SLICEABLE GROUPS and TOWERS OF FIELDS

In memory of Oleg V. Mel'nikov

by

Sigrid Böge, Universität Heidelberg, boege@mathi.uni-heidelberg.de,
Moshe Jarden*, Tel Aviv University, jarden@post.tau.ac.il, and
Alexander Lubotzky**, The Hebrew University in Jerusalem, alex.lubotzky@mail.huji.ac.il

Abstract

Let l be a prime number, K a finite extension of $\mathbb{Q}_l$, and D a finite dimensional central division algebra over K. We prove that the profinite group $G = D^\times/K^\times$ is **finitely sliceable**, i.e. G has finitely many closed subgroups $H_1, \ldots, H_n$ of infinite index such that $G = \bigcup_{i=1}^n H_i^G$. Here, $H_i^G = \{h^g \mid h \in H_i,\ g \in G\}$. On the other hand, we prove for $l \neq 2$ that no open subgroup of $\mathrm{GL}_2(\mathbb{Z}_l)$ is finitely sliceable and give an arithmetic interpretation to this result, based on the possibility to realize $\mathrm{GL}_2(\mathbb{Z}_l)$ as a Galois group over $\mathbb{Q}$. Nevertheless, we prove that $G = \mathrm{GL}_2(\mathbb{Z}_l)$ has an **infinite slicing**, that is $G = \bigcup_{i=1}^\infty H_i^G$, where each H_i is a closed subgroup of G of infinite index and $H_i \cap H_j$ has infinite index in both H_i and H_j if $i \neq j$.

MR Classification 12E30

30 August 2015

---

* Research supported by the Minkowski Center for Geometry at Tel Aviv University, established by the Minerva Foundation, and by an ISF grant.

** The third author acknowledges "Dr. Max Rössler, the Walter Haefner Foundation", the ETH Foundation, and the ETH Institute for Theoretical studies for support and hospitality. In addition, the author acknowledges support by ISF and NSF.

26 August 2015

Introduction

This work grew out of questions coming from both arithmetic and group theory. We start with the arithmetical motivation.

KRONECKER TOWERS. We denote the set of prime numbers p that have a prime divisor $\mathfrak{p}$ of degree 1 in a given number field K by $D(K)$. Jehne [Jeh77] calls two number fields L and L' **Kronecker equivalent** if $D(L)$ and $D(L')$ differ only by finitely many elements. An **infinite Kronecker tower** is a strictly increasing sequence $L_1 \subset L_2 \subset L_3 \subset \cdots$ of Kronecker equivalent number fields. The existence of such a tower has been posed by Jehne [Jeh77, Sec. 7] as an open problem. It has also been stated as [FrJ08, p. 467, Problem 21.5.8]. To the best of our knowledge, that problem has never been solved (see also Notes to Chapter 21 of [FrJ08]).

A theorem of Dedekind and Kummer [Lan70, p. 27, Prop. 25] gives a number theoretic interpretation to the Kronecker equivalence of two number fields L and L': Let x (resp. x') be an integral primitive element for $L/\mathbb{Q}$ (resp. $L'/\mathbb{Q}$) and let $f = \mathrm{irr}(x, \mathbb{Q})$ (resp. $f' = \mathrm{irr}(x', \mathbb{Q})$). Then, L and L' are Kronecker equivalent if and only if for **almost all** p (i.e. for all but finitely many p's), $f(X)$ has a root modulo p if and only if $f'(X)$ has one.

Chebotarev's density theorem provides a group theoretic interpretation to the Kronecker equivalence of L and L': Let N be a finite Galois extension of $\mathbb{Q}$ that contains both L and L' and set $G = \mathrm{Gal}(N/\mathbb{Q})$. Then, L and L' are Kronecker equivalent if and only if

$$\bigcup_{\sigma \in G} \mathrm{Gal}(N/L)^\sigma = \bigcup_{\sigma \in G} \mathrm{Gal}(N/L')^\sigma \tag{1}$$

[FrJ08, p. 464, Lemma 21.5.3]. A standard compactness argument implies that L and L' are Kronecker equivalent if and only if (1) is true for an arbitrary (possibly infinite) Galois extension N of $\mathbb{Q}$ that contains L and L'. So, the problem about the existence of an infinite Kronecker tower can be interpreted as follows:

PROBLEM A: *Does there exist a profinite group G which can be realized as a Galois group over $\mathbb{Q}$ and which has an infinite descending sequence $H_1 > H_2 > H_3 > \cdots$ of open subgroups such that for each n*

$$\bigcup_{\sigma\in G} H_n^\sigma = \bigcup_{\sigma\in G} H_{n+1}^\sigma? \tag{2}$$

Let $H = \bigcap_{n=1}^{\infty} H_n$. Again, a standard compactness argument shows that (2) is equivalent to the condition

$$H_1 \subseteq \bigcup_{\sigma\in G} H^\sigma.$$

Observe that H is a closed subgroup of G of infinite index. So, an affirmative solution to Problem A will imply an affirmative solution to the following one:

PROBLEM B: *Does there exist a profinite group G which has a closed subgroup H of infinite index such that $\bigcup_{\sigma\in G} H^\sigma$ contains an open subgroup U of G?*

This problem appears in the third paragraph of the Notes of [FrJ08, Sec. 21]. Of course, a negative answer to the group theoretic problem B would imply that there is no infinite Kronecker tower. On the other hand, the existence of a profinite group G as in Problem B which can be realized over a number field, implies the existence of a Kronecker tower.

SLICING. Given a group G and a subgroup H we write H^G for the set $\{h^g \mid h \in H \text{ and } g \in G\}$ of all **G-conjugates** (i.e. conjugates within G) of elements of H. In recent years group theorists showed some interest in groups G with proper subgroups H such that $H^G = G$, and in related questions [KLS14].

A well known counting argument shows that if G is a finite group and H is a proper subgroup, then $H^G \subset G$ [FrJ08, p. 238, Lemma 13.3.2]. A standard compactness argument extends this result to every profinite group G and every closed proper subgroup H of G. It is somewhat surprising that there are profinite groups which are union of conjugates of finitely many closed subgroups of infinite index.

To this end we say that a (profinite) group G is **n-sliceable** if there exist (closed) subgroups $H_1, \ldots, H_n$ of G of infinite index such that $G = \bigcup_{i=1}^{n} H_i^G$. In this case we

also say that G **admits an n-slicing**. We say that G is **finitely sliceable** if G is n-sliceable for some positive integer n.

Open subgroups. If U is an open subgroup of a profinite group G, $G = \bigcup_{j=1}^{s} x_j U$, and $H_1, \ldots, H_r$ are closed subgroups of G of infinite index such that $U \subseteq \bigcup_{i=1}^{r} H_i^G$, then $U = \bigcup_{i=1}^{r} \bigcup_{j=1}^{s} (U \cap H_i^{x_j})^U$. Hence, U is finitely sliceable. In particular, this is the case if G, H, and U are as in Problem B.

Arithmetical interpretation. The finite slicing of a profinite group has an arithmetical interpretation similar to the interpretation that infinite Kronecker towers give to the group theoretic situation that appears in Problem B.

Let K be a number field with ring of integers O_K. We say that an n-tuple $(L_1, \ldots, L_n)$ of finite extensions of K in its algebraic closure $\tilde{K}$ is **exhausting** over K if almost every non-zero prime ideal $\mathfrak{p}$ of O_K has a prime divisor of relative degree 1 in O_{L_j} for at least one j between 1 and n.

A sequence $(L_{i1}, \ldots, L_{in})_{i=1,2,3,\ldots}$ of exhausting n-tuples over K is said to be an **n-sliceable infinite Kronecker tower over** K, if $L_{ij} \subseteq L_{i+1,j}$ for all i and j and $L_j = \bigcup_{i=1}^{\infty} L_{ij}$ is an infinite extension of K for all j. Again, a **finitely sliceable infinite Kronecker tower over** K is just an n-sliceable infinite Kronecker tower over K for some positive integer n.

We prove:

Proposition C: *Let N be a Galois extension of a number field K with Galois group G. Then, G is n-sliceable if and only if N contains an n-sliceable infinite Kronecker tower over K (Proposition 5.4).*

Central division algebras. As indicated above, no profinite group is 1-sliceable. However, the Skolem-Noether theorem about division algebras gives a whole family of finitely sliceable profinite groups:

Theorem D: *Let l be a prime number, K a finite extension of $\mathbb{Q}_l$, and D a finite dimensional central division algebra over K. Then, $G = D^\times / K^\times$ is a finitely sliceable profinite group (Theorem 4.2).*

In particular, as indicated above, every open subgroup of $D^\times/K^\times$ with K and D as in Theorem D is finitely sliceable.

