Algebraic Groups and Number Theory
Algebraic Groups and Number Theory

Vladimir Platonov
Andrei Rapinchuk
Academy of Sciences
Belarus, Minsk

Translated by Rachel Rowen
Raanana, Israel
Contents

Preface to the English Edition ........................................ ix

Preface to the Russian Edition ...................................... ix

Chapter 1. Algebraic number theory ................................. 1
  1.1. Algebraic number fields, valuations, and completions .... 1
  1.2. Adeles and ideles; strong and weak approximation; the
       local-global principle ...................................... 10
  1.3. Cohomology .................................................. 16
  1.4. Simple algebras over local fields ........................... 27
  1.5. Simple algebras over algebraic number fields .............. 37

Chapter 2. Algebraic Groups ......................................... 47
  2.1. Structural properties of algebraic groups ................. 47
  2.2. Classification of $K$-forms using Galois cohomology ...... 67
  2.3. The classical groups ....................................... 78
  2.4. Some results from algebraic geometry .................... 96

Chapter 3. Algebraic Groups over Locally Compact Fields .... 107
  3.1. Topology and analytic structure ........................... 107
  3.2. The Archimedean case ..................................... 118
  3.3. The non-Archimedean case ................................ 133
  3.4. Elements of Bruhat-Tits theory ........................... 148
  3.5. Results needed from measure theory ...................... 158

Chapter 4. Arithmetic Groups and Reduction Theory .......... 171
  4.1. Arithmetic groups .......................................... 171
  4.2. Overview of reduction theory: reduction in $GL_n(R)$ .... 175
  4.3. Reduction in arbitrary groups ............................. 189
  4.4. Group-theoretic properties of arithmetic groups ........ 195
  4.5. Compactness of $G_R/G_Z$ ................................ 207
  4.6. The finiteness of the volume of $G_R/G_Z$ ................ 213
  4.7. Concluding remarks on reduction theory .................. 223
  4.8. Finite arithmetic groups .................................. 229
Chapter 5. Adeles ........................................... 243
  5.1. Basic definitions ..................................... 243
  5.2. Reduction theory for $G_A$ relative to $G_K$ ...... 253
  5.3. Criteria for the compactness and the finiteness of volume of $G_A/G_K$ .................................. 260
  5.4. Reduction theory for $S$-arithmetic subgroups ...... 266

Chapter 6. Galois cohomology ................................ 281
  6.1. Statement of the main results ....................... 281
  6.2. Cohomology of algebraic groups over finite fields .... 286
  6.3. Galois cohomology of algebraic tori ................. 300
  6.4. Finiteness theorems for Galois cohomology ........... 316
  6.5. Cohomology of semisimple algebraic groups over local fields and number fields ...................... 325
  6.6. Galois cohomology and quadratic, Hermitian, and other forms .............................................. 342
  6.7. Proof of Theorems 6.4 and 6.6: Classical groups ... 356
  6.8. Proof of Theorems 6.4 and 6.6: Exceptional groups ... 368

Chapter 7. Approximation in Algebraic Groups .......... 399
  7.1. Strong and weak approximation in algebraic varieties ......................................................... 399
  7.2. The Kneser-Tits conjecture ......................... 405
  7.3. Weak approximation in algebraic groups ............... 415
  7.4. The strong approximation theorem ........................ 427
  7.5. Generalization of the strong approximation theorem ...... 433

Chapter 8. Class numbers and class groups of algebraic groups ......................................................... 439
  8.1. Class numbers of algebraic groups and number of classes in a genus ...................................... 439
  8.2. Class numbers and class groups of semisimple groups of noncompact type; the realization theorem 450
  8.3. Class numbers of algebraic groups of compact type ............................................................... 471
  8.4. Estimating the class number for reductive groups ................................................................. 484
  8.5. The genus problem ........................................ 494

Chapter 9. Normal subgroup structure of groups of rational points of algebraic groups ......................... 509
  9.1. Main conjectures and results ........................... 509
  9.2. Groups of type $A_n$ .................................... 518

9.3. The classical groups ..................................... 537
9.4. Groups split over a quadratic extension ............... 546
9.5. The congruence subgroup problem (a survey) ........... 553

Appendix A ....................................................... 571
Appendix B. Basic Notation ................................... 579

Bibliography ................................................... 583

Index ............................................................. 609
Preface to the English Edition

After publication of the Russian edition of this book (which came out in 1991) some new results were obtained in the area; however, we decided not to make any changes or add appendices to the original text, since that would have affected the book's balanced structure without contributing much to its main contents.

As the editorial to the translation, A. Borel took considerable interest in the book. He read the first version of the translation and made many helpful comments. We also received a number of useful suggestions from G. Prasad. We are grateful to them for their help. We would also like to thank the translator and the publisher for their cooperation.

V. Platonov
A. Rapinchuk

Preface to the Russian Edition

This book provides the first systematic exposition in mathematical literature of the theory that developed on the meeting ground of group theory, algebraic geometry and number theory. This line of research emerged fairly recently as an independent area of mathematics, often called the arithmetic theory of (linear) algebraic groups. In 1967 A. Weil wrote in the foreword to Basic Number Theory: “In charting my course, I have been careful to steer clear of the arithmetical theory of algebraic groups; this is a topic of deep interest, but obviously not yet ripe for book treatment.”

The sources of the arithmetic theory of linear algebraic groups lie in classical research on the arithmetic of quadratic forms (Gauss, Hermite, Minkowski, Hasse, Siegel), the structure of the group of units in algebraic number fields (Dirichlet), discrete subgroups of Lie groups in connection with the theory of automorphic functions, topology, and crystallography (Riemann, Klein, Poincaré and others). Its most intensive development, however, has taken place over the past 20 to 25 years. During this period reduction theory for arithmetic groups was developed, properties of adele groups were studied and the problem of strong approximation solved, important results on the structure of groups of rational points over local and global fields were obtained, various versions of the local-global principle for algebraic groups were investigated, and the congruence problem for isotropic groups was essentially solved.

It is clear from this far from exhaustive list of major accomplishments in the arithmetic theory of linear algebraic groups that a wealth of important material of particular interest to mathematicians in a variety of areas
has been amassed. Unfortunately, to this day the major results in this area have appeared only in journal articles, despite the long-standing need for a book presenting a thorough and unified exposition of the subject. The publication of such a book, however, has been delayed largely due to the difficulty inherent in unifying the exposition of a theory built on an abundance of far-reaching results and a synthesis of methods from algebra, algebraic geometry, number theory, analysis and topology. Nevertheless, we finally present the reader such a book.

