Hecke Algebra Isomorphisms and Adelic Points on Algebraic Groups

Gunther Cornelissen and Valentijn Karemaker

Received: May 20, 2016
Revised: January 20, 2017

Communicated by Dan Ciubotaru

Abstract. Let G denote a linear algebraic group over $\mathbf{Q}$ and K and L two number fields. We establish conditions on the group G, related to the structure of its Borel groups, under which the existence of a group isomorphism $G(\mathbf{A}_{K,f}) \cong G(\mathbf{A}_{L,f})$ over the finite adeles implies that K and L have isomorphic adele rings. Furthermore, if G satisfies these conditions, K or L is a *Galois* extension of $\mathbf{Q}$, and $G(\mathbf{A}_{K,f}) \cong G(\mathbf{A}_{L,f})$, then K and L are isomorphic as fields.

We use this result to show that if for two number fields K and L that are Galois over $\mathbf{Q}$, the finite Hecke algebras for $\mathrm{GL}(n)$ (for fixed $n \geq 2$) are isomorphic by an isometry for the L^1-norm, then the fields K and L are isomorphic. This can be viewed as an analogue in the theory of automorphic representations of the theorem of Neukirch that the absolute Galois group of a number field determines the field, if it is Galois over $\mathbf{Q}$.

2010 Mathematics Subject Classification: 11F70, 11R56, 14L10, 20C08, 20G35, 22D20
Keywords and Phrases: algebraic groups, adeles, Hecke algebras, arithmetic equivalence

1. Introduction

Suppose that G is a linear algebraic group over $\mathbf{Q}$, and K and L are two number fields such that the (finite adelic) Hecke algebras for G over K and L are isomorphic. As we will see, a closely related hypothesis is: suppose that the groups of finite adelic

Part of this work was done when the authors visited the University of Warwick; we are grateful to Richard Sharp for hosting us. The second author would like to thank Jan Nekovář for interesting discussions. We thank Manfred Lochter for sending us a copy of [21], Dipendra Prasad for pointing us to existing results on isomorphisms of point groups over rings, and Julia Hartmann, Wilberd van der Kallen, Bart de Smit, Maarten Solleveld, and the referee for helpful comments on an earlier version of this paper.

points on G are isomorphic for K and L. What does this imply about the relationship between the fields K and L? Before stating the general result, let us discuss an example.

Example A. If $G = \mathbf{G}_a^r \times \mathbf{G}_m^s$ for any integers r, s, then for any two distinct imaginary quadratic fields K and L of discriminant < -8 we have an isomorphism of topological groups $G(\mathbf{A}_{K,f}) \cong G(\mathbf{A}_{L,f})$ while $\mathbf{A}_K \not\cong \mathbf{A}_L$ and $\mathbf{A}_{K,f} \not\cong \mathbf{A}_{L,f}$ (cf. Section 2). To prove this, one determines separately the abstract structures of the additive and multiplicative groups of the adele ring $\mathbf{A}_K$ and sees that they depend on only a few arithmetic invariants, allowing for a lot of freedom in "exchanging local factors". This example illustrates that at least some condition on the rank, unipotent rank, and action of the torus on the unipotent part will be required to deduce that we have a ring isomorphism $\mathbf{A}_K \cong \mathbf{A}_L$.

Let us now state the main technical condition, which we will elaborate on in Section 3.

Definition B. Let G denote a linear algebraic group over $\mathbf{Q}$. We call G *fertile* for a field $K/\mathbf{Q}$ if G contains a Borel group B which is split over K as $B = T \ltimes U$ with $T \neq \{1\}$ and $U \neq \{0\}$, and such that over K, the split maximal torus T acts non-trivially by conjugation on the abelianisation of the maximal unipotent group U. In Appendix A, it is shown that G being fertile for K is equivalent to G containing a K-split maximal torus and having a connected component which is *not* a direct product of a torus and a unipotent group.

Split tori and unipotent groups are not fertile for any K. On the other hand, for $n \geq 2$, $\mathrm{GL}(n)$ is fertile for all K. In general, fertility is slightly stronger than non-commutativity. Roughly speaking, it says that the group has semisimple elements that do not commute with certain unipotent elements.

Our first main result is:

Theorem C. *Let K and L be two number fields, and let G denote a linear algebraic group over $\mathbf{Q}$ which is fertile for K and L. There is a topological group isomorphism of finite adelic point groups $G(\mathbf{A}_{K,f}) \cong G(\mathbf{A}_{L,f})$ if and only if there is a topological ring isomorphism $\mathbf{A}_K \cong \mathbf{A}_L$.*

An isomorphism of adele rings $\mathbf{A}_K \cong \mathbf{A}_L$ implies (but is generally stronger than) arithmetic equivalence of K and L (Komatsu [20], cf. [18, VI.2]). Recall that K and L are said to be arithmetically equivalent if they have the same Dedekind zeta function: $\zeta_K = \zeta_L$. If K or L is a Galois extension of $\mathbf{Q}$, then this is known to imply that K and L are isomorphic as fields (Gaßmann [9], cf. [18, III.1]).
The question whether $G(R) \cong G(S)$ for algebraic groups G and rings R, S implies a ring isomorphism $R \cong S$ has been considered before (following seminal work of van der Waerden and Schreier from 1928 [36]), most notably when $G = \mathrm{GL}_n$ for $n \geq 3$ or when G is a Chevalley group and R and S are integral domains (see, e.g., [6], [31] and the references therein). The methods employed there make extensive use of root data and Lie algebras.
By contrast, our proof of Theorem C uses number theory in adele rings and, by not passing to Lie algebras, applies to a more general class of (not necessarily reductive)

algebraic groups. First, we prove in general that maximal divisible subgroups $\mathbf{D}$ of $G(\mathbf{A}_{K,f})$ and maximal unipotent point groups are the same up to conjugacy (Proposition 4.8; note that this does not apply at the archimedean places). The torus $\mathbf{T}$ (as a quotient of the normaliser $\mathbf{N}$ of the unipotent point group $\mathbf{D}$ by itself) acts on the abelian group $\mathbf{V} = [\mathbf{N}, \mathbf{D}]/[\mathbf{D}, \mathbf{D}]$, that decomposes as a sum of one-dimensional $\mathbf{T}$-modules, on which $\mathbf{T}$ acts by multiplication with powers. Now we use a formula of Siegel, which allows us to express any adele as a linear combination of fixed powers, to show how this implies that the centre of the endomorphism ring of the $\mathbf{T}$-module $\mathbf{V}$ is a a cartesian power of the finite adele ring. We then use the structure of the maximal principal ideals in the finite adele ring to find from these data the adele ring itself.

EXAMPLE D. Consider $G = \mathrm{GL}(2)$. Then $\mathbf{D} = \left(\begin{smallmatrix} 1 & \mathbf{A}_{K,f} \\ 0 & 1 \end{smallmatrix}\right) \cong (\mathbf{A}_{K,f}, +)$ is (conjugate to) a group of strictly upper triangular matrices, $\mathbf{N} = \begin{pmatrix} \mathbf{A}^*_{K,f} & \mathbf{A}_{K,f} \\ 0 & \mathbf{A}^*_{K,f} \end{pmatrix}$ and $\mathbf{T} \cong (\mathbf{A}^*_{K,f}, \cdot)^2$ (represented as diagonal matrices) acts on $\mathbf{V} \cong \mathbf{D}$, represented as upper triangular matrices, by multiplication. Now $\mathrm{End}_{\mathbf{T}}\mathbf{V} \cong \mathbf{A}_{K,f}$ as (topological) rings.

By the (finite adelic) *Hecke algebra* for G over K, we mean the convolution algebra $\mathscr{H}_G(K) := C_c^\infty(G(\mathbf{A}_{K,f}), \mathbf{R})$ of locally constant compactly supported real-valued functions on $G(\mathbf{A}_{K,f})$. By an L^1-*isomorphism* of Hecke algebras we mean one that respects the L^1-norm. The second main result is the following:

THEOREM E. *Let K and L be two number fields, and let G denote a linear algebraic group over $\mathbf{Q}$ that is fertile for K and L. There is an L^1-isomorphism of Hecke algebras $\mathscr{H}_G(K) \cong \mathscr{H}_G(L)$ if and only if there is a ring isomorphism $\mathbf{A}_K \cong \mathbf{A}_L$.*

This follows from the previous theorem by using some density results in functional analysis and a theorem on the reconstruction of an isomorphism of groups from an isometry of L^1-group algebras due to Wendel [41]. It seems that the analytic condition of being an isometry for the L^1-norm is necessary (cf. [16], which uses the Bernstein decomposition to show that purely algebraic isomorphisms of Hecke algebras of local fields cannot distinguish local fields).

Let $\mathfrak{G}_K$ denote the absolute Galois group of a number field K that is Galois over $\mathbf{Q}$. Neukirch [26] has proven that $\mathfrak{G}_K$ determines K (Uchida [39] later removed the condition that K is Galois over $\mathbf{Q}$). The set of one-dimensional representations of $\mathfrak{G}_K$, i.e., the abelianisation $\mathfrak{G}_K^{\mathrm{ab}}$, far from determines K (compare [29] or [2]). Several years ago, in connection with the results in [8], Jonathan Rosenberg asked the first author whether, in a suitable sense, two-dimensional irreducible—the "lowest-dimensional non-abelian"— representations of $\mathfrak{G}_K$ determine K. By the philosophy of the global Langlands programme, such representations of $\mathfrak{G}_K$ in $\mathrm{GL}(n, \mathbf{C})$ should give rise to automorphic representations, i.e., to certain modules over the Hecke algebra $\mathscr{H}_{\mathrm{GL}(n)}(K)$. If we consider the analogue of this question in the setting of $\mathscr{H}_{\mathrm{GL}(n)}(K)$-modules instead of n-dimensional Galois representations, our main theorem implies a kind of "automorphic anabelian theorem":

Corollary F. *Suppose that K and L are number fields that are Galois over $\mathbf{Q}$. There is an L^1-algebra isomorphism of Hecke algebras $\mathscr{H}_{\mathrm{GL}(n)}(K) \cong \mathscr{H}_{\mathrm{GL}(n)}(L)$ for some $n \geq 2$ if and only if there is a field isomorphism $K \cong L$.*

We now present some open problems:

(1) Is it possible to characterise *precisely* the linear algebraic groups for which $G(\mathbf{A}_K) \cong G(\mathbf{A}_L)$ implies $\mathbf{A}_K \cong \mathbf{A}_L$? Is Theorem C true without imposing that a maximal torus T of G splits over K and L?

