proposition describes the properties of norms in unramified extensions.

Proposition 1.3 *Let L/K_v be an unramified extension, and let U_v and U_L denote the groups of units in K_v and L, respectively. Then $U_v = N_{L/K}(U_L)$; in particular, $U_v \subset N_{L/K_v}(L^*)$.*

PROOF: Our argument utilizes the canonical filtration on the group of units, which is useful in other situations as well. Namely, for any integer $i \geq 1$, we let $U_v^{(i)} = 1 + \mathfrak{p}_v^i$ and $U_L^{(i)} = 1 + \mathfrak{P}_L^i$. It is easy to see that these sets are open subgroups which actually form bases of the neighborhoods of the identity in U_v and U_L, respectively. We have the following isomorphisms:

$$U_v/U_v^{(1)} \simeq k_v^*, \qquad U_v^{(i)}/U_v^{(i+1)} \simeq k_v^+, \qquad \text{for } i \geq 1, \tag{1.4}$$

where the first one is induced by the reduction map $a \mapsto a \pmod{\mathfrak{p}_v}$, and the second is obtained by fixing a uniformizer π of K_v and then mapping $1 + \pi^i a \mapsto a \pmod{\mathfrak{p}_v}$.

Similarly,

$$U_L/U_L^{(1)} \simeq \ell^*, \qquad U_L^{(i)}/U_L^{(i+1)} \simeq \ell^+, \qquad \text{for } i \geq 1. \tag{1.5}$$

Since L/K_v is unramified, π is also a uniformizer of L, so in the rest of the proof we will assume (as we may) that the second isomorphism in (1.5) is defined by means of π. For a in U_L, we have

$$\overline{N_{L/K_v}(a)} = \overline{\prod_{\sigma \in \mathrm{Gal}(L/K_v)} \sigma(a)} = \prod_{\tau \in \mathrm{Gal}(\ell/k_v)} \tau(\bar{a}) = N_{\ell/k_v}(\bar{a}),$$

where the bar denotes reduction modulo $\mathfrak{P}_L$.

Thus the norm map induces a homomorphism $U_L/U_L^{(1)} \to U_v/U_v^{(1)}$, which in terms of the identifications in (1.4) and (1.5) coincides with N_{ℓ/k_v}. Further, for any $i \geq 1$ and any a in $\mathcal{O}_L$, we have

$$N_{L/K_v}(1 + \pi^i a) = \prod_{\sigma \in \mathrm{Gal}(L/K_v)} \sigma(1 + \pi^i a) \equiv 1 + \pi^i \mathrm{Tr}_{L/K_v}(a) \pmod{\mathfrak{P}_v^{(i+1)}}.$$

It follows that N_{L/K_v} induces homomorphisms $U_L^{(i)}/U_L^{(i+1)} \to U_v^{(i)}/U_v^{(i+1)}$, which with the identifications in (1.4) and (1.5) become the trace map Tr_{ℓ/k_v}. But the norm and trace maps are surjective for extensions of finite fields; therefore the group $W = N_{L/K_v}(U_L)$ satisfies $U_v = WU_v^{(i)}$ for all $i \geq 1$. Since $U_v^{(i)}$ form a base of neighborhoods of identity, the latter condition means that W is dense in U_v. On the other hand, since U_L is compact and the norm map is continuous, the subgroup W is closed, and therefore $W = U_v$. □

The proof of Proposition 1.3 also yields

Corollary 1.4 *If L/K_v is an unramified extension, then $N_{L/K_v}(U_L^{(i)}) = U_v^{(i)}$ for any integer $i \geq 1$.*

We will need one additional statement about the compatibility of the norm map in arbitrary extensions with the above filtration.

Proposition 1.5 *For any finite extension L/K_v, we have the following:*

(1) $U_v^{(1)} \cap N_{L/K_v}(L^*) = N_{L/K_v}(U_L^{(1)})$;
(2) *if e is the ramification index of L/K_v, then for any integer $i \geq 1$, we have $N_{L/K_v}(U_L^{(i)}) \subset U_v^{(j)}$, where j is the smallest integer $\geq i/e$.*

PROOF: We begin with the second assertion. Let M be a Galois extension of K_v containing L. Then for a in L, $N_{L/K}(a) = \prod_\sigma \sigma(a)$, where the product is taken over all embeddings, $\sigma : L \hookrightarrow M$ over K_v. As we noted earlier, v *uniquely* extends to a valuation w of M, and consequently $w(a) = w(\sigma(a))$ for any a in L and any σ. In particular, if we choose a uniformizer π_L in L, we have $\sigma(\pi_L) = \pi_L b_\sigma$ for suitable b_σ in U_M. It follows that for $a = 1 + \pi_L^i c \in U_L^{(i)}$, we have

$$N_{L/K_v}(a) = \prod_\sigma \sigma(1 + \pi_L^i c) = \prod_\sigma (1 + \pi_L^i b_\sigma^i \sigma(c)) \in (1 + \pi_L^i \mathcal{O}_M) \cap K_v.$$