The first two chapters are introductory and review major results of algebraic number theory and the theory of algebraic groups which are used extensively in later chapters. Chapter 3 presents basic facts about the structure of algebraic groups over locally compact fields. Some of these facts also hold for any field complete relative to a discrete valuation. The fourth chapter presents the most basic material about arithmetic groups, based on results of A. Borel and Harish-Chandra.

One of the primary research tools for the arithmetic theory of algebraic groups is adele groups, whose properties are studied in Chapter 5. The primary focus of Chapter 6 is a complete proof of the Hasse principle for simply connected algebraic groups, published here in definitive form for the first time. Chapter 7 deals with strong and weak approximations in algebraic groups. Specifically, it presents a solution of the problem of strong approximation and a new proof of the Kneser-Tits conjecture over locally fields.

The classical problems of the number of classes in the genus of quadratic forms and of the class numbers of algebraic number fields influenced the study of class numbers of arbitrary algebraic groups defined over a number field. The major results achieved to date are set forth in Chapter 8. Most are attributed to the authors.

The results presented in Chapter 9 for the most part are new and rather intricate. Recently substantial progress has been made in the study of groups of rational points of algebraic groups over global fields. In this regard one should mention the works of Kneser, Margulis, Platonov, Rapinchuk, Prasad, Raghunathan and others on the normal subgroup structure of groups of rational points of anisotropic groups and the multiplicative arithmetic of skew fields, which use most of the machinery developed in the arithmetic theory of algebraic groups. Several results appear here for the first time. The final section of this chapter presents a survey of the most recent results on the congruence subgroup problem.

Thus this book touches on almost all the major results of the arithmetic theory of linear algebraic groups obtained to date. The questions related to the congruence subgroup problem merit exposition in a separate book, to which the authors plan to turn in the near future. It should be noted that many well-known assertions (especially in Chapters 5, 6, 7, and 9) are presented with new proofs which tend to be more conceptual. In many instances a geometric approach to representation theory of finitely generated groups is effectively used.

In the course of our exposition we formulate a considerable number of unresolved questions and conjectures, which may give impetus to further research in this actively developing area of contemporary mathematics.

The structure of this book, and exposition of many of its results, was strongly influenced by V. P. Platonov's survey article, "Arithmetic theory of algebraic groups," published in Uspekhi matematicheskikh nauk (1982, No. 3, pp. 3–54). Much assistance in preparing the manuscript for print was rendered by O. I. Tavgen, Y. A. Drakhokhrust, V. V. Benyashch-Krivetz, V. V. Kursov, and I. I. Voronovich. Special mention must be made of the contribution of V. I. Chernousov, who furnished us with a complete proof of the Hasse principle for simply connected groups and devoted considerable time to polishing the exposition of Chapter 6. To all of them we extend our sincerest thanks.

V. P. Platonov
A. S. Rapinchuk
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 these problems may be found in the works of Lang [2] and Weil [6] (cf. also Chapters 1–3 of ANT). It should be noted that, unlike such mathematicians as Weil, we have stated results here only for algebraic number fields, although the overwhelming majority of results also hold for global fields of characteristic > 0, i.e., fields of algebraic functions over a finite field. In §1.3 we present results about group cohomology, necessary for understanding the rest of the book, including definitions and statements of the basic properties of noncommutative cohomology. Sections 1.4–1.5 contain major results on simple algebras over local and global fields. Special attention is given to research on the multiplicative structure of division algebras over these fields, particularly the triviality of the Whitehead groups. Moreover, in §1.5 we collect useful results on lattices over vector spaces and orders in semisimple algebras.

The rest of the book presupposes familiarity with field theory, especially 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 $\mathbb{Q}$, and $\mathcal{O}_K$ the ring of integers of $K$. $\mathcal{O}_K$ is a classical object of interest in algebraic number theory. Its structure and arithmetic were first studied by Gauss, Dedekind, Dirichlet and others in the previous century, and continue to interest mathematicians today. From a purely algebraic point of view the ring $\mathcal{O} = \mathcal{O}_K$ is quite straightforward: if $[K : \mathbb{Q}] = n$, then $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank $n$. For any nonzero ideal $a \subset \mathcal{O}$ the quotient ring $\mathcal{O}/a$ is finite; in particular, any prime ideal is maximal. Rings with such properties (i.e., noetherian, integrally closed, with prime ideals maximal) are known as Dedekind rings. It follows that any nonzero ideal $a \subset \mathcal{O}$ can be written uniquely as the product of prime ideals: $a = p^{r_1} \ldots p^{r_c}$. This property is a generalization of the fundamental theorem of arithmetic on the uniqueness (up to associates) of factorization of any integer into a product of prime numbers. Nevertheless, the analogy here is not complete: unique factorization of the elements of $\mathcal{O}$ to prime elements, generally speaking, does not hold. This fact, which demonstrates that the arithmetic of $\mathcal{O}$ can differ significantly from the arithmetic of $\mathbb{Z}$, has been crucial in shaping the problems of algebraic number theory. The precise degree of deviation is measured by the ideal class group (previously called the divisor class
group) of $K$. Its elements are fractional ideals of $K$, i.e., $\mathcal{O}$-submodules $a$ of $K$, such that $xa \subset \mathcal{O}$ for a suitable nonzero $x$ in $\mathcal{O}$. Define the product of two fractional ideals $a, b \subset \mathcal{O}$ to be the $\mathcal{O}$-submodule in $K$ generated by all $xy$, where $x \in a, y \in b$. With respect to this operation the set of fractional ideals becomes a group, which we denote $\text{Id}(\mathcal{O})$, called the group of ideals of $K$. The principal fractional ideals, i.e., ideals of the form $x\mathcal{O}$ where $x \in K^*$, generate the subgroup $P(\mathcal{O}) \subset \text{Id}(\mathcal{O})$, and the factor group $\text{Cl}(\mathcal{O}) = \text{Id}(\mathcal{O})/P(\mathcal{O})$ is called the ideal class group of $K$. A classic result, due to Gauss, is that the group $\text{Cl}(\mathcal{O})$ 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 classic result (Dirichlet’s unit theorem) establishes that the group of invertible elements of $\mathcal{O}^*$ is finitely generated. These two facts are the starting point for the arithmetic theory of algebraic groups (cf. Preface). However generalizing classical arithmetic to algebraic groups we cannot appeal to ring-theoretic concepts, but rather we develop such number theoretic constructions as valuations, completions, and also adeles and ideles, etc.