Unfortunately, it seems to be unknown whether any of the groups G in the latter theorem can be realized over any number field as a Galois group. If we knew that there are no finitely sliceable infinite Kronecker towers over $\mathbb{Q}$ at all, it would follow from Proposition C and Theorem D that no group $D^\times/K^\times$ as in Theorem D can be realized over $\mathbb{Q}$.

THE GROUPS $\mathrm{GL}_2(\mathbb{Z}_l)$. In contrast to the groups $D^\times/K^\times$ mentioned above, each of the groups $\mathrm{GL}_2(\mathbb{Z}_l)$ appears as a Galois group of a Galois extension of $\mathbb{Q}$. This is proved via Serre's theory of division points of elliptic curves without complex multiplication. Using that $\mathrm{GL}_2(\mathbb{Z}_l)$ is an l-adic analytic group we prove:

THEOREM E: *Let l be an odd prime number. Then, no open subgroup of $\mathrm{GL}_2(\mathbb{Z}_l)$ is finitely sliceable (Theorem 3.10).*

Combining Proposition C with Theorem E for $\mathrm{GL}_2(\mathbb{Z}_l)$ we get:

THEOREM F: *Let N be a Galois extension of $\mathbb{Q}$ with Galois group $\mathrm{GL}_2(\mathbb{Z}_l)$ for some odd prime number l. Then, for each number field K in N, the field N contains no finitely sliceable infinite Kronecker tower over K (Theorem 5.6).*

In light of the latter "negative result", we wonder if there exists a finitely sliceable infinite Kronecker tower over a number field K in a Galois extension N of K.

Finally we complete the information given in Theorem E by proving that $\mathrm{GL}_2(\mathbb{Z}_l)$ admits "infinite slicing":

THEOREM G: *Let l be an odd prime number. Then, $G = \mathrm{GL}_2(\mathbb{Z}_l)$ has an infinite sequence $E_1, E_2, E_3, \ldots$ of closed subgroups of infinite index such that $G = \bigcup_{i=1}^{\infty} E_i^G$ and for all distinct positive integers i, j, the group $E_i \cap E_j$ has an infinite index in both E_i and E_j (Theorem 2.5).*

We use Theorem G (in its detailed form Theorem 2.5) in the proof of Theorem E.

ACKNOWLEDGEMENT: We thank Wulf-Dieter Geyer, Michael Larsen, Andrei Rapinchuk, Aharon Razon, and David Zywina for helpful communications and advice.

1. $\mathrm{GL}_2(\mathbb{Z}_l)$

We introduce for each odd prime number l an infinite family $\mathcal{H}$ of closed subgroups of $\mathrm{GL}_2(\mathbb{Z}_l)$ of infinite index. Then, we prove that each matrix in $\mathrm{GL}_2(\mathbb{Z}_l)$ which is $\mathrm{GL}_2(\mathbb{Z}_l)$-conjugate to elements of two distinct members of $\mathcal{H}$ is a scalar matrix.

We start with our basic notation. We fix an odd prime number l and consider the field $\mathbb{Q}_l$ of l-adic numbers. Let ord_l be the l-adic normalized valuation of $\mathbb{Q}_l$ (in particular, $\mathrm{ord}_l(l) = 1$). The discrete complete valuation ring of ord_l is $\mathbb{Z}_l = \{x \in \mathbb{Q}_l \mid \mathrm{ord}_l(x) \geq 0\}$. We write the elements of the $\mathbb{Z}_l$-module $\mathbb{Z}_l^2$ as columns of height 2 and abbreviate them by bold faced letters. Thus, $\mathbf{a}$ stands for the element $\binom{a_1}{a_2}$ of $\mathbb{Z}_l^2$. Let $M_2(\mathbb{Z}_l)$ be the ring of two by two matrices with entries in $\mathbb{Z}_l$. Then, $\mathrm{GL}_2(\mathbb{Z}_l)$ is the group of invertible matrices in $M_2(\mathbb{Z}_l)$, that is matrices whose determinants belong to $\mathbb{Z}_l^\times$.

Construction 1.1: To each non-square $d \in \mathbb{Z}_l$ we associate a closed subgroup C_d of $\mathrm{GL}_2(\mathbb{Z}_l)$ of infinite index in the following way:

Let $L = \mathbb{Q}_l(\sqrt{d})$ and $S = \mathbb{Z}_l[\sqrt{d}]$. We consider S as a free $\mathbb{Z}_l$-module with the basis $\{1, \sqrt{d}\}$. The group of units $S^\times$ of S acts on S by multiplication from the left. It defines a continuous embedding Φ_d: $S^\times \to \mathrm{GL}_2(\mathbb{Z}_l)$ of groups. Specifically, for each $\lambda = \alpha + \gamma\sqrt{d}$ in $S^\times$ with $\alpha, \gamma \in \mathbb{Z}_l$ let

$$\lambda \cdot 1 = \alpha + \gamma\sqrt{d}$$
$$\lambda \cdot \sqrt{d} = \gamma d + \alpha\sqrt{d}$$

Then,

$$\Phi_d(\lambda) = \begin{pmatrix} \alpha & \gamma \\ \gamma d & \alpha \end{pmatrix}.$$

Note that $\det(\Phi_d(\lambda)) = \alpha^2 - \gamma^2 d = \mathrm{Norm}_{L/\mathbb{Q}_l}\lambda \in \mathbb{Z}_l^\times$ and therefore $\Phi_d(\lambda)$ is indeed in $\mathrm{GL}_2(\mathbb{Z}_l)$. We write C_d for the image of $S^\times$ under Φ_d. Thus,

$$C_d = \Big\{ \begin{pmatrix} \alpha & \gamma \\ \gamma d & \alpha \end{pmatrix} \mid \alpha, \gamma \in \mathbb{Z}_l,\ \alpha^2 - \gamma^2 d \in \mathbb{Z}_l^\times \Big\}.$$

Since C_d is the image of an abelian group, C_d itself is abelian.

Note also that $\text{trace}(\Phi_d(\lambda)) = 2\alpha = \text{trace}_{L/\mathbb{Q}_l}\lambda$. Hence, with $\bar{\lambda} = \alpha - \gamma\sqrt{d}$, the characteristic polynomial of $\Phi_d(\lambda)$ is $X^2 - (\lambda+\bar{\lambda})X + \lambda\bar{\lambda}$, so λ and $\bar{\lambda}$ are the eigenvalues of $\Phi_d(\lambda)$. In particular, if $\lambda \notin \mathbb{Q}_l$, then λ and $\bar{\lambda}$ are distinct.

Suppose that d' is an element of $\mathbb{Z}_l$ such that $L' = \mathbb{Q}_l(\sqrt{d'}) \neq L$. If $A \in C_d \cap C_{d'}$, then each eigenvalue λ of A belongs to $L \cap L' = \mathbb{Q}_l$. Hence, $A = \Phi_d(\lambda) = \left(\begin{smallmatrix}\lambda & 0\\ 0 & \lambda\end{smallmatrix}\right)$. The same conclusion holds if A is an upper triangular matrix in $\text{GL}_2(\mathbb{Z}_l)$ that belongs to C_d. ∎

Notation 1.2: Using the notation of Construction 1.1, we consider for each integer $n \geq 0$ the matrix $\mathbf{l}_n = \left(\begin{smallmatrix} l^{-n} & 0\\ 0 & 1\end{smallmatrix}\right)$ of $\text{GL}_2(\mathbb{Q}_l)$ and the following subgroup of $\text{GL}_2(\mathbb{Z}_l)$:

(1) $$H_{d,n} = \mathbf{l}_n C_d \mathbf{l}_n^{-1} \cap \text{GL}_2(\mathbb{Z}_l) = \left\{ \begin{pmatrix} \alpha & \gamma \\ l^{2n}\gamma d & \alpha \end{pmatrix} \;\middle|\; \alpha, \gamma \in \mathbb{Z}_l \text{ and } \alpha^2 - l^{2n}\gamma^2 d \in \mathbb{Z}_l^\times \right\}.$$

Note that $H_{d,n} = C_{l^{2n}d}$ for all $n \geq 0$. Also note that $H_{d,0} = C_d$ and $H_{d,n} = \left\{ \left(\begin{smallmatrix}\alpha & \gamma\\ l^{2n}\gamma d & \alpha\end{smallmatrix}\right) \;\middle|\; \alpha \in \mathbb{Z}_l^\times \text{ and } \gamma \in \mathbb{Z}_l \right\}$ for $n \geq 1$. ∎

Remark 1.3: The union of all conjugates of a subgroup. Let H be a closed subgroup of a profinite group G. Then, $H^G = \{h^g \mid h \in H,\ g \in G\}$ is the image of the continuous map $\varphi\colon H \times G \to G$ given by $\varphi(h,g) = g^{-1}hg$. Since both groups involved are compact and Hausdorff, H^G is closed. ∎

We set $Z = \left\{ \left(\begin{smallmatrix} u & 0\\ 0 & u\end{smallmatrix}\right) \;\middle|\; u \in \mathbb{Z}_l^\times \right\}$ for the center of $\text{GL}_2(\mathbb{Z}_l)$.

