ARITHMETICITY OF LATTICES IN HIGHER RANK REAL GROUPS

ANDREAS WIESER

Abstract. These are lecture notes used in a talk in an informal reading course in Zurich, fall 2019. The aim of these notes is to deduce arithmeticity of lattices in higher-rank real groups from Margulis' superrigidity result.

Contents

1. Introduction

The aim of these notes is to prove the following theorem due to Margulis [5].

Theorem 1.1. *Let $G = \mathbf{G}(\mathbb{R})$ be the real points of a Zariski-connected semisimple $\mathbb{R}$-group*[1] $\mathbf{G}$*. Suppose that G has no compact factors and that $\mathrm{rank}_{\mathbb{R}}(G) \geq 2$. Then any irreducible lattice in G is arithmetic.*

We will recall the notion of an arithmetic lattice below in Section 2. As a blackbox for these notes, the following version (as proven earlier in the reading course mentioned in the abstrace) of the superrigidity theorem of Margulis will be assumed.

Theorem 1.2 (Superrigidity)**.** *Let $G = \mathbf{G}(\mathbb{R})$ be the real points of a semisimple $\mathbb{R}$-group. Suppose that G has no compact factors and that $\mathrm{rank}_{\mathbb{R}}(G) \geq 2$. Let $\Gamma < G$ be an irreducible lattice.*

Let $\mathbf{H}$ be a simple k-group where k is a local field of characteristic zero[2]*. Suppose that $\varphi : \Gamma \to H = \mathbf{H}(k)$ is a morphism (of abstract groups) so that $\varphi(\Gamma)$ is Zariski dense and unbounded. Then $\varphi : \Gamma \to H$ extends to a continuous morphism $G \to H$.*

[1] By this we mean a real linear algebraic group defined over $\mathbb{R}$.

[2] Any such local field is either $\mathbb{R}$, $\mathbb{Q}$ or a finite extension of $\mathbb{Q}_p$.

These notes are very much influenced by Benoist's lectures notes [1] on the same topic and by the book [10] of Zimmer. We will proceed as follows:

- In Section 2 we recall the definition of arithmetic lattices.
- In Section 3 we will give a slight reformulation of Margulis superrigidity theorem (Theorem 1.2). We recommend skipping Section 3 and returning to it in the course of the proof.
- In Section 4 we construct a faithful representation of $\mathbf{G}$ in which Γ acts by matrices with algebraic entries (in fact, entries in a number field). The representation will be constructed by considering the space of regular functions spanned by the $\mathbf{G}$-orbit of $\mathrm{Tr}(\mathrm{Ad}(g))$. Hence, the crucial input is to show that $\mathrm{Tr}(\mathrm{Ad}(\gamma))$ is algebraic for $\gamma \in \Gamma$. For this, we will use Theorem 1.2.
- In Section 5 we will proof the arithmeticity theorem using restriction of scalars
- In Section A of the appendix, we recall the construction of the restriction of scalars for linear algebraic groups.

2. Arithmetic lattices

Recall that by a theorem of Borel and Harish-Chandra [2] for any $\mathbb{Q}$-group $\mathbf{G} < \mathrm{SL}_N$ with no non-trivial $\mathbb{Q}$-characters the group

$$\mathbf{G}(\mathbb{Z}) = \mathbf{G}(\mathbb{Q}) \cap \mathrm{SL}_N(\mathbb{Z})$$

is a lattice in $\mathbf{G}(\mathbb{R})$. This is the first, basic example of what we will define to be an arithmetic lattice. A more elaborate example is the following:

Example 2.1 (An arithmetic lattice from compact quotient)**.** Consider the quadratic form

$$q(x) = x_1^2 + x_2^2 + x_3^2 - \sqrt{2}x_4^2$$

which is defined over $\mathbb{Q}(\sqrt{2})$. The group SO_q is then clearly only defined over $\mathbb{Q}(\sqrt{2})$ and not over $\mathbb{Q}$. We consider the subgroup $\Gamma = \mathrm{SO}_q(\mathbb{Z}[\sqrt{2}])$ of $\mathrm{SO}_q(\mathbb{R})$.

By restriction of scalars[3] we may however attain a semisimple $\mathbb{Q}$-group $\mathbf{G}$ with

$$\mathbf{G}(\mathbb{R}) \simeq \mathrm{SO}_q(\mathbb{R}) \times \mathrm{SO}_{q^\sigma}(\mathbb{R}).$$

Here, σ is the non-trivial Galois automorphism of $\mathbb{Q}(\sqrt{2})$ and q^σ is the quadratic form obtained by applying σ to the coefficients of q. That is, q^σ is the positive definite form $q(x) = x_1^2 + x_2^2 + x_3^2 + \sqrt{2}x_4^2$. In particular, $\mathrm{SO}_{q^\sigma}(\mathbb{R})$ is compact. Taking the image of the lattice

$$\mathbf{G}(\mathbb{Z}) \simeq \{(g, g^\sigma) : g \in \mathrm{SO}_q(\mathbb{Z}[\sqrt{2}])\}$$

under the projection to $\mathrm{SO}_q(\mathbb{R})$ yields Γ. Since $\mathrm{SO}_{q^\sigma}(\mathbb{R})$ is compact, Γ must be a lattice in $\mathrm{SO}_q(\mathbb{R})$.