### 1.1.2. Valuations and completions of algebraic number fields

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

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

If we replace condition 3 by the stronger condition

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

then the valuation is called non-archimedean; if not, it is archimedean.

An example of a valuation is the trivial valuation, defined as follows: $|x|_v = 1$ for all $x$ in $K^*$, and $|0|_v = 0$. We shall illustrate nontrivial valuations for the case $K = \mathbb{Q}$. The ordinary absolute value $|\cdot|_\infty$ is an archimedean valuation. Also, each prime number $p$ can be associated with a valuation $|\cdot|_p$, which we call the $p$-adic valuation. More precisely, writing any rational number $\alpha \neq 0$ in the form $p^{\tau} \cdot \beta/\gamma$, where $r, \beta, \gamma \in \mathbb{Z}$ and $p$ and $\gamma$ are not divisible by $p$, we write $|\alpha|_p = p^{-\tau}$ and $|0|_p = 0$. Sometimes, instead of the $p$-adic valuation $|\cdot|_p$, it is convenient to use the corresponding logarithmic valuation $v = v_p$, defined by the formula $v(\alpha) = \tau$ 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 of rational integers (or another ordered group) and $v(0) = -\infty$;
2. $v(xy) = v(x) + v(y)$;
3. $v(x + y) \geq \min\{v(x), v(y)\}$.

We shall use both ordinary valuations, as well as corresponding logarithmic valuations, and from the context it will be clear which is being discussed.

It is worth noting that the examples cited actually exhaust all the non-trivial valuations of $\mathbb{Q}$.

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

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

Thus, restricting any non-trivial valuation $|\cdot|_v$ of an algebraic number field $K$ to $\mathbb{Q}$, we obtain either an archimedean valuation $|\cdot|_\infty$ (or its equivalent) or a $p$-adic valuation. (It can be shown that the restriction of a non-trivial valuation is always non-trivial.) Thus any non-trivial valuation of $K$ is obtained by extending to $K$ one of the valuations of $\mathbb{Q}$. On the other hand, for any algebraic extension $L/K$, any valuation $|\cdot|_v$ of $K$ can be extended to $L$, i.e., there exists a valuation $|\cdot|_v$ of $L$ (denoted $v|_L$) such that $|\alpha|_v = |\alpha|_v$ for all $\alpha$ in $K$. In particular, proceeding from the given valuations of $\mathbb{Q}$ we can obtain 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 $\hat{K}_v$ of $K$ with respect to a valuation $|\cdot|_v$. If we look at the completion of $K$ as a metric space with respect to the distance arising from the valuation $|\cdot|_v$, we obtain a complete metric space $\hat{K}_v$, which becomes a field under the natural operations and is complete with respect to the corresponding extension of $|\cdot|_v$, for which we retain the same notation. It is well known that if $L$ is an algebraic extension of $\hat{K}_v$ (and, in general, of any field which is complete with respect to the valuation $|\cdot|_v$), then $|\cdot|_v$ has a unique extension $|\cdot|_w$ to $L$. Using the existence and uniqueness of the extension, we shall derive an explicit formula for $|\cdot|_w$, which can be taken for a definition of $|\cdot|_w$. Indeed, $|\cdot|_w$ extends uniquely to a valuation of the algebraic closure $\hat{K}_v$. It follows that $|\sigma(\alpha)|_w = |\alpha|_w$ for any $x$ in $\hat{K}_v$ and any $\sigma$ in $\text{Gal}(\hat{K}_v/\hat{K}_v)$. Now let $L/\hat{K}_v$ be a finite extension of degree $n$ and $\sigma_1, \ldots, \sigma_n$ various embeddings of $L$ in $\hat{K}_v$ over $\hat{K}_v$. Then for any $a$ in $L$ and its norm $N_{L/\hat{K}_v}(a)$ we have

$$|N_{L/\hat{K}_v}(a)|_w = \prod_{\sigma_i(a)} = \prod_{\sigma_i(a)} |\sigma_i(a)|_w = |a|_w^n.$$
Now let us consider extensions of valuations to a finite extension $L/K$, where $K$ is an algebraic number field. Let $| \cdot |_v$ be a valuation of $K$ and $| \cdot |_{\infty}$ its unique extension to the algebraic closure $\bar{K}_v$ of $K_v$. Then for any embedding $\tau : L \to \bar{K}_v$ over $L$ (of which there are $n$, where $n = [L : K]$), we can define a valuation $u$ over $L$, given by $|x|_u = |\tau(x)|_v$, which clearly extends the original valuation $| \cdot |_v$ of $K$. In this case the completion $L_u$ can be identified with the compositum $\tau(L)\bar{K}_v$. Moreover, any extension may be obtained in this way, and two embeddings $\tau_1, \tau_2 : L \to \bar{K}_v$ give the same extension if they are conjugate over $K_v$, i.e., if there exists $\lambda$ in $Gal(\bar{K}_v/K_v)$ with $\tau_2 = \lambda \tau_1$. In other words, if $L = K(a)$ and $f(t)$ is the irreducible polynomial of $a$ over $K_v$, then the extensions $| \cdot |_{u_1}, \ldots, | \cdot |_{u_n}$ of $| \cdot |_v$ over $L$ are in $1 : 1$ correspondence with the irreducible factors of $f$ over $K_v$, viz. $| \cdot |_{u_i}$ corresponds to $\tau_i : L \to \bar{K}_v$ sending $a$ 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

\[ L \bigotimes K_v \cong \bigoplus_{i=1}^{r} L_{u_i}; \]

in particular $[L : K]$ is the sum of all the local degrees $[L_{u_i} : K_v]$.

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

\[ N_{L/K}(a) = \prod_{u|v} N_{L_u/K_v}(a), \]
\[ Tr_{L/K}(a) = \sum_{u|v} Tr_{L_u/K_v}(a). \]

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 $V^K_\infty$ of the archimedean valuations, which are the extensions to $K$ of $| \cdot |_{\infty}$, the ordinary absolute value, on $Q$, and the set $V^K_p$ of non-archimedean valuations obtained as extensions of the $p$-adic valuation $| \cdot |_p$ of $Q$, for each prime number $p$. The archimedean valuations correspond to embeddings of $K$ in $R$ or in $C$, and are respectively called real or complex valuations (their respective completions being $R$ or $C$). If $v \in V^K$ is a real valuation, then an element $a$ 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 dimension of $L$ over $K$.