(2) What happens if G is not a linear algebraic group, but any algebraic group? (It follows from Chevalley's structure theorem that such G have a unique maximal linear subgroup H; can we deduce $H(\mathbf{A}_K) \cong H(\mathbf{A}_L)$ from $G(\mathbf{A}_K) \cong G(\mathbf{A}_L)$)? What happens if there is no linear part, i.e., G is an abelian variety, e.g., an elliptic curve? For every number field, is there a sufficiently interesting elliptic curve $E/\mathbf{Q}$ such that $E(\mathbf{A}_K)$ determines all localisations of K?

(3) What happens over global fields of positive characteristic?

(4) The category of $\mathscr{H}_G(K)$-modules does not seem to determine the field K, cf. [16]. Can the category be enriched in some way so as to determine K? Our theorem suggests to try and keep track of some analytic information about $\mathscr{H}_G(K)$ related to the L^1-norm.

The paper has the following structure. In Section 2, we discuss what happens if G is the additive or multiplicative group or a direct product thereof. In Section 3, we introduce and discuss the notion of fertility. In Section 4, we prove that maximal divisibility is equivalent to unipotency in finite-adelic point groups. In Section 5 we use this to prove Theorem C. In Section 6, we discuss Hecke algebras and prove Theorem E.

2. Additive and multiplicative groups of adeles

In this section, we elaborate on Example A from the introduction. We discuss the group structure of the additive and multiplicative groups of adeles of a number field, and we recall the notions of local isomorphism of number fields and its relation to isomorphism of adele rings and to arithmetic equivalence. We introduce *local* additive and multiplicative isomorphisms and prove that their existence implies arithmetic equivalence.

Arithmetic equivalence and local isomorphism.

2.1. Notations/Definitions. If K is a number field with ring of integers $\mathscr{O}_K$, let M_K denote the set of all places of K, $M_{K,f}$ the set of non-archimedean places of K, and $M_{K,\infty}$ the set of archimedean places. If $\mathfrak{p} \in M_{K,f}$ is a prime ideal, then $K_\mathfrak{p}$ denotes the completion of K at $\mathfrak{p}$, and $\mathscr{O}_{K,\mathfrak{p}}$ its ring of integers. Let $e(\mathfrak{p})$ and $f(\mathfrak{p})$ denote the ramification and residue degrees of $\mathfrak{p}$ over the rational prime p below $\mathfrak{p}$, respectively. The *decomposition type* of a rational prime p in a field K is the sequence $(f(\mathfrak{p}))_{\mathfrak{p}|p}$ of residue degrees of the prime ideals of K above p, in increasing order, with multiplicities.

For an archimedean place $\mathfrak{p}$ of K, we have $K_\mathfrak{p} = \mathbf{R}$ or $\mathbf{C}$ and we let $\mathscr{O}_{K,\mathfrak{p}} = K_\mathfrak{p}$.

2.2. DEFINITION. We use the notation $\prod'(G_i, H_i)$ for the restricted product of the groups G_i with respect to the subgroups H_i. We denote by

$$\mathbf{A}_K = \prod_{\mathfrak{p}\in M_K}{}'(K_\mathfrak{p}, \mathscr{O}_{K,\mathfrak{p}})$$

the adele ring of K, and by

$$\mathbf{A}_{K,f} = \prod_{\mathfrak{p}\in M_{K,f}}{}'(K_\mathfrak{p}, \mathscr{O}_{K,\mathfrak{p}})$$

its ring of finite adeles.

Two number fields K and L are *arithmetically equivalent* if for all but finitely many prime numbers p, the decomposition types of p in K and L coincide.
Two number fields K and L are called *locally isomorphic* if there is a bijection $\varphi\colon M_{K,f} \to M_{L,f}$ between their sets of prime ideals such that the corresponding local fields are topologically isomorphic, i.e. $K_\mathfrak{p} \cong L_{\varphi(\mathfrak{p})}$ for all $\mathfrak{p} \in M_{K,f}$.
The *Dedekind zeta function* of a number field K is defined as

$$\zeta_K(s) = \sum_{I\subseteq\mathscr{O}_K} (\#\,\mathscr{O}_K/I)^{-s},$$

where the sum ranges over the nonzero ideals of $\mathscr{O}_K$.

The main properties are summarised in the following proposition (see e.g. [18, III.1 and VI.2]):

2.3. PROPOSITION. *Let K and L be number fields. Then:*

(i) *K and L are locally isomorphic if and only if the adele rings $\mathbf{A}_K$ and $\mathbf{A}_L$ are isomorphic as topological rings, if and only if the rings of finite adeles $\mathbf{A}_{K,f}$ and $\mathbf{A}_{L,f}$ are isomorphic as topological rings.*
(ii) *K and L are arithmetically equivalent if and only if $\zeta_K = \zeta_L$, if and only if there is a bijection $\varphi\colon M_{K,f} \to M_{L,f}$ such that the local fields $K_\mathfrak{p} \cong L_{\varphi(\mathfrak{p})}$ are isomorphic for* all but finitely many $\mathfrak{p} \in M_{K,f}$.
(iii) *We have $K \cong L \Rightarrow \mathbf{A}_K \cong \mathbf{A}_L$ (as topological rings) $\Rightarrow \zeta_K = \zeta_L$ and none of the implications can be reversed in general, but if K or L is Galois over $\mathbf{Q}$, then all implications can be reversed.* $\square$

THE ADDITIVE GROUP OF ADELES.

2.4. PROPOSITION. *If H is a number field, then there are topological isomorphisms of additive groups*

$$(\mathbf{A}_{H,f}, +) \cong (\mathbf{A}_{\mathbf{Q},f}^{[H:\mathbf{Q}]}, +)$$

and

$$(\mathbf{A}_H, +) \cong (\mathbf{A}_{\mathbf{Q}}^{[H:\mathbf{Q}]}, +).$$

Proof. If $\mathfrak{p}$ is a prime of H above the rational prime p, then $\mathscr{O}_{H,\mathfrak{p}}$ is a free $\mathbf{Z}_p$-module of rank $e(\mathfrak{p})f(\mathfrak{p})$ (cf. [5, 5.3-5.4]). By tensoring with $\mathbf{Q}$, summing over all $\mathfrak{p} \mid p$ for fixed p, and using that $n := [H : \mathbf{Q}] = \sum_{\mathfrak{p}|p} e(\mathfrak{p})f(\mathfrak{p})$, we find that

$$\begin{aligned}(\mathbf{A}_{H,f}, +) &= \prod_{p \in M_{\mathbf{Q},f}}{}' \big(\bigoplus_{\mathfrak{p}|p} (H_{\mathfrak{p}}, +), \bigoplus_{\mathfrak{p}|p} (\mathscr{O}_{H,\mathfrak{p}}, +)\big) \\ &\cong \prod_{p \in M_{\mathbf{Q},f}}{}' ((\mathbf{Q}_p^n, +), (\mathbf{Z}_p^n, +)) \cong (\mathbf{A}_{\mathbf{Q},f}^n, +),\end{aligned}$$

and then the second statement follows from $(\mathbf{A}_H, +) = (\mathbf{A}_{H,f}, +) \times (\mathbf{R}^n, +)$. $\square$

2.5. COROLLARY. *The additive groups $(\mathbf{A}_K, +)$ and $(\mathbf{A}_L, +)$ are isomorphic (as topological groups) for two number fields K and L if and only if K and L have have the same degree over $\mathbf{Q}$, if and only if the additive groups $(\mathbf{A}_{K,f}, +)$ and $(\mathbf{A}_{L,f}, +)$ are isomorphic (as topological groups).*

Proof. By Proposition 2.4, we know that $[K : \mathbf{Q}] = [L : \mathbf{Q}]$ implies that $(\mathbf{A}_{K,f}, +) \cong (\mathbf{A}_{L,f}, +)$ and $(\mathbf{A}_K, +) \cong (\mathbf{A}_L, +)$.
Conversely, a topological isomorphism $(\mathbf{A}_K, +) \cong (\mathbf{A}_L, +)$ of additive groups induces a homeomorphism between their respective connected components of the identity, i.e., $\mathbf{R}^{[K:\mathbf{Q}]} \cong \mathbf{R}^{[L:\mathbf{Q}]}$. It follows that $[K : \mathbf{Q}] = [L : \mathbf{Q}]$ ([12, Theorem 2.26]).
Finally, let W be a compact open subgroup of $(\mathbf{A}_{K,f}, +)$. Locally at each place $\mathfrak{p} \mid p$, $W_{\mathfrak{p}}$ is a free $\mathbf{Z}_p$-module of rank $[K_{\mathfrak{p}} : \mathbf{Q}_p]$, so W is topologically isomorphic to $\hat{\mathbf{Z}}^{[K:\mathbf{Q}]}$. Hence, for a prime ℓ, we find that $W/\ell W$ is isomorphic to $(\mathbf{Z}/\ell\mathbf{Z})^{[K:\mathbf{Q}]}$. The image of W under an isomorphism of topological groups $(\mathbf{A}_{K,f}, +) \cong (\mathbf{A}_{L,f}, +)$ has the same property, and we find $[K : \mathbf{Q}] = [L : \mathbf{Q}]$. $\square$

