On Almost Strong Approximation Property in Reductive Algebraic Groups

by

Wojciech Tralle

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)

at the
University of Virginia
2025

Date of Final Oral Exam: March 19th, 2025
The dissertation is approved by the following members of the Final Oral Committee:

Andrei Rapinchuk, McConnell-Bernard Professor of Mathematics
Evangelia Gazaki, Assistant Professor of Mathematics
Mikhail Ershov, Professor of Mathematics
Israel Klich, Professor of Physics

On almost strong approximation property in reductive algebraic groups

Abstract

We investigate a slight weakening of the classical property of strong approximation, which we call *almost strong approximation*, for connected reductive algebraic groups over global fields with respect to special sets of valuations. While nonsimply connected groups (in particular, all algebraic tori) always fail to have strong approximation – and even almost strong approximation – with respect to any finite set of valuations, we show that under appropriate assumptions they do have almost strong approximation with respect to (infinite) *tractable* sets of valuations, i.e. those sets that contain all archimedean valuations and a generalized arithmetic progression minus a set having Dirichlet density zero. Almost strong approximation is likely to have a variety of applications, and as an example we use almost strong approximation for tori to extend the essential part of the result of Radhika and Raghunathan (cf. [22, Theorem 5.1]) on the congruence subgroup problem for inner forms of type A_n to all absolutely almost simple simply connected groups.

Acknowledgements

I want to first and foremost thank my academic advisor Professor Andrei Rapinchuk for all the time he sacrificed and all the help and guidance he provided me with during the entire Ph.D. program. All his efforts made me better matematician and taught me how to work more efficiently and productively. This dissertation would not be complete without Professor Rapinchuk's valuable comments and suggestions. I should also thank Professors Evangelia Gazaki and Mikhail Ershov who taught me several valuable graduate courses in areas related to my research and were always very patient with me. I firmly believe all their efforts helped me improve the quality of my research. It should be mentioned that a large part of my Ph.D. program consisted of teaching. Here I would especially like to thank Professors Brianna Kurtz and Daniel James who provided me with helpful suggestions on how to improve my teaching and communicate mathematics to students who come from very diverse backgrounds. I also want to thank my parents Aleksy Tralle and Irena Morocka-Tralle as well as my brothers Eugeniusz Tralle and Leon Morocki who were always very supportive in all my mathematical endeavors. Finally, let me thank Godfrey Dzhivhuho, a great friend who, as a researcher coming from a completely different area of study, shared with me valuable suggestions about how to deal with various difficulties arising in a Ph.D. program.

Contents

1 Algebraic number theory **10**
1.1 Adeles and ideles 10
1.1.1 Valuations and global fields 10
1.1.2 The ring of adeles 18
1.1.3 The group of ideles 27
1.2 Class field theory 33
1.2.1 Statements of key results from class field theory 33
1.2.2 Construction of the Artin map via the reciprocity law 35
1.2.3 The Hilbert symbol and Artin map for quadratic extensions . 39
1.2.4 (Generalized) arithmetic progressions and density theorems . . 42
1.3 Almost strong approximation for the multiplicative group of a field . 47
1.3.1 Motivating examples 47
1.3.2 Almost strong approximation for multiplicative group of a field 52

2 Algebraic groups and cohomology **57**
2.1 Algebraic groups 57
2.1.1 Definitions and examples 57
2.1.2 The group of adeles 62
2.2 Algebraic tori 67
2.2.1 Tori and restriction of scalars 67
2.2.2 G-modules, characters and co-characters of a torus 70
2.2.3 Equivalence of categories 82
2.3 Cohomology 90
2.3.1 Cohomology groups in lower dimensions 90
2.3.2 One consequence of Nakayama-Tate theorem 98
2.3.3 Nonabelian cohomology 101

3 Almost strong approximation in algebraic groups **104**
3.1 Almost strong approximation in tori 104
3.1.1 The case of quasi-split tori 106
3.1.2 The case of arbitrary tori 107
3.2 Almost strong approximation in reductive groups 109
3.2.1 Special case: H is simply connected. 110

3.2.2 Existence of special covers. 112
3.2.3 General case. 114
3.2.4 A counter-example to almost strong approximation 115
3.3 Application to congruence subgroup problem 123
3.3.1 Overview of the congruence subgroup problem. 123
3.3.2 Proof of Theorem B 126

Introduction

The goal of this thesis is to develop new results on strong approximation property for reductive algebraic groups and apply them to the congruence subgroup problem. While strong approximation in semi-simple *simply connected* groups has been one of the main tools in the arithmetic theory of algebraic groups since its inception, here we establish (under appropriate assumptions) a slightly weaker property that we term *almost strong approximation* for (connected reductive) *nonsimply connected groups* where strong approximation in the classical situation never holds.

More precisely, let G be a connected linear algebraic group defined over a global field K. Given a nonempty subset S of the set V^K of all inequivalent valuations of K, we let $\mathbb{A}_K(S)$ denote the *ring of S-adeles* of K (cf. Definition 1.1.15), and then let $G(\mathbb{A}_K(S))$ denote the *group of S-adeles* of G, equipped with the *S-adelic topology* (cf. Definition 2.1.3). The group of K-rational points $G(K)$ admits a diagonal embedding $G(K) \hookrightarrow G(\mathbb{A}_K(S))$, the image of which is usually identified with $G(K)$ and called the group of principal adeles of G. One says that G has *strong approximation* with respect to S if the diagonal embedding is dense, in other words, $\overline{G(K)}^{(S)} = G(\mathbb{A}_K(S))$ where $^{-(S)}$ denotes the closure in the S-adelic topology[1].

[1]For the context, we recall that the diagonal embedding $K \hookrightarrow \mathbb{A}_K(S)$ has discrete image if $S = \varnothing$, and dense image for any nonempty S (cf. Lemma 1.1.13). Thus, no nontrivial linear algebraic group G can have strong approximation for S empty – which is the reason why we always assume that $S \neq \varnothing$ here, while the additive group $G = \mathbb{G}_a$ does have strong approximation for every nonempty S.

Strong approximation in algebraic groups has been studied extensively since 1930s in the works of M. Eichler, M. Kneser, and other. For finite S, a criterion for strong approximation in reductive groups was obtained first by V.P. Platonov [13] in characteristic zero and later by G.A. Margulis [11] and G. Prasad [16] in positive characteristic (see [14, Theorem 7.12] for the precise statement). The "necessary" part of this criterion implies that G never has strong approximation for any finite S unless it is simply connected, and in fact in the nonsimply connected case the index $[G(\mathbb{A}_K(S)) : \overline{G(K)}^{(S)}]$ is always infinite.

In this thesis we consider sets S that contain V_∞^K and a generalized arithmetic progression minus an arbitrary set having Dirichlet density zero – we call such sets *tractable*. We then prove that for any connected reductive group G defined over a number field K and any tractable set S the quotient $G(\mathbb{A}_K(S))/\overline{G(K)}^{(S)}$ is in fact *finite* provided that a certain technical condition holds for the generalized arithmetic progression involved in the description of S. Since one cannot guarantee in the general case that this quotient is trivial (which would mean that G has strong approximation with respect to S in the classical sense), we introduce the following terminology: we say that an algebraic K-group has *almost strong approximation* (ASA) with respect to a subset $S \subset V^K$ if the index $[G(\mathbb{A}_K(S)) : \overline{G(K)}^{(S)}]$ is finite.

In order to give precise statements, we need the following definitions.

Definition A Let L/K be a finite Galois extension and let $\mathcal{C}$ be a conjugacy class in the Galois group $\mathrm{Gal}(L/K)$. A *generalized arithmetic progression* $\mathcal{P}(L/K, \mathcal{C})$ is the set of all $v \in V_f^K := V^K \setminus V_\infty^K$ such that v is unramified in L and for some (equivalently, any) extension $w|v$ the corresponding Frobenius automorphism $\mathrm{Fr}_{L/K}(w|v)$ lies in $\mathcal{C}$.

In this thesis, we will not differentiate between (finite) primes of a global field and the corresponding nonarchimedean valuations. Under this convention, the gen-

eralized arithmetic progression $\mathcal{P}(L/\mathbb{Q}, \mathcal{C}_a)$, where $L = \mathbb{Q}(\zeta_m)$ is the mth cyclotomic extension of $\mathbb{Q}$ and $\mathcal{C}_a$ with $(a, m) = 1$ consists of the automorphism $\sigma_a \in \mathrm{Gal}(L/K)$ defined by $\sigma_a(\zeta_m) = \zeta_m^a$ coincides with the set $\mathbb{P}_{a(m)}$ of rational primes p satisfying $p \equiv a (\mathrm{mod}\, m)$ (see section 1.2.4 for the detailed argument), hence the terminology. We also refer the reader to section 1.2.4 for the notion of Dirichlet density $\mathfrak{d}_K(\mathcal{P})$ of any set $\mathcal{P}$ of primes of K and its basic properties. Recall that finite sets of primes have Dirichlet density zero, however it is easy to construct infinite sets of primes with density zero for any K, and in fact for a given nontrivial finite extension $K/\mathbb{Q}$ the set of all primes of K that have relative degree > 1 over $\mathbb{Q}$ has density zero (see section 1.2.4). We are now ready for

Definition B A subset $S \subset V^K$ is *tractable* if it contains a set of the form $V_\infty^K \cup (\mathcal{P}(L/K, \mathcal{C}) \setminus \mathcal{P}_0)$ where $\mathcal{P}_0$ is a subset with $\mathfrak{d}_K(\mathcal{P}_0) = 0$.

Here is our main result on almost strong approximation for connected reductive groups.

Theorem A *For a connected reductive algebraic group G defined over a number field K, we let $T = Z(G)^\circ$ (resp., $H = [G, G]$) denote the maximal central torus (resp., the maximal semi-simple subgroup) so that $G = TH$ is an almost direct product. Set $E = PM$, where P/K is the minimal splitting field of T and M/K is the minimal Galois extension over which H becomes an inner form of a K-split group. Then for any tractable set of valuations S containing a set of the form $V_\infty^K \cup (\mathcal{P}(L/K, \mathcal{C}) \setminus \mathcal{P}_0)$ such that for some $\sigma \in \mathcal{C}$, we have*

$$\sigma|(E \cap L) = \mathrm{id}_{E \cap L}, \tag{1}$$

the closure $\overline{G(K)}^{(S)}$ is a finite index normal subgroup of $G(\mathbb{A}_K(S))$, and thus G has almost strong approximation with respect to S. Furthermore, the quotient $G(\mathbb{A}_K(S))/\overline{G(K)}^{(S)}$

is abelian and its order divides a constant $C(\ell, n, r)$ that depends only on ℓ = rank of G, $n = [L : K]$, and r = number of real valuations of K.

We note that if G is a semi-simple K-group which is an inner form of a K-split group, then the condition (1) in the theorem is trivially satisfied, so we obtain the following.

Corollary A *Let G be a semi-simple K-group which is an inner form of a K-split group. Then for any tractable set $S \subset V^K$, the group G has almost strong approximation with respect to S.*

On the other hand, it is important to point out that the condition (1) cannot be omitted in the general case. To demonstrate this, in section 3.2.4 we construct an example of a nonsimply connected semi-simple group that fails to have almost strong approximation for a tractable set S that does not satisfy (1).

The proof of Theorem A involves several stages that rely on different techniques. First, using results of class field theory and Chebotarev density theorem, we handle the case of quasi-split tori (see Theorem 3.1.2). We then present an arbitrary K-torus T as a quotient of a quasi-split one, and, using some cohomological computations involving the Nakayama-Tate theorem, prove that provided (1) holds the quotient $T(\mathbb{A}_K(S))/\overline{T(K)}^{(S)}$ is finite of order dividing a constant $\tilde{C}(d, n)$ that depends only on $d = \dim T$ and $n = [L : K]$, see Theorem 3.1.3 and (3.5).

For an arbitrary reductive K-group $G = TH$ having nontrivial semi-simple part H, we first consider the special case where H is simply connected – see Proposition 3.2.1, and then reduce the general case to the special case by using constructions and techniques from the theory of algebraic groups.

Being available for not necessarily simply connected groups, almost strong approximation is likely to expand the range of applications of the classical property

of strong approximation, many of which can be found in [14]. As an example of a new application, we present here a result on the *Congruence Subgroup Problem* (CSP). We refer the reader to section 3.3.1 for a discussion of the CSP, specifically for the notion of the congruence kernel, Serre's Congruence Subgroup Conjecture and available results. Among recent developments one can mention a uniform (i.e., requiring no case-by-case considerations) proof [20] of the triviality of the congruence kernel $C^S(G)$ for an absolutely almost simple simply connected algebraic group G over a global field K with respect to a set of valuations $S \subset V^K$ that contains V_∞^K and almost contains a generalized arithmetic progression but does not contain any nonarchimedean valuation v such that G is K_v-anisotropic – among other things, this result provides an additional evidence for Serre's conjecture. Subsequently, Radhika and Raghunathan [22] showed that the result remains valid for anisotropic inner forms of type A_n (i.e., for norm one groups $G = \mathrm{SL}_{1,D}$ associated with central division K-algebras) for a larger class of sets S that basically coincides with our tractable sets. Using our results on almost strong approximation for tori, we have been able to extend the result of [22] to all types.

Theorem B *Let G be an absolutely almost simple simply connected algebraic group defined over a global field K, and let M/K be a minimal Galois extension over which G becomes an inner form. Assume that the Margulis-Platonov conjecture (MP) (cf. §3.3.1) holds for $G(K)$. Let $S \subset V^K$ be a tractable set containing a set of the form $V_\infty^K \cup (\mathcal{P}(L/K, \mathcal{C}) \setminus \mathcal{P}_0)$, where*

$$\sigma|(M \cap L) = \mathrm{id}_{M\cap L} \quad \textit{for some} \quad \sigma \in \mathcal{C}, \tag{2}$$

and does not contain any nonarchimedean v for which G is K_v-anisotropic. Then the congruence kernel $C^S(G)$ is trivial.

It should be noted that in the cases where Serre's congruence subgroup conjecture remains open, this theorem is the best result available at this point. As we already pointed out, for inner forms of type A_n, Theorem B is due to Radhika and Raghunathan, and now we would like to transcribe it for outer forms of this type.

Corollary B *Let G be an absolutely almost simple simply connected outer form of type A_ℓ, i.e. $G = \mathrm{SU}_n(D, h)$, the special unitary group of an n-dimensional non-degenerate τ-hermitian form h over a division algebra D of degree d whose center M is a quadratic extension of K and the involution τ of D satisfies $M^\tau = K$, with $\ell = dn - 1$. Assume that (MP) holds for $G(K)$. Let $S \subset V^K$ be a tractable set containing a set of the form $V_\infty^K \cup (\mathcal{P}(L/K, \mathcal{C}) \setminus \mathcal{P}_0)$ where $\sigma|(M \cap L) = \mathrm{id}_{M\cap L}$ for some $\sigma \in \mathcal{C}$, and does not contain any nonarchimedean v for which G is K_v-anisotropic. Then $C^S(G) = \{1\}$.*

Two comments are in order. Since (MP) is known for inner forms of type A_n (see [25], [29]), no assumption on the truth of (MP) was needed in [22]. Second, since [22] deals only with inner forms, (2) holds automatically in their situation, while in the general case we need to assume (2) in order to apply our results on almost strong approximation.

The structure of this thesis is as follows. In Chapter 1, we familiarize the reader with all the necessary background from algebraic number theory. First, in section 1.1 we discuss the ring of adeles and the group of ideles together with their basic properties. Section 1.2 starts with the statements of two important results from class field theory (cf. Theorem 1.2.1 and Theorem 1.2.2) and then we discuss the basic properties of the Hilbert symbol in the context of the Artin map. Next, we state Dirichlet prime number Theorem, Chebotarev density theorem and define the notion of a generalized arithmetic progression. Section 1.3 is devoted to the investigation

of almost strong approximation for the multiplicative group of a field. We first examine several examples and then show that under some natural assumption, the multiplicative group satisfies almost strong approximation (cf. Proposition 1.3.7).

Chapter 2 provides an overview of algebraic groups (most importantly algebraic tori) and group cohomology. In section 2.1, we introduce all the relevant definitions from the theory of algebraic groups including the notion of the group of adeles of an algebraic group. Then in section 2.2, we study algebraic tori together with their groups of characters and co-characters. The most important result of this section is the equivalence between the category of tori and the category of finitely generated Galois modules without $\mathbb{Z}$-torsion (cf. Theorem 2.2.20). The purpose of section 2.3 is to provide all the necessary machinery of group cohomology. The two main results here are: Nakayama-Tate theorem (cf. Theorem 2.3.12) and Hasse local-global principle (cf. Theorem 2.3.15).

In Chapter 3 we prove the main results of this thesis. The goal of section 3.1 is to establish almost strong approximation for quasi-split tori over a global field (cf. Theorem 3.1.2) and then extend it to all tori using group cohomology (cf. Theorem 3.1.3). In section 3.2 we consider arbitrary reductive group $G = TH$ over a number field written as an almost direct product of its maximal central torus T and its maximal semi-simple subgroup H. The strategy is to first establish Theorem A in the case where H is simply connected (cf. Proposition 3.2.1) and then apply the classical criterion for strong approximation to H (cf. [14, Theorem 7.12]). Combining this with ASA for tori (Theorem 3.1.3) applied to T, this yields Theorem A in the case of simply connected H. The case of general semi-simple H is then handled by using its universal cover (cf. Lemma 3.2.3) together with some cohomological techniques and Hasse local-global principle (cf. Theorem 2.3.15). Next, we construct an example of an absolutely simple adjoint group, which is an outer form of a split group, that does

not have almost strong approximation with respect to a tractable set of valuations for which the condition (1) fails (cf. Theorem 3.2.6). Finally, in section 3.3 we review the required material dealing with the congruence subgroup problem, summarize the approach to proving the triviality of the congruence kernel developed in [20], and then apply our Theorem 3.1.3 to prove Theorem B.

Chapter 1

Algebraic number theory

1.1 Adeles and ideles

1.1.1 Valuations and global fields

Let K be a *number field*, i.e. a finite extension of $\mathbb{Q}$. One of the classical objects of study in algebraic number theory is the *ring of integers* of K, which will be denoted by $\mathcal{O}_K$. It is well-known that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$. Moreover, $\mathcal{O}_K$ is a *Dedekind domain* (cf. [2, Ch. I, §2, Proposition 1]) and consequently, one can show that any nonzero prime ideal in $\mathcal{O}_K$ has a unique factorization as the product of powers of prime ideals. This property is a generalization of the fundamental theorem of arithmetic, which states that any integer has a unique (up to associates) factorization into a product of powers of prime numbers. It should be noted however, that unlike in the case of $\mathbb{Z}$, the factorization of elements of $\mathcal{O}_K$ into irreducibles is not unique in general. Therefore, $\mathcal{O}_K$ does not have the same arithmetic as $\mathbb{Z}$. This difference motivated many problems in number theory and can be measured by the ideal class group of K, defined as follows. Any $\mathcal{O}_K$-submodule $\mathfrak{a}$ of K such that $x\mathfrak{a} \subset \mathcal{O}_K$ for some nonzero $x \in \mathcal{O}_K$ is called a *fractional ideal*. The product of two

fractional ideals $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ is defined as the $\mathcal{O}_K$-submodule in K, generated by all products xy for $x \in \mathfrak{a}, y \in \mathfrak{b}$. One shows that the set of fractional ideals of K with this operation becomes a group, which we denote by $\mathcal{I}_K$. The ideals of the form $x\mathcal{O}_K$ for some $x \in K^\times$ are called *principal fractional ideals*, and the set of all such ideals is a subgroup of $\mathcal{I}_K$, which we denote by $\mathcal{P}_K$. The quotient group $\mathrm{Cl}(K) = \mathcal{I}_K/\mathcal{P}_K$ is called the *ideal class group* of K. We may now recall the statements of two theorems from algebraic number theory, which will be later relevant for us:

Theorem 1.1.1 (Finiteness of the class group) *The group* $\mathrm{Cl}(K)$ *is finite.*

Proof. Cf. [12, Ch. I, §6, Theorem 6.3]. □

The order of the group $\mathrm{Cl}(K)$ is called the *class number* of K denoted by $h(K)$, therefore Theorem 1.1.1 will often be referred to as the *finiteness of the class number*. We will provide an alternative proof of finiteness of class number using the group of ideles in section 1.1.3. Moreover, the factorization into prime elements in $\mathcal{O}_K$ is unique precisely when the class number of K is one.

Theorem 1.1.2 (Dirichlet's Unit Theorem) *The group of units* $\mathcal{O}_K^\times$ *is finitely generated of rank* $r + s - 1$*, where* r *is the number of real embeddings of* K *and* s *is the number of conjugate pairs of complex embeddings of* K*.*

Proof. Cf. [12, Ch. I, §7, Theorem 7.4]. □

Some indications on how to prove Dirichlet's Unit theorem will be given in section 1.1.3. We may now introduce the notions of absolute value and valuation for a field K.

Definition 1.1.3 An *absolute value* on a field K is a map $|\cdot| \colon K \to \mathbb{R}$ satisfying the following conditions for all $x, y \in K$:

(1) $|x| = 0$ if and only if $x = 0$,

(2) $|xy| = |x| \cdot |y|$,

(3) $|x + y| \leq |x| + |y|$.

Any absolute value $|\cdot|$ on K endows K with the metric $d(x, y) = |x - y|$, which makes K into a *topological field*. Two absolute values $|\cdot|_1, |\cdot|_2$ on K are *equivalent* if they induce the same topology on K. One can show that two absolute values $|\cdot|_1, |\cdot|_2$ are equivalent if and only if $|\cdot|_1 = |\cdot|_2^{\alpha}$ for some real number $\alpha > 0$ (cf. [10, Ch. XII, §1, Proposition 1.1]).

An absolute value $|\cdot|$ is called *nonarchimedean* if the following *ultrametric triangle inequality* holds for all $x, y \in K$:

$$|x + y| \leq \max\{|x|, |y|\}.$$

Otherwise, $|\cdot|$ is *archimedean*. Clearly, the ultrametric triangle inequality is stronger than the usual triangle inequality (3) in Definition 1.1.3. Observe that on every field K one can define the *trivial* absolute value by setting $|0| = 0$ and $|x| = 1$ for any $x \in K^{\times}$. Clearly, the trivial absolute value induces discrete topology on K. In the next example we describe the nontrivial absolute values in the case when $K = \mathbb{Q}$.

Example 1.1.4 The usual absolute value on $\mathbb{Q}$, denoted by $|\cdot|_{\infty}$, is archimedean. For each prime p we can define the *p-adic absolute value* $|\cdot|_p$ as follows. Any rational number $x \in \mathbb{Q}^{\times}$ can be written as $x = p^r \cdot a/b$ with $a, b, r \in \mathbb{Z}$, $b \neq 0$, and $p \nmid a \cdot b$. Then we set

$$|x|_p := p^{-r}.$$

It is easy to check that $|\cdot|_p$ is a nonarchimedean absolute value. The only nontrivial absolute values on $\mathbb{Q}$ (up to equivalence) are $|\cdot|_{\infty}$ and $|\cdot|_p$ for each prime p. This result is known as Ostrowski's Theorem (cf. [15, Ch. 1, §1.1.2 , Theorem 1.1]).

Depending on the context we will also use the additive analogs of absolute values called valuations

Definition 1.1.5 A *valuation* on a field K is a map $v\colon K \to \mathbb{R} \cup \{\infty\}$ such that

(1) $v(x) = \infty$ if and only if $x = 0$,

(2) $v(xy) = v(x) + v(y)$ for all $x, y \in K$,

(3) $v(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K$.

A valuation v is called *discrete* if the *value group* $v(K^\times)$ is a discrete subgroup of $\mathbb{R}$, hence $v(K^\times) \simeq \mathbb{Z}$. Any valuation v on a field K gives rise to an absolute value $|\cdot|_v$ by setting

$$|x|_v := c^{-v(x)}$$

for a fixed real number $c > 1$. It is clear that the induced topology on K is independent of the choice of c and that the absolute value associated to a valuation is non-archimedean. We define the *p-adic valuation* v_p on $\mathbb{Q}$ by

$$v_p(x) := r,$$

where $x = p^r \cdot a/b$ with $a, b, r \in \mathbb{Z}$, $b \neq 0$ and $p \nmid a \cdot b$. Similarly to absolute values, one can define the notions of the *trivial valuation* and *equivalence of valuations* (cf. [34, Ch. 12, §12.2]).

Some of the techniques used to understand the arithmetic properties of algebraic groups involve number theoretic tools associated with valuations such as adeles and ideles. These notions can be defined over a slightly larger class of fields than number fields:

Definition 1.1.6 A *global field* is a field, which is one of the following two types

(a) *Number field*: a finite extension of $\mathbb{Q}$ (case of characteristic zero),

(b) *Global function field*: a field of rational functions of an irreducible algebraic curve over a finite field, or equivalently, a finite extension of $\mathbb{F}_q(t)$, where $\mathbb{F}_q(t)$ denotes the field of rational functions in one variable over the finite field $\mathbb{F}_q$ with q elements (case of positive characteristic).

Every global field comes with a natural family of (discrete) valuations. In characteristic zero, these valuations are associated with primes, and in positive characteristic - with closed points of the relative curve. Another special feature of global fields is that every such field can be realized as the field of fractions of a Dedekind domain and it satisfies the product formula (see section 1.1.3).

For any valuation v on a field K, we denote by K_v, the *completion* of K with respect to the corresponding absolute value $|\cdot|_v$. One constructs K_v as a quotient of the commutative ring of all Cauchy sequences in K (with respect to the topology induced by $|\cdot|_v$) by the ideal of all sequences converging to 0. An important consequence of this construction is that K_v is a complete space with respect to $|\cdot|_v$ which contains K as a dense subspace. The reader may want to consult [8, Ch. II, §2] for more details regarding the construction and properties of completion. If $K = \mathbb{Q}$ then K_v equals either the field of real numbers $\mathbb{Q}_\infty := \mathbb{R}$ if $|\cdot|_v = |\cdot|_\infty$ or the field of *p-adic numbers* $\mathbb{Q}_p$ (cf. [12, Ch. II, §1]) for some prime p if $|\cdot|_v = |\cdot|_p$.

If L is a finite extension of a number field K then any absolute value $|\cdot|_v$ on K may be *extended* to L. In other words, there exists an absolute value $|\cdot|_w$ on L such that $|x|_w = |x|_v$ for any $x \in K$. We denote this relation by $w|v$ and we say that w *lies above* v. For a detailed procedure of extension of absolute values, we refer the reader to [12, Ch. II, §8] and [15, Ch. 1, §1.1.2].

If K is any field then we write V^K to denote the set of all equivalence classes of valuations of K. For simplicity, the elements of V^K will also be called *valuations* (or

places). The set V^K is the union of the set of all archimedean valuations V_∞^K and the set of all nonarchimedean valuations V_f^K. Observe that if K is a number field then V_∞^K is the set of all extensions of $|\cdot|_\infty$ to K and V_f^K is the set of extensions of $|\cdot|_p$ for all prime numbers p. Furthermore, if $K = \mathbb{Q}$ then due to Ostrowski's theorem, the set $V_f^{\mathbb{Q}}$ may be identified with the set of all rational primes, denoted by $\mathbb{P}$. The unique archimedean valuation of $\mathbb{Q}$ will be denoted by the symbol ∞ so that $V^{\mathbb{Q}}$ will be routinely identified with $\mathbb{P} \cup \{\infty\}$.

If K is a number field then the archimedean valuations of K correspond to embeddings of K in $\mathbb{R}$ or in $\mathbb{C}$, and are called *real* or *complex* valuations, respectively. The description of completions corresponding to the nonarchimedean valuations of a number field K is more involved. Any $v \in V_f^K$ is an extension of some p-adic valuation v_p with $K_v/\mathbb{Q}_p$ a finite extension. The field $\mathbb{Q}_p$ is locally compact, so K_v is also locally compact with respect to the topology induced from $|\cdot|_v$.

A field K is called *local* if it is complete with respect to a nontrivial discrete valuation v and has finite residue field (cf. [12, Ch. II, §5]). Topologically, a local field is a Hausdorff locally compact non-discrete totally disconnected topological field. The archimedean fields $\mathbb{R}$ and $\mathbb{C}$ are by convention also considered to be local. The classification of local fields is given by the following theorem

Theorem 1.1.7 *Any local field K is one of the following:*

(a) *K is archimedean, and $K \simeq \mathbb{R}$ or $K \simeq \mathbb{C}$,*

(b) *K is nonarchimedean with* $\mathrm{char}(K) = 0$*, and K is a finite extension of $\mathbb{Q}_p$ for some prime p,*

(c) *K is nonarchimedean with* $\mathrm{char}(K) = p$*, and K is a finite extension of the field of Laurent series in one variable $\mathbb{F}_p((t))$ for some prime p. In this case, there is a (non-canonical) isomorphism $K \simeq \mathbb{F}_q((t))$ where q is a power of p.*

Proof. Cf. [12, Ch. II, §5, Proposition 5.2]. □

Given any field K with a discrete valuation v, we define the *valuation ring* of v by

$$\mathcal{O}_v = \Big\{ a \in K_v \;\Big|\; |a|_v \leq 1 \Big\}.$$

It is known that $\mathcal{O}_v$ is a local principal ideal domain with unique maximal ideal

$$\mathfrak{p}_v = \Big\{ a \in K_v \;\Big|\; |a|_v < 1 \Big\},$$

called the *valuation ideal* of v. In particular, $\mathcal{O}_v$ is a *Discrete Valuation Ring* (cf. [12, Ch. I, §11, Definition 11.3]). Observe that the group of units in $\mathcal{O}_v$ equals

$$\mathcal{O}_v^\times = \Big\{ a \in K_v \;\Big|\; |a|_v = 1 \Big\}.$$

The quotient $k(v) = \mathcal{O}_v/\mathfrak{p}_v$ is a field called the *residue field* of v. For example, the valuation ring of $\mathbb{Q}_p$ is the *ring of p-adic integers* $\mathbb{Z}_p$ (cf. [12, Ch. II, §1]) with the corresponding valuation ideal $p\mathbb{Z}_p$ and the residue field being the *finite field with p elements*, denoted by $\mathbb{F}_p$.

Returning to the general case, if K_v is a field that is complete with respect to some discrete valuation v, then the ideal $\mathfrak{p}_v$ is principal and any generator π of $\mathfrak{p}_v$ such that $v(\pi) \geq 0$ is called a *uniformizer*. It follows from the description of $\mathcal{O}_v^\times$ that if π is a fixed uniformizer then any element $x \in K_v^\times$ can be written in the form $x = \pi^k u$ for some $k \in \mathbb{Z}$ and $u \in \mathcal{O}_v^\times$. This furnishes a continuous isomorphism

$$K_v^\times \simeq \mathbb{Z} \times \mathcal{O}_v^\times.$$

One can show that $\mathcal{O}_v^\times$ is a compact group and

$$\mathcal{O}_v^\times \simeq \mu(K_v) \times \mathbb{Z}_p^n,$$

where $n = [K_v : \mathbb{Q}_p]$ and $\mu(K_v)$ is the *group of all roots of unity* in K_v (cf. [15, Ch. 1, §1.1.2]). Therefore,

$$K_v^\times \simeq \mathbb{Z} \times \mu(K_v) \times \mathbb{Z}_p^n.$$

For example, if p is an odd prime then

$$\mathbb{Q}_p^\times \simeq \mathbb{Z} \times \mathbb{F}_p^\times \times \mathbb{Z}_p$$

(also see [30, Ch. II, §3.2, Theorem 2]).

There are two important notions related to field extensions, called ramification index and residue degree. Let us first introduce these concepts locally, namely for fields that are complete with respect to a nonarchimedean valuation. Let L_w/K_v be a finite extension of degree n and let $\Gamma_w = w(L_w^\times)$, $\Gamma_v = v(K_v^\times)$ be the corresponding *valuation groups*. The index $e(w|v) = [\Gamma_w : \Gamma_v]$ is finite and we call it the *ramification index* of w with respect to v. Let $\mathfrak{P}_w$ be the valuation ideal of w and $l(w) = \mathcal{O}_w/\mathfrak{P}_w$ be the corresponding residue field. The index $f(w|v) = [l(w) : k(v)]$ is finite and we call it the *residue degree* of w with respect to v. We have the following formula (cf. [15, Ch. 1, §1.1.2]):

$$e(w|v) \cdot f(w|v) = n.$$

The extension L_w/K_v is called *unramified* if $e(w|v) = 1$ and *ramified* otherwise.

Now let L/K be an extension of a global fields with $[L : K] = n$. Then for any $v \in V_f^K$ and any extension w of v to L, we define the ramification index $e(w|v)$ and the residue degree $f(w|v)$ as the ramification index and residue degree of L_w/K_v,

respectively. One can show that if $w_1, \ldots, w_r$ are all the extensions of v to L then we have the following formula (cf. [12, Ch. II, §8, Proposition 8.5] and [15, Ch. 1, §1.1.2]):

$$\sum_{i=1}^{r} e(w_i|v) \cdot f(w_i|v) = n.$$

We say that v *splits completely* in L if we have $e(w_i|v) = f(w_i|v) = 1$ for all $i = 1, \ldots, r$. Another important property is that both ramification indices and residue degrees are multiplicative in towers (cf. [15, Ch. 1, §1.1.2 and §1.1.3]).

1.1.2 The ring of adeles

The goal of this section is to construct a topological ring $\mathbb{A}_K(S)$ associated with a global field K and any nonempty subset $S \subset V^K$, which will allow us to formulate the *strong approximation theorem* for a global field (cf. Theorem 1.1.16). As a starting point, let us state a property, called the *weak approximation*, which holds for any field K and will be used later in the analysis of the reciprocity map of global class field theory

Theorem 1.1.8 (Weak Approximation Theorem) *Let K be a field and let S be a finite set of pairwise inequivalent valuations $v_1, \ldots, v_r$. Set $K_S := \prod_{i=1}^{r} K_{v_i}$. Then the diagonal embedding $K \hookrightarrow K_S$ has dense image, where we consider K_S with the product topology. More explicitly, given $\varepsilon > 0$ and $x_1 \in K_{v_1}, \ldots, x_r \in K_{v_r}$, there exists $x \in K$ such that*

$$|x - x_i|_{v_i} < \varepsilon$$

for all $i = 1, \ldots, r$.

Proof. Cf. [10, Ch. XII, Theorem 1.2.]. □

The ring of adeles of a global field K is a number-theoretic object that takes into account all valuations of K at once. The usual direct product $\prod_{v \in V^K} K_v$ is not a

locally compact space. Thus, instead of taking the (full) direct product, we will use a more general construction called the restricted product

Definition 1.1.9 Let $\{X_i\}_{i\in I}$ be a family of topological spaces indexed by a set I and for each $i \in I$, let U_i be an open subset of X_i. The *restricted product* of $\{X_i\}_{i\in I}$ with respect to $\{U_i\}_{i\in I}$ is defined as:

$$\prod_{i\in I}{}'(X_i, U_i) := \Big\{(x_i)_{i\in I} \in \prod_{i\in I} X_i \;\Big|\; x_i \in U_i \text{ for almost all } i \in I\Big\},$$

with topology given by the following basis of open sets

$$\mathcal{B} := \Big\{ \prod_{i\in I} V_i \;\Big|\; V_i \subset X_i \text{ is open for all } i \in I \text{ and } V_i = U_i \text{ for almost all } i \in I\Big\},$$

where *for almost all* means for all but finitely many.

Let us examine how the usual direct product topology and the restricted product topology are related. For each $i \in I$ there is a natural continuous projection $\pi_i \colon \prod'_{i\in I}(X_i, U_i) \to X_i$ and as sets, we always have the inclusions

$$\prod_{i\in I} U_i \subset \prod_{i\in I}{}'(X_i, U_i).$$

However, the restricted product topology on $\prod'_{i\in I}(X_i, U_i)$ is not the same as the subspace topology it inherits from the product $\prod_{i\in I} X_i$. In fact, the restricted product has more open sets. For example, the set $\prod_{i\in I} U_i$ is open in $\prod'_{i\in I}(X_i, U_i)$, but unless $U_i = X_i$ for almost all $i \in I$, it is <u>not</u> open in $\prod_{i\in I} X_i$. The restricted product generalizes the direct product, and the two topologies coincide precisely when $U_i = X_i$ for almost all $i \in I$. For example, product topology and restricted topology coincide if the indexing set I is finite. Observe that the restricted product is fully

determined once we specify the U_i for all but finitely many $i \in I$. In other words, if $U_i = U_i'$ for almost all i then

$$\prod_{i\in I}{}'(X_i, U_i) = \prod_{i\in I}{}'(X_i, U_i').$$

For a more detailed exposition of restricted product we refer the reader to [2, Ch. II, §13].