Non-archimedean valuations lead to more complicated completions. To wit, if $v \in V^K_p$ is an extension of the $p$-adic valuation, then the completion $K_v$ is a finite extension of the field $Q_p$ of $p$-adic numbers. Since $Q_p$ 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 $O$ in $K_v$ is the valuation ring $O_v = \{ a \in K_v : |a|_v \leq 1 \}$, sometimes called the ring of $v$-adic integers. $O_v$ is a local ring with a maximal ideal $p_v = \{ a \in K_v : |a|_v < 1 \}$ (called the valuation ideal) and the group of invertible elements $U_v = O_v \setminus p_v = \{ a \in K_v : |a|_v = 1 \}$. It is easy to see that the valuation ring of $Q_p$ is the ring of $p$-adic integers $Z_p$, and the valuation ideal is $pZ_p$. In general, $O_v$ is a free module over $Z_p$, whose rank is the dimension $[K_v : Q_p]$, so $O_v$ is an open compact subring of $K_v$. Moreover, the powers $p_v^n$ of $p_v$ form a system of neighborhoods of zero in $O_v$. The quotient ring $k_v = O_v/p_v$ is a finite field and is called the residue field of $v$. $p_v$ is a principal ideal of $O_v$; any of its generators $\pi$ is called a uniformizing parameter and is characterized by $v(\pi)$ being the (positive) generator of the value group $\Gamma = v(K_v^\ast) \cong Z$. Once we have established a uniformizing parameter $\pi$, we can write any $a$ in $K_v^\ast$ as $a = \pi^n u$, for suitable $u \in U_v$; this yields a continuous isomorphism $K_v^\ast \cong Z \times U_v$, given by $a \mapsto (\pi^n, u)$, where $Z$ is endowed with the discrete topology. Thus, to determine the structure of $K_v^\ast$ we need only describe $U_v$. It can be shown quite simply that $U_v$ is a compact group, locally isomorphic to $O_v$. It follows that $U_v \cong F \times Z_p^n$, where $n = [K_v : Q_p]$, and $F$ is the group of all roots of unity in $K_v$. Thus $K_v^\ast \cong Z \times F \times Z_p^n$.

Two important concepts relating to field extensions are the ramification index and the residue degree. We introduce these concepts first for the local case. Let $L_w/K_v$ be a finite $n$-dimensional extension. Then the value group $\Gamma_w = v(K_w^\ast)$ has finite index in $\Gamma_w = w(L_w^\ast)$, and the corresponding index $e(w|v) = [\Gamma_w : \Gamma_v]$ is called the ramification index. The residue field $l_w = O_w/p_w$ is a finite extension of the residue field $k_v$, and $f(w|v) = [l_w : k_v]$ is the residue degree. Moreover $e(w|v)f(w|v) = n$. An extension for which $e(w|v) = 1$ is called unramified and an extension for which $f(w|v) = 1$ is called totally ramified.

Now let $L/K$ be a finite $n$-dimensional extension over an algebraic number field. Then for any valuation $v$ in $V^K$ and any extension $w$ to $L$, the ramification index $e(w|v)$ and residue degree $f(w|v)$ are defined respectively as the ramification index and residue degree for the extension of the completions $L_w/K_v$. (One can also give an intrinsic definition based on $O_v$.

\(^1\) Henceforth completions of a number field with respect to non-trivial valuations are called local fields. It can be shown that the class of local fields thus defined coincides with the class of non-discrete 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 stress this property will say non-archimedean local field.
the value groups $\Gamma_v = \nu(K^*)$, $\Gamma_w = w(L^*)$ and the residue fields

$$\bar{k}_w = \mathcal{O}_K(v)/\mathfrak{p}_K(v), \quad \bar{l}_w = \mathcal{O}_L(w)/\mathfrak{p}_L(w),$$

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 $\Gamma_v = \Gamma_w, \Gamma_w = \Gamma_w, k_v = k_w$ and $l_w = l_w$.) \[L_w : K_w = e(w/v)f(w/v).\] Thus, if

$$w_1, \ldots, w_r$$

are all the extensions of $v$ to $L$, then

$$\sum_{i=1}^r e(w_i/v)f(w_i/v) = \sum_{i=1}^r |L_{w_i} : K_{w_i}| = n.$$

Generally speaking $e(w_i/v)$ and $f(w_i/v)$ may differ for different $i$, but there is an important case when they are the same; namely, when $L/K$ is a Galois extension. Let $\mathcal{G}$ denote its Galois group. 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 $\sigma_i$ in $\mathcal{G}$ such that $w_i(x) = w_i(\sigma_i(x))$ for all $x$ in $L$. It follows that $e(w_i/v)$ and $f(w_i/v)$ are independent of $i$ (we shall write them merely as $e$ and $f$); moreover the number of different extensions $\tau$ is the index $[\mathcal{G} : \mathcal{G}(w_1)]$ of the decomposition group $\mathcal{G}(w_1) = \{ \sigma \in \mathcal{G} : w_1(\sigma(x)) = w_1(x) \}$ for all $x$ in $L$. Consequently $ef \tau = n$, 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 extension fields.

Let $v \in V^K$ and assume the associated residue field $k_v$ is the finite field $F_q$ of $q$ elements.

PROPOSITION 1.1. For any integer $n \geq 1$ there exists a unique unramified (or $n$-dimensional) extension $L/K_v$. It is generated over $K_v$ by all the $(q^n - 1)$-roots of unity, and therefore is a Galois extension. Sending $\sigma \in \text{Gal}(L/K_v)$ to the corresponding $\hat{\sigma} \in \text{Gal}(L/k_v)$, where $l \simeq F_q^r$ is the residue field of $L$, induces an isomorphism of the Galois groups $\text{Gal}(L/K_v) \simeq \text{Gal}(L/k_v)$.

In defining $\hat{\sigma}$ we note that the valuation ring $O_L$ and its valuation ideal $\mathfrak{p}_L$ are invariant under $\sigma$ and thus $\sigma$ induces an automorphism $\hat{\sigma}$ of the residue field $l = O_L/\mathfrak{p}_L$. Note further, that $\text{Gal}(L/k_v)$ is cyclic and is generated by the Frobenius automorphism given by $\varphi(x) = x^q$ for all $x$ in $k_v$; the corresponding element of $\text{Gal}(L/K_v)$ is also called the Frobenius automorphism (of the extension $L/K_v$) and is written as $\text{Fr}(L/k_v)$.