If, additionally, the isomorphism is "local", i.e. induced by local additive isomorphisms, then we have the following result:

2.6. PROPOSITION. *Let K and L be number fields such that there is a bijection $\varphi \colon M_{K,f} \to M_{L,f}$ with, for almost all places $\mathfrak{p}$, isomorphisms of topological groups $\Phi_{\mathfrak{p}} \colon (K_{\mathfrak{p}}, +) \cong (L_{\varphi(\mathfrak{p})}, +)$. Then K and L are arithmetically equivalent.*

Proof. A compact open subgroup W of $K_{\mathfrak{p}}$ is a free $\mathbf{Z}_p$-module of rank $e(\mathfrak{p})f(\mathfrak{p})$. It follows that for any prime number $\ell \neq p$, $W/\ell W \cong \{0\}$, while $W/pW \cong (\mathbf{F}_p^{e(\mathfrak{p})f(\mathfrak{p})}, +)$. Since the same holds for the image of W under $\Phi_{\mathfrak{p}}$, we conclude that for all non-archimedean places $\mathfrak{p} \in M_{K,f}$, we must have $e(\mathfrak{p})f(\mathfrak{p}) = e(\varphi(\mathfrak{p}))f(\varphi(\mathfrak{p}))$. At all but finitely many primes p, both K and L are unramified, so $f(\mathfrak{p}) = f(\varphi(\mathfrak{p}))$ for all but finitely many residue field degrees $f(\mathfrak{p})$. This implies that K and L are arithmetically equivalent. $\square$

THE MULTIPLICATIVE GROUP OF ADELES.

We start by quoting for future reference the following result from [11, Kapitel 15]: let H denote a number field and $\mathfrak{p} \in M_{H,f}$. Let $\pi_{\mathfrak{p}}$ be a local uniformiser at $\mathfrak{p}$ and let $\overline{H}_{\mathfrak{p}} = \mathscr{O}_{H,\mathfrak{p}}/\mathfrak{p}$ denote the residue field; then the unit group of $H_{\mathfrak{p}}$ is

$$\mathscr{O}_{H,\mathfrak{p}}^* \cong \overline{H}_{\mathfrak{p}}^* \times (1 + \pi_{\mathfrak{p}} \mathscr{O}_{H,\mathfrak{p}}) \tag{1}$$

and the one-unit group

$$1 + \pi_{\mathfrak{p}} \mathscr{O}_{H,\mathfrak{p}} \cong \mathbf{Z}_p^{[H_{\mathfrak{p}}:\mathbf{Q}_p]} \times \mu_{p^\infty}(H_{\mathfrak{p}}) \tag{2}$$

where $\mu_{p^\infty}(H_{\mathfrak{p}})$ is the group of p-th power roots of unity in $H_{\mathfrak{p}}$.

2.7. PROPOSITION. *If H is a number field with r_1 real and r_2 complex places, then there is a topological group isomorphism*

$$(\mathbf{A}_H^*, \cdot) \cong (\mathbf{R}^*)^{r_1} \times (\mathbf{C}^*)^{r_2} \times \left(\bigoplus_{\mathbf{Z}} \mathbf{Z} \right) \times \hat{\mathbf{Z}}^{[H:\mathbf{Q}]} \times \prod_{\mathfrak{p} \in M_{H,f}} (\overline{H}_{\mathfrak{p}}^* \times \mu_{p^\infty}(H_{\mathfrak{p}})).$$

Proof. We have

$$\mathbf{A}_H^* \cong (\mathbf{R}^*)^{r_1} \times (\mathbf{C}^*)^{r_2} \times \mathbf{A}_{H,f}^* \text{ and } \mathbf{A}_{H,f}^* \cong J_H \times \prod_{\mathfrak{p} \in M_{H,f}} \mathscr{O}_{H,\mathfrak{p}}^*,$$

where J_H is the topologically discrete group of fractional ideals of H, so $J_H \cong \bigoplus_{\mathbf{Z}} \mathbf{Z}$ with the index running over the set of prime ideals, and the entry of $\mathfrak{n} \in J_H$ corresponding to a prime ideal $\mathfrak{p}$ is given by $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{n})$. The result follows from (1) and (2). $\square$

It remains to determine the exact structure of the p-th power roots of unity, e.g.:

2.8. EXAMPLE. [2, Lemma 3.1 and Lemma 3.2] If $H \neq \mathbf{Q}(i)$ and $H \neq \mathbf{Q}(\sqrt{-2})$, then there is an isomorphism of topological groups

$$\prod_{\mathfrak{p} \in M_{H,f}} (\overline{H}_{\mathfrak{p}}^* \times \mu_{p^\infty}(H_{\mathfrak{p}})) \cong \prod_{n \geq 1} \mathbf{Z}/n\mathbf{Z}.$$

Hence we conclude: *If K and L are two imaginary quadratic number fields different from $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{-2})$, then we have a topological group isomorphism $\mathbf{A}_K^* \cong \mathbf{A}_L^*$.*

Combining Proposition 2.4 and Example 2.8, we obtain the claim made in Example A in the introduction:

2.9. COROLLARY. *For any two imaginary quadratic number fields K and L different from $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{-2})$ and for any integers r and s, there are topological group isomorphisms*

$$(\mathbf{A}_{K,f})^r \times (\mathbf{A}_{K,f}^*)^s \cong (\mathbf{A}_{L,f})^r \times (\mathbf{A}_{L,f}^*)^s.$$

and

$$(\mathbf{A}_K)^r \times (\mathbf{A}_K^*)^s \cong (\mathbf{A}_L)^r \times (\mathbf{A}_L^*)^s. \quad \square$$

On the other hand, we again have a "local" result:

2.10. PROPOSITION. *Let K and L be number fields such that there is a bijection $\varphi\colon M_{K,f} \to M_{L,f}$ with, for almost all places $\mathfrak{p}$, group isomorphisms $\Phi_{\mathfrak{p}}\colon (K_{\mathfrak{p}}^*, \cdot) \xrightarrow{\sim} (L_{\varphi(\mathfrak{p})}^*, \cdot)$. Then K and L are arithmetically equivalent.*

Proof. From $K_{\mathfrak{p}}^* \cong \mathbf{Z} \times \mathscr{O}_{K,\mathfrak{p}}^*$ and the isomorphisms (1) and (2), it follows that if we set $W = K_{\mathfrak{p}}^*/K_{\mathfrak{p},\mathrm{tors}}^*$, then for a prime ℓ we obtain

$$W/\ell W = \begin{cases} (\mathbf{Z}/p\mathbf{Z})^{[K_{\mathfrak{p}}:\mathbf{Q}_p]+1} & \text{if } \ell = p \\ \mathbf{Z}/\ell\mathbf{Z} & \text{if } \ell \neq p \end{cases}. \tag{3}$$

It follows from $K_{\mathfrak{p}}^* \cong L_{\varphi(\mathfrak{p})}^*$ that $\mathfrak{p}$ and $\mathfrak{q}$ lie above the same rational prime p, and $[K_{\mathfrak{p}} : \mathbf{Q}_p] = [L_{\varphi(\mathfrak{p})} : \mathbf{Q}_p]$. For all but finitely many primes, the extensions $K_{\mathfrak{p}}/\mathbf{Q}_p$ and $L_{\varphi(\mathfrak{p})}/\mathbf{Q}_p$ are unramified. Hence, we find that the bijection φ matches the decomposition types of all but finitely many primes. This implies that K and L are arithmetically equivalent. □

3. Set-up from algebraic groups and the notion of fertility

In this section, we set up notations and terminology from the theory of algebraic groups, and we elaborate on the notion of a group being fertile for a pair of number fields.

Algebraic groups.

3.1. Background (General references: [3] and [38]). Let G denote a linear (viz., affine) algebraic group over $\mathbf{Q}$. We denote the multiplicative group over $\mathbf{Q}$ by $\mathbf{G}_m$ and the additive group over $\mathbf{Q}$ by $\mathbf{G}_a$. A *torus* T is a linear algebraic group which is isomorphic, over $\overline{\mathbf{Q}}$, to $\mathbf{G}_m^r$, for some integer r, called the *rank* of T. When T is an algebraic subgroup of G and moreover a maximal torus inside G, then the *rank* of G is r as well. Suppose that a maximal torus *splits* over a field $F/\mathbf{Q}$, meaning that there exists an isomorphism $T \cong \mathbf{G}_m^r$ defined over F. All maximal F-split tori of G are $G(F)$-conjugate and have the same dimension, called the (F-)*rank* of G. A subgroup U of G is *unipotent* if $U(\overline{\mathbf{Q}})$ consists of unipotent elements. Every unipotent subgroup of $G/\mathbf{Q}$ splits over $\mathbf{Q}$, meaning that it has a composition series over $\mathbf{Q}$ in which every successive quotient is isomorphic to $\mathbf{G}_a$. Alternatively, it is isomorphic over $\mathbf{Q}$ to a subgroup of a group of strictly upper triangular matrices. Any connected group G that is not unipotent contains a non-trivial torus. A *Borel subgroup* B of G is a maximal connected solvable subgroup of G. If all successive quotients in the composition series of B over F are isomorphic to $\mathbf{G}_a$ or $\mathbf{G}_m$, then B is conjugate, over F, to a subgroup of an upper triangular matrix group, by the Lie-Kolchin theorem. Moreover, over F, for some split maximal torus T and maximal unipotent group U, we can write $B \cong T \ltimes U$ as a semi-direct product induced by the adjoint representation $\rho \colon T \to \mathrm{Aut}(U)$ (i.e., by the conjugation action of T on U). Furthermore, given U, B is the normaliser of U in G, and $T \cong B/U$.

