ACTA ARITHMETICA
169.1 (2015)

Modular embeddings and rigidity for Fuchsian groups

by

Robert A. Kucharczyk (Bonn)

1. Introduction. In 1968 George Mostow published his famous Rigidity Theorem [20]: if M_1 and M_2 are two closed oriented hyperbolic manifolds of dimension $n \geq 3$ and $f\colon \pi_1(M_1) \to \pi_1(M_2)$ is a group isomorphism, then there exists a unique isometry $M_1 \to M_2$ inducing f. This can be reformulated as a statement about lattices in the orientation-preserving isometry group $\mathrm{PSO}(1,n)$ of hyperbolic n-space $\mathbf{H}^n$:

Theorem (Mostow). *Let $n \geq 3$ and let $\mathit{\Gamma}_1, \mathit{\Gamma}_2 \subset \mathrm{PSO}(1,n)$ be cocompact lattices. Let $f\colon \mathit{\Gamma}_1 \to \mathit{\Gamma}_2$ be an isomorphism of abstract groups. Then f is the conjugation by some element of the full isometry group $\mathrm{PO}(1,n)$ of $\mathbf{H}^n$, in particular f extends to an algebraic automorphism of $\mathrm{PSO}(1,n)$.*

This was later generalised by various authors; in particular, the condition that $\mathit{\Gamma}_j$ be cocompact can be weakened to having finite covolume (see [24]). The condition that $n \neq 2$, however, is necessary: two-dimensional hyperbolic manifolds are the same as hyperbolic Riemann surfaces, which are well-known to admit deformations.

As a model for the hyperbolic plane take the upper half-plane $\mathfrak{H} = \{\tau \in \mathbb{C} \mid \operatorname{Im}\tau > 0\}$, so its orientation-preserving isometry group becomes identified with $\mathrm{PSL}(2,\mathbb{R})$ via Möbius transformations. In this article we prove that a variant of Mostow's Rigidity Theorem does hold in $\mathrm{Isom}^+(\mathfrak{H}) = \mathrm{PSL}(2,\mathbb{R})$ if we restrict ourselves to a certain class of lattices for which congruence subgroups are defined, and demand that the group isomorphism preserve congruence subgroups.

We first state our result in the simpler case of arithmetic groups. Recall that given a totally real number field $k \subset \mathbb{R}$, a quaternion algebra B over k which is split over the identity embedding $k \to \mathbb{R}$ and ramified over all

2010 *Mathematics Subject Classification*: Primary 20H10, 11F06, 20D60; Secondary 22E40, 14G35.

Key words and phrases: Fuchsian groups, rigidity, modular embeddings, congruence subgroups, arithmetic groups, semiarithmetic groups, thin groups.

DOI: 10.4064/aa169-1-5

other infinite places of k, an order $\mathscr{O} \subset B$ and an isomorphism $\varphi\colon B \otimes_k \mathbb{R} \to \mathrm{M}(2,\mathbb{R})$, we obtain a group homomorphism $\varphi\colon \mathscr{O}^1 \to \mathrm{PSL}(2,\mathbb{R})$ whose image is a lattice, where $\mathscr{O}^1$ is the group of units in $\mathscr{O}$ with reduced norm one. A lattice $\Gamma \subset \mathrm{PSL}(2,\mathbb{R})$ is called *arithmetic* if Γ is commensurable to some such $\varphi(\mathscr{O}^1)$.

For a non-zero ideal $\mathfrak{n} \subset \mathfrak{o}_k$ we then define the *principal congruence subgroup*

$$\mathscr{O}^1(\mathfrak{n}) = \{b \in \mathscr{O}^1 \mid b - 1 \in \mathfrak{n} \cdot \mathscr{O}\}.$$

If Γ contains a subgroup of finite index in $\varphi(\mathscr{O}^1)$, we set $\Gamma(\mathfrak{n}) = \Gamma \cap \varphi(\mathscr{O}^1(\mathfrak{n}))$, and a subgroup of Γ is a *congruence subgroup* if it contains some $\Gamma(\mathfrak{n})$.

Theorem (Special case of Theorem A below). *Let $\Gamma_1, \Gamma_2 \subset \mathrm{PSL}(2,\mathbb{R})$ be arithmetic Fuchsian groups, and let $f\colon \Gamma_1 \to \Gamma_2$ be an isomorphism of abstract groups such that for every subgroup $\Delta \subseteq \Gamma_1$ of finite index, Δ is a congruence subgroup of Γ_1 if and only if $f(\Delta)$ is a congruence subgroup of Γ_2. Then there exists some $a \in \mathrm{PGL}(2,\mathbb{R})$ such that f is the conjugation by a. In particular, $\Gamma_2 = a\Gamma_1 a^{-1}$.*

Without the assumption about congruence subgroups the conclusion no longer holds (see Remark 10.1).

Now both the notion of congruence subgroup and our result can be extended to a larger class of Fuchsian groups. For a subgroup $\Gamma \subseteq \mathrm{PSL}(2,\mathbb{R})$ denote its preimage in $\mathrm{SL}(2,\mathbb{R})$ by $\tilde{\Gamma}$. A lattice $\Gamma \subset \mathrm{PSL}(2,\mathbb{R})$ is called *semiarithmetic* if $\mathrm{tr}^2\,\gamma$ is a totally real algebraic integer for each $\gamma \in \tilde{\Gamma}$; this notion is invariant under commensurability. It was introduced in [25], and many classes of Fuchsian groups are semiarithmetic:

(i) Arithmetic lattices are semiarithmetic.

(ii) All Fuchsian triangle groups $\Delta(p,q,r)$ are semiarithmetic. However, they fall into infinitely many commensurability classes, only finitely many of which are arithmetic (see [31]).

(iii) In [25] further examples of semiarithmetic groups which are not arithmetic were constructed by giving explicit generators.

(iv) The theory of flat surfaces provides another construction of semiarithmetic groups. If X is a closed Riemann surface and ω is a holomorphic one-form on X which is not identically zero, a simple geometric construction yields the Veech group ([1]) $\mathrm{SL}(X,\omega)$ which is a discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$. In certain cases the Veech group is a lattice, and then its image in $\mathrm{PSL}(2,\mathbb{R})$ is a semiarithmetic group by [17, Theorems 5.1, 5.2] and [19, Proposition 2.6]. Veech groups are never cocompact (see [10, p. 509]), therefore a Veech

[1] The name first appeared in [9] but these groups were studied before from different points of view (see [33]).

group which is a lattice is arithmetic if and only if it is commensurable to $\mathrm{SL}(2,\mathbb{Z})$ ([2]). In [17] we find, for every real quadratic number field k, a construction of a lattice Veech group contained in $\mathrm{SL}(2,\mathfrak{o}_k)$, which is therefore semiarithmetic but not arithmetic.

Examples (ii) and (iv) intersect: in [2, Theorem 6.12] it is proved that every non-cocompact triangle group $\Delta(p,q,\infty)$ is commensurable to some Veech group. On the other hand, cocompact triangle groups can never be Veech groups, and only finitely many of the examples in [17] are commensurable with triangle groups.

The generalisation of the notion of congruence subgroups to semiarithmetic groups is a bit involved; we refer the reader to Section 4.

Now, the conclusion of Theorem A does not hold for general semiarithmetic groups; we need to impose one more condition, which is the existence of a *modular embedding*: Let $\Gamma \subset \mathrm{PSL}(2,\mathbb{R})$ be a semiarithmetic subgroup, and let k be the number field generated by all $\mathrm{tr}^2\gamma$ with $\gamma \in \tilde{\Gamma}$. Then for every embedding $\sigma\colon k \to \mathbb{R}$ there exists a group embedding $i_\sigma\colon \Gamma \to \mathrm{PSL}(2,\mathbb{R})$, unique up to conjugation in $\mathrm{PGL}(2,\mathbb{R})$, such that $\mathrm{tr}^2 i_\sigma(\gamma) = \sigma(\mathrm{tr}^2\gamma)$ for every $\gamma \in \Gamma$ (see [25, Remark 4]). The original group Γ is arithmetic precisely if no $i_\sigma(\Gamma)$ for σ different from the identity embedding contains a hyperbolic element. In general, let $\sigma_1,\dots,\sigma_r$ be those embeddings σ for which $i_\sigma(\Gamma)$ contains a hyperbolic element. Then the coordinate-wise embedding $(i_{\sigma_1},\dots,i_{\sigma_r})\colon \Gamma \to \mathrm{PSL}(2,\mathbb{R})^r$ maps Γ into an irreducible arithmetic group $\Lambda \subset \mathrm{PSL}(2,\mathbb{R})^r$; for the precise construction see Section 7.

We note that if Γ is not already arithmetic itself, it is mapped into Λ with Zariski-dense image of infinite index; such groups are called *thin*. This is essentially due to S. Geninska [8, Proposition 2.1 and Corollary 2.2]; we explain it below in Corollary 7.2.

Now Λ acts on $\mathfrak{H}^r$ by coordinate-wise Möbius transformations, and a *modular embedding* for Γ is then a holomorphic map $F\colon \mathfrak{H} \to \mathfrak{H}^r$ equivariant for $\Gamma \to \Lambda$.

(i) If Γ is arithmetic, then $r = 1$ and Λ contains Γ as a finite index subgroup. We may take $F(\tau) = \tau$ as a modular embedding.

(ii) All Fuchsian triangle groups admit modular embeddings (see [5, Theorem, p. 96]).

(iii) Most of the new examples of semiarithmetic groups in [25] do not admit modular embeddings (see [25, Corollary 4]).

(iv) Veech groups which are lattices always admit modular embeddings (see [19, Corollary 2.11]). This solves [25, Problem 1], which asks

[2] For a complete characterisation of (X,ω) whose Veech group is arithmetic see [9, Theorem 4].

> whether every Fuchsian group admitting a modular embedding is arithmetic or commensurable with a triangle group: there exist Veech groups which are neither [3], but do admit modular embeddings.

More generally, we say Γ *virtually admits a modular embedding* if some finite index subgroup of Γ admits one.

Theorem A. *For $j = 1, 2$, let $\Gamma_j \subset \mathrm{PSL}(2,\mathbb{R})$ be semiarithmetic lattices which virtually admit modular embeddings. Let $f\colon \Gamma_1 \to \Gamma_2$ be an isomorphism of abstract groups such that for every subgroup $\Delta \subseteq \Gamma_1$ of finite index, Δ is a congruence subgroup of Γ_1 if and only if $f(\Delta)$ is a congruence subgroup of Γ_2. Then there exists $a \in \mathrm{PGL}(2,\mathbb{R})$ such that f is conjugation by a. In particular, $\Gamma_2 = a\Gamma_1 a^{-1}$.*

This theorem will be proved in Section 8. It rests on the following result on congruence subgroups in semiarithmetic groups, which may be of independent interest.