Recall that two lattices Γ_1, Γ_2 in a locally compact group G are said to be *commensurable* if $\Gamma_1 \cap \Gamma_2$ has finite index in both Γ_1 and Γ_2.

[3] To make this note more self-contained, we will recall the construction in Appendix REF in the case of linear algebraic groups.

Definition 2.2 (Arithmetic lattices)**.** Let $G = \mathbf{G}(\mathbb{R})$ be the real points of a Zariski-connected semisimple $\mathbb{R}$-group $\mathbf{G}$ with trivial center. A lattice $\Gamma < G$ is said to *arithmetic* if there exists a semisimple $\mathbb{Q}$-group $\mathbf{H}$ and a continuous surjective morphism $\mathbf{H}(\mathbb{R}) \to G$ with compact kernel so that Γ is commensurable to the image of $\mathbf{H}(\mathbb{Z})$.

More generally, if $\mathbf{G}$ has non-trivial center, we say that a lattice $\Gamma < G$ is arithmetic if the image of Γ under the adjoint representation $\mathrm{Ad} : \mathbf{G} \to \mathrm{Ad}(\mathbf{G})$ is arithmetic in $\mathrm{Ad}(\mathbf{G})(\mathbb{R})$.

Remark 2.3 (Non-arithmetic lattices)*.* If $G = \mathbf{G}_{\mathbb{R}}$ has real rank 1, then non-arithmetic lattices might exist.

- For $\mathbf{G} = \mathrm{SL}_2$ there exists many non-arithmetic lattices. For example, Takeuchi [9] classifies all triangle groups which are arithmetic and in particular shows that there are only finitely many arithmetic ones.
- In $\mathbf{G} = \mathrm{SO}(n, 1)$ non-arithmetic lattices were constructed by Gromov and Piatetski-Shapiro [4] by 'interbreeding' two arithmetic lattices.
- In $\mathbf{G} = \mathrm{SU}(2, 1)$ and $\mathbf{G} = \mathrm{SU}(3, 1)$ Mostow [7] constructed non-arithmetic lattices.

3. A minor reformulation of the superrigidity theorem

In the applications of Theorem 1.2 used in the proof of Theorem 1.1 the following minor reformulation is useful.

Corollary 3.1. *Let $\mathbf{G}, G, \Gamma$ be as in Theorem 1.1. Let k be a local field of characteristic zero and let $\mathbf{H}$ be a simple k-group. Let $\phi : \Gamma \to H = \mathbf{H}_k$ be a morphism such that $\phi(\Gamma)$ is Zariski dense.*

- *If k is non-Archimedean, then $\phi(\Gamma)$ is bounded.*
- *If $k = \mathbb{R}$, then ϕ extends to a rational morphism $G \to H$.*

Proof of the non-archimedean case. Assume that k is non-archimedean and suppose that $\phi(\Gamma)$ is unbounded. Then there exists a continuous extension $\phi : G \to H$. But H is totally disconnected and G has only finitely many connected components. Thus, ϕ must have finite image which contradicts the Zariski-density of $\phi(\Gamma)$. □

For the archimedean case we need the following.

Lemma 3.2. *Let $G = \mathbf{G}(\mathbb{R})$ be the real points of an $\mathbb{R}$-group $\mathbf{G}$ and let $K < G$ be a compact subgroup. Then K is Zariski-closed in G.*

Proof. Suppose that $\mathbf{G} < \mathrm{SL}_N$ and let $g \notin K$. By Urysohn's lemma and the Stone-Weierstrass theorem we may find a polynomial p_0 on Mat_N such that $p_0(k) \leq \frac{1}{3}$ and $p_0(kg) \geq \frac{2}{3}$ for all $k \in K$. Define

$$p_1(h) = \int_K p_0(kh)\,\mathrm{d}m_K(k)$$

where m_K is the normalized Haar measure on K. This is a polynomial function as its attained from integration the coefficients of $p_0(k\cdot)$ against k. By construction, $p_1|_K$ is constant and bounded above by $\frac{1}{3}$. Also, $p_1(g) \geq \frac{2}{3}$. Letting $p = p_1 - p_1(\mathrm{id})$ we attain a polynomial vanishing on K that gives a non-zero value to g. □

Proof of Corollary 3.1 for $k = \mathbb{R}$. By Theorem 1.2 we need to show that $\phi(\Gamma)$ is unbounded. Suppose not and let $K = \overline{\phi(\Gamma)} < G$ be the compact group $\phi(\Gamma)$ generates. But by Lemma 3.2 K is Zariski-closed which contradicts the Zariski-density of $\phi(\Gamma)$. □

4. Lattice elements have algebraic entries

Let $\mathbf{G}$ be as in Theorem 1.1 and assume in addition that $\mathbf{G}$ has trivial center[4]. The aim of this section is to show the following:

Proposition 4.1. *There is a number field K (i.e. a finite extension of $\mathbb{Q}$) with a real embedding and a faithful representation $\iota : \mathbf{G} \to \mathrm{GL}_N$ over $\mathbb{R}$ such that $\iota(\Gamma) \subset \mathrm{GL}_N(K)$.*

We will use the superrigidity theorem (Theorem 1.2) in the proof, but remark that this is not strictly speaking necessary – see for instance [6, Section 2.1] and the reference therein. As an input, we will assume the following proposition without proof.