In this thesis, we are mostly interested in restricted products of *locally compact* topological spaces $\{X_i\}_{i\in I}$ with respect to a family of open subsets $\{U_i\}_{i\in I}$ such that U_i is compact for almost all $i \in I$. The key result for restricted product in this case is the following

Proposition 1.1.10 *Let $\{X_i\}_{i\in I}$ be a family of locally compact topological spaces and for each $i \in I$, let U_i be an open subset of X_i. Assume that for almost all $i \in I$, the set U_i is compact. Then the restricted product $\prod'_{i\in I}(X_i, U_i)$ is a locally compact space.*

Proof. Let $X = \prod'_{i\in I}(X_i, U_i)$ and for any finite subset $J \subset I$, put $X_J := \prod_{i\in J} X_i \times \prod_{i\in I\setminus J} U_i$. Since all X_i are locally compact, so is the product $\prod_{i\in J} X_i$. On the other hand, almost all U_i are compact so by Tychonoff's theorem, their product is compact. Thus, X_J is a locally compact space. Since the sets X_J with $J \subset I$ a finite subset, form an open cover of X, it follows that X is locally compact. □

The restricted product construction allows us to define the ring of adeles of a global field

Definition 1.1.11 Let K be a global field. For any $v \in V_\infty^K$, we put $\mathcal{O}_v := K_v$.

The *ring of adeles* $\mathbb{A}_K$ of K is defined as the following restricted product

$$\mathbb{A}_K = \prod_{v \in V^K}{}' (K_v, \mathcal{O}_v).$$

By definition $\mathbb{A}_K$ is a subring of the product $\prod_{v \in V^K} K_v$ and it comes together with the topology, given by basic open 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 and $W_v \subset K_v$ is an open subset for each $v \in S'$. The restricted product topology on $\mathbb{A}_K$ is called *adelic topology*. An important example of an open subring of $\mathbb{A}_K$ is the *subring of integral adeles* $\mathbb{A}_{K,\infty}$ defined by

$$\mathbb{A}_{K,\infty} = \prod_{v \in V_\infty^K} K_v \times \prod_{v \in V_f^K} \mathcal{O}_v.$$

Note that the restricted product topology on $\mathbb{A}_{K,\infty}$ coincides with the usual product topology. By Proposition 1.1.10, $\mathbb{A}_K$ is locally compact. Next, we have the following lemma:

Lemma 1.1.12 *There is a diagonal embedding $K \hookrightarrow \mathbb{A}_K$, and it restricts to $K^\times \hookrightarrow \mathbb{A}_K^\times$.*

Proof. Here we only show the argument for $K = \mathbb{Q}$ but the result holds for any global field (cf. [2, Ch. II, §14]). Let $x \in \mathbb{Q}$ and let us write $x = m/n$ with m and n coprime integers. Let $n = p_1^{\alpha_1} \cdot \ldots \cdot p_\ell^{\alpha_\ell}$ be the prime factorization of n. Then for any prime p outside of the finite set $\{p_1, \ldots, p_\ell\}$, we have $|x|_p \leq 1$, so $x \in \mathbb{Z}_p$. This shows that the diagonal map $\mathbb{Q} \to \mathbb{A}_\mathbb{Q}$ is well-defined. It is also injective because for each prime p we have the embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. By applying the same argument

to x^{-1}, we see that in fact $|x|_p = 1$ for almost all primes p, so $x \in \mathbb{Z}_p^\times$. Thus, the diagonal embedding $\mathbb{Q} \hookrightarrow \mathbb{A}_\mathbb{Q}$ induces $\mathbb{Q}^\times \hookrightarrow \mathbb{A}_\mathbb{Q}^\times$. More generally, for any global field K, we still have the diagonal embedding $K^\times \hookrightarrow \mathbb{A}_K^\times$ (cf. [2, Ch. II, §16]). The group of units $\mathbb{A}_K^\times$ of $\mathbb{A}_K$ will be studied in greater detail in the next section. □

The image of any $a \in K$ under the diagonal embedding $K \hookrightarrow \mathbb{A}_K$ is called the *principal adele* corresponding to a and will be denoted by (a) or simply by a. The image of K under this embedding forms a subring of $\mathbb{A}_K$, called the ring of *principal adeles*, which we routinely identify with K and it has the following important property

Lemma 1.1.13 *K is discrete in $\mathbb{A}_K$.*

Proof. Let us first explain the argument for $K = \mathbb{Q}$. Consider the following neighborhood of zero in $\mathbb{A}_\mathbb{Q}$

$$W = \Big(-\frac{1}{2}, \frac{1}{2}\Big) \times \prod_{p \in \mathbb{P}} \mathbb{Z}_p.$$

If $x \in \mathbb{Q} \cap W$, then $x \in \mathbb{Z}_p$ for all p, and therefore $x \in \mathbb{Z}$. At the same time, $x \in (-\frac{1}{2}, \frac{1}{2})$, so $x = 0$. Thus, $\mathbb{Q} \cap W = \{0\}$, and therefore $\mathbb{Q}$ is discrete in $\mathbb{A}_\mathbb{Q}$. □

Now let K be a number field and let us show that K is discrete in $\mathbb{A}_K$. There is a topological isomorphism

$$\prod_{v \in V_\infty^K} K_v \simeq K \otimes_\mathbb{Q} \mathbb{R},$$

(cf. [12, Ch. II, §8, Proposition 8.3] and [14, Ch. 1, §1.1.2]). Since the ring of integers $\mathcal{O}_K$ of K is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$, we may fix a $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_n$ of $\mathcal{O}_K$. Then the corresponding vectors $\omega_1 \otimes 1, \ldots, \omega_n \otimes 1$ are $\mathbb{R}$-linearly independent in $K \otimes_\mathbb{Q} \mathbb{R}$. This means that $\mathcal{O}_K$ becomes a *complete $\mathbb{Z}$-lattice* (cf. [12, Ch. I, §4, Definition 4.1]) in $K \otimes_\mathbb{Q} \mathbb{R}$, hence is discrete in $K \otimes_\mathbb{Q} \mathbb{R}$. Thus, $\mathcal{O}_K$ is discrete in $\prod_{v \in V_\infty^K} K_v$, so there exists a neighborhood of zero $\Omega \subset \prod_{v \in V_\infty^K} K_v$ such

that $\mathcal{O}_K \cap \Omega = \{0\}$. Then we consider the following neighborhood of 0 in $\mathbb{A}_K$

$$W = \Omega \times \prod_{v \in V_f^K} \mathcal{O}_v.$$

If $x \in K \cap W$ then $x \in \Omega \cap \mathcal{O}_K$, and hence $x = 0$, proving discreteness. For the proof in the case of an arbitrary global field see [2, Ch. II, §14, Theorem]. □

We will now examine the behavior of the ring of adeles under the base change. Let K be a global field. The canonical embedding $K \hookrightarrow \mathbb{A}_K$ makes $\mathbb{A}_K$ into a K-vector space. For any finite separable extension L/K, we may naturally view $\mathbb{A}_K \otimes_K L$ as an L-vector space. We have the following:

Proposition 1.1.14 *Let L be a finite separable extension of K. There is an isomorphism of topological rings*

$$\mathbb{A}_L \simeq \mathbb{A}_K \otimes_K L$$

that makes the following diagram commutative

$$\begin{array}{ccc} L & \xrightarrow{\simeq} & K \otimes_K L \\ \downarrow & & \downarrow \\ \mathbb{A}_L & \xrightarrow{\simeq} & \mathbb{A}_K \otimes_K L \end{array}$$

where the vertical maps are the natural embeddings.

Proof. Here we only briefly sketch the proof and for more details we refer the reader to [2, Ch. II, §14, Lemma]. The tensor product $\mathbb{A}_K \otimes_K L$ is isomorphic to the restricted product $\prod'_{v \in V^K}(K_v \otimes_K L, \mathcal{O}_v \otimes_{\mathcal{O}_K} \mathcal{O}_L)$. Explicitly, each element of $\mathbb{A}_K \otimes_K L$ is a finite sum of elements of the form $(a_v)_v \otimes x$, where $(a_v)_v \in \mathbb{A}_K$ and

$x \in L$ and the required isomorphism is given by:

$$\mathbb{A}_K \otimes_K L \to \prod_{v \in V^K}{}' (K_v \otimes_K L, \mathcal{O}_v \otimes_{\mathcal{O}_K} \mathcal{O}_L)$$

$$(a_v)_v \otimes x \mapsto (a_v \otimes x)_v.$$

On the other hand, we have $\mathbb{A}_L = \prod_{w \in V^L}{}' (L_w, \mathcal{O}_w)$. Since $K_v \otimes_K L \simeq \prod_{w \mid v} L_w$ and $\mathcal{O}_v \otimes_{\mathcal{O}_K} \mathcal{O}_L \simeq \prod_{w \mid v} \mathcal{O}_w$ (cf. [12, Ch. II, §8, Proposition 8.3] and [12, Ch. II, §8, Exercise 4]), we obtain the isomorphism of topological rings:

$$\mathbb{A}_K \otimes_K L \simeq \prod_{v \in V^K}{}' (K_v \otimes_K L, \mathcal{O}_v \otimes_{\mathcal{O}_K} \mathcal{O}_L) \simeq \prod_{w \in V^L} (L_w, \mathcal{O}_w) \simeq \mathbb{A}_L.$$

Observe that the image of $x \in L$ in $\mathbb{A}_K \otimes_K L$ via the canonical embedding of L into $\mathbb{A}_K \otimes_K L$ is $1 \otimes x = (1, 1, 1, ...) \otimes x$, whose image $(x, x, ...) \in \mathbb{A}_L$ is equal to the image of $x \in L$ under the canonical embedding of L to its adele ring $\mathbb{A}_L$. □

The formulation of strong approximation requires the following truncated version of the ring of adeles

Definition 1.1.15 Let K be a global field and let $S \subset V^K$ be a nonempty subset. Then we define the *ring of S-adeles* $\mathbb{A}_K(S)$ as the restricted product

$$\mathbb{A}_K(S) = \prod_{v \in V^K \setminus S}{}' (K_v, \mathcal{O}_v).$$

Alternatively, one can define $\mathbb{A}_K(S)$ as the projection of $\mathbb{A}_K$ onto $\prod_{v \in V^K \setminus S} K_v$. By definition, any basic open set in $\mathbb{A}_K(S)$ is of the form

$$\prod_{v \in S'} W_v \times \prod_{v \in V^K \setminus (S \cup S')} \mathcal{O}_v,$$

where $S' \subset V^K \setminus S$ is a finite subset and $W_v \subset K_v$ is an open subset for each $v \in S'$. The topology defined in this way will be referred to as *S-adelic topology*. We have the induced diagonal embedding $K \hookrightarrow \mathbb{A}_K(S)$ and one may ask if its image is dense in $\mathbb{A}_K(S)$ considered with the S-adelic topology. Observe that if S was the empty set, then $\mathbb{A}_K(S)$ equals the (full) ring of adeles $\mathbb{A}_K$, but the diagonal embedding $K \hookrightarrow \mathbb{A}_K$ has the image which is discrete and closed (cf. Lemma 1.1.13) so it cannot be dense. However, as we will see, the situation changes completely if S is nonempty. If the canonical embedding $K \hookrightarrow \mathbb{A}_K(S)$ has dense image, we say that K satisfies *strong approximation property* with respect to set S (the reader may also want to compare this with Definition 2.1.6). It turns out that this property holds for any global field as long as S is nonempty:

Theorem 1.1.16 (Strong approximation theorem) *Let K be a global field and let $S \subset V^K$ be any nonempty subset. Then K satisfies strong approximation with respect to S. In other words, the diagonal embedding $K \hookrightarrow \mathbb{A}_K(S)$ has dense image.*

Before proceeding with the proof, let us make a few remarks about the statement of the theorem. For any finite S we have $\mathbb{A}_K = \mathbb{A}_K(S) \times \prod_{v \in S} K_v$. Written out in terms of any basic open set, strong approximation is equivalent to the following. Given any finite subset $S' \subset V^K$ disjoint from S with elements $x_v \in K_v$ for each $v \in S'$, and $\varepsilon > 0$, there exists $x \in K$ such that $|x - x_v| < \varepsilon$ for all $v \in S'$ and $x \in \mathcal{O}_v$ for all $v \in V^K \setminus (S \cup S')$. Therefore, weak approximation follows from strong approximation by forgetting the S-components and weakly approximating x_v for each $v \in S'$. For weak approximation, we only require a finite number of conditions to hold with no control of the valuations $v \in V^K \setminus S$. By contrast, in strong approximation, we have specified conditions at all $v \in V^K \setminus S$: approximation for $v \in S'$ together the integrality for the valuations in $V^K \setminus (S \cup S')$.

Proof of Theorem 1.1.16. We will only sketch the proof of Theorem 1.1.16 in the case $S = V_\infty^K$, where the result follows from the Chinese Remainder Theorem. In particular, this shows that strong approximation has arithmetic nature. The reader may want to see [2, Ch. II, §15, Theorem] for the proof of strong approximation theorem in the general case.

First, let us show that the image of the embedding $\mathcal{O}_K \hookrightarrow \prod_{v \in V_f^K} \mathcal{O}_v$ is dense. We need to show that for any finite subset $S' \subset V_f^K$ and any nonempty open sets $W_v \subset \mathcal{O}_v$ for $v \in S'$, the open set

$$\prod_{v \in S'} W_v \times \prod_{v \in V_f^K \setminus S'} \mathcal{O}_v$$

intersects $\mathcal{O}_K$. Without loss of generality, we may assume that each W_v is an open ball, namely it is of the form

$$W_v = \left\{ x \in \mathcal{O}_v \,|\, x \equiv a_v (\mathrm{mod}\, \mathfrak{p}_v^{d_v}) \right\}$$

for some $a_v \in \mathcal{O}_v$ and some integer $d_v \geq 1$. Then what we need to show is that there exists $a \in \mathcal{O}_K$ satisfying

$$a \equiv a_v (\mathrm{mod}\, \mathfrak{p}_v^{d_v}) \text{ for all } v \in S'.$$

Since $\mathcal{O}_K$ is dense in $\mathcal{O}_v$, we can assume that $a_v \in \mathcal{O}_K$, and then the existence of such a follows from the Chinese Remainder Theorem. Now, given any $a \in \mathbb{A}_K(S)$, one can find nonzero $\alpha \in \mathcal{O}_K$ such that $\alpha a \in \prod_{v \in S'} \mathcal{O}_v$. This means that αa belongs to the closure of $\mathcal{O}_K$. Then a belongs to the closure of $\frac{1}{\alpha}\mathcal{O}_K$, and in particular to the closure of K. Thus, K is dense in $\mathbb{A}_K(S)$. □

Corollary 1.1.17 *We have* $\mathbb{A}_K = \mathbb{A}_{K,\infty} + K$.

Proof. Indeed, let $S = V_\infty^K$ and $a \in \mathbb{A}_K(S)$. Then $a + \prod_{v \in V_f^K} \mathcal{O}_v$ is an open subset of $\mathbb{A}_K(S)$, so by Theorem 1.1.16 it must intersect K. Thus, $\mathbb{A}_K(S) = \prod_{v \in V_f^K} \mathcal{O}_v + K$. Taking pullbacks we obtain our claim. □

Proposition 1.1.18 *The quotient $\mathbb{A}_K/K$ is compact.*

Proof. As we saw earlier, $\mathcal{O}_K$ is a complete lattice in $\prod_{v \in V_\infty^K} K_v \simeq K \otimes_{\mathbb{Q}} \mathbb{R}$, so there exists a compact subset $\Omega \subset \prod_{v \in V_\infty^K} K_v$ such that $\prod_{v \in V_\infty^K} K_v = \Omega + \mathcal{O}_K$. Then

$$\mathbb{A}_K = \mathbb{A}_{K,\infty} + K = \Big(\prod_{v \in V_\infty^K} K_v \times \prod_{v \in V_f^K} \mathcal{O}_v \Big) + K = \Big(\Omega \times \prod_{v \in V_f^K} \mathcal{O}_v \Big) + K.$$

Since $\Omega \times \prod_{v \in V_f^K} \mathcal{O}_v$ is compact, our claim follows. □

1.1.3 The group of ideles

We shall now examine the group of units of $\mathbb{A}_K$, called the group of ideles

Definition 1.1.19 We define the *group of ideles* $\mathbb{I}_K$ of K as the restricted product

$$\mathbb{I}_K = \prod_{v \in V^K}{}' (K_v^\times, \mathcal{O}_v^\times).$$

For almost all $v \in V_f^K$, the groups $\mathcal{O}_v^\times$ are compact, so Proposition 1.1.10 implies that $\mathbb{I}_K$ is a locally compact topological group. By definition, $\mathbb{I}_K$ has a basis of open sets of the form

$$\prod_{v \in S'} W_v \times \prod_{v \in V^K \setminus S'} \mathcal{O}_v^\times,$$

where $S' \subset V^K$ is a finite subset and $W_v \subset K_v^\times$ is an open subset for each $v \in S'$. The restricted product topology on $\mathbb{I}_K$ will be called *idelic topology*. An important

example of an open subgroup of $\mathbb{I}_K$ is the *group of integral ideles* $\mathbb{I}_{K,\infty}$ defined by

$$\mathbb{I}_{K,\infty} = \prod_{v \in V_\infty^K} K_v^\times \times \prod_{v \in V_f^K} \mathcal{O}_v^\times.$$

Note that the restricted product topology on $\mathbb{I}_{K,\infty}$ coincides with the usual product topology. Observe that algebraically, $\mathbb{I}_K$ coincides with $\mathbb{A}_K^\times$ but the topology on $\mathbb{I}_K$ is not the topology induced from $\mathbb{A}_K$. In fact, the subspace topology does not make $\mathbb{I}_K$ into a topological group. We illustrate this in the following example

Example 1.1.20 Let $K = \mathbb{Q}$ and let us consider the sequence $x(p) = (x(p)_q)_{q \in \mathbb{P} \cup \{\infty\}}$ in $\mathbb{A}_\mathbb{Q}$ defined by

$$x(p)_q = \begin{cases} 1 & \text{if } q \neq p \\ p & \text{if } q = p. \end{cases}$$

Clearly, $x(p) \in \mathbb{I}_\mathbb{Q}$ for all p, and $x(p) \to 1$ in $\mathbb{A}_\mathbb{Q}$. On the other hand, $x(p)^{-1}$ does not converge to 1 in $\mathbb{A}_\mathbb{Q}$, because given the open neighborhood

$$W = \mathbb{R} \times \prod_{q \in \mathbb{P}} \mathbb{Z}_q$$

of 1 in $\mathbb{A}_\mathbb{Q}$, all terms of the sequence $x(p)^{-1}$ lie outside of W. This means that the inversion map $x \mapsto x^{-1}$ is not continuous in the induced topology.

As we saw in the proof of Lemma 1.1.12, we have the diagonal embedding $K^\times \hookrightarrow \mathbb{I}_K$. Since the topology on $\mathbb{I}_K$ is stronger than the topology induced from $\mathbb{A}_K$ and K is discrete in $\mathbb{A}_K$, we deduce that $K^\times$ is a discrete subgroup of $\mathbb{I}_K$ and we call it the group of *principal ideles*. Any element of this subgroup (called the *principal idele*) corresponds to some $a \in K^\times$ and will be denoted by (a) or simply by a.

In contrast to the case of adeles where the quotient $\mathbb{A}_K/K$ is compact, the analogous quotient $\mathbb{I}_K/K^\times$ is noncompact. The group $\mathbb{I}_K/K^\times$ will be denoted by

C_K and called the *idele class group* of K.

Let us sketch the proof of noncompactess of C_K for $K = \mathbb{Q}$. Recall that we denote by $|\cdot|_\infty$ the usual (archimedean) absolute value on $\mathbb{Q}$, and for every rational prime p, we write $|\cdot|_p$ for the p-adic absolute value on $\mathbb{Q}$, defined by $|x|_p = p^{-v_p(x)}$ where $v_p(x) = r$ if $x = p^r \cdot a/b$ and $p \nmid a \cdot b$. Consider the continuous homomorphism $\nu\colon \mathbb{I}_\mathbb{Q} \to \mathbb{R}_{>0}$ given by $\nu((x_p)_p) = \prod_{p \leq \infty} |x_p|_p$. First, observe that ν is well-defined since for almost all primes p, we have $|x_p|_p \leq 1$. For any $x \in \mathbb{Q}^\times$ the following *product formula* holds

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} |x|_p = 1,$$

(cf. [12, Ch. II, §2, Proposition 2.1]) so ν factors through $\mathbb{Q}^\times$ and induces the homomorphism $\tilde{\nu}\colon \mathbb{I}_\mathbb{Q}/\mathbb{Q}^\times \to \mathbb{R}_{>0}$. Since $\tilde{\nu}$ is surjective and $\mathbb{R}_{>0}$ is not compact, we have that $\tilde{\nu}(\mathbb{I}_\mathbb{Q}/\mathbb{Q}^\times)$ is not compact and therefore $\mathbb{I}_\mathbb{Q}/\mathbb{Q}^\times$ is not compact either. For arbitrary global field K, one can also consider *normalized valuations* (cf. [2, Ch. II, §7, Definition]) and the homomorphism

$$\nu\colon \mathbb{I}_K \to \mathbb{R}_{>0} \tag{1.1}$$

$$(x_v)_v \mapsto \prod_{v \in V^K} |x_v|_v,$$

to prove that $\mathbb{I}_K/K^\times$ is not compact (cf. [2, Ch. II, §12, Theorem]).

Let K be a global field. We define the *group of ideles of K with content one*, $\mathbb{I}_K^{(1)}$ as the kernel of the map ν in (1.1). It follows from the product formula that $\mathbb{I}_K^{(1)}$ contains $K^\times$. The main result of reduction theory for the group of ideles, which is important for class field theory, is the following

Theorem 1.1.21 *Let K be a global field. The quotient $\mathbb{I}_K^{(1)}/K^\times$ is compact.*

Proof. Cf. [2, Ch. II, §16, Theorem]. □

One can derive from Theorem 1.1.21, the Dirichlet's Unit Theorem (see Theorem 1.1.2) and the finiteness of the class number (see Theorem 1.1.1). For the proof of Dirichlet's Unit Theorem relying on the compactness of $\mathbb{I}_K^{(1)}/K^\times$, we refer the reader to [2, Ch. II, §18, Theorem]. Here we will see how compactness of $\mathbb{I}_K^{(1)}/K^\times$ implies the finiteness of the class number. We need the following lemma

Lemma 1.1.22 *Let K be a global field. The class group $\mathrm{Cl}(K)$ is isomorphic to the quotient $\mathbb{I}_K/K^\times\mathbb{I}_{K,\infty}$.*

Proof. Recall that we denote by $\mathcal{I}_K$ the group of all fractional ideals of K. For any $v \in V_f^K$, we denote the prime ideal $\mathfrak{p}_v \cap \mathcal{O}_K$ by $\mathfrak{p}(v)$. There is a group homomorphism

$$\rho_K \colon \mathbb{I}_K \to \mathcal{I}_K$$

$$(x_v)_v \mapsto \prod_{v \in V_f^K} \mathfrak{p}(v)^{v(x_v)},$$

where $\mathfrak{p}_v$ denotes the valuation ideal in the valuation ring $\mathcal{O}_v$. According to the definition of the group of ideles, we have $v(x_v) = 0$ for almost all $v \in V_f^K$, so that the product is actually finite and the map ρ_K is well-defined. Since any fractional ideal decomposes uniquely as the product of powers of prime ideals we see that ρ_K is surjective. Observe that $\ker \rho_K$ coincides with $\mathbb{I}_{K,\infty}$. On the other hand, $\rho_K(K^\times)$ equals the subgroup of principal fractional ideals $\mathcal{P}_K$. Thus, ρ_K induces the claimed isomorphism

$$\mathbb{I}_K/K^\times\mathbb{I}_{K,\infty} \simeq \mathcal{I}_K/\mathcal{P}_K = \mathrm{Cl}(K).$$

□

Proof of Theorem 1.1.1. The subgroup $\mathbb{I}_{K,\infty} \subset \mathbb{I}_K$ is open, so the product $K^\times\mathbb{I}_{K,\infty}$ is also an open subgroup of $\mathbb{I}_K$. Thus, the quotient $\mathbb{I}_K/K^\times\mathbb{I}_{K,\infty}$ is a discrete group.

On the other hand, for ν as in (1.1), we have $\nu(\prod_{v\in V_\infty^K} K_v^\times) = \mathbb{R}_{>0}$ implying that $\mathbb{I}_K = \mathbb{I}_K^{(1)}\mathbb{I}_{K,\infty}$. This means that the canonical homomorphism $\mathbb{I}_K^{(1)}/K^\times \to \mathbb{I}_K/K^\times\mathbb{I}_{K,\infty}$ is surjective. Since $\mathbb{I}_K^{(1)}/K^\times$ is compact by Theorem 1.1.21, we conclude that $\mathbb{I}_K/K^\times\mathbb{I}_{K,\infty}$ is compact. But a topological group which is simultaneously discrete and compact must be finite. □

Remark 1.1.23 Conversely, assuming the finiteness of the class number and Dirichlet's Unit Theorem one can derive the compactness of $\mathbb{I}_K^{(1)}/K^\times$. Let us first show this for $K = \mathbb{Q}$. Since the class number of $\mathbb{Q}$ is one, we have $\mathbb{I}_\mathbb{Q} = \mathbb{Q}^\times\mathbb{I}_{\mathbb{Q},\infty}$. Since $\mathbb{Q}^\times \subset \mathbb{I}_\mathbb{Q}^{(1)}$, we deduce that

$$\mathbb{I}_\mathbb{Q}^{(1)} = \mathbb{Q}^\times(\mathbb{I}_{\mathbb{Q},\infty} \cap \mathbb{I}_\mathbb{Q}^{(1)}).$$

On the other hand, we have $|x|_p = 1$ for any $x \in \mathbb{Z}_p^\times$, so

$$\mathbb{I}_{\mathbb{Q},\infty} \cap \mathbb{I}_\mathbb{Q}^{(1)} = \{\pm 1\} \times \prod_{p\in\mathbb{P}} \mathbb{Z}_p^\times,$$

which is compact, and therefore $\mathbb{I}_\mathbb{Q}^{(1)}/\mathbb{Q}^\times$ is also compact.

Now let K be an arbitrary global field. Since the quotient $\mathbb{I}_K/K^\times\mathbb{I}_{K,\infty} \simeq \mathrm{Cl}(K)$ is finite, it is enough to prove the compactness of

$$(\mathbb{I}_K^{(1)} \cap K^\times\mathbb{I}_{K,\infty})/K^\times \simeq (\mathbb{I}_K^{(1)} \cap \mathbb{I}_{K,\infty})/(K^\times \cap \mathbb{I}_{K,\infty}).$$

It is easy to see that $\mathbb{I}_{K,\infty} \cap K^\times = \mathcal{O}_K^\times$. Furthermore, since $|x|_v = 1$ for any $x \in \mathcal{O}_v^\times$, we deduce that

$$\mathbb{I}_K^{(1)} \cap \mathbb{I}_{K,\infty} = \left(\prod_{v\in V_\infty^K} K_v^\times \cap \mathbb{I}_K^{(1)}\right) \times \left(\prod_{v\in V_f^K} \mathcal{O}_v^\times\right),$$

and therefore

$$(\mathbb{I}_K^{(1)} \cap \mathbb{I}_{K,\infty})/(K^\times \cap \mathbb{I}_{K,\infty}) \simeq \frac{\left(\prod_{v\in V_\infty^K} K_v^\times\right) \cap \mathbb{I}_K^{(1)}}{\mathcal{O}_K^\times} \times \prod_{v\in V_f^K} \mathcal{O}_v^\times.$$

Thus, the compactness of this quotient is equivalent to the compactness of $\left(\prod_{v\in V_\infty^K} K_v^\times \cap \mathbb{I}_K^{(1)}\right)/\mathcal{O}_K^\times$, which is equivalent to the Dirichlet's Unit Theorem (cf. [2, Ch. II, §18, Theorem]).

Our next goal is to extend the field norm to the group of ideles. Let L/K be a finite extension of global fields. As we saw earlier, for a fixed $v \in V^K$, we have $L \otimes_K K_v \simeq \prod_{w|v} L_w$, which results in the following formula for the norm

$$N_{L/K}(x) = \prod_{w|v} N_{L_w/K_v}(x) \tag{1.2}$$

(cf. [15, Ch. 1, §1.1.2]). This formula supports the following way of extending the norm map $N_{L/K}\colon L \to K$ to a map $N_{L/K}\colon \mathbb{A}_L \to \mathbb{A}_K$. Namely, given $x = (x_w)_{w\in V^L} \in \mathbb{A}_L$, we define

$$N_{L/K}(x) = \Big(\prod_{w|v} N_{L_w/K_v}(x_w)\Big)_{v\in V^K}.$$

It is easy to see that $N_{L/K}(\mathbb{A}_L) \subset \mathbb{A}_K$. It also follows from (1.2) that the map $N_{L/K}$ takes principal adeles in $\mathbb{A}_L$ to principal adeles in $\mathbb{A}_K$, and in fact coincides on principal adeles with the usual norm map. Since norm of a unit is a unit, we see that $N_{L/K}(\mathbb{I}_L) \subset \mathbb{I}_K$. Consequently, $N_{L/K}$ induces a map on idele class groups $N_{L/K}\colon C_L \to C_K$.

Similarly to the case of adeles one can define truncated ideles and these will be more relevant for us later

Definition 1.1.24 Let K be a global field and let $S \subset V^K$ be a subset. We define the *group of S-ideles* $\mathbb{I}_K(S)$ as the restricted product

$$\mathbb{I}_K(S) = \prod_{v \in V^K \setminus S}{}' (K_v^\times, \mathcal{O}_v^\times).$$

It follows from the definition that any basic open set in $\mathbb{I}_K(S)$ is of the form

$$\prod_{v \in S'} W_v \times \prod_{v \in V^K \setminus (S \cup S')} \mathcal{O}_v^\times,$$

where $S' \subset V^K \setminus S$ is a finite subset and $W_v \subset K_v^\times$ is open for each $v \in S'$. The restricted product topology on $\mathbb{I}_K(S)$ will be called *S-idelic topology*. We have the induced diagonal embedding $K^\times \hookrightarrow \mathbb{I}_K(S)$ and one may ask whether it has dense image. This question will be studied in greater detail in section 1.3.

1.2 Class field theory

1.2.1 Statements of key results from class field theory

In this section we state two fundamental results of global class field theory – the fundamental isomorphism of class field theory and the existence theorem. Let K be a global field and let L/K be a finite (not necessarily abelian) Galois extension with Galois group $G = \mathrm{Gal}(L/K)$.

Theorem 1.2.1 (Fundamental Isomorphism of class field theory) *There is a natural isomorphism*

$$\psi_{L/K} \colon \mathbb{I}_K / K^\times N_{L/K}(\mathbb{I}_L) \longrightarrow G^{\mathrm{ab}},$$

where G^{ab} denotes the abelianization $G/[G,G]$ of G.

Proof. Cf. [2, Ch. VII, §5.1, Theorem (B)], [2, Ch. VII, §5.4] and [2, Ch. VII, §11.3, p.197]. □

The isomorphism $\psi_{L/K}$ is called the *Artin map* and some indications on how to construct it will be given in section 1.2.2. Observe that if L/K is *abelian*, then $\psi_{L/K}$ implements an isomorphism between $\mathbb{I}_K/K^\times N_{L/K}(\mathbb{I}_L)$ and G. The naturality of the isomorphism $\psi_{L/K}$ means that it behaves well with respect to towers of extensions. More precisely, if $K \subset L \subset M$ is a tower of abelian extensions, then the following diagram commutes

$$\begin{array}{ccc} \mathbb{I}_K/K^\times N_{M/K}(\mathbb{I}_M) & \xrightarrow{\psi_{M/K}} & \mathrm{Gal}(M/K) \\ \downarrow{\scriptstyle i_{ML}} & & \downarrow{\scriptstyle j_{ML}} \\ \mathbb{I}_K/K^\times N_{L/K}(\mathbb{I}_L) & \xrightarrow{\psi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

where i_{ML} is the canonical quotient map that exists due to the inclusion $N_{M/K}(\mathbb{I}_M) \subset N_{L/K}(\mathbb{I}_L)$, and j_{ML} is the canonical quotient map from Galois theory given by restriction of automorphisms (cf. [2, Ch. VII, §5, Theorem 5.1(C)]).

Observe that for any finite Galois extension L/K we have $\mathbb{I}_K/K^\times N_{L/K}(\mathbb{I}_L) = C_K/N_{L/K}(C_L)$. A subgroup $D \subset C_K$ is called a *norm subgroup* if there exists a finite abelian extension L/K such that $D = N_{L/K}(C_L)$. It follows from Theorem 1.2.1 that every norm subgroup is of finite index. Furthermore, for every $v \in V^K$ and $w|v$ we have that the norm subgroup $N_{L_w/K_v}(L_w^\times) \subset K_v^\times$ is open. Moreover, almost all $v \in V_f^K$ are unramified in L, and then $N_{L_w/K_v}(\mathcal{O}_w^\times) = \mathcal{O}_v^\times$ (cf. [32, Ch. V, §2, Proposition 3]). It follows that $N_{L/K}(\mathbb{I}_L) \subset \mathbb{I}_K$ is open and consequently $N_{L/K}(C_L) \subset C_K$ is open. Conversely, we have the following:

Theorem 1.2.2 (Existence Theorem) *Every open subgroup $N \subset C_K$ of finite*

index is a norm subgroup. In fact, there exists a unique abelian extension L/K such that $N_{L/K}(C_L) = N$.

Proof. Cf. [2, Ch. VII, §5, Theorem 5.1(D)]. □

These results of class field theory imply that the assignment $L \mapsto N_{L/K}(C_L)$ yields an inclusion reversing correspondence between all abelian extensions of K and all finite index open subgroups of C_K.

1.2.2 Construction of the Artin map via the reciprocity law

While the construction of the Artin map can be done for any finite Galois extension, here we are mainly interested in the case of finite abelian extensions. In section 1.2.3 we will specify further to quadratic extensions and provide an alternative description of the Artin map in this case, using the Hilbert symbol. The main tool we need for the construction of the Artin map in the general case, is the Artin reciprocity law (see Theorem 1.2.3). Let K be a global field and let L/K be a finite Galois extension with $G = \mathrm{Gal}(L/K)$. If $v \in V_f^K$ and w is some extension of v to L, we denote the corresponding *Frobenius automorphism* by $\mathrm{Fr}_{L/K}(w|v)$ or simply by $\mathrm{Fr}(w|v)$ if the underlying field extension L/K is clear from the context. If we consider a different extension $w'|v$, then $\mathrm{Fr}(w|v)$ and $\mathrm{Fr}(w'|v)$ are conjugate in $G = \mathrm{Gal}(L/K)$. Furthermore, if L/K is abelian, we have that $\mathrm{Fr}(w|v) = \mathrm{Fr}(w'|v)$, in which case the Frobenius automorphism $\mathrm{Fr}(w|v)$ is independent of the choice of the extension $w|v$, and therefore will be denoted simply by $\mathrm{Fr}(v)$. For the construction and a more detailed study of the Frobenius automorphism, we refer the reader to [2, Ch. VII, §2].

Let L be a finite abelian extension of a global field K with Galois group $G = \mathrm{Gal}(L/K)$. Recall that for any $v \in V_f^K$, we denote by $\mathfrak{p}(v)$, the prime ideal $\mathfrak{p}_v \cap \mathcal{O}_K$. Fix a finite subset $S \subset V^K$ that contains V_∞^K and also all $v \in V_f^K$ that are ramified

in L (the set of $v \in V_f^K$ that ramify in L is always finite – see [2, Ch. I, §5, Corollary 2]). Let $\mathcal{I}_K^S$ be the subgroup of the group of fractional ideals $\mathcal{I}_K$ generated by the prime ideals $\mathfrak{p}(v)$ for $v \in V^K \setminus S$. Note that $\mathcal{I}_K^S$ is a free abelian group on this set. We can then define the following map

$$\phi_{L/K}^S \colon \mathcal{I}_K^S \to G$$

$$\mathfrak{p}(v) \mapsto \mathrm{Fr}(v).$$

For any $\sigma \in G$ there exist infinitely many $v \in V^K \setminus S$ such that $\phi_{L/K}^S(\mathfrak{p}(v)) = \sigma$, so the homomorphism $\phi_{L/K}^S \colon \mathcal{I}_K^S \to G$ is surjective. There is a natural continuous homomorphism

$$\rho_K^S \colon \mathbb{I}_K(S) \to \mathcal{I}_K^S$$

$$(x_v)_v \mapsto \prod_{v \in V^K \setminus S} \mathfrak{p}(v)^{v(x_v)}.$$

Setting $\psi_{L/K}^S := \phi_{L/K}^S \circ \rho_K^S$, we obtain a continuous homomorphism $\psi_{L/K}^S \colon \mathbb{I}_K(S) \to G$. Our goal is to extend it to a continuous homomorphism $\psi_{L/K} \colon \mathbb{I}_K \to G$. The extension procedure relies on the reciprocity law, and in fact, if one assumes the latter, then the extension can be shown to be unique. We will see several formulations of the reciprocity law, but all of them have to do with the values of $\psi_{L/K}^S$ on certain principal ideles.