Theorem B. *Let $\Gamma \subset \mathrm{PSL}(2,\mathbb{R})$ be a semiarithmetic lattice satisfying the trace field condition [4] with trace field k. Then there exists a finite set $S(\Gamma)$ of rational primes with the following properties:*

(i) *If $\mathfrak{p}$ is a prime ideal in k not dividing any element of $S(\Gamma)$, then $\Gamma/\Gamma(\mathfrak{p}) \simeq \mathrm{PSL}(2, \mathfrak{o}_k/\mathfrak{p})$.*

(ii) *If q is a rational prime power not divisible by any element of $S(\Gamma)$ and Δ is a normal congruence subgroup of Γ with $\Gamma/\Delta \simeq \mathrm{PSL}(2,q)$, then there exists a unique prime ideal $\mathfrak{p}$ of k of norm q with $\Delta = \Gamma(\mathfrak{p})$.*

Here, (i) is a combination of Proposition 4.5 and Lemma 5.1; (ii) is Proposition 8.1.

In particular, the information which groups $\mathrm{PSL}(2,q)$ appear how often as congruence quotients determines the splitting behaviour of all but finitely many primes in k (see Remark 8.2). On the other hand, allowing non-congruence quotients we get many more finite groups. The collection of all these finite groups will determine the abstract isomorphism type of a Fuchsian lattice, but of course no more (see [4, Theorem 1.1]).

Outline. In Sections 2 and 3 we fix the notation and recall standard results on the group PSL(2), both over the reals and over finite fields. In

[3] Almost all of McMullen's genus two examples in [17] do the job: only finitely many real quadratic fields appear as invariant trace fields of triangle groups, so if k is not among them, then any lattice Veech group with trace field k cannot be commensurable to a triangle group, and it cannot be arithmetic either since it is not cocompact.

[4] This is a technical condition which is always satisfied after passing to a finite index subgroup (see Definition 4.1).

Sections 4 and 5 we introduce semiarithmetic subgroups of $\mathrm{PSL}(2,\mathbb{R})$ and study their congruence subgroups. The object of Section 6 is the deduction of a statement about $\mathrm{PSL}(2)$ from an analogous result for $\mathrm{SL}(2)$ by Culler and Shalen [6, Proposition 1.5.2]: a finitely generated subgroup of $\mathrm{PSL}(2,\mathbb{R})$ is determined up to conjugacy by its squared traces. This allows us to work with numbers instead of matrices in the remainder of the article. In Section 7 we formally define modular embeddings and discuss some consequences of their existence. Then in Section 8 the previous observations are used to prove Theorem A and the hard part of Theorem B. Section 9 presents an example with two arithmetic groups, sharpening the statement of Theorem A considerably in this special case. Finally Section 10 discusses some possible and impossible generalisations.

2. Traces on $\mathrm{PSL}(2)$ and Möbius transformations.

For every ring A we set $\mathrm{PGL}(2,A) = \mathrm{GL}(2,A)/A^\times$ where $A^\times$ is embedded by means of scalar matrices. We also set $\mathrm{PSL}(2,A) = \mathrm{SL}(2,A)/\{\pm\mathbf{1}\}$. There is an obvious homomorphism $\mathrm{PSL}(2,A) \to \mathrm{PGL}(2,A)$, but in general it is neither injective nor surjective.

Let k be a field. The determinant homomorphism $\mathrm{GL}(2,k) \to k^\times$ descends to a homomorphism $\mathrm{PGL}(2,k) \to k^\times/(k^\times)^2$, and we obtain a short exact sequence

$$1 \to \mathrm{PSL}(2,k) \to \mathrm{PGL}(2,k) \to k^\times/(k^\times)^2 \to 1. \tag{1}$$

In particular, $\mathrm{PSL}(2,\mathbb{C})$ and $\mathrm{PGL}(2,\mathbb{C})$ are naturally isomorphic whereas for $k=\mathbb{R}$ or a finite field of odd characteristic, $\mathrm{PSL}(2,k)$ becomes identified with an index two normal subgroup of $\mathrm{PGL}(2,k)$.

Note that since $\mathrm{PSL}(2,k)$ is a normal subgroup of $\mathrm{PGL}(2,k)$, the latter operates faithfully on the former by conjugation. Since $\mathrm{tr}(-g) = -\mathrm{tr}\, g$, the squared trace map $\mathrm{tr}^2\colon \mathrm{SL}(2,k) \to k$ descends to a map

$$\mathrm{tr}^2\colon \mathrm{PSL}(2,k) \to k, \qquad \{g,-g\} \mapsto (\mathrm{tr}\, g)^2.$$

For $k=\mathbb{R}$ we also define

$$|\mathrm{tr}|\colon \mathrm{PSL}(2,\mathbb{R}) \to \mathbb{R}, \qquad \{g,-g\} \mapsto |\mathrm{tr}\, g|.$$

Let $\mathfrak{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}\,\tau > 0\}$ be the upper half-plane. The group $\mathrm{SL}(2,\mathbb{R})$ operates on $\mathfrak{H}$ in the well-known way by Möbius transformations, descending to a faithful action by $\mathrm{PSL}(2,\mathbb{R})$. This in fact identifies $\mathrm{PSL}(2,\mathbb{R})$ with both the group of holomorphic automorphisms and that of orientation-preserving isometries (for the Poincaré metric) of $\mathfrak{H}$. Elements of $\mathrm{PSL}(2,\mathbb{R})$ can be classified by their behaviour on $\mathfrak{H}$ (see [11, Section 1.3]):

Proposition 2.1. *Let $\pm\mathbf{1} \neq g \in \mathrm{PSL}(2,\mathbb{R})$. Then g belongs to exactly one of the following classes:*

(i) *g is* elliptic: *it has a unique fixed point in $\mathfrak{H}$, and* $\operatorname{tr}^2 g < 4$.

(ii) *g is* parabolic: *it has a unique fixed point in $\mathbb{P}^1(\mathbb{R})$, but not in $\mathfrak{H}$. Its squared trace satisfies* $\operatorname{tr}^2 g = 4$.

(iii) *g is* hyperbolic: *it has two distinct fixed points in $\mathbb{P}^1(\mathbb{R})$, one of them repelling and one of them attracting, but no fixed points in $\mathfrak{H}$. Its squared trace satisfies* $\operatorname{tr}^2 g > 4$.

3. The finite groups $\mathrm{PSL}(2,q)$**.** Next we study PSL(2) over finite fields. With $\mathbb{F}_q$ being the field of q elements we also write $\mathrm{PSL}(2,q)$ instead of $\mathrm{PSL}(2,\mathbb{F}_q)$.

Proposition 3.1. *If $q > 3$ is an odd prime power, then* $\mathrm{PSL}(2,q)$ *is a simple group of order $\frac{1}{2}q(q^2-1)$. Furthermore* $\mathrm{PSL}(2,q) \simeq \mathrm{PSL}(2,q')$ *if and only if $q = q'$.*

Proof. The simplicity of $\mathrm{PSL}(2,q)$ is a well-known fact, see e.g. [34, Section 3.3.2]. The order of $\mathrm{PSL}(2,q)$ is easily calculated using (1), for instance. The function $q \mapsto \frac{1}{2}q(q^2-1)$ is strictly increasing on $\mathbb{N}$, therefore if $\mathrm{PSL}(2,q)$ and $\mathrm{PSL}(2,q')$ have the same orders, then $q = q'$. ∎

As remarked in Section 2, $\mathrm{PGL}(2,q)$ operates by conjugation on $\mathrm{PSL}(2,q)$. Furthermore the Frobenius automorphism $\varphi\colon \mathbb{F}_q \to \mathbb{F}_q$ defined by $\varphi(x) = x^p$, where p is the prime of which q is a power, defines an automorphism φ of $\mathrm{PSL}(2,q)$. The following is also well-known (see e.g. [34, Theorem 3.2(ii)]):

Proposition 3.2. *The automorphism group of* $\mathrm{PSL}(2,q)$ *is generated by* $\mathrm{PGL}(2,q)$ *and φ.*

In particular if $q = p$ is a prime, then every automorphism of $\mathrm{PSL}(2,p)$ is the restriction of an inner automorphism of $\mathrm{PGL}(2,p)$, and the map $\operatorname{tr}^2\colon \mathrm{PSL}(2,p) \to \mathbb{F}_p$ is invariant under all automorphisms. So the following definition works:

Definition 3.3. Let G be a finite group which is abstractly isomorphic to some $\mathrm{PSL}(2,p)$ for an odd prime p. Then the map $\operatorname{tr}^2_G\colon G \to \mathbb{F}_p$ is defined as follows: choose some isomorphism $\alpha\colon G \to \mathrm{PSL}(2,p)$, then set $\operatorname{tr}^2_G = \operatorname{tr}^2 \circ \alpha$.

If p is replaced by a prime power q, the corresponding map on G is only well-defined up to automorphisms of $\mathbb{F}_q$, i.e. we may define a map $\operatorname{tr}^2_G\colon G \to \mathbb{F}_q/\operatorname{Aut}\mathbb{F}_q$.

Lemma 3.4. *Let $n \in \mathbb{N}$ and let $q_1,\ldots,q_n,q'$ be odd prime powers. Let*

$$\beta\colon G = \mathrm{PSL}(2,q_1) \times \cdots \times \mathrm{PSL}(2,q_n) \to \mathrm{PSL}(2,q')$$

be a group epimorphism. Then there is a $1 \le j \le n$ such that $q' = q_j$ and for some automorphism α of $\mathrm{PSL}(2,q')$ *we can write $\beta = \alpha \circ \mathrm{pr}_j$, where pr_j is the projection on the jth factor.*

Proof. By the Jordan–Hölder Theorem, the only simple quotients of G are the $\mathrm{PSL}(2, q_j)$, so $q' = q_j$ for some j.

We now proceed by induction on n. For $n = 1$ the lemma is trivial, so assume the lemma has been proved for n. Let $\beta\colon G \to \mathrm{PSL}(2, q')$ be an epimorphism where G has $n + 1$ factors. For cardinality reasons it cannot be injective, so there exists some $g \in G \setminus \{1\}$ with $\beta(g) = 1$. Write $g = (g_1, \ldots, g_{n+1})$. Then $g_j \neq 1$ for some j; for simplicity of notation assume that $j = n + 1$. Since $\mathrm{PSL}(2, q_{n+1})$ has trivial centre, there exists some $h_{n+1} \in G$ which does not commute with g_{n+1}. Then set

$$h = (1, \ldots, 1, h_{n+1}) \in G$$

and compute

$$1 = \beta(h)\beta(h^{-1}) = \beta(ghg^{-1}h^{-1}) = \beta(1, \ldots, 1, g_{n+1}h_{n+1}g_{n+1}^{-1}h_{n+1}^{-1})$$

using $\beta(g) = 1$. That is, β restricted to the $(n + 1)$st factor has non-trivial kernel. Since that factor is simple, the restriction of β to the $(n+1)$st factor has to be trivial, so β factors through the projection onto the first n factors, hence (by induction hypothesis) onto one of them. ■

4. Semiarithmetic groups and their congruence subgroups. Let $\Gamma \subset \mathrm{PSL}(2, \mathbb{R})$ be a lattice and let $\tilde{\Gamma}$ be its preimage in $\mathrm{SL}(2, \mathbb{R})$. By $\Gamma^{(2)}$ we denote the subgroup of Γ generated by all γ^2 with $\gamma \in \Gamma$. Since Γ is finitely generated, $\Gamma^{(2)}$ is then a normal subgroup of finite index in Γ.