The norm properties of unramified extensions give

PROPOSITION 1.2. Let $L/K_v$ be an unramified extension. Then $U_v = N_{L/K_v}(U_L)$; in particular $U_v \subset N_{L/K_v}(L^*)$.

PROOF: We base our argument on the canonical filtration of the group of units, which is useful in other cases as well. Namely, for any integer $i \geq 1$ 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 and actually form bases of the neighborhoods of the identity in $U_v$ and $U_L$ respectively. We have the following isomorphisms:

$$U_v/U_v^{(1)} \simeq k_v^*, \quad U_v^{(i)}/U_v^{(i+1)} \simeq k_v^+, \quad \text{for } i \geq 1.$$

(1.4)

(1.5)

Since $L/K_v$ is unramified, $\pi$ is also a uniformizing parameter of $L$, and in what follows we shall also be assuming that the second isomorphism in (1.5) is defined by means of $\pi$. For a in $U_L$ we have (with bar denoting reduction modulo $\mathfrak{p}_L$)

$$N_{L/K_v}(a) = \prod_{\sigma \in \text{Gal}(L/K_v)} \sigma(a) = \prod_{\tau \in \text{Gal}(L/k_v)} \tau(a) = N_{L/k_v}(\bar{a}).$$

Thus the norm map induces a homomorphism $U_L/U_L^{(1)} ightarrow U_v/U_v^{(1)}$, which with identifications (1.4) and (1.5) is $N_{L/k_v}$. Further, for any $i \geq 1$ and any $a$ in $O_L$ we have

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

(1.6)

It follows that $N_{L/K_v}$ induces homomorphisms $U_L^{(i)}/U_L^{(i+1)} ightarrow U_v^{(i)}/U_v^{(i+1)}$, which with identifications (1.4) and (1.5) is the trace map $\text{Tr}_{L/k_v}$. But the norm and trace 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 $U_L^{(i)}$ form a base of neighborhoods of identity, the above condition means that $W$ is dense in $U_v$. On the other hand, since $U_L$ is compact and the norm is continuous, it follows that $W$ is closed, and therefore $W = U_v$. Q.E.D.

The proof of Proposition 2 also yields

COROLLARY. 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 need one more assertion concerning the properties of the filtration in the group of units under the norm map, in arbitrary extensions.

**Proposition 1.3.** For any finite extension $L/K_v$, we have

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

**Proof:** We begin with the second assertion. Let $M$ be a Galois extension of $K_v$ containing $L$. Then for a in $L$, $N_{M/K_v}(a) = \prod \sigma(a)$, where the product is taken over all embeddings $\sigma : L \hookrightarrow M$ over $K_v$. Since in the local case $v$ extends to a unique valuation $w$ on $L$, it follows that $w(a) = w(\sigma(a))$ for any a in $L$ and any $\sigma$; in particular, if we choose a uniformizing parameter $\pi_L$ in $L$ we have $\sigma(\pi_L) = \pi_Lb_v$ for suitable $b_v$ in $M$. It follows that for $a = 1 + \pi_L^j \in U_L^{(1)}$ we have

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

But from our definition of the ramification index we have $p_v \mathcal{O}_L = \mathcal{P}_L$, so that $\pi_L^j \mathcal{O}_M \cap K_v = \pi_L^j \mathcal{O}_L \cap K_v = \mathcal{P}_L \cap \mathcal{O}_L \subset \mathcal{P}_L$ (where $j$ is chosen as indicated in the assertion) and $N_{L/K_v}(a) \in U_L^{(1)}$. In particular $N_{L/K_v}(U_L^{(1)}) \subset U_v^{(1)}$; therefore to prove the first assertion we must show that $U_v^{(1)} \cap N_{L/K_v}(L^*) \subset N_{L/K_v}(U_L^{(1)})$. Let $a \in L^*$ and $N_{L/K_v}(a) \in U_v^{(1)}$. Then (1.1) implies $a \in U_v$. Isomorphism (1.5) shows that $U_L^{(1)}$ is a maximal pro-p-subgroup in $U_v$ for the prime $p$ corresponding to the valuation $v$, from which it follows that $U_L \simeq U_L^{(1)} \times U_L^{(1)}$. In particular, $a = b c$ where $c \in U_L^{(1)}$ and $b$ is an element of finite order coprime to $p$. We have $d = N_{L/K_v}(b) = N_{L/K_v}(a) N_{L/K_v}(c)^{-1} \in U_v^{(1)}$. Any element of finite order taken from $U_v^{(1)}$ has order a power of $p$; on the other hand, the order of $d$ is a divisor of the order of $b$ and hence is coprime to $p$. Thus $d = 1$ and $N_{L/K_v}(a) = N_{L/K_v}(c) \in N_{L/K_v}(U_L^{(1)})$. Q.E.D.

Now we return to the unramified completions 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, and $\text{Gal}(K_v^{nr}/K_v)$ is isomorphic to the Galois group $\text{Gal}(k_v/k_v)$ of the algebraic closure of the residue field $k_v$, i.e., isomorphic to $\mathbb{Z}$, the profinite completion of the infinite cyclic group whose generator is the Frobenius automorphism.

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

We know that any two valuations $w_1, w_2$ extending $v$ are conjugate under $\mathcal{G}$, from which it follows that the Frobenius automorphisms $\text{Fr}(L_w/K_w)$ corresponding to all extensions of $v$ form a conjugacy class $F(v)$ in $\mathcal{G}$. But does this produce all the conjugacy classes in $\mathcal{G}$? In other words, for any $\sigma$ in $\mathcal{G}$ is there a valuation $v \in V_F^K$ such that for suitable $w|v$ the extension $L_w/K_v$ is unramified and $\text{Fr}(L_w/K_v) = \sigma$?

**Theorem 1.2 (Chebotarev).** Let $L/K$ be a finite Galois extension with Galois group $\mathcal{G}$. Then, for any $\sigma$ 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 $\text{Fr}(L_w/K_v) = \sigma$.

In particular, there exist infinitely many $v$ such that $L_w = K_v$, i.e., $L \subset K_v$.