3.2. Definition. We call a linear algebraic group G over $\mathbf{Q}$ *fertile* for a number field K if there exists a Borel K-subgroup B of G which is split over K, meaning that $B \cong_K T \ltimes U$ for T a K-split maximal torus and U a maximal unipotent group, such that $T \neq \{1\}$ acts non-trivially (by conjugation) on the abelianisation U^{ab} of $U \neq \{0\}$.

Appendix A contains an equivalent definition of fertility.

3.3. EXAMPLES.

(i) Tori and unipotent groups are *not* fertile for any K, and neither are direct product of such groups.

(ii) The general linear group $\mathrm{GL}(n)$ for $n \geq 2$ is fertile for any K. Here, T is the group of diagonal matrices, split over $\mathbf{Q}$, which acts non-trivially on the group of strictly upper triangular matrices. Similarly, the Borel group of (non-strictly) upper triangular matrices is fertile.

(iii) Let $G = \mathrm{Res}^F_{\mathbf{Q}}(\mathbf{G}_m \ltimes \mathbf{G}_a)$ denote the "$ax+b$"-group of a number field F, as an algebraic group over $\mathbf{Q}$. This group is fertile for any number field K that contains F.

ADELIC POINT GROUPS.

3.4. DEFINITION. Let G denote a linear algebraic group over $\mathbf{Q}$ and let K a number field with adele ring $\mathbf{A}_K$. As described in Section 3 of [28] (compare [22]) we may use any of the following equivalent definitions for the *group of adelic points of G over K* (also called the *adelic point group*), denoted $G(\mathbf{A}_K)$:

(1) Since $\mathbf{A}_K$ is a $\mathbf{Q}$-algebra, $G(\mathbf{A}_K)$ is its scheme theoretic set of points.

(2) Let S be a suitable finite set of places of $\mathbf{Q}$, including the archimedean place, and let $\mathscr{G}$ be a smooth separated group scheme of finite type over the S-integers $\mathbf{Z}_S$, whose generic fibre is G. Then

$$G(\mathbf{A}_K) = \varinjlim_{S' \supset S} \prod_{\mathfrak{p} \in S'} G(K_\mathfrak{p}) \times \prod_{\mathfrak{p} \notin S'} \mathscr{G}(\mathscr{O}_\mathfrak{p})$$

where S' runs over subsets of $M_{K,f}$ that contain divisors of primes in S.

(3) Choose a $\mathbf{Q}$-isomorphism $\varphi\colon G \hookrightarrow \mathbb{A}^N$ of G onto a closed subvariety of a suitable affine space $\mathbb{A}^N$. For every $\mathfrak{p} \in M_{K,f}$, we define $G(\mathscr{O}_\mathfrak{p})$ to be the set of points $x \in G(K_\mathfrak{p})$ for which $\varphi(x) \in \mathscr{O}_\mathfrak{p}^N$. Then $G(\mathbf{A}_K)$ is the restricted product

$$G(\mathbf{A}_K) = \prod_{\mathfrak{p} \in M_{K,f}}{}' (G(K_\mathfrak{p}), G(\mathscr{O}_\mathfrak{p}))) \times \prod_{\mathfrak{p} \in M_{K,\infty}} G(K_\mathfrak{p}).$$

The second and third definitions immediately provide $G(\mathbf{A}_K)$ with a topology induced from the $\mathfrak{p}$-adic topologies. Also, the group law on G induces a topological group structure on $G(\mathbf{A}_K)$. The definitions are, up to isomorphism, independent of the choices of $S, \mathscr{G}$ and φ.
We define the *finite-adelic point group* $G(\mathbf{A}_{K,f})$ completely analogously.

In Section 2, we considered the group of adelic points on $\mathbf{G}_a$ and $\mathbf{G}_m$, in the sense of the above definition, cf. Example A from the introduction.

4. DIVISIBILITY AND UNIPOTENCY

In this section, we show (Proposition 4.8) how to characterise maximal unipotent point groups inside finite-adelic point groups in a purely group theoretic fashion, using divisibility. This is used later to deduce an isomorphism of unipotent point groups from an isomorphism of ambient point groups. We first prove a series of results, relating divisibility and unipotency over local and global fields. Throughout, G will be a linear algebraic group over $\mathbf{Q}$, K a number field, and $\mathfrak{p} \in M_{K,f}$ a finite place of K.

4.1. Definition. If $\mathbf{H}$ is a subgroup of a group $\mathbf{G}$, an element $h \in \mathbf{H}$ is called *divisible in* $\mathbf{G}$ if for every integer $n \in \mathbf{Z}_{>0}$, there exists an element $g \in \mathbf{G}$ such that $h = g^n$. The subgroup $\mathbf{H} \leq \mathbf{G}$ is called divisible (in $\mathbf{G}$) if all of its elements are divisible in $\mathbf{G}$.

4.2. Lemma. *All divisible elements of $G(K_\mathfrak{p})$ are unipotent.*

Proof. We fix an embedding $G \hookrightarrow GL_N$ throughout, and consider elements of G as matrices. Let v denote a divisible element of $G(K_\mathfrak{p})$, and, for each $n \in \mathbf{Z}_{>0}$, let $w_n \in G(K_\mathfrak{p})$ satisfy $w_n^n = v$ for $n \in \mathbf{Z}_{>0}$. The splitting field L_n of the characteristic polynomial of w_n (seen as $N \times N$-matrix) has *bounded* degree $[L_n : K] \leq N!$. Since by Krasner's Lemma (e.g., [27, 8.1.6]), there are only finitely many extensions of $K_\mathfrak{p}$ of bounded degree, the compositum L of all L_n is a discretely valued field, in which all the eigenvalues λ_i of v are n-th powers (namely, of eigenvalues of w_n) for all integers n. Since L is non-archimedean,

$$\bigcap_{n \geq 1} L^n = \{1\},$$

by discreteness of the absolute value and the structure of $\mathcal{O}_H^*$ as described in (1) and (2). We conclude that all eigenvalues of v are 1 and v is unipotent. $\square$

4.3. Remark. The lemma is not true for archimedean places. To give an example at a real place, the rotation group $\mathrm{SO}(2, \mathbf{R}) \subseteq \mathrm{SL}(2, \mathbf{R})$ is divisible but contains non-unipotent elements.

4.4. Lemma. *Let U be a maximal unipotent algebraic subgroup of an algebraic group G, both defined over a field F of characteristic zero. Then $U(F)$ is divisible in $G(F)$.*

Proof. Consider the exponential map

$$\exp\colon \mathfrak{u} \to U(F)$$

from the nilpotent Lie algebra $\mathfrak{u}$ of $U(F)$ to $U(F)$, which is bijective since F has characteristic zero (cf. [25, Theorem 6.5]). For an integer $n \in \mathbf{Z}_{>0}$ and an element $\mathfrak{x} \in \mathfrak{u}$ we find (by the Baker-Campbell-Hausdorff formula) that

$$\exp(n\mathfrak{x}) = \exp(\mathfrak{x})^n,$$

since multiples of the same $\mathfrak{x}$ commute. Hence (multiplicative) divisibility in the unipotent algebraic group corresponds to (additive) divisibility in the nilpotent Lie algebra $\mathfrak{u}$. Since the latter is an F-vector space and any integer n is invertible in F, we find the result. $\square$

We will also need the following global version:

4.5. Lemma. *The group $U(\mathbf{A}_{K,f})$ is divisible in $G(\mathbf{A}_{K,f})$.*

Proof. Let $v = (v_\mathfrak{p})_\mathfrak{p} \in U(\mathbf{A}_{K,f})$, let $n \in \mathbf{Z}_{\geq 0}$, and for every $\mathfrak{p} \in M_{K,f}$, let $w_\mathfrak{p} \in U(K_\mathfrak{p})$ be such that $w_\mathfrak{p}^n = v_\mathfrak{p}$ (which exists by the previous lemma applied to $F = K_\mathfrak{p}$). We claim that $w_\mathfrak{p} \in U(\mathscr{O}_\mathfrak{p})$ for all but finitely many $\mathfrak{p}$, which shows that $w = (w_\mathfrak{p})_\mathfrak{p} \in U(\mathbf{A}_{K,f})$ and proves the lemma. Indeed, it suffices to prove that $w_\mathfrak{p} \in GL_N(\mathscr{O}_\mathfrak{p})$ for all but finitely many $\mathfrak{p}$. This follows from the Taylor series

$$w_\mathfrak{p} = \sqrt[n]{1 + (v_\mathfrak{p} - 1)} = \sum_{k=0}^{\infty} \binom{1/n}{k} (v_\mathfrak{p} - 1)^k,$$

which is a finite sum since $v_\mathfrak{p} - 1$ is nilpotent, by noting that for fixed n, the binomial coefficients introduce denominators at only finitely many places. □

4.6. LEMMA. *Any maximal divisible subgroup of $G(K_\mathfrak{p})$ is conjugate to $U(K_\mathfrak{p})$ in $G(K_\mathfrak{p})$.*

Proof. Let $\mathbf{D}$ denote a maximal divisible subgroup of $G(K_\mathfrak{p})$. By Lemma 4.2, it consists of unipotent elements. Since unipotency is defined by polynomial equations in the affine space of $N \times N$ matrices, the Zariski closure of $\mathbf{D}$ in $G_{K_\mathfrak{p}}$ is a unipotent algebraic subgroup U' of $G_{K_\mathfrak{p}}$. Moreover, Lemma 4.4 implies that $U'(K_\mathfrak{p})$ consists of divisible elements, so by maximality of $\mathbf{D}$, we find that U' is a *maximal* unipotent algebraic subgroup of $G_{K_\mathfrak{p}}$. Theorem 8.2 of Borel-Tits [4] implies that there exists an element $\gamma_\mathfrak{p} \in G(K_\mathfrak{p})$ such that $\gamma_\mathfrak{p} U' \gamma_\mathfrak{p}^{-1} = U$, for U any chosen maximal unipotent algebraic subgroup of G. Hence, $\gamma_\mathfrak{p} \mathbf{D} \gamma_\mathfrak{p}^{-1} \subseteq U(K_\mathfrak{p})$. Since $\gamma_\mathfrak{p}^{-1} U(K_\mathfrak{p}) \gamma_\mathfrak{p}$ is maximal divisible, the result follows. □

The proof to the following lemma was suggested to us by Maarten Solleveld.

