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.

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

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) $|x+y|_v \leq |x|_v + |y|_v$.

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

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

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

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) $v(x+y) \ge \min\{v(x), v(y)\}$.

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 $w|v$)

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

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 $\sigma_1, \dots, \sigma_n$ 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 $|\ |_{u_1}, \dots, |\ |_{u_r}$ 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 $[L_{u_i}\colon K_v]$.

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

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

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

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*

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

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

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

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 $[K_v : \mathbb{Q}_p]$, 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 $n = [K_v : \mathbb{Q}_p]$, 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 $w_1, \ldots, w_r$ 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 $w_1, \ldots, w_r$ of v to L are conjugate under $\mathcal{G}$, i.e., for any $i = 1, \ldots, r$, 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

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

$e(w_i|v)$ 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* $\mathcal{G}(w_1) = \{\sigma \in \mathcal{G}\colon w_1(\sigma x) = w_1(x)$ for all x 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:

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

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

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 $\geq i/e$.*

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

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 $\mathcal{G}$.

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

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.*

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

To study ramification in a Galois extension L/K with Galois group $\mathcal{G}$, one defines certain subgroups $\mathcal{G}_i$ for $i \geq -1$, called the *ramification groups*. Given $v \in V_f^K$ and $w|v$, we define $\mathcal{G}_{-1}$ to be the decomposition group $\mathcal{G}(w)$ of w, which can be identified with the local Galois group $\mathrm{Gal}(L_w/K_v)$. Next,

$$\mathcal{G}_0 = \{\sigma \in \mathcal{G}_{-1} : \sigma(a) \equiv a (\mathrm{mod}\, \mathfrak{P}_{L_w}) \text{ for all } a \in \mathcal{O}_{L_w}\}$$

is the *inertia group*. It is clear that $\mathcal{G}_0$ is precisely the kernel of the homomorphism $\mathrm{Gal}(L_w/K_v) \to \mathrm{Gal}(\ell_w/k_v)$ that sends each automorphism of L_w to its reduction. Therefore, $\mathcal{G}_0$ is a normal subgroup of $\mathcal{G}_{-1}$ and by the surjectivity of the reduction homomorphism, we have $\mathcal{G}_{-1}/\mathcal{G}_0 \simeq \mathrm{Gal}(\ell_w/k_v)$. Moreover, the fixed field $E = L_w^{\mathcal{G}_0}$ is the maximal unramified extension of K_v contained in L_w, and L_w/E is totally ramified. The higher ramification groups are defined as follows:

$$\mathcal{G}_i = \{\sigma \in \mathcal{G}_{-1} : \sigma(a) \equiv a (\mathrm{mod}\, \mathfrak{P}_{L_w}^{i+1}) \text{ for all } a \in \mathcal{O}_{L_w}\}.$$

They are normal in $\mathcal{G}_{-1}$, and $\mathcal{G}_i = \{e\}$ for sufficiently large i. Furthermore, for $i \geq 1$, the quotients $\mathcal{G}_i/\mathcal{G}_{i+1}$ are p-groups, where p is the prime corresponding to v. We note that the groups $\mathcal{G}_i = \mathcal{G}_i(v)$ defined above depend on the choice of an extension $w|v$, and for a different choice of w they would be replaced by suitable conjugates. In particular, the fixed field $L^{\mathcal{H}}$ of the subgroup $\mathcal{H} \subset \mathcal{G}$ generated by the inertia groups $\mathcal{G}_0(w)$ for all extensions $w|v$, is the maximal normal subextension in L that is unramified with respect to all valuations extending v.

1.2 Adeles and Ideles; Strong and Weak Approximation; the Local-Global Principle

To gain insights into the arithmetic properties of a number field K, rather than looking at individual valuations, it is often useful to work with families of valuations (e.g., with the entire set V^K) and the corresponding completions simultaneously. In this section, we introduce constructions that enable us to do that.

1.2.1 Adeles and Ideles

The *set of adeles* A_K of a number field K is defined to be the subset of the direct product $\prod_{v \in V^K} K_v$ consisting of $x = (x_v)$ such that $x_v \in \mathcal{O}_v$ for almost all v in V_f^K. Clearly, A_K is a ring with respect to the natural componentwise operations. Furthermore, A_K can be endowed with a topology, called the *adele topology*,

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

by taking sets of the form $\prod_{v\in S} W_v \times \prod_{v\in V^K\setminus S} \mathcal{O}_v$, where $S \subset V^K$ is a finite subset containing V_∞^K and $W_v \subset K_v$ are open subsets for each v in S, as a base of open sets (observe that this topology is stronger than the topology induced from the direct product $\prod_{v\in V^K} K_v$). It is easy to see that with respect to the adele topology, A_K is a locally compact topological ring. Next, for any finite subset $S \subset V^K$ containing V_∞^K, one defines the subring of *S-integral adeles* as

$$A_K(S) = \prod_{v\in S} K_v \times \prod_{v\notin S} \mathcal{O}_v;$$

if $S = V_\infty^K$, then the corresponding ring is called the *ring of integral adeles* and denoted $A_K(\infty)$. It is clear that $A_K = \bigcup_S A_K(S)$, where the union is taken over all finite subsets $S \subset V^K$ containing V_∞^K. It is easy to show that for any a in K and almost all $v \in V_f^K$, we have $|a|_v \leq 1$, i.e., $a \in \mathcal{O}_v$. Moreover, if $a \in K^*$, then, applying this inequality to a^{-1}, we obtain that, in fact, $a \in U_v$ for almost all $v \in V_f^K$, i.e., the set $V(a) := \{v \in V_f^K : a \notin U_v\}$ is finite. It follows that we have a diagonal embedding $K \to A_K$, given by $x \mapsto (x, x, \ldots)$, whose image, called the *ring of principal adeles*, will usually be identified with K.

Proposition 1.10 *The ring of principal adeles is discrete in A_K.*

Note that since $\mathcal{O} = \bigcap_{v\in V_f^K}(K \cap \mathcal{O}_v)$, the intersection $K \cap A_K(\infty)$ is the ring of integers $\mathcal{O} \subset K$; thus to prove our proposition it suffices to establish the discreteness of $\mathcal{O}$ in $\prod_{v\in V_\infty^K} K_v = K \otimes_{\mathbb{Q}} \mathbb{R}$. Let $x_1, \ldots, x_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}$ that is also a $\mathbb{Q}$-basis of K, and consequently also an $\mathbb{R}$-basis of $K \otimes_{\mathbb{Q}} \mathbb{R}$. Thus, $\mathcal{O}$ can be identified with a $\mathbb{Z}$-lattice in the space $K \otimes_{\mathbb{Q}} \mathbb{R}$, and the desired discreteness follows from the discreteness of $\mathbb{Z}$ in $\mathbb{R}$. (Incidentally, we note that $K \cap A_K(S)$ (where $S \supset V_\infty^K$) is the ring of S-integers

$$\mathcal{O}(S) = \{x \in K : |x|_v \leq 1 \text{ for all } v \in V^K \setminus S\},$$

and moreover $\mathcal{O}(V_\infty^K)$ is the usual ring of integers $\mathcal{O}$.)

The multiplicative analog of the ring A_K of adeles of K is the group J_K of ideles, which, by definition, consists of $x = (x_v) \in \prod_{v\in V^K} K_v^*$, such that $x_v \in U_v$ for almost all v in V_f^K. It is clear that J_K is a subgroup of the direct product and in fact is precisely the group of invertible elements of A_K. Observe, however, that J_K is *not* a topological group with respect to the topology induced from A_K (taking inverses is not a continuous operation for this topology). The

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

"correct" topology on J_K is the pullback of the product topology on $A_K \times A_K$ by means of the embedding $J_K \to A_K \times A_K$, $x \mapsto (x, x^{-1})$. Explicitly, this topology can be described by taking for a base of open sets all sets of the form $\prod_{v \in S} W_v \times \prod_{v \in V^K \setminus S} U_v$ where $S \subset V^K$ is a finite subset containing V_∞^K and $W_v \subset K_v^*$ are open subsets for v in S. This topology, called the *idele topology*, is stronger than the topology induced by the adele topology, and with respect to the former, J_K is a locally compact topological group. (One cannot help but note the analogy between adeles and ideles. Indeed, both concepts are special cases of the notion of the group of adeles of an algebraic group and of the more general construction of a restricted topological product, which we will consider in Chapter 5.) Continuing the analogy between adeles and ideles, we can define, for any finite subset $S \subset V^K$ containing V_∞^K, the *subgroup of S-integral ideles* by

$$J_K(S) = \prod_{v \in S} K_v^* \times \prod_{v \notin S} U_v;$$

in the case where $S = V_\infty^K$, this subgroup is called the *subgroup of integral ideles* and is denoted by $J_K(\infty)$. As we noted earlier, if $a \in K^*$, then $a \in U_v$ for almost all v, and consequently we have the diagonal embedding $K^* \to J_K$, whose image is called the *group of principal ideles*.

Proposition 1.11 *The group of principal ideles is discrete in J_K.*

The assertion follows from Proposition 1.10 and the fact that the induced adele topology on J_K is weaker than the idele topology.

An alternate proof can be given by using the *product formula*, which states that $\prod_{v \in V^K} |a|_v^{n_v} = 1$ for any a in K^*, where V^K consists of the extensions of the valuations $|\ |_p$ and $|\ |_\infty$ of $\mathbb{Q}$, and $n_v = [K_v : \mathbb{Q}_p]$ (respectively $n_v = [K_v : \mathbb{R}]$) is the local degree. The product formula can be stated more elegantly as $\prod_{v \in V^K} \|a\|_v = 1$, where $\|a\|_v = |a|_v^{n_v}$ is the so-called *normalized valuation*. The function $\|\ \|_v$ defines the same topology on K as the original valuation $|\ |_v$, and is actually a valuation equivalent to $|\ |_v$, except for the case where v is complex. For a non-Archimedean v, the normalized valuation has the following intrinsic description: if $\pi \in K_v$ is a uniformizer, then $\|\pi\|_v = q^{-1}$, where q is the number of elements of the residue field k_v.

Now let us return to the proof of Proposition 1.11. For archimedean v, we set $W_v = \left\{x \in K_v^* : \|x - 1\|_v < \frac{1}{2}\right\}$. We claim that the neighborhood of the identity $\Omega = \prod_{v \in V_\infty^K} W_v \times \prod_{v \in V_f^K} U_v$ satisfies $\Omega \cap K^* = \{1\}$. Indeed, if $a \in \Omega \cap K^*$ and $a \neq 1$, then we would have

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

$$\prod_{v\in V^K} \|a-1\|_v < \prod_{v\in V^K_\infty} \frac{1}{2} \cdot \prod_{v\in V^K_f} 1 < 1,$$

which contradicts the product formula.

Using normalized valuations, we can define a continuous homomorphism $J_K \to \mathbb{R}^+$ by $(x_v) \mapsto \prod_N \|x_v\|_v$. Its kernel J^1_K is called the *group of special ideles* (note that by the product formula $J^1_K \supset K^*$). Since K is discrete in A_K and K^* is discrete in J_K, the problem that naturally arises is that of constructing fundamental domains for K in A_K and for K^* in J_K. We are not going to explore these questions in detail at this point (cf. Lang [1994] or [ANT]), but rather will consider them later in the more general context of arbitrary algebraic groups. We just note that the quotients A_K/K and J^1_K/K^* are compact, but the quotient J_K/K^* is not.

Let us now describe the fundamental isomorphism i between the quotient $J_K/J_K(\infty)K^*$ and the ideal class group $\mathrm{Cl}(K)$ of K. First, note that there is a natural bijection between the set V^K_f of non-Archimedean valuations of K and the set $\mathcal{P}$ of nonzero prime (maximal) ideals of $\mathcal{O}$ defined by sending a valuation v to the ideal $\mathfrak{p}(v) = \mathcal{O} \cap \mathfrak{p}_v$, where $\mathfrak{p}_v$ is the valuation ideal of v. Then for an idele $x = (x_v)$, we define

$$i(x) = \prod_{v\in V^K_f} \mathfrak{p}(v)^{v(x_v)}.$$

Note that the product is well defined as $v(x_v) = 0$ for almost all v in V^K_f because $x \in J_K$, and belongs to the group $\mathrm{Id}(K)$ of fractional ideals of K (cf. 1.1.1). Using the theorem that any fractional ideal in K (just as any nonzero ideal in $\mathcal{O}$) factors uniquely as a product of powers of prime ideals, we see that $i\colon x \mapsto i(x)$ is a surjective homomorphism of J_K onto $\mathrm{Id}(K)$, whose kernel is the group $J_K(\infty)$ of integral ideles. In view of the fact that $i(K^*)$ coincides with the group of principal fractional ideals, i induces the required isomorphism $J_K/J_K(\infty)K^* \simeq \mathrm{Cl}(K)$. In particular, the index $[J_K : J_K(\infty)K^*]$ is the class number h_K of K. This observation is fundamental to the definition of the class number of algebraic groups (cf. section 5.1 and Chapter 8 in [AGNT]).

1.2.2 Weak and Strong Approximation

We will need the ring of truncated adeles $A_{K,S}$, where S is a finite subset of V^K, which we define as the image of $A = A_K$ under the natural projection onto the direct product $\prod_{v\notin S} K_v$. For any finite subset $T \subset V^K$ containing S, we shall let $A_{K,S}(T)$ denote the image of the ring of T-integral adeles $A_K(T)$ in $A_{K,S}$.

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

To simplify the notation, we will write A_S and $A_S(T)$ rather than $A_{K,S}$ and $A_{K,S}(T)$, respectively, when the field is clear from the context. In particular, for $S = V_\infty^K$, the ring A_{K,V_∞^K} will be denoted A_f and called the ring of *finite adeles*. We can introduce a topology on A_S in the obvious way by taking sets of the form $\prod_{v \in T} W_v \times \prod_{v \notin S \cup T} \mathcal{O}_v$, where $T \subset V^K \backslash S$ is a subset, and W_v is an open subset of K_v for each v in T, as a base of open sets. We note the decomposition $A = K_S \times A_S$ where $K_S = \prod_{v \in S} K_v$. If K_S is given the product topology, then this decomposition is actually a product of topological rings K_S and A_S. Moreover, the diagonal embedding of K into A is the product of the diagonal embeddings of K into K_S and A_S, respectively.

It is worth noting that even though the image of the diagonal embedding of K in A is discrete, each of the embeddings

$$K \hookrightarrow K_S \text{ and } K \hookrightarrow A_S$$

is *dense*.

Theorem 1.12 (Weak approximation). *The image of K under the diagonal embedding is dense in K_S.*

Theorem 1.13 (Strong approximation). *If $S \neq \emptyset$, then the image of K under the diagonal embedding is dense in A_S.*

Observe that while Theorem 1.12 holds for any field K and any finite set S of inequivalent valuations, Theorem 1.13 (and all concepts pertaining to adeles) is meaningful only for number fields (or, more generally, global fields). To clarify the arithmetic meaning of Theorem 1.13, let us consider the case of $K = \mathbb{Q}$ and $S = V_\infty^{\mathbb{Q}}$. Since for any adele $x \in A_f = A_{\mathbb{Q},S}$ we can find a nonzero integer m such that $mx \in A_f(\infty) = \prod_p \mathbb{Z}_p$, it suffices to show that the image of $\mathbb{Z}$ under the diagonal embedding $\mathbb{Z} \hookrightarrow A_f(\infty)$ is dense. Any open subset of $A_f(\infty)$ contains a set of the form

$$W = \prod_{i=1}^{r} (a_i + p_i^{\alpha_i} \mathbb{Z}_{p_i}) \times \prod_{p \neq p_i} \mathbb{Z}_p$$

where $\{p_1, \ldots, p_r\}$ is a finite collection of primes, α_i are positive integers, and $a_i \in \mathbb{Z}$. Then showing that $\mathbb{Z} \cap W$ is nonempty is equivalent to finding an $x \in \mathbb{Z}$ that satisfies the system of congruences $x \equiv a_i \,(\mathrm{mod}\; p_i^{\alpha_i})\,(i = 1, 2, \ldots, r)$, which can be done by the Chinese Remainder Theorem. Thus, in the case at hand, the strong approximation theorem is equivalent to the Chinese

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

Remainder Theorem. We refer the reader to [AGNT, Chapter 7] for the analysis of weak and strong approximation for algebraic groups.