Theorem 1.2.3 (Reciprocity Law) *Let L/K be a finite abelian extension of global fields and let $S \subset V^K$ be a finite subset containing V_∞^K and all $v \in V_f^K$ that ramify in L. Then there exists $\varepsilon > 0$ such that if $a \in K^\times$ and $|a - 1|_v < \varepsilon$ for all $v \in S$, then*

$$\psi_{L/K}^S((a)^S) = 1$$

where $(a)^S \in \mathbb{I}_K(S)$ *denotes the principal idele corresponding to* a*.*

Proof. Cf. [2, Chapter VII, §3, 3.3]. □

It is worth mentioning that the Artin reciprocity law implies the classical quadratic reciprocity law (cf. [3, Ch. 5, §3]). For the statement and different proofs of quadratic reciprocity law, we refer the reader to [30, Ch. I, §3.3, Theorem 6] and [28, Ch. VI, §6.5].

We will now assume the reciprocity law and show that the continuous homomorphism $\psi_{L/K}^S \colon \mathbb{I}_K(S) \to G$ can be extended uniquely to a continuous homomorphism $\psi_{L/K} \colon \mathbb{I}_K \to G$ such that $\psi_{L/K}(K^\times) = 1$. We start with the obvious decomposition

$$\mathbb{I}_K = \mathbb{I}_K(S) \times K_S^\times,$$

where $K_S = \prod_{v \in S} K_v$. Given $x \in \mathbb{I}_K$, we will write it as $x = x^S x_S$ with $x^S \in \mathbb{I}_K(S)$ and $x_S \in K_S^\times$. In particular, we will write a principal idele $(a) \in \mathbb{I}_K$ for $a \in K^\times$ as $(a) = (a)^S (a)_S$. We want $\psi_{L/K}((a)) = 1$, so

$$1 = \psi_{L/K}((a)^S (a)_S) = \psi_{L/K}((a)^S)\psi_{L/K}((a)_S),$$

and therefore, we must have

$$\psi_{L/K}((a)_S) = \psi_{L/K}((a)^S)^{-1} = \psi_{L/K}^S((a)^S)^{-1}.$$

On the other hand, by weak approximation theorem $K^\times$ is dense in $K_S^\times$ (cf. Theorem 1.1.8). So, if $\psi_{L/K}$ is continuous, then it is unique. To prove the existence, suppose $x \in K_S^\times$. Then again using weak approximation, we have that there exists a sequence $a_n \in K^\times$ such that $a_n \to x$ in $K_S^\times$. Let $\varepsilon > 0$ be as in the statement of Theorem 1.2.3. Then there exists a positive integer N such that

$|a_m/a_n - 1|_v < \varepsilon$ for all $m, n > N$ and all $v \in S$. Then $\psi^S_{L/K}((a_m/a_n)^S) = 1$, so $\psi^S_{L/K}((a_m)^S) = \psi^S_{L/K}((a_n)^S)$. The inverse of this common value is by definition $\psi_{L/K}(x)$, i.e. $\psi_{L/K}(x) = \psi^S_{L/K}((a_n)^S)^{-1}$ for n sufficiently large, where $a_n \in K^\times$ is any sequence such that $a_n \to x$ in $K^\times_S$. It is not difficult to see that $\psi_{L/K}$ defined this way, gives a continuous homomorphism $K^\times_S \to G$. Indeed, if $a_n \to x$ and $b_n \to y$, then $a_n b_n \to xy$. We can choose N so that for $n > N$ we have

$$\psi_{L/K}(x) = \psi^S_{L/K}((a_n)^S)^{-1}, \quad \psi_{L/K}(y) = \psi^S_{L/K}((b_n)^S)^{-1}$$

and $\psi_{L/K}(xy) = \psi^S_{L/K}((a_n b_n)^S)$. But

$$\psi^S_{L/K}((a_n b_n)^S) = \psi^S_{L/K}((a_n)^S)\psi^S_{L/K}((b_n)^S)$$

for all $n > N$, implying that $\psi_{L/K}(xy) = \psi_{L/K}(x)\psi_{L/K}(y)$. Now it is enough to prove the continuity at 1. In fact, let us consider the following neighborhood of 1 in $K^\times_S$

$$W = \Big\{(x_v)_v \in \prod_{v\in S} K^\times_v \;\Big|\; |x_v - 1|_v < \varepsilon\Big\},$$

where ε is as in Theorem 1.1.8. We claim that $\psi_{L/K}(W) = \{1\}$, which will prove the continuity. If $x \in W$ and a_n is a sequence in $K^\times$ with $a_n \to x$ then $a_n \in K^\times \cap W$ for sufficiently large n, which in view of the reciprocity law yields $\psi^S_{L/K}((a_n)^S) = 1$. On the other hand, we have that $\psi_{L/K}(x) = \psi^S_{L/K}((a_n)^S)^{-1}$ for all sufficiently large n. It follows that $\psi_{L/K}(x) = 1$, as required. Thus, $\psi_{L/K}$ is continuous on $K^\times_S$. Furthermore, $\psi^S_{L/K}$ is continuous on $\mathbb{I}_K(S)$ because it is trivial on $\prod_{v\in V^K\setminus S} \mathcal{O}^\times_v$. Thus, $\psi_{L/K}\colon \mathbb{I}_K \to G$, defined by $\psi_{L/K}(x) = \psi^S_{L/K}(x^S)\psi_{L/K}(x_S)$ is a continuous homomorphism satisfying the following two conditions:

(1) $\psi_{L/K}$ extends $\psi^S_{L/K}$

(2) $\psi_{L/K}(K^\times) = \{1\}$

If we assume the reciprocity law, then such an extension is unique. Furthermore, one can show that $\ker \psi_{L/K}$ is exactly equal to $K^\times N_{L/K}(\mathbb{I}_L)$ (cf. [2, Ch. VII, §5.1, Theeorem (B)]) which together with the construction of $\psi_{L/K}$ yields

Corollary 1.2.4 *Let L/K be a finite abelian extension of global fields. Assume that $v \in V_f^K$ is unramified in L and $K_v^\times \subset K^\times N_{L/K}(\mathbb{I}_L)$, where we routinely identify $K_v^\times$ with its image $\iota_v(K_v^\times)$ via the natural embedding $\iota_v \colon K_v \to \mathbb{I}_K$. Then L splits completely at v, i.e. $L_w = K_v$ for any $w|v$.*

Proof. Our assumption implies that $\psi_{L/K}(\iota_v(K_v^\times)) = \{1\}$. On the other hand, by the construction of $\psi_{L/K}$, we have $\psi_{L/K}(\iota_v(\pi_v)) = \mathrm{Fr}(v)$, for any uniformizer $\pi_v \in K_v^\times$. So, $L_w = K_v$ for any $w|v$. □

1.2.3 The Hilbert symbol and Artin map for quadratic extensions

In this section we introduce the Hilbert symbol together with its basic properties in the case of local and global fields. Hilbert symbol will be used to provide an alternative construction of the Artin map in the case of quadratic extensions. Let $\mathcal{K}$ be a local field.

Definition 1.2.5 For any $a, b \in \mathcal{K}^\times$, we define the *Hilbert symbol* $(a,b)_{\mathcal{K}}$ of a and b, relative to $\mathcal{K}$ by:

$$(a,b)_{\mathcal{K}} = \begin{cases} +1 & \text{if } x^2 - ay^2 - bz^2 = 0 \text{ has a nonzero solution } (x,y,z) \in \mathcal{K}^3, \\ -1 & \text{otherwise} \end{cases}$$

In this section, we will write (a, b) for $(a, b)_{\mathcal{K}}$ when the field $\mathcal{K}$ is clear from the context. From the definition, we see that the Hilbert symbol defines a map $\mathcal{K}^\times/\mathcal{K}^{\times 2} \times \mathcal{K}^\times/\mathcal{K}^{\times 2} \to \{\pm 1\}$. The basic local properties of the Hilbert symbol are given by the following two propositions

Proposition 1.2.6 *Let $a, b \in \mathcal{K}^\times$ and let $\mathcal{L} = \mathcal{K}(\sqrt{b})$. For $(a, b) = 1$ it is necessary and sufficient that $a \in N_{\mathcal{L}/\mathcal{K}}(\mathcal{L}^\times)$.*

Proof. Cf. [30, Ch. III, §1, Proposition 1]. □

Proposition 1.2.7 *The Hilbert symbol satisfies the following formulas:*

(1) $(a, b) = (b, a)$ *and* $(a, c^2) = 1$,

(2) $(a, -a) = 1$ *and* $(a, 1 - a) = 1$,

(3) *If* $(a, b) = 1$ *then* $(aa', b) = (a', b)$,

(4) $(a, b) = (a, -ab) = (a, (1 - a)b)$.

In all these formulas a, a', b, c are arbitrary elements of $\mathcal{K}^\times$ but we assume that $a \neq 1$ whenever the formula contains the term $1 - a$.

Proof. Cf. [30, Ch. III, §1, Proposition 2]. □

Theorem 1.2.8 *The Hilbert symbol is a nondegenerate bilinear form on the $\mathbb{F}_2$-vector space $\mathcal{K}^\times/\mathcal{K}^{\times 2}$.*

Proof. Cf. [30, Ch. III, §1, Theorem 2]. □

In order to construct the Artin map for quadratic extensions we will also need two global properties of the Hilbert symbol, namely the product formula and the existence of rational numbers with given Hilbert symbols. Let K be a global field. For any $v \in V^K$ and any $a, b \in K^\times$, we write $(a, b)_v$ to denote the (local) Hilbert symbol of a and b, considered as elements of the completion K_v.

Theorem 1.2.9 (Product Formula for Hilbert symbol) *For any $a, b \in K^\times$, we have*

$$\prod_{v \in V^K} (a,b)_v = 1.$$

Proof. Cf. [30, Ch. III, §2, Theorem 3]. □

Theorem 1.2.10 *Let $a \in K^\times$, and assume we are given $\varepsilon_v = \pm 1$ for all $v \in V^K$ such that the following three conditions hold:*

(1) *For almost all $v \in V^K$, we have $\varepsilon_v = 1$,*

(2) $\prod_{v \in V^K} \varepsilon_v = 1$,

(3) *For each $v \in V^K$, there exists $x_v \in K_v^\times$ with $(a, x_v)_v = \varepsilon_v$.*

Then there exists $x \in K^\times$ such that $(a,x)_v = \varepsilon_v$ for all v.

Proof. Cf. [30, Ch. III, §2, Theorem 4]. □

We may now provide another description of the Artin map for quadratic extensions, which will be used later in section 1.3.1. Let K be a global field and let $L = K(\sqrt{d})$ with $d \in K^\times \setminus K^{\times 2}$. Define a map

$$\Psi_{L/K} \colon \mathbb{I}_K \to \{\pm 1\}$$

$$(x_v)_v \mapsto \prod_{v \in V^K} (d, x_v)_v.$$

We note that d and x_v are units for almost all v, which implies that $(d, x_v)_v = 1$ for almost all v, so the above product is actually finite and $\Psi_{L/K}$ is well-defined. Moreover, we have the following

Proposition 1.2.11 *$\Psi_{L/K}$ induces an isomorphism $\mathbb{I}_K / K^\times N_{L/K}(\mathbb{I}_L) \simeq \{\pm 1\}$.*

Proof. Since $d \in K^\times \setminus K^{\times 2}$, there exists $v \in V^K$ such that $d \in K_v^\times \setminus K_v^{\times 2}$, and then by the nondegeneracy of $(*,*)_v$, we can find $x_v \in K_v^\times$ with $(d, x_v)_v = -1$. This shows that $\Psi_{L/K}$ is surjective. The product formula for the Hilbert symbol implies that $K^\times \subset \ker \Psi_{L/K}$, so $K^\times N_{L/K}(\mathbb{I}_L) \subset \ker \Psi_{L/K}$. Conversely, suppose $(x_v)_v \in \mathbb{I}_K$ belongs to $\ker \Psi_{L/K}$. Set $\varepsilon_v = (d, x_v)_v$ for $v \in V^K$. These numbers satisfy all the assumptions of Theorem 1.2.10, so there exists $x \in K^\times$ such that

$$(d, x)_v = \varepsilon_v = (d, x_v)_v$$

for all $v \in V^K$. Since the Hilbert symbol is bilinear we have that

$$(d, x^{-1}x_v)_v = (d, x^{-1})_v (d, x_v)_v = (d, x^2 x^{-1})_v (d, x_v)_v = (d, x)_v (d, x_v)_v = \varepsilon_v^2 = 1.$$

By Proposition 1.2.6 we have that $x^{-1}x_v \in N_{L_w/K_v}(L_w^\times)$ where $w|v$. Moreover, $x^{-1}x_v \in \mathcal{O}_v^\times$ for almost all v, and then $x^{-1}x_v \in N_{L_w/K_v}(\mathcal{O}_w)$. Thus, $x^{-1}(x_v)_v \in N_{L/K}(\mathbb{I}_L)$, and $(x_v)_v \in K^\times N_{L/K}(\mathbb{I}_L)$ as claimed. □

1.2.4 (Generalized) arithmetic progressions and density theorems

In this section, we discuss two important density theorems: Dirichlet Prime Number theorem on primes in arithmetic progression and its generalization to arbitrary global fields due to Chebotarev, known as Chebotarev Density theorem. Recall that we denote by $\mathbb{P}$ the set of all rational primes. For any two relatively prime positive integers m and a we denote by $\mathbb{P}_{a(m)}$ the set of all rational primes p such that $p \equiv a (\mathrm{mod}\, m)$, namely $\mathbb{P}_{a(m)}$ consists of primes in *arithmetic progression*. Dirichlet showed that the set $\mathbb{P}_{a(m)}$ is infinite by using the following notion of density

Definition 1.2.12 Let $\mathcal{P} \subset \mathbb{P}$ be an arbitrary subset. The *Dirichlet density* of $\mathcal{P}$ is defined as the following limit (if it exists)

$$\mathfrak{d}(\mathcal{P}) = \lim_{s \to 1^+} \frac{\sum_{p \in \mathcal{P}} p^{-s}}{\sum_{p \in \mathbb{P}} p^{-s}}.$$

It is known that for any $s > 1$ the series $\sum_{p \in \mathbb{P}} p^{-s}$ converges and that $\sum_{p \in \mathbb{P}} p^{-s} \to \infty$ when $s \to 1^+$ (cf. [30, Ch. VI, §3.2, Corollary 1] and [30, Ch. VI, §3.2, Corollary 2]). Consequently, every finite set of primes has density zero. Dirichlet established the precise value of density of $\mathbb{P}_{a(m)}$

Theorem 1.2.13 (Dirichlet Prime Number Theorem) *Let a and m be two positive relatively prime integers. Then*

$$\mathfrak{d}(\mathbb{P}_{a(m)}) = \frac{1}{\varphi(m)}$$

where φ denotes the Euler totient function. In particular, the set $\mathbb{P}_{a(m)}$ is infinite.

Proof. Cf. [30, Ch. VI, §4.1, Theorem 2]. □

However, it should be noted that one can construct many examples of infinite sets with zero Dirichlet density. In fact, let Ω be any set of primes $p_1 < p_2 < \dots$ such that $\sum_{i=1}^{\infty} p_i^{-1} < \infty$. For example, one may take p_i such that $p_i > 2^i$ for each $i \geq 1$ so that $\sum_{i=1}^{\infty} p_i^{-1} < \sum_{i=1}^{\infty} 2^{-i} = 1 < \infty$. Then we have

$$\mathfrak{d}(\Omega) = \lim_{s \to 1^+} \frac{\sum_{p_i \in \Omega} p_i^{-s}}{\sum_{p \in \mathbb{P}} p^{-s}} = 0.$$

Chebotarev proved a vast generalization of Theorem 1.2.13, which applies to arbitrary global fields; however the statement requires a more general notion of density, which will also be referred to as Dirichlet density

Definition 1.2.14 Let K be a global field and let $\mathcal{P} \subset V_f^K$ be a subset. The *Dirichlet Density* of $\mathcal{P}$ is defined to be the following limit (if it exists)

$$\mathfrak{d}_K(\mathcal{P}) = \lim_{s \to 1^+} \frac{\sum\limits_{v \in \mathcal{P}} \mathcal{N}(\mathfrak{p}_v)^{-s}}{\sum\limits_{v \in V_f^K} \mathcal{N}(\mathfrak{p}_v)^{-s}},$$

where $\mathcal{N}(\mathfrak{p}_v)$ denotes the norm of the ideal $\mathfrak{p}_v$, i.e. the cardinality of the residue field $k(v) = \mathcal{O}_v/\mathfrak{p}_v$.

It is clear that the notion of density in Definition 1.2.14 generalizes the one in Definition 1.2.12. One can show the following two facts (cf. [12, Ch. VII, §13]):

(1) The series $\sum_{v \in V_f^K} \mathcal{N}(\mathfrak{p}_v)^{-s}$ (hence also the series $\sum_{v \in \mathcal{P}} \mathcal{N}(\mathfrak{p}_v)^{-s}$ for any subset $\mathcal{P} \subset V_f^K$) converges for $s > 1$,

(2) We have $\sum_{v \in V_f^K} \mathcal{N}(\mathfrak{p}_v)^{-s} \xrightarrow{s \to 1^+} \infty$, and consequently every finite set has Dirichlet density 0.

It should be noted that for arbitrary global fields one can also construct infinite sets with zero Dirichlet density zero. A very well-known example of such a set is the set of all primes of any number field K which have relative degree ≥ 2 (cf. [12, Ch. VII, §13]). For example, let $K = \mathbb{Q}(i)$ and consider the set

$$\Omega = \left\{ w \in V_f^K \;\middle|\; w|v_p \text{ with } p \text{ prime such that } p \equiv 3 (\mathrm{mod}\, 4) \right\}.$$

For any prime p such that $p \equiv 3 (\mathrm{mod} 4)$ there exists a unique valuation $w \in V_f^K$ such that $w|v_p$. Then $f(w|v_p) = 2$ and if we denote by $\mathfrak{p}$ the ideal of $\mathcal{O}_K$ corresponding to w then $\mathcal{N}(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = p^2$. Thus, for $s \geq 1$, we have

$$\sum_{\mathfrak{p} \in \Omega} \mathcal{N}(\mathfrak{p})^{-s} = \sum_{p \equiv 3 (\mathrm{mod}\, 4)} p^{-2s} \leq \sum_{n \geq 1} n^{-2s} < \infty.$$

Hence $\mathfrak{d}_K(\Omega) = 0$.

Theorem 1.2.15 (Chebotarev Density Theorem) *Let K be a global field and let L/K be a finite Galois extension with $G = \mathrm{Gal}(L/K)$. Fix a conjugacy class $\mathcal{C}$ in G. Let $\mathcal{P}(L/K, \mathcal{C})$ be the set of all $v \in V_f^K$ such that v is unramified in L and for some (equivalently, any) extension $w|v$ the Frobenius automorphism $\mathrm{Fr}_{L/K}(w|v)$ lies in $\mathcal{C}$. Then*

$$\mathfrak{d}_K(\mathcal{P}(L/K, \mathcal{C})) = \frac{|\mathcal{C}|}{|G|}.$$

In particular, $\mathcal{P}(L/K, \mathcal{C})$ is an infinite set.

Proof. Cf. [12, Ch. VII, §13, Theorem 13.4]. □

Let us now explain the connection between the Dirichlet Prime Number theorem and the Chebotarev Density theorem. Let $K = \mathbb{Q}$ and let $L = \mathbb{Q}(\zeta_m)$ be a cyclotomic extension with ζ_m a primitive mth root of unity. It is well-known that $\mathrm{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ and this isomorphism is given by sending the class of any integer a which is relatively prime to m to the automorphism $\sigma_a \colon L \to L$, $\sigma_a(\zeta_m) = \zeta_m^a$ (cf. [10, Ch. VI, §3, Theorem 3.1]). We claim that the set $\mathcal{P}(L/\mathbb{Q}, \{\sigma_a\})$ coincides with the arithmetic progression $\mathbb{P}_{a(m)}$, where we routinely identify $V_f^{\mathbb{Q}}$ with $\mathbb{P}$. In fact, by definition $\mathcal{P}(L/\mathbb{Q}, \{\sigma_a\})$ consists of all those $p \in \mathbb{P}$ which are unramified in L and for some $w|v_p$, we have $\mathrm{Fr}_{L/\mathbb{Q}}(w|v_p) = \sigma_a$. Thus, $p \in \mathcal{P}(L/\mathbb{Q}, \{\sigma_a\})$ if $p \nmid m$ (cf. [2, Ch. III, §1, Lemma 6]) and $\mathrm{Fr}_{L/\mathbb{Q}}(w|v_p)(\zeta_m) = \zeta_m^a$. On the other hand, $\mathrm{Fr}_{L/\mathbb{Q}}(w|v_p)(\zeta_m) = \zeta_m^p$ (cf. [2, Ch. VII, §3.4, Proposition]). Thus, $\zeta_m^p = \zeta_m^a$, which is equivalent to $p \equiv a (\mathrm{mod} m)$ because $p \nmid m$. This shows that $\mathcal{P}(L/\mathbb{Q}, \{\sigma_a\}) = \mathbb{P}_{a(m)}$. Hence the sets of the form $\mathcal{P}(L/K, \mathcal{C})$ *generalize* the sets of prime numbers in arithmetic progression $\mathbb{P}_{a(m)}$ and we recover all the $\mathbb{P}_{a(m)}$ precisely in the case of cyclotomic extensions. The sets of the form $\mathcal{P}(L/K, \mathcal{C})$ are central to this thesis and the observation that they generalize usual sets of primes in arithmetic progressions motivates the following definition

Definition 1.2.16 Let K be a global field and let L/K be a finite Galois extension with $G = \mathrm{Gal}(L/K)$. Fix a conjugacy class $\mathcal{C}$ in G. A *generalized arithmetic progression* $\mathcal{P}(L/K, \mathcal{C})$ is the set of all $v \in V_f^K$ such that v is unramified in L and for some (equivalently, any) extension $w|v$ the Frobenius automorphism $\mathrm{Fr}(w|v)$ lies in $\mathcal{C}$.

We will derive one important consequence of Theorem 1.2.15. We let $\mathrm{Spl}(L/K)$ denote the set of all nonarchimedean valuations of K that split completely in L. We will only use this notion when L/K is a finite Galois extension. Then $\mathrm{Spl}(L/K)$ consists precisely of those valuations $v \in V_f^K$, which are unramified in L and $\mathrm{Fr}_{L/K}(w|v) = \mathrm{id}_L$ for some (equivalently any) extension $w|v$. By Chebotarev's Density Theorem, $\mathrm{Spl}(L/K)$ has Dirichlet density $1/n$ where $n = [L : K]$. In particular, $\mathrm{Spl}(L/K)$ is an infinite set. Moreover, for any subset $\mathcal{P}_0 \subset \mathrm{Spl}(L/K)$ of density zero, the set $\mathrm{Spl}(L/K) \setminus \mathcal{P}_0$ still has density $1/n$.

Given any two subsets $A, B \subset V_f^K$, we will write $A \dot{\subset} B$ if $A \setminus \mathcal{P}_0 \subset B$ for some subset $\mathcal{P}_0 \subset A$ with $\mathfrak{d}_K(\mathcal{P}_0) = 0$ and in that case we say that B *almost contains* A.

Proposition 1.2.17 *Let K be a global field and let L and M be finite Galois extensions of K. Then the inclusion $L \subset M$ is equivalent to* $\mathrm{Spl}(M/K) \dot{\subset} \mathrm{Spl}(L/K)$.

Proof. It is clear that $L \subset M$ implies the inclusion $\mathrm{Spl}(M/K) \subset \mathrm{Spl}(L/K)$. This follows from the multiplicativity of the ramification index and the residual degree (cf. [15, Ch. 1, §1.1.2 and §1.1.3]). In particular, we have $\mathrm{Spl}(M/K) \dot{\subset} \mathrm{Spl}(L/K)$. Conversely, suppose that $\mathrm{Spl}(M/K) \dot{\subset} \mathrm{Spl}(L/K)$, i.e. $\mathrm{Spl}(M/K) \setminus \mathcal{P}_0 \subset \mathrm{Spl}(L/K)$ for some $\mathcal{P}_0 \subset V_f^K$ with $\mathfrak{d}_K(\mathcal{P}_0) = 0$. Assume that $L \not\subset M$, and set $E = LM$. Then E/M is a Galois extension and $E \neq M$, so we may choose $\sigma \in \mathrm{Gal}(E/M) \setminus \{\mathrm{id}_E\}$. By Chebotarev's Density Theorem we can pick $v \in V_f^K \setminus \mathcal{P}_0$ which is unramified in

E and for which $\mathrm{Fr}_{E/K}(w|v) = \sigma$ for some extension $w|v$. Set $u := w|_M$. Then

$$\mathrm{Fr}_{M/K}(u|v) = \sigma|_M = \mathrm{id}_M,$$

implying that $v \in \mathrm{Spl}(M/K) \setminus \mathcal{P}_0$. On the other hand, $\sigma|_L$ is nontrivial, meaning that v does not split completely in L. This yields a contradiction. □

It should be noted that while we will not use Proposition 1.2.17 directly, a similar argument used in its proof, will be used in the proof of almost strong approximation for the multiplicative group of a field (cf. Proposition 1.3.7).

1.3 Almost strong approximation for the multiplicative group of a field

1.3.1 Motivating examples

Let K be a global field and let $S \subset V^K$ be any nonempty subset. We saw that the additive group of K satisfies strong approximation property with respect to S, namely the diagonal embedding $K \hookrightarrow \mathbb{A}_K(S)$ has dense image in the S-adelic topology (cf. Theorem 1.1.16). This is no longer true, however for the multiplicative group of K. In other words, the induced diagonal embedding $K^\times \hookrightarrow \mathbb{I}_K(S)$ may not have dense image in the S-idelic topology. In this section we consider several examples that, on the one hand, motivate the property of strong approximation and, on the other hand, exhibit some constraints on the situations where this property can be expected to hold. Recall that the group of S-ideles $\mathbb{I}_K(S)$ is a locally compact

topological group and admits a basis of open sets consisting of sets of the form

$$\prod_{v\in S'} W_v \times \prod_{v\notin S'\cup S} \mathcal{O}_v^\times, \tag{1.3}$$

where $S' \subset V^K \setminus S$ is an arbitrary finite subset, and $W_v \subset K_v^\times$ are arbitrary open subsets for $v \in S'$. In particular, $\mathbb{I}_K(S)$ has the following distinguished open subgroup

$$\mathbb{U}(S) := \prod_{v\in V^K\setminus S} \mathcal{O}_v^\times.$$

It follows from Lemma 1.1.22 that for a number field K and $S = V_\infty^K$, the index $[\mathbb{I}_K(V_\infty^K) : K^\times\mathbb{U}(V_\infty^K)]$ (with $K^\times$ embedded in $\mathbb{I}_K(S)$ diagonally) equals the class number $h(K)$ of K, hence is always finite. Thus, for any $S \supset V_\infty^K$ the index $[\mathbb{I}_K(S) : K^\times\mathbb{U}(S)]$ is finite, and is equal to one if $h(K) = 1$. The intersection $\mathbb{E}(S) := \mathbb{U}(S) \cap K^\times$ will be called the *group of S-units*, and as $\mathbb{U}(S)$ is open in $\mathbb{I}_K(S)$, we conclude that the index of the closure $[\mathbb{I}_K(S) : \overline{K^\times}^{(S)}]$ is finite if and only if the index $[\mathbb{U}(S) : \overline{\mathbb{E}(S)}^{(S)}]$ is finite, where $^{-(S)}$ always denotes the closure in the S-idelic topology. Moreover, if $\overline{K^\times}^{(S)} = \mathbb{I}_K(S)$ then $\overline{\mathbb{E}(S)}^{(S)} = \mathbb{U}(S)$, and the converse is true if $h(K) = 1$. Similar remarks are valid also in the function field case, but we will not formulate them here since in our examples we will stick to the number field case.

After these preliminaries, we are ready to test strong approximation for $K^\times$ when $K = \mathbb{Q}$. To simplify the notation, for any subset $S \subset V^{\mathbb{Q}}$ we will write $\mathbb{I}(S)$ (resp. $\mathbb{A}(S)$) rather than $\mathbb{I}_{\mathbb{Q}}(S)$ (resp. $\mathbb{A}_{\mathbb{Q}}(S)$). If $S = \{v_\infty\}$, where v_∞ denotes the unique archimedean valuation of $\mathbb{Q}$, then $\mathbb{E}(S) = \{\pm 1\}$, and hence the index $[\mathbb{U}(S) : \overline{\mathbb{E}(S)}^{(S)}]$ is infinite, so the index $[\mathbb{I}(S) : \overline{\mathbb{Q}^\times}^{(S)}]$ is also infinite. Now, let $S = \{v_\infty\} \cup \{v_2\}$ where v_2 is the dyadic valuation of $K = \mathbb{Q}$, in which case $\mathbb{E}(S) = \langle -1, 2\rangle$ is already infinite. Set $Q = \mathbb{P}_{1(8)}$, which is infinite by Dirichlet's Prime Number Theorem. For every

$q \in Q$ we have $\mathbb{E}(S) \subset \mathbb{Z}_q^{\times 2}$; in other words, $\mathbb{E}(S)$ is contained in the kernel of the canonical continous surjective homomorphism

$$\mathbb{U}(S) \longrightarrow \prod_{q \in Q} \mathbb{Z}_q^{\times} / \mathbb{Z}_q^{\times 2}, \tag{1.4}$$

implying that the indices $[\mathbb{U}(S) : \overline{\mathbb{E}(S)}^{(S)}]$, hence also $[\mathbb{I}(S) : \overline{\mathbb{Q}^{\times}}^{(S)}]$, are infinite. It is easy to see that this result extends to any subset S of the form $S = \{v_\infty\} \cup \{v_{p_1}, \ldots, v_{p_r}\}$ for any finite collection of primes $p_1, \ldots, p_r$: one simply needs to take $Q = \mathbb{P}_{1(4p_1 \cdots p_r)}$ in the above argument[1]. On the other hand, an argument of this type cannot be implemented whenever S is infinite, which raises the question if $K^{\times}$ always has strong approximation for S infinite. The following example shows that this is not the case.

Example 1.3.1 For a prime $p > 2$ and any integer x not divisible by p, we let $\left(\frac{x}{p}\right)$ denote the corresponding Legendre symbol. As above, it is enough to construct two *infinite* disjoint subsets $P = \{p_1, p_2, \ldots\}$ and $Q = \{q_1, q_2, \ldots\}$ of $\mathbb{P}_{1(4)}$ such that

$$\left(\frac{p}{q}\right) = 1 \quad \text{for all} \quad p \in P,\ q \in Q. \tag{1.5}$$

Indeed, then for $S = \{v_\infty\} \cup \{v_p \,|\, p \in P\}$, the group $\mathbb{E}(S)$, which is generated by -1 and all primes $p \in P$, is contained in the kernel of the map (1.4), making the index $[\mathbb{I}(S) : \overline{\mathbb{Q}^{\times}}^{(S)}]$ infinite.

We construct the required sets P and Q inductively. Pick an arbitrary $p_1 \in \mathbb{P}_{1(4)}$ (e.g., one can take $p_1 = 5$) and choose $q_1 \in \mathbb{P}_{1(4)}$ so that $q_1 \equiv 1 (\mathrm{mod}\, p_1)$ (e.g., take

[1] This argument can be extended even further to arbitrary global field K and any finite set $S \subset V^K$ using Dirichlet's Unit Theorem and Chebotarev's Density Theorem – cf. [26, 2.2] for details in the number field case.

$q_1 = 11$). Then using quadratic reciprocity we obtain

$$\left(\frac{p_1}{q_1}\right) = \left(\frac{q_1}{p_1}\right) = \left(\frac{1}{p_1}\right) = 1.$$

Suppose that we have already found $p_1, \ldots, p_\ell$ and $q_1, \ldots, q_\ell$ ($\ell \geq 1$) such that

$$\left(\frac{p_i}{q_j}\right) = 1 \quad \text{for all} \quad i, j = 1, \ldots, \ell.$$

Now, choose $p_{\ell+1} \in \mathbb{P}_{1(4)}$ to satisfy $p_{\ell+1} \equiv 1 (\mathrm{mod}\, q_1 \cdots q_\ell)$, and $q_{\ell+1} \in \mathbb{P}_{1(4)}$ to satisfy $q_{\ell+1} \equiv 1 (\mathrm{mod}\, p_1 \cdots p_{\ell+1})$. Then

$$\left(\frac{p_{\ell+1}}{q_j}\right) = \left(\frac{1}{q_j}\right) = 1 \text{ for } j = 1, \ldots, \ell, \text{ and } \left(\frac{p_i}{q_{\ell+1}}\right) = \left(\frac{q_{\ell+1}}{p_i}\right) = \left(\frac{1}{p_i}\right) = 1 \text{ for } i = 1, \ldots, \ell+1$$

by quadratic reciprocity, as required. Observe that from our construction it follows that $p_\ell > p_1^{\ell-1}$ for all $\ell > 1$, which implies that the set of primes P has Dirichlet density zero.

We will now turn to an example of a *special* set of primes having positive Dirichlet density (that comes from an arithmetic progression) for which $K^\times$ does have strong approximation.

Example 1.3.2 Let $S = \{v_\infty\} \cup \{v_p \,|\, p \in \mathbb{P}_{1(4)}\}$. We will now show that multiplicative group of $K = \mathbb{Q}$ has strong approximation with respect to S. As we noted above, due to $h(\mathbb{Q}) = 1$, it is enough to show that the subgroup $\mathbb{E}(S)$, which is generated by -1 and all primes $p \in \mathbb{P}_{1(4)}$, is dense in $\mathbb{U}(S)$. Since sets of the form (1.3) constitute a basis of open sets for the S-idelic topology, it is enough to show

that every set of the form

$$U = \prod_{i=1}^{r} (a_i + p_i^{\alpha_i}\mathbb{Z}_{p_i}) \times \prod_{q \in \mathbb{P}\setminus(\mathbb{P}_{1(4)} \cup P)} \mathbb{Z}_q^{\times}$$

where $P = \{p_1 = 2, p_2, \ldots, p_r\} \subset \mathbb{P} \setminus \mathbb{P}_{1(4)}$ is a finite subset, and $\alpha_i \geq 1$ and a_i are integers with $(a_i, p_i) = 1$ for $i = 1, \ldots, r$, intersects $\mathbb{E}(S)$. Set $\varepsilon = 1$ if $a_1 \equiv 1 (\mathrm{mod}\, 4)$, and $\varepsilon = -1$ if $a_1 \equiv 3 (\mathrm{mod}\, 4)$, so that $\varepsilon a_1 \equiv 1 (\mathrm{mod}\, 4)$ in all cases. Using the Chinese Remainder Theorem, we can find $c \in \mathbb{Z}$ satisfying

$$\begin{cases} c \equiv \varepsilon a_i (\mathrm{mod}\, p_i^{\alpha_i}) \text{ for } i = 1, \ldots, r, \\ c \equiv 1 (\mathrm{mod}\, 4). \end{cases}$$

Next, by Dirichlet's Prime Number Theorem, there exists a prime $p \equiv c (\mathrm{mod}\, 4p_1^{\alpha_1} \cdots p_r^{\alpha_r})$. Then $\varepsilon p \in \mathbb{E}(S) \cap U$. This completes the proof of the fact that $\overline{\mathbb{E}(S)}^{(S)} = \mathbb{U}(S)$.

In the next section we will see that for any relatively prime integers a, m and $S = \{v_\infty\} \cup \mathbb{P}_{a(m)}$, the index $[\mathbb{I}(S) : \overline{\mathbb{Q}^{\times}}^{(S)}]$ is finite (cf. Proposition 1.3.7). However, as we will now show, it is not always equal to one.