Proposition 4.2. *Any lattice in $G' = \mathbf{G}'(\mathbb{R})$ for an $\mathbb{R}$-group $\mathbf{G}'$ is finitely generated.*

Remark 4.3. Proposition 4.2 in this generality is due to Raghunathan [8]. When G' does not contain any simple factor of rank 1, the proposition follows from Property (T).

Assume that $\mathbf{G} < \mathrm{SL}_N$. By Proposition 4.2 we may choose a finite generating set of Γ. Letting K be the field extension of $\mathbb{Q}$ generated by all entries of lattice elements in this generating set, we obtain a finitely generated field extension $K/\mathbb{Q}$ with $\Gamma \subset \mathrm{SL}_N(K)$. Our aim is now to show that K may be chosen to be finite over $\mathbb{Q}$ by choosing a potentially different linear representation. We will use Theorem 1.2 as well as the following fact to do so.

Lemma 4.4. *Let $K/\mathbb{Q}$ be a finitely generated extension of $\mathbb{Q}$. Then there exists for any $\lambda \in K$ transcendental and for any prime p an embedding*

$$\phi : K \hookrightarrow k$$

into a finite extension $k/\mathbb{Q}_p$ with $|\phi(\lambda)| > 1$.

Proof. Let $\lambda_1, \ldots, \lambda_n$ be a transcendence basis of K with $\lambda_1 = \lambda$. This means that $K' = \mathbb{Q}(\lambda_1, \ldots, \lambda_n)$ is isomorphic to the function field over K in n-variables and that K'/K is algebraic. Since K'/K is also finitely generated, it is a finite extension.

Since $\mathbb{Q}_p$ is uncountable, it has infinite transcendence degree as an extension of $\mathbb{Q}$. Given any choice of algebraically independent $a_1, \ldots, a_n \in \mathbb{Q}_p$. we may thus find an embedding

$$\phi' : K' \to \mathbb{Q}_p$$

by mapping λ_i to a_i for every i. By multiplying a_1 with a large enough power of p we may assume that $|a_1| > 1$. Thus, ϕ' satisfies $|\phi'(\lambda)| > 1$.

Since K/K' is algebraic, any embedding $K' \to \overline{\mathbb{Q}_p}$ for an algebraic closure $\overline{\mathbb{Q}_p}$ may be extended to an embedding $K \to \overline{\mathbb{Q}_p}$. We thus obtain an embedding $\phi : K \to k$ for a finite extension $k/\mathbb{Q}_p$. By compatility of norms we still have $|\phi(\lambda)| > 1$. □

[4]By virtue of the definition of arithmetic lattices in Definition 2.2 this is no restriction.

Lemma 4.5. *For any $\gamma \in \Gamma$ the trace* $\mathrm{Tr}(\mathrm{Ad}(\gamma))$ *is an algebraic number.*

Proof. Let us show that any eigenvalue of γ must be algebraic over $\mathbb{Q}$ which clearly implies the lemma. Let K be the field generated by the coefficients of $\mathrm{Ad}(\gamma)$ (in some basis of $\mathrm{Lie}(G)$) where γ runs over a finite generating set of Γ. Notice that $K/\mathbb{Q}$ is in particular of finite transcendence degree. We may replace K by a finite extension so that the characteristic polynomial of γ is completely split over K.

Let $\lambda \in K$ be an eigenvalue of $\mathrm{Ad}(\gamma)$ and suppose that λ is transcendental. Let k be a finite extension of $\mathbb{Q}_p$ and let $\iota : K \to k$ be as in Lemma 4.4 for λ. We view $K \subset k$.

Let $\mathbf{G}'$ be a k-simple factor of $\mathbf{G}$ such that λ is an eigenvalue of the restriction of $\mathrm{Ad}(\gamma)$ to $\mathrm{Lie}(\mathbf{G}')$. Let us now consider the composition ϕ of the maps

$$\Gamma \hookrightarrow \mathbf{G}_k \to \mathbf{G}'_k$$

where we view Γ as a subgroup of $\mathbf{G}_k$ via $K \subset k$ and where $\mathbf{G}_k \to \mathbf{G}'_k$ is the projection. Note that $\phi(\gamma)$ is by construction an unbounded element and that $\phi(\Gamma)$ is Zariski-dense. This is a contradiction by the superrigidity theorem (Corollary 3.1) and hence λ is algebraic over $\mathbb{Q}$. □

Proof of Proposition 4.1. We construct an injective morphism $\iota : \mathbf{G} \to \mathrm{GL}_N$ such that $\iota(\Gamma) \subset \mathrm{GL}_N(\overline{\mathbb{Q}})$. This is indeed sufficient: as Γ and hence also $\iota(\Gamma)$ are finitely generated (Proposition 4.2), we may let K be the field generated by all matrix entries of a finite generating set of $\iota(\Gamma)$ to obtain $\iota(\Gamma) \subset \mathrm{GL}_N(K)$.