DEFINITION 4.1. The *trace field* of Γ is the field $\mathbb{Q}(\operatorname{tr} \Gamma) \subset \mathbb{R}$ generated by all $\operatorname{tr} \gamma$ with $\gamma \in \tilde{\Gamma}$. The *invariant trace field* of Γ is the trace field of $\Gamma^{(2)}$.

A lattice Γ satisfies the *trace field condition* if its trace field and its invariant trace field agree.

Clearly the trace field contains the invariant trace field, but the two are not always equal. As the name suggests, the invariant trace field is the more useful invariant: commensurable lattices have the same invariant trace field, see [14, Theorem 3.3.4], but not necessarily the same trace field. Hence, if Γ is any lattice, then $\Gamma^{(2)}$ satisfies the trace field condition. Therefore any lattice has a finite index normal sublattice which satisfies the trace field condition.

DEFINITION 4.2. A lattice $\Gamma \subset \mathrm{PSL}(2, \mathbb{R})$ is called *semiarithmetic* if its invariant trace field is a totally real number field and every trace $\operatorname{tr} \gamma$ for $\gamma \in \tilde{\Gamma}$ is an algebraic integer ([5]).

Being semiarithmetic is stable under commensurability, therefore every semiarithmetic lattice contains a semiarithmetic lattice satisfying the trace

[5] It follows from [14, Lemma 3.5.6] that this is equivalent to the definition given in the introduction.

field condition. For the following constructions let Γ be a semiarithmetic lattice satisfying the trace field condition, and let $k = \mathbb{Q}(\operatorname{tr}\gamma)$. Then the k-vector subspace $B = k[\Gamma]$ of $\mathrm{M}(2,\mathbb{R})$ generated by $\tilde{\Gamma}$ is in fact a k-subalgebra, more precisely a quaternion algebra over k. The $\mathfrak{o}_k$-subalgebra $\mathfrak{o}_k[\tilde{\Gamma}]$ of B generated by $\tilde{\Gamma}$ is an order in B, though not necessarily a maximal one. We choose a maximal order $\mathscr{O} \supseteq \mathfrak{o}_k[\tilde{\Gamma}]$.

If $\mathscr{O}^1$ denotes the subgroup of $\mathscr{O}^\times$ consisting of elements with reduced norm one, $\tilde{\Gamma}$ becomes a subgroup of $\mathscr{O}^1$. Also write $\mathrm{P}\mathscr{O}^1 = \mathscr{O}^1/\{\pm\mathbf{1}\}$ so that Γ is a subgroup of $\mathrm{P}\mathscr{O}^1$.

Proposition 4.3. *Let $\Gamma \subset \mathrm{PSL}(2,\mathbb{R})$ be a semiarithmetic lattice satisfying the trace field condition. Then the following are equivalent:*

(i) *Γ is arithmetic.*
(ii) *Let $k = \mathbb{Q}(\operatorname{tr}\Gamma) \subset \mathbb{R}$. Then for every embedding $\sigma\colon k \to \mathbb{R}$ other than the identity inclusion and every $\gamma \in \tilde{\Gamma}$ one has $|\sigma(\operatorname{tr}\gamma)| \leq 2$.*
(iii) *For every embedding $\sigma\colon k \to \mathbb{R}$ other than the identity inclusion, $B \otimes_{k,\sigma} \mathbb{R}$ is isomorphic to Hamilton's quaternions $\mathbb{H}$.*
(iv) *$\mathrm{P}\mathscr{O}^1$ is a discrete subgroup of $\mathrm{PSL}(2,\mathbb{R})$.*
(v) *The index $(\mathrm{P}\mathscr{O}^1 : \Gamma)$ is finite.*

Proof. The equivalence (i)⇔(ii) is the main result in [30]; the other equivalences follow from the explicit classification of arithmetic lattices in $\mathrm{PSL}(2,\mathbb{R})$ (see e.g. [11, Chapter 5] or [14, Chapter 8]). ∎

Now we discuss congruence subgroups. For an elementary definition, let $\Gamma \subset \mathrm{PSL}(2,\mathbb{R})$ be a semiarithmetic lattice satisfying the trace field condition, and let k and $\mathscr{O}$ be as above. Then every non-zero ideal $\mathfrak{a}$ of $\mathfrak{o}_k$ defines a subgroup

$$\tilde{\Gamma}(\mathfrak{a}) = \{\gamma \in \tilde{\Gamma} \mid \gamma - \mathbf{1} \in \mathfrak{a}\cdot\mathscr{O}\}$$

and its image $\Gamma(\mathfrak{a})$ in Γ, called the *principal congruence subgroup* of level $\mathfrak{a}$. A *congruence subgroup* of Γ is then a subgroup containing some principal congruence subgroup. Similarly we define principal congruence subgroups $\mathscr{O}^1(\mathfrak{a})$ and congruence subgroups of $\mathscr{O}^1$.

These groups can also be defined more abstractly using algebraic groups: there is a canonical linear algebraic group H over k with $H(k) = B^1$; we may define it functorially by setting $H(A) = (B \otimes_k A)^1$ for every k-algebra A. Then H is a twisted form of $\mathrm{SL}(2)_k$. By Weil restriction of scalars we obtain an algebraic group $G = \operatorname{Res}_{k/\mathbb{Q}} H$ with a canonical identification $G(\mathbb{Q}) = H(k) = B^1$. Then G is a twisted form of $\mathrm{SL}(2)_{\mathbb{Q}}^d$ where $d = [k : \mathbb{Q}]$; in particular $G(\mathbb{C})$ is isomorphic to $\mathrm{SL}(2,\mathbb{C})^d$.

Choosing a faithful representation $G \to \mathrm{GL}(n)$, we can define a congruence subgroup in $G(\mathbb{Q})$ to be one that contains the preimage of a congruence subgroup of $\mathrm{GL}(n,\mathbb{Z})$ as a finite index subgroup. This notion of congruence subgroup is independent of the representation $G \to \mathrm{GL}(n)$ (see [18, Proposition 4.1]); that it is equivalent to the more elementary one given before follows by taking the representation of $G \to \mathrm{GL}(4d)$ by left multiplication on B, the latter considered as a $4d$-dimensional $\mathbb{Q}$-vector space with the lattice $\mathscr{O}$.

Let $\mathbb{A}^f$ be the ring of finite adeles of $\mathbb{Q}$, and endow $G(\mathbb{A}^f)$ with the adelic topology. Similarly let $\mathbb{A}_k^f$ be the ring of finite adeles of k; then there is a canonical isomorphism $\mathbb{A}^f \otimes_{\mathbb{Q}} k = \mathbb{A}_k^f$ inducing $G(\mathbb{A}^f) = H(\mathbb{A}_k^f)$. The closure of $\mathscr{O}^1$ in $G(\mathbb{A}^f)$ can be identified with the completion of $\mathscr{O}^1$ with respect to all congruence subgroups; equivalently, with the group of elements of reduced norm one in the profinite completion of $\mathscr{O}$. Therefore we denote it by $\widehat{\mathscr{O}}^1$. It is a maximal compact open subgroup of $G(\mathbb{A}^f)$.

There is a canonical bijection between open subgroups of $\widehat{\mathscr{O}}^1$ and congruence subgroups of $\mathscr{O}^1$: with a congruence subgroup of $\mathscr{O}^1$ we associate its closure in $G(\mathbb{A}^f)$, and with an open subgroup of $\widehat{\mathscr{O}}^1$ we associate its intersection with $\mathscr{O}^1$. For the proof see again [18, Proposition 4.1].

PROPOSITION 4.4 (Strong approximation for semiarithmetic groups). *The closure of $\tilde{\Gamma}$ in $G(\mathbb{A}^f) = H(\mathbb{A}_k^f)$ is open.*

Proof. First we claim that $\tilde{\Gamma}$ is Zariski-dense in G. It suffices to show that $\tilde{\Gamma}$ is Zariski-dense in $G(\mathbb{C}) \simeq \mathrm{SL}(2,\mathbb{C})^d$, and the proof of an analogous but more complicated statement over the reals [8, Proposition 2.1 and Corollary 2.2] carries over mutatis mutandis.

Then we use a special case of a result of M. Nori [21, Theorem 5.4] (see also [16]): if G is an algebraic group over $\mathbb{Q}$ such that $G(\mathbb{C})$ is connected and simply connected (which is the case for our G since $\pi_1(\mathrm{SL}(2,\mathbb{C})) = \pi_1(\mathrm{SU}(2)) = \pi_1(S^3) = 1$), and Γ is a finitely generated Zariski-dense subgroup of $G(\mathbb{Q})$ contained in some arithmetic subgroup of G, then the closure of Γ in $G(\mathbb{A}^f)$ is open. ■

PROPOSITION 4.5. *There exists a non-zero ideal $\mathfrak{m}$ of $\mathfrak{o}_k$, depending on Γ, such that for every ideal $\mathfrak{a}$ of $\mathfrak{o}_k$ prime to $\mathfrak{m}$ the homomorphism $\tilde{\Gamma} \hookrightarrow \mathscr{O}^1 \twoheadrightarrow \mathscr{O}^1/\mathscr{O}^1(\mathfrak{a})$ is surjective, i.e. the canonical homomorphism*

$$\Gamma/\Gamma(\mathfrak{a}) \to \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{a})$$

is an isomorphism of finite groups.

The proof uses several results that will be used later on, so we mention them separately.

THEOREM 4.6 (Strong approximation for quaternion algebras). $G(\mathbb{Q}) = H(k)$ *is dense in* $G(\mathbb{A}^f) = H(\mathbb{A}_k^f)$ (6).

(6) Usually this result is phrased differently: if $\mathbb{A} = \mathbb{A}^f \times \mathbb{R}$ denotes the full adele ring, then $G(\mathbb{Q}) \cdot G(\mathbb{R})$ is dense in $G(\mathbb{A})$. But the latter is canonically isomorphic to $G(\mathbb{A}^f) \times G(\mathbb{R})$, which shows the equivalence to our formulation.

For the proof see e.g. [23, Theorem 7.12].

We shall now investigate the quotient groups $\mathcal{O}^1/\mathcal{O}^1(\mathfrak{a})$. These are best understood locally: if $\mathfrak{p}$ is a finite prime of k, we set $\mathcal{O}_{\mathfrak{p}} = \mathcal{O} \otimes_{\mathfrak{o}_k} \mathfrak{o}_{\mathfrak{p}}$. We can then consider the group $\mathcal{O}_{\mathfrak{p}}^1$ of its elements of norm one, and its congruence subgroups $\mathcal{O}_{\mathfrak{p}}^1(\hat{\mathfrak{p}}^r)$. Recall that $\mathcal{O}_{\mathfrak{p}}$ is a maximal order in $B_{\mathfrak{p}}$.

Proposition 4.7. *Let $\mathfrak{a}$ be an ideal of k with prime factorisation $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$. Then the canonical homomorphism*

$$\mathcal{O}^1/\mathcal{O}^1(\mathfrak{a}) \to \prod_{j=1}^{n} \mathcal{O}_{\mathfrak{p}_j}^1/\mathcal{O}_{\mathfrak{p}_j}^1(\hat{\mathfrak{p}}_j^{r_j}) \tag{2}$$

is an isomorphism of groups.