4.7. LEMMA. *Let $B \subset G$ denote a K-split Borel subgroup of G. Then for all but finitely many $\mathfrak{p} \in M_{K,f}$, we have*

$$G(K_\mathfrak{p}) = B(K_\mathfrak{p}) G(\mathscr{O}_\mathfrak{p}).$$

Proof. Since G/B is projective, the space $(G/B)(\mathbf{A}_{K,f})$ is compact and equals $(G/B)(\mathbf{A}_{K,f}) = G(\mathbf{A}_{K,f})/B(\mathbf{A}_{K,f})$ (both follow from [32, p. 258]). The open compact group $\prod_\mathfrak{p} G(\mathscr{O}_\mathfrak{p})$ (where the product runs over all finite places of K) of $G(\mathbf{A}_{K,f})$ acts on $(G/B)(\mathbf{A}_{K,f})$ by left multiplication. By compactness, the action has only finitely many orbits, i.e.,

$$\left(\prod_\mathfrak{p} G(\mathscr{O}_\mathfrak{p}) \right) \backslash G(\mathbf{A}_{K,f}) / B(\mathbf{A}_{K,f}) = \prod_\mathfrak{p} \left(G(\mathscr{O}_\mathfrak{p}) \backslash G(K_\mathfrak{p}) / B(K_\mathfrak{p}) \right)$$

is finite. In particular, for all but finitely many finite places $\mathfrak{p}$ of K, $G(\mathscr{O}_\mathfrak{p}) \backslash G(K_\mathfrak{p}) / B(K_\mathfrak{p})$ is trivial, so that $G(K_\mathfrak{p}) = B(K_\mathfrak{p}) G(\mathscr{O}_\mathfrak{p})$. □

In Appendix B, we provide an alternative cohomological proof that gives some more information about the set of excluded places. Finally, we prove the main result of this section:

4.8. PROPOSITION. *Suppose that G contains a K-split Borel subgroup. Let U be a maximal unipotent algebraic subgroup of G. Then any maximal divisible subgroup of $G(\mathbf{A}_{K,f})$ is conjugate to $U(\mathbf{A}_{K,f})$ in $G(\mathbf{A}_{K,f})$.*

Proof. Let $\mathbf{D}$ denote a maximal divisible subgroup of $G(\mathbf{A}_{K,f})$ and $\mathbf{D}_\mathfrak{p} = \mathbf{D} \cap G(K_\mathfrak{p})$ its local component for $\mathfrak{p} \in M_{K,f}$. Let $\gamma_\mathfrak{p} \in G(K_\mathfrak{p})$ be as in Lemma 4.6, i.e., such that $\gamma_\mathfrak{p} \mathbf{D}_\mathfrak{p} \gamma_p^{-1} = U(K_\mathfrak{p})$. Let $B = N_G(U)$ be a Borel subgroup containing U; since G is assumed to be fertile, we may choose these such that B is a *split* Borel K-subgroup of G. Lemma 4.7 implies that for all but finitely many $\mathfrak{p}$, we may replace $\gamma_\mathfrak{p}$ by an element in $\mathscr{G}(\mathscr{O}_\mathfrak{p})$, which we again denote by $\gamma_\mathfrak{p}$ for ease of notation. This way, we find $\gamma = \prod\limits_{\mathfrak{p} \in M_{K,f}} \gamma_\mathfrak{p} \in G(\mathbf{A}_{K,f})$ with

$$\mathbf{D} \subseteq \gamma^{-1} \prod U(K_\mathfrak{p}) \gamma \cap G(\mathbf{A}_{K,f}) = \gamma^{-1} U(\mathbf{A}_{K,f}) \gamma \subseteq \mathbf{D},$$

where the last inclusion holds by Lemma 4.5. □

Note that when G is fertile for K, it satisfies the hypotheses of Proposition 4.8.

5. Proof of Theorem C

We now turn to the proof of Theorem C. Let $\mathbf{G} := G(\mathbf{A}_{K,f})$ as a topological group. We will apply a purely group theoretic construction to $\mathbf{G}$, to end up with the adele ring $\mathbf{A}_K$; this shows that the isomorphism type of the adele ring is determined by the topological group $\mathbf{G}$. We first reconstruct some cartesian power of $\mathbf{A}_{K,f}$.

Let $\mathbf{D}$ denote a maximal divisible subgroup of $\mathbf{G}$. Consider the normaliser $\mathbf{N} := N_\mathbf{G}\mathbf{D}$ of $\mathbf{D}$ in $\mathbf{G}$. Let $\mathbf{V} := [\mathbf{N}, \mathbf{D}]/[\mathbf{D}, \mathbf{D}] \leq \mathbf{D}^{\mathrm{ab}}$, and let $\mathbf{T} := \mathbf{N}/\mathbf{D}$. Note that $\mathbf{T}$ acts naturally on $\mathbf{V}$ by conjugation. Since $\mathbf{V}$ is locally compact Hausdorff, we can give $\mathrm{End}\mathbf{V}$, the endomorphisms of the abelian group $\mathbf{V}$, the compact-open topology.

5.1. Proposition. *There exists an integer $\ell \geq 1$ such that there is a topological ring isomorphism*

$$Z(\mathrm{End}_\mathbf{T}\mathbf{V}) \cong \mathbf{A}_{K,f}^\ell,$$

where the left hand side is the centre of the ring of continuous endomorphism of the $\mathbf{T}$-module $\mathbf{V}$.

Proof. First, we relate the subgroups of $\mathbf{G}$ to points groups of algebraic subgroups of G. From Proposition 4.8, we may assume that $\mathbf{D} = U(\mathbf{A}_{K,f})$ for a fixed maximal unipotent algebraic subgroup of G. The normaliser of U in G as an algebraic group is a Borel group B inside the fertile group G (Theorem of Chevalley, e.g. [3, 11.16]); again, we choose U such that B is split over K. Since taking points and taking normalisers commute ([24, Proposition 6.3]), we obtain that

$$\mathbf{N} = N_\mathbf{G}\mathbf{D} = N_{G(\mathbf{A}_{K,f})} U(\mathbf{A}_{K,f}) = (N_G U)(\mathbf{A}_{K,f}) = B(\mathbf{A}_{K,f}).$$

and $\mathbf{T} \cong T(A_{K,f})$ for T any maximal torus in B, which is K-split by assumption.

Next, we analyse the action of $\mathbf{T}$ on $\mathbf{V}$, knowing the action of T on U. The hypothesis that T splits over K implies that $T \cong \mathbf{G}_m^r$ over K for some r. The adjoint action of T by conjugation on U maps commutators to commutators, so it factors through the abelianisation U^{ab}, and we can consider the linear adjoint action $\rho\colon T \to \mathrm{Aut}(U^{\mathrm{ab}})$ over K. Note that $U^{\mathrm{ab}} \cong \mathbf{G}_a^k$ for some integer k, so we have an action over K

$$\rho\colon T(\cong \mathbf{G}_m^r) \to \mathrm{Aut}(\mathbf{G}_a^k) = \mathrm{GL}(k), \tag{4}$$

which is diagonalisable over K as a direct sum $\rho = \oplus \chi_i$ of k characters $\chi_i \in \mathrm{Hom}_K(T, \mathbf{G}_m)$ of algebraic groups. In coordinates $t = (t_1, \dots, t_r) \in \mathbf{G}_m^r = T$, any such character is of the form

$$\chi(t) = \chi(t_1, \dots, t_r) = t_1^{n_1} \cdot \dots \cdot t_r^{n_r} \tag{5}$$

for some $n_1, \dots, n_r \in \mathbf{Z}$. Since the action of $\mathbf{T}$ on $\mathbf{V}$ is given by specialisation from the action of T on a subspace of U^{ab}, we find an isomorphism of $\mathbf{T}$-modules

$$\mathbf{V} \cong \bigoplus_{i=1}^{\ell} \mathbf{A}_{K,f,\chi_i}^{\mu_i},$$

where χ_i $(i = 1, \dots \ell)$ are the distinct non-trivial characters that occur in $\mathbf{V}$, μ_i is the multiplicity of χ_i in $\mathbf{V}$, and $\mathbf{A}_{K,f,\chi_i}$ is the $\mathbf{T}$-module $\mathbf{A}_{K,f}$ where $\mathbf{T}$ acts via χ_i. Hence,

$$\mathrm{End}_{\mathbf{T}}\mathbf{V} = \prod_{i=1}^{\ell}\prod_{j=1}^{\ell} \mathrm{Mat}_{\mu_j \times \mu_i}\left(\mathrm{Hom}_{\mathbf{T}}(\mathbf{A}_{K,f,\chi_i}, \mathbf{A}_{K,f,\chi_j})\right). \tag{6}$$

The assumption of fertility means precisely that $\ell \geq 1$. To conclude that

$$Z\left(\mathrm{End}_{\mathbf{T}}\mathbf{V}\right) = Z\left(\prod_{i=1}^{\ell} \mathrm{Mat}_{\mu_i \times \mu_i}\left(\mathbf{A}_{K,f}\right)\right) = \mathbf{A}_{K,f}^{\ell},$$

as required, we now prove that if χ_i and χ_j are non-trivial characters occurring in this decomposition, then there is a topological ring isomorphism

$$\mathrm{Hom}_{\mathbf{T}}(\mathbf{A}_{K,f,\chi_i}, \mathbf{A}_{K,f,\chi_j}) \cong \begin{cases} \mathbf{A}_{K,f} & \text{if } \chi_i = \chi_j \\ \{0\} & \text{otherwise}. \end{cases}$$

Indeed, a homomorphism of additive groups $f\colon (\mathbf{A}_{K,f,\chi_i}, +) \to (\mathbf{A}_{K,f,\chi_j}, +)$ is $\mathbf{T}$-equivariant precisely if $f(\chi_i(t)(u)) = \chi_j(t)f(u)$ for all $t \in \mathbf{T}$ and $u \in \mathbf{A}_{K,f}$. The χ are specialisations of algebraic characters as in (5), and some powers are non-zero by the assumption of fertility. If $\chi_i \neq \chi_j$, this means that

$$f(t^n u) = t^m f(u), \forall t \in \mathbf{A}_{K,f}^*,\ \forall u \in \mathbf{A}_{K,f} \tag{7}$$

for some $n, m > 0$, $n \neq m$, which is impossible unless $f = 0$: indeed, choose $t \in \mathbf{Z}_{>0}$; then the equation says that $t^n f(u) = t^m f(u)$ for any u, so $m = n$. So we must have $\chi_i = \chi_j$, and we find that

$$f(t^n u) = t^n f(u), \forall t \in \mathbf{A}_{K,f}^*,\ \forall u \in \mathbf{A}_{K,f} \tag{8}$$

for some $n > 0$.