Let us consider the regular function

$$\varphi(g) = \mathrm{Tr}(\mathrm{Ad}(g))$$

on $\mathbf{G}$. We let $\mathbf{G}$ act on regular functions ψ via $g.\psi(h) = \psi(hg)$. Viewing $\mathbf{G} < \mathrm{GL}_n$ for some n if ψ is the restriction of a polynomial of degree d to $\mathbf{G}$ then so is $g.\psi$. Hence, the vector space

$$V = \langle g.\varphi : g \in \mathbf{G} \rangle$$

is finite-dimensional.

Since $\Gamma < \mathbf{G}$ is Zariski-dense, V is spanned by $\gamma.\varphi$ for $\gamma \in \mathbf{G}$ and we may choose a basis of V of elements of the form $\gamma_1.\varphi, \ldots, \gamma_N.\varphi$ for $\gamma_1, \ldots, \gamma_N \in \Gamma$. Write $\varphi_i = \gamma_i.\varphi$ for $i = 1, \ldots, N$.

We now aim at showing that the Γ-action on V represented in the above basis is given by $\mathrm{GL}_N(\overline{\mathbb{Q}})$-matrices. For any $\gamma \in \Gamma$ let us write

$$\gamma.\varphi_i = \sum_{j=1}^{N} a_{i,j}(\gamma)\varphi_j. \tag{4.1}$$

Note that any linear relation between the restriction of $\varphi_1, \ldots \varphi_N$ to Γ extends to $\mathbf{G}$ and hence $\varphi_1|_\Gamma, \ldots, \varphi_N|_\Gamma$ are linearly independent. We may thus find $\eta_1, \ldots, \eta_N \in \Gamma$ such that the matrix $B = (\varphi_i(\eta_j))_{ij}$ is invertible. Evaluating (4.1) at η_k we obtain

$$\gamma.\varphi_i(\eta_k) = \sum_{j=1}^{N} a_{i,j}(\gamma)\varphi_j(\eta_k)$$

By invertability of B we obtain that

$$a_{ij}(\gamma) = \sum_k \gamma.\varphi_i(\eta_k)(B^{-1})_{kj}$$

Now note that $\gamma.\varphi_i(\eta_k) = \varphi_i(\eta_k\gamma) = \mathrm{Tr}(\mathrm{Ad}(\eta_k\gamma\gamma_i) \in \overline{\mathbb{Q}}$. Similarly, $B \in \mathrm{GL}_N(\overline{\mathbb{Q}})$ and so $a_{ij}(\gamma) \in \overline{\mathbb{Q}}$ as claimed.

It remains to show that ι is injective. So suppose that $\iota(g) = \mathrm{id}$ so that for any $x \in \mathbf{G}$

$$\mathrm{Tr}(\mathrm{Ad}(x)\,\mathrm{Ad}(g)) = \mathrm{Tr}(\mathrm{Ad}(xg)) = g.\varphi(x) = \varphi(x) = \mathrm{Tr}(\mathrm{Ad}(x)).$$

Evaluating at $x = g$ for any $n \in \mathbb{N}$ and iterating we obtain that $\mathrm{Tr}(\mathrm{Ad}(g^n)) = \mathrm{Tr}(\mathrm{Ad}(g))$. Also, putting $x = g^{-1}$ we obtain that $\mathrm{Tr}(\mathrm{Ad}(g)) = \mathrm{Tr}(\mathrm{Ad}(\mathrm{id})) = \dim(\mathfrak{g})$. Thus, $\mathrm{Ad}(g)$ needs to be unipotent. This shows that the kernel of ι consists of unipotent elements. But since ι is a homomorphism, the kernel is also a normal subgroup and hence is either finite or semisimple. By the assumption on the center it cannot be finite. Also, no semisimple group can consist of unipotent elements and hence the proposition follows. □

5. Proof of Theorem 1.1

We now turn to proving Theorem 1.1. By Proposition 4.1 we may assume that there is some number field $K \subset \mathbb{R}$ and that $\mathbf{G} < \mathrm{SL}_N$ for some $N \geq 2$ so that $\Gamma \subset \mathrm{SL}_N(K)$. Since $\Gamma < \mathbf{G}$ is Zariski-dense by the Borel density theorem (see for example [3]) we obtain that $\mathbf{G}$ is defined over K. We let $\phi_i : K \to \mathbb{C}$ for $i = 1, \ldots, d$ be the field embeddings of K with $\phi_1 = \mathrm{id}$.

We now perform restriction of scalars and let

$$\varphi : \mathbf{G}(K) \to \mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G})(\mathbb{Q}), \quad p : \mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G})(\mathbb{Q}) \to \mathbf{G}(K)$$

be the natural isomorphisms so that $\varphi \circ p = \mathrm{id}$. See for example Appendix A for a quick and self-contained construction of the restriction of scalars.