Proof. Injectivity is easy, so we only show surjectivity. We use the description of $H(\mathbb{A}_k^f)$ as the restricted direct product of the completions $B_{\mathfrak{l}}^1 = (B \otimes_k k_{\mathfrak{l}})^1$, restricted with respect to the compact subgroups $\mathcal{O}_{\mathfrak{l}}^1$. For $j = 1, \ldots, n$ take an element $x_j \in \mathcal{O}_{\mathfrak{p}_j}^1$. The Strong Approximation Theorem furnishes us with an element $\beta \in H(k) = B^1$ with the following properties:

- For $j = 1, \ldots, n$, β considered as an element of $B_{\mathfrak{p}_j}^1$ is congruent to x_j modulo $\mathcal{O}_{\mathfrak{p}_j}^1(\hat{\mathfrak{p}}_j^{r_j})$ (note that the latter is an open subgroup of $B_{\mathfrak{p}_j}^1$).
- For each finite prime $\mathfrak{l}$ different from all $\mathfrak{p}_j$'s, β is in $\mathcal{O}_{\mathfrak{l}}^1$.

Then $\beta \in \mathcal{O}^1$, and its class on the left hand side of (2) maps to $(x_1, \ldots, x_n)$. ■

Note that our proof also shows that the map

$$\mathcal{O}^1/\mathcal{O}^1(\mathfrak{a}) \to \prod_{j=1}^{n} \mathcal{O}^1/\mathcal{O}^1(\mathfrak{p}_j^{r_j})$$

is an isomorphism.

Corollary 4.8. *The canonical homomorphism*

$$\mathrm{P}\mathcal{O}^1/\mathrm{P}\mathcal{O}^1(\mathfrak{a}) \to \prod_{j=1}^{n} \mathrm{P}\mathcal{O}^1/\mathrm{P}\mathcal{O}^1(\mathfrak{p}_j^{r_j})$$

is an epimorphism whose kernel is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^d$ for some $d < n$.

Proof. The homomorphism

$$\mathcal{O}^1/\mathcal{O}^1(\mathfrak{p}_j^{r_j}) \to \mathrm{P}\mathcal{O}^1/\mathrm{P}\mathcal{O}^1(\mathfrak{p}_j^{r_j})$$

is always surjective, and it is injective precisely when $\mathfrak{p}_j^{r_j}$ divides (2), otherwise it has kernel isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Similarly the kernel of $\mathcal{O}^1/\mathcal{O}^1(\mathfrak{a}) \to \mathrm{P}\mathcal{O}^1/\mathrm{P}\mathcal{O}^1(\mathfrak{a})$ is either trivial or $\mathbb{Z}/2\mathbb{Z}$. So the corollary follows from the remark preceding it. ■

Corollary 4.9. *Let $\varDelta \subseteq \mathscr{O}^1$ be a congruence subgroup containing $\mathscr{O}^1(\mathfrak{m})$ for some ideal $\mathfrak{m}$ of k. Let $\mathfrak{a}$ be an ideal of k which is coprime to $\mathfrak{m}$. Then the composition*

$$\varDelta \hookrightarrow \mathscr{O}^1 \twoheadrightarrow \mathscr{O}^1/\mathscr{O}^1(\mathfrak{a})$$

is surjective.

Proof. This is equivalent to the statement $\mathscr{O}^1(\mathfrak{m}) \cdot \mathscr{O}^1(\mathfrak{a}) = \mathscr{O}^1$, and this in turn follows from the isomorphism of finite groups

$$\mathscr{O}^1/(\mathscr{O}^1(\mathfrak{m}) \cap \mathscr{O}^1(\mathfrak{a})) \to \mathscr{O}^1/\mathscr{O}^1(\mathfrak{m}) \times \mathscr{O}^1/\mathscr{O}^1(\mathfrak{a}). \ ■$$

Proof of Proposition 4.5. By Proposition 4.4 there exists some ideal $\mathfrak{m}$ of k with $\mathscr{O}^1(\mathfrak{m}) \subseteq \overline{\tilde{\varGamma}}$, where the latter denotes the closure of $\tilde{\varGamma}$ in $\widehat{\mathscr{O}}^1 \subset G(\mathbb{A}^f)$. This does the job by Corollary 4.9. ■

Corollary 4.10. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be coprime ideals of k which are both prime to* 2*. Then the canonical homomorphism*

$$\mathrm{P}\mathscr{O}^1(\mathfrak{a})/\mathrm{P}\mathscr{O}^1(\mathfrak{ab}) \to \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{b})$$

is an isomorphism. ■

5. Congruence quotients of semiarithmetic groups. Our next step is to determine the quotients on the right hand side of (2). This is done by distinguishing between the ramified and the unramified case. To simplify notation, let K be a p-adic field with ring of integers $\mathfrak{o}_K$ and prime ideal $\mathfrak{p} = (\pi)$. Let $q = p^f$ be the cardinality of the residue class field $\kappa = \mathfrak{o}_K/\mathfrak{p}$. Let B be an unramified quaternion algebra over K, and let $\mathscr{O} \subset B$ be a maximal order. We may assume that $B = \mathrm{M}(2, K)$ and $\mathscr{O} = \mathrm{M}(2, \mathfrak{o}_K)$; then $\mathscr{O}^1 = \mathrm{SL}(2, \mathfrak{o}_K)$, and $\mathscr{O}^1(\mathfrak{p})$ is the kernel of the reduction map $\mathrm{SL}(2, \mathfrak{o}_K) \to \mathrm{SL}(2, \kappa)$.

Lemma 5.1. *Let $r \geq 1$. The reduction map $\mathrm{SL}(2, \mathfrak{o}_K) \to \mathrm{SL}(2, \mathfrak{o}_K/\mathfrak{p}^r)$ is surjective and thus induces an isomorphism $\mathscr{O}^1/\mathscr{O}^1(\mathfrak{p}^r) \to \mathrm{SL}(2, \mathfrak{o}_K/\mathfrak{p}^r)$. In particular $\mathscr{O}^1/\mathscr{O}^1(\mathfrak{p})$ is isomorphic to $\mathrm{SL}(2, q)$.*

Proof. Let

$$\overline{\gamma} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \in \mathrm{SL}(2, \mathfrak{o}_K/\mathfrak{p}^r)$$

and lift $\overline{\gamma}$ arbitrarily to a matrix

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathfrak{o}_K).$$

The determinant $\delta = \det\gamma$ is an element of $1+\mathfrak{p}^r$, hence so is its inverse $1/\delta$. Therefore

$$\gamma' = \begin{pmatrix} a/\delta & b/\delta \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathfrak{o}_K)$$

still reduces to $\overline{\gamma}$. ∎

Lemma 5.2. *Let $r \geq 1$. Under the assumptions as before, the quotient $\mathscr{O}^1(\mathfrak{p}^r)/\mathscr{O}^1(\mathfrak{p}^{r+1})$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{3f}$.*

Proof. We consider the map

$$(\mathscr{O}/\mathfrak{p}\mathscr{O})_0 \to \mathrm{SL}(2, \mathfrak{o}_K/\mathfrak{p}^{r+1}), \qquad [A] \mapsto [1 + \pi^r A].$$

Here the left hand side denotes the subgroup of those elements of $\mathscr{O}/\mathfrak{p}\mathscr{O} = \mathrm{M}(2, \kappa)$ that have trace $\equiv 0 \bmod \mathfrak{p}$. Note $\det(1+\pi^r A) \equiv 1+\pi^r \operatorname{tr} A \bmod \mathfrak{p}^{r+1}$, so the map is indeed well-defined. It is an injective group homomorphism, and its image is precisely the image of $\mathscr{O}^1(\mathfrak{p}^r)$ in $\mathrm{SL}(2, \mathfrak{o}_K/\mathfrak{p}^{r+1})$, which is isomorphic to $\mathscr{O}^1(\mathfrak{p}^r)/\mathscr{O}^1(\mathfrak{p}^{r+1})$. ∎

Now we turn to the ramified case. We use the explicit description of B and $\mathscr{O}$ given in [14, Section 6.4]. Let L/K be the unique unramified quadratic extension. Then B is up to isomorphism given by

$$B = \left\{ \begin{pmatrix} a & b \\ \pi b' & a' \end{pmatrix} \,\middle|\, a, b \in L \right\},$$

where $a \mapsto a'$ is the non-trivial element of $\mathrm{Gal}(L/K)$. This contains a unique maximal order

$$\mathscr{O} = \left\{ \begin{pmatrix} a & b \\ \pi b' & a' \end{pmatrix} \,\middle|\, a, b \in \mathfrak{o}_L \right\},$$

and $\mathscr{O}$ has a unique maximal two-sided ideal

$$\mathscr{M} = \begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix} \mathscr{O} = \left\{ \begin{pmatrix} \pi a & b \\ \pi b' & \pi a' \end{pmatrix} \,\middle|\, a, b \in \mathfrak{o}_L \right\}.$$

It satisfies $\mathscr{M}^2 = \mathfrak{p}\mathscr{O}$. We now define congruence subgroups $\mathscr{O}^1(\mathscr{M}^r) = \mathscr{O}^1 \cap (1 + \mathscr{M}^r)$, so that $\mathscr{O}^1(\mathfrak{p}^r) = \mathscr{O}^1(\mathscr{M}^{2r})$.

Lemma 5.3. *The quotient $\mathscr{O}^1/\mathscr{O}^1(\mathscr{M})$ is a cyclic group of order $q + 1$.*

Proof. Since L/K is unramified, the quotient $\lambda = \mathfrak{o}_L/\pi\mathfrak{o}_L$ is a finite field of order q^2. We consider the map

$$\mathscr{O}^1/\mathscr{O}^1(\mathscr{M}) \to \lambda^\times, \qquad \left[\begin{pmatrix} a & b \\ \pi b' & a' \end{pmatrix} \right] \mapsto a \bmod \pi.$$

This is easily seen to be an injective group homomorphism whose image is the kernel of the norm map $N_{\lambda/\kappa}$. That norm map is surjective to $\kappa^\times$, so its kernel has order $(q^2-1)/(q-1) = q+1$. ■

Lemma 5.4. *Let $r \geq 1$. Then $\mathscr{O}^1(\mathscr{M}^r)/\mathscr{O}^1(\mathscr{M}^{r+1})$ is isomorphic to the additive group of κ.*

Proof. We consider the injective group homomorphisms

$$\mathscr{O}^1(\mathscr{M}^{2r})/\mathscr{O}^1(\mathscr{M}^{2r+1}) \to \lambda, \qquad \left[\begin{pmatrix} a & b \\ \pi b' & a' \end{pmatrix}\right] \mapsto \frac{a-1}{\pi^r} \bmod \pi,$$

$$\mathscr{O}^1(\mathscr{M}^{2r-1})/\mathscr{O}^1(\mathscr{M}^{2r}) \to \lambda, \qquad \left[\begin{pmatrix} a & b \\ \pi b' & a' \end{pmatrix}\right] \mapsto \frac{b}{\pi^{r-1}} \bmod \pi.$$

The image is in both cases the kernel of the trace map $\mathrm{tr}_{\lambda/\kappa}$. ■

We summarise the results, reformulated for number fields:

Corollary 5.5. *Let k be a number field and B a quaternion algebra over k, unramified over at least one infinite place of k. Let $\mathscr{O} \subset B$ be a maximal order, and let $\mathfrak{p}$ be a prime of k of norm $q = p^f$. Let $r \geq 1$ and $H = \mathscr{O}^1/\mathscr{O}^1(\mathfrak{p}^r)$.*

(i) *If B is ramified at $\mathfrak{p}$, then H is solvable; the prime numbers appearing as orders in its composition series are p and the prime divisors of $q+1$.*

(ii) *If B is unramified at $\mathfrak{p}$ and $\mathfrak{p} \nmid 6$, then H is not solvable. Its composition factors are: once $\mathbb{Z}/2\mathbb{Z}$, once $\mathrm{PSL}(2,q)$ and $3f(r-1)$ times $\mathbb{Z}/p\mathbb{Z}$.*

In case (ii) for $\mathfrak{p} \mid 6$ we have to replace $\mathrm{PSL}(2,q)$, which is not necessarily simple then, by its composition factors.