Example 1.3.3 Let $K = \mathbb{Q}$, let $q \in \mathbb{P}_{1(4)}$, and set $S = \{v_\infty\} \cup \{v_p \,|\, p \in \mathbb{P}_{1(q)}\}$. Then

$$[\mathbb{I}(S) : \overline{\mathbb{Q}^{\times}}^{(S)}] > 1. \tag{1.6}$$

Our proof will use the Artin map associated with the quadratic extension $L = \mathbb{Q}(\sqrt{q})$, and we would like to point out that a suitable generalization of this approach will play a crucial role also in the proof of Proposition 1.3.7. We let $(*,*)_p$ (resp., $(*,*)_\infty$) denote the Hilbert symbol over $\mathbb{Q}_p$ (resp., over $\mathbb{R}$). If we identify the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ with $\{\pm 1\}$, then as we saw in section 1.2.3 the Artin map

$\Psi_{L/\mathbb{Q}}\colon \mathbb{I}_{\mathbb{Q}} \to \mathrm{Gal}(L/\mathbb{Q})$ is given by

$$(x_p)_p \mapsto (x_\infty, q)_\infty \cdot \prod_{p\in\mathbb{P}} (x_p, q)_p.$$

Then by class field theory for $L/\mathbb{Q}$, the kernel $N := \ker \Psi_{L/\mathbb{Q}} \subset \mathbb{I}_{\mathbb{Q}}$ is an open subgroup containing $\mathbb{Q}^\times$ and having index two. Let $\pi_S\colon \mathbb{I}_{\mathbb{Q}} \to \mathbb{I}(S)$ be the canonical projection. Then $\pi_S(N)$ is an open subgroup of $\mathbb{I}(S)$ containing $\mathbb{Q}^\times$, and to prove (1.6) it is enough to show that $N \supset \ker \pi_S$ as then $\pi_S(N) \neq \mathbb{I}(S)$. For this we observe that $q \in \mathbb{Q}_v^{\times 2}$ for all $v \in S$. This is obvious for $v = v_\infty$, and follows from

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{1}{q}\right) = 1$$

for $v = v_p$ with $p \in \mathbb{P}_{1(q)}$. Let now $x = (x_p)_p \in \ker \pi_S$, i.e. $x_p = 1$ for $p \in \mathbb{P} \setminus \mathbb{P}_{1(q)}$. Then

$$\Psi_{L/\mathbb{Q}}(x) = (x_\infty, q)_\infty \cdot \prod_{p\in\mathbb{P}_{1(q)}} (x_p, q)_p = 1,$$

proving that $N \supset \ker \pi_S$. Using the cyclotomic extension $\mathbb{Q}(\zeta_q)$ in place of L in the above argument, one can show that the index in (1.6) can be arbitrarily large.

1.3.2 Almost strong approximation for multiplicative group of a field

The main takeaway from the examples in the previous section is that the property that can be expected to hold for the multiplicative group of a field with respect to arithmetic progressions is not strong approximation in the classical sense but rather its variation (in fact, a slight weakening) of the latter which in this section we define only for the multiplicative group of a field but we will define it for arbitrary algebraic

groups in Chapter 2 (cf. Definition 2.1.7).

Definition 1.3.4 Let K be a global field and let $S \subset V^K$ be a nonempty subset. We say that $K^\times$ satisfies *almost strong approximation* with respect to S if the index $[\mathbb{I}_K(S) : \overline{K^\times}^{(S)}]$ is finite.

Examples in section 1.3.1 motivate our next definition

Definition 1.3.5 Let K be a global field. A subset $S \subset V^K$ is called *tractable* if it contains a set of the form $V_\infty^K \cup (\mathcal{P}(L/K, \mathcal{C}) \setminus \mathcal{P}_0)$ for some generalized arithmetic progression $\mathcal{P}(L/K, \mathcal{C})$ and a subset $\mathcal{P}_0$ with $\mathfrak{d}_K(\mathcal{P}_0) = 0$.

Now let S be any tractable set in K. The main goal of this section is to prove that if F/K is any finite separable extension then under some technical condition (see (1.7)) we have that $F^\times$ has almost strong approximation with respect to $\bar{S}$, where $\bar{S}$ denotes the set of all extensions of valuations $v \in S$ to F. We begin with the following lemma

Lemma 1.3.6 *The group $\mathbb{I}_F(\bar{S})/\overline{F^\times}^{(\bar{S})}$ is profinite.*

Proof. Recall that $\mathbb{I}_F^{(1)}$ is the kernel of the surjective homomorphism $\nu\colon \mathbb{I}_F \to \mathbb{R}_{>0}$ given by $(x_w)_w \mapsto \prod_{w \in V^F} |x_w|_w$. On the other hand, for any $w \in V^F$ the product $F_w^\times \mathbb{I}_F^{(1)}$ is a closed subgroup of $\mathbb{I}_F$. In fact, if $w \in V_\infty^F$ then $\nu(F_w^\times) = \mathbb{R}_{>0}$ and if $w \in V_f^F$ then $\nu(F_w^\times)$ is a discrete subgroup of $\mathbb{R}_{>0}$ so it is of the form $\{\lambda^n\}_{n \in \mathbb{Z}}$ for some $\lambda \in \mathbb{R}_{>0}$ (using multiplicative notation). Thus, $\nu(F_w^\times)$ is closed for any $w \in V^F$ and $F_w^\times \mathbb{I}_F^{(1)} = \nu^{-1}(\nu(F_w^\times))$ is closed since ν is continuous. By product formula, we have $F^\times \subset \mathbb{I}_F^{(1)}$, so $F_w^\times \mathbb{I}_F^{(1)}$ also contains the closure of $F^\times$ in $\mathbb{I}_F$. Furthermore, $\mathbb{I}_F / F_w^\times \mathbb{I}_F^{(1)}$ is compact. In fact, if $w \in V_\infty^F$ then

$$\mathbb{I}_F / F_w^\times \mathbb{I}_F^{(1)} \simeq \nu(\mathbb{I}_F)/\nu(F_w^\times \mathbb{I}_F^{(1)}) \simeq \mathbb{R}_{>0}/\mathbb{R}_{>0}$$

is trivial. On the other hand, if $w \in V_f^F$ then

$$\mathbb{I}_F/F_w^\times \mathbb{I}_F^{(1)} \simeq \nu(\mathbb{I}_F)/\nu(F_w^\times \mathbb{I}_F^{(1)}) \simeq \mathbb{R}_{>0}/\{\lambda^n\}_{n\in\mathbb{Z}} \simeq \mathbb{R}/\mathbb{Z}$$

where the last isomorphism is induced by the homeomorphism $\log\colon \mathbb{R}_{>0} \to \mathbb{R}$, which sends $\{\lambda^n\}_{n\in\mathbb{Z}}$ to $\{n\log\lambda\}_{n\in\mathbb{Z}} \simeq \mathbb{Z}$. There is a natural continuous projection $\mathbb{I}_F \to \mathbb{I}_F(\bar{S})$ so the quotient $\mathbb{I}_F(\bar{S})/\overline{F^\times}^{(\bar{S})}$ is also compact. Since $\bar{S} \supset V_\infty^F$, we deduce that $\mathbb{I}_F(\bar{S})/\overline{F^\times}^{(\bar{S})}$ is totally disconnected and therefore it is a profinite group. □

Proposition 1.3.7 *Let F be a finite separable extension of a global field K, and let $S \subset V^K$ be a tractable subset containing a set of the form $V_\infty^K \cup (\mathcal{P}(L/K,\mathcal{C}) \setminus \mathcal{P}_0)$ where $\mathcal{P}_0$ has Dirichlet density zero. Assume that there exists $\sigma \in \mathcal{C}$ such that*

$$\sigma|(F \cap L) = \mathrm{id}_{F\cap L}. \tag{1.7}$$

Then the index $[\mathbb{I}_F(\bar{S}) : \overline{F^\times}^{(\bar{S})}]$ is finite and divides $n = [L : K]$.

Proof. By Lemma 1.3.6, we may write

$$\overline{F^\times}^{(\bar{S})} = \bigcap_{B\in\mathcal{B}} B,$$

where $\mathcal{B}$ denotes the family of all open subgroups of $\mathbb{I}_F(\bar{S})$ that contain $F^\times$. Every such subgroup B is automatically of finite index, and it is enough to show that

$$\text{for every } B \in \mathcal{B}, \text{ the index } [\mathbb{I}_F(\bar{S}) : B] \text{ divides } m = [FL : F] \tag{$\star$}$$

as obviously $m|n$. In fact, consider the map $f\colon \mathcal{B} \to \mathbb{N}$ defined by $f(B) = [\mathbb{I}_F(\bar{S}) : B]$. The degree $m = [FL : F]$ is a *uniform bound* that does not depend on any B, so if we prove ($\star$) then one can choose $B_0 \in \mathcal{B}$ such that $f(B_0)$ is maximal. Now,

if B' is any other subgroup in $\mathcal{B}$ then $B' \cap B_0 \subset B_0$ so $f(B_0) \leq f(B' \cap B_0)$ but because $f(B_0)$ is maximal, we deduce $f(B' \cap B_0) = f(B_0)$. By iteration, we obtain $f(\bigcap_{B \in \mathcal{B}} B) = f(\overline{F^\times}^{(\bar{S})}) = f(B_0)$.

Let $\pi_{\bar{S}} \colon \mathbb{I}_F \to \mathbb{I}_F(\bar{S})$ be the natural projection, and set $M := \pi_{\bar{S}}^{-1}(B)$. Then M is an open subgroup of $\mathbb{I}_F$ containing $F^\times$ and having index $[\mathbb{I}_F : M] = [\mathbb{I}_F(\bar{S}) : B]$. By the Existence Theorem of class field theory (cf. Theorem 1.2.2) there is an abelian extension P/F such that $M = F^\times N_{P/F}(\mathbb{I}_P)$. On the other hand, due to the fundamental isomorphism of class field theory (cf. Theorem 1.2.1), the index $[\mathbb{I}_F : N]$ of the norm subgroup $N := F^\times N_{FL/F}(\mathbb{I}_{FL})$ divides $[FL : F] = m$. Thus, it is enough to prove the inclusion $P \subset FL$ as then $N \subset M$.

Suppose that $P \not\subset FL$. Pick $\sigma \in \mathcal{C}$ that satisfies (1.7), and using the canonical isomorphism of Galois groups $\mathrm{Gal}(FL/F) \simeq \mathrm{Gal}(L/(F \cap L))$, find $\tilde{\sigma} \in \mathrm{Gal}(FL/F)$ such that $\tilde{\sigma}|L = \sigma$. Let E be a finite Galois extension of K that contains F, L and P. We claim that there exists $\tau \in \mathrm{Gal}(E/K)$ such that

$$\tau|FL = \tilde{\sigma} \quad \text{and} \quad \tau|P \neq \mathrm{id}_P. \tag{1.8}$$

Indeed, otherwise the set of all $\tau \in \mathrm{Gal}(E/K)$ satisfying $\tau|FL = \tilde{\sigma}$, which is a right coset of the subgroup $\mathrm{Gal}(E/FL)$, would be contained in $\mathrm{Gal}(E/P)$. This would imply the inclusion $\mathrm{Gal}(E/FL) \subset \mathrm{Gal}(E/P)$ yielding the inclusion $P \subset FL$ that contradicts our original assumption.

So, fix $\tau \in \mathrm{Gal}(E/K)$ satisfying (1.8). By Chebotarev's Density Theorem (cf. Theorem 1.2.15), the set of $v \in V_f^K$ that are unramified in E and admit an extension $w \in V_f^E$ such that $\mathrm{Fr}_{E/K}(w|v) = \tau$ has positive Dirichlet density. Since $\mathfrak{d}_K(\mathcal{P}_0) = 0$ by our assumption, such a v can actually be found outside of $\mathcal{P}_0$; we then let w denote the extension of v as above. The fact that $\tau|L = \sigma$ implies that $v \in S$,

placing $u' := w|F$ in $\bar{S}$. Furthermore, since τ generates $\mathrm{Gal}(E_w/K_v)$, the facts that $\tau|F = \mathrm{id}_F$ and $\tau|P \neq \mathrm{id}_P$ mean that $F_{u'} = K_v$ while for $u'' := w|P$ we have $P_{u''} \neq F_{u'}$ (note that $u''|u'$). On the other hand, since $u' \in \bar{S}$, it follows from the construction of M that we have the inclusion $F_{u'}^{\times} \subset M$. But M coincides with the kernel of the Artin map $\psi_{P/F} \colon \mathbb{I}_F \to \mathrm{Gal}(P/F)$, so the restriction of $\psi_{P/F}$ to $F_{u'}^{\times} \subset \mathbb{I}_F$ is trivial. Since by construction of the Artin map we have

$$\psi_{P/F}(F_{u'}^{\times}) = \langle \mathrm{Fr}_{P/F}(u''|u') \rangle = \mathrm{Gal}(P_{u''}/F_{u'}),$$

we obtain that $P_{u''} = F_{u'}$, a contradiction. Thus, $P \subset FL$, completing the argument. □

Finally, observe that Proposition 1.3.7 establishes Theorem A of the Introduction in the case of multiplicative group of a global field. It should be noted that Proposition 1.3.7 also extends [20, Proposition 5.1], where $\mathcal{P}_0$ was only allowed to be a finite subset and not an arbitrary set of density zero.

Chapter 2

Algebraic groups and cohomology

2.1 Algebraic groups

2.1.1 Definitions and examples

Let F be an algebraically closed field. In this section we introduce some basic definitions and results on algebraic groups over F. A *linear algebraic group* G is a subgroup of some *general linear group* $\mathrm{GL}_n = \mathrm{GL}_n(F)$, which is closed in the Zariski topology, i.e. G is defined by some polynomial equations. For a general study of algebraic varieties, we refer the reader to [7, Ch. I]. Both the general linear group GL_n and the *special linear group* SL_n are examples of algebraic groups. In fact, by definition,

$$\mathrm{SL}_n = \Big\{ X \in M_n(F) \;\Big|\; \det X = 1 \Big\},$$

so it is given by a single polynomial equation. It is worth noting that one can realize GL_n as a closed subgroup of SL_{n+1} by adjoining an additional variable as follows:

$$\mathrm{GL}_n = \Big\{ ((x_{ij}), y) \in M_n(F) \times F \;\Big|\; y \det(x_{ij}) - 1 = 0 \Big\}.$$

An important special case of the general linear group is the *multiplicative group* of the field F, denoted $\mathbb{G}_m := \mathrm{GL}_1$.

Since we will later be working with groups of adeles, it is important to mention a more abstract definition of an algebraic group. An *affine algebraic group* G is an algebraic variety with a group structure such that the multiplication map $\mu\colon G\times G \to G,\ (x,y)\mapsto xy$ and the inverse map $\iota\colon G\to G,\ x\mapsto x^{-1}$ are morphisms of algebraic varieties. It is well-known that the notions of linear and affine algebraic groups are equivalent (cf. [1, Ch. I, §1, Proposition 1.10] and [7, Ch. II, §8.6, Theorem]). In this thesis we will be only interested in linear algebraic groups. For a detailed treatment of algebraic groups using the affine approach, we refer the reader to [7, Ch. II] and [1, Ch. I].

A map $f\colon G\to G'$ between two algebraic groups G and G' is called a *morphism* of algebraic groups if it is a morphism of algebraic varieties, which is also a group homomorphism. A morphism of algebraic groups that has an inverse (morphism), is called an *isomorphism* of algebraic groups. An important example of a morphism of algebraic groups is the determinant map $\det\colon \mathrm{GL}_n \to \mathbb{G}_m$. Since in this thesis we will only work with linear algebraic groups, the word linear will often be omitted. Clearly, any closed subgroup of an algebraic group is an algebraic group. Another important example of an algebraic subgroup of GL_n (apart from SL_n) is the *orthogonal group* defined by

$$\mathrm{O}_n = \Big\{ X \in M_n(F) \,\Big|\, XX^t = X^tX = I_n \Big\},$$

where I_n denotes the n by n identity matrix. The *ring of regular functions* of GL_n is given by

$$F[\mathrm{GL}_n] = F[x_{11}, x_{12}, \ldots, x_{nn}, \det(x_{ij})^{-1}].$$

Furthermore, one defines the ring of regular functions of an algebraic group $G \subset \mathrm{GL}_n$

to be $F[\mathrm{GL}_n]/\mathcal{I}(G)$, where $\mathcal{I}(G)$ is the ideal of all regular functions in $F[\mathrm{GL}_n]$ that vanish on G.

Let $K \subset F$ be any subfield. Our main case of interest in this thesis is when K is either a number field or more generally a global field. We say that an algebraic group $G \subset \mathrm{GL}_n$ is *defined over* K (or that G is a *K-group*) if the ideal $\mathcal{I}(G)$ is generated by

$$\mathcal{I}(G) \cap K[x_{11}, x_{12}, \ldots, x_{nn}, \det(x_{ij})^{-1}]$$

(cf. [15, Ch. 2, §2.1.1]). For any algebraic group $G \subset \mathrm{GL}_n$, we define the *group of K-points $G(K)$ of G* as $G(K) = G \cap \mathrm{GL}_n(K)$. Suppose that G is a K-group. Then for any field extension L/K, we define the group of L-points of G as the set of points in $\mathrm{GL}_n(L)$ that satisfy all the equations defining G. For example, the group of L-points of SL_n equals

$$\mathrm{SL}_n(L) = \Big\{ X \in M_n(L) \;\Big|\; \det(X) = 1 \Big\}.$$

If a morphism $f\colon G \to G'$ of two K-groups $G \subset \mathrm{GL}_n$ and $G' \subset \mathrm{GL}_m$, can be defined by polynomials with coefficients in K then we say that f is *defined over K* (or f is a *K-morphism*). If $f\colon G \to G'$ is a K-morphism of algebraic groups then for any field extension L/K, we have an induced continuous map $f_L\colon G(L) \to G'(L)$ on the level of L-points. For any algebraic group G its irreducible components are exactly its connected components (for the Zariski topology) (cf. [7, Ch. II, §7.3, Proposition]). The *connected component* of the identity in G, denoted by G°, is an open and closed normal subgroup of finite index in G (cf. [7, Ch. II,§7.3, Proposition, (a)]). Most algebraic groups considered in this thesis, are *connected*, so that $G = G^\circ$.

An algebraic group G is called *diagonalizable* (over F) if there exists a faithful

representation $\rho\colon G \to \mathrm{GL}_n$ for which the group $\rho(G)$ is conjugate to a subgroup of the group of the diagonal n by n matrices. Any connected diagonalizable algebraic group is called an *algebraic torus* (see Definition 2.2.1 for an equivalent characterization). Note that the simplest example of a torus is the multiplicative group $\mathbb{G}_m$. Tori are among the most important examples of algebraic groups in this thesis and they will be studied in greater detail in section 2.2.

For any abstract group G one defines the *derived series* $\mathcal{D}^n(G)$ of G for all $n \geq 0$ inductively by

$$\mathcal{D}^0(G) = G, \quad \mathcal{D}^{n+1}(G) = [\mathcal{D}^n(G), \mathcal{D}^n(G)],$$

where $[\mathcal{D}^n(G), \mathcal{D}^n(G)]$ denotes the commutator subgroup of $\mathcal{D}^n(G)$. We say that G is *solvable* if $\mathcal{D}^n(G) = \{1\}$ for some n. While the notion of solvable group comes from abstract group theory, here it will only be considered in the context of algebraic groups. We refer the reader to [1, Ch. I, §2.4] for a careful study of solvable groups in the context of algebraic groups.

Until the end of this section let us assume that F has characteristic 0 and $K \subset F$ is any subfield. Let G be an algebraic K-group. A maximal connected solvable subgroup B of G is called a *Borel subgroup*. Any two Borel subgroups of G are conjugate (cf. [33, Ch. 6, §6.2, Theorem 6.2.7(iii)]). The group G does not necessarily have a K-defined Borel subgroup. A K-group for which there exists a K-defined Borel subgroup is called *K-quasi-split*. For example, the group of all invertible upper triangular matrices in GL_n is a Borel subgroup.

An algebraic group $G \subset \mathrm{GL}_n$ is called *unipotent* if all of its elements are unipotent, i.e. for any $g \in G$ there exists a positive integer k such that $(g - I_n)^k = 0$. An example of a unipotent group is the *additive group* of F, denoted by $\mathbb{G}_a$. This group

admits the following matrix representation

$$\mathbb{G}_a = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(F) \,\middle|\, x \in F \right\}.$$

More generally the group of upper *unitriangular* matrices, i.e. upper triangular matrices which have only ones on the diagonal, is unipotent.

Let G be an algebraic group. The maximal connected solvable normal subgroup of G is denoted by $R(G)$ and we call it the *radical* of G. The maximal connected unipotent normal subgroup of G is called the *unipotent radical* of G and we denote it by $R_u(G)$. We say that G is *reductive* if $R_u(G) = \{1\}$ and that G is *semi-simple* if $R(G) = \{1\}$. Observe that any semi-simple group is automatically reductive. The main example of a reductive (resp. semi-simple) group is GL_n (resp. SL_n). Clearly, if G is connected then $G/R(G)$ is semi-simple and $G/R_u(G)$ is reductive. The key structure result for reductive groups is the following

Theorem 2.1.1 *Let G be a reductive group. Then*

(1) *The radical $R(G)$ is the connected component $T = Z(G)^\circ$ of the center and T is a torus,*

(2) *The commutator subgroup $H = [G, G]$ is a semi-simple group,*

(3) *G is an almost direct product TH of T and H, i.e. $T \cap H$ is finite.*

Proof. Cf. [15, Ch. 2, §2.1.10, Theorem 2.8]. □

Furthermore, if G is defined over a subfield $K \subset F$ then H is also defined over K. An important instance of Theorem 2.1.1 is that GL_n is an almost direct product of $\mathbb{G}_m$ and SL_n with $\mathbb{G}_m \cap \mathrm{SL}_n$ being the *group of nth roots of unity*, denoted μ_n.

Any surjective morphism of algebraic groups $f\colon G \to G'$ with finite kernel is called an *isogeny*. For example, the product map $\mathbb{G}_m \times \mathrm{SL}_n \to \mathrm{GL}_n$ is surjective

and has kernel equal to μ_n, so it is an isogeny. A connected noncommutative algebraic group G is called (*absolutely almost simple*) if it does not have any nontrivial connected normal subgroups. Any semi-simple group is an almost direct product of finitely many absolutely almost simple groups (cf. [15, Ch. 2, §2.1.13, Proposition 2.11]). A connected algebraic group G is called *simply connected* if any isogeny $f\colon N \to G$, with N connected, is an isomorphism. For example, SL_n and the *special unitary group* $\mathrm{SU}_n(q)$ associated with a nondegenerate Hermitian form q (cf. [15, Ch. 2, §2.3.3]) are both simply connected, while GL_n is not simply connected. If any isogeny $f\colon G \to N$, with N connected, is an isomorphism then we say G is *adjoint*. For a more detailed exposition of algebraic groups, we refer the reader to [7, Ch. II, §7.1 - §7.5] and [15, Ch. 2, §2.1 - §2.3].

2.1.2 The group of adeles

In this section we introduce the adele groups and discuss their basic properties. Adele groups play a crucial role in the arithmetic theory of algebraic groups. We saw that standard results of number theory such as finiteness of class number and Dirichlet's Unit Theorem can be expressed in terms of ideles. Similarly, some arithmetic results about algebraic groups can be described using the language of groups of adeles. Let K be a global field.

Definition 2.1.2 Let G be an algebraic group over K. Fix a K-embedding $G \hookrightarrow \mathrm{GL}_n$. As before, for any $v \in V_\infty^K$ we set $\mathcal{O}_v := K_v$. Now for each $v \in V^K$ we set

$$G(\mathcal{O}_v) := G \cap \mathrm{GL}_n(\mathcal{O}_v).$$

We define the *group of adeles* $G(\mathbb{A}_K)$ of G over K to be the following restricted

product in both set-theoretic and topological sense

$$G(\mathbb{A}_K) = \prod_{v \in V^K}{}' (G(K_v), G(\mathcal{O}_v)).$$

It follows from the construction that $G(\mathbb{A}_K)$ is a locally compact topological group that has the basis of open sets of the form

$$\prod_{v \in S'} \Omega_v \times \prod_{v \in V^K \setminus S'} G(\mathcal{O}_v),$$

where $S' \subset V^K$ is a finite subset and $\Omega_v \subset G(K_v)$ is an open subset for each $v \in S'$ (with respect to the topology induced by the valuation v). It follows from Lemma 1.1.12 that the group $G(K)$ admits a diagonal embedding $G(K) \hookrightarrow G(\mathbb{A}_K)$, the image of which is called the *subgroup of principal adeles* of G. Observe that since K is discrete in $\mathbb{A}_K$ (cf. Lemma 1.1.13), the subgroup $G(K)$ is also discrete and closed in $G(\mathbb{A}_K)$.

Just as in the case of the ring of adeles, we will be mainly interested in the groups of truncated adeles, which we define as follows

Definition 2.1.3 Let G be an algebraic group over K and let $S \subset V^K$ be any subset. We define the *group of S-adeles* of G as the restricted product

$$G(\mathbb{A}_K(S)) = \prod_{v \in V^K \setminus S}{}' (G(K_v), G(\mathcal{O}_v))$$

so it has a basis of open sets of the form

$$\prod_{v \in S'} \Omega_v \times \prod_{v \in V^K \setminus (S \cup S')} G(\mathcal{O}_v),$$

where $S' \subset V^K \setminus S$ is some finite subset and $\Omega_v \subset G(K_v)$ is an open subset for each

$v \in S'$.

For example, if $K = \mathbb{Q}$, $S = \{v_\infty\}$ and $G = \mathrm{SL}_n$, then

$$\mathrm{SL}_n(\mathbb{A}_K(S)) = \prod_{p\in\mathbb{P}}{}'(\mathrm{SL}_n(\mathbb{Q}_p), \mathrm{SL}_n(\mathbb{Z}_p)).$$

Let $f\colon G_1 \to G_2$ be a K-morphism of two algebraic groups G_1 and G_2. For each $v \in V^K$, there is an induced continuous map $f_{K_v}\colon G_1(K_v) \to G_2(K_v)$, which gives rise to the product map

$$\prod_{v\in V^K} f_{K_v}\colon \prod_{v\in V^K} G_1(K_v) \to \prod_{v\in V^K} G_2(K_v).$$

The restriction of $\prod_{v\in V^K} f_{K_v}$ to $G(\mathbb{A}_K)$ will be denoted by $f_{\mathbb{A}_K}$. In fact, for any subset $S \subset V^K$, one can restrict $f_{\mathbb{A}_K}$ further to $G(\mathbb{A}_K(S))$ and we will denote this restriction by $f_{\mathbb{A}_K(S)}$. The next proposition states that $f_{\mathbb{A}_K(S)}$ preserves the S-adelic points of G_1

Proposition 2.1.4 *Let $f\colon G_1 \to G_2$ be a K-morphism of two K-groups G_1 and G_2. Then*

$$f_{\mathbb{A}_K(S)}(G_1(\mathbb{A}_K(S))) \subset G_2(\mathbb{A}_K(S))$$

and the map $f_{\mathbb{A}_K(S)}\colon G_1(\mathbb{A}_K(S)) \to G_2(\mathbb{A}_K(S))$ is continuous.

Proof. Cf. [15, Ch. 5, §5.1, Lemma 5.3]. □

The map $f_{\mathbb{A}_K(S)}$ will be called the *adelization of f* with respect to S. One of the most important results on adelization that we will need in proofs in Chapter 3 states that adelization of any surjective morphism of algebraic groups is always *open*. More precisely we have the following

Proposition 2.1.5 *Let $S \subset V^K$ be any subset and let $\pi\colon G_1 \to G_2$ be a surjective morphism of connected algebraic groups. Assume* $\ker \pi$ *is connected. Then*

$$\pi(G_1(\mathcal{O}_v)) = G_2(\mathcal{O}_v)$$

for almost all $v \in V^K \setminus S$, and thus the corresponding map $\pi_{\mathbb{A}_K(S)}\colon G_1(\mathbb{A}_K(S)) \to G_2(\mathbb{A}_K(S))$ is open.

Proof. Cf. [14, Ch. 6, §6.2, Proposition 6.5]. □

The classical property of strong approximation for an arbitrary algebraic group defined over a global field K is defined as follows

Definition 2.1.6 Let G be an algebraic K-group and let $S \subset V^K$ be any nonempty subset. We say that G satisfies *strong approximation* property with respect to S if the image of $G(K)$ under the diagonal embedding $G(K) \hookrightarrow G(\mathbb{A}_K(S))$ is dense.

Observe that if we denote by $\overline{G(K)}^{(S)}$ the closure of the image of $G(K)$ in $G(\mathbb{A}_K(S))$ under the diagonal embedding then strong approximation for G with respect to S is equivalent to the equality

$$\overline{G(K)}^{(S)} = G(\mathbb{A}_K(S)).$$

In this thesis we are interested in a slightly weaker property than strong approximation, called almost strong approximation, defined as follows

Definition 2.1.7 Let G be an algebraic K-group and let $S \subset V^K$ be a nonempty subset. We say that G has *almost strong approximation* with respect to S if the index

$$[G(\mathbb{A}_K(S)) : \overline{G(K)}^{(S)}]$$

is finite.

For example, multiplicative group $\mathbb{G}_m$ has almost strong approximation over $K = \mathbb{Q}$ for any set of the form $S = \{v_\infty\} \cup \{v_p \,|\, p \in \mathbb{P}_{a(m)}\}$ with a and m relatively prime integers (cf. Proposition 1.3.7) but it does not have almost strong approximation with respect to any finite set S – see examples in section 1.3.1. As we observed in the previous section, the multiplicative group $\mathbb{G}_m$ is the simplest example of one of the most important classes of algebraic groups in this thesis, namely algebraic tori which will be discussed in greater detail in the next section.

The "necessary" part of the classical criterion for strong approximation implies that if G is a nonsimply connected group then the index $[G(\mathbb{A}_K(S)) : \overline{G(K)}^{(S)}]$ is always infinite, whenever S is finite (cf. [14, Theorem 7.12]). This applies, in particular, to any nontrivial algebraic K-torus T, where one can actually show that the quotient $T(\mathbb{A}_K(S))/\overline{T(K)}^{(S)}$ is a group of infinite exponent for any finite S (cf. [26, Proposition 2.1]). On the other hand, it was shown in [20, Theorem 5.3] (see also [18, Theorem 3]) that the exponent of the quotient $T(\mathbb{A}_K(S))/\overline{T(K)}^{(S)}$ becomes finite if S contains V_∞^K and contains *all but finitely many* valuations in a generalized arithmetic progression that satisfies one technical condition (which cannot be omitted). In this thesis we consider more general sets of valuations S, namely tractable sets (cf. Definition 1.3.5) and we will prove that for a K-torus T and any tractable set S the quotient $T(\mathbb{A}_K(S))/\overline{T(K)}^{(S)}$ is in fact *finite* provided that the same technical condition as in [20, Theorem 5.3] holds for the generalized arithmetic progression involved in the description of S (cf. Theorem 3.1.3).

Remark 2.1.8 Observe that if $[G(\mathbb{A}_K(S)) : \overline{G(K)}^{(S)}] < \infty$ then there exists a finite subset $W \subset V^K \setminus S$ such that $\overline{G(K)}^{(S\cup W)} = G(\mathbb{A}_K(S \cup W))$, i.e. G has strong approximation with respect to $(S \cup W)$. Indeed, as usual we may assume

that $S \supset V_\infty^K$. Since $\overline{G(K)}^{(S)}$ is open in $G(\mathbb{A}_K(S))$, we can find a finite subset $W_1 \subset V^K \setminus S$ for which

$$\overline{G(K)}^{(S)} \supset \prod_{v \in V^K \setminus (S \cup W_1)} G(\mathcal{O}_v).$$

Now, let $\{g^1\overline{G(K)}^{(S)}, \ldots, g^t\overline{G(K)}^{(S)}\}$ be a system of coset representatives of $G(\mathbb{A}_K(S))$ by $\overline{G(K)}^{(S)}$, where $g^j = (g_v^j)_v \in G(\mathbb{A}_K(S))$ for each $j = 1, \ldots, t$. Then there exists a finite subset $W_2 \subset V^K \setminus S$ such that

$$g_v^j \in G(\mathcal{O}_v) \text{ for all } j = 1, \ldots, t \text{ and all } v \in V^K \setminus (S \cup W_2).$$

Set $W = W_1 \cup W_2$. Then projecting $G(\mathbb{A}_K(S)) = \bigcup_{j=1}^{t} g^j\overline{G(K)}^{(S)}$ to $G(\mathbb{A}_K(S \cup W))$, we obtain $G(\mathbb{A}_K(S \cup W)) = \overline{G(K)}^{(S \cup W)}$, as required. This observation justifies the term "almost strong approximation."

Finally, it should be noted that the notions of the *space of adeles* and strong approximation property can be studied for an arbitrary algebraic variety X over K (cf. [15, Ch. 5, §5.1]), however in this thesis we will only consider strong approximation in the context of algebraic groups.

2.2 Algebraic tori

2.2.1 Tori and restriction of scalars

In this section, we introduce algebraic tori and construct an important class of examples called quasi-split tori, obtained by a general construction called restriction of scalars. Let F be an algebraically closed field.

Definition 2.2.1 An algebraic group T such that $T \simeq \mathbb{G}_m^d$ (over F) for some integer $d \geq 1$, is called *algebraic torus*.

As we observed earlier tori can be equivalently characterized as exactly those algebraic groups which are connected and diagonalizable over F (cf. section 2.1.1).

We will now introduce an important functorial construction, which furnishes a new class of examples of tori. Let $K \subset F$ be a subfield and let L/K be any finite separable extension with $[L : K] = r$. Let X be an algebraic variety over L. There is a canonical way to obtain a K-variety from X. If additionally X is a linear algebraic L-group then the resulting K-variety has a natural structure of an algebraic K-group. Here we only provide a brief description of this construction but it will be discussed with all the details in Example 2.2.2 below. Assume that X is an affine variety in the n-dimensional affine space over L and is given by the zero locus of a collection of polynomials $\{f_i\}_i$ with $f_i \in L[x_1, \ldots, x_n]$ for each i. We may routinely identify L^n with an nr-dimensional vector space over K. Choose a basis $\{\alpha_1, \ldots, \alpha_r\}$ of L over K. By expressing each of the variables in terms of that basis $x_j = \sum_{\ell=1}^{r} y_\ell^j \alpha_\ell$, we can view each polynomial equation $f_i(x_1, \ldots, x_n)$ with coefficients in L as r polynomial equations with coefficients in K. The resulting system of polynomials yields a closed subvariety in K^{nr}, which we denote by $\mathrm{R}_{L/K}(X)$ and we have $\mathrm{R}_{L/K}(X)(K) \simeq X(L)$ (cf. [4, A.5]). The construction we just described is called the *restriction of scalars* (or the *Weil restriction*) of X with respect to L/K and one can show that it does not depend on the choice of basis up to K-isomorphism. For a more detailed exposition of Weil restriction, we refer the reader to [14, Ch. 2, §2.1.2] and to [4, A.5]. Our next example explains both the procedure of restricting scalars and how it produces an important class of tori called quasi-split tori

Example 2.2.2 Let $L = K(\sqrt{d})$ be a quadratic extension of K and let $T = \mathbb{G}_m$ be

the 1-dimensional split torus over L. Consider the natural basis $\{1, \sqrt{d}\}$ of L over K and let $\rho\colon L \to M_2(K)$ be the left regular representation. By definition, ρ sends any element l of L to the matrix of left multiplication $x \mapsto lx$. Write $l = a + b\sqrt{d}$ for some $a, b \in K$ and observe that the matrix corresponding to l is of the form

$$\mathfrak{t}(a,b) := \begin{pmatrix} a & bd \\ b & a \end{pmatrix}.$$

The torus T is defined by a single polynomial equation $f(x_1, x_2) = x_1x_2 - 1$ over L. Now if we write $x_1 = \mathfrak{t}(y_1, y_2)$ and $x_2 = \mathfrak{t}(y_3, y_4)$ with $y_1, y_2, y_3, y_4 \in K$ and plug into the original equation defining T then after equating coefficients we obtain the system of two equations over K

$$\begin{cases} y_1y_3 + y_2y_4 = 1 \\ y_1y_4 + y_2y_3 = 0 \end{cases}$$

After solving this system we see that the resulting algebraic group $\mathrm{R}_{L/K}(T) = \mathrm{R}_{L/K}(\mathbb{G}_m)$ has the following set of K-points

$$\mathrm{R}_{L/K}(\mathbb{G}_m)(K) = \left\{ (y_1, y_2) \in K^2 \;\middle|\; (y_1, y_2) \neq (0,0) \right\} \simeq \mathbb{G}_m(L) = L^\times.$$

Furthermore, $\mathrm{R}_{L/K}(\mathbb{G}_m)$ is a 2-dimensional K-torus. In fact, if we denote by $\mathfrak{s}$ the matrix $\begin{pmatrix} \frac{1}{2\sqrt{d}} & \frac{1}{2} \\ \frac{-1}{2\sqrt{d}} & \frac{1}{2} \end{pmatrix}$ then it is easy to see that for any $\mathfrak{t}(a,b) \in \mathrm{R}_{L/K}(\mathbb{G}_m)$ we have

$$\mathfrak{s}\mathfrak{t}(a,b)\mathfrak{s}^{-1} = \begin{pmatrix} \frac{1}{2\sqrt{d}} & \frac{1}{2} \\ \frac{-1}{2\sqrt{d}} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} a & bd \\ b & a \end{pmatrix} \begin{pmatrix} \frac{1}{2\sqrt{d}} & \frac{1}{2} \\ \frac{-1}{2\sqrt{d}} & \frac{1}{2} \end{pmatrix}^{-1} = \begin{pmatrix} a + b\sqrt{d} & 0 \\ 0 & a - b\sqrt{d} \end{pmatrix}.$$

In particular, we see that the torus $\mathrm{R}_{L/K}(\mathbb{G}_m)$ splits over L but not over K. Alternatively, one can compute the characteristic polynomial of $\mathfrak{t}(a,b)$ to obtain two distinct eigenvalues, $a+b\sqrt{d}$ and $a-b\sqrt{d}$.