1.2.3 The Local-Global Principle

Investigating arithmetic questions over local fields is a considerably simpler task than the original problem of analyzing them over number fields. This naturally brings us to the question underlying the so-called local-global method: when does the fact that a given property holds over all completions K_v of a number field K imply that it also holds over K? One of the basic results of this kind is the classical

Theorem 1.14 (Hasse–Minkowski) *Let $f = f(x_1, \ldots, x_n)$ be a nondegenerate quadratic form over an algebraic number field K. If f is isotropic*[2] *over all completions K_v, then f is isotropic over K as well.*

If, in a particular situation, the transition from local to global is possible, we say that in this case, the *local-global principle* (also called the *Hasse principle*) holds. As we will see in subsequent chapters, various forms of the local-global principle are critical to the arithmetic theory of algebraic groups. However, we would like to point out that the local-global principle does not always hold, which we illustrate by the following classical example.

First, we need to discuss the connection between the adele ring A_K of K and the adele ring A_L of a finite extension L of K. The point is that there is a natural (algebraic and topological) isomorphism $A_K \otimes_K L \simeq A_L$, which is obtained from the local isomorphisms $K_v \otimes_K L \simeq \prod_{w|v} L_w$ in (1.2); all we need to observe is that for almost all v in V_f^K, these induce isomorphisms $\mathcal{O}_v \otimes \mathcal{O}_L \simeq \prod_{w|v} \mathcal{O}_w$. Furthermore, (1.3) shows that the norm and trace maps $N_{L/K}$ and $\mathrm{Tr}_{L/K}$ extend to the maps

$$N_{L/K} \colon A_L \to A_K \quad \text{and} \quad \mathrm{Tr}_{L/K} \colon A_L \to A_K$$

defined by

$$N_{L/K}((x_w)) = \left(\left(\prod_{w|v} N_{L_w/K_v}(x_w) \right)_v \right),$$

[2] I.e., the equation $f(x_1, \ldots, x_n) = 0$ has a nontrivial solution.

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

$$\mathrm{Tr}_{L/K}((x_w)) = \left(\left(\sum_{w|v} \mathrm{Tr}_{L_w/K_v}(x_w)\right)_v\right).$$

One can easily verify that the norm map $N_{L/K}$ thus defined induces a continuous homomorphism of idele groups $N_{L/K}\colon J_L \to J_K$. We say that the *Hasse norm principle* holds for the extension L/K if

$$N_{L/K}(J_L) \cap K^* = N_{L/K}(L^*).$$

Given $a \in K^*$, for almost all $v \in V_f^K$, we have $a \in U_v$ and the extension L_w/K_v is unramified, so it follows from Proposition 1.3 that the condition $a \in N_{L_w/K_v}(L_w^*)$ is actually equivalent to

$$a \in N_{L/K}\left(\prod_{w|v} L_w^*\right) = N_{L/K}((L \otimes_K K_v)^*) \text{ for all } v \text{ in } V^K.$$

In the language of algebraic geometry, this means that if $f(x_1, \ldots, x_n)$ is the homogeneous polynomial of degree $n = [L\colon K]$ giving the norm of an element $x \in L$ in terms of its coordinates $x_1, \ldots, x_n$ with respect to a fixed basis of L/K, then the equation $f(x_1, \ldots, x_n) = a$ has a solution over each completion K_v. So, the validity of the Hasse norm principle in this situation means that then the equation has a solution over K as well. (It would be incorrect to formulate the norm principle in the form

$$a \in N_{L/K}(L^*) \iff a \in N_{L_w/K_v}(L_w^*) \text{ for all } v \in V^K \text{ and all } w|v$$

since, in general, $N_{L/K}(L^*) \not\subset N_{L_w/K_v}(L_w^*)$ if L/K is not a Galois extension.)

The Hasse norm theorem (cf. Hasse [1930] and [AGNT, corollary of Theorem 6.11]) states that the norm principle always holds for cyclic Galois extensions. On the other hand, it turns out that the norm principle fails for $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{13}, \sqrt{17})$, i.e., when L/K is an abelian Galois extension with Galois group of type (2,2). To be more precise, by a simple computation with Hilbert symbols (cf. [ANT, ex. 5.3]) it can be shown that 5^2 is a local norm everywhere, but is not a global norm. (See [AGNT, §6.3] for a more detailed discussion of the Hasse norm principle.)

1.3 Cohomology

1.3.1 Basic Concepts

By and large, cohomological formalism is used in this book in a rather limited way. A major exception, however, is the Galois cohomology of algebraic

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

groups over local and global fields. This involves noncommutative cohomology, which is typically omitted in most books on homological algebra. So, we recall the relevant definitions, constructions, and results in this section. For completeness, however, we begin with a quick review of some essential properties of ordinary (commutative) cohomology, whose proofs may be found in Cartan and Eilenberg (1956); Serre (1997); Brown (1982), as well as Chapter 4 of [ANT].

Let A be an abelian G-group, i.e., an abelian group on which G acts by automorphisms.[3] Then one can define a family of abelian groups $\{H^i(G,A)\}_{i\geq 0}$ called the *cohomology groups* of G with coefficients in A. Namely, define $H^0(G,A) = A^G$ to be the subgroup of G-fixed elements of A. To define the higher cohomology groups, we first introduce the groups $C^i(G,A)$ of *cochains*, consisting of all functions $f\colon G^i \to A$ (with $C^0(G,A) = A$), together with the *coboundary* operators $d_i\colon C^i(G,A) \to C^{i+1}(G,A)$ given by

$$\begin{aligned}(d_if)(g_1,\dots,g_{i+1}) = g_1f(g_2,\dots,g_{i+1})\\ &+ \sum_{j=1}^{i}(-1)^j f(g_1,\dots,g_jg_{j+1},\dots,g_{i+1})\\ &+ (-1)^{i+1}f(g_1,\dots,g_i).\end{aligned}$$

Then $H^i(G,A) = \ker d_i/\mathrm{im}\ d_{i-1}$; the elements of $\ker d_i =: Z^i(G,A)$ are called *cocycles* and the elements of $\mathrm{im}\ d_{i-1} =: B^i(G,A)$ are called *coboundaries*. A fundamental property of cohomology groups is that they produce a cohomological extension (in other words, form a δ-functor) of the fixed point functor $F(A) = H^0(G,A)$. This means that if

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

is a short exact sequence of G-groups and G-homomorphisms (i.e., homomorphisms that commute with the action of G), then there exist connecting homomorphisms $\delta_i\colon H^i(G,C) \to H^{i+1}(G,A)$ such that the sequence

$$\begin{aligned}&0 \to H^0(G,A) \to H^0(G,B) \to H^0(G,C) \xrightarrow{\delta_0} H^1(G,A) \to \cdots\\ &\to H^i(G,A) \to H^i(G,B) \to H^i(G,C) \xrightarrow{\delta_i} H^{i+1}(G,A) \to \cdots \qquad (1.6)\end{aligned}$$

is exact. (The remaining homomorphisms are induced naturally by the homomorphisms in the original sequence $0 \to A \to B \to C \to 0$.)

Low-dimensional cohomology groups have concrete interpretations. For example, $H^1(G,A)$ is the quotient group of the group of crossed homomorphisms $f\colon G \to A$, which are functions satisfying $f(g_1g_2) = f(g_1) + g_1f(g_2)$,

[3] It is more common to refer to such an A as a *G-module*, since giving A the structure of a G-group is equivalent to giving it the structure of a module over the integral group ring $\mathbb{Z}[G]$. We use the term “G-group” to be consistent with the terminology used in the noncommutative setting.

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

modulo the subgroup consisting of maps of the form $f(g) = ga - a$ for some a in A. In particular, if G acts trivially on A, then $H^1(G,A) = \text{Hom}\ (G,A)$. On the other hand, if $G = \langle\sigma\rangle$ is a cyclic group of order n, then for any G-group A we have $H^1(G,A) = A_0/A_1$, where A_0 is the kernel of the operator $\text{Tr}\, a = a + \sigma a + \cdots + \sigma^{n-1}a$, and A_1 is the subgroup consisting of elements of the form $\sigma a - a$ with a in A.

Next, $H^2(G,A)$ is the quotient of the group of *factor sets*, i.e., functions $f\colon G \times G \to A$ satisfying

$$g_1 f(g_2,g_3) - f(g_1g_2,g_3) + f(g_1,g_2g_3) - f(g_1,g_2) = 0,$$

modulo the subgroup of *trivial* factor sets, which consists of functions of the form

$$f(g_1,g_2) = \varphi(g_1) + g_1\varphi(g_2) - \varphi(g_1g_2)$$

for some function $\varphi\colon G \to A$. Factor sets arise naturally in the study of group extensions E of G by A, i.e., of exact sequences of the form

$$1 \to A \to E \to G \to 1.$$

More specifically, using factor sets, one establishes a bijection between the elements of $H^2(G,A)$ and the equivalence classes of extensions that induce the given action of G on A. In particular, if G acts trivially on A, then $H^2(G,A)$ parametrizes central extensions of G by A. In [AGNT, Chapter 9], one encounters the group $H^2(G,\mathbf{J})$, where $\mathbf{J} = \mathbb{Q}/\mathbb{Z}$ and G acts trivially on $\mathbf{J}$, which is called the *Schur multiplier* of G. The following basic facts are needed for the analysis there.

Lemma 1.15 (1) *Let* $1 \to \mathbf{J} \longrightarrow E \xrightarrow{\rho} G \to 1$ *be a central extension. Then for any two subgroups* $A, B \subset G$ *that commute elementwise, the map*

$$\varphi\colon A \times B \to \mathbf{J},\ \ (a,b) \mapsto [\tilde{a},\tilde{b}],$$

where $\tilde{a} \in \rho^{-1}(a), \tilde{b} \in \rho^{-1}(b)$ *and* $[x,y] = xyx^{-1}y^{-1}$, *is well defined and bimultiplicative.*

(2) *If G is a finitely generated abelian group, then the central extension*

$$1 \to \mathbf{J} \to E \to G \to 1$$

is trivial (i.e., splits) if and only if E is abelian. In particular, if G is cyclic, then $H^2(G,\mathbf{J}) = 0$.

The first statement is proved by direct computation. The proof of the second one relies on the divisibility of $\mathbf{J}$ and the fact that an abstract group whose quotient by a central subgroup is cyclic, is necessarily commutative.

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

Let us also mention the computation of $H^2(S_n, \mathbf{J})$ for the symmetric group S_n.

Lemma 1.16 (1) *If $n \leq 3$, then for any subgroup H of S_n, we have $H^2(H, \mathbf{J}) = 0$.*

(2) *If $n \geq 4$, then $H^2(S_n, \mathbf{J})$ has order 2 and for any subgroup $C \subset S_n$ generated by two disjoint transpositions, the restriction map*

$$H^2(S_n, \mathbf{J}) \to H^2(C, \mathbf{J})$$

(defined below) is an isomorphism.

PROOF: For any finite group G and any prime p dividing its order, the p-torsion subgroup of $H^i(G, A)$ injects into $H^i(G_p, A)$ for each $i \geq 1$, where G_p is any Sylow p-subgroup of G (cf. [ANT], Chapter 4, §6). Therefore, assertion (1) follows from Lemma 1.15(2) and the fact that for $n \leq 3$, the Sylow subgroups of S_n are all cyclic.

The fact that $H^2(S_n, \mathbf{J})$ has order 2 for $n \geq 4$ was discovered by Schur (1911) (cf. also Huppert [1967]). Also, it is not difficult to see that $H^2(C, \mathbf{J})$ has order 2. Therefore, it suffices to find a cocycle α in $H^2(S_n, \mathbf{J})$ whose restriction to C is nontrivial. We can construct it as follows: consider the abstract group $\tilde{S}_n$ with generators σ, τ_i $(i = 1, \ldots, n-1)$ and relations

$$\sigma^2 = \tau_i^2 = [\tau_i, \sigma] = 1, \quad i = 1, \ldots, n-1,$$

$$(\tau_i \tau_{i+1})^3 = 1, \quad i = 1, \ldots, n-2, \tag{1.7}$$

$$[\tau_i, \tau_j] = \sigma, \quad i + 1 < j.$$

Since S_n is generated by the transpositions $(i, i+1)$, for $i = 1, \ldots, n-1$, with the defining set of relations

$$(i, i+1)^2 = 1, \quad i = 1, \ldots, n-1,$$

$$((i, i+1)(i+1, i+2))^3 = 1, \quad i = 1, \ldots, n-2, \tag{1.8}$$

$$[(i, i+1), (j, j+1)] = 1, \quad i + 1 < j$$

(cf. Huppert [1967]), there exists a unique homomorphism $\tilde{S}_n \xrightarrow{\theta} S_n$ such that $\theta(\sigma) = 1, \theta(\tau_i) = (i, i+1)$. It follows from (1.7) and (1.8) that $\ker \theta \subset \tilde{S}_n$ is the cyclic central subgroup of order two generated by σ. We identify σ with $\frac{1}{2} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ and let α denote the cocycle in $H^2(S_n, \mathbf{J})$ corresponding to the

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

extension $\tilde{S}_n \xrightarrow{\theta} S_n$. In other words, consider an arbitrary section $\varphi\colon S_n \to \tilde{S}_n$ and let

$$\alpha(g,h) = \varphi(g)\varphi(h)\varphi(gh)^{-1}.$$

Replacing C by a conjugate, we may assume that C is generated by the transpositions (12) and (34). If the restriction of α to C were trivial, then by Lemma 1.15(2), $\theta^{-1}(C)$ must be abelian. However,

$$[\varphi((1,2)),\varphi((3,4))] = [\tau_1,\tau_2] = \sigma \neq 1,$$

a contradiction. □

The only higher cohomology groups that we will need are the groups $H^3(G,\mathbb{Z})$, where G is a finite group acting trivially on $\mathbb{Z}$, which arise in the analysis of the obstruction to the Hasse norm principle (cf. [AGNT, §6.3]). However, as the following lemma shows, their computation reduces to that of $H^2(G,\mathbf{J})$.

Lemma 1.17 *Let G be a finite group. Then there exists a natural isomorphism* $H^3(G,\mathbb{Z}) \simeq H^2(G,\mathbf{J})$, *where* $\mathbb{Z}$ *and* $\mathbf{J}$ *are considered as trivial G-modules.*

Indeed, it is well known (cf. [ANT, Chapter 4, §6]) that the cohomology groups $H^i(G,A)$ are annihilated by multiplication by $|G|$. Since the additive group $\mathbb{Q}$ is uniquely divisible, it follows that $H^i(G,\mathbb{Q}) = 0$ for all $i \geq 1$. As the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbf{J} \to 0$ yields the exact sequence

$$0 = H^2(G,\mathbb{Q}) \to H^2(G,\mathbf{J}) \to H^3(G,\mathbb{Z}) \to H^3(G,\mathbb{Q}) = 0,$$

the desired result follows.