We now reinterpret a formula of Siegel [37, p. 134] as saying the following: *Let R denote a ring and n a positive integer such that $n!$ is invertible in R. Then any element of R belongs to the $\mathbf{Z}$-linear span of the n-th powers in R. In particular, we have the following explicit formula for any $z \in R$:*

$$z = \sum_{k=0}^{n-1} (-1)^{n-k-1} \binom{n-1}{k} \left\{ \left(\frac{z}{n!} + k\right)^n - k^n \right\}.$$

Applied to $R = \mathbf{A}_{K,f}$, in which $n!$ is invertible, Siegel's formula expresses any element of $\mathbf{A}_{K,f}$ as $\mathbf{Z}$-linear combination of n-th powers in $\mathbf{A}_{K,f}$. We conclude from (8) and additivity of f that

$$f(tu) = tf(u), \forall t \in \mathbf{A}^*_{K,f},\ \forall u \in \mathbf{A}_{K,f}. \tag{9}$$

Hence, $f(t) = tf(1)$ is completely determined by specifying a value for $f(1) \in \mathbf{A}_{K,f}$, and

$$\mathrm{End}_{\mathbf{T}}(\mathbf{A}_{K,f,\chi}) \to \mathbf{A}_{K,f} \colon f \mapsto f(1)$$

is the required ring isomorphism. It is continuous, since evaluation maps (such as this one) are continuous in the compact-open topology on $\mathrm{End}_{\mathbf{T}}(\mathbf{A}_{K,f,\chi})$. The inverse map is $\alpha \mapsto (x \mapsto \alpha x)$, which is also continuous in the finite-adelic topology on $\mathbf{A}_{K,f}$. Hence, we find an isomorphism of topological groups, as required. □

5.2. Theorem (Theorem C). *Let K and L be two number fields, and let G denote a linear algebraic group over $\mathbf{Q}$, fertile for K and L. There is a topological group isomorphism of adelic point groups $G(\mathbf{A}_{K,f}) \cong G(\mathbf{A}_{L,f})$ if and only if there is a topological ring isomorphism $\mathbf{A}_K \cong \mathbf{A}_L$.*

Proof. Using Proposition 5.1, from $\mathbf{G} = G(\mathbf{A}_{K,f})$ we group theoretically construct $Z\left(\mathrm{End}_{\mathbf{T}}\mathbf{V}\right) = \mathbf{A}^{\ell}_{K,f}$. Now consider the maximal ideals in $\mathbf{A}^{\ell}_{K,f}$.

For any ring R, let $\mathscr{M}(R)$ denote its set of principal maximal ideals. Observe that $\mathscr{M}(R^{\ell}) = \mathscr{M}(R) \times \mathbf{Z}/\ell\mathbf{Z}$, since a maximal ideal in R^{ℓ} is of the form $R^{\ell_1} \times \mathfrak{m} \times R^{\ell_2}$ for some maximal ideal $\mathfrak{m}$ of R and a decomposition $\ell = \ell_1 + \ell_2 + 1$. We recall the description of the principal maximal ideals in an adele ring $\mathbf{A}_{K,f}$ as given by Iwasawa and Lochter ([21, Satz 8.6] and [14, p. 340–342], cf. [18, VI.2.4]):

$$\mathscr{M}(\mathbf{A}_{K,f}) = \{\mathfrak{m}_{\mathfrak{p}} = \ker\left(\mathbf{A}_{K,f} \to K_{\mathfrak{p}}\right)\}.$$

Note that $\mathbf{A}_{K,f}/\mathfrak{m}_{\mathfrak{p}} \cong K_{\mathfrak{p}}$. Hence the multiset

$$\{\mathbf{A}^{\ell}_{K,f}/\mathfrak{m} \colon \mathfrak{m} \in \mathscr{M}(\mathbf{A}^{\ell}_{K,f})\}$$

contains a copy of the local field $K_{\mathfrak{p}}$ exactly $\ell r_{\mathfrak{p}}$ times, where $r_{\mathfrak{p}}$ is the number of local fields of K isomorphic to $K_{\mathfrak{p}}$. Thus, we have constructed the multiset of local fields

$$\{K_{\mathfrak{p}} \colon \mathfrak{p} \in M_{K,f}\}$$

of K, up to isomorphism of local fields.

If K and L are two number fields with $G(\mathbf{A}_{K,f}) \cong G(\mathbf{A}_{L,f})$ as topological groups, then these multisets are in bijection, i.e., there exists a bijection of places $\varphi \colon M_{K,f} \to M_{L,f}$ such that $K_{\mathfrak{p}} \cong L_{\varphi(\mathfrak{p})}$ for all $\mathfrak{p} \in M_{K,f}$. Hence K and L are locally isomorphic (in the sense of Section 2.1), and we find ring isomorphisms $\mathbf{A}_{K,f} \cong \mathbf{A}_{L,f}$ and $\mathbf{A}_K \cong \mathbf{A}_L$, by Proposition 2.3.

For the reverse implication $\mathbf{A}_K \cong \mathbf{A}_L \Rightarrow G(\mathbf{A}_{K,f}) \cong G(\mathbf{A}_{L,f})$, we use that a topological ring isomorphism $\mathbf{A}_K \cong \mathbf{A}_L$ implies the existence of topological isomorphisms $\Phi_{\mathfrak{p}} \colon K_{\mathfrak{p}} \cong L_{\varphi(\mathfrak{p})}$ of local fields for some bijection of places $\varphi \colon M_{K,f} \to M_{L,f}$ (again by Proposition 2.3). The fact that all $\Phi_{\mathfrak{p}}$ are homeomorphisms implies in particular that $\Phi_{\mathfrak{p}}(\mathscr{O}_{K,\mathfrak{p}}) = \mathscr{O}_{L,\varphi(\mathfrak{p})}$ for all $\mathfrak{p}$. Now $G(\mathbf{A}_{K,f}) \cong G(\mathbf{A}_{L,f})$ is immediate from the definition of finite-adelic point groups (with topology) in 3.4(2) or, equivalently, 3.4(3). This finishes the proof of Theorem C. □

6. HECKE ALGEBRAS AND PROOF OF THEOREM E

6.1. DEFINITION. Let G denote a linear algebraic group over $\mathbf{Q}$. Because $\mathbf{A}_{K,f}$ is locally compact, $G\{K\} := G(\mathbf{A}_{K,f})$ is a locally compact topological group for the topology described in Definition 3.4, equipped with a (left) invariant Haar measure $\mu_{G\{K\}}$. The *finite (or non-archimedean) real Hecke algebra* $\mathscr{H}_G(K) = C_c^\infty(G\{K\}, \mathbf{R})$ of G over K is the algebra of all real-valued locally constant compactly supported continuous functions $\Phi : G\{K\} \to \mathbf{R}$ with the convolution product

$$\Phi_1 * \Phi_2 : g \mapsto \int_{G\{K\}} \Phi_1(gh^{-1})\Phi_2(h) d\mu_{G\{K\}}(h).$$

(Replacing $\mathbf{R}$ by $\mathbf{C}$ yields the finite-adelic complex Hecke algebra; the results in this section also hold in the complex setting.)

Every element of $\mathscr{H}_G(K)$ is a finite linear combination of characteristic functions on double cosets $\mathbf{K}h\mathbf{K}$, for $h \in G\{K\}$ and $\mathbf{K}$ a compact open subgroup of $G\{K\}$. Alternatively, we may write

$$\mathscr{H}_G(K) = \varinjlim_{\mathbf{K}} \mathscr{H}(G\{K\} /\!\!/ \mathbf{K}),$$

where $\mathscr{H}(G\{K\} /\!\!/ \mathbf{K})$ is the Hecke algebra of $\mathbf{K}$-biinvariant smooth functions on $G\{K\}$ (for example, if $\mathbf{K}$ is maximally compact, this is the spherical Hecke algebra).

6.2. DEFINITION. We define the L^1-*norm* on functions on $G\{K\}$ through

$$||f||_1 = \int_{G\{K\}} |f| d\mu_{G\{K\}}.$$

Then let $L^1(G\{K\})$ denote the *group algebra*, i.e., the algebra of real-valued L^1-functions on $G\{K\}$ with respect to the Haar measure $\mu_{G\{K\}}$, under convolution.