6. Characters for Fuchsian groups. In this section we prove a criterion for two isomorphic lattices in $\mathrm{PSL}(2,\mathbb{R})$ to be conjugate:

Theorem 6.1. *Let Γ be a group, and for $j = 1, 2$ let $\varrho_j : \Gamma \to \mathrm{PSL}(2,\mathbb{R})$ be an injective group homomorphism such that $\varrho_j(\Gamma)$ is a lattice. Let $\Delta \subseteq \Gamma$ be a finite index subgroup, and assume that*

$$\mathrm{tr}^2\,\varrho_1(\gamma) = \mathrm{tr}^2\,\varrho_2(\gamma) \quad \textit{for all } \gamma \in \Delta. \tag{3}$$

Then there exists a unique $a \in \mathrm{PGL}(2,\mathbb{R})$ such that $\varrho_2(\gamma) = a\varrho_1(\gamma)a^{-1}$ for all $\gamma \in \Gamma$.

The proof of Theorem 6.1 rests on the following result, see [6, Proposition 1.5.2], as well as on subsequent elementary lemmas.

THEOREM 6.2 (Culler–Shalen). *Let $\varrho_1, \varrho_2 \colon \Gamma \to \mathrm{SL}(2,\mathbb{C})$ be two representations such that*

$$\operatorname{tr} \varrho_1(\gamma) = \operatorname{tr} \varrho_2(\gamma) \quad \text{for every } \gamma \in \Gamma, \tag{4}$$

and assume that ϱ_1 is irreducible. Then there exists $a \in \mathrm{SL}(2,\mathbb{C})$, unique up to sign, such that $\varrho_2(\gamma) = a\varrho_1(\gamma)a^{-1}$ for every $\gamma \in \Gamma$.

LEMMA 6.3. *Let $g \in \mathrm{PSL}(2,\mathbb{R})$, and let $\Sigma \subset \mathrm{PSL}(2,\mathbb{R})$ be a group generated by two hyperbolic elements without common fixed points. Then there exists $s \in \Sigma$ with sg hyperbolic.*

Proof. Lift g to an element $G \in \mathrm{SL}(2,\mathbb{R})$. First we will show that there exists some $S \in \tilde{\Sigma}$ with $\operatorname{tr}(SG) \neq 0$.

Assume, on the contrary, that $\operatorname{tr}(SG) = 0$ for all $S \in \tilde{\Sigma}$. Choose two hyperbolic elements $S_1, S_2 \in \tilde{\Sigma}$ without common fixed points; without loss of generality we may assume that

$$S_1 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \qquad S_2 = \begin{pmatrix} w & x \\ y & z \end{pmatrix}, \qquad G = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

for some $\lambda > 1$ and $xy \neq 0$. Then

$$\lambda a + \lambda^{-1} d = \operatorname{tr}(S_1 G) = 0 = \operatorname{tr} G = a + d,$$

hence $a = d = 0$ and

$$G = \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}, \quad bc = -\det G = -1, \text{ so } b, c \neq 0.$$

But then

$$cx + by = \operatorname{tr}(S_2 G) = 0 = \operatorname{tr}(S_1 S_2 G) = \lambda cx + \lambda^{-1} by,$$

hence $cx = by = 0$; however, we know that $b, c, x, y \neq 0$, a contradiction.

So there exists some $S \in \tilde{\Sigma}$ with $\operatorname{tr}(SG) \neq 0$; without loss of generality we assume that already $\operatorname{tr} G \neq 0$. Take some arbitrary hyperbolic $T \in \tilde{\Sigma}$; by the elementary equation

$$\operatorname{tr}(AB) + \operatorname{tr}(AB^{-1}) = \operatorname{tr}(A) \cdot \operatorname{tr}(B) \quad \text{for all } A, B \in \mathrm{SL}(2,\mathbb{C}) \tag{5}$$

we then have

$$|\operatorname{tr}(T^N G)| + |\operatorname{tr}(T^{-N} G)| \geq |\operatorname{tr}(T^N G) + \operatorname{tr}(T^{-N} G)| = |\operatorname{tr}(T^N) \operatorname{tr}(G)|.$$

But the right hand side goes to ∞ as $N \to \infty$, so for sufficiently large N, at least one of $|\operatorname{tr}(T^N G)|$ and $|\operatorname{tr}(T^{-N} G)|$ must be larger than 2. ∎

LEMMA 6.4. *Let $\Gamma \subset \mathrm{PSL}(2,\mathbb{R})$ be a lattice. Then there exists a finite generating system of Γ only consisting of hyperbolic elements.*

Proof. Assume that Γ is generated by $g_1, \ldots, g_n$. By [11, Exercise 2.13], Γ contains two hyperbolic elements h_1, h_2 without common fixed points; let them generate the group S. For each $1 \le j \le n$ choose some $s_j \in S$ with $s_j g_j$ hyperbolic. Then Γ is generated by the hyperbolic elements $h_1, h_2, s_1 g_1, \ldots, s_n g_n$. ■

LEMMA 6.5. *Let $a \in \mathrm{SL}(2,\mathbb{C})$, and let $\Gamma \subset \mathrm{SL}(2,\mathbb{R})$ be a lattice with $a\Gamma a^{-1} \subset \mathrm{SL}(2,\mathbb{R})$. Then $a \in \mathbb{C}^\times \cdot \mathrm{GL}(2,\mathbb{R})$.*

Proof. As Γ is Zariski-dense in $\mathrm{SL}(2,\mathbb{R})$, we may deduce that $a\mathrm{SL}(2,\mathbb{R})a^{-1} \subseteq \mathrm{SL}(2,\mathbb{R})$. The $\mathbb{R}$-vector subspace of $\mathrm{M}(2,\mathbb{C})$ generated by $\mathrm{SL}(2,\mathbb{R})$ is $\mathrm{M}(2,\mathbb{R})$, so $a\mathrm{M}(2,\mathbb{R})a^{-1} = \mathrm{M}(2,\mathbb{R})$. By the Skolem–Noether Theorem, the automorphism $g \mapsto aga^{-1}$ of $\mathrm{M}(2,\mathbb{R})$ has to be an inner automorphism, i.e. there exists $b \in \mathrm{GL}(2,\mathbb{R})$ with $aga^{-1} = bgb^{-1}$ for all $g \in \mathrm{M}(2,\mathbb{R})$, and hence, by linear extension, also for all $g \in \mathrm{M}(2,\mathbb{C})$. But this means that ba^{-1} is in the centre of $\mathrm{M}(2,\mathbb{C})$, which is $\mathbb{C}^\times$. ■

Proof of Theorem 6.1. Without loss of generality we may assume that Δ is torsion-free by Selberg's Lemma [26, Lemma 8], hence it has a presentation

$$\Delta = \langle g_1, \ldots, g_m \mid [g_1, g_{n+1}][g_2, g_{n+2}] \cdots [g_n, g_{2n}] = 1 \rangle \quad \text{with } m = 2n$$

(in the cocompact case), or is free on some generators $g_1, \ldots, g_m$ (otherwise). By [27, Theorem 4.1] each $\varrho_j|_\Delta$ can be lifted to representations $\tilde{\varrho}_j\colon \Delta \to \mathrm{SL}(2,\mathbb{R})$; furthermore again by that theorem we can arbitrarily prescribe the sign of each lift of $\varrho_j(g_i)$, so we may assume that

$$\mathrm{tr}\,\tilde{\varrho}_1(g_i) = \mathrm{tr}\,\tilde{\varrho}_2(g_i) \quad \text{for all } 1 \le i \le m. \tag{6}$$

More generally,

$$\mathrm{tr}\,\tilde{\varrho}_1(\gamma) = \varepsilon(\gamma) \cdot \mathrm{tr}\,\tilde{\varrho}_2(\gamma) \quad \text{for all } \gamma \in \Delta,$$

where ε is some function $\Delta \to \{\pm 1\}$. Note that ε is uniquely determined by this equation because the traces cannot be zero since elements of $\varrho_j(\Delta)$ are not elliptic. Furthermore $\varepsilon(g_i) = 1$ for every generator g_i by (6).

We now show that ε is identically 1. The crucial step is the following implication:

$$\text{If } \varepsilon(\gamma) = \varepsilon(\delta) = 1, \text{ then } \varepsilon(\gamma\delta) = \varepsilon(\gamma\delta^{-1}) = 1. \tag{7}$$

So assume that $\varepsilon(\gamma) = \varepsilon(\delta) = 1$. From (5) we deduce

$$\begin{aligned} \varepsilon(\gamma\delta)\,\mathrm{tr}\,\tilde{\varrho}_1(\gamma\delta) + \varepsilon(\gamma\delta^{-1})\,\mathrm{tr}\,\tilde{\varrho}_1(\gamma\delta^{-1}) &= \mathrm{tr}\,\tilde{\varrho}_2(\gamma\delta) + \mathrm{tr}\,\tilde{\varrho}_2(\gamma\delta^{-1}) \\ = \mathrm{tr}\,\tilde{\varrho}_2(\gamma) \cdot \mathrm{tr}\,\tilde{\varrho}_2(\delta) &= \mathrm{tr}\,\tilde{\varrho}_1(\gamma) \cdot \mathrm{tr}\,\tilde{\varrho}_1(\delta) = \mathrm{tr}\,\tilde{\varrho}_1(\gamma\delta) + \mathrm{tr}\,\tilde{\varrho}_1(\gamma\delta^{-1}). \end{aligned} \tag{8}$$

If $\varepsilon(\gamma\delta)$ and $\varepsilon(\gamma\delta^{-1})$ were both negative, (8) would entail $\mathrm{tr}\,\tilde{\varrho}_2(\gamma) \cdot \mathrm{tr}\,\tilde{\varrho}_2(\delta) = 0$, which is absurd because Δ does not contain elliptic elements. If $\varepsilon(\gamma\delta) = 1$ and $\varepsilon(\gamma\delta^{-1}) = -1$, then $\mathrm{tr}\,\tilde{\varrho}_2(\gamma\delta^{-1}) = 0$, which is again absurd; the other mixed case is ruled out in an analogous way. This proves (7).