Claim. *The $\mathbb{Q}$-group $\mathbf{H} = \overline{\varphi(\Gamma)}$ is semisimple and the restriction of the projection $\mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G}) \to \mathbf{G}$ defined over K is surjective.*

Proof. Over the Galois closure, we may identify $\mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G}) = \prod_i \mathbf{G}^{\phi_i}$ so that $\Gamma \to \mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G})$ is given by $\gamma \mapsto (\phi_i(\gamma))_{i=1,\ldots,d}$. As $\varphi(\Gamma)$ is Zariski-dense and the projection $p_i : \mathbf{H}(\mathbb{Q}) \to \mathbf{G}^{\phi_i}(\phi_i(K))$ contains $\phi_i(\Gamma)$, $\mathbf{H}$ surjects onto each $\mathbf{G}^{\phi_i}$. In particular, it surjects onto each $\overline{\mathbb{Q}}$-simple factor of $\mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G})$. Such a group needs to semisimple. □

Identifying $\mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G}) = \prod_i \mathbf{G}^{\phi_i}$ as in the above proof, recall that the projection onto of $\mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G})$ the first factor $\mathbf{G}^{\phi_1} = \mathbf{G}$ is defined over K (and in particular over $\mathbb{R}$). We denote the restriction to $\mathbf{H}$ by $p : \mathbf{H} \to \mathbf{G}$ as well. We will show that $p : \mathbf{H}(\mathbb{R}) \to \mathbf{G}(\mathbb{R})$ has compact kernel and that the image of $\mathbf{H}(\mathbb{Z})$ is commensurable to Γ.

Lemma 5.1. *There exists a subgroup of $\varphi(\Gamma)$ of finite index that is contained in $\mathbf{H}_{\mathbb{Z}}$.*

Proof. Since Γ is finitely generated, there exist finitely many primes $p_1, \ldots, p_s$ such that

$$\varphi(\Gamma) \subset \mathbf{H}(\mathbb{Z}[p_i^{-1} : 1 \leq i \leq s])$$

We now fix one of these primes $p = p_i$ and consider for any $\mathbb{Q}_p$-simple factor $\mathbf{H}'$ of $\mathbf{H}$ the composition

$$f : \Gamma \to \mathbf{H}'(\mathbb{Q}) \to \mathbf{H}'(\mathbb{Q}_p)$$

By the superrigidity theorem (cf. Corollary 3.1) $f(\Gamma)$ needs to be bounded and hence contained in a compact open subgroup K. The index of $\mathbf{H}(\mathbb{Z}_p)$ in K is finite and hence the preimage Γ' of the identity coset under the map $\Gamma \to K/\mathbf{H}(\mathbb{Z}_p)$ satisfies

$$\varphi(\Gamma') \subset \mathbf{H}(\mathbb{Z}[p_i^{-1} : 1 \leq i \leq s,\ p_i \neq p]).$$

Proceeding like this for all remaining primes yields the lemma. □

Note that the projection $p : \mathbf{H}(\mathbb{R}) \to \mathbf{G}(\mathbb{R})$ is surjective as its image contains Γ. By Lemma 5.1, Γ and the image of $\mathbf{H}_{\mathbb{Z}}$ are commensurable.

It thus remains to show that the kernel of p in $\mathbf{H}(\mathbb{R})$ is compact. So suppose that $\mathbf{F}$ is an $\mathbb{R}$-simple factor of the kernel $\ker(p)$ with the property that $\mathbf{F}(\mathbb{R})$ is non-compact. Let π be the projection onto this factor. Then $\pi(\varphi(\Gamma))$ is Zariski-dense in $\mathbf{F}$ and by superrigidity (cf. Corollary 3.1) we obtain a continuous morphism $\psi : \mathbf{G}(\mathbb{R}) \to \mathbf{F}(\mathbb{R})$ extending $\pi \circ \varphi$. In fact, ψ can be seen to be rational. Now write (up to isomorphism) $\mathbf{H} = \mathbf{G}\mathbf{F}\mathbf{F}'$ where $\mathbf{F}'$ is the product of all other simple factors of $\ker(p)$. Then $\varphi(\Gamma)$ is contained in the Zariski-closed subgroup $\mathrm{graph}(\psi)\mathbf{F}'$. By Zariski-density of $\varphi(\Gamma)$ this is ridiculous and we obtain that $\ker(p)$ has to be compact. This proves Theorem 1.1.

Appendix A. Restriction of scalars

To deduce the arithmeticity theorem (Theorem 1.1) from Proposition 4.1 and the superrigidity theorem (Theorem 1.2) we used restriction of scalars, which we recall here. This is a rather general discussion for which we let K be a number field and $\mathbf{G}$ be any K-linear algebraic group.