6.3. DEFINITION. An isomorphism of Hecke algebras $\Psi : \mathscr{H}_G(K) \xrightarrow{\sim} \mathscr{H}_G(L)$ which is an isometry for the L^1-norms arising from the Haar measures (i.e., which satisfies $||\Psi(f)||_1 = ||f||_1$ for all $f \in \mathscr{H}_G(K)$) is called an L^1-*isomorphism.* We will denote this by

$$\mathscr{H}_G(K) \cong_{L^1} \mathscr{H}_G(L).$$

Before we give its proof, let us recall the statement of Theorem E:

6.4. THEOREM (Theorem E). *Let K and L be two number fields, and let G denote a linear algebraic group over $\mathbf{Q}$, fertile for K and L. There is an L^1-isomorphism of Hecke algebras $\mathscr{H}_G(K) \cong_{L^1} \mathscr{H}_G(L)$ if and only if there is a ring isomorphism $\mathbf{A}_K \cong \mathbf{A}_L$.*

Proof. The proof consists of two steps: first we show, using the Stone-Weierstrass theorem, that the Hecke algebras are dense in the group algebras, and then we use results on reconstructing a locally compact group from its group algebra due to Wendel.

Step 1: $\mathscr{H}_G(K) \cong_{L^1} \mathscr{H}_G(L)$ implies $L^1(G\{K\}) \cong_{L^1} L^1(G\{L\})$. By the locally compact real version of the Stone-Weierstrass theorem [13, 7.37(b)], $\mathscr{H}_G(K)$ is dense in $C_0(G\{K\})$ for the sup-norm, where $C_0(G\{K\})$ denotes the functions that vanish at infinity, i.e., such that $|f(x)| < \varepsilon$ outside a compact subset of $G\{K\}$. Indeed, one needs to check the nowhere vanishing and point separation properties of the algebra. Since $\mathscr{H}_G(K)$ contains the characteristic function of any compact subset $\mathbf{K} \subseteq G\{K\}$, the algebra vanishes nowhere, and the point separating property follows since $G\{K\}$ is Hausdorff. A fortiori, $\mathscr{H}_G(K)$ is dense in the compactly supported functions $C_c(G\{K\})$ for the sup-norm, and hence also in the L^1-norm. Now $C_c(G\{K\})$ is dense in $L^1(G\{K\})$, and the claim follows.

Step 2: $L^1(G\{K\}) \cong_{L^1} L^1(G\{L\})$ implies $G\{K\} \cong G\{L\}$. Indeed, an L^1-isometry $\mathscr{H}_G(K) \cong_{L^1} \mathscr{H}_G(L)$ implies an L^1-isometry of group algebras $L^1(G\{K\}) \cong_{L^1} L^1(G\{L\})$. Hence the result follows from a theorem due to Wendel [41, Theorem 1], which says that an L^1-isometry of group algebras of locally compact topological groups is always induced by an isomorphism of the topological groups.

Step 3: If G is fertile, $G\{K\} \cong G\{L\}$ implies $\mathbf{A}_K \cong \mathbf{A}_L$. This is Theorem C. $\square$

6.5. Corollary. *If G is a connected linear algebraic group over $\mathbf{Q}$ which is fertile for K and L, where K and L are two numbers fields which are Galois over $\mathbf{Q}$, then an L^1-isomorphism of Hecke algebras $\mathscr{H}_G(K) \cong \mathscr{H}_G(L)$ implies that the fields K and L are isomorphic.*

Proof. Since the hypotheses imply that the fields are arithmetically equivalent, the result follows from Proposition 2.3.(iii). $\square$

Since $\mathrm{GL}(n)$ is fertile if $n \geq 2$, we obtain Corollary F.

Variations on Theorem E.

(1) The theorem is also true if the real-valued Hecke algebra is replaced by the complex-valued Hecke algebra (using the complex versions of Stone-Weierstrass and Kawada/Wendel).
(2) It seems that the theorem also holds for the full Hecke algebra $\mathscr{H}_G \otimes \mathscr{H}_G^\infty$, where $\mathscr{H}_G^\infty$ is the archimedean Hecke algebra for G, viz., the convolution algebra of distributions on $G(\mathbf{R} \otimes_{\mathbf{Q}} K)$ supported on a maximal compact subgroup of $G(\mathbf{R} \otimes_{\mathbf{Q}} K)$, but we have not checked the analytic details.

Appendix A. An equivalent definition of fertility

The following was observed by Wilberd van der Kallen:

A.1. Proposition. *G is fertile over K if and only if it contains a K-split maximal torus, and the connected component of the identity G^0 is not a direct product of a torus and a unipotent group.*

Proof. Suppose for the entire proof that G contains a K-split maximal torus.
Since Borel groups are connected, the identity component G^0 contains a Borel group, and since Borel groups are conjugate over $\overline{K}$, the condition of fertility in Definition

3.2 is equivalent to G^0 containing a Borel subgroup with non-trivial action of its torus T on the abelianization U^{ab} of its maximal unipotent subgroup U.
We claim that T acts non-trivially on U^{ab} if and only if T acts non-trivially on U. Hence, G is not fertile if and only if G^0 contains a Borel subgroup in which the torus acts trivially on the unipotent part. If this happens, we conclude from the short exact sequence of algebraic groups

$$1 \to R_u(G) \to G^0 \to S \to 1,$$

where $R_u(G)$ is the unipotent radical of G and S is a reductive group, that S has only trivial roots. The classification of reductive groups in characteristic zero implies that S is a torus, so $R_u(G) = U$, $S = T$, and G^0 is itself a Borel group $T \times U$, which is what we wanted to prove.
Let us now prove the claim. Since we are in characteristic zero and T is reductive, it is linearly reductive. Hence, by [7, Corollary A.8.11], T acts trivially on a connected algebraic group if and only if it acts trivially on its Lie algebra. Thus, it suffices to show that T acts non-trivially on $\mathrm{Lie}(U)$ if and only if it acts non-trivially on $\mathrm{Lie}(U^{\mathrm{ab}})$.
By linear reductivity, $\mathrm{Lie}(U^{\mathrm{ab}})$ is a direct factor of $\mathfrak{u} := \mathrm{Lie}(U)$ as a T-module, so necessity is clear. For the converse, observe that since T acts via the adjoint representation, it preserves the lower central series $\mathfrak{u}_0 := \mathfrak{u}$; $\mathfrak{u}_i := [\mathfrak{u}, \mathfrak{u}_{i-1}]\,(i \geq 1)$ of $\mathfrak{u}$. We will show that if T acts trivially on $\mathfrak{u}/\mathfrak{u}_{j-1}$ for some $j \geq 2$, then it acts trivially on $\mathfrak{u}/\mathfrak{u}_j$. The result will then follow, since $\mathrm{Lie}(U^{\mathrm{ab}}) = \mathfrak{u}/\mathfrak{u}_1$ and $\mathfrak{u}/\mathfrak{u}_k = \mathfrak{u}$ for sufficiently large k, as $\mathfrak{u}$ is nilpotent.
To prove our claim, we use that, by assumption, T acts trivially on the subalgebra $\mathfrak{u}_{j-2}/\mathfrak{u}_{j-1}$ of $\mathfrak{u}/\mathfrak{u}_{j-1}$. The bracket $[\cdot,\cdot]\colon \mathfrak{u} \times \mathfrak{u}_{j-2} \to \mathfrak{u}_{j-1}$ factors through to give a surjective T-equivariant map

$$[\cdot,\cdot]\colon \mathfrak{u}/\mathfrak{u}_{j-1} \otimes \mathfrak{u}_{j-2}/\mathfrak{u}_{j-1} \to \mathfrak{u}_{j-1}/\mathfrak{u}_j.$$

Hence, T acts trivially on $\mathfrak{u}_{j-1}/\mathfrak{u}_j$. By linear reductivity of T, the short exact sequence of T-modules

$$0 \to \mathfrak{u}_{j-1}/\mathfrak{u}_j \to \mathfrak{u}/\mathfrak{u}_j \to \mathfrak{u}/\mathfrak{u}_{j-1} \to 0,$$

splits, and we conclude that T acts trivially on the middle term, too. $\square$

Appendix B. Alternative proof of Lemma 4.7

The following is an alternative proof of Lemma 4.7 using cohomological methods and providing some insight into the set of exceptional places. It was inspired by an answer by Bhargav Bhatt on `mathoverflow.net/a/2231`.
Let $\mathscr{B} \subset \mathscr{G}$ denote any inclusion of smooth finite-type separated group schemes over the ring of S-integers $\mathscr{O}_{K,S}$ for a suitable finite set of primes S, so that the generic fibre of $\mathscr{B}$ is B and that of $\mathscr{G}$ is G. By [1, Theorem 4.C], the fppf sheaf quotient $\mathscr{G}/\mathscr{B}$ is a scheme over $\mathscr{O}_{K,S}$; choose S such that it contains the (finitely many, cf. [10, Troisième partie, 9.6.1]) places where the special fibre of $\mathscr{G}/\mathscr{B}$ is not proper. Since fppf quotients commute with base change, the generic fibre of $\mathscr{G}/\mathscr{B}$ is G/B.