Now we can prove that $\varepsilon(\gamma) = 1$ for every $\gamma \in \Delta$ by using induction on the word length $\ell(\gamma)$: this is the number of factors $g_j^{\pm 1}$ needed to obtain

γ as a product. If $\ell(\gamma) = 1$ then $\gamma = g_j^{\pm 1}$; since $\varepsilon(\gamma) = \varepsilon(\gamma^{-1})$, this must be equal to $\varepsilon(g_j) = 1$. If $\varepsilon(\gamma) = 1$ for all γ with $\ell(\gamma) \leq n$, we may use (7) and the trivial identity $\varepsilon(\gamma^{-1}) = \varepsilon(\gamma)$ to show the statement for all γ with $\ell(\gamma) \leq n+1$. Therefore by induction, ε is identically 1, hence

$$\operatorname{tr} \tilde{\varrho}_1(\gamma) = \operatorname{tr} \tilde{\varrho}_2(\gamma) \quad \text{for all } \gamma \in \varDelta.$$

By Theorem 6.2 this means that $\tilde{\varrho}_1$ is conjugate to $\tilde{\varrho}_2$ within $\mathrm{SL}(2,\mathbb{C})$; but since all images are real, the conjugation must be possible within $\mathrm{GL}(2,\mathbb{R})$ by Lemma 6.5. This in turn means $\varrho_1|_\varDelta$ and $\varrho_2|_\varDelta$ are conjugate in $\mathrm{PGL}(2,\mathbb{R})$.

We need to extend this to the entire group $\varGamma$. Without loss of generality we may assume that $\varrho_1|_\varDelta = \varrho_2|_\varDelta$. By Lemma 6.4 there exists a generating system $\gamma_1, \ldots, \gamma_m$ of $\varGamma$, not necessarily related in any way to that of $\varDelta$, such that all $\varrho_1(\gamma_j)$ are hyperbolic. But some power of each γ_j is contained in $\varDelta$, and hence $\varrho_1(\gamma_j)^N = \varrho_2(\gamma_j)^N$. Under the assumptions on γ_j this entails $\varrho_1(\gamma_j) = \varrho_2(\gamma_j)$, that is, $\varrho_1 = \varrho_2$. ∎

7. Modular embeddings. Let once again $\varGamma \subset \mathrm{PSL}(2,\mathbb{R})$ be a semi-arithmetic lattice satisfying the trace field condition, with trace field k, quaternion algebra B, maximal order $\mathscr{O}$ and algebraic group $G = \operatorname{Res}_{k/\mathbb{Q}} H$. As explained above, $\varGamma$ is a subgroup of the arithmetic group $\mathrm{P}\mathscr{O}^1$. Now that latter group naturally lives on the symmetric space of G, i.e. on $G(\mathbb{R})/K$ for a maximal compact subgroup K. This space can be described explicitly as $\mathfrak{H}^r$ where $\mathfrak{H}$ is the upper half-plane and $r \leq d = [k:\mathbb{Q}]$. Let $\sigma_1, \ldots, \sigma_d \colon k \to \mathbb{R}$ be the field embeddings, where σ_1 is the identity embedding. We may also assume that the quaternion algebra $B \otimes_{k,\sigma_i} \mathbb{R}$ is isomorphic to $\mathrm{M}(2,\mathbb{R})$ for $1 \leq i \leq r$ and to $\mathbb{H}$ for $r < i \leq d$.

For each $1 \leq i \leq r$ we choose an isomorphism $\alpha_i \colon B \otimes_{k,\sigma_i} \mathbb{R} \to \mathrm{M}(2,\mathbb{R})$. We obtain an embedding

$$\alpha \colon \mathscr{O}^1 \hookrightarrow \mathrm{SL}(2,\mathbb{R})^r, \qquad x \mapsto (\alpha_1(x), \ldots, \alpha_r(x)),$$

descending to an embedding $\alpha \colon \mathrm{P}\mathscr{O}^1 \hookrightarrow \mathrm{PSL}(2,\mathbb{R})^r$. We denote the image by $\varLambda = \alpha(\mathrm{P}\mathscr{O}^1)$.

Theorem 7.1. *$\varLambda$ is an irreducible arithmetic lattice in* $\mathrm{PSL}(2,\mathbb{R})^r$.

For the proof see e.g. [28].

Note that $\alpha(\varGamma)$ becomes a subgroup of $\varLambda$. It has finite index precisely if $\varGamma$ is already arithmetic; in every case $\alpha(\varGamma)$ is a Zariski-dense subgroup of $\varLambda$ by the proof of Proposition 4.4. Zariski-dense subgroups of infinite index in arithmetic groups are called *thin*, and so we have shown:

Corollary 7.2. *If $\varGamma$ is not arithmetic itself, the embedding $\alpha \colon \varGamma \to \varLambda$ realises $\varGamma$ as a thin group.*

Let $\mathrm{PSL}(2,\mathbb{R})^r$ operate by component-wise Möbius transformations on $\mathfrak{H}^r$; the induced action of Λ on $\mathfrak{H}^r$ is properly discontinuous and has a quotient of finite volume. This motivates the following definition:

DEFINITION 7.3. A *modular embedding* of Γ is a holomorphic embedding $F\colon \mathfrak{H} \to \mathfrak{H}^r$ such that

$$F(\gamma\tau) = \alpha(\gamma)F(\tau)$$

for every $\gamma \in \Gamma$ and every $\tau \in \mathfrak{H}$.

The following result which will be used later on is [25, Corollary 5]:

PROPOSITION 7.4. *Let $\Gamma \subset \mathrm{PSL}(2,\mathbb{R})$ be a semiarithmetic group which satisfies the trace field property and admits a modular embedding, and let $k = \mathbb{Q}(\mathrm{tr}\,\Gamma)$. Let $\gamma \in \tilde{\Gamma}$ be hyperbolic and let $\sigma\colon k \to \mathbb{R}$ be an embedding which is not the identity inclusion. Then $|\sigma(\mathrm{tr}\,\gamma)| < |\mathrm{tr}\,\gamma|$.*

Note that if Γ is an arithmetic group, then even $|\sigma(\mathrm{tr}\,\gamma)| < 2$ by Proposition 4.3.

8. Congruence rigidity. Let $\Gamma \subset \mathrm{PSL}(2,\mathbb{R})$ be a semiarithmetic lattice satisfying the trace field condition, with trace field $k = \mathbb{Q}(\mathrm{tr}\,\Gamma)$. Let $B = k[\tilde{\Gamma}]$ be the associated quaternion algebra and G the algebraic group over $\mathbb{Q}$ with $G(\mathbb{Q}) = B^1$. Let $\mathscr{O} \subset B$ be a maximal order containing $\tilde{\Gamma}$, and let $\mathfrak{m} \subset \mathfrak{o}_k$ be such that a finite index subgroup of Γ is adelically dense in $\mathrm{P}\mathscr{O}^1(\mathfrak{m})$; in particular, $\mathfrak{m}$ satisfies the conclusion of Proposition 4.5.

For the statement of the next proposition, we need to introduce some finite sets of rational primes:

(i) Let $\mathfrak{m} = \mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}$ be the prime factorisation of $\mathfrak{m}$, and let ℓ_j be the norm of the prime ideal $\mathfrak{l}_j$. Then $S(\mathfrak{m})$ denotes the set of all rational primes diving some $|\mathrm{PSL}(2,\ell_j)|$ (this includes the primes dividing ℓ_j or $\ell_j + 1$). Note that if $\mathfrak{m}'$ is an ideal which has the same prime divisors as $\mathfrak{m}$, and if ℓ is a rational prime dividing the order of $\mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{m}')$, then $\ell \in S(\mathfrak{m})$.

(ii) $S(6)$ is the set consisting of 2, 3 and all prime divisors of orders of $\mathrm{PSL}(2,q)$ where q is the norm of a prime ideal $\mathfrak{p}$ in k with $\mathfrak{p} \mid 6$.

(iii) $S(B)$ is the set of all rational primes that lie below those finite primes of k in which B is ramified.

Then we set $S(\Gamma) = S(\mathfrak{m}) \cup S(6) \cup S(B)$.

PROPOSITION 8.1. *Let Γ be as above, and let $q = p^f$ be an odd prime power which is prime to all primes in $S(\Gamma)$. Let $\Delta \subset \Gamma$ be a normal congruence subgroup such that $\Gamma/\Delta \simeq \mathrm{PSL}(2,q)$. Then there exists a unique prime $\mathfrak{p}$ of norm q in k such that $\Delta = \Gamma(\mathfrak{p})$.*

Proof. There exists an ideal $\mathfrak{n}$ such that $\Delta \supseteq \Gamma(\mathfrak{n})$ and a finite index subgroup of Δ is adelically dense in $\mathrm{P}\mathscr{O}^1(\mathfrak{n})$. We may assume that $\mathfrak{m}$ divides $\mathfrak{n}$. Write $\mathfrak{n} = \mathfrak{n}' \cdot \mathfrak{n}_{\mathfrak{m}}$ with $\mathfrak{n}'$ coprime to $\mathfrak{m}$, and $\mathfrak{n}_{\mathfrak{m}}$ having the same prime divisors as $\mathfrak{m}$; then Γ also contains a subgroup which is adelically dense in $\mathrm{P}\mathscr{O}^1(\mathfrak{n}_{\mathfrak{m}})$. By Proposition 4.5 this entails that Γ surjects onto $\mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{n}')$.

Denote the quotient map modulo Δ by

$$\pi\colon \Gamma \to \mathrm{PSL}(2,q).$$

Note that π is continuous in the adelic topology on Γ since it vanishes on $\Gamma(\mathfrak{n})$.

Now $\Gamma(\mathfrak{n}') = \Gamma \cap \mathrm{P}\mathscr{O}^1(\mathfrak{n}')$ is a normal subgroup of Γ, hence its image under π is a normal subgroup of $\mathrm{PSL}(2,q)$. Since that group is simple, the image can only be $\mathrm{PSL}(2,q)$ or the trivial group. Assume it were the entire group; then in the sequence

$$\mathrm{PSL}(2,q) \twoheadleftarrow \Gamma(\mathfrak{n}')/\Gamma(\mathfrak{n}) \hookrightarrow \mathrm{P}\mathscr{O}^1(\mathfrak{n}')/\mathrm{P}\mathscr{O}^1(\mathfrak{n}) \simeq \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{n}_{\mathfrak{m}})$$

(where the isomorphism is by Corollary 4.10) the order of the left hand side would divide the order of the right hand side. But the former is divisible by p, the latter only by primes in $S(\Gamma)$. This is a contradiction, hence the image of $\Gamma(\mathfrak{n}')$ under π is the trivial group. In other words,

$$\Delta \supseteq \Gamma(\mathfrak{n}').$$

This implies that π descends to an epimorphism

$$\pi\colon \Gamma/\Gamma(\mathfrak{n}') \twoheadrightarrow \mathrm{PSL}(2,q).$$

By Proposition 4.5 the inclusion $\Gamma \subseteq \mathrm{P}\mathscr{O}^1$ induces an isomorphism

$$\alpha\colon \Gamma/\Gamma(\mathfrak{n}') \xrightarrow{\simeq} \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{n}').$$

So by composition we obtain an epimorphism $\pi \circ \alpha^{-1}\colon \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{n}') \twoheadrightarrow \mathrm{PSL}(2,q)$.