It is clear that $H^i(G,A)$ is functorial in the second argument, viz. any G-homomorphism of abelian G-groups $f\colon A \to B$ induces a homomorphism of cohomology groups $f^*\colon H^i(G,A) \to H^i(G,B)$. We will now discuss some aspects of functoriality in the first argument. First, if H is a subgroup of G, then by restricting cocycles to H we obtain the *restriction map*

$$\mathrm{res}\colon H^i(G,A) \to H^i(H,A).$$

Next, if N is a normal subgroup of G and A an abelian G-group, then the group of fixed points A^N is a (G/N)-group, and the canonical homomorphism $G \to G/N$ induces the *inflation map*

$$\inf\colon H^i(G/N,A^N) \to H^i(G,A).$$

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

Moreover, in this case one can define an action of G/N on $H^i(N,A)$ such that the image of the restriction map $\mathrm{res}\colon H^i(G,A) \to H^i(N,A)$ lies in the group of fixed points $H^i(N,A)^{G/N}$. Lastly, one can define the *transgression map*

$$\mathrm{tra}\colon H^1(N,A)^{G/N} \to H^2(G,A^N)$$

such that we have an exact sequence

$$\begin{aligned}0 \to H^1(G/N,A^N) \overset{\mathrm{inf}}{\to} H^1(G,A) \overset{\mathrm{res}}{\to} H^1(N,A)^{G/N} \\ \overset{\mathrm{tra}}{\to} H^2(G/N,A^N) \overset{\mathrm{inf}}{\to} H^2(G,A),\end{aligned} \qquad (1.9)$$

which is actually the initial segment of the Hochschild–Serre spectral sequence corresponding to the extension

$$1 \to N \to G \to G/N \to 1$$

(we refer the reader to Koch [1970] for details of the construction).

Let us now recall a method that allows one to replace the cohomology of a subgroup $H \subset G$ by that of G. First, given any H-module A, we define the *induced* G-module $\mathrm{ind}_G^H(A)$ as the set of all maps $f\colon G \to A$ satisfying $f(hg) = hf(g)$ for all $g \in G$ and $h \in H$; the G-action on $\mathrm{ind}_G^H(A)$ is given by $(gf)(x) = f(xg)$. The evaluation map at the identity $\mathrm{ind}_G^H(A) \to A, f \mapsto f(1)$, gives rise to a homomorphism

$$H^i(G,\mathrm{ind}_G^H(A)) \to H^i(H,A). \qquad (1.10)$$

It turns out that this homomorphism is an isomorphism ("Shapiro's Lemma"). Now assume that H is of finite index in G and that A is a G-group. Let $\pi : \mathrm{ind}_G^H(A) \to A$ be the G-homomorphism given by

$$\pi(f) = \sum_{x \in G/H} xf(x^{-1}).$$

Passing to cohomology, we obtain the *corestriction map*

$$\mathrm{cor}\colon H^i(H,A) \simeq H^i(G,\mathrm{ind}_G^H(A)) \to H^i(G,A),$$

where $\simeq$ denotes the inverse of the isomorphism in (1.10), and the second map is induced by π. Note that in dimension zero, $\mathrm{cor}\colon A^H \to A^G$ coincides with the trace map $\mathrm{Tr}(a) = \sum_{g \in G/H} ga$ (or, in multiplicative notation, the norm map).

Sometimes one needs to consider continuous cohomology of a topological group G with coefficients in a topological abelian group A endowed with a continuous action $G \times A \to A$. These cohomology groups are defined by considering continuous cochains in place of the usual ones. In this book, we will deal exclusively with continuous cohomology of a profinite (i.e., compact

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

totally disconnected) group G with coefficients in a discrete G-group A. In this setting, the continuity of the action of G on A means that $A = \bigcup_U A^U$, where the union is taken over all open normal subgroups $U \subset G$. A profinite group G can be described as the projective (inverse) limit $G = \varprojlim G/U$, where U runs over a fundamental system of neighborhoods of the identity consisting of normal subgroups (the basic properties of profinite groups will be reviewed in §3.2); then the cohomology group $H^i(G,A)$ of a discrete G-group A can be written as the inductive (direct) limit $\varinjlim H^i(G/U, A^U)$ taken with respect to the inflation maps $H^i(G/U, A^U) \to H^i(G/V, A^V)$ for $U \supset V$. An important example of a continuous action of a profinite group on a discrete group is when the absolute Galois group $\mathcal{G} = \mathcal{G}(\bar{K}/K)$ of a perfect field K (endowed with the Krull topology) acts on the additive or multiplicative group of $\bar{K}$ or on some other object A with a K-structure (cf. §2.2). Then the corresponding cohomology groups $H^i(\mathcal{G}, A)$ are called *Galois cohomology* groups and denoted $H^i(K,A)$.

One can easily show that the cohomology of a profinite group G with coefficients in a discrete group A retains all the standard properties of abstract cohomology. In particular, a short exact sequence of discrete G-groups and G-homomorphisms $0 \to A \to B \to C \to 0$ gives rise to the long exact cohomology sequence (1.6), and an extension $1 \to N \to G \to G/N \to 1$ of profinite groups induces the initial segment of the Hochschild–Serre spectral sequence (1.9).

1.3.2 Non-abelian Cohomology

In the theory of algebraic groups, one often encounters cocycles with values in the group of points of an algebraic group over some (finite or infinite) Galois extension of the base field, i.e., generally speaking, in a noncommutative group. Such noncommutative cocycles arise elsewhere, for example in the study of crossed products of a noncommutative algebra with a finite group. We refer the reader to Giraud (1971) for a detailed study of noncommutative cohomology and its various applications. In this section, we will briefly review some basic concepts related to noncommutative cohomology (cf. Serre [1997] for the details) that we will need in our treatment of the Galois cohomology of algebraic groups.

Let G be a (discrete or profinite) group that acts on a set A; in the topological setting, we assume that A is discrete and the action of G is continuous. We then call A a *G-set*. If A is a group and G acts on A by group automorphisms, we

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

call A a *G-group*. Given a G-set A, we define $H^0(G,A)$ to be the set A^G of G-fixed elements. If A is a G-group, then clearly $H^0(G,A)$ is a group.

For a G-group A, a continuous map $f\colon G \to A$ is said to be a *1-cocycle* with values in A if, for any s,t in G, we have $f(st) = f(s)s(f(t))$. It is often convenient to treat 1-cocycles as families indexed by elements of G and to write f as $\{f_s\colon s \in G\}$ where $f_s = f(s)$. Sometimes we will use exponential notation for the action of G, writing ${}^s a$ instead of $s(a)$. With these notations, the 1-cocycle condition becomes $f_{st} = f_s{}^s f_t$. The set of all 1-cocycles will be denoted by $Z^1(G,A)$. Note that $Z^1(G,A)$ is always nonempty as it contains the trivial cocycle given by $f_s = e$, the identity element of A, for all s in G. Two cocycles (a_s) and (b_s) are said to be *equivalent* if there is an element c in A such that $b_s = c^{-1}a_s{}^s c$ for all s in G. (One can easily verify that this indeed defines an equivalence relation on $Z^1(G,A)$.) The set of equivalence classes is called the *first cohomology set* and is denoted by $H^1(G,A)$. If A is an abelian group, then this definition of H^1 is consistent with the one given in §1.3.1; in particular, $H^1(G,A)$ is then an abelian group. In general, $H^1(G,A)$ does not have any natural group structure and is only a pointed set whose distinguished element is the equivalence class of the trivial cocycle. As in the commutative case, if $G = \varprojlim G/U$ is a profinite group, then $H^1(G,A) = \varinjlim H^1(G/U, A^U)$ is the direct limit of pointed sets taken relative to the inflation maps $H^1(G/U, A^U) \to H^1(G/V, A^V)$ for $U \supset V$, defined in the obvious way. In general, if $g\colon H \to G$ is a group homomorphism and $f\colon A \to B$ is a homomorphism of a G-group A into an H-group B compatible with g, i.e., satisfying $f({}^{g(s)}a) = {}^s f(a)$ for all $s \in H, a \in A$, then we can define a map $Z^1(G,A) \to Z^1(H,B)$ by sending (a_s) to $(b_s = f(a_{g(s)}))$, which then induces a map of pointed sets $H^1(G,A) \to H^1(H,B)$.

We say that a sequence of cohomology sets is *exact* if it is exact as a sequence of pointed sets, i.e., if the preimage of the distinguished element is equal to the image of the preceding map. (The distinguished element in the zero dimensional cohomology $H^0(G,A)$ is the identity element of A.) We now describe some useful exact sequences that we will need later. Let A be a subgroup of a G-group B that is invariant under the action of G. Then there is a natural action of G on B/A which makes B/A into a G-set, and we can consider the set $H^0(G,B/A)$, whose distinguished element is the coset A. For any element of $H^0(G,B/A) = (B/A)^G$, choose a representative b in B, and for s in G let $a_s = b^{-1}\,{}^s b$. It is easily seen that $a_s \in A$ and $(a_s) \in Z^1(G,A)$. Moreover, the equivalence class of this cocycle does not depend on the choice of b, so we obtain a map $\delta\colon H^0(G,B/A) \to H^1(G,A)$.

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

Direct computation shows that we have the following exact sequence of pointed sets

$$1 \to H^0(G,A) \to H^0(G,B) \to H^0(G,B/A) \xrightarrow{\delta} H^1(G,A) \xrightarrow{\alpha} H^1(G,B), \quad (1.11)$$

where α is induced by the embedding $A \hookrightarrow B$. Furthermore, if $c_1, c_2 \in H^0(G,B/A)$, then $\delta(c_1) = \delta(c_2)$ if and only if there exists b in B^G with $c_2 = bc_1$. Consequently, the elements of the kernel of the map $H^1(G,A) \to H^1(G,B)$ are in one-to-one correspondence with the orbits of B^G on $(B/A)^G$. If A is a normal subgroup of B, then (1.11) can be extended by one more term:

$$\cdots \to H^0(G,B/A) \xrightarrow{\delta} H^1(G,A) \xrightarrow{\alpha} H^1(G,B) \xrightarrow{\beta} H^1(G,B/A). \quad (1.12)$$

Of special interest is the case where A is a central subgroup of B, as this is precisely the situation arising in the analysis of universal covers of algebraic groups. Set $C = B/A$ and let $\varphi\colon B \to C$ be the canonical homomorphism. Then $H^1(G,A)$ is a group and the map $\delta\colon H^0(G,C) = C^G \to H^1(G,A)$ is a group homomorphism, which in the sequel will be called the *coboundary map*. Using the centrality of A, we can define a natural action of the group $H^1(G,A)$ on the set $H^1(G,B)$ as follows: given $a = (a_s) \in Z^1(G,A)$ and $b = (b_s) \in Z^1(G,B)$, we set $a \cdot b = (a_s b_s) \in Z^1(G,B)$. It turns out that the orbits of this action are precisely the fibers of the map $\beta\colon H^1(G,B) \to H^1(G,C)$. Furthermore, since A is commutative, the group $H^2(G,A)$ is defined, and as we will now show, there is a map $\partial\colon H^1(G,C) \to H^2(G,A)$ extending (1.12) to an exact sequence

$$\cdots \to H^1(G,B) \xrightarrow{\beta} H^1(G,C) \xrightarrow{\partial} H^2(G,A). \quad (1.13)$$

Let $c = (c_s) \in Z^1(G,C)$, and for each s in G, let b_s in B be such that $\varphi(b_s) = c_s$. Then set $a_{s,t} = b_s {}^s b_t b_{st}^{-1}$. It is clear that $a_{s,t} \in A$ and moreover, one easily checks that the map $G \times G \to A$ given by $(s,t) \mapsto a_{s,t}$ is a 2-cocycle (i.e., an element of $Z^2(G,A)$). It turns out that the cohomology class of this cocycle depends neither on the choice of the cocycle c in its cohomology class in $H^1(G,C)$ nor on that of the elements b_s, so we obtain a well-defined connecting morphism $\partial\colon H^1(G,C) \to H^2(G,A)$. The fact that (1.13) is exact is verified by direct computation. Note that in the noncommutative case, ∂ may not be related to any group structure; moreover, its image in $H^2(G,A)$ is generally not a subgroup.

In the noncommutative case, the exact sequences described earlier carry substantially less information than in the commutative case, as information about the kernel of a map of pointed sets generally does not allow us to draw any conclusions about other fibers. This difficulty can be partially overcome

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

by using a method based on the concept of *twisting* (cf. Serre [1997], Chapter 1, §5). We now recall some basic definitions. Let A be a G-group and F be a G-set with a given A-action that is compatible with the action of G, i.e., $s(a \cdot f) = s(a) \cdot s(f)$ for any $s \in G, a \in A, f \in F$. Then, given an arbitrary cocycle $a = (a_s) \in Z^1(G,A)$, we can define a new action of G on F by the formula

$$\bar{s}(f) = a_s(s(f)) \quad \text{for } s \text{ in } G.$$

We denote F equipped with this action by ${}_aF$, and say that ${}_aF$ is obtained from F by twisting using a. It is easy to see that ${}_aF$ depends functorially on F (with respect to A-morphisms $F \to F'$) and that twisting commutes with direct products. If a and b are equivalent cocycles, then the G-sets ${}_aF$ and ${}_bF$ are isomorphic. Moreover, if F has some additional structure (such as that of a group) that is preserved by the action of A, then ${}_aF$ also inherits this structure. We will examine a whole series of examples of twists in §2.3, but for now we will limit ourselves to one example that comes up in the analysis of exact sequences. Namely, consider the case where $A = F$ acts on itself by inner automorphisms. Then, for any cocycle a in $Z^1(G,A)$ the twisted group ${}_aA$ is defined, and moreover, the first cohomology sets of A and $A' = {}_aA$ are related as follows:

Lemma 1.18 *There is a bijection $t_a\colon Z^1(G,A') \to Z^1(G,A)$ defined by sending a cocycle $x = (x_s)$ in $Z^1(G,A')$ to the cocycle $y = (x_s a_s)$ in $Z^1(G,A)$. Passing to cohomology, t_a induces a bijection $\tau_a\colon H^1(G,A') \to H^1(G,A)$, which takes the distinguished element of $H^1(G,A')$ to the class of the cocycle a.*

This enables us to "multiply" cocycles, although the result has values in the twisted group. By this method, replacing the groups in sequences (1.11)–(1.13) by the corresponding twisted groups (i.e., by *twisting* these sequences), one can describe the fibers of all the maps in the original sequences. For example, take $a \in Z^1(G,A)$, and let us describe the fiber $\alpha^{-1}(\alpha(a))$ in the sequence (1.11), where a is also used to denote the corresponding cohomology class in $H^1(G,A)$. For this, we need to pass to the twisted groups $A' = {}_aA$ and $B' = {}_aB$ and examine the corresponding exact sequence:

$$1 \to H^0(G,A') \to H^0(G,B') \to H^0(G,B'/A') \xrightarrow{\delta} H^1(G,A') \xrightarrow{\alpha'} H^1(G,B'). \tag{1.11$'$}$$

Then the bijection τ_a of Lemma 1.18 gives rise to a bijection between the elements of $\ker \alpha'$ and those of the fiber $\alpha^{-1}(\alpha(a))$. On the other hand, it follows

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

from (1.11′) that the elements of ker α' are in one-to-one correspondence with the orbits of $(B')^G$ on $(B'/A')^G$.

We will next give a criterion for the class of a cocycle $b \in Z^1(G,B)$ to lie in the image of α. For this, we consider the action of B on the homogeneous space B/A by left translations; then one can define the twisted space ${}_b(B/A)$ for any b in $Z^1(G,B)$.

Lemma 1.19 *$b \in im\,\alpha \Leftrightarrow H^0(G, {}_b(B/A)) \neq \emptyset$.*

The fibers of ∂ in the sequence (1.13) are computed in a similar way. Namely, let $c = (c_s) \in Z^1(G,C)$. Since A is a central subgroup of B, the conjugation action of B descends to an action of C that is trivial on A. Twisting the exact sequence $1 \to A \to B \to C \to 1$ by means of c, we obtain the exact sequence $1 \to A \to {}_cB \to {}_cC \to 1$, which gives rise to a new connecting morphism ∂_c: $H^1(G, {}_cC) \to H^2(G,A)$. Direct computation shows that this map interacts with the bijection $\tau_c : H^1(G, {}_cC) \to H^1(G,C)$ from Lemma 1.18 as follows:

$$\partial(\tau_c(x)) = \partial_c(x)\partial(c),$$

where the product is taken in $H^2(G,A)$. It follows that the elements of the fiber $\partial^{-1}(\partial(c))$ are in one-to-one correspondence with the elements of ker ∂_c, which in turn correspond bijectively to the orbits of $H^1(G,A)$ on $H^1(G, {}_cB)$.