Actually Chebotarev defined a quantitative measure (density) of the set of $v \in V_F^K$ such that the conjugacy class $F(v)$ is a given conjugacy class $C \subset \mathcal{G}$. The density is equal to $|C|/|\mathcal{G}|$ (and the density of the entire set $V_F^K$ is thereby 1). Therefore, Theorem 1.2 (more precisely, the corresponding assertion about the density) is called the Chebotarev Density Theorem. For cyclic extensions of $K = \mathbb{Q}$ it is equivalent to Dirichlet’s theorem on prime numbers in arithmetic progressions. We note, further, that the last part of Theorem 1.2 can be proven indirectly, without using analytical methods.

Using geometric number theory one can prove

**Theorem 1.3 (Hermite).** If $K/Q$ is a finite extension, unramified relative to all primes $p$ (i.e., $K_v/Q_p$ is unramified for all $p$ and all $v|p$), then $K = Q$.

We will not present a detailed analysis of totally ramified extensions (in particular, the distinction between weakly and strongly ramified extensions) at this point, but we limit ourselves to describing them using Eisenstein polynomials. Recall that a polynomial $e(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in K_v[t]$ is called an Eisenstein polynomial if $a_i \in \mathbb{Z}_p$ for all $i = 0, \ldots, n - 1$ and $a_0 \notin \mathbb{Z}_p$. It is well known that an Eisenstein polynomial is irreducible in $K_v[t]$.

**Proposition 1.4.** If $\Pi$ is the root of an Eisenstein polynomial $e(t)$, then $L = K_v[\Pi]$ is a totally ramified extension of $K_v$ with uniformizing parameter $\Pi$. Conversely, if $L/K_v$ is totally ramified and $\Pi$ is a uniformizing
Chapter 1. Algebraic number theory

1.2. Adeles, approximation, local-global principle

The parameter of $L$ then $L = K_v[\Pi]$ and the minimal polynomial of $\Pi$ over $K_v$ is an Eisenstein polynomial.

**Corollary.** If $L/K_v$ is totally ramified, then $N_{L/K_v}(L^*)$ contains a uniformizing parameter of $K_v$. The ramification groups $G_i$ ($i \geq 0$), subgroups of $G$, are helpful in studying ramification in a Galois extension $L/K$ with Galois group $G$. If $w|v$, then by definition $G^0$ is the decomposition group $G(w)$ of $w$, which can be identified with the local Galois group $\text{Gal}(L_w/K_v)$. Next,

$$G^{(1)} = \{ \sigma \in G^0 : \sigma(a) \equiv a \pmod{\mathfrak{p}_L} \text{ for all } a \in O_L \}$$

is the inertia group. It is the kernel of the homomorphism $\text{Gal}(L_w/K_v) \to \text{Gal}(l_w/k_v)$ sending each automorphism of $L_w$ to the induced automorphism of $l_w$. Therefore $G^{(1)}$ is a normal subgroup of $G^0$ and by the surjectivity of the above homomorphism $G^0/G^{(1)} \simeq \text{Gal}(l_w/k_v)$. Moreover, the fixed field $E = L^{G^{(1)}}$ is the maximal unramified extension of $K_v$ contained in $L_w$, and $L_w/E$ is completely ramified. The ramification groups are defined as follows: $G^{(i)} = \{ \sigma \in G^0 : \sigma(a) \equiv a \pmod{\mathfrak{p}_L^i} \}$. They are normal in $G^0$, and $G^{(1)} = \{ e \}$ for suitably large $i$. Furthermore, the factors $G^{(i)}/G^{(i+1)}$ for $i \geq 1$ are $p$-groups where $p$ is the prime corresponding to $v$.

Note that the groups $G^{(i)} = G^{(i)}(v)$ thus defined are dependent on the particular extension $w|v$ and for other choice of $w$ would be replaced by suitable conjugates. In particular, the fixed field $L^{H}$ of the subgroup $H \subset G$ generated by the inertia groups $G^{(i)}(w)$ for all extensions $w|v$, is the maximal normal subextension in $L$ which is unramified with respect to all valuations extending $v$.

1.2. Adeles and idèles; strong and weak approximation; the local-global principle.

An individual valuation $v$ in $V^K$ does not have a significant effect on the arithmetic of $K$. However when several valuations are considered together (for example, when taking the entire set $V^K$), we are led to important insights in the arithmetic properties of $K$. In this section we introduce constructions which enable us to study all the completions of $K$ simultaneously.

**1.2.1. Adeles and idèles.** The set of adeles $A_K$ of the algebraic number field $K$ is the subset of the direct product $\prod_{v \in V^K} K_v$ consisting of those $x = (x_v)$ such that $x_v \in O_v$ for almost all $v$ in $V^K$. $A_K$ is a ring with respect to the operations in the direct product. We shall introduce a topology on $A_K$; namely, the base of the open sets consists of 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 $V^K_{\infty}$ and $W_v \subset K_v$ are open subsets for each $v$ in $S$. (This topology, called the adele topology, is stronger than the topology induced from the direct product $\prod_{v \in V^K} K_v$.) $A_K$ is a locally compact topological ring with respect to the adele topology. For any finite subset $S \subset V^K$ containing $V^K_{\infty}$ the ring $S$-integrated adeles is defined: $A_K(S) = \prod_{v \in S} K_v \times \prod_{v \in V^K \setminus S} \mathcal{O}_v$, if $S = V^K_{\infty}$ then the corresponding ring is called the ring of integral adeles and is written $A_K(\infty)$. 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 $V^K_{\infty}$. It is easy to show that for any $a \in K$ and almost all $v \in V^K_{\infty}$ we have $|a|_v \leq 1$, i.e., $a \in \mathcal{O}_K$. If $a \in K^\times$, then applying this inequality to $a^{-1}$ actually yields $a \in U_v$ for almost all $v \in V^K_{\infty}$. Below we shall use the notation $V(a) = \{ v \in V^K_{\infty} : a \notin U_v \}$. It follows that there exists a diagonal embedding $K \to A_K$, given by $x \mapsto (x, x, \ldots)$, whose image is called the ring of principal adeles and can be identified with $K$.