In our example an explicit computation showed that the group of K-points of $\mathrm{R}_{L/K}(\mathbb{G}_m)$ coincides with the group of L-points of $\mathbb{G}_m$. More generally, if E/K is a finite separable extension and G is any algebraic E-group then $G' := \mathrm{R}_{E/K}(G)$ is an algebraic K-group such that for any K-algebra A there is a natural group isomorphism $G'(A) \simeq G(A \otimes_K E)$ (cf. [4, A.5] and [14, Ch. 2, §2.1.2])). In particular, for the 1-dimensional split E-torus $\mathbb{G}_m$ and $T = \mathrm{R}_{E/K}(\mathbb{G}_m)$ we have $T(K) = E^\times$. Observe that for any finite separable extension E/K the group $\mathrm{R}_{E/K}(\mathbb{G}_m)$ is a K-torus of dimension $[E:K]$.

Definition 2.2.3 Any finite product of K-tori of the form $\mathrm{R}_{E/K}(\mathbb{G}_m)$ where E/K is a finite separable extension is called a *quasi-split* K-torus.

To every torus $T = \mathrm{R}_{L/K}(\mathbb{G}_m)$ one can associate a subtorus called the norm torus constructed as follows. Denote by φ the restriction of the determinant map to T. In other words, we can view φ as a K-morphism $T \to \mathbb{G}_m$. On the level of K-points φ is precisely the norm map $\varphi_K = N_{L/K} : L^\times \to K^\times$. We define the *norm torus* associate with the extension L/K to be the kernel of φ and denote it by $\mathrm{R}^{(1)}_{L/K}(\mathbb{G}_m)$. Observe that if $L = K(\sqrt{d})$ is a quadratic extension of K then the group $\mathrm{R}^{(1)}_{L/K}(\mathbb{G}_m)$ consists precisely of all matrices $\mathfrak{t}(a,b)$ such that $a^2 - db^2 = 1$.

2.2.2 G-modules, characters and co-characters of a torus

Let G be a group. We begin this section by introducing the notion of an abstract G-module but we will be mostly interested in the special case when G is the Galois group of some (possibly infinite) Galois extension. Then we consider two important

examples of G-modules associated with a torus, namely its groups of characters and co-characters.

Definition 2.2.4 Let G be an abstract group. An abelian group A (written additively), is a *G-module* if G acts on A by automorphisms. This amounts to the following three properties:

(1) $1_G \cdot a = a$ for all $a \in A$,

(2) $g_1(g_2 a) = (g_1 g_2)a$ for all $a \in A$, $g_1, g_2 \in G$,

(3) $g(a + b) = ga + gb$ for all $g \in G$, $a, b \in A$.

Alternatively, one can say that a G-module is a unital module over the integral group ring $\mathbb{Z}[G]$. For any two G-modules A and B, we say that a map $f\colon A \to B$ is a *G-module homomorphism* if it is a group homomorphism, which commutes with the action of G or equivalently, f is a homomorphism of $\mathbb{Z}[G]$-modules.

The most important examples of G-modules for us are the ones where G is a Galois group; these are called *Galois modules*.

Example 2.2.5 Let K be any field and let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Then both the additive group L^+ and the multiplicative group $L^\times$ are clearly G-modules. Furthermore, it is easy to see that given $a \in L$, the left multiplication map $\lambda_a\colon L^+ \to L^+$, $x \mapsto ax$, is a G-module homomorphism if and only if $a \in K$. On the other hand, observe that the squaring map $\sigma\colon L^\times \to L^\times$, $x \mapsto x^2$, is always a G-module homomorphism.

Let G be a finite (or profinite) group acting on a set A. In the case of profinite G, we endow A with discrete topology and the action of G on A is called *continuous* if the stabilizer of every element of A in G is open. If the action of G on A is

continuous, then we say that A is a *G-set*. Furthermore, if A is additionally a group (possibly nonabelian) and G acts on A by automorphisms then we say that A is a *G-group*. Now we will see how Example 2.2.5 can be extended to obtain more examples of G-sets

Example 2.2.6 Let again L/K be a finite Galois extension with $G = \mathrm{Gal}(L/K)$. Fix a polynomial $f \in K[x_1, \ldots, x_n]$, and consider the set of its zeros in the n-dimensional affine space over L

$$\mathcal{V}_L(f) = \Big\{(a_1, \ldots, a_n) \in L^n \;\Big|\; f(a_1, \ldots, a_n) = 0\Big\}.$$

For any $\sigma \in G$ and any $(a_1, \ldots, a_n) \in L^n$ we have

$$\sigma \cdot (f(a_1, \ldots, a_n)) = f(\sigma(a_1), \ldots, \sigma(a_n)),$$

so G acts on $\mathcal{V}_L(f)$ by the rule $(\sigma, (a_1, \ldots, a_n)) \mapsto (\sigma(a_1), \ldots, \sigma(a_n))$, making $\mathcal{V}_L(f)$ into a G-set. More generally, if we have a (possibly infinite) family $\mathcal{F} = \{f_\alpha\}_\alpha$ of polynomials $f_\alpha \in K[x_1, \ldots, x_n]$, then the set of their common zeros $\mathcal{V}_L(\mathcal{F}) = \bigcap_{f_\alpha \in \mathcal{F}} \mathcal{V}_L(f_\alpha)$ in L^n is a G-set.

Let us specialize the construction from Example 2.2.6 as follows. Let $G = \mathrm{Gal}(L/K)$ be as above. Consider the nonabelian group $\mathrm{GL}_n(L)$ and observe that the rule $\sigma \cdot (a_{ij}) = (\sigma(a_{ij}))$ for $\sigma \in G$, $(a_{ij}) \in \mathrm{GL}_n(L)$, defines a natural action of G on $\mathrm{GL}_n(L)$ by group automorphisms, making $\mathrm{GL}_n(L)$ into a (noncommutative) G-group. Now, suppose $A \subset \mathrm{GL}_n(L)$ is a commutative subgroup defined by polynomials with coefficients in K. In other words, suppose that there exists a family

of polynomials $\mathcal{F} = \{f_\alpha\}_\alpha$ in $K[x_{11}, x_{12}, \ldots, x_{nn}]$ such that

$$A = \Big\{(a_{ij}) \in \mathrm{GL}_n(L) \,\Big|\, f_\alpha((a_{ij})) = 0 \ \text{ for all } f_\alpha \in \mathcal{F}\Big\}.$$

Combining this with our considerations in Example 2.2.6, we see that A is a G-module for the natural action described above. To have a more concrete example, consider the following

Example 2.2.7 Fix $d \in L^\times$ and consider the set M of all matrices of the form $\mathfrak{t}(a,b) = \begin{pmatrix} a & bd \\ b & a \end{pmatrix} \in \mathrm{GL}_2(L)$. The set M is clearly given by polynomial equations with coefficients in L and one easily checks that it is an abelian subgroup of $\mathrm{GL}_2(L)$. This makes M into a G-module. Observe that if $d \in L^\times \setminus L^{\times 2}$ then $M = \mathrm{R}_{L(\sqrt{d})/L}(\mathbb{G}_m)(L)$ (cf. section 2.2.1). Moreover, the determinant map $\begin{pmatrix} a & bd \\ b & a \end{pmatrix} \mapsto a^2 - db^2$ yields a G-module homomorphism $\det\colon M \to L^\times$. We also note that the kernel of this homomorphism given by $\left\{ \begin{pmatrix} a & bd \\ b & a \end{pmatrix} \in \mathrm{GL}_2(L) \,\middle|\, a^2 - db^2 = 1 \right\}$ yields another example of G-module and if additionally we have $d \in L^\times \setminus L^{\times 2}$, then this G-module is exactly the norm torus $\mathrm{R}^{(1)}_{L(\sqrt{d})/L}(\mathbb{G}_m)(L)$ (cf. section 2.2.1).

With any algebraic torus T one can associate an important group, called the group of characters defined as follows:

Definition 2.2.8 A *character* of a torus T is a morphism of algebraic groups $\chi\colon T \to \mathbb{G}_m$. The set of all characters of T is an abelian group under the operation

$$(\chi_1 + \chi_2)(t) := \chi_1(t) \cdot \chi_2(t)$$

and we denote this group by $X(T)$.

Note that if $T = \mathbb{G}_m$ then any character $\chi \in X(T)$ is of the form $t \mapsto t^k$ for a unique integer k. More generally, if $T = \mathbb{G}_m^d$ then any character $\chi \in X(T)$ is of the form $(t_1, \ldots, t_d) \mapsto t_1^{n_1} \cdots t_d^{n_d}$ for unique integers $n_1, \ldots, n_d$. Thus, for any d-dimensional torus T there is an isomorphism of abelian groups $X(T) \simeq \mathbb{Z}^d$; in particular, $X(T)$ is a finitely generated torsion-free $\mathbb{Z}$-module.

Let $\bar{K}$ be a fixed separable closure of K and let Γ denote the *absolute Galois group* $\mathrm{Gal}(\bar{K}/K)$. If T is K-torus then there is a natural continuous action of Γ on $X(T)$ given by

$$\Gamma \times X(T) \to X(T)$$

$$(\sigma, \chi) \mapsto \sigma \cdot \chi,$$

where

$$\sigma \cdot \chi(t) = \sigma_{\mathbb{G}_m} \circ \chi \circ \sigma_T^{-1}(t)$$

for any $\sigma \in \mathcal{G}, \chi \in X(T)$ and $t \in T$. Here $\sigma_{\mathbb{G}_m}$ and σ_T denote the natural maps induced by σ on $\bar{K}$-points of algebraic groups $\mathbb{G}_m$ and T, respectively. With respect to this action $X(T)$ becomes a discrete module over the profinite group Γ.

Definition 2.2.9 An algebraic K-torus T is called *K-split* if there is an isomorphism $T \simeq \mathbb{G}_m^d$ defined over K.

It is easy to see that a torus T is K-split if and only if any of the following equivalent conditions holds

(1) All characters of T are defined over K,

(2) For some (or equivalently any) faithful K-defined representation $\rho\colon T \to \mathrm{GL}_n$, the group $\rho(T)$ is diagonalizable over K, i.e. it is conjugate to a subgroup of diagonal $(n \times n)$-matrices by a matrix from $\mathrm{GL}_n(K)$,

(3) The absolute Galois group Γ acts trivially on $X(T)$.

Definition 2.2.10 A K-torus T is called *anisotropic* if it has no characters defined over K.

For example, if L/K is a finite separable extension then the corresponding norm torus $\mathrm{R}^{(1)}_{L/K}(\mathbb{G}_m)$ is anisotropic (cf. [15, Ch. 2, §2.1.7, Example]).

In general, for any K-torus T one can find a finite separable extension P/K such that T *splits* over P, namely T is diagonalizable over P and any such extension is called a *splitting field* of T. Observe that a field extension P/K is a splitting field for a K-torus T is and only if the characters of T are defined over P. It turns out that one can always find a finite Galois splitting field. More precisely, we have the following

Proposition 2.2.11 *Let T be a K-torus. There is a finite Galois extension P/K such that T splits over P.*

Proof. Let T be a K-torus of dimension d and let $\chi_1, \ldots, \chi_d$ be a $\mathbb{Z}$-basis of $X(T)$. Denote by H_i the stabilizer of χ_i in Γ for each $i = 1, \ldots, d$. Set $H := \bigcap_{i=1}^{d} H_i$. Since the action of Γ on $X(T)$ is continuous, each stablilizer H_i is an open subgroup. Thus, H is also an open subgroup of Γ. By construction, H acts trivially on $X(T)$ so it is also a normal subgroup of Γ. Since Γ is profinite and H is open, we have $[\Gamma : H] < \infty$. By Galois theory, the subgroup H corresponds to some finite Galois extension P/K with $P \subset \bar{K}$ and $H = \mathrm{Gal}(\bar{K}/P)$ acts trivially on $X(T)$, so P/K furnishes the required splitting field for T.

□

In particular, we see that any torus T has a *minimal* splitting field which is a finite Galois extension of K. An important consequence of this observation is that any K-torus T admits a decomposition as an almost direct product of a maximal

anisotropic K-subtorus and a maximal split K-subtorus. More precisely, we have the following

Theorem 2.2.12 *Let T be a K-torus. There exist the largest anisotropic subtorus $T_a \subset T$ defined over K and the largest split subtorus $T_s \subset T$ defined over K such that T is an almost direct product of T_a and T_s, i.e. $T = T_a \cdot T_s$ and $T_a \cap T_s$ is finite.*

For the proof of Theorem 2.2.12 in the case of an arbitrary K-torus, we refer the reader to [1, Ch. III, §8.15, Proposition]. Here we would like to demonstrate how to find the required decomposition in the special case of a quasi-split torus associated with a quadratic extension. For this we will need the notion of complete reducibility from representation theory and Maschke's theorem

Definition 2.2.13 Let G be an abstract group and let V be a vector space over a field K. A representation $\rho\colon G \to \mathrm{GL}(V)$ is called *completely reducible* (or *semi-simple*) if for any G-invariant subspace $W \subset V$ there exists another G-invariant subspace $W' \subset V$ such that

$$V = W \oplus W'.$$

Theorem 2.2.14 (Maschke) *Let G be a finite group. Then every representation $\rho\colon G \to \mathrm{GL}(V)$ on a finite dimensional vector space V over a field K of characteristic not dividing the order of G, is completely reducible.*

Proof. Cf. [10, Ch. XVIII, §1, Theorem 1.2]. □

Example 2.2.15 Let $L = K(\sqrt{d})$ be a quadratic extension of K with the corresponding Galois group $G = \mathrm{Gal}(L/K)$ and let $T = \mathrm{R}_{L/K}(\mathbb{G}_m)$. Recall that any element of T can be represented by a matrix $\mathfrak{t}(a,b) = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}$. First, let us explicitly describe the group of characters of T. As we saw earlier $\mathfrak{t}(a,b)$ can be

diagonalized to $\begin{pmatrix} a+b\sqrt{d} & 0 \\ 0 & a-b\sqrt{d} \end{pmatrix}$, which yields the natural $\mathbb{Z}$-basis $\{\chi_1, \chi_2\}$ of $X(T)$, where $\chi_1 \colon \mathfrak{t}(a,b) \mapsto a+b\sqrt{d}$ and $\chi_2 \colon \mathfrak{t}(a,b) \mapsto a-b\sqrt{d}$. Set $V := X(T) \otimes_{\mathbb{Z}} \mathbb{Q}$, so that V is a $\mathbb{Q}$-vector space with natural Galois action of G via the first component. Since G is finite, by Theorem 2.2.14, we can write

$$V = V^G \oplus W,$$

where V^G denotes the subspace of G-fixed points of V and W is a G-invariant complement to V^G. Set $X_1 := V^G \cap X(T)$ and $X_2 := W \cap X(T)$. It is easy to see that X_1 is spanned by $\chi_1+\chi_2$ and X_2 is spanned by $\chi_1-\chi_2$. Set $T_a := \ker(\chi_1+\chi_2)$. Then

$$\begin{aligned} T_a &= \Big\{ \mathfrak{t}(a,b) \in T \;\Big|\; (\chi_1+\chi_2)(\mathfrak{t}(a,b)) = 1 \Big\} \\ &= \Big\{ \mathfrak{t}(a,b) \in T \;\Big|\; \chi_1(\mathfrak{t}(a,b)) \cdot \chi_2(\mathfrak{t}(a,b)) = 1 \Big\} \\ &= \Big\{ \mathfrak{t}(a,b) \in T \;\Big|\; a^2 - b^2 d = 1 \Big\} \\ &= \mathrm{R}^{(1)}_{L/K}(\mathbb{G}_m) \end{aligned}$$

Clearly, T_a is an anisotropic K-torus. On the other hand, if we set $T_s := \ker(\chi_1-\chi_2)$ then

$$T_s = \Big\{ \mathfrak{t}(a,b) \in T \;\Big|\; \chi_1(\mathfrak{t}(a,b)) = \chi_2(\mathfrak{t}(a,b)) \Big\} = \Big\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \;\Big|\; a \in K^\times \Big\},$$

which is a K-split torus.

Let us now observe that the natural Galois action on the group of characters is given by the same formula as the standard action of Galois group on polynomials,

i.e. it is the usual action on coefficients. If L/K is a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$ and $L[x_1, \ldots, x_n]$ is the polynomial ring in n variables with coefficients in L then the standard action of G on $L[x_1, \ldots, x_n]$ is defined as follows. Let $\sigma \in G$ and let $f(x_1, \ldots, x_n) = \sum_{i_1,\ldots,i_n} c_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n} \in L[x_1, \ldots, x_n]$. Then for any $(a_1 \ldots, a_n) \in L^n$ the action of σ on $f(a_1, \ldots, a_n)$ is given by $\sigma \cdot f(a_1 \ldots, a_n) := \sigma(f(\sigma^{-1}(a_1, \ldots, a_n)))$. Observe that this is the exact same formula as for the Galois action on the group of characters we defined above. It is often called the natural *action on coefficients* because we have

$$\sigma \cdot f(a_1 \ldots, a_n) = \sigma\Big(\sum_{i_1,\ldots,i_n} c_{i_1 \ldots i_n} \sigma^{-1}(a_1)^{i_1} \cdots \sigma^{-1}(a_n)^{i_n} \Big) = \sum_{i_1,\ldots,i_n} \sigma(c_{i_1 \ldots i_n}) a_1^{i_1} \cdots a_n^{i_n}.$$

Definition 2.2.16 Any free finitely generated $\mathbb{Z}$-module which has a basis that is permuted by the action of the absolute Galois group is called a *permutation module*.

For example, the group of characters of a quasi-split torus associated with a quadratic extension is a permutation module. More precisely, let $L = K(\sqrt{d})$ be a quadratic extension with $\mathcal{G} = \mathrm{Gal}(L/K) = \{1, \sigma\}$ and let $T = \mathrm{R}_{L/K}(\mathbb{G}_m)$. Recall that $X(T)$ has a natural $\mathbb{Z}$-basis $\{\chi_1, \chi_2\}$ where $\chi_1(\mathfrak{t}(a, b)) = a + b\sqrt{d}$ and $\chi_2(\mathfrak{t}(a, b)) = a - b\sqrt{d}$. It is easy to see that σ permutes χ_1 with χ_2 so $X(T)$ may be identified with the permutation module $\mathbb{Z}[\mathcal{G}]$.

More generally, let L/K be any finite separable extension of degree $d \geq 2$ and let $T = R_{L/K}(\mathbb{G}_m)$. Choose a basis $\chi_1, \ldots, \chi_d$ of $X(T)$. Let P be the normal closure of L over K, so that P is the minimal splitting field of T. Let $\mathcal{G} = \mathrm{Gal}(P/K)$ and $\mathcal{H} = \mathrm{Gal}(P/L)$. Then $\mathcal{G}$ acts transitively on $X(T)$ and $\mathcal{H}$ acts trivially on $X(T)$. Choose a system of coset representatives $\sigma_1\mathcal{H}, \ldots, \sigma_d\mathcal{H}$ for $\mathcal{G}/\mathcal{H}$. Then we have the

isomorphism of $\mathbb{Z}[\mathcal{G}]$-modules

$$\mathbb{Z}[\mathcal{G}/\mathcal{H}] \to X(T) \tag{2.1}$$

$$\sum_{i=1}^{d} n_i \sigma_i \mathcal{H} \mapsto \sum_{i=1}^{d} n_i \sigma_i \cdot \chi_i,$$

where $n_i \in \mathbb{Z}$. In fact, this isomorphism extends to a bijective correspondence between all permutation modules and all quasi-split tori (cf. [15, Ch. 2, §2.1.7]).

Now let G be an arbitrary algebraic group. We will consider tori contained in G. Since G has finite dimension, it always has *maximal tori*. Moreover, any two maximal tori in G are conjugate (cf. [1, Ch. V, §19, Theorem 19.2]). In particular, the dimension of a maximal torus in G is well-defined and we call it the (*absolute*) *rank* of G and denote it by $\operatorname{rk} G$. If G is defined over K then there is always a maximal K-torus T in G (cf. [1, Ch. V, §18, Theorem 18.2]). We say that G is *K-split* if there exists a maximal torus $T \subset G$ which is K-split. Observe that since any two maximal K-split tori in G are conjugate over K, the dimension of a maximal K-split torus of G is well-defined and we call it the *K-rank of G* and denote it by $\operatorname{rk}_K G$. If $\operatorname{rk}_K G > 0$ then we say that G is *K-isotropic* (otherwise G is *K-anisotropic*). Clearly, GL_n and SL_n are both K-isotropic groups. An important example of anisotropic group is $\mathrm{SL}_1(D)$ which consists of all those elements of a finite dimensional central division K-algebra D which have reduced norm one (cf. [15, Ch. 1, §1.4.1]).

For every torus one can define a notion which is dual to the notion of group of characters, called the group of co-characters

Definition 2.2.17 Let T be a torus. Any group homomorphism $\mathbb{G}_m \to T$ is called a *co-character* of T. The group of co-characters $\operatorname{Hom}(\mathbb{G}_m, T)$ will be denoted by

$X_*(T)$.

For any $\varphi \in X_*(T)$ and $\chi \in X(T)$, the composition $\chi \circ \varphi$ is a map $\mathbb{G}_m \to \mathbb{G}_m$, so it must be of the form $(\chi \circ \varphi)(z) = z^k$ for a unique integer k, which we denote by $\langle \varphi, \chi \rangle$. We obtain a well-defined map $X_*(T) \times X(T) \to \mathbb{Z}$, given by $(\varphi, \chi) \mapsto \langle \varphi, \chi \rangle$, which can easily be seen to be nondegenerate. This map, called the *natural pairing* (of characters and co-characters) allows to identify $X_*(T)$ with $\mathrm{Hom}(X(T), \mathbb{Z})$.

We will now compute explicit formulas for the dual bases of co-characters of a quasi-split torus associated with a quadratic extension and the corresponding norm torus.

Example 2.2.18 Let $L = K(\sqrt{d})$ be a quadratic extension of K and let $T = \mathrm{R}_{L/K}(\mathbb{G}_m)$. Let $\{\chi_1, \chi_2\}$ be the natural basis for $X(T)$ that we saw earlier. We construct a dual basis $\{\chi_1^*, \chi_2^*\}$ of co-characters $\mathbb{G}_m \to T$. The map χ_1^* must be of the form $u \mapsto \mathfrak{t}(x(u), y(u))$. Using the natural pairing, we see that we must have

$$\chi_1 \circ \chi_1^*(u) = u^1 = u = x(u) + y(u)\sqrt{d}$$

and

$$\chi_2 \circ \chi_1^*(u) = u^0 = 1 = x(u) - y(u)\sqrt{d}.$$

This yields two equations with two variables $x(u), y(u)$ and after solving, we obtain

$$x(u) = \frac{u+1}{2}, \quad y(u) = \frac{u-1}{2\sqrt{d}}.$$

Hence, χ_1^* is given by the matrix $\chi_1^*(u) = \mathfrak{t}(\frac{u+1}{2}, \frac{u-1}{2\sqrt{d}})$. Similarly, one can verify that the conditions $\chi_1 \circ \chi_2^*(u) = 1$ and $\chi_2 \circ \chi_2^*(u) = u$ yield the formula for the other co-character $\chi_2^*(u) = \mathfrak{t}(\frac{u+1}{2}, \frac{1-u}{2\sqrt{d}})$. For completeness, let us also check that χ_1^* is a

group homomorphism. For $u, v \in \mathbb{G}_m$ we compute

$$\chi_1^*(u)\chi_1^*(v) = \mathfrak{t}\Big(\frac{u+1}{2}, \frac{u-1}{2\sqrt{d}}\Big) \cdot \mathfrak{t}\Big(\frac{v+1}{2}, \frac{v-1}{2\sqrt{d}}\Big) = \mathfrak{t}\Big(\frac{uv+1}{2}, \frac{uv-1}{2\sqrt{d}}\Big) = \chi_1^*(uv).$$

Similarly, χ_2^* is a group homomorphism.

Example 2.2.19 Let $L = K(\sqrt{d})$ be a quadratic extension of K and let $T = \mathrm{R}^{(1)}_{L/K}(\mathbb{G}_m)$. Let $\chi_0 \colon T \to \mathbb{G}_m$ be the character of T given by $\chi_0(\mathfrak{t}(a,b)) = a + b\sqrt{d}$, where $a^2 - b^2 d = 1$. The dual co-character $\chi_0^* \colon \mathbb{G}_m \to T$ is of the form $u \mapsto \mathfrak{t}(x(u), y(u))$ for some functions $x(u), y(u)$. The natural pairing and norm one condition yield the following two equations

$$\chi_0 \circ \chi_0^*(u) = u = x(u) + y(u)\sqrt{d}$$

$$x(u)^2 - y(u)^2 d = 1.$$

After solving for $x(u)$ and $y(u)$, we obtain

$$x(u) = \frac{u^2+1}{2u}, \quad y(u) = \frac{u^2-1}{2u\sqrt{d}}.$$

Hence the dual co-character χ_0^* is given by the matrix $\chi_0^*(u) = \mathfrak{t}(\frac{u^2+1}{2u}, \frac{u^2-1}{2u\sqrt{d}})$.

Now let T be any K-torus. Similarly to the group of characters, there is a natural action of the absolute Galois group $\Gamma = \mathrm{Gal}(\bar{K}/K)$ on $X_*(T)$:

$$\Gamma \times X_*(T) \to X_*(T),$$

$$(\sigma, \varphi) \mapsto \sigma \cdot \varphi,$$

where

$$(\sigma \cdot \varphi)(t) = \sigma_T \circ \varphi \circ \sigma_{\mathbb{G}_m}^{-1}(t),$$

for $\sigma \in \Gamma, \varphi \in X_*(T)$ and $t \in T$. Finally, the natural pairing is Γ-invariant, i.e.

$$\langle \sigma \cdot \varphi, \sigma \cdot \chi \rangle = \langle \varphi, \chi \rangle,$$

for any $\sigma \in \Gamma$, $\varphi \in X_*(T)$ and $\chi \in X(T)$. In fact, we have

$$\begin{aligned} t^{\langle \sigma\cdot\varphi, \sigma\cdot\chi\rangle} &= (\sigma \cdot \chi) \circ (\sigma \cdot \varphi)(t) \\ &= (\sigma_{\mathbb{G}_m} \chi \sigma_T^{-1}) \circ (\sigma_T \varphi \sigma_{\mathbb{G}_m}^{-1})(t) \\ &= \sigma_{\mathbb{G}_m}(\chi \circ \varphi)\sigma_{\mathbb{G}_m}^{-1}(t) \\ &= \sigma_{\mathbb{G}_m} \circ (\sigma_{\mathbb{G}_m}^{-1}(t)^{\langle \varphi, \chi \rangle}) \\ &= \sigma_{\mathbb{G}_m} \circ \sigma_{\mathbb{G}_m}^{-1}(t^{\langle \varphi, \chi \rangle}) \\ &= t^{\langle \varphi, \chi \rangle}. \end{aligned}$$

2.2.3 Equivalence of categories

In this section we state and explore the equivalence between the category of tori and the category of $\mathbb{Z}$-torsion free finitely generated Galois modules. This fact will be crucial for proofs of our results about tori in Chapter 3.

Theorem 2.2.20 *Let $\mathcal{C}$ be the category of K-tori split over a finite Galois extension P/K with Galois group $\mathcal{G} = \mathrm{Gal}(P/K)$ considered with K-morphisms and let $\mathcal{D}$ be the category of $\mathbb{Z}$-torsion free finitely generated $\mathbb{Z}[\mathcal{G}]$-modules with $\mathcal{G}$-equivariant homomorphisms. Then $\Phi\colon \mathcal{C} \to \mathcal{D}$ given by $T \mapsto X(T)$ defines a contravariant equivalence of categories and $\Psi\colon \mathcal{C} \to \mathcal{D}$ given by $T \mapsto X_*(T)$ yields a covariant equivalence of categories.*

Proof. Cf. [1, Ch. III, §8.12, Proposition] and [7, Ch. 16, §16.2].

□

Let us begin by showing how the equivalence of categories $\Phi\colon \mathcal{C} \to \mathcal{D}$ can be used to compute the character module of a norm torus corresponding to a quasi-split torus $\mathrm{R}_{L/K}(\mathbb{G}_m)$

Example 2.2.21 Case 1: L/K quadratic extension

Let $L = K(\sqrt{d})$ be a quadratic extension of K with $\mathcal{G} = \mathrm{Gal}(L/K)$ and let $T = \mathrm{R}_{L/K}(\mathbb{G}_m)$. By definition of the norm torus associated to T, we have the following short exact sequence of tori

$$1 \to \mathrm{R}^{(1)}_{L/K}(\mathbb{G}_m) \to T \xrightarrow{\mathrm{N}} \mathbb{G}_m \to 1,$$

where N denotes the restriction of the determinant map to T. Using the contravariant equivalence of categories $\Phi\colon \mathcal{C} \to \mathcal{D}$, the norm map $\mathrm{N}\colon T \to \mathbb{G}_m$ corresponds to a homomorphism of $\mathbb{Z}[\mathcal{G}]$-modules, $\mathrm{N}^{\#}\colon X(\mathbb{G}_m) \to X(T)$. After identifying $X(\mathbb{G}_m) \simeq \mathbb{Z}$ and $X(T) \simeq \mathbb{Z}[\mathcal{G}]$, we see that the map $\mathrm{N}^{\#}$ is uniquely determined by the value on generator $1 \in \mathbb{Z}$. In fact, for any $t \in T(K) \simeq L^{\times}$, on the level of K-points we have

$$\mathrm{N}^{\#}(1)(t) = 1 \circ N_{L/K}(t) = \chi_1(t) \cdot \chi_2(t) = (\chi_1 + \chi_2)(t) = \mathrm{Tr}_{L/K}(t),$$

where $N_{L/K}$ is the norm map and $\mathrm{Tr}_{L/K}$ denotes the trace map.

Case 2: L/K arbitrary separable extension

Let L/K be any finite separable extension of degree ≥ 2 and let $T = \mathrm{R}_{L/K}(\mathbb{G}_m)$. Let P be the minimal splitting field of T. There is an isomorphism $X(T) \simeq \mathbb{Z}[\mathcal{G}/\mathcal{H}]$ of $\mathbb{Z}[\mathcal{G}]$-modules where $\mathcal{G} = \mathrm{Gal}(P/K)$ and $\mathcal{H} = \mathrm{Gal}(P/L)$ – see (2.1). Then the norm map $\mathrm{N}\colon T \to \mathbb{G}_m$ corresponds to the augmentation map $\mathrm{N}^{\#}\colon \mathbb{Z} \to$

$\mathbb{Z}[\mathcal{G}/\mathcal{H}]$, $1 \mapsto \sum_{g\in\mathcal{G}} g\mathcal{H}$. Hence $X(\mathrm{R}^{(1)}_{L/K}(\mathbb{G}_m)) \simeq \mathbb{Z}[\mathcal{G}/\mathcal{H}]/\mathbb{Z}\xi$ as $\mathbb{Z}[\mathcal{G}]$-modules, where $\xi = \sum_{g\in\mathcal{G}} g\mathcal{H}$.

Let us now illustrate how the equivalence of categories above allows us to classify all tori which split over a quadratic extension:

Remark 2.2.22 Let L/K be a quadratic extension with $\mathcal{G} = \mathrm{Gal}(L/K)$ and let T be a K-torus which splits over L. Since $X(T)$ is finitely generated $\mathbb{Z}[\mathcal{G}]$-module which has no $\mathbb{Z}$-torsion, it can be written in the form:

$$\mathbb{Z}^a \times \mathbb{Z}[\mathcal{G}]^b \times I^c,$$

where I is the kernel of the augmentation map $\mathbb{Z}[\mathcal{G}] \to \mathbb{Z}$ and a, b, c are uniquely determined nonnegative integers (cf. [15, Ch. 2, §2.2.4]). Since T splits over L, using the equivalence of categories (cf. Theorem 2.2.20), we see that T must be isomorphic to

$$(\mathbb{G}_m)^a \times (\mathrm{R}_{L/K}(\mathbb{G}_m))^b \times (\mathrm{R}^{(1)}_{L/K}(\mathbb{G}_m))^c.$$

In particular, for $K = \mathbb{R}$ and $L = \mathbb{C}$ this yields full classification of all $\mathbb{R}$-tori.

For the general construction of the inverse functor $\mathcal{D} \to \mathcal{C}$, we refer the reader to [1, Ch. III, §8.12, Proposition] and [7, Ch. 16, §16.2]. Here we will show in an example how one can recover the structure of a torus from its character module using *Hopf algebras*. If G is a linear algebraic group then one can reformulate the group axioms for G as a set of conditions on its affine algebra $K[G]$. More precisely, the multiplication map $m\colon G \times G \to G$ corresponds to *co-multiplication*

$$\Delta\colon K[G] \to K[G \times G] \simeq K[G] \otimes_K K[G]$$

$$f \mapsto \sum_i g_i \otimes h_i$$

if $f(xy) = \sum_i g_i(x)h_i(y)$. If we view the identity element 1_G of G as a morphism $e\colon \{1_G\} \to G$, then the corresponding *co-unit* is given by

$$\varepsilon\colon K[G] \to K$$

$$f \mapsto f(1_G).$$

The inverse map $\iota\colon G \to G$, corresponds to *co-inverse* map

$$\sigma\colon K[G] \to K[G]$$

$$f \mapsto \sigma(f),$$

where $(\sigma(f))(x) = f(\iota(x)) = f(x^{-1})$. The *co-associativity*, *co-identity* and *co-inverse* axioms in $K[G]$ can be written in terms of the following three commutative diagrams

$$\begin{array}{ccc} K[G] \otimes_K K[G] \otimes_K K[G] & \xleftarrow{\Delta\otimes 1} & K[G] \otimes_K K[G] \\ {\scriptstyle 1\otimes\Delta}\uparrow & & \uparrow{\scriptstyle \Delta} \\ K[G] \otimes_K K[G] & \xleftarrow{\quad\Delta\quad} & K[G] \end{array} \qquad \begin{array}{ccc} K[G] & \xleftarrow{e\otimes 1} & K[G] \otimes_K K[G] \\ {\scriptstyle 1\otimes e}\uparrow & & \uparrow{\scriptstyle \Delta} \\ K[G] \otimes_K K[G] & \xleftarrow{\quad\Delta\quad} & K[G] \end{array}$$

$$\begin{array}{ccc} K[G] & \xleftarrow{\sigma\otimes 1} & K[G] \otimes_K K[G] \\ {\scriptstyle 1\otimes\sigma}\uparrow & & \uparrow{\scriptstyle \Delta} \\ K[G] \otimes_K K[G] & \xleftarrow{\quad\Delta\quad} & K[G] \end{array}$$

Any algebraic variety G is uniquely determined by its affine algebra $K[G]$, so in order to define a structure of an algebraic group on G, we only need to specify maps $\varepsilon, \Delta, \sigma$ such that the three diagrams above commute. This makes $K[G]$ into a *Hopf algebra* with identity (cf. [1, Ch. 1, §1.5] and [7, Ch. II, §7.6])

Example 2.2.23 Let $G = \mathbb{G}_m$. Then $K[G] = K[t, t^{-1}]$ and the maps $\Delta, \varepsilon, \sigma$ are given by the formulas $\Delta(t) = t \otimes t$, $\varepsilon(t) = 1$ and $\sigma(t) = t^{-1}$. Observe that

$$(\Delta \otimes 1) \circ \Delta(t) = (\Delta \otimes 1)(t \otimes t) = t \otimes t \otimes t = (1 \otimes \Delta) \circ \Delta(t).$$

One can similarly verify the commutativity of the other two diagrams. More generally, if $G = \mathrm{GL}_n$ then $K[G] = K[x_{11}, \ldots, x_{nn}, \det(x_{ij})^{-1}]$ and one can show that the maps $\varepsilon(x_{ij}) = \delta_{ij}$, $\Delta(x_{ij}) = \sum_k x_{ik} \otimes x_{kj}$ and $\sigma(x_{ij}) = (-1)^{i+j} \det(x_{ij})^{-1} \cdot \det((x_{kl})_{k \neq j, l \neq i})$ endow $K[G]$ with a Hopf algebra structure (cf. [7, Ch. II, §7.6]).