If H is a normal subgroup of G (which we assume to be closed in the topological setting), then, as in the commutative case, the quotient group G/H acts on A^H, so one can define the set $H^1(G/H, A^H)$ and the inflation map $H^1(G/H,A^H) \to H^1(G,A)$. If $H^1(G,A) \to H^1(H,A)$ is the restriction map, then the sequence

$$1 \to H^1(G/H, A^H) \to H^1(G,A) \to H^1(H,A),$$

which is the noncommutative analog of the Hochschild–Serre spectral sequence (1.9), is exact.

We conclude this section by considering induced sets and a noncommutative version of Shapiro's lemma. Since these topics are not treated in Serre (1997), we provide all the details. Let H be a (closed) subgroup of G. Then for any H-set (respectively H-group) B we can define the G-set (respectively G-group) $A = \mathrm{ind}_G^H(B)$ consisting of all (continuous) maps a: $G \to B$ satisfying $a(ts) = {}^t a(s)$ for all $t \in H$, $s \in G$, on which G acts by ${}^r a(s) = a(sr)$ for r in G. The G-set (respectively G-group) A, or any G-set (G-group) that is isomorphic to A, is said to be *induced*. The map $A \to B$ given by $a \mapsto a(1)$ is compatible with the inclusion $H \subset G$, hence it induces maps

$$\varphi_i : H^i(G,A) \to H^i(H,B) \ \text{ for } \ i = 0, 1.$$

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

Proposition 1.20 (SHAPIRO'S LEMMA, NONCOMMUTATIVE VERSION). *The maps φ_i are bijections.*

PROOF: We will consider the cases $i = 0$ and $i = 1$ separately. First, let $i = 0$. If $a \in H^0(G, A)$, then a is a map $G \to B$, which is fixed by the action of G, i.e., $a = {}^r a$ for all $r \in G$. The definition of the G-action on A shows that the latter is equivalent to $a(s) = a(sr)$ for all $s, r \in G$, so setting $s = 1$ we see a is a constant map. By construction $\varphi_0(a) = a(1) \in B^H = H^0(H, B)$, hence $\varphi_0(a) = \varphi_0(b)$ implies $a = b$, proving that φ_0 is injective. On the other hand, for any c in $H^0(H, B)$, the constant map $a\colon G \to B$ given by $a(s) = c$ lies in A; moreover, it is clear that $a \in H^0(G, A)$ and $\varphi_0(a) = c$. Thus, φ_0 is surjective, hence bijective.

Now let $i = 1$. To show that φ_1 is injective, suppose we have cocycles $a = (a_r)$ and $b = (b_r) \in Z^1(G, A)$ such that φ_1 takes the same value on the corresponding cohomology classes. This means that there exists $c \in B$ such that

$$a_r(1) = c^{-1} b_r(1)\, {}^r c \quad \text{for all} \quad r \in H.$$

Then, letting d be an element of A such that $d(1) = c$ and replacing b by the equivalent cocycle $b' = (d^{-1} b_r\, {}^r d)$, we may assume that

$$a_r(1) = b_r(1) \quad \text{for all} \quad r \in H. \tag{1.14}$$

The definition of a 1-cocycle yields the following identities for all $r, s, t \in G$:

$$\begin{aligned} a_{rs}(t) &= a_r(t)\, {}^r a_s(t) = a_r(t) a_s(tr), \\ b_{rs}(t) &= b_r(t)\, {}^r b_s(t) = b_r(t) b_s(tr). \end{aligned}$$

Plugging in $r = t^{-1}$ in (1.14), we obtain

$$a_{t^{-1}s}(t) b_{t^{-1}s}(t)^{-1} = a_{t^{-1}}(t) b_{t^{-1}}(t)^{-1} \tag{1.15}$$

for all s in H. Let us define a function $c\colon G \to B$ by

$$c(t) = b_{t^{-1}}(t) a_{t^{-1}}(t)^{-1}.$$

Then (1.15) implies that for all $s \in H$ we have

$$\begin{aligned} c(st) &= b_{t^{-1}s^{-1}}(st) a_{t^{-1}s^{-1}}(st)^{-1} \\ &= s(b_{t^{-1}s^{-1}}(t) a_{t^{-1}s^{-1}}(t)^{-1}) = s(b_{t^{-1}}(t) a_{t^{-1}}(t)^{-1}) = s(c(t)), \end{aligned}$$

proving that $c \in A$. On the other hand, one easily verifies that $a_r = c^{-1} b_r\, {}^r c$ for all r in G, so a and b are equivalent cocycles. This proves that φ_1 is injective.

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

To prove surjectivity, let us take an arbitrary cocycle $b = (b_r) \in Z^1(H, B)$. Let $v \colon H\backslash G \to G$ be a (continuous) section such that $v(H) = 1$. For s in G, set $w(s) = sv(Hs)^{-1} \in H$. We define $a_s \colon G \to B$ for $s \in G$ by

$$a_s(t) = {}^{w(t)}b_{w(v(t)s)}.$$

Direct computation shows that $a_s \in A$ and the family $a = (a_s)$ is a cocycle in $Z^1(G, A)$ such that $\varphi_1(a) = b$. This establishes surjectivity and completes the proof of the proposition. □

The following simple statement is often useful:

Lemma 1.21 *Suppose H is of finite index in G. Then a G-group A is induced (with respect to H) if and only if there exists an H-subgroup $B \subset A$ such that A is the direct product of the translates ${}^sB$, where s runs over some system of right coset representatives modulo H.*

For example, if L is a finite Galois extension of a number field K with Galois group $\mathcal{G}$, and we fix an extension u of $v \in V^K$ to L and let $\mathcal{H} = \mathcal{G}(u)$ denote the corresponding decomposition group, then it follows from (1.2) that the $\mathcal{G}$-module $L \otimes_K K_v$ is isomorphic to $\mathrm{ind}_{\mathcal{G}}^{\mathcal{H}}(L_u)$.

1.4 Simple Algebras over Local Fields

1.4.1 Simple Algebras and the Brauer Group

Let A be a finite-dimensional central simple algebra over a field K. By the Artin–Wedderburn Theorem, A is isomorphic to a matrix algebra $M_n(D)$ over a unique (up to isomorphism) central division K-algebra D, and then $\dim_K A = n^2 \dim_K D$. In turn, one shows that $\dim_K D$ is the square of a positive integer d, called the *index* of D (and also of A). It is well known that if K is finite or algebraically closed, then necessarily $d = 1$, in other words, there are no noncommutative finite-dimensional central division algebras over K. If $K = \mathbb{R}$ and $d > 1$, then D is isomorphic to the division algebra $\mathbb{H}$ of Hamilton quaternions. Over non-Archimedean local fields and number fields, there exist division algebras of arbitrary index. To describe them we will need several results from the theory of simple algebras (cf., for example, Farb and Dennis [1993]; Gille and Szamuely [2017]; Herstein [1994]; Pierce [1982]).

One of the basic results is the Skolem–Noether Theorem: if B_1 and B_2 are simple subalgebras of a central simple K-algebra A, then any isomorphism $\sigma \colon B_1 \to B_2$ of K-algebras extends to an inner automorphism of A. To analyze

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

the structure of a division algebra D, one often employs maximal subfields $P \subset D$. Any maximal subfield P contains K, the degree $[P\colon K]$ equals d, the index of D, and $D \otimes_K P \simeq M_d(P)$ (i.e., P is a *splitting field* of D). Conversely, any field $P \supset K$ such that $[P\colon K] = d$ and $D \otimes_K P \simeq M_d(P)$ is isomorphic to a maximal subfield of D.

Now consider an arbitrary splitting field P of a simple algebra A (for example, one could take an algebraic closure $\bar{K}$ of K), and fix an isomorphism $\varphi\colon A \otimes_K P \simeq M_r(P)$. Then the map $\mathrm{Nrd}_{A/K}(x) = \det \varphi(x \otimes 1)$, called the *reduced norm*, is multiplicative and moreover can be shown to be independent of P and φ. The reduced norm is given by a homogeneous polynomial of degree r with coefficients in K, in terms of the coordinates of x with respect to a given basis A over K; in particular, $\mathrm{Nrd}_{A/K}(A^*) \subset K^*$. An important property of the reduced norm is that for any x in D and any maximal subfield $P \subset D$ containing x, the reduced norm $\mathrm{Nrd}_{D/K}(x)$ coincides with the usual norm $N_{P/K}(x)$. The study of the multiplicative group A^* essentially reduces to the study of the image $\mathrm{Nrd}_{A/K}(A^*)$ and the corresponding special linear group $SL_1(A) = \{x \in A^*\colon \mathrm{Nrd}_{A/K}(x) = 1\}$. The structure of $SL_1(A)$ (particularly when $A = M_n(D)$ with $n > 1$, cf. [AGNT, §7.2]) in turn depends on whether or not $SL_1(A)$ coincides with the commutator subgroup $[A^*, A^*]$ (the inclusion $[A^*, A^*] \subset SL_1(A)$ is clear from the multiplicativity of the reduced norm). The question of whether equality always holds, which is obviously equivalent to the question of the triviality of the *reduced Whitehead group* $SK_1(A) = SL_1(A)/[A^*, A^*]$ from algebraic K-theory, was raised by Tannaka and Artin in 1943 (see [AGNT, §7.2] regarding the connection between these problems and the well-known Kneser–Tits conjecture in the theory of algebraic groups). In 1975, Platonov showed that the Tannaka–Artin problem in general has a negative solution. In a series of papers, he developed reduced K-theory, which in many cases makes it possible to compute $SK_1(A)$ and establishes its connections with other important problems (cf. [AGNT, Chapter 7]). Nevertheless, we should point out that for central simple algebras over local and global fields, which are the main cases of interest for us, the group $SK_1(A)$ is always trivial. This was proved for local fields by Nakayama and Matsushima (1943) and for number fields by Wang (1950). Since this result will be used repeatedly in the sequel, we will give a new proof that is substantially shorter and more conceptual than the original argument (see Theorem 1.35).

One introduces an equivalence relation for central simple K-algebras by defining $A_1 = M_{n_1}(D_1) \sim A_2 = M_{n_2}(D_2)$ if the division algebras D_1 and D_2 are isomorphic; in the sequel, we let $[A]$ denote the equivalence class of A. Furthermore, one defines the product of two equivalence classes by $[A_1] \cdot [A_2] = [A_1 \otimes_K A_2]$. (Note that the tensor product over K of two simple

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

K-algebras, one of which is central, is also a simple K-algebra.) This operation makes the set of equivalence classes of finite-dimensional central simple K-algebras into an abelian group, with the inverse of $[A]$ being the class of the opposite algebra A° obtained from A by defining a new product $a \cdot b = ba$, where the product in the right-hand side is the original product in A. This group is called the *Brauer group* of K and is denoted by $\mathrm{Br}(K)$. For any extension L/K, the equivalence classes of central simple K-algebras that split over L form a subgroup of $\mathrm{Br}(K)$, which we denote by $\mathrm{Br}(L/K)$. The order of an element $[A]$ in $\mathrm{Br}(K)$ is always finite and is called the *exponent* (or *period*) of A. Note that the exponent of A divides the index, but, in general, the two numbers may be different. An important result in the theory of central simple algebras is that the exponent and index coincide over local and global fields. There is a conjecture due to M. Artin (1982) that this property also holds for the so-called C_2-fields; an important partial result was obtained by A. J. de Jong (2004). For a connection between the exponent and index over general C_m-fields, see Matzri (2016). Let us also note that $\mathrm{Br}(K)$ has a cohomological interpretation, namely, associating to a simple algebra its factor set yields an isomorphism $\mathrm{Br}(K) \simeq H^2(K, \bar{K}^*)$.

1.4.2 Simple Algebras over Local Fields

Throughout this section, K will denote a non-Archimedean local field with valuation v; we let $\mathcal{O}$, $\mathfrak{p}$, and U denote the corresponding valuation ring, valuation ideal, and group of units. Now, let D be a central division K-algebra of index n. The valuation v uniquely extends to D by the formula

$$\tilde{v}(x) = \frac{1}{n} v(\mathrm{Nrd}_{D/K}(x)) \quad \text{for } x \in D, \tag{1.16}$$

and one can show that D is complete with respect to the metric defined by $\tilde{v}$. Let

$$\mathcal{O}_D = \{x \in D \colon \tilde{v}(x) \geq 0\} \text{ and } \mathfrak{P}_D = \{x \in D \colon \tilde{v}(x) > 0\}$$

be the valuation ring and the valuation ideal of $\tilde{v}$, respectively. Clearly, every element $a \in \mathcal{O}_D \backslash \mathfrak{P}_D$ is invertible in $\mathcal{O}_D$, so the quotient $\bar{D} := \mathcal{O}_D / \mathfrak{P}_D$ is a division algebra, called the *residue algebra*. For an element $a \in \mathcal{O}_D$, we typically write $\bar{a}$ to denote its image in $\bar{D}$. Let $f = [\bar{D} \colon k]$ (where k is the residue field of K) and let $e = [\tilde{\Gamma} : \Gamma]$ be the corresponding ramification index (where $\Gamma = v(K^*)$ and $\tilde{\Gamma} = \tilde{v}(D^*)$ are the respective value groups of v and $\tilde{v}$). Then, as in the commutative case (cf. §1.1.2), we have $ef = \dim_K D = n^2$. On the other hand, being a finite division ring, $\bar{D}$ is commutative, and consequently

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

$\bar{D} = k(\alpha)$ for a suitable α in $\bar{D}$. Let $\beta \in \mathcal{O}_D$ be an element such that $\bar{\beta} = \alpha$. Then for the field $L = K(\beta)$ and its corresponding residue field ℓ, we have

$$f = [\bar{D}\colon \bar{K}] = [\ell : k] \leq [L\colon K] = n.$$

It follows from (1.16) that $n\tilde{\Gamma} \subset \Gamma$, so since $\Gamma \simeq \mathbb{Z}$, we see that

$$e = [\tilde{\Gamma} : \Gamma] \leq n.$$

Thus $e = f = n$ and $\bar{D}$ coincides with the residue field ℓ of a suitable subfield $L \subset D$, which is automatically a maximal subfield of D and is unramified over K. Since the value group $\tilde{\Gamma}$ is $\frac{1}{n}\mathbb{Z}$, there exists an element Π in D^*, called a *uniformizer*, such that $\tilde{v}(\Pi) = \frac{1}{n}$. Then we have $\mathfrak{P}_D = \Pi\mathcal{O}_D = \mathcal{O}_D\Pi$, and any other uniformizer $\Pi' \in \mathcal{O}_D$ is of the form $\Pi' = \Pi u$, for some $u \in U_D = \mathcal{O}_D^*$. Similarly, for any $i \geq 1$ we have $\mathfrak{P}_D^i = \Pi^i\mathcal{O}_D = \mathcal{O}_D\Pi^i$.

Let us now fix an unramified maximal subfield $L \subset D$. (We note that any other unramified maximal subfield $L' \subset D$ is isomorphic to L over K, hence is conjugate to L by the Skolem–Noether Theorem.) Then L is cyclic Galois extension of K with Galois group $\mathrm{Gal}(L/K)$ generated by the Frobenius automorphism φ (cf. §1.1.3). Again by the Skolem–Noether Theorem, there exists an element g in D^* such that

$$\varphi(x) = gxg^{-1} \qquad \forall x \in L. \tag{1.17}$$

Then $\tilde{v}(g) \in \frac{1}{n}\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ is well defined; it is called the *invariant* of D and will be denoted $\mathrm{inv}_K D$. The invariant $\mathrm{inv}_K\, A$ of a central simple K-algebra $A = M_n(D)$ is then defined to be the invariant of D.