Let $\mathfrak{n}' = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$ with distinct prime ideals $\mathfrak{p}_j$, and let $\mathrm{rad}(\mathfrak{n}') = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Then $\mathrm{P}\mathscr{O}^1(\mathrm{rad}(\mathfrak{n}'))/\mathrm{P}\mathscr{O}^1(\mathfrak{n}')$ is a solvable normal subgroup of $\mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{n}')$ by Lemma 5.2, so its image by $\pi \circ \alpha^{-1}$ has to be a solvable normal subgroup of $\mathrm{PSL}(2,q)$, i.e. trivial. Therefore $\pi \circ \alpha^{-1}$ factors through $\mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathrm{rad}(\mathfrak{n}'))$; we summarise this in a diagram:

$$\begin{tikzcd}
\Gamma/\Gamma(\mathfrak{n}') \arrow[r, "\simeq", "\alpha"'] \arrow[dr, two heads, "\pi"'] & \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{n}') \arrow[r, two heads] \arrow[d, two heads] & \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathrm{rad}(\mathfrak{n}')) \arrow[dl, dashed, two heads] \\
& \mathrm{PSL}(2,q) &
\end{tikzcd} \tag{9}$$

Now the rightmost entry projects onto

$$\mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{p}_1) \times \cdots \times \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{p}_n), \tag{10}$$

and by Corollary 4.8 the kernel of this projection is an abelian normal subgroup, which is therefore mapped to the identity element by the dashed arrow in (9). Hence that dashed arrow is defined on (10); by Lemma 3.4 it actually has to factor through the projection onto one of them, composed with an isomorphism. We hence obtain

$$\begin{tikzcd}
\Gamma/\Gamma(\mathfrak{n}') \arrow[r, "\simeq", "\alpha"'] \arrow[dr, two heads, "\pi"'] & \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{n}') \arrow[r, two heads] \arrow[d, two heads] & \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{p}_j) \arrow[dl, dashed, "\simeq"] \\
& \mathrm{PSL}(2,q) &
\end{tikzcd}$$

for some $1 \le j \le n$. We may shorten this to

(11)
$$\begin{tikzcd}
\Gamma/\Gamma(\mathfrak{p}_j) \arrow[rr, "\simeq", "\alpha'"'] \arrow[dr, two heads, "\pi'"'] & & \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{p}_j) \arrow[dl, dashed, "\simeq"] \\
& \mathrm{PSL}(2,q) &
\end{tikzcd}$$

with α' again induced by the inclusion $\Gamma \subseteq \mathrm{P}\mathscr{O}^1$. In this diagram π' is obviously an isomorphism, therefore $\Delta = \ker \pi$ is equal to $\Gamma(\mathfrak{p}_j)$. The dashed isomorphism in (11) shows that the norm of $\mathfrak{p}_j$ is q. ■

Remark 8.2. We note that this proposition enables us to reconstruct the splitting behaviour of almost all primes in k from Γ and its congruence subgroups: Let $p \notin S(\Gamma)$ be a rational prime in Γ. Then there exist only finitely many normal congruence subgroups $\Delta \lhd \Gamma$ such that $\Gamma/\Delta \simeq \mathrm{PSL}(2,q)$ for some power q of p. Let these be $\Delta_1, \dots, \Delta_n$, and let the corresponding quotients be $\mathrm{PSL}(2,p^{f_1}), \dots, \mathrm{PSL}(2,p^{f_n})$.

On the other hand consider the prime decomposition $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_m$ in k. Then $n = m$, and up to renumeration $\Delta_j = \Gamma(\mathfrak{p}_j)$ and $N(\mathfrak{p}_j) = p^{f_j}$. In particular we can reconstruct $[k\colon \mathbb{Q}] = f_1 + \cdots + f_n$ from the knowledge of Γ and its congruence subgroups.

Proof of Theorem A. By Theorem 6.1 we may replace Γ_j by finite index subgroups corresponding to each other under f. Hence we may assume that each Γ_j is torsion-free and satisfies the trace field condition. Again by Theorem 6.1 it suffices to show that $\mathrm{tr}^2 f(\gamma) = \mathrm{tr}^2 \gamma \in \mathbb{R}$ for each $\gamma \in \Gamma_1$.

Denote the trace field of Γ_j by k_j. Each number $a \in \mathfrak{o}_{k_j}$ has a *characteristic polynomial* $\chi_a(x) \in \mathbb{Z}[x]$ which can be described as follows:

- it is the characteristic polynomial of the map $k_j \to k_j$, $v \mapsto av$, interpreted as a $\mathbb{Q}$-linear map;
- it is equal to $\prod_\sigma (x - \sigma(a))$; here σ runs through a system of representatives of $\mathrm{Gal}(L_j/\mathbb{Q})$ modulo $\mathrm{Gal}(L_j/k_j)$ where L_j is the Galois closure of k_j.

Now let p be a rational prime not in $S(\Gamma_1) \cup S(\Gamma_2)$. By Remark 8.2 we can decompose $p\mathfrak{o}_{k_j}$ into prime ideals

$$p\mathfrak{o}_{k_1} = \mathfrak{p}_1 \cdots \mathfrak{p}_n, \qquad p\mathfrak{o}_{k_2} = \mathfrak{q}_1 \cdots \mathfrak{q}_n$$

in such a way that

$$f(\Gamma_1(\mathfrak{p}_j)) = \Gamma_2(\mathfrak{q}_j) \quad \text{and} \quad \mathfrak{o}_{k_1}/\mathfrak{p}_j \simeq \mathfrak{o}_{k_2}/\mathfrak{q}_j. \tag{12}$$

Then

$$\mathfrak{o}_{k_1}/p\mathfrak{o}_{k_1} \simeq \mathfrak{o}_{k_1}/\mathfrak{p}_1 \times \cdots \times \mathfrak{o}_{k_1}/\mathfrak{p}_d \tag{13}$$

is a finite-dimensional $\mathbb{F}_p$-algebra, and we may similarly define the characteristic polynomial $\chi_{\bar{b}}(x) \in \mathbb{F}_p[x]$ of an element $\bar{b} \in \mathfrak{o}_{k_1}/p\mathfrak{o}_{k_1}$ as the characteristic polynomial of the $\mathbb{F}_p$-linear endomorphism of $\mathfrak{o}_{k_1}/p\mathfrak{o}_{k_1}$ given by multiplication by $\bar{b}$. Then for $a \in \mathfrak{o}_{k_1}$ clearly

$$\chi_a(x) \bmod p = \chi_{a \bmod p}(x) \in \mathbb{F}_p[x]. \tag{14}$$

We now claim that the characteristic polynomials of $\operatorname{tr}^2\gamma$ and $\operatorname{tr}^2 f(\gamma)$ are congruent modulo p. To see this we use the abstract version of squared traces on finite groups introduced in Section 3. For each $1 \le j \le n$, using (12) we obtain an isomorphism of finite groups $\bar{f}\colon \Gamma_1/\Gamma_1(\mathfrak{p}_j) \to \Gamma_2/\Gamma_2(\mathfrak{q}_j)$. By the remark after Definition 3.3, $\operatorname{tr}^2\gamma \bmod \mathfrak{p}_j$ and $\operatorname{tr}^2 f(\gamma) \bmod \mathfrak{q}_j$ are Galois-conjugate elements of the finite field $\mathbb{F}_q \simeq \mathfrak{o}_{k_1}/\mathfrak{p}_j \simeq \mathfrak{o}_{k_2}/\mathfrak{q}_j$. Hence there exists an isomorphism of $\mathbb{F}_p$-algebras

$$\alpha_j\colon \mathfrak{o}_{k_1}/\mathfrak{p}_j \xrightarrow{\simeq} \mathfrak{o}_{k_2}/\mathfrak{q}_j$$

with $\alpha_j(\operatorname{tr}^2\gamma \bmod \mathfrak{p}_j) = \operatorname{tr}^2 f(\gamma) \bmod \mathfrak{q}_j$. Gluing these together componentwise in (13) yields an isomorphism of $\mathbb{F}_p$-algebras $\alpha\colon \mathfrak{o}_{k_1}/p\mathfrak{o}_{k_1} \to \mathfrak{o}_{k_2}/p\mathfrak{o}_{k_2}$ with $\alpha(\operatorname{tr}^2\gamma \bmod p) = \operatorname{tr}^2 f(\gamma) \bmod p$. Since characteristic polynomials are stable under algebra isomorphisms, we obtain

$$\chi_{\operatorname{tr}^2\gamma \bmod p}(x) = \chi_{\operatorname{tr}^2 f(\gamma) \bmod p}(x) \in \mathbb{F}_p[x].$$

By (14), this means

$$\chi_{\operatorname{tr}^2\gamma}(x) \equiv \chi_{\operatorname{tr}^2 f(\gamma)}(x) \bmod p.$$

But this holds for infinitely many p, so

$$\chi_{\operatorname{tr}^2\gamma}(x) = \chi_{\operatorname{tr}^2 f(\gamma)}(x) \in \mathbb{Z}[x].$$

Since we assumed Γ_1 to be torsion-free, γ cannot be elliptic. If it is parabolic, then $\operatorname{tr}^2\gamma = 4$ and therefore $\chi_{\operatorname{tr}^2\gamma}(x) = (x-4)^d$. Hence also the characteristic polynomial of $f(\gamma)$ is $(x-4)^d$, and since $\operatorname{tr}^2 f(\gamma)$ is a zero of this polynomial, $\operatorname{tr}^2 f(\gamma) = 4$, so $f(\gamma)$ is parabolic as well.

Finally assume that γ is hyperbolic. Then $f(\gamma)$ must also be hyperbolic because it cannot be parabolic (else γ would be parabolic by the inverse of the previous argument). By Proposition 7.4, $\mathrm{tr}^2\gamma$ is the largest zero of $\chi_{\mathrm{tr}^2\gamma}(x)$, similarly for $\mathrm{tr}^2 f(\gamma)$. Therefore $\mathrm{tr}^2\gamma = \mathrm{tr}^2 f(\gamma)$. ∎

9. An example. In our proof of Theorem A we did not use the full assumption that all congruence subgroups are mapped to congruence subgroups by the given isomorphism. We spell out in a concrete example how far an isomorphism between non-conjugate arithmetic groups can be from preserving congruence subgroups.

In [32] we find a complete list of all arithmetic groups of signature $(1;2)$, i.e. whose associated Riemann surfaces have genus one and which have one conjugacy class of elliptic elements, these elements being of order two. In particular all these groups are abstractly isomorphic, and we may just pick the first two of them: Γ_1' is generated by the two Möbius transformations

$$\alpha_1 = \pm\begin{pmatrix} \frac{1+\sqrt{5}}{2} & 0 \\ 0 & \frac{-1+\sqrt{5}}{2} \end{pmatrix} \quad\text{and}\quad \beta_1 = \pm\begin{pmatrix} \sqrt{3} & \sqrt{2} \\ \sqrt{2} & \sqrt{3} \end{pmatrix},$$

and Γ_2' by the two Möbius transformations

$$\alpha_2 = \pm\begin{pmatrix} \sqrt{2}+1 & 0 \\ 0 & \sqrt{2}-1 \end{pmatrix} \quad\text{and}\quad \beta_2 = \pm\frac{1}{2}\begin{pmatrix} \sqrt{6} & \sqrt{2} \\ \sqrt{2} & \sqrt{6} \end{pmatrix}.$$

These are, respectively, generators satisfying the relation $(\alpha_j\beta_j\alpha_j^{-1}\beta_j^{-1})^2 = 1$. So there exists a group isomorphism $f\colon \Gamma_1' \to \Gamma_2'$ with $f(\alpha_1) = \alpha_2$ and $f(\beta_1) = \beta_2$. The Γ_j' do not satisfy the trace field condition, but the $\Gamma_j = (\Gamma_j')^{(2)}$ (between which f also induces an isomorphism) do; in both cases the invariant trace field is $\mathbb{Q}$.