A.1. **Construction of the restriction of scalars.** Choose a basis $a_1, \ldots, a_d$ of K as a $\mathbb{Q}$-vector space where $d = [K : \mathbb{Q}]$. The choice of basis for K as a $\mathbb{Q}$-vector space yields an embedding of $\mathbb{Q}$-algebras

$$\iota : K \hookrightarrow \mathrm{Mat}_d(\mathbb{Q}).$$

Indeed, letting $\lambda \in K$ act on K by left-multiplication we obtain a $\mathbb{Q}$-linear map $L_\lambda : K \to K$ which we may represent in the basis $a_1, \ldots, a_d$. One checks that ι is indeed a morphism of $\mathbb{Q}$-algebras. Also, it is injective as $L_\lambda = \mathrm{id}$ implies $L_\lambda(1) = 1$ and hence $\lambda = 1$.

The map ι induces also for any $n \in \mathbb{N}$ an embedding of $\mathbb{Q}$-algebras

$$\iota : \mathrm{Mat}_n(K) \hookrightarrow \mathrm{Mat}_n(\mathrm{Mat}_d(\mathbb{Q}))$$

by applying ι to every entry. Note that as a $\mathbb{Q}$-vector space $\mathrm{Mat}_n(\mathrm{Mat}_d(\mathbb{Q})) \simeq \mathrm{Mat}_{nd}(\mathbb{Q})$ by viewing elements of $\mathrm{Mat}_{nd}(\mathbb{Q})$ as $n \times n$-matrices whose entries are $d \times d$ matrices (block matrices). For any polynomial $p \in K[X_{11}, \ldots, X_{nn}]$ we obtain a polynomial map

$$\tilde{p} : \mathrm{Mat}_n(\mathrm{Mat}_d(\mathbb{Q})) \to \mathrm{Mat}_d(\mathbb{Q})$$

Indeed, if p^ι is the polynomial in $\mathrm{Mat}_d(\mathbb{Q})[X_{11},\ldots,X_{nn}]$ attained by applying ι to the coefficients of p we may evaluate p^ι on $\mathrm{Mat}_n(\mathrm{Mat}_d(\mathbb{Q}))$ to get $\tilde{p}$. By construction, the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Mat}_n(K) & \xrightarrow{\;p\;} & K \\ \downarrow \iota & & \downarrow \iota \\ \mathrm{Mat}_n(\mathrm{Mat}_d(\mathbb{Q})) & \xrightarrow[\tilde{p}]{} & \mathrm{Mat}_d(\mathbb{Q}) \end{array}$$

We denote by $\mathbf{V} \subset \mathrm{Mat}_n(\mathrm{Mat}_d) \simeq \mathrm{Mat}_{nd}$ be the subspace (commutative subalgebra) defined by the image of ι (which is defined over $\mathbb{Q}$). Let I_K be the ideal of K-rational functions vanishing on $\mathbf{G}$. We define $\mathbf{H}$ to be the subvariety of $\mathbf{V}$ defined by the vanishing of $\tilde{p}$ for $p \in I_K$. This is a variety defined over $\mathbb{Q}$ by definition.

We implicitly extend ι to a map

$$\iota : \mathrm{Mat}_n(K \otimes_{\mathbb{Q}} A) \xrightarrow{\sim} \mathbf{V}(A) \subset \mathrm{Mat}_n(\mathrm{Mat}_d(A)).$$

The above commutative diagram shows that $\iota(\mathbf{G}(K \otimes_{\mathbb{Q}} A)) = \mathbf{H}(A)$. Thus, $\mathbf{H}$ is a $\mathbb{Q}$-subgroup of GL_{nd} with

$$\mathbf{H}(A) \simeq \mathbf{G}(K \otimes_{\mathbb{Q}} A)$$

given by ι. In particular, we have an isomorphism $\mathbf{G}(K) \simeq \mathbf{H}(\mathbb{Q})$ given by ι. We shall call $\mathbf{H}$ the *restriction of scalars* of G over the extension $K/\mathbb{Q}$ and denote it by $\mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G})$.

Example A.1. Let $K = \mathbb{Q}(\sqrt{d})$ for $d \in \mathbb{Z} \neq \{0,1\}$ square-free be a quadratic field. Then a $\mathbb{Q}$-basis of K is given by $1, \sqrt{d}$ and for any $a + b\sqrt{d} \in K$ we have

$$(a+b\sqrt{d}) \cdot 1 = a + b\sqrt{d}, \quad (a+b\sqrt{d}) \cdot \sqrt{d} = db + a\sqrt{d}.$$

Thus, the above map $\iota : K \hookrightarrow \mathrm{Mat}_2(\mathbb{Q})$ is given by

$$\iota : a + b\sqrt{d} \in K \mapsto \begin{pmatrix} a & db \\ b & a \end{pmatrix}.$$

Considering now for instance the K-group $\mathbf{G} = \mathrm{SL}_2$ we obtain that $\mathrm{Res}_{K/\mathbb{Q}}(\mathrm{SL}_2)$ consists of matrices of the form

$$\begin{pmatrix} a_1 & db_1 & a_2 & db_2 \\ b_1 & a_1 & b_2 & a_2 \\ a_3 & db_3 & a_4 & db_4 \\ b_3 & a_3 & b_4 & a_4 \end{pmatrix}$$

under the additional equation

$$\begin{pmatrix} a_1 & db_1 \\ b_1 & a_1 \end{pmatrix}\begin{pmatrix} a_4 & db_4 \\ b_4 & a_4 \end{pmatrix} - \begin{pmatrix} a_2 & db_2 \\ b_2 & a_2 \end{pmatrix}\begin{pmatrix} a_3 & db_3 \\ b_3 & a_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