LEMMA 1.4: *Let d be a non-square element of $\mathbb{Z}_l$ and set $G = \text{GL}_2(\mathbb{Z}_l)$. Then, $H_{d,i}^G \cap H_{d,j}^G = Z$ for all distinct non-negative integers i, j.*

Proof: Taking $\gamma = 0$ in (1), we find that Z is a subgroup of $H_{d,i}$ for each $i \geq 0$. Hence, it suffices to prove that $(H_{d,i}^G \cap H_{d,j}^G) \smallsetminus Z = \emptyset$.

To this end we consider distinct non-negative integers i, j and let $\mathbf{a} = \left(\begin{smallmatrix}\alpha & \gamma\\ l^{2i}\gamma d & \alpha\end{smallmatrix}\right)$ and $\mathbf{c} = \left(\begin{smallmatrix}\beta & \delta\\ l^{2j}\delta d & \beta\end{smallmatrix}\right)$ be matrices in $H_{d,i}$ and $H_{d,j}$, respectively. We assume toward contradiction that

(2) $\mathbf{a}$ and $\mathbf{c}$ are conjugate in G and $\gamma \neq 0$.

In particular, $2\alpha = \text{trace}(\mathbf{a}) = \text{trace}(\mathbf{c}) = 2\beta$, so $\alpha = \beta$. Also, $\alpha^2 - l^{2i}\gamma^2 d = \det(\mathbf{a}) = \det(\mathbf{c}) = \alpha^2 - l^{2j}\delta^2 d$, so $l^{2i}\gamma^2 = l^{2j}\delta^2$. Hence,

(3) $$l^i\gamma = \pm l^j\delta.$$

By (2), there exists a matrix $\mathbf{q} = \left(\begin{smallmatrix} q & r \\ s & t \end{smallmatrix}\right) \in G$ such that

$$\mathbf{qa} = \mathbf{cq}. \tag{4}$$

Hence,

$$rl^{2i}\gamma d = \delta s \quad \text{and} \quad tl^{2i}\gamma d = l^{2j}\delta dq. \tag{5}$$

Using (3), we replace $l^i\gamma$ by $\pm l^j\delta$ in (5) and get

$$s = \pm rl^{i+j}d \quad \text{and} \quad tl^i = \pm l^j q. \tag{6}$$

Since $i \neq j$, one of the non-negative integers i and j is positive. Hence, by the left equality of (6), $s \notin \mathbb{Z}_l^\times$. Since $\left(\begin{smallmatrix} q & r \\ s & t \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}_l)$, we must have $q, t \in \mathbb{Z}_l^\times$. It follows from the right equality of (6) that $i = j$, in contrast to our assumption. ∎

We fix a root of unity ζ of order $l-1$ in $\mathbb{Q}_l$.

LEMMA 1.5: *Let S be the ring of integers of a quadratic extension L of $\mathbb{Q}_l$. Then $L = \mathbb{Q}_l(\sqrt{d})$ and $S = \mathbb{Z}_l[\sqrt{d}]$, where d is one of the elements l, ζ, or $l\zeta$.*

Proof: The multiplicative group $\mathbb{Q}_l^\times$ has a direct factorization $\mathbb{Q}_l^\times = \langle l \rangle \times \langle \zeta \rangle \times U_1$, where $\langle l \rangle = \{l^n \mid n \in \mathbb{Z}\} \cong \mathbb{Z}$, $\langle \zeta \rangle$ is the set of all roots of unity in $\mathbb{Q}_l^\times$, and $U_1 = 1 + l\mathbb{Z}_l$. [Koc70, p. 78]. In particular, ζ is not a square in $\mathbb{Q}_l^\times$. Since $l \neq 2$, Hensel's lemma implies that each of the elements of U_1 is a square in $\mathbb{Q}_l$. Also, l, ζ are multiplicatively independent modulo $(\mathbb{Q}_l^\times)^2$, otherwise $l\zeta = x^2$ for some $x \in \mathbb{Q}_l$, so $1 = \mathrm{ord}_l(l\zeta) = 2\mathrm{ord}_l(x)$, which is a contradiction.

Hence, $l, \zeta, l\zeta$ represent the cosets of $\mathbb{Q}_l^\times$ modulo the subgroup of squares. By Kummer's theory, L is one of the fields $\mathbb{Q}_l(\sqrt{l})$, $\mathbb{Q}_l(\sqrt{\zeta})$, or $\mathbb{Q}_l(\sqrt{l\zeta})$. In the first case $S = \mathbb{Z}_l[\sqrt{l}]$ [CaF67, p. 23, Thm. 1(ii)]. In the second case $g(X) = \mathrm{irr}(\sqrt{\zeta}, \mathbb{Q}_l) = X^2 - \zeta$ and $N_{L/\mathbb{Q}_l} g'(\sqrt{\zeta}) = -4\zeta$ is a unit of $\mathbb{Z}_l$. Hence, $S = \mathbb{Z}_l[\sqrt{\zeta}]$ [FrJ08, p. 109, Lemma 6.1.2]. In the third case $S = \mathbb{Z}_l[\sqrt{l\zeta}]$, similar to the first case. ∎

Notation 1.6: We denote the group of all upper triangular matrices in $\mathrm{GL}_2(\mathbb{Z}_l)$ by B. We note that $(\mathrm{GL}_2(\mathbb{Z}_l) : B) = \infty$ and $Z \leq B$. Then, we set $\mathcal{H} = \{H_{d,i} \mid d \in \{l, \zeta, l\zeta\},\ i \in \{0, 1, 2, \ldots\}\} \cup \{B\}$. ∎

LEMMA 1.7: *Let a_1 and a_2 be relatively prime elements of $\mathbb{Z}_l$. Then there exist $b_1, b_2 \in \mathbb{Z}_l$ such that $\binom{a_1}{a_2}$ and $\binom{b_1}{b_2}$ generate $\mathbb{Z}_l^2$.*

Proof: The ideal generated by a_1 and a_2 is $\mathbb{Z}_l$. In particular, there exist $b_1, b_2 \in \mathbb{Z}_l$ such that $a_1b_2 - a_2b_1 = 1$. Hence, $\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_l)$. We conclude from Cramer's rule that $\binom{a_1}{a_2}$ and $\binom{b_1}{b_2}$ generate $\mathbb{Z}_l^2$. ∎

LEMMA 1.8: *The eigenvalues of the matrices in B belong to $\mathbb{Z}_l^\times$. Conversely, if the eigenvalues λ_1, λ_2 of a matrix $\mathbf{a} \in \mathrm{GL}_2(\mathbb{Z}_l)$ belong to $\mathbb{Q}_l$, then $\mathbf{a}$ is $\mathrm{GL}_2(\mathbb{Z}_l)$-conjugate to a matrix in B.*

Proof: By definition, each matrix $\mathbf{a}$ in B has the form $\left(\begin{smallmatrix} \alpha & \beta \\ 0 & \delta \end{smallmatrix}\right)$ with $\alpha, \beta, \delta \in \mathbb{Z}_l$ and $\alpha\delta = \det(\mathbf{a}) \in \mathbb{Z}_l^\times$. It follows that the eigenvalues α and δ of $\mathbf{a}$ belong to $\mathbb{Z}_l^\times$.