Let us show how one can construct the inverse of the functor $\Phi \colon \mathcal{C} \to \mathcal{D}$ in a specific example. More precisely, we will illustrate how one can recover the multiplicative structure on a quasi-split torus T associated with a quadratic extension entirely from its character module $X(T)$. The argument uses the Hopf algebra structure on $K[T]$ and we show by explicit computation that it is compatible with multiplication in T.

Example 2.2.24 Let $L = K(\sqrt{d})$ be a quadratic extension with $G = \mathrm{Gal}(L/K)$ and let $T = \mathrm{R}_{L/K}(\mathbb{G}_m)$. Recall that any element of T can be represented by a matrix $\mathfrak{t}(a, b)$ and one easily checks that multiplication in T is given by

$$\mathfrak{t}(a_1, b_1) \cdot \mathfrak{t}(a_2, b_2) = \mathfrak{t}(a_1 a_2 + b_1 b_2 d, a_2 b_1 + a_1 b_2). \tag{2.2}$$

Let $\{\chi_1, \chi_2\}$ be the usual basis of $X(T)$. Since G acts in a natural way on both L and $X(T)$, there is a natural action of G on the group algebra $L[X(T)]$. We will see that the subalgebra of G-fixed points $L[X(T)]^G$ is the required algebra, namely its Hopf algebra structure allows us to recover the multiplicative structure on T given in (2.2).

First, let us show that $L[X(T)]^G = K[\alpha, \beta]$ where $\alpha = \frac{\chi_1+\chi_2}{2}$ and $\beta = \frac{\chi_1-\chi_2}{2\sqrt{d}}$. Clearly, $\alpha, \beta \in L[X(T)]^G$. Any element in $L[X(T)]$ is a finite sum of the form $u = \sum_{i,j\geq 0}(a_{ij} + b_{ij}\sqrt{d})\chi_1^i\chi_2^j$ with $a_{ij}, b_{ij} \in K$. We may regroup the terms of u according to the rule that we put together all the terms with the same sum of indices $i + j$. Let us show by only considering the linear terms, i.e. the case $i + j \leq 1$ that any $u \in L[X(T)]^G$ belongs to $K[\alpha, \beta]$. It will be clear from our computation that the argument generalizes to higher order terms. In fact, let $u = (a_{00} + b_{00}\sqrt{d}) + (a_{10} + b_{10}\sqrt{d})\chi_1 + (a_{01} + b_{01}\sqrt{d})\chi_2$ be an element of $L[X(T)]^G$. Then $\sigma(u) = u$. By equating the coefficients we obtain the system of equations

$$\begin{cases} a_{00} - b_{00}\sqrt{d} = a_{00} + b_{00}\sqrt{d} \\ a_{10} - b_{10}\sqrt{d} = a_{01} + b_{01}\sqrt{d} \\ a_{01} - b_{01}\sqrt{d} = a_{10} + b_{10}\sqrt{d} \end{cases}$$

which yields $b_{00} = 0, a_{10} = a_{01}, b_{10} = -b_{01}$. Thus, $u = a_{00}+a_{10}(\chi_1+\chi_2)+b_{10}\sqrt{d}(\chi_1-\chi_2) = a_{00} + 2a_{10}\alpha + 2db_{10}\beta$ which is an element of $K[\alpha, \beta]$.

Now

$$\alpha(\mathfrak{t}(a, b)) = \frac{1}{2}\chi_1(\mathfrak{t}(a, b)) + \frac{1}{2}\chi_2(\mathfrak{t}(a, b)) = \frac{1}{2}(a + b\sqrt{d}) + \frac{1}{2}(a - b\sqrt{d}) = a$$

and similarly $\beta(\mathfrak{t}(a, b)) = b$. Observe that for any character χ on T we have $\Delta(\chi) = \chi \otimes \chi$. In fact,

$$\Delta(\chi)(g, h) = \chi(m(g, h)) = \chi(gh) = \chi(g)\chi(h) = (\chi \otimes \chi)(g, h).$$

Thus, from the Hopf algebra structure on $L[X(T)]^G$, we obtain that $\Delta(\alpha) = \frac{\chi_1\otimes\chi_1}{2} + \frac{\chi_2\otimes\chi_2}{2}$ and $\Delta(\beta) = \frac{\chi_1\otimes\chi_1}{2\sqrt{d}} - \frac{\chi_2\otimes\chi_2}{2\sqrt{d}}$. On the other hand, from the Hopf algebra structure

on $K[T]$ that comes from multiplication in T, we must have $\Delta(\alpha) = \alpha \otimes \alpha + d\beta \otimes \beta$ and $\Delta(\beta) = \alpha \otimes \beta + \beta \otimes \alpha$ (cf. Example 2.2.23). It remains to check that we have indeed an equality. In fact,

$$\begin{aligned}
\Delta(\alpha) &= \frac{\chi_1 \otimes \chi_1}{2} + \frac{\chi_2 \otimes \chi_2}{2} \\
&= \frac{1}{4}(\chi_1 \otimes \chi_1 + \chi_1 \otimes \chi_2 + \chi_2 \otimes \chi_1 + \chi_2 \otimes \chi_2) + \frac{1}{4}(\chi_1 \otimes \chi_1 - \chi_1 \otimes \chi_2 - \chi_2 \otimes \chi_1 + \chi_2 \otimes \chi_2) \\
&= \frac{\chi_1 + \chi_2}{2} \otimes \frac{\chi_1 + \chi_2}{2} + d \cdot \frac{\chi_1 - \chi_2}{2\sqrt{d}} \otimes \frac{\chi_1 - \chi_2}{2\sqrt{d}} \\
&= \alpha \otimes \alpha + d\beta \otimes \beta
\end{aligned}$$

Similarly, we obtain $\Delta(\beta) = \frac{\chi_1 \otimes \chi_1}{2\sqrt{d}} - \frac{\chi_2 \otimes \chi_2}{2\sqrt{d}} = \alpha \otimes \beta + \beta \otimes \alpha$. Thus, we recovered the multiplicative structure on the torus T from the Hopf algebra structure on $L[X(T)]^G$, as claimed.

We will end this section with one more application of our equivalence of categories. The functor Ψ in Theorem 2.2.20 can be used to show that any torus may be covered by a quasi-split torus in the sense of certain exact sequence of tori. While the existence of this sequence is well-known, here we establish an explicit upper bound on the dimension of the tori appearing in that sequence. We will need the following definition

Definition 2.2.25 Any integral-valued function $\psi(d)$ defined on integers $d \geq 1$ is called *super-increasing* if for any $1 \leq d_1 \leq d_2$ we have that $\psi(d_1)|\psi(d_2)$, i.e. $\psi(d_1)$ divides $\psi(d_2)$.

The equivalence of categories Ψ can be used to obtain the following

Proposition 2.2.26 *Let T be a torus of dimension d defined over an arbitrary field K, and let P be the minimal splitting field of T. Then there is an exact sequence of*

K-tori and K-defined morphisms

$$1 \to T_1 \longrightarrow T_0 \xrightarrow{\pi} T \to 1,$$

where T_0 is a product of d copies of $\mathrm{R}_{P/K}(\mathbb{G}_m)$ (hence quasi-split), and $\dim T_1 \leq \lambda(d)$, with λ being an explicit increasing function on integers $d \geq 1$.

Proof. Let $\mathcal{G} = \mathrm{Gal}(P/K)$. Being a free abelian group of rank d, the group of co-characters $X_*(T) = \mathrm{Hom}(X(T), \mathbb{Z})$ can be generated by d elements as $\mathbb{Z}[\mathcal{G}]$-module, and therefore there exists an exact sequence of $\mathbb{Z}[\mathcal{G}]$-modules of the form

$$0 \to Y \longrightarrow \mathbb{Z}[\mathcal{G}]^d \longrightarrow X_*(T) \to 0.$$

Using the functor Ψ from Theorem 2.2.20 we obtain the corresponding exact sequence of K-tori and K-morphisms

$$1 \to T_1 \longrightarrow T_0 \longrightarrow T \to 1,$$

with $X_*(T_1) = Y$ and $X_*(T_0) = \mathbb{Z}[\mathcal{G}]^d$. Then $T_0 \simeq \mathrm{R}_{P/K}(\mathbb{G}_m)^d$, and it remains to estimate $\dim T_1$ in terms of d. We have $X(T) \simeq \mathbb{Z}^d$ as abelian groups, and hence the action of $\mathcal{G}$ on $X(T)$ gives rise to a representation $\mathcal{G} \to \mathrm{GL}_d(\mathbb{Z})$. Furthermore, the fact that P is the *minimal* splitting field of T implies that this representation is *faithful*, i.e. $\mathcal{G}$ is isomorphic to a subgroup of $\mathrm{GL}_d(\mathbb{Z})$. It follows from the reduction theory for arithmetic groups (cf. [15, Theorem 4.9]) that $\mathrm{GL}_d(\mathbb{Z})$ has finitely many conjugacy classes of finite subgroups, so there is an integer $\gamma(d)$ depending only on d such that the order of every finite subgroup of $\mathrm{GL}_d(\mathbb{Z})$ divides $\gamma(d)$. In fact, one can give an explicit bound $\gamma(d)$ by using Minkowski's Lemma (cf. [15, Ch. 4, §4.8, Lemma 4.63]), according to which for any prime $p > 2$, the kernel of the reduction

map $\rho_p\colon \mathrm{GL}_d(\mathbb{Z}) \to \mathrm{GL}_d(\mathbb{Z}/p\mathbb{Z})$ (in other words, the *congruence subgroup of level* p) is torsion-free, and consequently, the order of every finite subgroup of $\mathrm{GL}_d(\mathbb{Z})$ divides $|\mathrm{GL}_d(\mathbb{Z}/p\mathbb{Z})|$. Using $p = 3$, we see that one can take

$$\gamma(d) := |\mathrm{GL}_d(\mathbb{Z}/3\mathbb{Z})| = \prod_{i=0}^{d-1}(3^d - 3^i) \tag{2.3}$$

(obviously, this function is super-increasing). Since the order of $\mathcal{G}$ divides $\gamma(d)$ we have that

$$\dim T_1 = \dim T_0 - \dim T = (|\mathcal{G}| - 1)d,$$

so one can take $\lambda(d) := d(\gamma(d) - 1)$. □

Similarly one can use the contravariant functor Φ in Theorem 2.2.20 to show that any torus T may be embedded into a quasi-split torus. In other words, we have the following

Proposition 2.2.27 *Let T be a torus defined over an arbitrary field K, and let P be the minimal splitting field of T. Then there is an exact sequence of K-tori and K-defined morphisms*

$$1 \to T \to T_0 \to T' \to 1,$$

where T_0 is a quasi-split torus, and both tori T' and T_0 split over P.

Proof. Cf. [15, Ch. 2, §2.1.7, Proposition 2.2]. □

2.3 Cohomology

2.3.1 Cohomology groups in lower dimensions

We start this section by introducing cohomology groups in dimensions 0 and 1. Next, we prove a few finiteness results for H^1. These facts will be used in proofs in

Chapter 3. Let G be an abstract group and let A be a G-module. We let A^G denote the subgroup of *G-fixed points* in A, i.e. $A^G = \{a \in A \mid ga = a \text{ for all } g \in G\}$ and set $H^0(G, A) := A^G$. It is clear that for any G-module homomorphism $f\colon A \to B$ we have $f(A^G) \subset B^G$. In other words, the correspondence $A \mapsto H^0(G, A) = A^G$ defines a functor, called the *functor of G-fixed points* from the category of G-modules to the category of abelian groups. The introduction of higher cohomology groups is motivated by the analysis of exactness properties of this functor. More precisely, let

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

be an exact sequence of G-modules and G-homomorphisms. Then the induced sequence

$$0 \to A^G \xrightarrow{\alpha} B^G \xrightarrow{\beta} C^G$$

is also exact. We express this by saying that the fixed point functor is *left-exact*. However, the sequence $0 \to A^G \xrightarrow{\alpha} B^G \xrightarrow{\beta} C^G \to 0$ is not necessarily exact, namely the fixed point functor is not right-exact in general. In fact, consider the following example

Example 2.3.1 Let $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. We then have the following exact sequence of G-modules and G-module homomorphisms

$$1 \to \mu_2 \to \mathbb{C}^\times \xrightarrow{[2]} \mathbb{C}^\times \to 1,$$

where $\mu_2 = \{\pm 1\}$ and $[2]$ denotes the squaring map. After passing to G-fixed points, we obtain the sequence

$$1 \to \mu_2 \to \mathbb{R}^\times \xrightarrow{[2]} \mathbb{R}^\times \to 1,$$

which is not exact because the image of $\mathbb{R}^\times$ in the squaring map [2] equals $\mathbb{R}^{\times 2} = \mathbb{R}_{>0} \neq \mathbb{R}^\times$.

The cohomology groups $H^1(G, \cdot)$ are introduced precisely to fix the non-exactness of the functor $H^0(G, \cdot)$. Let G be a group and A a G-module. A function $f\colon G \to A$ is called a 1-*cocycle* if it satisfies the following condition

$$f(g_1 g_2) = f(g_1) + g_1 f(g_2), \quad \text{for all } g_1, g_2 \in G.$$

The set of all 1-cocycles is denoted by $Z^1(G, A)$. A function $f\colon G \to A$ is called a 1-*coboundary* if there exists $a \in A$ such that $f(g) = ga - a$ for all $g \in G$. The set of all 1-coboundaries is denoted by $B^1(G, A)$. Observe that both $Z^1(G, A)$ and $B^1(G, A)$ are subgroups of the abelian group $F^1(G, A)$ of all functions $f\colon G \to A$ with the standard operation given by

$$(f_1 + f_2)(g) = f_1(g) + f_2(g),$$

where $f_1, f_2 \in F^1(G, A)$. It is easy to check that there is an inclusion $B^1(G, A) \subset Z^1(G, A)$. We define $H^1(G, A)$ to be the quotient group $Z^1(G, A)/B^1(G, A)$. For example, if G acts trivially on A then $Z^1(G, A) = \mathrm{Hom}(G, A)$ and $B^1(G, A) = \{0\}$, so $H^1(G, A) = \mathrm{Hom}(G, A)$.

Next, let us discuss functoriality of cohomology. Let G be any group. Then any map $\alpha\colon A \to B$ gives rise to the post-composition map $\alpha^1\colon F^1(G, A) \to F^1(G, B)$, namely $\alpha^1(f) = \alpha \circ f$ for any $f \in F^1(G, A)$. Furthermore, if A and B are both G-modules and α is a homomorphism of G-modules, then one easily checks that $\alpha^1(Z^1(G, A)) \subset Z^1(G, B)$ and $\alpha^1(B^1(G, A)) \subset B^1(G, B)$.

As was mentioned earlier, one motivation for introducing cohomology groups is to fix the problem of nonexactness of the functor of fixed points. More precisely, we

have the following:

Proposition 2.3.2 *Let* $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ *be a short exact sequence of* G*-modules and* G*-homomorphisms. Then there exists a homomorphism* $\delta\colon C^G \to H^1(G, A)$ *of abelian groups such that the sequence*

$$0 \to A^G \xrightarrow{\alpha} B^G \xrightarrow{\beta} C^G \xrightarrow{\delta} H^1(G, A) \xrightarrow{\alpha^1} H^1(G, B) \xrightarrow{\beta^1} H^1(G, C)$$

is exact.

Proof. Here we will only construct δ and check the exactness at $H^1(G, A)$. Let $c \in C^G$. Since β is surjective, there exists $b \in B$ such that $\beta(b) = c$. Define $\widetilde{f}\colon G \to B$ by $\widetilde{f}(g) = gb - b$. Then

$$\beta(\widetilde{f}(g)) = \beta(gb - b) = g(\beta(b)) - \beta(g) = gc - c = 0.$$

Since α is injective, for each $g \in G$ there exists a unique $f(g) \in A$ such that $\alpha(f(g)) = \widetilde{f}(g)$. We claim that the resulting function $f\colon G \to A$ belongs to $Z^1(G, A)$. Indeed, for any $g, h \in G$, we have

$$\alpha(f(gh)) = \widetilde{f}(gh) = (gh)b - b = \widetilde{f}(g) + g\widetilde{f}(h) = \alpha(f(g) + gf(h)).$$

So, $\alpha(f(gh) - (f(g) + gf(h))) = 0$, and therefore $f(gh) = f(g) + gf(h)$, since α is injective. Thus, $f \in Z^1(G, A)$. We define $\delta(c) = f + B^1(G, A) \in H^1(G, A)$. Note that $b \in B$ such that $\beta(b) = c$ is not unique, so we need to make sure that the cohomology class $\delta(c)$ is well-defined, i.e. does not depend on the choice of b. Let $b' \in B$ be another element such that $\beta(b') = c$. Then $\beta(b' - b) = 0$, so there exists

$a \in A$ such that $b' = b + \alpha(a)$. Then for the corresponding function $\widetilde{f'}$, we have

$$\widetilde{f'}(g) = gb' - b' = (gb - b) + \alpha(ga - a) = \widetilde{f}(g) + \alpha(ga - a).$$

Then $f'(g) = f(g) + (ga - a)$ for all $g \in G$. This means that f and f' define the same class in $H^1(G, A)$. It remains to verify the exactness at $H^1(G, A)$. By construction, for $c \in C^G$, the image $\delta(c)$ is the cohomology class given by $f \in Z^1(G, A)$ such that $\alpha(f(g)) = \widetilde{f}(g) = gb - b$. Thus, $\alpha^1(\delta(c)) = 0$, proving the inclusion im $\delta \subset \ker \alpha^1$. Conversely, suppose that for $f \in Z^1(G, A)$, we have $\widetilde{f} := \alpha^1(f) = \alpha \circ f \in B^1(G, B)$, i.e. there exists $b \in B$ such that $\widetilde{f}(g) = \alpha(f(g)) = gb - b$, for all $g \in G$. Put $c = \beta(b) \in C$. Observe that for any $g \in G$, we have

$$gc = g\beta(b) = \beta(gb) = \beta(b + \alpha(f(g))) = \beta(b) = c,$$

so $c \in C^G$. Thus, $\delta(c) = f + B^1(G, A)$ and $\ker \alpha^1 \subset$ im δ.

□

The homomorphism δ in Proposition 2.3.2 is called the *connecting homomorphism* or the *coboundary map*. It should be noted that the long exact sequence in Proposition 2.3.2 can be further extended to higher cohomology groups $H^i(G, A), H^i(G, B)$ and $H^i(G, C)$ for all $i \geq 2$ (cf. [14, Ch. 1, §1.3.1]) and [6, Ch. 17, §17.2, Theorem 21]. The following example illustrates an explicit computation of the coboundary map:

Example 2.3.3 Let $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$, where σ is the nontrivial automorphism and consider the exact sequence from Example 2.3.1

$$1 \to \mu_2 \to \mathbb{C}^\times \xrightarrow{[2]} \mathbb{C}^\times \to 1.$$

After taking G-fixed points, we obtain the sequence

$$1 \to \mu_2 \to \mathbb{R}^\times \xrightarrow{[2]} \mathbb{R}^\times \xrightarrow{\delta} H^1(G, \mu_2) \to H^1(G, \mathbb{C}^\times) \to H^1(G, \mathbb{C}^\times).$$

Note that we may identify $H^1(G, \mu_2) \simeq \mu_2$ via $f \mapsto f(\sigma)$. Let $c \in \mathbb{R}^\times$ and let $b = \sqrt{c}$. It follows from the construction of δ that $\delta(g) = g(\sqrt{c})/\sqrt{c}$ for any $g \in G$, so $f(\sigma) = \sigma(\sqrt{c})/\sqrt{c} \in \{\pm 1\}$ and δ can be viewed as the *sign homomorphism.*

Now let G be an abstract group and let A be a G-module. There are some situations when elementary group theory properties allow us to say more about $H^1(G, A)$. For example, we have the following result:

Proposition 2.3.4 *Let G be a finite group of order n. Then n annihilates $H^1(G, A)$.*

Proof. Let $f \in Z^1(G, A)$. Then for any $g, h \in G$ we have $f(gh) = f(g) + gf(h)$. Taking the sum over all $h \in G$ on both sides yields

$$\sum_{h \in G} f(gh) = nf(g) + g \sum_{h \in G} f(h).$$

Set $a = \sum_{h \in G} f(gh)$. Then $a = nf(g) + ga$, so $nf(g) = g(-a) - (-a)$ and $nf \in B^1(G, A)$. Thus, n annihilates $H^1(G, A)$ as claimed. □

Corollary 2.3.5 *Let G be a finite group of order s and let A be a G-module which can be generated by r elements as an abelian group. Then $H^1(G, A)$ is finite of order dividing $s^{r(s-1)}$.*

Proof. The finiteness of $H^1(G, A)$ is well-known (cf. [27, Ch. 10, Theorem 10.29]), but since no explicit estimate for the order has been recorded, we will redo the entire argument. The group $H^1(G, A)$ is a quotient of the group of 1-cocycles

$Z^1(G,A)$ which in turn is a subgroup of the group $F^1(G,A)$ of functions satisfying $f(1)=0$. Clearly, $F^1(G,A)\simeq A^{s-1}$ can be generated by $\leq r(s-1)$ elements as an abelian group, and hence the same is true for $Z^1(G,A)$. On the other hand, $s=|G|$ annihilates $H^1(G,A)$ by Proposition 2.3.4, making the latter a quotient of $Z^1(G,A)/sZ^1(G,A)$. The above estimate on the number of generators yields that $Z^1(G,A)/sZ^1(G,A)$ is finite of order dividing $|(\mathbb{Z}/s\mathbb{Z})^{r(s-1)}|=s^{r(s-1)}$, and the required fact follows. □

As a very important special case of Corollary 2.3.5, we obtain an explicit estimate on the order of $H^1(\mathcal{G},X(T))$, where T is any d-dimensional K-torus with minimal splitting field P and $\mathcal{G}=\mathrm{Gal}(P/K)$ that only depends on d. More precisely, we have the following

Corollary 2.3.6 *There exists an explicit integral-valued super-increasing function $\psi(d)$ defined on integers $d\geq 1$ such that for any d-dimensional torus T, the group $H^1(\mathcal{G},X(T))$ is finite of order dividing $\psi(d)$.*

Proof. Let $\gamma(d)$ be as in (2.3). The character group $X(T)$ can be generated by d elements as $\mathbb{Z}[\mathcal{G}]$-module and as we saw in the proof of Proposition 2.2.26, the order of $\mathcal{G}$ divides $\gamma(d)$, which is a super-increasing function. Thus, applying Corollary 2.3.5, we see that the function

$$\psi(d):=\gamma(d)^{d(\gamma(d)-1)}$$

meets our requirements. □

Corollary 2.3.7 *Let $\psi(d)$ be as in the Corollary 2.3.6. Then for every d-dimensional K-torus T and any finite Galois extension F/K that splits T, with Galois group $G=\mathrm{Gal}(F/K)$, the order of $H^1(G,X(T))$ divides $\psi(d)$.*

Proof. Indeed, since P is the minimal splitting field of T, we have the inclusion $P \subset F$, and then $\mathcal{G} = G/H$ where $H := \mathrm{Gal}(F/P)$; in fact, H is the kernel of the natural action of G on $X(T)$. The inflation-restriction sequence (cf. [2, Ch. 4, §5]) yields the following exact sequence

$$0 \to H^1(\mathcal{G}, X(T)) \xrightarrow{\mathrm{Inf}} H^1(G, X(T)) \xrightarrow{\mathrm{Res}} H^1(H, X(T)).$$

Since $X(T)$ is torsion-free, we see that $H^1(H, X(T)) = \mathrm{Hom}(H, X(T))$ is trivial, so the inflation map yields is an isomorphism, and our claim follows from Corollary 2.3.6. □

In the proofs in Chapter 3 we will need different variants of Hilbert's Theorem 90, which in its original form only treats the case of multiplicative group of a field but it can be generalized to several other groups, including quasi-split tori.

Theorem 2.3.8 (Hilbert's Theorem 90, classical form) *Let L/K be a cyclic extension. Then any element $a \in L^\times$ such that $N_{L/K}(a) = 1$, is of the form $\sigma(b)/b$ for some $b \in L^\times$.*

Proof. [6, Ch. 14, §14.2, Exercise 23]. □

Theorem 2.3.9 (Hilbert's Theorem 90, cohomological form) *Let L/K be any (possibly infinite) Galois extension with Galois group G. Then $H^1(G, L^\times)$ is trivial.*

Proof. [15, Ch. 2, §2.2.2, Lemma 2.17]. □

Let K be any field and let $\bar{K}$ denote some fixed separable closure of K. For any $\mathrm{Gal}(\bar{K}/K)$-module A we will simply write $H^1(K, A)$ to denote the cohomology group $H^1(\mathrm{Gal}(\bar{K}/K), A)$.

Theorem 2.3.10 (Hilbert's Theorem 90, form for quasi-split tori) *Let K be any field and let T be a quasi-split K-torus. Then $H^1(K,T)$ is trivial.*

Proof. Cf. [15, Ch. 2, §2.2.3, Lemma 2.21]. Since cohomology is functorial, we may assume that $T = \mathrm{R}_{E/K}(\mathbb{G}_m)$ for some finite separable extension E/K. By Shapiro's Lemma (cf. [6, Ch. 17, §17.2, Proposition 23]) there is an isomorphism $H^1(K,T) \simeq H^1(E,\mathbb{G}_m)$. On the other hand, $H^1(E,\mathbb{G}_m)$ is trivial by Theorem 2.3.9. □

2.3.2 One consequence of Nakayama-Tate theorem

In this section we will combine Corollary 2.3.6 with the Nakayama-Tate theorem (cf. Theorem 2.3.12) to derive an arithmetic result that we will need for proofs in Chapter 3 (cf. Corollary 2.3.13). Let T be a torus defined over a *global* field K, let F/K be a finite Galois extension that splits T, and let $G = \mathrm{Gal}(F/K)$ be the corresponding Galois group. We let $K[T]$ (resp., $F[T]$) denote the coordinate ring of T over K (resp., over F); recall that $F[T]$ is naturally identified with the group algebra $F[X(T)]$ and that this identification is compatible with Galois action. For any F-algebra B we have

$$T(B) = \mathrm{Hom}_{K\text{-alg}}(K[T],B) \simeq \mathrm{Hom}_{F\text{-alg}}(F[T],B) \simeq \mathrm{Hom}(X(T),B^\times).$$

Moreover, if G acts on B by semi-linear transformations, then the identification $T(B) \simeq \mathrm{Hom}(X(T),B^\times)$ is compatible with the action of G. We recall that the adele ring $\mathbb{A}_F$ is equipped with a semi-linear G-action via the identification $\mathbb{A}_F \simeq \mathbb{A}_K \otimes_K F$ (cf. Proposition 1.1.14). Then the natural map of G-modules $T(F) \to T(\mathbb{A}_F)$ gets identified with the map $\mathrm{Hom}(X(T),F^\times) \to \mathrm{Hom}(X(T),\mathbb{I}_F)$ induced by the diagonal embedding $F^\times \to \mathbb{I}_F$. Now, we let $C_F = \mathbb{I}_F/F^\times$ be the idele class group of F and

set $C_F(T) := \mathrm{Hom}(X(T), C_F)$ with the standard G-action. Since $X(T)$ is a free abelian group, the exact sequence

$$1 \to F^\times \longrightarrow \mathbb{I}_F \longrightarrow C_F \to 1$$

induces an exact sequence of G-modules

$$1 \to T(F) \longrightarrow T(\mathbb{A}_F) \longrightarrow C_F(T) \to 1. \tag{2.4}$$

The corresponding cohomological exact sequence contains the following fragment

$$H^1(G, T(F)) \xrightarrow{\theta} H^1(G, T(\mathbb{A}_F)) \longrightarrow H^1(G, C_F(T)). \tag{2.5}$$

Proposition 2.3.11 *In the exact sequence (2.5), the cokernel coker θ is finite of order dividing $\psi(d)$ (the function from Corollary 2.3.6).*

The necessary tool to prove Proposition 2.3.11, is the Nakayama-Tate Theorem (cf. Theorem 2.3.12). In order to state this theorem, we need to introduce the notion of Tate cohomology.

Let G be a finite group, and let A be a G-module. We define the trace map $\mathrm{Tr}_G\colon A \to A$ by $\mathrm{Tr}_G(a) = \sum_{g\in G} ga$. It is easy to see that $\mathrm{Tr}_G(A) \subset A^G$ and $\omega_G \subset \ker \mathrm{Tr}_G$, where ω_G is the submodule of A generated by elements of the form $ga - a$ for all $g \in G$ and $a \in A$. Then the *ith Tate cohomology group* $\hat{H}^i(G, A)$ is defined as follows.

$$\hat{H}^i(G, A) := H^i(G, A) \text{ for all } i \geq 1,$$

$$\hat{H}^0(G, A) := A^G/\mathrm{Tr}_G(A),$$

$$\hat{H}^{-1}(G, A) := (\ker \mathrm{Tr}_G)/\omega_G,$$

$$\hat{H}^{-i}(G, A) := H_{i-1}(G, A) \text{ for all } i \geq 2,$$

where $H_i(G, A)$ denotes the *ith homology group* (cf. [27, Ch. 1, p. 20]). It turns out that Tate cohomology retains all the basic properties of the usual cohomology. In particular, any short exact sequence of G-modules and G-module homomorphisms $0 \to A \to B \to C \to 0$ induces the following long exact sequence of groups which is infinite in both directions:

$$\ldots \to \hat{H}^i(G, A) \to \hat{H}^i(G, B) \to \hat{H}^i(G, C) \to \hat{H}^{i+1}(G, A) \to \ldots$$

([14, Ch. 6, §6.3]).

The long (Tate) cohomology sequence induced from (2.4) contains the Tate cohomology groups $\hat{H}^i(\mathcal{G}, C_P(T))$, which can be further described via the following theorem

Theorem 2.3.12 (Nakayama-Tate) *Let K be a global field. Then for any integer i and any K-torus T with a splitting field P and Galois group $\mathcal{G} = \mathrm{Gal}(P/K)$, there is an isomorphism*

$$\hat{H}^i(\mathcal{G}, C_P(T)) \simeq \hat{H}^{2-i}(\mathcal{G}, X(T)).$$

Proof. Cf. [35, Ch. 4, §11.3 , Theorem 6] and [14, Ch. 6, §6.1]. □

Proof of Proposition 2.3.11. Due to the exact sequence (2.5), the cokernel coker θ embeds into $H^1(G, C_F(T))$. On the other hand, the Nakayama-Tate theorem (with $i = 1$) furnishes an isomorphism

$$H^1(G, C_F(T)) \simeq H^1(G, X(T)).$$

Our claim now follows from Corollary 2.3.7. □

We conclude this section with one consequence of Proposition 2.3.11. Let $S \subset$

V^K be an arbitrary subset, and let $\bar{S}$ be the set of all extensions of $v \in S$ to F. Then G acts on $\mathbb{A}_F(\bar{S}) \simeq \mathbb{A}_K(S) \otimes_K F$ through the second factor, making $T(\mathbb{A}_K(\bar{S}))$ into a G-module, with the diagonal embedding $F \hookrightarrow \mathbb{A}_F(\bar{S})$ yielding a homomorphism of cohomology groups

$$\theta_{\bar{S}} \colon H^1(G, T(F)) \longrightarrow H^1(G, T(\mathbb{A}_F(\bar{S}))).$$

Furthermore, the projection $T(\mathbb{A}_F) \to T(\mathbb{A}_F(\bar{S}))$ defines the top arrow in the following commutative diagram

$$\begin{array}{ccc} H^1(G, T(\mathbb{A}_F)) & \xrightarrow{\nu} & H^1(G, T(\mathbb{A}_F(\bar{S}))) \\ {\scriptstyle\theta}\uparrow & & \uparrow{\scriptstyle\theta_{\bar{S}}} \\ H^1(G, T(F)) & \xrightarrow{=} & H^1(G, T(F)) \end{array}$$

Since $T(\mathbb{A}_F(\bar{S}))$ is a direct product factor of $T(\mathbb{A}_F)$ as G-module, ν is surjective. So, Proposition 2.3.11 yields the following.

Corollary 2.3.13 *For any subset $S \subset V^K$, the cokernel coker $\theta_{\bar{S}}$ is finite of order dividing $\psi(d)$.*

2.3.3 Nonabelian cohomology

In the proof of one of our results in Chapter 3, we use the Hasse principle for semi-simple simply connected algebraic groups. For this, we need to introduce all the relevant definitions and properties of nonabelian cohomology.

Let G be a finite or profinite group acting on some group A. Assume that G acts on A by automorphisms, i.e. $g(ab) = (ga)(gb)$ for all $g \in G$ and all $a, b \in A$ so that A is a G-group. Then we define $H^0(G, A)$ to be the subgroup of G-fixed points A^G.

A continuous map $f \colon G \to A$ is called a 1-*cocycle* if for any $g, h \in G$ we have

$f(gh) = f(g)(gf(h))$. The set of 1-cocycles will be denoted by $Z^1(G, A)$. Note that $Z^1(G, A)$ is never empty as it always contains the trivial cocycle $e\colon G \to A$ given by $e(g) = 1_A$ for all $g \in G$. Two cocycles f and f' are *equivalent* and we write $f \sim f'$ if there exists an element $a \in A$ such that $f'(g) = a^{-1}f(g)(ga)$ for all $g \in G$. It is easy to verify that $\sim$ is an equivalence relation on $Z^1(G, A)$. We define the *first cohomology set* $H^1(G, A)$ as the quotient $H^1(G, A) = Z^1(G, A)/\sim$. Observe that if A is abelian then this definition coincides with the definition of $H^1(G, A)$ in section 2.3.1 and then $H^1(G, A)$ is an abelian group. In general, $H^1(G, A)$ is only a set without any natural group structure. The group $H^1(G, A)$ always contains the equivalence class of the trivial cocycle $e\colon G \to A$, which we call the *distinguished element* of $H^1(G, A)$.

If $\alpha\colon A \to B$ is a homomorphism of two G-groups compatible with the G-action, i.e. $\alpha(ga) = g\alpha(a)$ for all $g \in G, a \in A$, then we may define $Z^1(G, A) \to Z^1(G, B)$ sending $f(g)$ to $\alpha(f(g))$, which induces a morphism of sets with distinguished element $H^1(G, A) \to H^1(G, B)$. We say that a sequence of cohomology sets is *exact* if the preimage of each distinguished element is equal to the image of the preceding map. Note that the distinguished element in the zero cohomology set $H^0(G, A)$ is the identity element 1_A.

Let A be a G-group and let B be a subgroup of A that is invariant under the G-action. There is a natural action of G on A/B, which makes A/B into a G-module. Thus, we obtain the cohomology set $H^0(G, A/B) = (A/B)^G$ with distinguished element being the class B. We have the following analog of Proposition 2.3.2 in the nonabelian setting

Proposition 2.3.14 *There is a coboundary map $\delta\colon H^0(G, A/B) \to H^1(G, B)$ such that the following sequence is an exact sequence of cohomology sets with a distin-*

guished element

$$1 \to H^0(G,B) \to H^0(G,A) \to H^0(G,A/B) \xrightarrow{\delta} H^1(G,B) \to H^1(G,A). \qquad (2.6)$$

Proof. Cf. [15, Ch. 1, §1.3.2, (1.11)]. □

Now let K be a number field and let G be a simply connected algebraic K-group. The main example of a cohomology set which will appear in this thesis is $H^1(\mathrm{Gal}(\bar{K}/K), G)$, where $\mathrm{Gal}(\bar{K}/K)$ is the *absolute Galois group* of K. For simplicity, we will always denote the cohomology set $H^1(\mathrm{Gal}(\bar{K}/K), G)$ by $H^1(K,G)$. There is a canonical *local-global* map for G (cf. [14, Ch. 6, §6.1]):

$$\theta_G \colon H^1(K,G) \to \prod_{v \in V_\infty^K} H^1(K_v, G).$$

We may now state the main result from nonabelian cohomology we need for proofs in Chapter 3

Theorem 2.3.15 (Hasse Principle) *Let K be a number field and let G be a semi-simple simply connected algebraic K-group. Then the map θ_G is bijective.*

Proof. Cf. [14, Ch. 6, §6.1 , Theorem 6.6]. □

For a more detailed exposition of nonabelian cohomology, we refer the reader to [15, Ch. 1, §1.3.2].