We will show that for $\mathfrak{p} \in M_{K,f}$ not contained in S, we have $G(K_\mathfrak{p}) = B(K_\mathfrak{p})\mathscr{G}(\mathscr{O}_\mathfrak{p})$. It suffices to show that

$$G(K_\mathfrak{p})/B(K_\mathfrak{p}) = \mathscr{G}(\mathscr{O}_\mathfrak{p})/\mathscr{B}(\mathscr{O}_\mathfrak{p}) \tag{10}$$

for all $\mathfrak{p} \notin S$. We will prove this by arguing that both sides of (10) equal $(\mathscr{G}/\mathscr{B})(\mathscr{O}_\mathfrak{p})$. First consider the long exact sequence in fppf-cohomology associated to the exact sequence

$$1 \to \mathscr{B} \to \mathscr{G} \to \mathscr{G}/\mathscr{B} \to 1$$

of smooth group schemes (cf. [33, p. 151-152 and Theorem 6.5.10]), over $M = K_\mathfrak{p}$ or $M = \mathscr{O}_\mathfrak{p}$:

$$1 \to \mathscr{B}(M) \to \mathscr{G}(M) \to (\mathscr{G}/\mathscr{B})(M) \to H^1(M, \mathscr{B}) \to \dots$$

To rewrite the left hand side of (10), we take $M = K_\mathfrak{p}$, so we are dealing with $\mathrm{Gal}(\overline{K}_\mathfrak{p}/K_\mathfrak{p})$-cohomology. The short exact sequence

$$1 \to U \to B \to T \to 1,$$

for U a unipotent group and T a maximal K-split torus, induces a long exact sequence

$$1 \to U(K_\mathfrak{p}) \to B(K_\mathfrak{p}) \to T(K_\mathfrak{p}) \to H^1(K_\mathfrak{p}, U) \to H^1(K_\mathfrak{p}, B) \to H^1(K_\mathfrak{p}, T) \to \dots.$$

Since T is split over K, hence split (and a fortiori quasisplit) over $K_\mathfrak{p}$, and $K_\mathfrak{p}$ is a perfect field, applying [32, Lemma 2.4] yields $H^1(K_\mathfrak{p}, T) = 1$. Moreover, since $K_\mathfrak{p}$ has characteristic zero, $H^1(K_\mathfrak{p}, U) = 1$ by [32, Lemma 2.7]. Thus, we find that

$$H^1(K_\mathfrak{p}, B) = 1.$$

Hence,

$$G(K_\mathfrak{p})/B(K_\mathfrak{p}) = (G/B)(K_\mathfrak{p}).$$

Since G/B is projective and $\mathscr{G}/\mathscr{B}$ is proper, the valuative criterion of properness implies that

$$(G/B)(K_\mathfrak{p}) = (\mathscr{G}/\mathscr{B})(\mathscr{O}_\mathfrak{p}).$$

For the right hand side of (10), we set $M = \mathscr{O}_\mathfrak{p}$ and argue as in Step 3 of [33, Theorem 6.5.12]: $H^1(\mathscr{O}_\mathfrak{p}, \mathscr{B})$ classifies $\mathscr{B}$-torsors over $\mathscr{O}_\mathfrak{p}$; let $\mathscr{T} \to \mathrm{Spec}\,\mathscr{O}_\mathfrak{p}$ denote such a torsor. By Lang's theorem, its special fibre $\mathscr{T}_\mathfrak{p} \to \mathrm{Spec}\,\mathbf{F}_\mathfrak{p}$ over the finite residue field $\mathbf{F}_\mathfrak{p}$ has a rational point. Since $\mathscr{B}$ smooth, so is $\mathscr{T}$, so we can lift the rational point by Hensel's Lemma. Hence, $\mathscr{T}$ is also trivial, so $H^1(\mathscr{O}_\mathfrak{p}, \mathscr{B}) = 1$. We conclude that

$$(\mathscr{G}/\mathscr{B})(\mathscr{O}_\mathfrak{p}) = \mathscr{G}(\mathscr{O}_\mathfrak{p})/\mathscr{B}(\mathscr{O}_\mathfrak{p}).$$

References

[1] Sivaramakrishna Anantharaman, *Schémas en groupes, espaces homogènes et espaces algébriques sur une base de dimension 1*, Sur les groupes algébriques, Bull. Soc. Math. France, Mém. vol. 33, Soc. Math. France, Paris, 1973, pp. 5–79.

[2] Athanasios Angelakis and Peter Stevenhagen, *Imaginary quadratic fields with isomorphic abelian galois groups*, ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium (eds. Everett W. Howe and Kiran S. Kedlaya), The Open Book Series, vol. 1, MSP, Berkeley, 2013, pp. 21–39.

[3] Armand Borel, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991.

[4] Armand Borel and Jacques Tits, *Groupes réductifs*, Inst. Hautes Études Sci. Publ. Math. 27 (1965), pp. 55–150.

[5] John W. S. Cassels, *Local Fields*, London Mathematical Society Student Texts, vol. 3, Cambridge University Press, Cambridge, 1986.

[6] Yu Chen, *Isomorphisms of adjoint Chevalley groups over integral domains*, Trans. Amer. Math. Soc., 348 (1996), pp. 521–541.

[7] Brian Conrad, Ofer Gabber, and Gopal Prasad, *Pseudo-reductive groups*, second ed., New Mathematical Monographs, vol. 26, Cambridge University Press, Cambridge, 2015.

[8] Gunther Cornelissen and Matilde Marcolli, *Quantum statistical mechanics, L-series and anabelian geometry*, arXiv:1009.0736, preprint (2010).

[9] Fritz Gaßmann, *Bemerkungen zur Vorstehenden Arbeit von Hurwitz: Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppen.*, Math. Z. 25 (1926), pp. 661(665)–675.

[10] Alexander Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV*, Inst. Hautes Études Sci. Publ. Math. 32 (1967).

[11] Helmut Hasse, *Zahlentheorie*, Dritte berichtigte Auflage, Akademie-Verlag, Berlin, 1969.

[12] Allen Hatcher, *Algebraic topology*, Cambridge University Press, Cambridge, 2002.

[13] Edwin Hewitt and Karl Stromberg, *Real and abstract analysis*, third ed., Graduate Texts in Mathematics, vol. 25, Springer-Verlag, New York-Heidelberg, 1975.

[14] Kenkichi Iwasawa, *On the rings of valuation vectors*, Ann. of Math. (2) 57 (1953), pp. 331–356.

[15] Irving Kaplansky, *Fields and Rings*, Chicago Lectures in Mathematics, The University of Chicago Press, 1969.

[16] Valentijn Karemaker, *Hecke algebras for* GL_n *over local fields*, Arch. d. Math. 107, nr. 4, pp. 341–353.

[17] Yukiyosi Kawada, *On the group ring of a topological group*, Math. Japonicae 1 (1948), pp. 1–5.

[18] Norbert Klingen, *Arithmetical similarities: Prime decomposition and finite group theory*, Oxford Mathematical Monographs, Oxford University Press, 1998.

[19] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, vol. 44, American Mathematical Society, Providence, RI, 1998.

[20] Keiichi Komatsu, *On adèle rings of arithmetically equivalent fields*, Acta Arith. 43 (1984), no. 2, pp. 93–95.

[21] Manfred Lochter, *Arithmetische Ähnlichkeiten zwischen globalen Körpern positiver Characteristik*, Diplomarbeit Universität Köln (1989).

[22] Oliver Lorscheid and Cecília Salgado, *Schemes as functors on topological rings*, J. Number Theory 159 (2016), pp. 193–201.

[23] William Massey, *Singular homology theory*, Graduate Texts in Mathematics vol. 70, Springer-Verlag, New York-Berlin, 1980.

[24] James S. Milne, *Basic theory of affine group schemes*, 2012, available at www.jmilne.org/math/.

[25] James S. Milne, *Lie Algebras, Algebraic Groups, and Lie Groups*, 2013, available at www.jmilne,org/math/.

[26] Jürgen Neukirch, *Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper*, Invent. Math. 6 (1969), pp. 296–314.

[27] Jürgen Neukirch, Alexander Schmidt and Kay Wingberg, *Cohomology of Number Fields*, Grundl. Math. Wiss. vol. 323, Springer-Verlag, Berlin, 2000.

[28] Joseph Oesterlé, *Nombres de Tamagawa et groupes unipotents en caractéristique p*, Invent. Math. 78 (1984), pp. 13–88.

[29] Midori Onabe, *On the isomorphisms of the Galois groups of the maximal abelian extensions of imaginary quadratic fields*, Natur. Sci. Rep. Ochanomizu Univ. 27 (1976), no. 2, pp. 155–161, available from http://ci.nii.ac.jp.

[30] Robert Perlis, *On the equation $\zeta_K(s) = \zeta_{K'}(s)$*, J. Number Theory 9 (1977), no. 3, pp. 342–360.

[31] Vasilij M. Petechuk, *Automorphisms of matrix groups over commutative rings*, Mat. Sb. (N.S.) 117 (1982), pp. 534– 547.

[32] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press, Inc., Boston, 1994.

[33] Bjorn Poonen, *Rational points on varieties*, 2015, available at http://math.mit.edu/ poonen/.

[34] Joseph J. Rotman, *An introduction to homological algebra*, second ed., Universitext, Springer, New York, 2009.

[35] Jean-Pierre Serre, *Galois Cohomology*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1997.

[36] Otto Schreier and Bartel L. van der Waerden, *Die Automorphismen der projektiven Gruppen*, Abh. Math. Sem. Univ. Hamburg 9 (1928), pp. 303–322.

[37] Carl Ludwig Siegel, *Generalization of Waring's problem to algebraic number fields*, Amer. J. Math. 66 (1944), pp. 122–136.

[38] Tonny A. Springer, *Linear algebraic groups*, second ed., Progress in Mathematics, vol. 9, Birkhäuser Boston, Inc., Boston, 1998.

[39] Kôji Uchida, *Isomorphisms of Galois groups*, J. Math. Soc. Japan 28 (1976), no. 4, pp. 617–620.

[40] Steven Weintraub, *Fundamentals of algebraic topology*, Graduate Texts in Mathematics, vol. 270, Springer, New York, 2014.

[41] James G. Wendel, *On isometric isomorphism of group algebras*, Pacific J. Math. 1 (1951), pp. 305–311.

Gunther Cornelissen
Mathematisch Instituut
Universiteit Utrecht
Postbus 80.010
3508 TA
Utrecht, Nederland
g.cornelissen@uu.nl

Valentijn Karemaker
Department of Mathematics
University of Pennsylvania
David Rittenhouse Labs
209 South 33rd Street
Philadelphia, PA 19104-6395
U.S.A.
vkarem@math.upenn.edu