Theorem 1.22 *The map $A \mapsto \mathrm{inv}_K\, A$ defines an isomorphism* $\mathrm{Br}(K) \simeq \mathbb{Q}/\mathbb{Z}$. *Moreover, if P/K is a finite extension of degree m, then we have the following commutative diagram, where $[m]$ denotes multiplication by m:*

$$\begin{tikzcd}
\mathrm{Br}(K) \arrow[r, "\mathrm{inv}_K"] \arrow[d, "{\begin{matrix}[A]\\ \downarrow \\ [A\otimes_K P]\end{matrix}}"'] & \mathbb{Q}/\mathbb{Z} \arrow[d, "{[m]}"] \\
\mathrm{Br}(P) \arrow[r, "\mathrm{inv}_P"] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd} \tag{1.18}$$

It follows from the commutativity of (1.18) that given a central division algebra D over K of index n, for any field extension P/K of degree n, we have $D \otimes_K P \simeq M_n(P)$, and consequently P is isomorphic to a maximal subfield of D. Another important observation is that the exponent and index of any

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

central division algebra over K coincide. To prove this, we need to show that if $\tilde{v}(g) = \frac{a}{n}$, then $\gcd(a, n) = 1$. First, note that it follows from (1.16) that $\mathcal{O}_D$ and $\mathfrak{P}_D$ are invariant under conjugation in D and therefore any element $h \in D^*$ induces an automorphism $\sigma_h \colon \bar{x} \mapsto \overline{hxh^{-1}}$ of $\bar{D}$ over k. Set $\sigma = \sigma_\Pi$. Since $\bar{D}$ is commutative, it follows that $\sigma_u =$ id for u in U_D, hence σ is independent of the choice of Π. As we noted earlier, $\bar{D}$ coincides with the residue field ℓ of an unramified maximal subfield $L \subset D$, so actually $\sigma \in \mathrm{Gal}(\ell/k)$. Now, $g = \Pi^a u$ for a suitable $u \in U_D$, so $\varphi = \sigma^a$, where the Frobenius automorphisms of L/K and of ℓ/k are both denoted by φ. Since φ generates $\mathrm{Gal}(\ell/k)$, we necessarily have $\gcd(a, n) = 1$. As a by-product, we have shown that $\sigma = \sigma_\Pi$ generates $\mathrm{Gal}(\ell/k)$, a fact to be used later.

The preceding results on the structure of division algebras over p-adic fields go back to Hasse (1931) and Witt (1937). Subsequently, structure theorems were obtained for a broad class of division algebras over arbitrary Henselian fields (cf. Platonov and Yanchevskiĭ [1987], the survey article by Wadsworth [2002], and the book by Tignol and Wadsworth [2015]).

1.4.3 Multiplicative Structure of Division Algebras over Local Fields

We first establish that for any finite-dimensional central division algebra D over a local field K, we have $\mathrm{Nrd}_{D/K}(D^*) = K^*$ and that $SL_1(D)$ coincides with the commutator group $[D^*, D^*]$. (A more thorough analysis of D^*, based on the filtration by congruence subgroups, will be given in the next section.)

As we have already seen, there exists an unramified maximal subfield $L \subset D$, so the group of units U is contained in $N_{L/K}(L^*) \subset \mathrm{Nrd}_{D/K}(D^*)$ (cf. Proposition 1.3). It remains to show that $\mathrm{Nrd}_{D/K}(D^*)$ also contains a uniformizer $\pi \in K$. For this, we observe that $t^n + (-1)^n \pi$ (where n is the index of D) is an Eisenstein polynomial (cf. §1.1.3), and therefore defines an extension P/K of degree n for which $\pi \in N_{P/K}(P^*)$. But as we noted earlier, P is isomorphic to a maximal subfield of D, and therefore $N_{P/K}(P^*) \subset \mathrm{Nrd}_{D/K}(D^*)$, implying that $\pi \in \mathrm{Nrd}_{D/K}(D^*)$. Thus,

$$\mathrm{Nrd}_{D/K}(D^*) = K^*.$$

Proving that $SL_1(D)$ (which for simplicity we will denote by $D^{(1)}$) coincides with $[D^*, D^*]$ requires somewhat more work. First, we note that

$$L^{(1)} := L \cap D^{(1)}$$

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

is contained in $[D^*, D^*]$. Indeed, since $L^{(1)} = \{t \in L^*: N_{L/K}(t) = 1\}$, by Hilbert's Theorem 90 (cf. Lang [2002, Chapter VI, §6], and §2.2.2), any element $x \in L^{(1)}$ can be written in the form $x = \varphi(y)y^{-1}$ for suitable y in L^*. So, by (1.17) we have $x = gyg^{-1}y^{-1} \in [D^*, D^*]$. Hence the assertion that $D^{(1)} = [D^*, D^*]$ is a consequence of the following result.

Theorem 1.23 (Platonov and Yanchevskiĭ [1973b]) *The normal subgroup of $D^{(1)}$ generated by $L^{(1)}$ coincides with $D^{(1)}$.*

Proof: Let $x \in D^{(1)}$. Then its residue $\bar{x}$ lies in

$$\ell^{(1)} = \{a \in \ell^*: N_{\ell/k}(a) = 1\}.$$

Indeed, due to the fact that $\bar{D} = \ell$, we can write $x = ab$, with a contained in the group of units U_L of L and $b \in 1 + \mathfrak{P}_D$. Then $\bar{x} = \bar{a}$. On the other hand,

$$N_{L/K}(a) = \mathrm{Nrd}_{D/K}(a) = \mathrm{Nrd}_{D/K}(b^{-1}) = N_{M/K}(b)^{-1}$$

for a maximal subfield $M \subset D$ containing b. But $b \in (1 + \mathfrak{P}_D) \cap M = 1 + \mathfrak{P}_M$, so by Proposition 1.5, $N_{M/K}(b^{-1}) \in 1 + \mathfrak{p}$, where $\mathfrak{p}$ is the valuation ideal in K. Therefore,

$$N_{\ell/k}(\bar{a}) = \prod_{i=0}^{n-1} \varphi^i(\bar{a}) = \overline{\prod_{i=0}^{n-1} \varphi^i(a)} = \overline{N_{L/K}(a)} = 1.$$

Since the group $\ell^{(1)}$ is cyclic, there exists an element $z \in \ell^{(1)}$ such that $\bar{x}z$ is a generator of $\ell^{(1)}$, and consequently $\ell = k(\bar{x}z)$. But $z = \bar{y}$ for a suitable y in $L^{(1)}$. Indeed, by Hilbert's Theorem 90 we can write $z = \varphi(s)/s$ for some $s \in \ell^*$; then, if $u \in U_L$ is such that $\bar{u} = s$, the element $y = \varphi(u)/u$ is as required. Furthermore, note that the extension $P := K(xy)$ is an unramified maximal subfield of D, since

$$n \geq [P: K] \geq [k(\overline{xy}): k] = [\ell: k] = n,$$

hence $[P: K] = [k(\overline{xy}): k] = n$. Thus, $P \simeq L$ over K and consequently, by the Skolem–Noether Theorem, $P = sLs^{-1}$ for some $s \in D^*$. Taking into account that $N_{L/K}(L^*) = UK^{*n}$ (Proposition 1.3) and that $\gcd(v(\mathrm{Nrd}_{D/K}(g)), n) = 1$ for g (as in (1.17) – cf. §1.4.2), we see that $\mathrm{Nrd}_{D/K}(s) = \mathrm{Nrd}_{D/K}(g^i c)$ for suitable $i \in \mathbb{Z}$ and $c \in L$. Letting $t = s(g^i c)^{-1}$, we will have

$$P = tg^i cLc^{-1}g^{-i}t^{-1} = tLt^{-1} \quad \text{and} \quad \mathrm{Nrd}_{D/K}(t) = 1.$$

Consequently, $x \in P^{(1)}y^{-1} \subset t^{-1}L^{(1)}tL^{(1)}$. □

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

An interesting consequence of the proof of Theorem 1.23 is that any element of $D^{(1)}$ is the product of at most two commutators. It is not known, however, if every element of $D^{(1)}$ is, in fact, a single commutator.

1.4.4 Filtrations on D^* and $D^{(1)}$

The material of this section is needed only in [AGNT, §9.5], and therefore may be skipped on the first reading.

As before, let D be a division algebra of index n over a local field K. We will continue using the notations introduced in §1.4.2–1.4.3. In addition, we set

$$U_i = 1 + \mathfrak{P}_D^i \ \text{ and } \ C_i = U_i \cap D^{(1)} \ \text{ for } i \geq 1,$$

letting $U_0 = U_D = \mathcal{O}_D^*$ and $C_0 = D^{(1)}$. It follows from (1.16) that U_i and C_i are normal subgroups of D^* (called the *congruence subgroups* of D and $D^{(1)}$ respectively, of level $\mathfrak{P}_D^i$ or simply of level i). Since U_D and $D^{(1)}$ are clearly compact groups, and U_i and C_i are open in U_D and $D^{(1)}$ respectively (and, in fact, constitute a base of neighborhoods of the identity), the indices $[U\colon U_i]$ and $[D^{(1)}\colon C_i]$ are finite. We begin by describing the structure of the quotients U_i/U_{i+1} and C_i/C_{i+1}.

Proposition 1.24 *There are natural isomorphisms*

$$\rho_0\colon U_0/U_1 \to \ell^*, \ \textit{and}$$
$$\rho_i\colon U_i/U_{i+1} \to \ell^+ \ \textit{for} \ i \geq 1,$$

where ℓ^+ denotes the additive group of ℓ. Moreover,

$$\rho_0(C_0) = \ell^{(1)} := \{x \in \ell^* \colon N_{\ell/k}(x) = 1\}$$

and $\rho_i(C_i) = \ell$ if $i \not\equiv 0(\text{mod}\, n)$ and

$$\rho_i(C_i) = \ell^{(0)} := \{x \in \ell \colon \mathrm{Tr}_{\ell/k}(x) = 0\}$$

if $i \equiv 0(\text{mod}\, n)$.

Proof: As above, for a in $\mathcal{O}_D$, we denote by $\bar{a}$ its image in $\ell = \mathcal{O}_D/\mathfrak{P}_D$. Then ρ_0 is induced by $a \mapsto \bar{a}$ and ρ_i $(i \geq 1)$ is induced by $1 + a\Pi^i \mapsto \bar{a}$. (Note that the map ρ_i for $i \geq 1$ depends on the choice of a uniformizer Π.) We computed the image $\rho_0(C_0)$ in the proof of Theorem 1.23. To compute $\rho_i(C_i)$ $(i \geq 1)$, we need the following.

Lemma 1.25 *For $i \geq 1$, we have* $\mathrm{Nrd}_{D/K}(1 + \mathfrak{P}_D^i) = 1 + \mathfrak{p}^j$*, where j is the smallest integer $\geq i/n$.*

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

The proof easily follows from Proposition 1.5.

Now, given $x \in \ell$, pick $a \in \mathcal{O}_D$ so that $\bar{a} = x$. Let $z = 1 + a\Pi^i$. Then $t := \mathrm{Nrd}_{D/K}(z) \in 1 + \mathfrak{p}^j$, where j is the smallest integer $\geq i/n$. If $i \not\equiv 0 \pmod{n}$, then $j \geq \frac{i+1}{n}$, and by Lemma 1.25, there exists $y \in U_{i+1}$ satisfying $\mathrm{Nrd}_{D/K}(y) = t$. Then, for $z_1 = zy^{-1}$, we have $\mathrm{Nrd}_{D/K}(z_1) = 1$, hence $z_1 \in C_i$, and $\rho_i(z_1) = x$. It follows that $\rho_i(C_i) = \ell$ for $i \not\equiv 0 (\mathrm{mod}\, n)$.

Next, suppose that $i = jn$. Since $\mathcal{O}_D = \mathcal{O}_L + \mathfrak{P}_D$, we have

$$\mathfrak{P}_D^i = \mathcal{O}_L \pi^j + \mathfrak{P}_D \pi^j = \mathfrak{p}_L^j + \mathfrak{P}_D^{i+1}$$

(where $\mathcal{O}_L$, $\mathfrak{P}_L$ are, respectively, the valuation ring and the valuation ideal of L; note that $\mathfrak{P}_L = \mathcal{O}_L \pi$ for the uniformizer $\pi \in K$ since L/K is unramified). It follows that

$$U_i \cap L^* = 1 + \mathfrak{p}_L^j \text{ and } U_i = (U_i \cap L^*)U_{i+1}.$$

Then, if $z \in C_i$ is written in the form $z = st$, where $s \in U_i \cap L^*, t \in U_{i+1}$, we have $N_{L/K}(s) = \mathrm{Nrd}_{D/K}(t)^{-1} \in 1 + \mathfrak{p}^{j+1}$. On the other hand, if $s = 1 + r\pi^j$ with $r \in \mathcal{O}_L$, then

$$N_{L/K}(s) = \prod_{m=0}^{n-1} \varphi^m(1 + r\pi^j) \equiv 1 + \mathrm{Tr}_{L/K}(r)\pi^j \pmod{\mathfrak{p}^{j+1}}.$$

Thus, $\mathrm{Tr}_{L/K}(r) \equiv 0 \pmod{\mathfrak{p}}$, and hence $\mathrm{Tr}_{\ell/k}(\bar{r}) = 0$ and $\rho_i(C_i) \subset l^{(0)}$. Conversely, if $\mathrm{Tr}_{L/K}(r) \equiv 0 (\mathrm{mod}\, \mathfrak{p})$, then for $s = 1 + r\pi^j$ we have $N_{L/K}(s) \in 1 + \mathfrak{p}^{j+1}$, so there is a $t \in 1 + \mathfrak{p}_L^{j+1}$ such that

$$N_{L/K}(s) = N_{L/K}(t).$$

Then the element $z = st^{-1} \in L^{(1)} \cap (1 + \mathfrak{p}_L^j)$ satisfies $\rho_i(z) \equiv \bar{r}$. □

Corollary 1.26 *For any $i \geq 0$, the quotients U_0/U_i and C_0/C_i are finite solvable groups. Consequently, the groups U_0 and C_0 are pro-solvable.*

The solvability of the quotients U_0/U_i and C_0/C_i immediately follows from the proposition. As we have noted above, U_i and C_i for $i \geq 1$ constitute a base of neighborhoods of the identity in U_0 and C_0 respectively, and therefore (cf. §3.3)

$$U_0 = \varprojlim U_0/U_i \text{ and } C_0 = \varprojlim C_0/C_i$$

are prosolvable groups.

Now, following Riehm (1970a), we will identify the commutator groups $[C_0, C_i]$ and $[C_1, C_i]$ $(i \geq 1)$. For this, we need the following computation.

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

Lemma 1.27 *Let $x = 1 + a\Pi^i$, $y = 1 + b\Pi^j$, where $a, b \in \mathcal{O}_D$ and $i, j \geq 1$. Then the commutator $[x, y] = xyx^{-1}y^{-1}$ is of the form $1 + c\Pi^{i+j}$ with*

$$\bar{c} = \bar{a}\sigma^i(\bar{b}) - \sigma^j(\bar{a})\bar{b},$$

where σ is the automorphism of ℓ over k given by $\bar{d} \mapsto \overline{\Pi d \Pi^{-1}}$ (cf. §1.4.2). In particular, $[U_i, U_j] \subset U_{i+j}$.