Conversely, we consider a matrix $\mathbf{a} \in \mathrm{GL}_2(\mathbb{Z}_l)$ with eigenvalues $\lambda_1, \lambda_2 \in \mathbb{Q}_l$. These eigenvalues are the roots of the characteristic polynomial $X^2 - \mathrm{tr}(\mathbf{a})X + \det(\mathbf{a})$ whose coefficients belong to $\mathbb{Z}_l$. Since $\mathbb{Z}_l$ is integrally closed, $\lambda_1, \lambda_2 \in \mathbb{Z}_l$. Let $\mathbf{x}_1 = \binom{x_{11}}{x_{12}} \in \mathbb{Q}_l^2$ be an eigenvector of $\mathbf{a}$ that belongs to λ_1:

$$\mathbf{a}\mathbf{x}_1 = \lambda_1\mathbf{x}_1.$$

We multiply $\mathbf{x}_1$ by an appropriate power of l, if necessary, to assume that x_{11}, x_{12} are relatively prime elements of $\mathbb{Z}_l$. By Lemma 1.7, there exists $\mathbf{x}_2 \in \mathbb{Z}_l^2$ such that $\mathbf{x}_1, \mathbf{x}_2$ generate $\mathbb{Z}_l^2$. In particular, there exist $\gamma, \delta \in \mathbb{Z}_l$ such that

$$\mathbf{a}\mathbf{x}_2 = \gamma\mathbf{x}_1 + \delta\mathbf{x}_2.$$

Hence, $\mathbf{x} = (\mathbf{x}_1\ \mathbf{x}_2) \in \mathrm{GL}_2(\mathbb{Z}_l)$ and $\mathbf{a}\mathbf{x} = \mathbf{x}\left(\begin{smallmatrix} \lambda_1 & \gamma \\ 0 & \delta \end{smallmatrix}\right)$, so $\mathbf{x}^{-1}\mathbf{a}\mathbf{x} = \left(\begin{smallmatrix} \lambda_1 & \gamma \\ 0 & \delta \end{smallmatrix}\right) \in B$.

Note that the latter equality implies also that the characteristic polynomial of $\mathbf{a}$ is $(X-\lambda_1)(X-\delta)$. Since that polynomial is also equals to $(X-\lambda_1)(X-\lambda_2)$, we deduce that $\delta = \lambda_2$. ∎

LEMMA 1.9: *Let $G = \mathrm{GL}_2(\mathbb{Z}_l)$. If H and H' are distinct groups in $\mathcal{H}$, then $H^G \cap (H')^G = Z$.*

Proof: The case where $H = H_{d,i}$ and $H' = H_{d,j}$ with $d \in \{l, \zeta, l\zeta\}$ and $i \neq j$ is proved in Lemma 1.4.

Assume toward contradiction that d, d' are distinct elements of the set $\{l, \zeta, l\zeta\}$, i, j are non-negative integers, and there exists $\mathbf{a} \in H^G_{d,i} \cap H^G_{d',j} \smallsetminus Z$. Then, $\mathbf{a}$ is $\mathrm{GL}_2(\mathbb{Q}_l)$-conjugate to an element $\mathbf{b}$ of $C_d \smallsetminus Z$. By Construction 1.1, each eigenvalue λ of $\mathbf{b}$, hence of $\mathbf{a}$, lies in $\mathbb{Q}_l(\sqrt{d}) \smallsetminus \mathbb{Q}_l$. Similarly, $\lambda \in \mathbb{Q}_l(\sqrt{d'})$. This contradicts the fact that $\mathbb{Q}_l(\sqrt{d}) \cap \mathbb{Q}(\sqrt{d'}) = \mathbb{Q}_l$.

Finally, assume that $\mathbf{a} \in H^G_{d,i} \cap B^G \smallsetminus Z$ where $d \in \{l, \zeta, l\zeta\}$ and $i \geq 0$ is an integer. Then, $\mathbf{a}$ is conjugate in $\mathrm{GL}_2(\mathbb{Q}_l)$ to an element of $C_d \smallsetminus Z$. Hence, by Construction 1.1, the eigenvalues of A do not belong to $\mathbb{Q}_l$. On the other hand, $\mathbf{a}$ is conjugate to an element of B, so the eigenvalues of $\mathbf{a}$ are in $\mathbb{Q}_l$ (Lemma 1.8). This is a contradiction. ∎

2. $\mathrm{GL}_2(\mathbb{Z}_l)$-Conjugacy versus $\mathrm{GL}_2(\mathbb{Q}_l)$-Conjugacy

We fix for the whole section an odd prime number l, a root of unity ζ of order $l-1$ in $\mathbb{Z}_l$, and an element d of the set $\{l, \zeta, l\zeta\}$. Thus, $\mathrm{ord}_l(d) = 0$ or $\mathrm{ord}_l(d) = 1$. Using Notation 1.6, we prove a detailed version of Theorem G, namely that $\mathrm{GL}_2(\mathbb{Z}_l) = \bigcup_{H\in\mathcal{H}} H^G$ is an infinite slicing of $G = \mathrm{GL}_2(\mathbb{Z}_l)$.

LEMMA 2.1: *Let l and d be as above and let $\mathbf{a}$ be a matrix in $\mathrm{GL}_2(\mathbb{Z}_l)$ with an eigenvalue $\lambda \in \mathbb{Q}_l(\sqrt{d}) \smallsetminus \mathbb{Q}_l$. Then, $\lambda = \alpha+\gamma\sqrt{d}$ with $\alpha, \gamma \in \mathbb{Z}_l$ and $\gamma \neq 0$. Moreover, $\mathbf{a}$ is $\mathrm{GL}_2(\mathbb{Q}_l)$-conjugate to the matrix $\mathbf{a}' = \left(\begin{smallmatrix} \alpha & \gamma \\ \gamma d & \alpha \end{smallmatrix}\right)$ of $\mathrm{GL}_2(\mathbb{Z}_l)$.*

Proof: The eigenvalue λ is a root of the characteristic polynomial $X^2 - \mathrm{trace}(\mathbf{a})X + \det(\mathbf{a})$. The latter is monic with coefficients in $\mathbb{Z}_l$. Hence, λ is integral over $\mathbb{Z}_l$. By assumption $\lambda \notin \mathbb{Q}_l$, so $[\mathbb{Q}_l(\lambda) : \mathbb{Q}_l] = 2$. It follows from Lemma 1.5 that $\lambda = \alpha + \gamma\sqrt{d}$ with $\alpha, \gamma \in \mathbb{Z}_l$. Moreover, $\gamma \neq 0$ because $\lambda \notin \mathbb{Q}_l$. Note that $\bar{\lambda} = \alpha - \gamma\sqrt{d}$ is the other eigenvalue of $\mathbf{a}$. Like λ, we have $\bar{\lambda} \notin \mathbb{Q}_l$.

We consider each element of $\mathbb{Q}_l(\sqrt{d})^2$ as a column of height 2. Let $\mathbf{v} \in \mathbb{Q}_l(\sqrt{d})^2$ be an eigenvector of $\mathbf{a}$ that belongs to λ:

$$\mathbf{a}\mathbf{v} = \lambda\mathbf{v}. \tag{1}$$

Write $\mathbf{v} = \mathbf{v}_0+\sqrt{d}\cdot\mathbf{v}_1$ with $\mathbf{v}_0, \mathbf{v}_1 \in \mathbb{Q}_l^2$. By (1), $\mathbf{a}(\mathbf{v}_0+\sqrt{d}\cdot\mathbf{v}_1) = (\alpha+\gamma\sqrt{d})(\mathbf{v}_0+\sqrt{d}\cdot\mathbf{v}_1)$, which may be written as

$$\begin{aligned} \mathbf{a}\mathbf{v}_0 &= \alpha\mathbf{v}_0 + \gamma d\mathbf{v}_1 \\ \mathbf{a}\mathbf{v}_1 &= \gamma\mathbf{v}_0 + \alpha\mathbf{v}_1. \end{aligned} \tag{2}$$

Note that $\mathbf{v}_0$ and $\mathbf{v}_1$ are linearly independent over $\mathbb{Q}_l$, since otherwise each of the equalities in (2) will give an eigenvalue for $\mathbf{a}$ that belongs to $\mathbb{Q}_l$. Thus, $(\mathbf{v}_0\ \mathbf{v}_1) \in \mathrm{GL}_2(\mathbb{Q}_l)$. By (2), $\mathbf{a}(\mathbf{v}_0\ \mathbf{v}_1) = (\mathbf{v}_0\ \mathbf{v}_1)\left(\begin{smallmatrix} \alpha & \gamma \\ \gamma d & \alpha \end{smallmatrix}\right)$. Hence, $\mathbf{a}$ is $\mathrm{GL}_2(\mathbb{Q}_l)$-conjugate to the matrix $\mathbf{a}'$. Since $\det(\mathbf{a}') = \det(\mathbf{a}) \in \mathbb{Z}_l^\times$, the matrix $\mathbf{a}'$ lies in $\mathrm{GL}_2(\mathbb{Z}_l)$. Indeed, $\mathbf{a}' \in C_d$. ∎

We compute the structure of the centralizer $C_{\mathbf{a}'}$ of $\mathbf{a}'$ in $\mathrm{GL}_2(\mathbb{Q}_l)$ and prove that each double coset $\mathrm{GL}_2(\mathbb{Z}_l)\mathbf{x}C_{\mathbf{a}'}$ with $\mathbf{x} \in \mathrm{GL}_2(\mathbb{Q}_l)$ contains a matrix of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & l^n \end{smallmatrix}\right)$

with $n \geq 0$. We use the latter matrix to prove that $\mathbf{a}$ is $\mathrm{GL}_2(\mathbb{Z}_l)$-conjugate to an element of $C_{d,n}$.