**Proposition 1.5.** The ring of principal adeles is discrete in $A_K$.

Note that since $\mathcal{O} = \bigcap_{v \in V^K_{\infty}} (K \cap \mathcal{O}_v)$, 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 $\bigcap_{v \in V^K_{\infty}} K_v = K \otimes_{\mathbb{Q}} \mathbb{R}$. Let $x_1, \ldots, x_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}$ which is also a $\mathbb{Q}$-basis of $K$, and consequently also an $\mathbb{R}$-basis of $K \otimes_{\mathbb{Q}} \mathbb{R}$. Thereby is a $\mathbb{Z}^n$-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 $S \subset V^K_{\infty}$) 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 $O(V^K_{\infty})$ is the usual ring of integers $\mathcal{O}$.)

The multiplicative analog of adeles is idèles of $K$, the set $J_K$ which, by definition, consists of $x = (x_v) \in \prod_{v \in V^K} K_v^\times$, such that $x_v \in U_v$ for almost all $v \in V^K$. $J_K$ is clearly a subgroup of the direct product; moreover, $J_K$ actually is the group of invertible elements of $A_K$. We note, however, that $J_K$ curiously is not a topological group with respect to the topology induced from $A_K$ (taking the inverse element is not a continuous operation in this topology.) The “proper” topology on $J_K$ is induced by the topology on $A_K \times A_K$ with the embedding $J_K \to A_K \times A_K$, $x \mapsto (x, x^{-1})$. Explicitly, this topology can be given via a base of open sets, which consists of 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 $V^K_n$ and $W_v \subset K_v^*$ are open subsets for $v$ in $S$. This topology, called the idele topology, is stronger than the induced adele topology, and with respect to it $J_K$ is a locally compact topological group. (One cannot help but note the analogy between adeles and ideles. Indeed, both concepts are special cases of adeles of algebraic groups and of the more general construction of a bounded topological product, which we shall look at in Chapter 5).

The analogy between adeles and ideles can be taken further. For any finite subset $S \subset V^K$ containing $V^K_n$, the group of $S$-integral ideles is defined: $J_K(S) = \prod_{v \in S} K_v^* \times \prod_{v \in S} U_v$, which for $S = V^K_n$ is called the group of integral ideles and is denoted by $J_K(\infty)$. As we have noted, 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 1.6.** The group of principal ideles is discrete in $J_K$.

The assertion follows from Proposition 1.5 and the fact that the induced adele topology on $J_K$ is weaker than the idele topology.

An alternate proof may be presented using the product formula, which asserts that $\prod_{v \in V^K} |a|_v^{w_v} = 1$ for any $a$ in $K^*$, where $V^K$ consists of the extensions of the valuations $|_p$ and $|_\infty$ of $\mathbb{Q}$, and $w_v = [K_v : \mathbb{Q}_p]$ (respectively $w_v = [K_v : R]$) is the local dimension with respect to the $p$-adic (respectively, Archimedean) valuation $v$. The product formula can be stated more elegantly as $\prod_{v \in V^K} \|a\|_v = 1$, introducing the normalized valuation $\|a\|_v = |a|_v^{w_v}$. This defines the same topology on $K$ as the original valuation $|_v$, and actually $\|\|_v$ is a valuation equivalent to $|_v$, except for the case where $v$ is complex. For non-Archimedean $v$ the normalized valuation admits the following intrinsic description: if $r \in K_v$ is a uniformizing parameter, then $\|r\|_v = q^{1/n}$, where $q$ is the number of elements of the residue field $k_v$.

Now let us return to Proposition 1.6. For Archimedean $v$ we shall let $W_v = \{x \in K_v^* : \|x - 1\|_v < 1/2\}$ and shall observe that the neighborhood of the identity $\Omega = \prod_{v \in V^K_n} W_v \times \prod_{v \in V^K \setminus S} U_v$ satisfies $\Omega \cap K^* = \{1\}$. Indeed, if $a \in \Omega \cap K^*$ and $a \neq 1$, then we would have $\prod_{v \in V^K_n} \|a - 1\|_v < \prod_{v \in V^K_n} \frac{1}{2} < \prod_{v \in V^K} 1 < 1$, which contradicts the product formula.

Using normalized valuations we can define a continuous homomorphism $J_K \to \mathbb{R}^+$, given by $(x_v) \mapsto \prod_{v \in V^K_n} \|x_v\|_v$, whose kernel $J_K^1$ is called the group of special ideles. (Note, that by the product formula $J_K^1 \subseteq K^*$.) Since $K$ is discrete in $A_K$ and $K^*$ is discrete in $J_K$, naturally the question arises of constructing fundamental domains for $K$ in $A_K$ and for $K^*$ in $J_K$. We shall not explore these questions in detail at this point (cf. Lang [2], ANT), but will consider them later, more generally, in connection with arbitrary algebraic groups. Let us note only that the factor spaces $A_K/K$ and $J_K/K^*$ are compact, but $J_K/K^*$ is not.

Let us state the fundamental isomorphism from the group $J_K/J_K(\infty)K^*$ to the ideal class group $\text{Cl}(K)$ of $K$. We can describe it as follows. First, establish a bijection between the set $V^K_\infty$ of non-Archimedean valuations of $K$ and the set $P$ of non-zero prime (maximal) ideals of $\mathcal{O}$, under which the ideal $p(v) = \mathcal{O} \cap p_v$ corresponds to $v$. Then the ideal $i(x) = \prod_{v \in V^K} p(v)$ corresponds to the idele $x = (x_v)$. (Note that since $x \in J_K$, $v(x_v) = 0$ for almost all $v$ in $V^K_\infty$, so the product is well-defined.) Moreover, the power $p^a$ of $p$ for a negative integer $a$ is defined in the group $\text{Id}(K)$ of fractional ideals of $K$ (cf. §1.1, ¶1). From the theorem that any fractional ideal in $K$ (as well as any non-zero ideal in $\mathcal{O}$) uniquely decomposes as the product of powers of prime ideals it is easy to see that $i : x \mapsto i(x)$ is a surjection of $J_K$ onto $\text{Id}(K)$, whose kernel is the group $J_K(\infty)$ of ideal ideles. In view of the fact that $i(K^*)$ is the group of principal fractional ideals, $i$ induces the requisite isomorphism $J_K/J_K(\infty)K^* \cong \text{Cl}(K)$. 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. Chapter 8).