Proof: We will write (s, t) to denote $st - ts$. One easily verifies that

$$[x, y] = 1 + (x - 1, y - 1)x^{-1}y^{-1},$$

and consequently

$$[x, y] = 1 + (a\Pi^i b\Pi^j - b\Pi^j a\Pi^i)x^{-1}y^{-1} = 1 + c\Pi^{i+j},$$

where

$$c = (a\Pi^i b\Pi^{-i} - b\Pi^j a\Pi^{-j})(\Pi^{i+j}x^{-1}y^{-1}\Pi^{-(i+j)}).$$

Passing to the residues and taking into account that $\bar{x} = \bar{y} = 1$, we obtain the required result. □

Theorem 1.28 *Let $n > 2$. Then*

$$(1) \qquad [C_1, C_i] = C_{i+1} \text{ for any } i \geq 1;$$

$$(2) \qquad [C_0, C_i] = \begin{cases} C_i, & \text{if } i \not\equiv 0 (\text{mod } n), \\ C_{i+1}, & \text{if } i \equiv 0 (\text{mod } n). \end{cases}$$

In particular, $[C_0, C_0] = C_1$.

Proof: First, we will show that $\rho_{i+1}([C_1, C_i]) = \rho_{i+1}(C_{i+1})$. Indeed, it follows from Lemma 1.27 and Proposition 1.24 that the image $\rho_i([C_1, C_i])$ is generated as an abelian group by elements of the form

$$\alpha\sigma(\beta) - \sigma^i(\alpha)\beta,$$

where $\alpha \in \ell$, and $\beta \in \ell$ or $\ell^{(0)}$, depending on whether or not i is divisible by n. We leave it to the reader to verify that since $n > 2$, these elements generate ℓ when $i + 1 \not\equiv 0 (\text{mod } n)$ and $\ell^{(0)}$ otherwise, which coincides with $\rho_{i+1}(C_{i+1})$ in all cases. Thus, for any $i \geq 1$ we have

$$[C_1, C_i]C_{i+2} = C_{i+1}. \tag{1.19}$$

Let us now show that actually $[C_1, C_i] = C_{i+1}$. We can either argue directly, as Riehm does, or use Theorem 3.10, which implies that any noncentral normal subgroup of $D^{(1)}$ is open (we should emphasize that the proof of Theorem 3.10 does not rely on Theorem 1.28). Then for a suitable j, we have $[C_1, C_i] \supset C_j$,

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

and we may take j to be the smallest integer with this property. Suppose that $j > i+1$; then $j-2 \geq i$, so that by (1.19), we have

$$[C_1, C_i] \supset [C_1, C_{j-2}]C_j = C_{j-1},$$

which contradicts the definition of j. Thus, $j = i+1$, proving the first assertion.

It follows from (1) that $[C_0, C_i] \supset [C_1, C_i] = C_{i+1}$, so to prove (2), we only need show that

$$\rho_i([C_0, C_i]) = \begin{cases} \ell, & \text{if} \quad i \not\equiv 0 \pmod{n}, \\ 0, & \text{if} \quad i \equiv 0 \pmod{n}. \end{cases} \tag{1.20}$$

Direct computation shows that for $x \in U_D$ and $y = 1 + a\Pi^i$, where $i \geq 1$, we have $\rho_i([x,y]) = (\bar{x}\sigma^i(\bar{x})^{-1} - 1)\bar{a}$. If $i \equiv 0 (\mathrm{mod}\ n)$, then clearly $\rho_i([x,y]) = 0$. On the other hand, if $i \not\equiv 0 (\mathrm{mod}\ n)$, then, using the structure of finite fields, one can easily establish the existence of an element α in $\ell^{(0)}$ such that $\sigma^i(\alpha) \neq \alpha$. Choosing an element x from $D^{(1)}$ such that $\bar{x} = \alpha$ and varying y (i.e., a), we obtain the first equality in (1.20). To complete the proof of Theorem 1.28, we only need to observe that in all cases, we have the inclusion $[C_0, C_0] \subset C_1 = [C_0, C_1]$, and therefore $[C_0, C_0] = C_1$. □

Remark Some refinement of the preceding argument enables one to consider also the case $n = 2$. The results due to Riehm (1970a) are as follows:

If $p = \mathrm{char}\ k$ is $\neq 2$, then all the assertions of Theorem 1.28 still hold; for $n = p = 2$, the analog of assertion (1) assumes the form

$$\begin{aligned} [C_1, C_{2i+1}] &= C_{2i+2} && \text{if either } |k| > 2 \text{ or } i \geq 1; \\ [C_1, C_{2i}] &= C_{2(i+1)} && \text{for all } i. \end{aligned}$$

If $|k| = 2$, then $[C_1, C_1]$ contains C_4 but not C_3. The second assertion of Theorem 1.28 holds in all cases; in particular, we always have $[C_0, C_0] = C_1$.

Corollary 1.29 $C_0 = L^{(1)}[C_0, C_0]$, *where* L *is an unramified maximal subfield of* D.

For $n > 2$ (respectively, $n = 2$), this follows from Theorem 1.28 and Proposition 1.24 (respectively, from the above remark and Proposition 1.24). Another proof, which does not distinguish between the cases $n > 2$ and $n = 2$, can be easily obtained from Theorem 1.23.

In [AGNT, §9.5], one needs information about the structure of the quotients $F(i) = C_i/C_{i+1}$ for ($i \geq 1$) as modules over the group $\Delta = C_0/C_1$ for the action induced by the conjugation action of C_0 (we note by Theorem 1.28

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

the group C_1 acts trivially on $F(i)$). Using the maps ρ_0 and ρ_i from Proposition 1.24, we can identify Δ and $F(i)$ respectively with $\ell^{(1)}$ and $\ell^{(0)}$ or ℓ depending on whether or not i is divisible by n. Then a simple computation shows that the Δ-module structure on $F(i)$ is given by

$$\delta \cdot x = \delta\sigma^i(\delta)^{-1}x \quad \text{for } \delta \in \Delta \text{ and } x \in F(i) \tag{1.21}$$

(we note that the product in the right-hand side is taken in ℓ).

Proposition 1.30 *If $i \not\equiv 0 \,(\mathrm{mod}\ n)$, then $F(i)$ is a simple Δ-module, except when ℓ/k is $\mathbb{F}_9/\mathbb{F}_3$ or $\mathbb{F}_{64}/\mathbb{F}_4$ (where $\mathbb{F}_q$ denotes the finite field with q elements). In the latter case, the Δ-submodules of $F(i) \simeq \mathbb{F}_{64}$ correspond to the vector subspaces of $\mathbb{F}_{64}$ over $\mathbb{F}_8$.*

PROOF: Let m denote the subfield of ℓ generated over the prime subfield by elements of the form $\delta\sigma^i(\delta)^{-1}$ with $\delta \in \ell^{(1)}$. Then the assertion is clearly equivalent to the fact that $m = \ell$ if ℓ/k is different from $\mathbb{F}_9/\mathbb{F}_3$ or $\mathbb{F}_{64}/\mathbb{F}_4$, and $m = \mathbb{F}_8$ if ℓ/k is $\mathbb{F}_{64}/\mathbb{F}_4$. The proof is elementary and is left to the reader. □

Using Proposition 1.30, Riehm obtained a complete description of the normal subgroups of C_0. Since we will not need these results in the sequel, we will limit ourselves to stating the result in the "generic" situation and omitting the information about exceptional cases. For this we set $E_r = (K^* \cap C_0)C_r$ and say that a normal subgroup $N \subset C_0$ has *level* r if $N \subset E_r$ but $N \not\subset E_{r+1}$. Since

$$\bigcap_r E_r = K^* \cap C_0,$$

any noncentral normal subgroup in C_0 has a certain (finite) level.

Theorem 1.31 *Suppose D is not a quaternion algebra over a finite extension of $\mathbb{Q}_2$. If $N \subset C_0$ is a normal subgroup of level r, then*

$$C_{r+1} \subset N \subset E_r.$$

If $n \nmid r$ and the Δ-module $F(r)$ is simple, then the stronger condition $C_r \subset N \subset E_r$ holds.

Note that the inclusion $C_r \subset N \subset E_r$ means that N may differ from a congruence subgroup only by a central subgroup, which provides a complete description of the normal subgroups.

We will also use Proposition 1.30 for a different purpose, namely to describe the space $B = B(F(1), F(r))$ of Δ-invariant bilinear maps

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

$$b\colon F(1) \times F(r) \to \mathbb{F}_p,$$

where $p = \operatorname{char} k$ and Δ acts on $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ trivially.

Theorem 1.32 (PRASAD AND RAGHUNATHAN [1988])

(1) *If* $r \not\equiv -1 \,(\operatorname{mod} n)$*, then* $B = 0$.
(2) *If* $r \equiv -1 \,(\operatorname{mod} n), n > 2$*, then* B *consists precisely of all maps of the form*

$$b(\lambda)(x,y) = \operatorname{Tr}_{\ell/\mathbb{F}_p}(\lambda x \sigma(y)) \text{ with } \lambda \in \ell \tag{1.22}$$

in the case where ℓ/k *is different from* $\mathbb{F}_{64}/\mathbb{F}_4$*, and of maps of the form*

$$b(\lambda,\mu)(x,y) = \operatorname{Tr}_{\ell/\mathbb{F}_p}(\lambda x \sigma(y) + \mu x \sigma(y)^8) \text{ with } \lambda,\mu \in \ell \tag{1.23}$$

in the case where $\ell/k \simeq \mathbb{F}_{64}/\mathbb{F}_4$.

(The appearance of the trace map in (1.22) and (1.23) is not accidental. Indeed, for any finite separable field extension P/M, one has the nondegenerate bilinear form

$$f(x,y) = \operatorname{Tr}_{P/M}(xy),$$

so any M-linear functional $\varphi\colon P \to M$ can be written in the form $\varphi(x) = \operatorname{Tr}_{P/M}(ax)$ for a suitable $a \in P$.)

PROOF: Let $r,s > 0$ be such that $r + s \equiv 0(\operatorname{mod} n)$. Then, for any $\lambda \in \ell$, the bilinear form given by

$$b_r(\lambda)(x,y) = \operatorname{Tr}_{\ell/\mathbb{F}_p}(\lambda x \sigma^r(y)) \tag{1.24}$$

is Δ-invariant. Indeed, by (1.21), for any δ in Δ we have

$$\begin{aligned} b_r(\lambda)(\delta \cdot x, \delta \cdot y) &= \operatorname{Tr}_{\ell/\mathbb{F}_p}(\lambda(\delta\sigma^r(\delta)^{-1})x\sigma^r(\delta\sigma^s(\delta)^{-1}y)) \\ &= \operatorname{Tr}_{\ell/\mathbb{F}_p}(\lambda(\delta\sigma^{r+s}(\delta)^{-1})x\sigma^r(y)) = b_r(\lambda)(x,y), \end{aligned}$$

since $r + s = 0(\operatorname{mod} n)$. If, moreover, $r \not\equiv 0(\operatorname{mod} n)$, then both $F(r)$ and $F(s)$ can be identified with ℓ and $b_r(1)$ yields a nondegenerate bilinear pairing $F(r) \times F(s) \to \mathbb{F}_p$, hence defines an isomorphism between $F(r)$ and the dual module $\widehat{F(s)} = \operatorname{Hom}(F(s), \mathbb{F}_p)$. In the case where $r \equiv 0(\operatorname{mod} n)$, both $F(r)$ and $F(s)$ are trivial Δ-modules, and therefore $F(r) \simeq F(s)$. Since clearly $B(F(r),F(s)) = \operatorname{Hom}_\Delta(F(r), \widehat{F(s)})$, to prove the first assertion of the theorem, it suffices to show that

$$\operatorname{Hom}_\Delta(F(r),F(s)) = 0$$

if $r \not\equiv s(\operatorname{mod} n)$.

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

Suppose $\varphi \in \mathrm{Hom}_\Delta(F(r), F(s))$, $\varphi \not\equiv 0$. Then, for any a in $F(r)$ and any δ in Δ, we have

$$\varphi(\delta(\sigma^r(\delta))^{-1}a) = \delta(\sigma^s(\delta))^{-1}\varphi(a). \tag{1.25}$$

Let $\mathcal{F}_1$ and $\mathcal{F}_2$ denote the additive subgroups of ℓ generated by elements of the form $\delta(\sigma^r(\delta))^{-1}$ and $\delta(\sigma^s(\delta))^{-1}$ respectively. Picking $a \in F(r)$ so that $\varphi(a) \neq 0$ and using (1.25), we obtain that for $\delta_i \in \Delta$, the condition $\sum \delta_i(\sigma^r(\delta_i))^{-1} = 0$ implies $\sum \delta_i(\sigma^s(\delta_i))^{-1} = 0$. It follows that the correspondence

$$\psi\colon \delta(\sigma^r(\delta))^{-1} \mapsto \delta(\sigma^s(\delta))^{-1}$$

extends to an additive homomorphism from $\mathcal{F}_1$ to $\mathcal{F}_2$. Moreover, $\mathcal{F}_1$ and $\mathcal{F}_2$ are clearly closed under multiplication, i.e., in effect are finite fields, and the extension of ψ is actually an isomorphism of $\mathcal{F}_1$ onto $\mathcal{F}_2$. It follows that $\psi(x) = x^{p^l}$ for a suitable integer l. So, (1.25) becomes

$$(\delta(\sigma^r(\delta))^{-1})^{p^l} = \delta(\sigma^s(\delta))^{-1} \tag{1.26}$$

for any δ in Δ. Suppose that $k = \mathbb{F}_{p^a}$. Then $\Delta = \{x^{p^a-1} : x \in \ell^*\}$ and $\sigma(x) = x^{p^{ab}}$ for a suitable integer b. Then (1.26) yields

$$x^{-p^l(p^{abr}-1)(p^a-1)} = x^{-(p^{abs}-1)}$$

for all x in ℓ^*, whence

$$p^l(p^{abr} - l)(p^a - 1) \equiv p^{abs} - 1 \pmod{p^{an} - 1}.$$

It was shown in Prasad and Raghunathan (1983, appendix to §7), that the last equation implies that $br \equiv bs (\mathrm{mod}\, n)$, hence $r \equiv s (\mathrm{mod}\, n)$ as $\gcd(b, n) = 1$. This proves the first assertion.

To prove the second assertion, we first suppose that ℓ/k is different from $\mathbb{F}_{64}/\mathbb{F}_4$, so that $F(r)$ is a simple Δ-module as $n > 2$. Let $b = b(x, y) \in B$. Then $x \mapsto b(x, 1)$ is an $\mathbb{F}_p$-linear map from ℓ to $\mathbb{F}_p$, and hence $b(x, 1) = \mathrm{Tr}_{\ell/\mathbb{F}_p}(\lambda x)$ for a suitable $\lambda \in \ell$. Consider $b_0 = b - b_1(\lambda)$, where $b_1(\lambda)$ is given by (1.24). Since b and $b_1(\lambda)$ are Δ-invariant, the set

$$F(1)^\perp := \{y \in F(r)\colon b_0(x, y) = 0 \text{ for all } x \in F(1)\}$$

is a Δ-submodule of $F(r)$ containing 1. Thus, $F(1)^\perp = F(r)$, hence $b_0 = 0$ and $b = b_1(\lambda)$, as required.