LEMMA 2.2: *In the notation of Lemma 2.1, the centralizer $C_{\mathbf{a}'}$ of $\mathbf{a}'$ in $\mathrm{GL}_2(\mathbb{Q}_l)$ consists of all matrices of the form $\left(\begin{smallmatrix} q & r \\ rd & q \end{smallmatrix}\right)$ with $q, r \in \mathbb{Q}_l$ not both zero.*

Proof: Indeed, a matrix $\left(\begin{smallmatrix} q & r \\ s & t \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbb{Q}_l)$ belongs to $C_{\mathbf{a}'}$ if and only if $\left(\begin{smallmatrix} q & r \\ s & t \end{smallmatrix}\right)\left(\begin{smallmatrix} \alpha & \gamma \\ \gamma d & \alpha \end{smallmatrix}\right) = \left(\begin{smallmatrix} \alpha & \gamma \\ \gamma d & \alpha \end{smallmatrix}\right)\left(\begin{smallmatrix} q & r \\ s & t \end{smallmatrix}\right)$. This happens if and only if $q\alpha + r\gamma d = \alpha q + \gamma s$, $q\gamma + r\alpha = \alpha r + \gamma t$, $s\alpha + t\gamma d = \gamma dq + \alpha s$, and $s\gamma + t\alpha = \gamma dr + \alpha t$. Since $\gamma, d \neq 0$, the latter condition is equivalent to $t = q$ and $s = rd$, as claimed. ∎

LEMMA 2.3: *In the notation of Lemma 2.2, every double coset $\mathrm{GL}_2(\mathbb{Z}_l)\mathbf{x}C_{\mathbf{a}'}$ in $\mathrm{GL}_2(\mathbb{Q}_l)$ contains a matrix of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & l^n \end{smallmatrix}\right)$ with a non-negative integer n.*

Proof: Let $\mathbf{x} \in \mathrm{GL}_2(\mathbb{Q}_l)$. We multiply $\mathbf{x}$ from the left by matrices belonging to $\mathrm{GL}_2(\mathbb{Z}_l)$ and from the right by matrices belonging to $C_{\mathbf{a}'}$ in order to get a matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & l^n \end{smallmatrix}\right)$ with $n \geq 0$.

The multiplication of $\mathbf{x} = \left(\begin{smallmatrix} x_{00} & x_{10} \\ x_{01} & x_{11} \end{smallmatrix}\right)$ from the left by elements of $\mathrm{GL}_2(\mathbb{Z}_l)$ can be achieved successively by the following operations:

(3a) The product of a row of $\mathbf{x}$ by a unit of $\mathbb{Z}_l$.

(3b) Exchange of the rows of $\mathbf{x}$.

(3c) Addition of a row of $\mathbf{x}$ multiplied by an element κ of $\mathbb{Z}_l$ to the other row.

Indeed, if $u \in \mathbb{Z}_l^\times$, then $\left(\begin{smallmatrix} u & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} x_{00} & x_{10} \\ x_{01} & x_{11} \end{smallmatrix}\right) = \left(\begin{smallmatrix} ux_{00} & ux_{10} \\ x_{01} & x_{11} \end{smallmatrix}\right)$. Also, $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} x_{00} & x_{10} \\ x_{01} & x_{11} \end{smallmatrix}\right) = \left(\begin{smallmatrix} x_{01} & x_{11} \\ x_{00} & x_{10} \end{smallmatrix}\right)$. Finally, $\left(\begin{smallmatrix} 1 & 0 \\ \kappa & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} x_{00} & x_{10} \\ x_{01} & x_{11} \end{smallmatrix}\right) = \left(\begin{smallmatrix} x_{00} & x_{10} \\ \kappa x_{00} + x_{01} & \kappa x_{10} + x_{11} \end{smallmatrix}\right)$.

CLAIM A: *The double coset $\mathrm{GL}_2(\mathbb{Z}_l)\mathbf{x}C_{\mathbf{a}'}$ contains a matrix $\left(\begin{smallmatrix} l^i & q \\ 0 & l^j \end{smallmatrix}\right)$ with $i, j \in \mathbb{Z}$ and $q \in \mathbb{Q}_l$.* Indeed, if $x_{00}, x_{01} \neq 0$, we write $x_{00} = ul^i$ and $x_{01} = vl^k$ with $u, v \in \mathbb{Z}_l^\times$ and $i, k \in \mathbb{Z}$. Exchanging the rows, if necessary, we may assume that $i \leq k$. Then, we add the first row of $\mathbf{x}$ multiplied by $-u^{-1}vl^{k-i}$ to the second row to make x_{01} zero. Then, we multiply each of the rows by an element of $\mathbb{Z}_l^\times$ in order to bring $\mathbf{x}$ to the form $\left(\begin{smallmatrix} l^i & q \\ 0 & l^j \end{smallmatrix}\right)$ with $i, j \in \mathbb{Z}$ and $q \in \mathbb{Q}_l$, as claimed.

CLAIM B: *The double coset $\mathrm{GL}_2(\mathbb{Z}_l)\mathbf{x}C_{\mathbf{a}'}$ contains a matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & l^m \end{smallmatrix}\right)$ for some integer m.* Indeed, by Part A, we may assume that $\mathbf{x} = \left(\begin{smallmatrix} l^i & q \\ 0 & l^j \end{smallmatrix}\right)$ with $i, j \in \mathbb{Z}$ and $q \in \mathbb{Q}_l$.

If $q = 0$, we may multiply $\left(\begin{smallmatrix} l^i & 0 \\ 0 & l^j \end{smallmatrix}\right)$ from the right by the matrix $\left(\begin{smallmatrix} l^{-i} & 0 \\ 0 & l^{-i} \end{smallmatrix}\right)$ of $C_{\mathbf{a}'}$ and get the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & l^{j-i} \end{smallmatrix}\right)$ that has the desired form.

We therefore assume that $q \neq 0$ and write $q = ul^k$ with $k \in \mathbb{Z}$ and $u \in \mathbb{Z}_l^\times$. If $k \geq j$, we multiply the second row of $\mathbf{x}$ by $-ul^{k-j}$ and add to the first row in order to get $\left(\begin{smallmatrix} l^i & 0 \\ 0 & l^j \end{smallmatrix}\right)$. Then, we apply the operation of the preceding paragraph.

We may therefore assume that

(4) $\mathbf{x} = \left(\begin{smallmatrix} l^i & q \\ 0 & l^j \end{smallmatrix}\right)$ with $q = ul^k$, $k < j$, and $u \in \mathbb{Z}_l^\times$. Thus, $\mathrm{ord}_l(q) < \mathrm{ord}_l(l^j)$.

In this case we consider the matrix $\mathbf{z} = \left(\begin{smallmatrix} 1 & -l^{-i}q \\ -l^{-i}qd & 1 \end{smallmatrix}\right)$ of $C_{\mathbf{a}'}$ (Lemma 2.2). Then, $\mathbf{x}' = \left(\begin{smallmatrix} l^i - l^{-i}q^2d & 0 \\ -l^{j-i}qd & l^j \end{smallmatrix}\right) = \mathbf{xz}$ is in the same double coset as $\mathbf{x}$.

Now we claim that

$$\mathrm{ord}_l(l^{2i} - q^2d) = \min(\mathrm{ord}_l(l^{2i}), \mathrm{ord}_l(q^2d)). \tag{5}$$

Indeed, this is the case if $\mathrm{ord}_l(d) = 1$, because then $\mathrm{ord}_l(q^2d)$ is odd while $\mathrm{ord}_l(l^{2i})$ is even. Thus, the two orders are distinct and we may apply the basic rules of valuations to conclude (5).

The other possibility is $\mathrm{ord}_l(d) = 0$. In this case we write again $q = ul^k$ as in (4). If (5) is not an equality, then by the basic rules of valuations, $\mathrm{ord}_l(l^{2i}) = \mathrm{ord}_l(q^2d)$ and the left hand side of (5) is greater than its right hand side. The first condition implies that $i = k$. Then, the second one implies that $\mathrm{ord}_l(l^{2i} - u^2l^{2i}d) > \mathrm{ord}_l(l^{2i})$, so $\mathrm{ord}_l(1 - u^2d) > 0$. Since $l \neq 2$, Hensel's lemma implies that d is a square in $\mathbb{Q}_l$, in contrast to our assumption. This concludes the proof of (5).