But according to the definition of the ramification index, we have $\mathfrak{p}_v \mathcal{O}_L = \mathfrak{P}_L^e$, so that $\pi_L^i \mathcal{O}_M \cap K_v = \pi_L^i \mathcal{O}_L \cap K_v = \mathfrak{P}_L^i \cap \mathcal{O}_v \subset \mathfrak{p}_v^j$ (where j is chosen as indicated in the statement of the proposition) and $N_{L/K_v}(a) \in U_v^{(j)}$. In particular, $N_{L/K_v}(U_L^{(1)}) \subset U_v^{(1)}$, so to prove the first assertion, it suffices to show that $U_v^{(1)} \cap N_{L/K_v}(L^*) \subset N_{L/K_v}(U_L^{(1)})$. Let $a \in L^*$ be such that $N_{L/K_v}(a) \in U_v^{(1)}$. Then (1.1) implies that $a \in U_L$. The isomorphism in (1.5) shows that $U_L^{(1)}$ is a maximal pro-p-subgroup in U_L for the prime p corresponding to the valuation v, from which it follows that $U_L \simeq U_L/U_L^{(1)} \times U_L^{(1)}$. In particular, $a = bc$ where $c \in U_L^{(1)}$ and b is an element of finite order coprime to p. We have

$$d = N_{L/K_v}(b) = N_{L/K_v}(a) N_{L/K_v}(c)^{-1} \in U_v^{(1)}.$$

We now observe that the order of any torsion element in $U_v^{(1)}$ is a power of p while the order of d divides that of b, hence is prime to p. It follows that $d = 1$ and therefore $N_{L/K_v}(a) = N_{L/K_v}(c) \in N_{L/K_v}(U_L^{(1)})$. □

Let us now return to unramified extensions of K_v. It can be shown that the composite of unramified extensions is unramified; hence, there exists a maximal unramified extension K_v^{nr} of K_v, which is Galois, with $\mathrm{Gal}(K_v^{nr}/K_v)$ isomorphic to the Galois group $\mathrm{Gal}(\bar{k}_v/k_v)$ of the algebraic closure of the residue field k_v. Thus, it is isomorphic to $\hat{\mathbb{Z}}$, the profinite completion of the infinite cyclic group with generator the Frobenius automorphism.

Now, let L/K be a finite extension of a number field K. It is known that almost all valuations v in V_f^K are unramified in L/K, i.e., the corresponding extension of the completions L_w/K_v is unramified for any $w|v$; in particular, the Frobenius automorphism $\mathrm{Fr}(L_w/K_v)$ is defined. If L/K is a Galois extension, then, as we noted earlier, $\mathrm{Gal}(L_w/K_v)$ can be identified with the decomposition subgroup $\mathcal{G}(w)$ of the valuation w in the Galois group $\mathcal{G} = \mathrm{Gal}(L/K)$, so $\mathrm{Fr}(L_w/K_v)$ may be viewed as an element of $\mathcal{G}$.

We know that any two valuations w_1, w_2 extending v are conjugate under $\mathcal{G}$, from which it follows that the Frobenius automorphisms $\mathrm{Fr}(L_w/K_v)$ corresponding to *all* extensions of v form a conjugacy class $F(v)$ in $\mathcal{G}$. The natural question arises if all conjugacy classes in $\mathcal{G}$ can be obtained in this way. In other words, for a given σ in $\mathcal{G}$, does there exist a valuation v in V_f^K such that for a suitable $w|v$, the extension L_w/K_v is unramified with $\mathrm{Fr}(L_w/K_v) = \sigma$?

Theorem 1.6 (CHEBOTAREV) *Let L/K be a finite Galois extension with Galois group $\mathcal{G}$. Then, for any σ in $\mathcal{G}$, there are infinitely many v in V_f^K such that for suitable $w|v$, the extension L_w/K_v is unramified and $\mathrm{Fr}(L_w/K_v) = \sigma$. In particular, there exist infinitely many v such that $L_w = K_v$, i.e., $L \subset K_v$.*

In fact, Chebotarev determined a quantitative measure (density) of the set of v in V_f^K such that the conjugacy class $F(v)$ coincides with a given conjugacy class $C \subset \mathcal{G}$. The density turned out to be $|C|/|\mathcal{G}|$ (while the density of the set V_f^K itself is 1). Therefore, Theorem 1.6 (or, more precisely, the corresponding assertion about the density) is called the *Chebotarev Density Theorem*. For cyclotomic extensions of $K = \mathbb{Q}$, it is equivalent to Dirichlet's theorem on prime numbers in arithmetic progression. We note that the last part of Theorem 1.6 can in fact be proved without using any analytic techniques.

Next, using the geometry of numbers, one proves

Theorem 1.7 (HERMITE) *If $K/\mathbb{Q}$ is a finite extension that is unramified at all primes p (i.e., $K_v/\mathbb{Q}_p$ is unramified for all p and all $v|p$), then $K = \mathbb{Q}$.*

We will not present here a detailed analysis of totally ramified extensions (in particular, we will not define tamely and wildly ramified extensions), but rather will limit ourselves to describing them using Eisenstein polynomials. Recall that a monic polynomial $e(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in K_v[t]$ is called an *Eisenstein polynomial* if $a_i \in \mathfrak{p}_v$ for all $i = 0, \ldots, n-1$ and $a_0 \notin \mathfrak{p}_v^2$. It is well known that an Eisenstein polynomial is irreducible in $K_v[t]$.

Proposition 1.8 *If Π is the root of an Eisenstein polynomial $e(t)$, then $L = K_v[\Pi]$ is a totally ramified extension of K_v with uniformizer Π. Conversely, if L/K_v is totally ramified and Π is a uniformizer of L, then $L = K_v[\Pi]$ and the minimal polynomial of Π over K_v is an Eisenstein polynomial.*

Corollary 1.9 *If L/K_v is totally ramified, then $N_{L/K_v}(L^*)$ contains a uniformizer of K_v.*