It remains to consider the case where $\ell = \mathbb{F}_{64}$ and $k = \mathbb{F}_4$. Here the Δ-submodules of $F(r)$ correspond to vector subspaces of ℓ over $\mathbb{F}_8$, and the only nontrivial automorphism of $\mathbb{F}_{64}/\mathbb{F}_8$ has the form $x \mapsto x^8$. Let $z \in \ell \setminus \mathbb{F}_8$. Then, arguing as above, we obtain that there exist $\theta, \omega \in \ell$ such that

$$\begin{aligned} b(x,1) &= \mathrm{Tr}_{\ell/\mathbb{F}_p}(\theta x), \\ b(x,z) &= \mathrm{Tr}_{\ell/\mathbb{F}_p}(\omega x) \end{aligned}$$

for all x in ℓ. Since $z^8 \neq z$, one can find λ, μ in ℓ satisfying the equations

$$\lambda + \mu = \theta,$$
$$\lambda\sigma(z) + \mu\sigma(z)^8 = \omega.$$

In our situation, $\delta(\sigma^r(\delta))^{-1} \in \mathbb{F}_8$ for all $\delta \in \ell^{(1)}$, which implies that the bilinear map $b(\lambda, \mu)$ defined by (1.23) is Δ-invariant. Then

$$b_0 := b - b(\lambda, \mu)$$

is also Δ-invariant. It follows that the subspace $F(1)^{\perp}$ introduced earlier is a Δ-submodule of $F(r)$, containing 1 and z, hence $F(1)^{\perp} = F(r)$. Thus $b_0 = 0$ and $b = b(\lambda, \mu)$. □

1.5 Simple Algebras over Number Fields

1.5.1 The Brauer Group

Let A be a central simple algebra over a number field K. Then, for any $v \in V^K$, the algebra $A_v := A \otimes_K K_v$ remains simple, so in the notations of §1.4.1, the correspondence $[A] \to [A_v]$ defines a homomorphism of Brauer groups $\mathrm{Br}(K) \xrightarrow{\theta_v} \mathrm{Br}(K_v)$. To describe $\mathrm{Br}(K)$, we consider the product

$$\theta = \prod_{v \in V^K} \theta_v : \mathrm{Br}(K) \to \prod_{v \in V^K} \mathrm{Br}(K_v).$$

In §1.4.2 we saw that, for $v \in V_f^K$, there is a canonical isomorphism $\mathrm{inv}_{K_v} : \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$. To treat all the valuations in a unified manner, we will define the invariant of the algebra of Hamiltonian quaternions over $K_v = \mathbb{R}$ to be the class $\frac{1}{2} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. Then, the homomorphism $\mathrm{inv}_{K_v} : \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$ is defined for all v and is injective.

Theorem 1.33 (ALBERT, BRAUER, HASSE, NOETHER) *The map θ is an injective homomorphism, and its image consists of $a = (a_v) \in \prod_v \mathrm{Br}(K_v)$ such that $a_v = 0$ for almost all v and $\sum_v \mathrm{inv}_{K_v} a_v = 0$.*

Thus, any finite-dimensional central division algebra D over K is determined up to isomorphism by the invariants $\mathrm{inv}_{K_v}[D_v]$ of the algebras $D_v = D \otimes_K K_v$, which, for simplicity, we will denote by $\mathrm{inv}_v\, D$. Conversely, for any choice of

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

invariants, almost all of which equal 0 and the sum of which also equals 0, there is a central division algebra over K having these invariants.

The injectivity of θ has several important consequences. First, it follows from §1.4.1 that, given a central division algebra D over K of index n, a field extension P/K of degree n is isomorphic to a maximal subfield of D if and only if $D_v \otimes_{K_v} P_w$ is the matrix algebra for all $v \in V^K$ and all $w|v$ (which is equivalent to the condition that the local degrees $[P_w : K_v]$ are divisible by the index of D_v for all v in V^K and all $w|v$). Then, by applying the Grunwald–Wang theorem from class field theory (cf., for example, Artin and Tate [2009]), one can conclude that D contains a maximal subfield $L \subset D$, which is a cyclic extension of K.

Taking into account the structure of division algebras over local fields, it is natural to ask the more subtle question of whether there always exists a maximal subfield $L \subset D$, which is a cyclic extension of K and for which the local extensions L_v/K_v are unramified extensions for all v in V_f^K such that D_v is a division algebra. Unfortunately, an extension L with these properties does not always exist, and in fact one can construct counterexamples even over $\mathbb{Q}$. However, such an L does exist if D satisfies some minor additional restrictions (cf. Platonov and Rapinchuk [1984]).

Theorem 1.33 also enables one to show that over number fields, just as over local fields, the exponent of a simple algebra coincides with is its index, and, in particular, the only division algebras of exponent 2 are the algebras of generalized quaternions.

1.5.2 Multiplicative Structure

Let D be a central division algebra of index n over a number field K. In this section, we will describe the image of the reduced norm $\mathrm{Nrd}_{D/K}(D^*)$ and also show that the group

$$SL_1(D) = \{x \in D^* : \mathrm{Nrd}_{D/K}(x) = 1\}$$

coincides with the commutator group $[D^*, D^*]$ of the multiplicative group D^*.

Theorem 1.34 (Eichler) *The group $\mathrm{Nrd}_{D/K}(D^*)$ coincides with the set of elements of K^* that are positive with respect to all real valuations $v \in V_\infty^K$ such that $D_v \not\simeq M_n(K_v)$.*

Proof: See Weil (1995), pp. 279–284 (cf. also [AGNT, §6.7]). □

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

Theorem 1.35 (WANG [1950]) $SL_1(D) = [D^*, D^*]$.

Wang's original proof of this theorem is quite complicated and relied on deep results from number theory. We will present a modified argument (cf. Platonov [1976a], Yanchevskiĭ [1975]) that uses only Eichler's theorem.

First, we will reduce the proof of Theorem 1.35 to division algebras of prime power index. For this, we will need some results about the Dieudonné determinant (cf. Artin [1988], Dieudonné [1971]). Let $GL_m(D)$ be the group of invertible elements of a matrix algebra $A = M_m(D)$. Then there exists a surjective group homomorphism

$$\delta\colon GL_m(D) \longrightarrow D^*/[D^*, D^*],$$

called the *Dieudonné determinant*, for which

$$\delta\left(\begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_m \end{pmatrix}\right) = a_1 \cdots a_m [D^*, D^*].$$

Furthermore, it is well known that in all cases except when $m = 2$ and $D = \mathbb{F}_2$, the kernel of δ coincides with the commutator subgroup $[GL_m(D), GL_m(D)]$. In particular, δ induces an isomorphism $SK_1(A) \simeq SK_1(D)$, and therefore for any field P (different from $\mathbb{F}_2$ when $m = 2$), the group $SL_m(P)$ is precisely the commutator subgroup of the group $GL_m(P)$.

Lemma 1.36 *Let $a \in SL_1(D)$ and suppose that*

$$a \in [(D \otimes_K B)^*, (D \otimes_K B)^*],$$

where B is an associative m-dimensional K-algebra with identity. Then $a^m \in [D^*, D^*]$.

PROOF: The regular representation $B \to M_m(K)$ induces an embedding $D \otimes B \to M_m(D)$, under which an element $x \in D$ is mapped to the matrix

$$\begin{pmatrix} x & & 0 \\ & \ddots & \\ 0 & & x \end{pmatrix}.$$

Now, if $a \in SL_1(D)$ and $a \in [(D \otimes_K B)^*, (D \otimes_K B)^*]$, then clearly

$$\begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix} \in [GL_m(D), GL_m(D)].$$

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

Applying the Dieudonné determinant, we obtain that $a^m \in [D^*, D^*]$, as required. □

Lemma 1.36 yields

Corollary 1.37 *For a central division algebra D of index n, the group $SK_1(D)$ has exponent dividing n.*

Indeed, pick a maximal subfield $L \subset D$. Then

$$[L\colon K] = n \text{ and } D \otimes_K L = M_n(L).$$

Applying Lemma 1.36 to $B = L$ and using the preceding remark that $SL_n(L) = [GL_n(L), GL_n(L)]$, we obtain our claim.

Furthermore, it is well known (cf. Herstein [1994], Theorem 4.4.6) that, if $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, then

$$D = D_1 \otimes_K \cdots \otimes_K D_r,$$

where D_i is a division algebra of index $p_i^{\alpha_i}$. In these notations, we have

Corollary 1.38 *If* $SK_1(D_i) = 1$ *for all* $i = 1, \dots, r$*, then* $SK_1(D) = 1$.

For the proof, we let B_i denote the tensor product $\bigotimes_{j \neq i} D_j^\circ$ of the corresponding opposite algebras. Then B_i is a K-algebra of dimension n_i^2, where $n_i = n/p_i^{\alpha_i}$; moreover, $D \otimes_K B_i \simeq M_{n_i^2}(D_i)$ for all $i = 1, \dots, r$. It follows from the properties of the Dieudonné determinant and the triviality of $SK_1(D_i)$ that $SL_{n_i^2}(D_i) = [GL_{n_i^2}(D_i), GL_{n_i^2}(D_i)]$. Invoking Lemma 1.36, we see that for any a in $SL_1(D)$ we have $a^{n_i^2} \in [D^*, D^*]$ for all $i = 1, \dots, r$. But the numbers n_i^2 $(i = 1, \dots, r)$ are relatively prime, so we have $u_i n_i^2 + \cdots + u_r n_r^2 = 1$ for suitable integers u_i, whence

$$a = (a^{n_1^2})^{u_1} \cdots (a^{n_r^2})^{u_r} \in [D^*, D^*],$$

as required.

Thus, we only need prove Theorem 1.35 in the case of a division algebra D having index p^α, where p is a prime and $\alpha \geq 0$. We will do this by induction on α, noting that the assertion clearly holds for $\alpha = 0$. Now, let us assume that $SK_1(\Delta) = 1$ for any central division algebra Δ of index $p^{\alpha-1}$ over any number field. We will then show that $SK_1(D) = 1$ for a central division algebra D of index p^α over any number field as well.

Let D be a central division algebra of index p^α with center K, and let $a \in SL_1(D)$. It suffices to find an extension F/K of degree coprime to p such that

$$a \in [(D \otimes_K F)^*, (D \otimes_K F)^*]. \tag{1.27}$$

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

Indeed, by Lemma 1.36, we would then have $a^{[F:\,K]} \in [D^*, D^*]$. At the same time, $a^{p^\alpha} \in [D^*, D^*]$ by Corollary 1.37. Since p and $[F:\,K]$ are relatively prime, we can find $s, t \in \mathbb{Z}$ such that $s[F : K] + tp^\alpha = 1$, and then

$$a = (a^{[F:K]})^s (a^{p^\alpha})^t \in [D^*, D^*],$$

as required. In order to construct such an F, let us consider a maximal subfield $L \subset D$ containing a. Let P be the normal closure of L over K, and let $\mathcal{G} = \mathrm{Gal}(P/K)$ be the corresponding Galois group. Fix a Sylow p-subgroup $\mathcal{G}_p \subset \mathcal{G}$, and set $F = P^{\mathcal{G}_p}$. Then the degree $[F:\,K]$ is clearly coprime to p, and it remains to establish (1.27).

The Galois group $\mathrm{Gal}(P/F)$ is $\mathcal{G}_p$. Let $\mathcal{H} \subset \mathcal{G}_p$ be the subgroup corresponding to the subfield $LF \subset P$. It follows from the properties of p-groups that there exists a normal subgroup $\mathcal{N} \subset \mathcal{G}_p$ of index p, containing $\mathcal{H}$. Then the corresponding fixed field $M = P^{\mathcal{N}}$ is a cyclic extension of F of degree p, which is contained in LF.

If $\alpha = 1$, then $M = LF$ is itself a cyclic extension of F of degree p. The fact that $a \in SL_1(D)$ implies that $N_{M/F}(a) = 1$, so that by Hilbert's Theorem 90, we can write $a = \sigma(b)/b$ for a suitable $b \in (LF)^*$, where σ is a generator of $\mathrm{Gal}(M/F)$. But by the Skolem–Noether Theorem, there exists an element $g \in (D \otimes_K F)^*$ such that $\sigma(b) = gbg^{-1}$ (where we identify LF with $L \otimes_K F \subset D \otimes_K F$), and consequently

$$a = gbg^{-1}b^{-1} \in [(D \otimes_K F)^*, (D \otimes_K F)^*],$$

as required. (Note that in this argument, we never used the hypothesis that K is a number field, and thus $SK_1(D) = 1$ for any division algebra D of a prime index p over an arbitrary field K.)

If $\alpha > 1$, we let Δ denote the centralizer of M in $D \otimes_K F$. By the Double Centralizer Theorem (cf. Herstein [1994], Theorem 4.3.2), Δ is a central division algebra of index $p^{\alpha-1}$ over M. Clearly $a \in \Delta$, and moreover

$$\begin{aligned} 1 &= \mathrm{Nrd}_{(D\otimes_K F)/F}(a) = N_{LF/F}(a) \\ &= N_{M/F}(N_{LF/M}(a)) = N_{M/F}(\mathrm{Nrd}_{\Delta/M}(a)). \end{aligned}$$

So, by Hilbert's Theorem 90, the element $t := \mathrm{Nrd}_{\Delta/M}(a)$ can be written in the form

$$t = \sigma(s)/s \tag{1.28}$$

for some $s \in M^*$, where σ is a generator of $\mathrm{Gal}(M/F)$. Again, by the Skolem–Noether Theorem there exists $g \in (D \otimes_K F)^*$ such that $\sigma(b) = gbg^{-1}$ for all b in M. Since Δ is the centralizer of M, we easily see that $g\Delta g^{-1} = \Delta$, and moreover

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

$$\mathrm{Nrd}_{\Delta/M}(gxg^{-1}) = g\,\mathrm{Nrd}_{\Delta/M}(x)g^{-1} \quad \text{for all } x \in \Delta.$$

Now assume that we have been able to choose an element s in (1.28), which is defined up to multiplication by an element of F^*, from the image $\mathrm{Nrd}_{\Delta/M}(\Delta^*)$ of the reduced norm. Then, writing $s = \mathrm{Nrd}_{\Delta/M}(z)$, with $z \in \Delta^*$, we obtain

$$\mathrm{Nrd}_{\Delta/M}(gzg^{-1}z^{-1}) = \sigma(s)/s = \mathrm{Nrd}_{\Delta/M}(a),$$

and therefore $a' := a(gzg^{-1}z^{-1})^{-1} \in SL_1(\Delta)$. By induction,

$$SL_1(\Delta) = [\Delta^*, \Delta^*] \subset [(D \otimes_K F)^*, (D \otimes_K F)^*],$$

and (1.27) follows.

It remains to show that s in (1.28) can indeed be found in $\mathrm{Nrd}_{\Delta/M}(\Delta^*)$. For this we will use Theorem 1.34. If p is odd, then $\Delta_w = \Delta \otimes_M M_w$ is the matrix algebra for all w in V_∞^M, so $\mathrm{Nrd}_{\Delta/M}(\Delta^*) = M^*$, and there is nothing to prove. Now let $p = 2$. In this case, M is a quadratic extension of F, and $\mathrm{Nrd}_{\Delta/M}(\Delta^*)$ consists of those $m \in M$ that are positive with respect to all real w in V_∞^M such that Δ_w is not the matrix algebra. We let S denote the set of all such w's, and let S_0 be the set of restrictions of the valuations $w \in S$ to F. Then each $v \in S_0$ has two extensions $w', w'' \in S$ with $w'' = w' \circ \sigma$ and $M_{w'} = M_{w''} = F_v$. If $s \in M^*$ is an arbitrary element satisfying (1.28), then since $t = \sigma(s)/s \in \mathrm{Nrd}_{\Delta/M}(\Delta^*)$, the element s has the same sign with respect to w' and w'', and therefore there exists $f_v \in K_v^*$ such that sf_v is positive with respect to both w' and w''. Using Theorem 1.12 on weak approximation, we can choose an element $f \in K^*$ so that f and f_v have the same sign in K_v for all v in S_0. Now, setting $s_1 = sf$, we obtain $t = \sigma(s)/s = \sigma(s_1)/s_1$, i.e., (1.28) holds with s replaced by s_1. At the same time, it follows from our construction that $s_1 \in \mathrm{Nrd}_{\Delta/M}(\Delta^*)$, as required. This completes the proof of Theorem 1.35.