It follows from (5) that

$$\begin{aligned} \mathrm{ord}_l(l^i - l^{-i}q^2d) &= -i + \mathrm{ord}_l(l^{2i} - q^2d) \\ &= -i + \min(2i, \mathrm{ord}_l(qqd)) \\ &\leq -i + \min(2i, \mathrm{ord}_l(l^jqd)) \qquad \text{(by (4))} \\ &\leq \mathrm{ord}_l(l^{j-i}qd). \end{aligned}$$

Thus, $\mathbf{x}' = \left(\begin{smallmatrix} u'l^r & 0 \\ v'l^s & l^j \end{smallmatrix}\right)$ with $u', v' \in \mathbb{Z}_l^\times$ and integers $r \leq s$. Adding the first row multiplied by $-(u')^{-1}v'l^{s-r}$ to the second row, we obtain a matrix $\mathbf{x}'' = \left(\begin{smallmatrix} u'l^r & 0 \\ 0 & l^j \end{smallmatrix}\right)$ in the same

double coset as $\mathbf{x}'$. Then, we multiply the first row by $(u')^{-1}$ and multiply the resulting matrix from the right by $\left(\begin{smallmatrix} l^{-r} & 1 \\ 0 & l^{-r} \end{smallmatrix}\right)$ to get $\left(\begin{smallmatrix} 1 & 0 \\ 0 & l^{j-r} \end{smallmatrix}\right)$ as required by Claim B.

If $j-r \geq 0$, we are done. Otherwise, we still have to apply the next claim in order to achieve the desired conclusion.

CLAIM C: *Every double coset* $\mathrm{GL}_2(\mathbb{Z}_l)\left(\begin{smallmatrix} 1 & 0 \\ 0 & l^{-i} \end{smallmatrix}\right)C_{\mathbf{a}'}$ *with a positive integer* i *contains a matrix* $\left(\begin{smallmatrix} 1 & 0 \\ 0 & l^{n} \end{smallmatrix}\right)$ *for some non-negative integer* n.

First assume that $\mathrm{ord}_l(d) = 0$. Then, $\det\left(\begin{smallmatrix} 1 & 1 \\ d & l^{2i} \end{smallmatrix}\right) = l^{2i} - d \in \mathbb{Z}_l^{\times}$, so $\left(\begin{smallmatrix} 1 & 1 \\ d & l^{2i} \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}_l)$. By Lemma 2.2, $\left(\begin{smallmatrix} 1 & l^{-i} \\ l^{-i}d & 1 \end{smallmatrix}\right) \in C_{\mathbf{a}'}$. Now, observe that

$$\begin{pmatrix} 1 & 1 \\ d & l^{2i} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & l^{-i} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & l^{i} \end{pmatrix}\begin{pmatrix} 1 & l^{-i} \\ l^{-i}d & 1 \end{pmatrix},$$

which implies

$$\begin{pmatrix} 1 & 0 \\ 0 & l^{i} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ d & l^{2i} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & l^{-i} \end{pmatrix}\begin{pmatrix} 1 & l^{-i} \\ l^{-i}d & 1 \end{pmatrix}^{-1}$$

and gives the desired conclusion.

The other case is that $\mathrm{ord}_l(d) = 1$. Then, $l^{-1}d \in \mathbb{Z}_l^{\times}$ and $2i - 1 \geq 1$, so $\det\left(\begin{smallmatrix} 1 & 1 \\ l^{-1}d & l^{2i-1} \end{smallmatrix}\right) = l^{2i-1} - l^{-1}d \in \mathbb{Z}_l^{\times}$. In addition,

$$\begin{pmatrix} 1 & 1 \\ l^{-1}d & l^{2i-1} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & l^{-i} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & l^{i-1} \end{pmatrix}\begin{pmatrix} 1 & l^{-i} \\ l^{-i}d & 1 \end{pmatrix}.$$

Since $i - 1 \geq 0$, we get the desired conclusion as in the preceding paragraph. ∎

We complete Lemma 1.9 with the following result:

LEMMA 2.4: *Let* $\mathbf{a}$ *be a matrix in* $\mathrm{GL}_2(\mathbb{Z}_l)$ *with an eigenvalue* $\lambda \notin \mathbb{Q}_l$. *Then,* $\mathbf{a}$ *is* $\mathrm{GL}_2(\mathbb{Z}_l)$*-conjugate to a matrix that lies in one of the groups* $H_{d,n}$ *(Notation 1.2) with* $d \in \{l, \zeta, l\zeta\}$ *and* $n \in \{0, 1, 2, \ldots\}$.

Proof: Lemma 2.1 gives a matrix $\mathbf{a}' = \left(\begin{smallmatrix} \alpha & \gamma \\ \gamma d & \alpha \end{smallmatrix}\right)$ in C_d for some $d \in \{l, \zeta, l\zeta\}$ and a matrix $\mathbf{x} \in \mathrm{GL}_2(\mathbb{Q}_l)$ such that $\mathbf{x}\mathbf{a}'\mathbf{x}^{-1} = \mathbf{a}$. Lemma 2.3 produces a matrix $\mathbf{g} \in \mathrm{GL}_2(\mathbb{Z}_l)$, a matrix $\mathbf{z} \in \mathrm{GL}_2(\mathbb{Q}_l)$ that commutes with $\mathbf{a}'$, and a non-negative integer n such that $\mathbf{x} = \mathbf{g}\left(\begin{smallmatrix} 1 & 0 \\ 0 & l^{n} \end{smallmatrix}\right)\mathbf{z}$. It follows that

$$\mathbf{a} = \mathbf{g}\begin{pmatrix} 1 & 0 \\ 0 & l^{n} \end{pmatrix}\mathbf{a}'\begin{pmatrix} 1 & 0 \\ 0 & l^{-n} \end{pmatrix}\mathbf{g}^{-1}. \tag{6}$$

Now, taking into account that $\left(\begin{smallmatrix} l^n & 0 \\ 0 & l^n \end{smallmatrix}\right)$ lies in the center of $\mathrm{GL}_2(\mathbb{Z}_l)$, we use the identity $\left(\begin{smallmatrix} 1 & 0 \\ 0 & l^n \end{smallmatrix}\right) = \left(\begin{smallmatrix} l^{-n} & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} l^n & 0 \\ 0 & l^n \end{smallmatrix}\right)$ to rewrite (6) as

$$\mathbf{g}^{-1}\mathbf{a}\mathbf{g} = \begin{pmatrix} l^{-n} & 0 \\ 0 & 1 \end{pmatrix} \mathbf{a}' \begin{pmatrix} l^n & 0 \\ 0 & 1 \end{pmatrix}. \tag{7}$$

The left hand side of (7) belongs to $\mathrm{GL}_2(\mathbb{Z}_l)$, while its right hand side is in $\mathbf{l}_n C_d \mathbf{l}_n^{-1}$. By Notation 1.2, $\mathbf{g}^{-1}\mathbf{a}\mathbf{g} \in H_{d,n}$, as desired. ∎

Finally, we combine Lemmas 1.8, 2.4, and Lemma 1.9:

THEOREM 2.5: *Let l be an odd prime, ζ a root of unity of order $l-1$ in $\mathbb{Z}_l$, and $H_{d,n}$ as in Notation 1.2. Then, with $G = \mathrm{GL}_2(\mathbb{Z}_l)$,*

$$\mathrm{GL}_2(\mathbb{Z}_l) = B^G \cup \bigcup_{d\in\{l,\zeta,l\zeta\}} \bigcup_{n=0}^{\infty} H_{d,n}^G \tag{8}$$

and $H^G \cap (H')^G = Z$ for all distinct groups $H, H' \in \mathcal{H}$ (Notation 1.6).

Proof: By Lemma 1.8, the eigenvalues of a matrix $\mathbf{a}$ in $\mathrm{GL}_2(\mathbb{Z}_l)$ belong to $\mathbb{Q}_l$ if and only if $\mathbf{a} \in B^G$. If the eigenvalues of $\mathbf{a}$ do not belong to $\mathbb{Q}_l$, then by Lemma 2.4, $\mathbf{a} \in \bigcup_{d\in\{l,\zeta,l\zeta\}} \bigcup_{n=0}^{\infty} H_{d,n}^G$, as claimed. ∎

3. Closed subgroups of $\mathrm{GL}_2(\mathbb{Z}_l)$

We prove for an odd prime number l that no open subgroup of $\mathrm{GL}_2(\mathbb{Z}_l)$ admits a finite slicing. Our proof relies on the theory of l-adic analytic groups and its relation to the theory of l-adic Lie algebras. We summarize the facts about these groups and algebras that we use for the benefit of our audience, especially for the field arithmeticians.