A.2. **The restriction of scalars over the Galois closure.** Let us denote by $\phi_i : K \to \mathbb{C}$ for $i = 1,\ldots,d$ the distinct field embeddings of K. For concreteness, one may write $K = \mathbb{Q}(\xi)$ for some $\xi \in K$ in which case any field embedding is defined by mapping ξ to one of the other roots of the minimal polynomial of ξ. We let L be the Galois closure of K (i.e. the field generated by all roots of the minimal polynomial of some ξ as above). In particular, $\phi_i(K) \subset L$ for any $i = 1,\ldots,d$.

Using the above field embeddings we attain for any $n \in \mathbb{N}$ an embedding

$$\phi : K^n \to (L^n)^d, \quad (x_1, \ldots, x_n) \mapsto \big((\phi_i(x_1), \ldots, \phi_i(x_n))\big)_{i=1,\ldots,d}.$$

If $B \in \mathrm{Mat}_n(K)$ and $x \in K^n$ then $\phi_i(Bx) = \phi_i(B)\phi_i(x)$ where $\phi_i(x)$ is attained by applying ϕ_i componentwise and the same holds for $\phi_i(B)$. Let $\phi(B)$ be the map on $(L^n)^d$ given by applying $\phi_i(B)$ to the i-th vector for every i. Identifying $(L^n)^d$ with L^{nd} by taking first the standard basis of the first copy of L^n, then the standard basis of the second copy and so on, we may view $\phi(B)$ as a block-diagonal matrix whose blocks are $\phi_1(B), \phi_2(B), \ldots, \phi_d(B)$ in this order. The definition of ϕ and $\phi(B)$ gives the following commutative diagram

$$\begin{CD} K^n @>\phi>> (L^n)^d \\ @VBVV @VV\phi(B)V \\ K^n @>>\phi> (L^n)^d \end{CD}$$

On the other hand, the choice of basis of K yields an isomorphism $\psi : K \to \mathbb{Q}^d$ which by construction of ι satisfies for any $B \in \mathrm{Mat}_n(K)$

$$\begin{CD} K^n @>\psi>> (\mathbb{Q}^d)^n \\ @VBVV @VV\iota(B)V \\ K^n @>>\psi> (\mathbb{Q}^d)^n \end{CD}$$

The matrix[5] $T = \phi \circ \psi^{-1}$ with entries in L is invertible as ψ is bijective and ϕ is injective. Putting the above considerations together and tensoring with L we also obtain that the diagram

$$\begin{CD} (L^d)^n @>T>> (L^n)^d \\ @V\iota(B)VV @VV\phi(B)V \\ (L^d)^n @>>T> (L^n)^d \end{CD}$$

commutes. Thus, conjugation by T brings $\iota(B)$ into block-diagonal form. In the following we will identify both $(L^d)^n$ and $(L^n)^d$ with L^{nd} in the fashion explained above.

For any $m \in \mathbb{N}$ let Δ_m be the rational subspace of Mat_{md} consisting of block-diagonal matrices of size $m \times m$. By the above we have a linear injection

$$c_T : v \in \mathbf{V} \mapsto TvT^{-1} \in \Delta_n.$$

Since $\dim(\mathbf{V}) = \dim(\Delta_n) = dn^2$ this is an isomorphism (defined over L).

[5]Explicitly, a quick computation shows that it is a block matrix with $d \times d$-many square blocks $T_{ij} \in \mathrm{Mat}_n(L)$ for $1 \leq i, j \leq d$ where T_{ij} satisfies that only the j-th row is non-zero and is given by $(\phi_i(a_1), \ldots, \phi_i(a_d))$.

Returning to the group $\mathbf{G}$ and its restriction of scalars $\mathbf{H}$ we want to analyse the conjugate of $\mathbf{H}$ by T. Denote by $\mathbf{G}^i < \mathrm{GL}_n$ the group defined by p^{ϕ_i} for $p \in I_K$. Then ϕ yields a map $\phi : \mathbf{G} \to \prod_i \mathbf{G}^i$. Viewing $\prod_i \mathbf{G}^i$ as diagonally embedded in GL_{nd} this is the same map ϕ as above (when restricted from Mat_n to $\mathbf{G}$).