Then, with finitely many exceptions, $\Gamma_1/\Gamma_1(p) \simeq \mathrm{PSL}(2,p) \simeq \Gamma_2/\Gamma_2(p)$ for rational primes p; nevertheless, the proof of Theorem A shows that there can only be finitely many p such that $f(\Gamma_1(p))$ is a congruence subgroup (and hence only finitely many p with $f(\Gamma_1(p)) = \Gamma_2(p)$).

10. Concluding remarks

Remark 10.1. In Theorem A, the assumption that f preserves congruence subgroups is necessary, even in the arithmetic case. For example [7], let Δ be the triangle group of signature $(2,3,7)$. This is an arithmetic group, and since it is generated by elements of odd finite orders, $\Delta = \Delta^{(2)}$. Therefore, Δ satisfies the trace field condition with trace field $k = \mathbb{Q}(\cos 2\pi/7)$, and the associated quaternion order is maximal and unramified at all finite primes of k. The rational prime 13 decomposes as $(13) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ in k, with three Galois-conjugate primes $\mathfrak{p}_j$ of norm 13.

[7] This example was suggested to the author by the referee.

We set $\Gamma_j = \Delta(\mathfrak{p}_j)$. These groups still satisfy the trace field condition, and from the standard presentation of Δ we see that all non-trivial normal subgroups of Δ are torsion-free. A simple Euler characteristic calculation using $\Delta/\Gamma_j \simeq \mathrm{PSL}(2,13)$ shows that the Γ_j are cocompact surface groups of genus 14. Hence there exists some group isomorphism $f\colon \Gamma_1 \to \Gamma_2$, say. But there are various ways to see the Γ_j cannot be conjugate in $\mathrm{PGL}(2,\mathbb{R})$, for example by studying the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the algebraic curves $\Gamma_j \setminus \mathfrak{H}$ (see [29]), or by exploiting the fact that Δ is a maximal discrete subgroup of $\mathrm{PSL}(2,\mathbb{R})$, hence the normaliser of Γ_j in $\mathrm{PSL}(2,\mathbb{R})$ is Δ. So, arguing as in Section 9 we see that only finitely many of the $f(\Gamma_1(\ell))$, where ℓ runs through the rational primes inert in k, can be congruence subgroups again.

For more information on the principal congruence subgroups of Δ and proofs of the above-mentioned facts see [7].

Remark 10.2. The assumption that both groups admit a modular embedding is crucial, although it only enters in the very last step of the proof. If Γ is a semiarithmetic lattice with invariant trace field k and $\sigma\colon k \to \mathbb{R}$ a field embedding, we obtain in a natural way a group $i_\sigma(\Gamma) \subset \mathrm{PSL}(2,\mathbb{R})$ (see [25, Remark 4]). There exist semiarithmetic lattices Γ with non-trivial Galois conjugates $i_\sigma(\Gamma)$ that are again lattices, and then the isomorphism $\Gamma \to i_\sigma(\Gamma)$ preserves congruence subgroups but not traces. For an explicit construction see e.g. [1] referring to [3, Proposition 4.11]. But if Γ admits a modular embedding, then none of the non-trivial Galois conjugates $i_\sigma(\Gamma)$ can be discrete by [25, Theorem 3].

Note that the existence of a modular embedding enters the proof via Proposition 7.4 which is its only genuinely non-algebraic ingredient: it is a consequence of the Schwarz Lemma.

One may still ask whether a weakened version of our main theorem holds in the general case: if $f\colon \Gamma_1 \to \Gamma_2$ is an isomorphism between semiarithmetic lattices in $\mathrm{PSL}(2,\mathbb{R})$ respecting congruence subgroups, is it the composition of an inner automorphism of $\mathrm{PGL}(2,\mathbb{R})$ with a Galois conjugation of the trace field?

Remark 10.3. There exist arithmetic Fuchsian groups with different trace fields but whose congruence completions are isomorphic away from a finite set of primes. To see this, start with the polynomial in the remark after [15, Theorem 5.1]: the splitting field of this polynomial is a totally real Galois extension of $\mathbb{Q}$ with Galois group $\mathrm{PSL}(2,7)$. By the discussion in [22, pp. 358–359] such a field contains two subfields k_1, k_2 which are not isomorphic but have the same Dedekind zeta function. Then there exists a finite set S of rational primes such that $\mathbb{A}_{k_1}^S \simeq \mathbb{A}_{k_2}^S$. From this we can easily construct arithmetic Fuchsian groups over k_1 and k_2 with isomorphic prime-to-S congruence completion.

There also exist non-isomorphic number fields with isomorphic finite adele rings (at all primes) (see [12]). But no construction seems to be known where these fields are totally real.

Acknowledgments. The author wishes to thank Ursula Hamenstädt for many fruitful discussions, and helpful comments on earlier versions of this article. He is also indebted to the anonymous referee for careful proofreading and some suggestions for improvement, most notably the example described in Remark 10.1.

References

[1] I. Agol, *mathoverflow answer to: Can Galois conjugates of lattices in* $\mathrm{SL}(2,\mathbb{R})$ *be discrete?*, 2014, http://mathoverflow.net/questions/155798/can-galois-conjugates-of-lattices-in-sl2-r-be-discrete.

[2] I. I. Bouw and M. Möller, *Teichmüller curves, triangle groups, and Lyapunov exponents*, Ann. of Math. 172 (2010), 139–185.

[3] B. H. Bowditch, *Markoff triples and quasi-Fuchsian groups*, Proc. London Math. Soc. 77 (1998), 697–736.

[4] M. R. Bridson, M. D. E. Conder, and A. W. Reid, *Determining Fuchsian groups by their finite quotients*, arXiv:1401.3645v1 (2014).

[5] P. Cohen and J. Wolfart, *Modular embeddings for some nonarithmetic Fuchsian groups*, Acta Arith. 56 (1990), 93–110.

[6] M. Culler and P. B. Shalen, *Varieties of group representations and splittings of 3-manifolds*, Ann. of Math. 117 (1983), 109–146.

[7] A. Džambić, *Macbeath's infinite series of Hurwitz groups*, in: Arithmetic and Geometry around Hypergeometric Functions, Progr. Math. 260, Birkhäuser, Basel, 2007, 101–108.

[8] S. Geninska, *Examples of infinite covolume subgroups of* $\mathrm{PSL}(2,\mathbb{R})^r$ *with big limit sets*, Math. Z. 272 (2012), 389–404.

[9] E. Gutkin and C. Judge, *The geometry and arithmetic of translation surfaces with applications to polygonal billiards*, Math. Res. Lett. 3 (1996), 391–403.

[10] P. Hubert and T. A. Schmidt, *An introduction to Veech surfaces*, in: Handbook of Dynamical Systems, Vol. 1B, Elsevier, Amsterdam, 2006, 501–526.

[11] S. Katok, *Fuchsian Groups*, Chicago Lectures in Math., Univ. of Chicago Press, Chicago, IL, 1992.

[12] K. Komatsu, *On adele rings of arithmetically equivalent fields*, Acta Arith. 43 (1984), 93–95.

[13] R. Kucharczyk, *On arithmetic properties of Fuchsian groups and Riemann surfaces*, Ph.D. thesis, Univ. of Bonn, 2014.

[14] C. Maclachlan and A. W. Reid, *The Arithmetic of Hyperbolic 3-Manifolds*, Grad. Texts in Math. 219, Springer, New York, 2003.

[15] G. Malle, *Multi-parameter polynomials with given Galois group*, J. Symbolic Comput. 30 (2000), 717–731.

[16] C. R. Matthews, L. N. Vaserstein, and B. Weisfeiler, *Congruence properties of Zariski-dense subgroups. I*, Proc. London Math. Soc. 48 (1984), 514–532.

[17] C. T. McMullen, *Billiards and Teichmüller curves on Hilbert modular surfaces*, J. Amer. Math. Soc. 16 (2003), 857–885.

[18] J. S. Milne, *Introduction to Shimura varieties*, in: Harmonic Analysis, the Trace Formula, and Shimura Varieties, Clay Math. Proc. 4, Amer. Math. Soc., Providence, RI, 2005, 265–378.

[19] M. Möller, *Variations of Hodge structures of a Teichmüller curve*, J. Amer. Math. Soc. 19 (2006), 327–344.

[20] G. D. Mostow, *Quasi-conformal mappings in n-space and the rigidity of hyperbolic space forms*, Inst. Hautes Études Sci. Publ. Math. 34 (1968), 53–104.

[21] M. V. Nori, *On subgroups of* $\mathrm{GL}_n(\mathbf{F}_p)$, Invent. Math. 88 (1987), 257–275.

[22] R. Perlis, *On the equation* $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory 9 (1977), 342–360.

[23] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Pure Appl. Math. 139, Academic Press, Boston, MA, 1994.

[24] G. Prasad, *Strong rigidity of* $\mathbf{Q}$*-rank* 1 *lattices*, Invent. Math. 21 (1973), 255–286.

[25] P. Schmutz Schaller and J. Wolfart, *Semiarithmetic Fuchsian groups and modular embeddings*, J. London Math. Soc. (2) 61 (2000), 13–24.

[26] A. Selberg, *On discontinuous groups in higher-dimensional symmetric spaces*, in: Contributions to Function Theory (Bombay, 1960), Tata Inst. Fund. Res., Bombay, 1960, 147–164.

[27] M. Seppälä and T. Sorvali, *Traces of commutators of Möbius transformations*, Math. Scand. 68 (1991), 53–58.

[28] G. Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. 85 (1967), 58–159.

[29] M. Streit, *Field of definition and Galois orbits for the Macbeath–Hurwitz curves*, Arch. Math. (Basel) 74 (2000), 342–349.

[30] K. Takeuchi, *A characterization of arithmetic Fuchsian groups*, J. Math. Soc. Japan 27 (1975), 600–612.

[31] K. Takeuchi, *Arithmetic triangle groups*, J. Math. Soc. Japan 29 (1977), 91–106.

[32] K. Takeuchi, *Arithmetic Fuchsian groups with signature* $(1; e)$, J. Math. Soc. Japan 35 (1983), 381–407.

[33] W. A. Veech, *Teichmüller curves in moduli space, Eisenstein series and an application to triangular billiards*, Invent. Math. 97 (1989), 553–583; Erratum, ibid. 103 (1991), 447.

[34] R. A. Wilson, *The Finite Simple Groups*, Grad. Texts in Math. 251, Springer, London, 2009.

Robert A. Kucharczyk
Mathematisches Institut
Universität Bonn
Endenicher Allee 60
53115 Bonn, Germany
E-mail: rak@math.uni-bonn.de

Received on 18.11.2014
and in revised form on 24.2.2015 (8005)