Remark 3.1: Dimension. Let G be an **l-adic analytic group** [DDMS99, p. 183, Def. 8.8] of **dimension** d. Thus, d is a non-negative integer such that G is covered by l-adically open subsets U_i, $i \in I$ (called **charts**), each of which is homeomorphic to an open subset of $\mathbb{Z}_l^d$ [DDMS99, p. 201, Thm. 8.36].

We use the following facts on l-adic analytic groups and their dimensions:

(1a) $\mathrm{GL}_n(\mathbb{Q}_l)$ is an l-adic analytic group [DDMS99, p. 188, Examples 8.17(iv)].

(1b) Every closed subgroup H of an l-adic analytic group G is l-adic analytic and every quotient G/N, where N is a closed normal subgroup is l-adic analytic [DDMS99, p. 220, Thm. 9.6].

(1c) Since the l-adic topology of each $\mathbb{Z}_l^d$ is Hausdorff and totally disconnected, so is the l-adic topology of G. If in addition, G is compact in the l-adic topology, then G is profinite [RiZ00, p. 11, Thm. 1.1.12] and the topology induced on G by its structure as a profinite group coincides with its l-adic topology. In the notation of (1b) we then have, $\dim(G) = \dim(N) + \dim(G/N)$ [DDMS99, p. 204, Exer. 4]. The leading example for a profinite group in this context is $\mathrm{GL}_2(\mathbb{Z}_l) = \varprojlim \mathrm{GL}_2(\mathbb{Z}/l^n\mathbb{Z})$.

∎

Remark 3.2: l-adic Lie algebras. Recall that a $\mathbb{Q}_l$-algebra L with a product of two elements x, y denoted by $[x, y]$ is called an **l-adic Lie algebra** if the bracket multiplication satisfies $[x, x] = 0$ for each $x \in L$ and the Jacobi identity [Ser92, p. 2, Def. 1]. There is a functor from the category of l-adic analytic groups to the category of l-adic Lie algebras that assigns to each l-adic analytic group G an l-adic Lie algebra $\mathcal{L}(G)$ and to each morphism f between l-adic analytic groups a morphism f^* of the corresponding l-adic Lie algebras. That functor satisfies the following conditions for l-adic analytic groups and Lie algebras of finite dimensions:

(2a) $\dim(G) = \dim(\mathcal{L}(G))$ [DDMS99, p. 229, Thm. 9.11].

(2b) Let f_1, f_2: $G \to H$ be morphisms of l-adic analytic groups and let f_i^*: $\mathcal{L}(G) \to \mathcal{L}(H)$, $i = 1, 2$, be the morphisms of the corresponding algebras. Then, $f_1^* = f_2^*$ if and only if G has an open subgroup G_0 such that $f_1|_{G_0} = f_2|_{G_0}$ [DDMS99, p. 229, Thm. 9.11(ii)].

Here are some consequences of the rule (2) for a given l-adic analytic group G of finite dimension:

(3a) If G_1, G_2 are closed subgroups of G, then $\mathcal{L}(G_1) = \mathcal{L}(G_2)$ if and only if G has a closed subgroup G_0 which is open in both G_1 and G_2 [Ser92, p. 131, Cor. 2].

(3b) If H is a closed subgroup of G, then $\dim(H) \leq \dim(G)$. Moreover, $\dim(H) = \dim(G)$ if and only if H is open in G (apply (2a) and (3a)).

(3c) $\mathcal{L}(\mathrm{GL}_n(\mathbb{Q}_l)) = M_n(\mathbb{Q}_l)$ [Ser92, p. 130, (1)], so by (2a), $\dim(\mathrm{GL}_n(\mathbb{Q}_l)) = \dim(M_n(\mathbb{Q}_l)) = n^2$. Since $\mathbb{Z}_l^\times$ is l-adically open in $\mathbb{Q}_l = M_1(\mathbb{Q}_l)$, we have $\dim(\mathbb{Z}_l^\times) = 1$. It follows that the center of $\mathrm{GL}_n(\mathbb{Z}_l)$, which is isomorphic to $\mathbb{Z}_l^\times$, has dimension 1. In particular, the center Z of $\mathrm{GL}_2(\mathbb{Z}_l)$ has dimension 1.

Moreover, if $\mathbf{a} \in \mathrm{GL}_n(\mathbb{Z}_l)$ and $\mathbf{b} \in \mathrm{M}_n(\mathbb{Z}_l)$, then $(1 - l\mathbf{a}^{-1}\mathbf{b})^{-1} = \sum_{i=0}^{\infty} l^i(\mathbf{a}^{-1}\mathbf{b})^i \in \mathrm{M}_n(\mathbb{Z}_l)$. Therefore, $\mathbf{a} - l\mathbf{b} \in \mathrm{GL}_n(\mathbb{Z}_l)$, so $\mathrm{GL}_n(\mathbb{Z}_l)$ is l-adically open in $M_n(\mathbb{Z}_l)$, hence also in $\mathrm{GL}_n(\mathbb{Q}_l)$. It follows from (3b) that $\dim(\mathrm{GL}_n(\mathbb{Z}_l)) = \dim(\mathrm{GL}_n(\mathbb{Q}_l)) = n^2$. ∎

Example 3.3: We prove that for each non-square d of $\mathbb{Z}_l$ the dimension of each of the closed subgroups $H_{d,n}$ (Notation 1.2) of $\mathrm{GL}_2(\mathbb{Z}_l)$, where n is a non-negative integer, is 2.

By definition (in Construction 1.1), C_d is isomorphic to the l-adic analytic group $\mathbb{Z}_l[\sqrt{d}]^\times$. The latter is contained in $\mathbb{Z}_l[\sqrt{d}]$ which is homeomorphic to $\mathbb{Z}_l \oplus \mathbb{Z}_l$, hence of dimension 2. Therefore, $\dim(\mathbb{Z}_l[\sqrt{d}]^\times) \leq 2$. On the other hand, the analytic group $\mathbb{Z}_l^\times$ of dimension 1 is contained in $\mathbb{Z}_l[\sqrt{d}]^\times$. Moreover, using the binomial expansion, we find that for each positive integer k there exist $r, s \in \mathbb{N}$ with $(1 + l\sqrt{d})^k = r + s\sqrt{d}$. In particular, $(1 + l\sqrt{d})^k \in \mathbb{Z}_l[\sqrt{d}] \smallsetminus \mathbb{Z}_l$, hence $(1 + l\sqrt{d})^k \in \mathbb{Z}_l[\sqrt{d}]^\times \smallsetminus \mathbb{Z}_l^\times$. Hence, $(\mathbb{Z}_l[\sqrt{d}]^\times : \mathbb{Z}_l^\times) = \infty$. By (3b), $\dim(\mathbb{Z}_l[\sqrt{d}]^\times) \geq 2$. It follows that $\dim(C_d) = \dim(\mathbb{Z}_l[\sqrt{d}]^\times) = 2$.

Since $H_{d,n} = C_{l^{2n}d}$ (Notation 1.2), we have $\dim(H_{d,n}) = 2$ for each $n \geq 0$. ∎

We denote the group scheme over $\mathbb{Z}_l$ that consists of all upper triangular invertible matrices by $\mathbf{B}$. In particular, $\mathbf{B}(\mathbb{Z}_l) = B$ (Notation 1.6).

LEMMA 3.4: *Let I be an l-adically closed solvable subgroup of $\mathrm{GL}_2(\mathbb{Z}_l)$ of dimension 3. Then, I is $\mathrm{GL}_2(\mathbb{Z}_l)$-conjugate to an open subgroup of B.*

Proof: We break up the proof into two parts.

PART A: *Change of base field.* Since I is solvable, so is the Zariski-closure $\tilde{I}$ of I in $\mathrm{GL}_2(\widetilde{\mathbb{Q}_l})$ [Bou89, p. 342, Cor. 2]. Hence, the connected component $\tilde{J}$ of $\tilde{I}$ is also solvable.