**1.2.2. Strong and weak approximation.** We shall need truncations $A_{K,S}$ of adele rings, 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 $\prod_{v \in S} K_v$. 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 $A_{K,S}$. To simplify the notation we shall write respectively $A_S, A_S(T)$ instead of $A_{K,S}, A_{K,S}(T)$ when the field is clear from the context. In particular, for $S = V^K_\infty$ the ring $A_{K,V^K_\infty}$ will be written as $A_T$ and called the ring of finite adeles. A topology is introduced on $A_S$ in the obvious way: for the base of open sets we take the sets of the form $\prod_{v \in T} W_v \times \prod_{v \in V^K \setminus T} \mathcal{O}_v$, where $T \subset V^K \setminus S$ is a subset, and $W_v$ is an open subset of $K_v$ for each $v$ in $T$. We have $A = K_S \times A_S$ for $K_S = \prod_{v \in S} K_v$. $K_S$ is given the direct product topology, and then $A$ is the product of the topological rings $K_S$ and $A_S$. Moreover, the diagonal embedding of $K$ in $A$ is the product of the diagonal embeddings in $K_S$ and $A_S$, respectively.

It is worth noting that although the image of the diagonal embedding of
Chapter 1. Algebraic number theory

1.2. Adeles, approximation, local-global principle

$K$ in $A$ is discrete, each embedding $K \rightarrow K_S$, $K \rightarrow A_S$ is dense.

**Theorem 1.4 (Weak Approximation).** The image of $K$ under the diagonal embedding is dense in $K_S$.

**Theorem 1.5 (Strong Approximation).** If $S \neq \emptyset$ then the image of $K$ under the diagonal embedding is dense in $A_S$.

Theorem 1.4 holds for any field $K$ and any finite set $S$ of inequivalent valuations; but, in contrast, Theorem 1.5 (and all concepts pertaining to adeles) is meaningful only for number fields (or, more generally, global fields). To elucidate the arithmetic meaning of Theorem 1.4 let us analyze in detail the case where $K = \mathbb{Q}$ and $S = \{\infty\}$. Since, for any adele $x \in A_f = A_0, S$ we can select an integer $m$ such that $mz \in A_f(\infty)$, we actually need only show that $Z$ is densely embedded in the product $A_f(\infty) = \prod_p \mathbb{Z}_p$.

Any open subset of $A_f(\infty)$ contains a set of the form

$$W = \prod_{i=1}^{r} (a_i + p_i^{\alpha_i} \mathbb{Z}_p) \times \prod_{p \not\in S} \mathbb{Z}_p$$

where $\{p_1, \ldots, p_r\}$ is a finite collection of prime numbers, $\alpha_i > 0$ are integers, and $a_i \in \mathbb{Z}$. Then asking whether $Z \cap W$ is non-empty is the same as asking whether the system of equivalences $x \equiv a_i \mod p_i^{\alpha_i}$ ($i = 1, 2, \ldots, r$) is solvable, and, by the classic Chinese remainder theorem, it is. Thus, in the given case the strong approximation theorem is equivalent to the Chinese remainder theorem. In Chapter 7 we shall examine weak and strong approximation for algebraic groups.

1.2.3. The local-global principle. Investigating arithmetic questions over local fields is considerably simpler than the original task of looking at them over number fields. This naturally brings us to the question underlying the local-global method: when does the fact that a given property is satisfied over all completions $K_v$ of a number field $K$ mean that it is satisfied over $K$? One of the first results in this area is the classical

**Theorem 1.6 (Minkowski-Hasse).** Let $f = f(x_1, \ldots, x_n)$ be a non-degenerate 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.

The assertion on the feasibility of moving from local to global in a given case is called the local-global, or Hasse, principle. The local-global principle pervades the arithmetic theory of algebraic groups, and various of its aspects will come up time and again throughout the book. One should not, however, think that the local-global principle for homogeneous forms always holds. We shall conclude this section with a classic example.

First let us point out several aspects of the connection between the adele ring $A_K$ of $K$ and the adele ring $A_L$ of a finite extension $L$ of $K$. There exists a natural isomorphism $A_K \otimes \mathbb{L} \simeq A_L$ in both the algebraic and the topological sense. This isomorphism is obtained from the local isomorphisms $(1.2)$, $K_v \otimes\mathbb{L} \simeq \prod_{v|L} L_w$, and we need only note that for almost all $v$ in $V^K$ these isomorphisms yield $\mathcal{O}_v \otimes \mathcal{O}_L \simeq \prod_{w|v} \mathcal{O}_w$. Further, the formulas in $(1.3)$ show that the norm and trace maps $N_{L/K}$ and $\text{Tr}_{L/K}$ extend to maps $N_{L/K} : A_L \rightarrow A_K$ and $\text{Tr}_{L/K} : A_L \rightarrow A_K$ by the formulas

$$N_{L/K}(x_w) = (\prod_{w|v} N_{L_w/K_v}(x_w))^v$$
$$\text{Tr}_{L/K}(x_w) = (\sum_{w|v} \text{Tr}_{L_w/K_v}(x_w))^v.$$ 

We can easily verify that the norm map $N_{L/K}$ thus obtained induces a continuous homomorphism of idele groups, $N_{L/K} : J_L \rightarrow J_K$. The Hasse norm principle is said to be satisfied for the extension $L/K$ if

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

By Proposition 1.2 for almost all $v$ in $V^K$ any element $a$ in $K^*$ belongs to $U_v$ and $L_w/K_v$ is unramified, hence the condition $a \in N_{L/K}(J_L)$ is actually equivalent to $a \in N_{L/K}(\prod L_w) = N_{L/K}(L \otimes K_v)$ for all $v$ in $V^K$. In the language of algebraic geometry, this means that for all $v$ in $V^K$ there is a solution over all $K_v$ for the equation $f(x_1, \ldots, x_n) = a$, where $f$ is the homogeneous polynomial of degree $n$ describing the norm of an element $x$ in terms of its coordinates $x_1, \ldots, x_n$, with respect to a given base of $L/K$; and the validity of the Hasse norm principle in this case means that there is a solution over $K$. (It would be incorrect to formulate the norm principle as $a \in N_{L/K}(L^*) \iff a \in N_{L_v/K_v}(L_v^*)$ for all $v$ and all $w|v$, since in general $N_{L/K}(L^*) \subseteq N_{L_v/K_v}(L_v^*)$ when $L/K$ is not a Galois extension.)

Hasse’s norm theorem (cf. Hasse [1], also the corollary of Theorem 6.11) states that the norm principle holds for cyclic Galois extensions. On the other hand, it has been found that the norm principle is not satisfied for $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{3}, \sqrt{7})$, 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 $5^*$ is a local norm at each point, but is not a global norm. (We shall return to the Hasse norm principle in Chapter 6, §6.3.)