Lemma A.2. *Conjugation by T yields an isomorphism $\mathbf{H} \simeq \prod_i \mathbf{G}^i$ defined over L.*

Proof. Denote by $\hat{p}$ for $p \in I_K$ the polynomial map

$$A = \mathrm{diag}(A_1, \ldots, A_d) \in \Delta_n \mapsto \mathrm{diag}(p^{\phi_1}(A_1), \ldots, p^{\phi_d}(A_d)) \in \Delta_1.$$

We then have the following commutative diagram

$$\begin{array}{ccc} \mathrm{Mat}_n(K) & \xrightarrow{\;p\;} & K \\ \phi \big\downarrow & & \big\downarrow \phi \\ \Delta_n & \xrightarrow[\hat{p}]{} & \Delta_1 \end{array}$$

Combing this with the analogous commutative diagram obtained in Section A.1 we obtain that the diagram

$$\begin{array}{ccc} \Delta_n & \xrightarrow{\;\hat{p}\;} & \Delta_1 \\ c_T^{-1} \big\downarrow & & \big\downarrow c_{T_1}^{-1} \\ V & \xrightarrow[\tilde{p}]{} & \mathrm{Mat}_d \end{array}$$

commutes. Here, T_1 is the map attained at the beginning of this section in the case $n = 1$ and c_{T_1} is conjugation with T_1 defined in analogy to c_T. Since $\prod_i \mathbf{G}^i$ is defined as a subvariety of Δ_n by the vanishing of $\hat{p}$ for $p \in I_K$ and $\mathbf{H}$ is defined as a subvariety of V by the vanishing of $\tilde{p}$ for $p \in I_K$ this proves the lemma. □

Theorem A.3 (Restriction of scalars)**.** *Let $K \subset \mathbb{C}$ be a number field, let $\phi_i : K \to \mathbb{C}$ for $i = 1, \ldots, d$ be the complex embeddings of K and let L/K be the Galois closure of K. We may suppose that $\phi_1 = \mathrm{id}$.*

Let $\mathbf{G}$ be a linear algebraic group defined over K. Then there exists a linear algebraic group $\mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G})$ defined over $\mathbb{Q}$ with the following properties:

(i) For any $\mathbb{Q}$-algebra A we have an isomorphism $\iota : \mathbf{G}(K \otimes A) \to \mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G})(A)$.

(ii) Over L the group $\mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G})$ is isomorphic to the L-group $\prod_i \mathbf{G}^{\phi_i}$. The induced map $\pi_1 : \mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G}) \to \mathbf{G} = \mathbf{G}^{\phi_1}$ is defined over K and satisfies that $\pi_1 \circ \iota : \mathbf{G}_{\mathbb{Q}} \to \mathbf{G}_{\mathbb{Q}}$ is the identity.

(iii) If $\mathbf{G}$ is semisimple, then so is $\mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G})$.

Proof. We have already proven most of the above claims. The observation in (iii) follows from (ii) as $\mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G})(\mathbb{C})$ is isomorphic to some power of $\mathbf{G}(\mathbb{C})$. To verify (ii), it suffices now by Lemma A.2 to show that π_1 is defined over K. To prove the claim, we may show that the composition

$$\pi_1 : \mathbf{V} \xrightarrow{c_T} \Delta_n \to \mathrm{Mat}_d$$

is defined over K where the latter map is the projection onto the first block. It's inverse is however given by ι and which is clearly defined over K and so the theorem follows. □

Remark A.4 (Restriction of scalars and lattices of integer points). Let $\mathcal{O}_K$ be the ring of integers in K and let $a_1, \ldots, a_d$ be a $\mathbb{Z}$-basis[6] of $\mathcal{O}$. Then ι satisfies that $\iota(g)$ has integer entries if and only if $g \in \mathrm{Mat}_n(\mathcal{O})$. Thus, $\mathbf{G}(\mathcal{O})$ is isomorphic to $\mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G})(\mathbb{Z})$ under the isomorphism in Theorem A.3(i). The latter is a lattice in $\mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G})(\mathbb{R})$ if $\mathbf{G}$ is semisimple.

References

1. Y. Benoist, *Réseaux des groupes de Lie*, 2008, Lecture notes.
2. A. Borel and Harish-Chandra, *Arithmetic subgroups of algebraic groups*, Ann. Math. **75** (1962), 485–535.
3. H. Furstenberg, *A note on Borel's density theorem*, Proc. Am. Math. Soc **55** (1976), no. 1, 209–212.
4. M. Gromov and I. Piatetski-Shapiro, *Non-arithmetic groups in Lobachevsky spaces*, Publ. Math. IHÉS **66** (1987), 93–103.
5. G. A. Margulis, *Arithmeticity of the irreducible lattices in the semi-simple groups of rank greater than 1*, Invent. Math. **76** (1984), 93–120, appendix to Russian translation of M. Raghunathan, Discrete subgroups of Lie groups (1977) (in Russian)).
6. G.A. Margulis and A. Mohammadi, *Arithmeticity of hyperbolic* 3*-manifolds containing infinitely many totally geodesic surfaces*, arXiv:1902.07267 (2019).
7. G. D. Mostow, *Discrete subgroups of Lie groups*, Astérisque **S131** (1985), 289–309.
8. M.S. Raghunathan, *Discrete subgroups of Lie groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 68, Springer, 1972.
9. K. Takeuchi, *Arithmetic triangle groups*, J. Math. Soc. Japan **29** (1977), no. 1, 91–106.
10. R.J. Zimmer, *Ergodic theory and semisimple groups*, second ed., Monographs in Mathematics, vol. 81, Birkhäuser Basel, 1984.

[6] More generally, one can take any order $\mathcal{O}$ and a $\mathbb{Z}$-basis of a proper-$\mathcal{O}$-ideal.