1.5.3 Lattices and Orders

Let K be a number field with ring of integers $\mathcal{O}$. A *lattice* (or, more precisely, an $\mathcal{O}$-lattice) in a finite-dimensional vector space V over K is a finitely generated $\mathcal{O}$-submodule $L \subset V$ that contains a basis of V over K. A lattice $L \subset V$ is said to be *free* if it is a free $\mathcal{O}$-module, i.e., possesses an $\mathcal{O}$-basis. When $\mathcal{O}$ is a principal ideal domain or, equivalently, the class number of K equals 1, any lattice is free. In general, any lattice $L \subset V$ has a *pseudobasis*, i.e., there exist $x_1, \ldots, x_n \in V$, where $n = \dim_K V$, such that

$$L = \mathcal{O}x_1 \oplus \cdots \oplus \mathcal{O}x_{n-1} \oplus \mathfrak{a}x_n$$

for some ideal $\mathfrak{a} \subset \mathcal{O}$ (cf. O'Meara [2000]).

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

An *order* in a finite-dimensional K-algebra A is an $\mathcal{O}$-lattice $B \subset A$ that is simultaneously a subring containing the identity element of A. An order is said to be *maximal* if it is not properly contained in any larger order.

The study of lattices and orders essentially reduces to the study of their local counterparts. More precisely, by a (local) lattice in a finite-dimensional K_v-vector space V_{K_v}, where $v \in V_f^K$, we mean a finitely generated $\mathcal{O}_v$-submodule $L_v \subset V_{K_v}$ containing a basis of V_{K_v}. Since $\mathcal{O}_v$ is a principal ideal domain, any local lattice has an $\mathcal{O}_v$-basis. One defines orders and maximal orders in the obvious way. Clearly, if L is a lattice in a finite-dimensional vector space V over K (respectively, if B is an order in a finite-dimensional K-algebra A), then $L_v := L \otimes_{\mathcal{O}} \mathcal{O}_v$ (respectively, $B_v := B \otimes_{\mathcal{O}} \mathcal{O}_v$) is a lattice in the space $V_{K_v} := V \otimes_K K_v$ (respectively, in the algebra $A_{K_v} := A \otimes_K K_v$). Thus, to each lattice $L \subset V$ one can associate the set of localizations $\{L_v \subset V_{K_v} : v \in V_f^K\}$. So, a natural question to ask is the extent to which L is determined by its localizations L_v.

Theorem 1.39 (1) $L = \bigcap_v (V \cap L_v)$*, in particular a lattice is uniquely determined by its localizations;*

(2) *for any two lattices* $L, M \subset V$*, we have* $L_v = M_v$ *for almost all* v*;*

(3) *if* $L \subset V$ *is a lattice and* $\{N_v \subset V_{K_v}\}$ *is an arbitrary set of local lattices such that* $N_v = L_v$ *for almost all* v*, then there exists a lattice* $M \subset V$ *such that* $M_v = N_v$ *for all* $v \in V_f^K$*.*

PROOF: Let L, M be two lattices, let $x_1, \ldots, x_n$ be a basis of V contained in L, and let $y_1, \ldots, y_r$ be a finite system of generators of M as an $\mathcal{O}$-module. Then we can write $y_i = \sum_{j=1}^{n} a_{ij} x_j$ for some $a_{ij} \in K$. If we choose an integer $m \neq 0$ so that $m a_{ij} \in \mathcal{O}$ for all i, j, then $mM \subset L$. By interchanging L and M, we can likewise find an integer $l \neq 0$ so that $lL \subset M$, hence $L \subset \frac{1}{l} M$. If now $v \notin V(lm)$ (notation as in §1.2.1), then $L_v = M_v$, proving the second assertion.

To prove assertions (1) and (3), we embed V into the associated adele space $V_{A_f} = V \otimes_K A_f$, where A_f is the ring of finite adeles of K. It follows from the strong approximation theorem (cf. Theorem 1.13) that

$$L_{A_f(\infty)} := L \otimes_{\mathcal{O}} A_f(\infty) = \prod_{v \in V_f^K} L_v$$

(where $A_f(\infty) = \prod_{v \in V_f^K} \mathcal{O}_v$ is the ring of integral finite adeles) coincides with the closure of L in V_{A_f}. Therefore

$$L' := \bigcap_{v \in V_f^K} L_v$$

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

is the closure of L in V in the topology induced from V_{A_f}. So, to prove the first assertion, we only need to establish that L is closed. To do this, let us take a basis $x_1, \dots, x_n$ of V in contained L, and set

$$M = \mathcal{O}x_1 + \cdots + \mathcal{O}x_n.$$

Since $\mathcal{O} = \bigcap_{v \in V_f^K} (K \cap \mathcal{O}_v)$, we see that $M = \bigcap_{v \in V_f^K} (V \cap M_v)$. But $\prod_{v \in V_f^K} M_v$, just as $\prod_{v \in V_f^K} L_v$, is open in V_{A_f}, so M is open in V, and consequently $L \subset V$ is open and closed.

Finally, if a collection of local lattices $N_v \subset V_{K_v}$ satisfies $N_v = L_v$ for almost all v, then $\prod_{v \in V_f^K} N_v$ is an open compact subgroup in V_{A_f} and therefore is commensurable with $\prod_{v \in V_f^K} L_v$ (i.e., their intersection has finite index in each of them). It follows that

$$M := \bigcap_{v \in V_f^K} (V \cap N_v)$$

is commensurable with $L = \bigcap_{v \in V_f^K} (V \cap L_v)$, implying that M is a lattice, as needed. □

We will now review some facts about orders in algebras. Our account will only include results about the existence of maximal orders and embedding an arbitrary order into a maximal one, as these are precisely the questions that arise in the study of maximal arithmetic and maximal compact subgroups of algebraic groups. First, we note the following consequence of Theorem 1.39.

Proposition 1.40 *An order $B \subset A$ is maximal if and only if for each v in V_f^K, the order $B_v \subset A_{K_v}$ is maximal.*

Elementary examples show that an arbitrary algebra may not contain any maximal orders. Our goal is to prove that maximal orders always exist in finite-dimensional *semisimple* algebras. Recall that a *semisimple K-algebra* is the direct sum of a finite number of simple (but not necessarily central) K-algebras. Thus, by the Artin–Wedderburn Theorem, a finite-dimensional semisimple algebra can be written in the form $A = \bigoplus_{i=1}^r M_{n_i}(D_i)$, where D_i is a finite-dimensional division algebra over K. In characteristic zero, a finite-dimensional K-algebra A is semisimple if and only if $A \otimes_K \bar{K} \simeq \bigoplus_{i=1}^r M_{m_i}(\bar{K})$ for some integers m_i (cf. Pierce [1982]). We therefore begin by considering maximal orders in the matrix algebra $A = M_n(K_v)$. Our treatment will

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

be based on the study of the natural action of A on $V = K_v^n$, in conjunction with some elementary topological considerations involving compactness. For a lattice $L \subset V$, we let

$$A^L = \{ g \in M_n(K_v) \colon g(L) \subset L \}$$

denote the *stabilizer* of L. We note that by choosing a basis of L, we may identify the stabilizer A^L with $M_n(\mathcal{O}_v)$, which implies in particular that A^L is an order and an open compact subring (we note that these characterizations are in fact equivalent).

Proposition 1.41 (1) *For any compact subring $B \subset A$, there is a lattice $L \subset V$ such that $B \subset A^L$;*
(2) *the ring A^L is a maximal order in A, for any lattice $L \subset V$;*
(3) *any order $B \subset A$ is contained in some maximal order, and there exist only finitely many (maximal) orders containing B.*

PROOF: Let $L_0 = \mathcal{O}_v^n$ be the lattice spanned by the standard basis vectors of $V = K_v^n$. Since A^{L_0} is open and B is compact, there exists a finite collection of elements $x_1, \ldots, x_r \in A$ such that $B \subset \bigcup_{i=1}^r (x_i + A^{L_0})$. It follows that the $\mathcal{O}_v$-submodule $L \subset V$ generated by $B(L_0) = \bigcup_{x \in B} x(L_0)$ is actually generated by $L_0 \cup x_1(L_0) \cup \cdots \cup x_r(L_0)$, hence is a lattice. On the other hand, it is clear that $B(L) \subset L$, which proves the first assertion.

Now assume that A^L is contained in some order $B \subset A$. Since any order is clearly an open compact subring, by part (1) we have $B \subset A^M$ for a suitable lattice $M \subset V$. Thus, $A^L \subset A^M$ and our goal is to show that $A^L = A^M$. Since replacing M with a lattice of the form αM for $\alpha \in K_v^*$ does not change the stabilizer A^M, we may assume that $M \subset L$, but $M \not\subset \pi L$, where π is a uniformizer of K_v. We can then choose a basis $e_1, \ldots, e_n$ of L so that M has a basis of the form $e_1, \pi^{\alpha_2} e_2, \ldots, \pi^{\alpha_n} e_n$ for some nonnegative integers $\alpha_2, \ldots, \alpha_n$. For $i > 1$, consider the transformation $g_i \in A^L$ that interchanges the vectors e_1 and e_i and fixes all e_j, for $j \neq 1, i$. Since $A^L \subset A^M$ we have $g_i \in A^M$, whence $g_i(e_1) = e_i \in M$ and $\alpha_i = 0$. Consequently $L = M$, so $A^L = A^M$, proving the second assertion.

It follows from parts (1) and (2) that any order $B \subset A$ is contained in some maximal order $C = A^L$, so it remains to show that the set $\{C_l\}$ of maximal orders in A containing B is finite. We can pick a lattice M_l and a nonnegative integer α so that $C_l = A^{M_l}$ and $B \supset \pi^\alpha C$. Then for any l we have $C_l \supset B \supset \pi^\alpha C$. Let us show that in this case, we have the inclusion $\pi^\alpha C_l \subset C$. Without loss of generality, as in the proof of (2), we may assume that the lattices L and M_l have bases of the form $e_1, e_2, \ldots, e_n$ and $e_1, \pi^{\alpha_2} e_2, \ldots, \pi^{\alpha_n} e_n$ for $\alpha_i \geq 0$,

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

respectively. Since $C_l \supset \pi^\alpha C$, we have $C(M_l) \subset \pi^{-\alpha} C_l(M_l) = \pi^{-\alpha} M_l$. Again, using the transformations $g_i \in C$ introduced earlier, we obtain $\alpha_i \leq \alpha$, hence $\pi^\alpha L \subset M_l$. Then $\pi^\alpha C_l(L) \subset C_l(M_l) = M_l \subset L$, so $\pi^\alpha C_l \subset C$. Thus, for any l we have the inclusions

$$\pi^\alpha C \subset C_l \subset \pi^{-\alpha} C.$$

Since the index $[\pi^{-\alpha} C : \pi^\alpha C]$ is finite, the number of distinct C_l's is also finite. This completes the proof of the proposition. □

Remark The description of maximal orders in $M_n(K_v)$ as stabilizers of lattices $L \subset V$ implies that any two maximal orders in $A = M_n(K_v)$ are conjugate.

The techniques employed in the proof of the proposition easily yield analogous assertions about maximal compact subgroups of $G = GL_n(K_v)$. For a lattice $L \subset V$, we let G^L denote the group of automorphisms of L, i.e., $G^L = \{g \in G \colon g(L) = L\}$ (more generally, for any subgroup $\Gamma \subset G$ we set $\Gamma^L = \{g \in \Gamma : g(L) = L\}$ and call Γ^L the *stabilizer* of L in Γ). Clearly, using a basis of L, one can identify $G^L = (A^L)^*$ with $GL_n(\mathcal{O}_v)$, so G^L is an open compact subgroup of G and $\det g \in U_v$ for any $g \in G^L$.

Proposition 1.42 (1) *Given a compact subgroup $B \subset G$, there is a lattice $L \subset V$ such that $B \subset G^L$;*

(2) *G^L is a maximal compact subgroup of G for any lattice $L \subset V$; in particular, any compact subgroup is contained in a maximal compact subgroup;*

(3) *all maximal compact subgroups of G are conjugate.*

The proof follows easily from Proposition 1.41.

One also derives from Proposition 1.41 the following fundamental result about orders in semisimple algebras over local fields.

Theorem 1.43 *Let A be a semisimple algebra over K_v. Then any order $B \subset A$ is contained in a maximal order, and there exist only finitely many (maximal) orders containing B.*

PROOF: Writing A as the direct sum of simple algebras, one reduces the proof to the case where A is simple. Let F be the center of A and let $\mathcal{O}_F$ be the corresponding valuation ring. Then, for any $\mathcal{O}_v$-order $B \subset A$, the product $\mathcal{O}_F B$ (of $\mathcal{O}_v$-submodules) is simultaneously an $\mathcal{O}_v$-order and an $\mathcal{O}_F$-order in A. So, it follows that we only need consider the case where $F = K_v$. Clearly, to prove the theorem it suffices to show that the set $\{B_i\}$ of all orders in A containing B is

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press

finite. For this, we pick a finite extension P of K_v such that $A \otimes_{K_v} P \simeq M_n(P)$, and set

$$\tilde{B} = B \otimes_{\mathcal{O}_v} \mathcal{O}_P, \quad \tilde{B}_i = B_i \otimes_{\mathcal{O}_v} \mathcal{O}_P.$$

Then $\tilde{B}$ and $\tilde{B}_i$ are orders in $M_n(P)$, and $\tilde{B} \subset \tilde{B}_i$. But by Proposition 1.41, among the orders $\tilde{B}_i$ there are only finitely many distinct orders. So, it suffices to show that $\tilde{B}_i = \tilde{B}_j$ can hold only if $B_i = B_j$. Indeed, pick $\mathcal{O}_v$-bases $x_1, \ldots, x_{n^2}$ and $y_1, \ldots, y_{n^2}$ of B_i and B_j respectively. Then $x_l = \sum_{m=1}^{n^2} a_{lm} y_m$ and $y_l = \sum_{m=1}^{n^2} b_{lm} x_m$ for suitable $a_{lm}, b_{lm} \in K_v$. Since $x_1, \ldots, x_{n^2}$ and $y_1, \ldots, y_{n^2}$ are also $\mathcal{O}_P$-bases of $\tilde{B}_i = \tilde{B}_j$, then actually $a_{lm}, b_{lm} \in \mathcal{O}_P \cap K_v = \mathcal{O}_v$, whence $B_i = B_j$. □

Combining Theorem 1.43 with Proposition 1.41, we obtain the existence of maximal orders in semisimple algebras over number fields.

Theorem 1.44 *Let A be a semisimple algebra over a number field K. Then any order $B \subset A$ is contained in some maximal order.*

PROOF: As above, the proof reduces to the case of a central simple K-algebra A. It suffices to show that the set $\{B_i\}$ of orders in A containing B is finite. We first prove this assertion for a matrix algebra $A = M_n(K)$. It follows from Propositions 1.40 and 1.41 that the order $C = M_n(\mathcal{O})$ is maximal in A. Then according to Theorem 1.39(2), $B_v = C_v$ is a maximal order in $A_{K_v} = M_n(K_v)$ for almost all $v \in V_f^K$. On the other hand, by Theorem 1.43, for the remaining v, the number of orders in A_{K_v} containing B_v is finite. Combining this with Theorem 1.39(1), we obtain the required result. To reduce the general case to that of a matrix algebra, we choose a finite extension P/K satisfying $A \otimes_K P \simeq M_n(P)$, and replace the orders B and B_i with the orders $\tilde{B} = B \otimes_{\mathcal{O}} \mathcal{O}_P$ and $\tilde{B}_i = B_i \otimes_{\mathcal{O}} \mathcal{O}_P$ in $M_n(P)$. Then there exist only finitely many distinct $\tilde{B}_i$'s, and therefore only finitely many distinct B_i's (as by considering localizations and arguing as in the proof of Theorem 1.43 we see that $\tilde{B}_i = \tilde{B}_j$ implies $B_i = B_j$). □

Remark Even though it can be shown that over K_v all maximal orders are conjugate for any semisimple algebra, over K there may, in general, exist nonconjugate maximal orders.

https://doi.org/10.1017/9781139017756.004 Published online by Cambridge University Press