Chapter 3

Almost strong approximation in algebraic groups

3.1 Almost strong approximation in tori

Let K be a global field. Recall that if $S \subset V^K$ is any finite subset, then the torus $\mathbb{G}_m$ does not have almost strong approximation with respect to S (cf. section 1.3.1) but it does have this property with respect to tractable sets S of valuations provided that the technical condition (1.7) holds (cf. Proposition 1.3.7). The goal of this section is to extend Proposition 1.3.7 to arbitrary tori, namely we prove that any K-torus T satisfies almost strong approximation with respect to any tractable set S under a similar assumption (see (3.4)) that relates the minimal splitting field of T and the generalized arithmetic progression almost contained in S (cf. Theorem 3.1.3). The proof consists of the following two parts:

(1) First, we prove our theorem for quasi-split tori (cf. Theorem 3.1.2). This follows from Proposition 1.3.7;

(2) Then we prove the theorem for arbitrary tori by reducing the general case to

the case of quasi-split tori using Proposition 2.2.26 (cf. Theorem 3.1.3).

Let us now illustrate by example that condition (3.4) cannot be omitted in general. More precisely, we show that a torus may not satisfy almost strong approximation with respect to a tractable set of valuations if (3.4) does not hold

Example 3.1.1 Let $K = \mathbb{Q}$ and let $S = \{v_\infty\} \cup \{v_p \,|\, p \in \mathbb{P}_{3(4)}\}$. We consider the norm torus $T = \mathrm{R}^{(1)}_{L/\mathbb{Q}}(\mathbb{G}_m)$ associated with the extension $L = \mathbb{Q}(i)$, $i^2 = -1$. Then

$$[T(\mathbb{A}(S)) : \overline{T(\mathbb{Q})}^{(S)}] = \infty. \tag{3.1}$$

To prove this, we adapt the strategy used in section 1.3.1, viz. we consider the open subgroup

$$\mathbb{U}_T(S) := \prod_{p \in \mathbb{P} \setminus \mathbb{P}_{3(4)}} T(\mathbb{Z}_p)$$

and set $\mathbb{E}_T(S) := \mathbb{U}_T(S) \cap T(\mathbb{Q})$. It is enough to show that $\mathbb{E}_T(S)$ is finite, as then $[\mathbb{U}_T(S) : \overline{\mathbb{E}_T(S)}^{(S)}] = \infty$, and (3.1) will follow.

Now, let $x \in \mathbb{E}_T(S)$. By the classical form of Hilbert's Theorem 90 (cf. Theorem 2.3.8), we can write $x = \sigma(y)/y$ for some $y \in L^\times$, where $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ is the nontrivial automorphism. For $p \notin \mathbb{P}_{1(4)}$, the valuation v_p has a unique extension w_p to L, and we set $\alpha_p = w_p(y)$. For $p \in \mathbb{P}_{1(4)}$, however, v_p has two extensions w'_p, w''_p (swapped by σ), but since $x \in T(\mathbb{Z}_p)$ we have $w'_p(y) = w''_p(y) =: \alpha_p$. Set

$$a := \prod_{p \neq 2} p^{\alpha_p} \quad \text{and} \quad z := y/a.$$

Then $x = \sigma(z)/z$ and by construction $w(z) = 0$ for all $w \in V_f^L \setminus \{w_2\}$. Since the prime element of $\mathbb{Z}[i]$ lying above 2 is $(1+i)$, we conclude that $z = \varepsilon \cdot (1+i)^\ell$ with $\varepsilon \in \mathbb{E} := \{\pm 1, \pm i\}$ (the unit group of $\mathbb{Z}[i]$) and $\ell \in \mathbb{Z}$. Then $x = \sigma(z)/z \in \mathbb{E}$, so $\mathbb{E}_T(S) = \mathbb{E}$ is finite, as required.

3.1.1 The case of quasi-split tori

In this section we establish almost strong approximation for quasi-split tori with respect to tractable subsets $S \subset V^K$. More precisely, we have the following

Theorem 3.1.2 *Let K be a global field and let $S \subset V^K$ be a tractable subset containing a set of the form $V_\infty^K \cup (\mathcal{P}(L/K, \mathcal{C}) \setminus \mathcal{P}_0)$ where $\mathcal{P}_0$ has Dirichlet density zero. Let $T = \mathrm{R}_{F_1/K}(\mathbb{G}_m) \times \ldots \times \mathrm{R}_{F_r/K}(\mathbb{G}_m)$, where $F_1, \ldots, F_r$ are finite separable extensions of K, be a quasi-split K-torus having dimension d and the minimal splitting field P. Assume that there exists $\sigma \in \mathcal{C}$ such that*

$$\sigma|(P \cap L) = \mathrm{id}_{P \cap L}. \tag{3.2}$$

Then the index $[T(\mathbb{A}_K(S)) : \overline{T(K)}^{(S)}]$ is finite and divides n^r, hence also n^d where $n = [L : K]$.

Proof. Let $T_i = \mathrm{R}_{F_i/K}(\mathbb{G}_m)$ so that $T = T_1 \times \cdots \times T_r$. We obviously have an isomorphism

$$T(\mathbb{A}_K(S))/\overline{T(K)}^{(S)} \simeq T_1(\mathbb{A}_K(S))/\overline{T_1(K)}^{(S)} \times \cdots \times T_r(\mathbb{A}_K(S))/\overline{T_r(K)}^{(S)}. \tag{3.3}$$

For each $i = 1, \ldots, r$, the (minimal) splitting field P_i of T_i coincides with the normal closure of F_i, and then P is the compositum of $P_1, \ldots, P_r$. Thus, our assumption (3.2) for $\sigma \in \mathcal{C}$ implies that the assumption (1.7) in Proposition 1.3.7 holds true for $F = F_i$ and all $i = 1, \ldots, r$. As we explained above, the proposition implies that each of the indices $[T_i(\mathbb{A}_K(S)) : \overline{T_i(K)}^{(S)}]$ divides n. In view of (3.3), the index $[T(\mathbb{A}_K(S)) : \overline{T(K)}^{(S)}]$ divides n^r, and hence also n^d as clearly $r \leq d$. □

3.1.2 The case of arbitrary tori

The goal of this section is to establish almost strong approximation for arbitrary tori with respect to tractable subsets $S \subset V^K$. More precisely, we want to prove the following

Theorem 3.1.3 *Let K be a global field, and let T be a K-torus with the minimal splitting field P/K. If S is a tractable set of valuations containing a set of the form $V_\infty^K \cup (\mathcal{P}(L/K, \mathcal{C}) \setminus \mathcal{P}_0)$, where $\mathcal{P}(L/K, \mathcal{C})$ is a generalized arithmetic progression associated with a finite Galois extension L/K and a conjugacy class $\mathcal{C} \subset \mathrm{Gal}(L/K)$, and $\mathcal{P}_0$ has Dirichlet density zero, such that*

$$\sigma|(P \cap L) = \mathrm{id}_{P\cap L} \quad \text{for some} \quad \sigma \in \mathcal{C}, \tag{3.4}$$

the torus T has almost strong approximation with respect to S, with the index $[T(\mathbb{A}_K(S)) : \overline{T(K)}^{(S)}]$ dividing a constant $\tilde{C}(d, n)$ that depends only on $d = \dim T$ and $n = [L : K]$.

Proof. We will show that the function

$$\tilde{C}(d, n) := n^d \cdot \psi(\lambda(d)), \tag{3.5}$$

where ψ and λ are the functions constructed in Corollary 2.3.6 and Proposition 2.2.26, satisfies the requirements of the theorem. So, let T be a d-dimensional torus defined over a global field K with the minimal splitting field P, let $\mathcal{G} = \mathrm{Gal}(P/K)$, and let $S \subset V^K$ be a tractable set as in the statement of the theorem. We then let $\bar{S}$ denote the set of all extensions of valuations $v \in S$ to P.

We now consider the exact sequence sequence of K-tori

$$1 \to T_1 \longrightarrow T_0 \xrightarrow{\pi} T \to 1,$$

constructed in Proposition 2.2.26 (so, in particular, $\dim T_1 \leqslant \lambda(d)$). The image of the embedding of abelian groups $\pi^*\colon X(T) \to X(T_0)$ has a complement (since coker $\pi^* \simeq X(T_1)$ is torsion-free), which gives rise to a P-defined section $T \to T_0$ for π. It follows that for any P-algebra B, the group homomorphism $\pi_B\colon T_0(B) \to T(B)$ is surjective. Thus, we obtain the following commutative diagram of $\mathcal{G}$-modules with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & T_1(\mathbb{A}_P(\bar{S})) & \longrightarrow & T_0(\mathbb{A}_P(\bar{S})) & \longrightarrow & T(\mathbb{A}_P(\bar{S})) & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & T_1(P) & \longrightarrow & T_0(P) & \longrightarrow & T(P) & \longrightarrow & 1 \end{array} \tag{3.6}$$

where the vertical maps are the natural diagonal embeddings. Since $\mathcal{G}$ acts on $\mathbb{A}_P(\bar{S}) \simeq \mathbb{A}_K(S) \otimes_K P$ through the second factor, and hence $\mathbb{A}_P(\bar{S})^{\mathcal{G}} = \mathbb{A}_K(S)$, by passing to cohomology we obtain the following commutative diagram with exact rows:

$$\begin{array}{ccccc} T_0(\mathbb{A}_K(S)) & \xrightarrow{\pi} & T(\mathbb{A}_K(S)) & \xrightarrow{\beta} & H^1(\mathcal{G}, T_1(\mathbb{A}_P(\bar{S}))) \\ \uparrow & & \uparrow & & \theta_{\bar{S}}\uparrow \\ T_0(K) & \longrightarrow & T(K) & \xrightarrow{\alpha} & H^1(\mathcal{G}, T_1(P)) \end{array} \tag{3.7}$$

Since $T_0 = (\mathrm{R}_{P/K}(\mathbb{G}_m))^d$, it follows from Theorem 3.1.2 that the index $[T_0(\mathbb{A}_K(S)) : \overline{T_0(K)}^{(S)}]$ is finite and divides n^d; in particular, $\overline{T_0(K)}^{(S)}$ is an open subgroup of $T_0(\mathbb{A}_K(S))$. On the other hand, by Proposition 2.1.5, the group homomorphism $\pi\colon T_0(\mathbb{A}_K(S)) \to T(\mathbb{A}_K(S))$ is open. So, $\pi(\overline{T_0(K)}^{(S)})$ is an open subgroup of

$T(\mathbb{A}_K(S))$ contained in $\overline{T(K)}^{(S)}$, and therefore

$$\overline{T(K)}^{(S)} = T(K) \cdot \pi(\overline{T_0(K)}^{(S)}).$$

To estimate the index $[T(\mathbb{A}_K(S)) : \overline{T(K)}^{(S)}]$, we set

$$\Omega := T(K) \cdot \pi(T_0(\mathbb{A}_K(S))).$$

Then $[\Omega : \overline{T(K)}^{(S)}]$ divides n^d, and it is enough to show that $[T(\mathbb{A}_K(S)) : \Omega]$ divides $\psi(\lambda(d))$. Using the exactness of the top row in (3.7), we see that

$$[T(\mathbb{A}_K(S)) : \Omega] = [\beta(T(\mathbb{A}_K(S))) : \beta(\Omega)],$$

hence divides $[H^1(\mathcal{G}, T_1(\mathbb{A}_P(\bar{S}))) : \beta(T(K))]$. But since T_0 is quasi-split, we have $H^1(\mathcal{G}, T_0(P))$ is trivial by Hilbert's 90 for quasi-split tori (cf. Theorem 2.3.10), and consequently α is surjective. Thus, the latter index equals $|\text{coker } \theta_{\bar{S}}|$, which divides $\psi(\lambda(d))$ according to Corollary 2.3.13 applied to T_1 (recall that $\dim T_1 = \lambda(d)$ and ψ is super-increasing). □

3.2 Almost strong approximation in reductive groups

Let G be a reductive algebraic group defined over a number field K, and suppose that $G = TH$, an almost direct product of a K-torus T and a semi-simple K-group H. We first prove Theorem A in the special case where H is assumed to be simply connected (cf. Proposition 3.2.1). The argument in this case has two major ingredients: the classical criterion for strong approximation (cf. [14, Ch. 7, §7.4, Theorem 7.12]) and our Theorem 3.1.3. The general case is then reduced to the

special case by means of a result stating that any reductive K-group is a quotient of a reductive K-group as in the special case by a quasi-split torus, see Lemma 3.2.3.

3.2.1 Special case: H is simply connected.

In this case, we have the following more streamlined statement that does not depend on the rank of H and the minimal Galois extension M of K over which H becomes an *inner form of the split group* (cf. [33, Ch. 12, §12.3.7] and [21, §4, Lemma 4.1]).

Proposition 3.2.1 *Let G be a reductive group over a number field K, and suppose that $G = TH$, an almost direct product of a K-torus T and a semi-simple simply connected K-group H. Furthermore, let $S \subset V^K$ be a tractable set of valuations containing a set of the form $V_\infty^K \cup (\mathcal{P}(L/K, \mathcal{C}) \setminus \mathcal{P}_0)$, where $\mathcal{P}_0$ is a set of valuations having Dirichlet density zero. Assume that there exists $\sigma \in \mathcal{C}$ such that*

$$\sigma|(P \cap L) = \mathrm{id}_{P \cap L}, \tag{3.8}$$

where P is the minimal splitting field of T. Then $\overline{G(K)}^{(S)}$ is a normal subgroup of $G(\mathbb{A}_K(S))$ for which the index $[G(\mathbb{A}_K(S)) : \overline{G(K)}^{(S)}]$ is finite and divides $2^{dr} \cdot \tilde{C}(d, n)$ where $d = \dim T$, $n = [L : K]$, r is number of real valuations of K, and $\tilde{C}(d, n)$ is the function from Theorem 3.1.3.

For the proof, we consider the exact sequence of K-groups

$$1 \to H \longrightarrow G \xrightarrow{\pi} T' \to 1,$$

where $T' = G/H$ and π is the quotient map. We have $H = H_1 \times \cdots \times H_\ell$, the direct product of K-simple groups H_i. Since S is infinite, for each $i = 1, \ldots, \ell$ there exists $v_i \in S$ such that H_i is K_{v_i}-isotropic (cf. [14, Ch. 6, §6.2, Theorem 6.7]). Using the

criterion for strong approximation (cf. [14, Ch. 7, §7.4, Theorem 7.12]), we conclude that H has strong approximation with respect to S, i.e. $\overline{H(K)}^{(S)} = H(\mathbb{A}_K(S))$. Then

$$[G(\mathbb{A}_K(S)), G(\mathbb{A}_K(S))] \subset H(\mathbb{A}_K(S)) \subset \overline{G(K)}^{(S)},$$

implying that $\overline{G(K)}^{(S)}$ is a normal subgroup of $G(\mathbb{A}_K(S))$. Furthermore,

$$G(\mathbb{A}_K(S))/\overline{G(K)}^{(S)} \simeq \pi(G(\mathbb{A}_K(S)))/\pi(\overline{G(K)}^{(S)}) \hookrightarrow T'(\mathbb{A}_K(S))/\pi(\overline{G(K)}^{(S)}),$$

and we have

$$[T'(\mathbb{A}_K(S)) : \pi(\overline{G(K)}^{(S)})] = [T'(\mathbb{A}_K(S)) : \overline{T'(K)}^{(S)}] \cdot [\overline{T'(K)}^{(S)} : \pi(\overline{G(K)}^{(S)})]. \quad (3.9)$$

Lemma 3.2.2 *The index $[T'(K) : \pi(G(K))]$ is finite and divides 2^{dr}.*

Proof. Let V_r^K be the set of all real valuations of K, and let $v \in V_r^K$. It follows from the Implicit Function Theorem that the subgroup $\pi(G(K_v)) \subset T'(K_v)$ is open (cf. [15, Ch. 3, §3.1, Corollary 3.7]), hence contains the *topological* connected component $T'(K_v)^\circ$. On the other hand, it is well-known that T' is isomorphic over $K_v = \mathbb{R}$ to a torus of the form

$$(\mathbb{G}_m)^a \times (\mathrm{R}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m))^b \times (\mathrm{R}^{(1)}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m))^c$$

for some nonnegative integers a, b and c (cf. Remark 2.2.22), and then $[T'(K_v) : T'(K_v)^\circ] = 2^a$ divides 2^d. It follows that for the subgroup

$$N := \bigcap_{v \in V_r^K} (T'(K) \cap T'(K_v)^\circ),$$

the index $[T'(K) : N]$ divides 2^{dr}, and it remains to show that $N \subset \pi(G(K))$.

For any field extension E/K, we have an exact sequence

$$G(E) \xrightarrow{\pi} T'(E) \xrightarrow{\delta_E} H^1(E, H).$$

Now, let $x \in N$. Due to the exactness of the above sequence for $E = K_v$, we need to show that the cohomology class $\xi := \delta_K(x)$ is trivial. However, for each $v \in V_r^K$, due to the inclusion $T'(K_v)^\circ \subset \pi(G(K_v))$ and the definition of N, we have that the class $\xi_v := \delta_{K_v}(x)$ is trivial. Thus, ξ lies in the kernel of the map

$$H^1(K, H) \xrightarrow{\theta_H} \prod_{v \in V_r^K} H^1(K_v, H).$$

But according to the Hasse principle for simply connected groups (cf. Theorem 2.3.15), θ_H is injective, and hence ξ is trivial, as required. □

Since $\pi\colon G(\mathbb{A}_K(S)) \to T'(\mathbb{A}_K(S))$ is open (cf. Proposition 2.1.5) and $\overline{G(K)}^{(S)}$ contains its kernel $H(\mathbb{A}_K(S))$, the image $\pi(\overline{G(K)}^{(S)})$ is closed, hence coincides with $\overline{\pi(G(K))}^{(S)}$. So, it follows from Lemma 3.2.2 that the index $[\overline{T'(K)}^{(S)} : \pi(\overline{G(K)}^{(S)})]$ divides 2^{dr}. On the other hand, due to (3.8), the index $[T'(\mathbb{A}_K(S)) : \overline{T'(K)}^{(S)}]$ divides $\tilde{C}(d, n)$. Now, Proposition 3.2.1 follows from (3.9).

3.2.2 Existence of special covers.

To consider the general case in Theorem A, we will first establish the existence of special covers of arbitrary reductive groups that enable one to realize every reductive group as a quotient of a reductive group with *simply connected* semi-simple part (= commutator subgroup) by a quasi-split torus.

Lemma 3.2.3 *Let G be a reductive algebraic group over a field K of characteristic zero, and suppose that $G = TH$, an almost direct product of a K-torus T and a*

semi-simple K-group H. Let ℓ be the rank of G, and let M be the minimal Galois extension of K over which H becomes an inner form of the split group. Then there exists an exact sequence of K-groups

$$1 \longrightarrow T_0 \longrightarrow \widetilde{G} \xrightarrow{\nu} G \to 1 \tag{3.10}$$

such that

(1) *T_0 is a quasi-split K-torus that becomes split over M;*

(2) *$\widetilde{G} = \widetilde{T}\widetilde{H}$ is an almost direct product of a K-torus $\widetilde{T}$ which is isogenous to $T_0 \times T$, with $\dim \widetilde{T} = \ell$, and a semi-simple simply connected K-group $\widetilde{H}$.*

Proof. Choose a K-defined universal cover $\alpha\colon \widetilde{H} \to H$ (cf. [15, Proposition 2.27]), set $D = T \times \widetilde{H}$, and consider the K-isogeny $\theta\colon D \to G$ obtained by composing $D \xrightarrow{\mathrm{id_T}\times\alpha} T \times H$ with the product morphism $T \times H \to G$. Let $\Phi = \ker\theta$, and observe that since the restriction $\theta|T$ is injective, the projection to $\widetilde{H}$ identifies Φ with its image. Now, let $\widetilde{H}_0$ be the K-quasi-split inner form of $\tilde{H}$, and let T_0 be a maximal K-torus of $\widetilde{H}_0$ contained in a K-defined Borel subgroup. Then T_0 is quasi-split over K (cf. [5, Exposé XXIV, §3, Proposition 3.13]), becomes split over M (since $\widetilde{H}_0$ is a quasi-split inner form over M, hence M-split), and Φ admits a K-embedding into T_0. Set

$$\widetilde{\Phi} = \{(x, x^{-1}) \in T_0 \times D \,|\, x \in \Phi\} \quad \text{and} \quad \widetilde{G} = (T_0 \times D)/\widetilde{\Phi}.$$

The composite morphism $\widetilde{H} \to D \to \widetilde{G}$ is a K-embedding, and we identify $\widetilde{H}$ with the image of this embedding. Furthermore, $\widetilde{G}$ is an almost direct product $\widetilde{T}\widetilde{H}$, where $\widetilde{T}$ is the image of $T_0 \times T \subset T_0 \times D$ in $\widetilde{G}$, and we note that $\dim \widetilde{T} = \ell$. By construction, the composite morphism $T_0 \times D \xrightarrow{\mathrm{pr}} D \xrightarrow{\theta} G$ vanishes on $\widetilde{\Phi}$, hence gives rise to a morphism $\nu\colon \widetilde{G} \to G$. Finally, $\ker\nu$ coincides with the image of $T_0 \times \Phi$

in $\widetilde{G}$, which is isomorphic to T_0. $\square$

Remark 3.2.4 One can choose an embedding of Φ into an M-split K-quasi-split torus T_0 in a variety of ways, and for some choices $\dim T_0$ may be $<$ rank H. This will result in choices for $\widetilde{G} = \widetilde{T}\widetilde{H}$ with $\dim \widetilde{T} < \ell$.

3.2.3 General case.

Let $G = TH$ be a (connected) reductive algebraic group defined over a number field K, let P (resp., M) be the minimal Galois extension of K over which T splits (resp., H becomes an inner form of the split group), and set $E = PM$. Furthermore, let $S \subset V^K$ be a tractable set of valuations containing a set of the form $V_\infty^K \cup (\mathcal{P}(L/K, \mathcal{C}) \setminus \mathcal{P}_0)$, and assume that there exists $\sigma \in \mathcal{C}$ such that (1) holds. Set

$$C(\ell, n, r) := 2^{\ell r} \cdot \tilde{C}(\ell, n),$$

where ℓ is the rank of G, $n = [L : K]$, and r is the number of real valuations of K. Our goal is to show that $\overline{G(K)}^{(S)}$ is a finite index normal subgroup of $G(\mathbb{A}_K(S))$, with the abelian quotient $G(\mathbb{A}_K(S))/\overline{G(K)}^{(S)}$ of order dividing $C(\ell, n, r)$.

For this, let us consider the exact sequence (3.10) constructed in Lemma 3.2.3. Since T_0 is K-quasi-split, it follows from Hilbert's Theorem 90 that $\nu(\widetilde{G}(F)) = G(F)$ for every field extension F/K (cf. Theorem 2.3.10), and in particular, $\nu(\widetilde{G}(K_v)) = G(K_v)$ for all $v \in V^K \setminus S$. On the other hand, since T_0 is connected, we have $\nu(\widetilde{G}(\mathcal{O}_v)) = G(\mathcal{O}_v)$ for almost all $v \in V^K \setminus S$ (cf. Proposition 2.1.5). It follows that

$$\nu(\widetilde{G}(\mathbb{A}_K(S))) = G(\mathbb{A}_K(S)). \tag{3.11}$$

Now, $\widetilde{G} = \widetilde{T}\widetilde{H}$ where $\widetilde{T}$ is a K-torus of dimension ℓ (= rank of G) which is

isogenous to $T_0 \times T$, hence has $E = PM$ as its (minimal) splitting field, and $\widetilde{H}$ is a semi-simple simply connected K-group. Since the condition (1) holds, we can apply Proposition 3.2.1 to conclude that $\overline{\widetilde{G}(K)}^{(S)}$ is a finite index normal subgroup of $\widetilde{G}(\mathbb{A}_K(S))$, with the abelian quotient $\widetilde{G}(\mathbb{A}_K(S))/\overline{\widetilde{G}(K)}^{(S)}$ of order dividing $C(\ell, n, r)$.

On the other hand, we have the inclusions

$$[G(\mathbb{A}_K(S)), G(\mathbb{A}_K(S))] = \nu([\widetilde{G}(\mathbb{A}_K(S)), \widetilde{G}(\mathbb{A}_K(S))]) \subset \nu(\overline{\widetilde{G}(K)}^{(S)}) \subset \overline{G(K)}^{(S)},$$

which imply that $\overline{G(K)}^{(S)}$ is a normal subgroup of $G(\mathbb{A}_K(S))$ with abelian quotient. Furthermore, it follows from (3.11) that ν induces a surjective homomorphism of abelian groups

$$\widetilde{G}(\mathbb{A}_K(S))/\overline{\widetilde{G}(K)}^{(S)} \longrightarrow G(\mathbb{A}_K(S))/\overline{G(K)}^{(S)},$$

and consequently the order of $G(\mathbb{A}_K(S))/\overline{G(K)}^{(S)}$ divides $C(\ell, n, r)$, completing the proof of Theorem A. □

Remark 3.2.5 The above argument actually shows that for any (connected) reductive K-group G and any *infinite* subset $S \subset V^K$, the closure $\overline{G(K)}^{(S)}$ is a normal subgroup of $G(\mathbb{A}_K(S))$ with abelian quotient $G(\mathbb{A}_K(S))/\overline{G(K)}^{(S)}$.

3.2.4 A counter-example to almost strong approximation

Let now G be a semi-simple algebraic group defined over a number field K, and let M be the minimal Galois extension of K over which G becomes an inner twist of a split group, and let S be a tractable set of valuations of K that contains a set of the form $V_\infty^K \cup (\mathcal{P}(L/K, \mathcal{C}) \setminus \mathcal{P}_0)$ in our standard notations. According to Theorem A, the condition that guarantees almost strong approximation in G is

$$\sigma|(M \cap L) = \mathrm{id}_{M \cap L} \quad \text{for some} \quad \sigma \in \mathcal{C}. \tag{3.12}$$

In particular, an inner form of a split group (i.e. when $M = K$) always has almost strong approximation for any tractable set S (cf. Corollary A).

The goal of this section is to show that condition (3.12) cannot be omitted in the general case. More precisely, we will construct an example of an absolutely simple *adjoint*[1] outer form that fails to have almost strong approximation for a suitable tractable set of valuations (for which (3.12) fails to hold).

Let $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$ with $i^2 = -1$ and let σ be the nontrivial automorphism in $\mathrm{Gal}(L/\mathbb{Q})$. For a set S of valuations of K, the corresponding ring of S-adeles of K will be denoted simply by $\mathbb{A}(S)$. Now, fix an odd integer $n \geq 3$, and let q denote an arbitrary nondegenerate σ-Hermitian form on L^n. Then the algebraic group $\widetilde{G} = \mathrm{SU}_n(q)$ associated with the special unitary group of q (cf. [15, Ch. 2, §2.3.3]) is an absolutely almost simple simply-connected algebraic $\mathbb{Q}$-group that is an outer form of type A_{n-1} (cf. [15, Ch. 2, §2.1.14] and [33, Ch. 12, §12.3.8]) with L being the minimal Galois extension of $\mathbb{Q}$ over which $\widetilde{G}$ becomes an inner form of the split group. We will be working with the corresponding adjoint group G and its central $\mathbb{Q}$-isogeny $\pi\colon \widetilde{G} \to G$. Note that $F := \ker \pi$ coincides with $\mathrm{R}^{(1)}_{L/\mathbb{Q}}(\mu_n)$, where μ_n is the group of n-th roots of unity, and will be identified with the n-torsion subgroup of the norm torus $T := \mathrm{R}^{(1)}_{L/\mathbb{Q}}(\mathbb{G}_m)$. Set

$$S := \{v_\infty\} \cup \{v_p \,|\, p \in \mathbb{P}_{3(4)}\} \cup \{v_2\}.$$

Observe that the primes $p \equiv 3 (\mathrm{mod}\, 4)$ correspond precisely to the valuations in the generalized arithmetic progression $\mathcal{P}(L/\mathbb{Q}, \{\sigma\})$, so S is a tractable set containing $\{v_\infty\} \cup \mathcal{P}(L/\mathbb{Q}, \{\sigma\})$, for which (3.12) obviously does not hold.

[1] As we already noted, it follows from the classical criterion for strong approximation that a simply connected semi-simple group always has strong approximation with respect to any infinite set S.

Our goal is to prove the following.

Theorem 3.2.6 *We have* $[G(\mathbb{A}(S)) : \overline{G(\mathbb{Q})}^{(S)}] = \infty$*, and thus* G *does not have almost strong approximation with respect to* S*.*

The proof is based on the observation that for every open subgroup U of $G(\mathbb{A}(S))$, we have the inclusion:

$$G(\mathbb{Q}) \cdot U \supset \overline{G(\mathbb{Q})}^{(S)},$$

So, to prove the theorem it suffices to find a sequence of open subgroups $U_1, U_2, \ldots$ such that the products $G(\mathbb{Q}) \cdot U_\ell$ are all subgroups of $G(\mathbb{A}(S))$ with the indices

$$[G(\mathbb{A}(S)) : G(\mathbb{Q}) \cdot U_\ell] \longrightarrow \infty \ \text{ as } \ \ell \longrightarrow \infty. \tag{3.13}$$

The implementation of this idea requires some preparation.

First, it is known that the quasi-split torus $T_0 := \mathrm{R}_{L/\mathbb{Q}}(\mathbb{G}_m)$ fails to have strong approximation with respect to S, and in fact the quotient $T_0(\mathbb{A}(S))/\overline{T_0(\mathbb{Q})}^{(S)}$ has infinite exponent (cf. [18, Proposition 4]). For our purposes, we need a statement along these lines for the norm torus $T = \mathrm{R}^{(1)}_{L/\mathbb{Q}}(\mathbb{G}_m)$. We have already seen in Example 3.1.1 that T does not have almost strong approximation with respect to S but here we will prove a somewhat stronger statement. To formulate it, for every integer $\ell \geq 1$, we pick a subset $\Pi_\ell \subset \mathbb{P}_{1(4n)}$ of size ℓ, and then consider the following subgroups of $T(\mathbb{A}(S))$:

$$\Gamma(\Pi_\ell) := \prod_{p \in \Pi_\ell} T(\mathbb{Z}_p) \times \prod_{p \in \mathbb{P}_{1(4)} \setminus \Pi_l} \{1\},$$

$$\Delta(\Pi_\ell) := \prod_{p \in \Pi_\ell} T(\mathbb{Z}_p)^n \times \prod_{p \in \mathbb{P}_{1(4)} \setminus \Pi_\ell} T(\mathbb{Z}_p),$$

where $T(\mathbb{Z}_p)^n$ denotes the subgroup of nth powers in $T(\mathbb{Z}_p)$. We note that $\Gamma(\Pi_\ell) \cap \Delta(\Pi_\ell) = \Gamma(\Pi_\ell)^n$ and that the product $\Gamma(\Pi_\ell)\cdot\Delta(\Pi_\ell)$ coincides with $\Delta := \prod_{p\in\mathbb{P}_{1(4)}} T(\mathbb{Z}_p)$.

Lemma 3.2.7 *We have*

$$i(\Pi_\ell) := [T(\mathbb{A}(S)) : T(\mathbb{Q}) \cdot \Delta(\Pi_\ell) \cdot T(\mathbb{A}(S))^n] \longrightarrow \infty \quad as \quad \ell \longrightarrow \infty$$

for any choice of Π_ℓ.

Proof. Since the class number of L is one, we have

$$T_0(\mathbb{A}(S)) = T_0(\mathbb{Q}) \cdot \Delta_0 \quad \text{where} \quad \Delta_0 = \prod_{p\in\mathbb{P}_{1(4)}} T_0(\mathbb{Z}_p) \tag{3.14}$$

(cf. [14, §5.1 and 8.1]). For each $p \in \mathbb{P}_{1(4)}$, there exists a $\mathbb{Z}_p$-defined isomorphism $T_0 \simeq \mathbb{G}_m\mathbb{G}_m$, with σ acting by switching the components, and then $T \simeq \{(t, t^{-1}) \,|\, t \in \mathbb{G}_m\}$. It follows that every $t \in T(\mathbb{Q}_p)$ (resp., $\in T(\mathbb{Z}_p)$) can be written in the form $t = \sigma(s)s^{-1}$ for some $s \in T_0(\mathbb{Q}_p)$ (resp., $\in T_0(\mathbb{Z}_p)$), and therefore all elements $t \in T(\mathbb{A}(S))$ are of the form $\sigma(s)s^{-1}$ for some $s \in T_0(\mathbb{A}(S))$. In conjunction with (3.14), this yields

$$T(\mathbb{A}(S)) = T(\mathbb{Q}) \cdot \Delta. \tag{3.15}$$

In particular, $T(\mathbb{A}(S))^n = T(\mathbb{Q})^n \cdot \Delta^n$, and since $\Delta(\Pi_\ell) \supset \Delta^n$, we obtain

$$i(\Pi_\ell) = [T(\mathbb{Q}) \cdot \Delta : T(\mathbb{Q}) \cdot \Delta(\Pi_\ell)] = [\Delta : \Delta(\Pi_\ell) \cdot (T(\mathbb{Q}) \cap \Delta)].$$

We now observe that since $T(\mathbb{Q}_p) = T(\mathbb{Z}_p)$ for all $p \in \mathbb{P} \setminus \mathbb{P}_{1(4)}$, we have

$$\Gamma := T(\mathbb{Q}) \cap \Delta = T(\mathbb{Q}) \cap \prod_{p\in\mathbb{P}} T(\mathbb{Z}_p) = T(\mathbb{Z}) = \{\pm 1, \pm i\}.$$

As $\Delta = \Gamma(\Pi_\ell) \cdot \Delta(\Pi_\ell)$, we now obtain that

$$i(\Pi_\ell) = [\Gamma(\Pi_\ell) : \Gamma(\Pi_\ell) \cap (\Gamma \cdot \Delta(\Pi_\ell))] = \frac{[\Gamma(\Pi_\ell) : \Gamma(\Pi_\ell) \cap \Delta(\Pi_\ell)]}{[\Gamma(\Pi_\ell) \cap (\Gamma \cdot \Delta(\Pi_\ell)) : \Gamma(\Pi_\ell) \cap \Delta(\Pi_\ell)]]}$$

$$\geq [\Gamma(\Pi_\ell) : \Gamma(\Pi_\ell)^n]/4.$$

But for any $p \in \mathbb{P}_{1(4n)}$, using a $\mathbb{Z}_p$-isomorphism $T \simeq \mathbb{G}_m$, we have

$$[T(\mathbb{Z}_p) : T(\mathbb{Z}_p)^n] = [\mathbb{Z}_p^\times : \mathbb{Z}_p^{\times n}] = [\mathbb{F}_p^\times : \mathbb{F}_p^{\times n}] = n$$

Thus, we get the estimate

$$i(\Pi_\ell) \geq n^\ell/4,$$

and our assertion follows. □

To prove Theorem 3.2.6, we will apply a variation of techniques developed in [14, Ch. 8, §8.2] to compute class numbers of semi-simple groups of noncompact type. We start with the exact sequence of $\mathbb{Q}$-groups and $\mathbb{Q}$-morphisms

$$1 \to F \to \widetilde{G} \xrightarrow{\pi} G \to 1, \tag{3.16}$$

which for every extension $P/\mathbb{Q}$ gives rise to the coboundary map $\psi_P \colon G(P) \to H^1(P, F)$ (cf. Proposition 2.3.2). Applying this to $P = \mathbb{Q}_p$ and taking the product over all $p \in \mathbb{P}_{1(4)}$, we obtain an exact sequence

$$\prod_{p \in \mathbb{P}_{1(4)}} \widetilde{G}(\mathbb{Q}_p) \xrightarrow{\Pi = \prod_p \pi_{\mathbb{Q}_p}} \prod_{p \in \mathbb{P}_{1(4)}} G(\mathbb{Q}_p) \xrightarrow{\Psi = \prod_p \psi_{\mathbb{Q}_p}} \prod_{p \in \mathbb{P}_{1(4)}} H^1(\mathbb{Q}_p, F). \tag{3.17}$$

We let $\pi_{\mathbb{A}(S)}$ and $\psi_{\mathbb{A}(S)}$ denote the restrictions of Π and Ψ to $\widetilde{G}(\mathbb{A}(S))$ and $G(\mathbb{A}(S))$,

respectively. Arguing as in the proof of [14, Proposition 8.8], one shows that

$$\Big(\prod_{p \in \mathbb{P}_{1(4)}} \pi_{\mathbb{Q}_p}(\widetilde{G}(\mathbb{Q}_p)) \Big) \cap G(\mathbb{A}(S)) = \pi_{\mathbb{A}(S)}(\widetilde{G}(\mathbb{A}(S))),$$

which implies the exactness of the following sequence of groups and group homomorphisms

$$\widetilde{G}(\mathbb{A}(S)) \xrightarrow{\pi_{\mathbb{A}(S)}} G(\mathbb{A}(S)) \xrightarrow{\psi_{\mathbb{A}(S)}} \prod_{p \in \mathbb{P}_{1(4)}} H^1(\mathbb{Q}_p, F). \tag{3.18}$$

Lemma 3.2.8 *For every open subgroup U of $G(\mathbb{A}(S))$,*

(i) *The product $G(\mathbb{Q}) \cdot U$ is a normal subgroup of $G(\mathbb{A}(S))$;*

(ii) *The map $\psi_{\mathbb{A}(S)}$ induces a group isomorphism of quotients*

$$G(\mathbb{A}(S))/(G(\mathbb{Q}) \cdot U) \simeq \psi_{\mathbb{A}(S)}(G(\mathbb{A}(S)))/\psi_{\mathbb{A}(S)}(G(\mathbb{Q}) \cdot U).$$

Proof. We argue as in the proof of [14, Proposition 8.8]. First, as we already mentioned, since S is infinite, $\widetilde{G}$ has strong approximation with respect S, and therefore $\widetilde{G}(\mathbb{A}(S)) = \widetilde{G}(\mathbb{Q}) \cdot \pi^{-1}_{\mathbb{A}(S)}(U)$ as $\pi_{\mathbb{A}(S)}$ is continuous (cf. Proposition 2.1.4). Combined with the exactness of (3.18), this yields

$$\ker \psi_{\mathbb{A}(S)} = \pi_{\mathbb{A}(S)}(\widetilde{G}(\mathbb{A}(S))) \subset G(\mathbb{Q}) \cdot U. \tag{3.19}$$

Since $\psi_{\mathbb{A}(S)}$ is a group homomorphism of $G(\mathbb{A}(S))$ to a commutative group, its kernel contains the commutator subgroup $[G(\mathbb{A}(S)), G(\mathbb{A}(S))]$. On the other hand, if the product of two subgroups of an abstract group contains the commutator subgroup of the group, the product is actually a normal subgroup. In conjunction with (3.19), these observations imply (i), and then (ii) follows from the third isomorphism theorem. □

Next, we will apply a similar argument to the Kummer sequence for T:

$$1 \to F \longrightarrow T \xrightarrow{[n]} T \to 1, \tag{3.20}$$

where $[n]$ denotes the morphism of raising to the nth power. Again, for any field extension $P/\mathbb{Q}$, we have the coboundary map $\delta_P \colon T(P) \to H^1(P, F)$ noting that $\ker \delta_P = T(P)^n$. Taking the product over all $p \in \mathbb{P}_{1(4)}$, and restricting the maps to $T(\mathbb{A}(S))$, we obtain an exact sequence similar to (3.15):

$$T(\mathbb{A}(S)) \xrightarrow{[n]} T(\mathbb{A}(S)) \xrightarrow{\delta_{\mathbb{A}(S)}} \prod_{p \in \mathbb{P}_{1(4)}} H^1(\mathbb{Q}_p, F). \tag{3.21}$$

Lemma 3.2.9 (i) *For any field extension $P/\mathbb{Q}$, the coboundary map $\delta_P \colon T(P) \to H^1(P, F)$ is surjective.*

(ii) *There exists a finite set of primes Ω such that for all $p \in \mathbb{P} \setminus \Omega$ we have*

$$\psi_{\mathbb{Q}_p}(G(\mathbb{Z}_p)) = \delta_{\mathbb{Q}_p}(T(\mathbb{Z}_p)).$$

(iii) $\psi_{\mathbb{A}(S)}(G(\mathbb{A}(S))) = \delta_{\mathbb{A}(S)}(T(\mathbb{A}(S)))$.

Proof. (i) In view of the exact sequence

$$T(P) \xrightarrow{\delta_P} H^1(P, F) \xrightarrow{\omega} H^1(P, T)$$

that comes from (3.20), it is enough to show that $\operatorname{im} \omega$ is trivial. By [14, Ch. 2, Lemma 2.22], the group $H^1(P, T)$ is isomorphic to $P^\times / N_{LP/P}((LP)^\times)$, hence has exponent ≤ 2. On the other hand, F is a cyclic group of order n, so $H^1(P, F)$ is annihilated by n. Since by our assumption n is *odd*, the triviality $\operatorname{im} \omega$ follows.

(ii) Let $\mathbb{Q}_p^{\mathrm{ur}}$ be the maximal unramified extension of $\mathbb{Q}_p$. It follows from [14, Ch. 6, Proposition 6.4] that there exists a finite subset $\Omega \subset \mathbb{P}$ such that for $p \in \mathbb{P} \setminus \Omega$ we have $F(\bar{\mathbb{Q}}) = F(\mathbb{Q}_p^{\mathrm{ur}})$ and

$$\psi_{\mathbb{Q}_p}(G(\mathbb{Z}_p)) = H^1(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p, F) = \delta_{\mathbb{Q}_p}(T(\mathbb{Z}_p)).$$

(iii) For every prime p, we have the exact sequence

$$G(\mathbb{Q}_p) \xrightarrow{\psi_{\mathbb{Q}_p}} H^1(\mathbb{Q}_p, F) \longrightarrow H^1(\mathbb{Q}_p, \widetilde{G}).$$

Since $\widetilde{G}$ is semi-simple and simply connected, we have $H^1(\mathbb{Q}_p, \widetilde{G}) = 1$ (cf. [14, Ch. 6, Theorem 6.4]), so

$$\psi_{\mathbb{Q}_p}(G(\mathbb{Q}_p)) = H^1(\mathbb{Q}_p, F) = \delta_{\mathbb{Q}_p}(T(\mathbb{Q}_p))$$

in view of part (i). In conjunction with part (ii), this yields our claim. □

Proof of Theorem 3.2.6. Let Ω be the exceptional set of primes in Lemma 3.2.9(ii). For $\ell \geq 1$, pick a subset $\Pi_\ell \subset \mathbb{P}_{1(4n)} \setminus \Omega$ of size ℓ and set $\Pi_\ell^* := \Pi_\ell \cup \Omega$. We will show that the open subgroups

$$U_\ell := \prod_{p \in \Pi_\ell^*} \pi_{\mathbb{Q}_p}(\widetilde{G}(\mathbb{Q}_p)) \times \prod_{p \in \mathbb{P}_{1(4)} \setminus \Pi_\ell^*} G(\mathbb{Z}_p)$$

satisfy (3.13). Indeed, by construction we have the inclusion $\psi_{\mathbb{A}(S)}(U_\ell) \subset \delta_{\mathbb{A}(S)}(\Delta(\Pi_\ell))$, and it follows from Lemma 3.2.9(i) that $\psi_{\mathbb{Q}}(G(\mathbb{Q})) \subset \delta_{\mathbb{Q}}(T(\mathbb{Q}))$. According to Lemma 3.2.8, the product $G(\mathbb{Q}) \cdot U_\ell$ is a normal subgroup of $G(\mathbb{A}(S)$, with the quotient isomorphic to $\psi_{\mathbb{A}(S)}(G(\mathbb{A}(S)))/\psi_{\mathbb{A}(S)}(G(\mathbb{Q}) \cdot U_\ell)$. The latter admits an epi-

morphism on

$$\delta_{\mathbb{A}(S)}(T(\mathbb{A}(S)))/\delta_{\mathbb{A}(S)}(T(\mathbb{Q})\cdot\Delta(\Pi_\ell)) \simeq T(\mathbb{A}(S))/T(\mathbb{Q})\cdot\Delta(\Pi_\ell)\cdot T(\mathbb{A}(S))^n$$

(the isomorphism follows from the exact sequence (3.21)). Thus,

$$[G(\mathbb{A}(S)) : G(\mathbb{Q})\cdot U_\ell] \geq i(\Pi_\ell),$$

and then (3.13) follows from Lemma 3.2.7.

3.3 Application to congruence subgroup problem

3.3.1 Overview of the congruence subgroup problem.

Let G be a linear algebraic group defined over a global field K. Given a subset $S \subset V^K$ containing V_∞^K, we let $\mathcal{O}_K(S)$ denote the corresponding ring of S-integers. First, we fix a faithful K-defined representation $\iota\colon G \hookrightarrow \mathrm{GL}_n$, which enables us to speak unambiguously about the group of $\mathcal{O}_K(S)$-points $\Gamma_S = G(\mathcal{O}_K(S))$ and its congruence subgroups $\Gamma_S(\mathfrak{a}) = G(\mathcal{O}_K(S),\mathfrak{a})$ for (nonzero) ideals $\mathfrak{a} \subset \mathcal{O}_K(S)$ – these are defined respectively as $\iota^{-1}(\iota(G(K)) \cap \mathrm{GL}_n(\mathcal{O}_K(S)))$ and $\iota^{-1}(\iota(G(K)) \cap \mathrm{GL}_n(\mathcal{O}_K(S),\mathfrak{a}))$, where

$$\mathrm{GL}_n(\mathcal{O}_K(S),\mathfrak{a}) = \Big\{X \in \mathrm{GL}_n(\mathcal{O}_K(S)) \,|\, X \equiv I_n (\mathrm{mod}\ \mathfrak{a})\Big\}.$$

Then $\Gamma_S(\mathfrak{a})$ is a finite index normal subgroup of Γ_S for any nonzero ideal $\mathfrak{a}$, and the *Congruence Subgroup Problem* (CSP) for Γ_S in its classical formulation is the question of whether every finite index normal subgroup of Γ_S contains a suitable congruence subgroup $\Gamma_S(\mathfrak{a})$. We refer the reader to the surveys [19] and [24] for

a discussion of various approaches developed to attack the CSP, and of the results obtained using these techniques. Here we only recall the reformulation of the CSP suggested by J.-P. Serre [31].

Let $\mathcal{N}_a^S$ (resp., $\mathcal{N}_c^S$) be the family of all finite index normal subgroups $N \subset \Gamma_S$ (resp., of all congruence subgroups $\Gamma_S(\mathfrak{a})$ for nonzero ideals $\mathfrak{a} \subset \mathcal{O}(S)$). Then there are topologies τ_a^S and τ_c^S (called the *S-arithmetic* and *S-congruence* topologies) on the group $G(K)$ that are compatible with the group structure and have $\mathcal{N}_a^S$ and $\mathcal{N}_c^S$ respectively as fundamental systems of neighborhoods of the identity. Furthermore, $G(K)$ admits completions with respect to the uniform structures associated with τ_a^S and τ_c^S that will be denoted $\widehat{G}^S$ and $\overline{G}^S$. Since τ_a^S is apriori stronger than τ_c^S, there exists a continuous group homomorphism $\pi\colon \widehat{G}^S \to \overline{G}^S$, which turns out to be surjective. Its kernel $C^S(G) := \ker \pi$ is a profinite group called the *S-congruence kernel*. Thus, we have the following exact sequence of locally compact topological groups

$$1 \to C^S(G) \longrightarrow \widehat{G}^S \xrightarrow{\pi} \overline{G}^S \to 1. \tag{CSP}$$

It is easy to see that the affirmative answer to the classical congruence subgroup problem for Γ amounts to fact that the topologies τ_a^S and τ_c^S coincide, which turns out to be equivalent to $C^S(G) = \{1\}$. In the general case, $C^S(G)$ measures the difference between the two topologies. So, Serre proposed to reinterpet the CSP as the problem of computation of $C^S(G)$ (it should be noted that the latter does not depend on the initial choice of the faithful representation ι). Furthermore, he formulated the following conjecture that qualitatively describes $C^S(G)$ in the main case where G is absolutely almost simple and simply connected and S is finite: *if* $\mathrm{rk}_S G := \sum_{v\in S} \mathrm{rk}_{K_v} G \geq 2$ *and* $\mathrm{rk}_{K_v} G > 0$ *for all* $v \in S \setminus V_\infty^K$ *then* $C^S(G)$ *should be finite, and if* $\mathrm{rk}_S G = 1$ *then it should be infinite.* In fact, if the Margulis-Platonov conjecture concerning the normal subgroup structure of $G(K)$ holds - see below, the

finiteness of $C^S(G)$ is equivalent to its *centrality* (i.e., to the fact that (CSP) is a central extension), in which case it is isomorphic to the *metaplectic kernel* $M(S,G)$ that was computed in [17] in all cases relevant to the CSP.

In this thesis, we are interested only in the higher rank part of Serre's conjecture which has been confirmed in a number of cases (see [19], [24]). Nevertheless, it remains completely open for anisotropic groups of types A_n (both inner and outer forms) and E_6, triality forms of type ${}^{3,6}\mathsf{D}_4$, and some other situations. Some evidence for Serre's conjecture in these cases has been generated through the investigation of CSP for *infinite* S. More precisely, the truth of Serre's conjecture combined with computations of the metaplectic kernel in [17] would imply that $C^S(G) = \{1\}$ for *any* infinite S such that $\mathrm{rk}_{K_v} G > 0$ for all $v \in S \setminus V_\infty^K$, so efforts have been made to prove this for certain infinite S. In particular, in [20] this was proved for absolutely almost simple simply connected groups of all types when S contains all but finitely many valuations in a generalized arithmetic progression, with an argument not requiring any case-by-case considerations. Subsequently, Radhika and Raghunathan [22] focused on anisotropic inner forms of type A_n (which are all of the form $\mathrm{SL}_{1,D}$ for some central division K-algebra D) and extended the result of [20] to a class of sets S which basically coincides with our tractable sets. We will use our results on almost strong approximation for tori to prove that $C^S(G) = \{1\}$ for all tractable sets S – see Theorem B for the precise formulation. We note that this formulation includes the Margulis-Platonov conjecture (MP) - see [14, §9.1] for a discussion, which we now recall for the reader's convenience:

Let G be an absolutely almost simple simply connected algebraic group over a global field K. Set $\mathcal{A} = \{v \in V_f^K \mid \mathrm{rk}_{K_v} G = 0\}$, and let $\delta\colon G(K) \to G_{\mathcal{A}} := \prod_{v\in\mathcal{A}} G(K_v)$ be the diagonal map. Then for every noncentral normal subgroup $N \subset G(K)$ there exists an open normal subgroup $W \subset G_{\mathcal{A}}$ such that $N = \delta^{-1}(W)$. In particular, if

$\mathcal{A} = \varnothing$ (which is always the case if the type of G is different from A_n), the group $G(K)$ does not have any proper noncentral normal subgroups.

For results on (MP) obtained prior to 1990 – see [14, Ch. IX]. Subsequently, (MP) was proved also for all anisotropic inner forms of type A_n – see [25], [29], which explains why no assumption on the truth of (MP) is made in [22].

3.3.2 Proof of Theorem B

Our argument will be an adaptation of the proof of Theorem B in [20]. We will freely use the notations introduced in the statement of Theorem B. In particular, G will denote an absolutely almost simple simply connected algebraic group defined over a global field K, and $S \subset V^K$ be a tractable set of valuations that contains a set of the form $V_\infty^K \cup (\mathcal{P}(L/K, \mathcal{C}) \setminus \mathcal{P}_0)$ in our standard notations. Furthermore, we let $\mathcal{A} = \{v \in V_f^K \mid \mathrm{rk}_{K_v} G = 0\}$ denote the (finite) set of nonarchimedean places where G is anisotropic as in the statement of the Margulis-Platonov conjecture above. We will prove Theorem B by analyzing the exact sequence (CSP) written for another set of valuations $\tilde{S}$ such that $V_\infty^K \subset \tilde{S} \subset S$ and $S \setminus \tilde{S}$ is finite. First, let $\tilde{S}$ be any such set, and let

$$1 \to C^{\tilde{S}}(G) \longrightarrow \widehat{G}^{\tilde{S}} \xrightarrow{\tilde{\pi}} \overline{G}^{\tilde{S}} \to 1 \tag{3.22}$$

be the congruence subgroup sequence (CSP) for the set $\tilde{S}$. It easily follows from the definitions that the $\tilde{S}$-congruence topology $\tau_c^{\tilde{S}}$ on $G(K)$ coincides with the $\tilde{S}$-adelic topology induced by the embedding $G(K) \hookrightarrow G(\mathbb{A}_K(\tilde{S}))$. Now, since $\tilde{S}$ is infinite, G has strong approximation with respect to $\tilde{S}$, implying that the completion $\overline{G}^{\tilde{S}}$ can be identified with $G(\mathbb{A}_K(\tilde{S}))$. Next, it is enough to prove that (3.22) is a central extension for *some* $\tilde{S}$ as above. Indeed, using the truth of (MP) and the assumption

that

$$\mathcal{A} \cap S = \varnothing, \tag{3.23}$$

one shows that the congruence kernel $C^{\tilde{S}}(G)$ is isomorphic to (the dual of) the metaplectic kernel $M(\tilde{S}, G)$ (cf. [24]). Again, since $\tilde{S}$ is infinite, the results of [17] imply that $M(\tilde{S}, G) = \{1\}$, hence $C^{\tilde{S}}(G) = \{1\}$. Since $S \supset \tilde{S} \supset V_\infty^K$, there is a natural homomorphism $C^{\tilde{S}}(G) \to C^S(G)$, which because of (3.23) is surjective (cf. [23, Lemma 6.2]). So, $C^S(G) = \{1\}$, as required.

In order to choose $\tilde{S}$ and establish the centrality of the corresponding sequence (3.22), we will use two statements from [20]. To formulate these, we need to introduce some additional notations. Let $v \in V^K$, and let T be a maximal K_v-torus of G. We let T^{reg} denote the Zariski-open subset of T consisting of *regular semi-simple elements* (cf. [15, §2.1.11]), and consider the map

$$\varphi_{v,T} \colon G(K_v) \times T^{\mathrm{reg}}(K_v) \to G(K_v)$$

$$(g, t) \mapsto gtg^{-1}$$

It follows from the Implicit Function Theorem (cf. [15, Ch. III]) that $\varphi_{v,T}$ is an open map, and in particular $\mathcal{U}(v, T) := \varphi_{v,T}(G(K_v) \times T^{\mathrm{reg}}(K_v))$ is open in $G(K_v)$. We also note that by construction there are natural maps $G(K) \to \widehat{G}^{\tilde{S}}$ and $G(K) \to \overline{G}^{\tilde{S}}$ (in other words, the exact sequence (3.22) splits over $G(K)$). In particular, if $t \in G(K)$ is a regular semi-simple element and $T = Z_G(t)$ is the corresponding torus[2], we can consider t as an element of both $\widehat{G}^{\tilde{S}}$ and $\overline{G}^{\tilde{S}}$, and then

$$\tilde{\pi}(Z_{\widehat{G}^{\tilde{S}}}(t)) \subset Z_{\overline{G}^{\tilde{S}}}(t) = T(\mathbb{A}_K(\tilde{S}))$$

[2]We note that the centralizer $Z_G(t)$ is automatically connected since G is simply connected.

(under the identification of $\overline{G}^{\tilde{S}}$ with $G(\mathbb{A}_K(\tilde{S}))$). We can now formulate a sufficient condition (in fact, a criterion) for the centrality of (3.22).

Theorem 3.3.1 ([20, Theorem 3.1(ii)]) *Assume that $G(K)$ satisfies (MP) and that $\mathcal{A} \cap \tilde{S} = \varnothing$, and suppose that there is an integer $m > 1$, a finite subset $V \subset V^K \setminus \tilde{S}$, and a maximal K_v-torus T_v of G for each $v \in V$ such that for any element $t \in G(K) \cap \prod_{v \in V} \mathcal{U}(v, T_v)$ (which is automatically regular semi-simple) and the corresponding torus $T = Z_G(t)$, the following inclusion holds:*

$$T(\mathbb{A}_K(\tilde{S}))^m \subset \tilde{\pi}(Z_{\widehat{G}^{\hat{s}}}(t)). \tag{3.24}$$

Then (3.22) is a central extension.

In order to be able to verify condition (3.24) using our results on almost strong approximation, we will need to choose $\tilde{S}$ appropriately. This is done using the following statement.

Lemma 3.3.2 ([20, Lemma 5.5]) *Let G be an absolutely almost simple simply connected algebraic group defined over a global field K, and let M be the minimal Galois extension of K over which G is an inner form. Furthermore, suppose we are given a finite subset $\mathbb{S} \subset V^K$ and a finite Galois extension L/K. Then there exists a finite subset $V \subset V^K \setminus \mathbb{S}$ and maximal K_v-tori T_v of G for each $v \in V$ such that for any $t \in G(K) \cap \prod_{v \in V} \mathcal{U}(v, T_v)$, the minimal splitting field P_T of the corresponding torus $T = Z_G(t)$ satisfies*

$$P_T \cap L = M \cap L.$$

We are now in a position to complete the proof of Theorem B. Let L/K be the Galois extension involved in the description of the generalized arithmetic progression in the statement of the theorem, and let M/K be the minimal Galois extension over

which G becomes an inner form. Applying Lemma 3.3.2 with $\mathbb{S} = \mathcal{A} \cup V_\infty^K$, we find a finite subset $V \subset V^K \setminus \mathbb{S}$ and maximal K_v-tori T_v of G for $v \in V$ so that for any $t \in G(K) \cap U$, where $U = \prod_{v \in V} \mathcal{U}(v, T_v)$, and the torus $T = Z_G(t)$ we have

$$P \cap L = M \cap L, \tag{3.25}$$

where P is the minimal splitting field of T. Set $\tilde{S} = S \setminus V$ (which is obviously tractable), and let $m = \tilde{C}(d, n)$ (the constant from Theorem 3.1.3) with $d = \operatorname{rk} G$ and $n = [L : K]$. We will now show that the assumptions of Theorem 3.3.1 hold true for this $\tilde{S}$, so the theorem will yield the centrality of (3.22), completing the argument. Let $t \in G(K) \cap U$ and $T = Z_G(t)$. Then (3.25) for the splitting field P of T, and therefore $\sigma|(P \cap L) = \mathrm{id}_{P \cap L}$ for some $\sigma \in \mathcal{C}$. Applying Theorem 3.1.3, we conclude that the index $[T(\mathbb{A}_K(\tilde{S})) : \overline{T(K)}^{(\tilde{S})}]$ divides m, and consequently,

$$T(\mathbb{A}_K(\tilde{S}))^m \subset \overline{T(K)}^{(\tilde{S})}. \tag{3.26}$$

On the other hand, since $C^{\tilde{S}}(G)$ is compact, the map $\tilde{\pi}$ is proper, so the image $\tilde{\pi}(Z_{\widehat{G}^{\tilde{S}}}(t))$ is closed in $\overline{G}^{\tilde{S}}$. In view of the obvious inclusion $Z_{\widehat{G}^{\tilde{S}}}(t) \supset T(K)$, we get the inclusion $\overline{T(K)}^{(\tilde{S})} \subset \tilde{\pi}(Z_{\widehat{G}^{\tilde{S}}}(t))$, which in conjunction with (3.26) verifies (3.24) and completes the argument.

List of symbols

$\varnothing$ empty set
$\mathbb{Z}$ ring of integers
$\mathbb{Q}$ field of rational numbers
$\mathbb{Z}_p$ ring of p-adic integers
$\mathbb{Q}_p$ field of p-adic integers
$\mathbb{Q}_p^{\mathrm{ur}}$ maximal unramified extension of $\mathbb{Q}_p$
$\mathbb{R}$ field of real numbers
$\mathbb{R}_{>0}$ set of all positive real numbers
$\mathbb{C}$ field of complex numbers
$\mathbb{F}_q$ finite field with q elements
$k(t)$ field of rational functions in one variable t over a field k
$k((t))$ field of Laurent series in one variable t over a field k
K field
$\mathrm{char}(K)$ characteristic of K
$\bar{K}$ separable closure of K
K^+ additive group of K
$K^\times$ multiplicative group of K
$K^{\times n}$ subgroup of nth powers of $K^\times$
μ_n group of nth root of unity in a given field K
$\mathcal{O}_K$ ring of integers of K
$\mathcal{O}_K(S)$ ring of S-integers of K
$\mathcal{N}(\mathfrak{a})$ norm of an ideal $\mathfrak{a}$ of $\mathcal{O}_K$
$\mathcal{I}_K$ group of fractional ideals of K
$\mathcal{P}_K$ group of principal fractional ideals of K
$\mathrm{Cl}(K)$ ideal class group of K
$h(K)$ class number of K
$|\cdot|_p$ p-adic absolute value on $\mathbb{Q}$
$|\cdot|_\infty$ archimedean absolute value on $\mathbb{Q}$
v_p p-adic valuation on $\mathbb{Q}$
v_∞ archimedean valuation on $\mathbb{Q}$
V^K set of all valuations of K
V_∞^K set of all archimedean valuations of K
V_f^∞ set of all nonarchimedean valuations of K

V_r^K set of all real valuations of K
S subset of V^K
$|\cdot|_v$ v-adic absolute value associated with valuation v
K_v completion of K with respect to a valuation v
$\mathcal{O}_v$ valuation ring of v in K_v
$\mathfrak{p}_v$ valuation ideal of v in $\mathcal{O}_v$
$k(v)$ residue field of $v \in V_f^K$
$\mathfrak{p}(v)$ prime ideal $\mathfrak{p}_v \cap \mathcal{O}_K$
$[L:K]$ degree of field extension L/K
$e(w|v)$ ramification index of w with respect to v
$f(w|v)$ residue degree of w with respect to v
$\prod'_{i\in I}(X_i, U_i)$ restricted product of $\{X_i\}_{i\in I}$ with respect to $\{U_i\}_{i\in I}$
$\mathbb{A}_K$ ring of adeles of a field K
$\mathbb{A}_{K,\infty}$ ring of integral adeles of field K
$\mathbb{A}_K(S)$ ring of S-adeles of field K
$\mathbb{A}(S)$ ring of S-adeles of $\mathbb{Q}$
$\mathbb{I}_K$ group of ideles of field K
$\mathbb{I}_K(S)$ group of S-ideles of field K
$\mathbb{I}(S)$ group of S-ideles of $\mathbb{Q}$
C_K idele class group of K
$\mathbb{I}_{K,\infty}$ group of integral ideles of K
$\mathbb{I}_K^{(1)}$ group of ideles of K with content 1
$\mathbb{U}(S)$ distinguished open subgroup $\prod_{v\in V^K\setminus S}\mathcal{O}_v^\times$ in $\mathbb{I}_K(S)$
$\mathbb{E}(S)$ group of S-units in K, i.e. $\mathbb{U}(S)\cap K^\times$
$\mathrm{Gal}(L/K)$ Galois group of field extension L/K
$N_{L/K}$ norm associated with field extension L/K
$\mathrm{Tr}_{L/K}$ trace associated with field extension L/K
$w|v$ valuation w lies above valuation v
$\mathrm{Fr}_{L/K}(w|v)$ Frobenius automorphism for $v \in V_f^K$ unramified in L and $w|v$
$\psi_{L/K}$ Artin map associated with a finite Galois extension L/K
$(a,b)_K$ Hilbert symbol of a and b relative to K
$\mathbb{P}$ set of all rational primes
(a,b) greatest common divisor of integers a and b
$a \nmid b$ a does not divide b
$a \equiv b (\mathrm{mod}\, m)$ a is congruent to b modulo m
$\mathbb{P}_{a(m)}$ arithmetic progression of all prime numbers p such that $p \equiv a(\mathrm{mod}\, m)$
$\mathcal{P}(L/K, \mathcal{C})$ generalized arithmetic progression defined by a Galois extension L/K and a conjugacy class $\mathcal{C} \subset \mathrm{Gal}(L/K)$
$\mathfrak{d}(\mathcal{P})$ Dirichlet density of any subset of rational primes $\mathcal{P} \subset \mathbb{P}$
$\mathfrak{d}_K(\mathcal{P})$ Dirichlet density of any subset of valuations $\mathcal{P} \subset V_f^K$
φ Euler totient function
$\mathrm{Spl}(L/K)$ set of all $v \in V_f^K$ that split completely in L for a field extension L/K

$A \dot{\subset} B$ set of valuations B almost contains a subset $A \subset B$
$[G, G]$ commutator subgroup of group G
G^{ab} abelianization of group G
$Z(G)$ center of group G
$Z_G(t)$ centralizer of an element t of group G
$M_n(K)$ algebra of n by n matrices over a field K
I_n identity n by n matrix
X^t transpose of a matrix X
G° connected component of linear algebraic group G
GL_n general linear group
SL_n special linear group
$\mathbb{G}_m$ multiplicative group of a field
O_n orthogonal group
SU_n special unitary group
$\mathbb{G}_a$ additive group of a field
$\mathrm{SL}_{1,D}$ group of elements of a finite dimensional central division K-algebra D with reduced norm one
T algebraic torus
$\mathrm{R}_{L/K}(G)$ restriction of scalars of L-group G with respect to field extension L/K
$\mathrm{R}_{L/K}(\mathbb{G}_m)$ quasi-split torus associated with field extension L/K
$\mathrm{R}^{(1)}_{L/K}(\mathbb{G}_m)$ norm torus associated with field extension L/K
$R(G)$ radical of G
$R_u(G)$ unipotent radical of G
$[G, G]$ commutator subgroup of G
$G(\mathbb{A}_K(S))$ group of S-adeles of G
f_K map induced on K-points by a morphism f of K-varieties
$f_{\mathbb{A}_K(S)}$ adelization of a morphism f with respect to subset $S \subset V^K$
$\overline{G(K)}^{(S)}$ closure of the group $G(K)$ diagonally embedded into $G(\mathbb{A}_K(S))$
$X(T)$ group of characters of T
$X_*(T)$ group of co-characters of T
$\mathbb{Z}[G]$ group ring of G over $\mathbb{Z}$
$K[G]$ affine algebra of regular functions of G over K
$K[X(T)]$ group algebra corresponding to character group $X(T)$ of a K-torus
$C_K(T)$ abelian group $\mathrm{Hom}(X(T), C_K)$
A^G group of G-fixed points of G-module A
$F^1(G, A)$ abelian group of all functions from group G to a G-module A
$Z^1(G, A)$ set of all 1-cocycles from G to A
$B^1(G, A)$ set of all 1-coboundaries of G with values in A
$\mathrm{Hom}(G, A)$ set of all group homomorphisms of G with values in A
$H^i(G, A)$ ith cohomology group of G with values in A
$H_i(G, A)$ ith homology group of G with values in A
$\hat{H}^i(G, A)$ ith Tate cohomology group of G with values in A

$\mathcal{A}$ set of all valuations v in V_f^K such that G is K_v-anisotropic
Γ_S group $G(\mathcal{O}_K(S))$ of S-integral points of G
$\Gamma_S(\mathfrak{a})$ principal S-congruence subgroup of level $\mathfrak{a}$
$\mathcal{N}_a^S$ family of all finite index normal subgroups in Γ_S
$\mathcal{N}_c^S$ family of all principal S-congruence subgroups in Γ_S
τ_a^S S-arithmetic topology
τ_c^S S-congruence topology
$\widehat{G}^S$ S-arithmetic completion of G
$\overline{G}^S$ S-congruence completion of G
$C^S(G)$ S-congruence kernel of G with respect to S
$M(S,G)$ S-metaplectic kernel of G

Bibliography

[1] A. Borel, *Linear Algebraic Groups,* 2nd enlarged edition, GTM 126, Springer, 1991.

[2] J.W.S. Cassels and A. Fröhlich, *Algebraic Number Theory*, 2nd edition, London Math. Soc., (1967), 162-202.

[3] N. Childress, *Class Field Theory*, Springer, (2009).

[4] B. Conrad, O. Gabber, G. Prasad, *Pseudo-reductive Groups*, 2nd edition, Cambridge Univ. Press, (2015), 422-441.

[5] M. Demazure, A. Grothendieck, *Structure des Schémas en Groupes Réductifs,* 153, Springer-Verlag, New York (1970), 352-353.

[6] D.S. Dummit and R.M. Foote, *Abstract Algebra,* Third edition. John Wiley & Sons. (2004), 798-831.

[7] J.E. Humphreys, *Linear Algebraic Groups,* Springer-Verlag, (1975), 51-105.

[8] G.J. Janusz, *Algebraic Number Fields,* 2nd edition, GSM 7, AMS, (1996), 135-167.

[9] M. Kneser, *Normalteiler ganzzahliger Spingruppen,* J. Reine und Angew. Math., **311**/**312**(1979), 191-214.

[10] S. Lang, *Algebra,* Revised Third Edition, Springer, (2002).

[11] G.A. Margulis, *Cobounded subgroups in algebraic groups over local fields,* Funct. Anal. Appl. **11**(1977), 119-128.

[12] J. Neukirch, *Algebraic Number Theory,* Springer, (2010), 542-549.

[13] V.P. Platonov, *The problem of strong approximation and the Kneser-Tits conjecture for algebraic groups,* Math. USSR Izv. **3**(1969), 1139-1147.

[14] V. Platonov, A. Rapinchuk, *Algebraic groups and Number Theory,* Academic Press, (1993).

[15] V. Platonov, A. Rapinchuk, I. Rapinchuk, *Algebraic groups and Number Theory,* Cambridge University Press, (2023).

[16] G. Prasad, *Strong approximation for semisimple groups over function fields,* Ann. math. **105**(1977), 553-572.

[17] G. Prasad and A.S. Rapinchuk, *Computation of the metaplectic kernel,* Publ. Math. Inst. Hautes Études Sci. no. **84**(1996), 91–187.

[18] G. Prasad, A.S. Rapinchuk, *Irreducible tori in semisimple groups,* IMRN (2001), No. **23**, 1229–1242.

[19] G. Prasad, A.S. Rapinchuk, *Developments on the congruence subgroup problem after the work of Bass, Milnor and Serre,* in: Collected works of John Milnor, vol. V 'Algebra,' AMS (2010), 307-325.

[20] G. Prasad, A.S. Rapinchuk, *On the congruence kernel for simple algebraic groups,* Proc. Steklov Inst. Math. **292**(2016), No. 1, 216–246.

[21] G. Prasad, A.S. Rapinchuk, *Weakly commensurable arithmetic groups and isospectral locally symmetric spaces,* Publ. Math. Inst. Hautes Études Sci., Vol. 109 (2009), 113-184.

[22] M.M. Radhika, M.S. Raghunathan, *On the congruence subgroup problem for anisotropic groups of inner type A_n,* Math. Z. **295**(2020), 583-594.

[23] M.S. Raghunathan, *On the congruence subgroup problem,* Publ. Math. Inst. Hautes Études Sci. No. **46**(1976), 107–161.

[24] A. Rapinchuk, *Congruence subgroup problem for algebraic groups: old and new*, Journées Arithmétiques, No.**209**(1992), 73–84.

[25] A.S. Rapinchuk, *The Margulis-Platonov conjecture for* $\mathrm{SL}_{1,D}$ *and 2-generation of finite simple groups,* Math. Z. **252**(2006), No. 2, 295–313.

[26] A.S. Rapinchuk, *Strong approximation for algebraic groups,* Thin groups and superstrong approximation, 269–298, Math. Sci. Res. Inst. Publ., 61, Cambridge Univ. Press, Cambridge (2014), 269-295.

[27] J.J. Rotman, *An Introduction to Homological Algebra,* Pure and Applied Mathematics, Academic Press, Inc. Harcourt Brace Jovanovich, Publishers, New York-London, No. **85**(1979), 292-293.

[28] P. Samuel, *Algebraic Theory of Numbers,* Hermann, Publishers in Arts and Sciences. (1970).

[29] Y. Segev, *On finite homomorphic images of the multiplicative group of a division algebra,* Ann. math. No. 1, **149**(1999), 219–251.

[30] J.P. Serre, *A Course in Arithmetic*, Springer. (1973).

[31] J.P. Serre, *Le problème des groupes de congruence pour* SL_2*,* Ann. of Math., No. **92**(1970), 489-527.

[32] J.P. Serre, *Local Fields*, Springer-Verlag. (1979).

[33] T.A. Springer, *Linear Algebraic Groups,* Birkhäuser, Second Edition, Vol. **9**(1998).

[34] J. Voight, *Quaternion algebras,* Springer. (2021).

[35] V.E. Voskresenskii, *Algebraic groups and their birational invariants,* Translations of Mathematical Monographs, American Mathematical Society, Providence, RI, No. **179** (1998), 114-117.