By Lie-Kolchin, $\tilde{J}$ is $\mathrm{GL}_2(\widetilde{\mathbb{Q}_l})$-conjugate to a subgroup $\tilde{J}^*$ of $\tilde{B} = \mathbf{B}(\widetilde{\mathbb{Q}_l})$ [Bor91, p. 137, Cor. 10.5]. The dimension of a Zariski-closure $\tilde{H}$ of an l-adic analytic group H in $\mathrm{GL}_2(\widetilde{\mathbb{Q}_l})$ is greater or equal to the dimension of H, because $\tilde{H} \cap \mathrm{GL}_2(\mathbb{Q}_l)$ is an l-adically closed subgroup of $\mathrm{GL}_2(\mathbb{Q}_l)$ that contains H. In particular, $\dim(I) \leq \dim(\tilde{I})$. By [Bor91, p. 46], $\tilde{J}$ is Zariski-open in $\tilde{I}$. Hence,

$$3 = \dim(I) \leq \dim(\tilde{I}) = \dim(\tilde{J}) = \dim(\tilde{J}^*) \leq \dim(\tilde{B}) = 3.$$

Therefore, $\tilde{J}^* = \tilde{B}$, so $\tilde{J}$ is conjugate to $\tilde{B}$. In particular, $\tilde{J}$ is a Borel subgroup of $\mathrm{GL}_2(\widetilde{\mathbb{Q}_l})$.

A direct computation proves that the commutator subgroup $[\tilde{B}, \tilde{B}]$ of $\tilde{B}$ consists of all matrices of the form $\left(\begin{smallmatrix} 1 & \beta \\ 0 & 1 \end{smallmatrix}\right)$ with $\beta \in \widetilde{\mathbb{Q}_l}$. It follows that $[\tilde{B}, \tilde{B}]$ is abelian and consists of all unipotent elements of $\tilde{B}$. Hence, $[\tilde{J}, \tilde{J}]$ is abelian and consists of all unipotent element of $\tilde{J}$.

Since $\tilde{J}$ is Zariski-open in $\tilde{I}$ and $\tilde{I}$ is the Zariski-closure of I in $\mathrm{GL}_2(\widetilde{\mathbb{Q}_l})$, the group $\tilde{J}$ is the Zariski-closure of $J = \tilde{J} \cap I$. This implies that J is non-abelian (otherwise $\tilde{J}$ is abelian, so $\tilde{B}$ is abelian, which is a contradiction). In other words, $[J, J]$ is non-trivial.

PART B: *Eigenmodules.* Let g be a non-trivial element of $[J, J]$. By Part A, 1 is the only eigenvalue of g. By Lemma 1.8, there exists $h \in \mathrm{GL}_2(\mathbb{Z}_l)$ such that $h^{-1}gh \in B$. Since conjugation preserves the eigenvalues, $h^{-1}gh = \left(\begin{smallmatrix} 1 & \beta \\ 0 & 1 \end{smallmatrix}\right)$ for some $\beta \in \mathbb{Z}_l$ with $\beta \neq 0$. Replacing I and J by $h^{-1}Ih$ and $h^{-1}Jh$, if necessary, we may assume that $g = \left(\begin{smallmatrix} 1 & \beta \\ 0 & 1 \end{smallmatrix}\right)$.

Next we consider the $\mathbb{Z}_l$-module $M = \mathbb{Z}_l\binom{1}{0}$ and observe that $M = \{\mathbf{v} \in \mathbb{Z}_l^2 \mid g\mathbf{v} = \mathbf{v}\}$. Each $g' \in [J, J]$ commutes with g. Hence, for each $\mathbf{v} \in M$ we have $g'\mathbf{v} = g'g\mathbf{v} = gg'\mathbf{v}$, so $g'\mathbf{v} \in M$. In other words, $g'M = M$.

Since $[J, J]$ is a characteristic subgroup of J and $J \triangleleft I$, we have $[J, J] \triangleleft I$. Thus, for each $i \in I$ we have $g' = i^{-1}gi \in [J, J]$. By the preceding paragraph, $g'\binom{1}{0} = \binom{1}{0}$. Hence, $gi\binom{1}{0} = ig'\binom{1}{0} = i\binom{1}{0}$. Therefore, $i\binom{1}{0} \in M$. Writing $i = \left(\begin{smallmatrix}\gamma & \delta\\ \varepsilon & \eta\end{smallmatrix}\right)$ with $\gamma, \delta, \varepsilon, \eta \in \mathbb{Z}_l$, there exists $\alpha \in \mathbb{Z}_l$ such that $\left(\begin{smallmatrix}\gamma & \delta\\ \varepsilon & \eta\end{smallmatrix}\right)\binom{1}{0} = \alpha\binom{1}{0}$, hence $\varepsilon = 0$. It follows that $I \leq B$. Since both groups have dimension 3, I is open in B, as needed to be proved. ∎

Lemma 3.5:

(a) *Every l-adic analytic group D of dimension 1 has an open subgroup which is isomorphic to $\mathbb{Z}_l$.*

(b) *Every l-adic analytic group E of dimension 2 has an open solvable subgroup.*

(c) *Let U be an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_l)$. Then, every closed subgroup E of $\mathrm{GL}_2(\mathbb{Z}_l)$ of dimension 2 that contains Z has an open subgroup $E_0 = \langle z, h\rangle$ such that $E_0 \leq U$, $z \in Z$, and $\langle h\rangle \cong \mathbb{Z}_l$.*

Proof of (a): By (2a), $\dim(\mathcal{L}(D)) = \dim(D) = 1$. Hence, $\mathcal{L}(D)$ is abelian. It follows from [Ser92, p. 151, Cor. 4] that D has an open subgroup which is isomorphic to $\mathbb{Z}_l$.

Proof of (b): By (2a), the dimension of the l-adic Lie algebra $\mathcal{L}(E)$ is 2. Let x, y be a $\mathbb{Q}_l$-basis of $\mathcal{L}(E)$. Since $[x, x] = [y, y] = 0$ (with $[\ ,\ ]$ being the bracket product in $\mathcal{L}(E)$), we have $[\mathcal{L}(E), \mathcal{L}(E)] = \mathbb{Q}_l[x, y]$ and the latter Lie sub-algebra is abelian. It follows that $\mathcal{L}(E)$ is a solvable l-adic Lie algebra. By [Bou89, p. 240, Prop. III.9.19], E has an open solvable subgroup E_0.

Proof of (c): By (3b) and (3c), $\dim(U \cap Z) = 1$. By (a), $U \cap Z$ has an open subgroup which is isomorphic to $\mathbb{Z}_l$. Let z be a generator of that group. Since Z is the center of $\mathrm{GL}_2(\mathbb{Z}_l)$, z is a central element of $U \cap E$ and $\dim(\langle z\rangle) = 1$. Hence, by (1c), $\dim(U \cap E/\langle z\rangle) = 1$.

Again, by (a), $U \cap E$ has an open subgroup E_0 that contains $\langle z\rangle$ such that $E_0/\langle z\rangle \cong \mathbb{Z}_l$. We choose $h \in E_0$ such that $E_0 = \langle z, h\rangle$, as claimed. ∎

Using the notation $\mathcal{H} = \{H_{d,j} \mid d \in \{l, \zeta, l\zeta\},\ j \in \{0,1,2,\ldots\}\} \cup \{B\}$ (Notation 1.6), we set $\mathcal{H}' = \mathcal{H} \cup \{\mathrm{SL}_2(\mathbb{Z}_l)\}$.

PROPOSITION 3.6: *Every closed subgroup D of $\mathrm{GL}_2(\mathbb{Z}_l)$ of infinite index contains an open subgroup D_0 which is $\mathrm{GL}_2(\mathbb{Z}_l)$-conjugate to a subgroup of a group H that belongs to $\mathcal{H}'$.*

Proof: By (3b) and (3c), $\dim(D) \leq 3$. We set $M = D \cap \mathrm{SL}_2(\mathbb{Z}_l)$. If M is open in D, we are done. Otherwise, by (3b), $\dim(M) < \dim(D)$. Hence, $\dim(M) \leq 2$. By Lemma 3.5(a),(b), M has an open solvable subgroup M_0. By [FrJ08, p. 8, Lemma 1.2.5(b)], D has an open subgroup D_1 such that $D_1 \cap M = M_0$, so $D_1 \cap \mathrm{SL}_2(\mathbb{Z}_l) = M_0$. Since $\mathrm{GL}_2(\mathbb{Z}_l)/\mathrm{SL}_2(\mathbb{Z}_l) \cong \mathbb{Z}_l^\times$ is solvable, we conclude that D_1/M_0 is solvable, so D_1 is solvable.

If $\dim(D_1) = 3$, then by Lemma 3.4, D_1 is $\mathrm{GL}_2(\mathbb{Z}_l)$-conjugate to an open subgroup of B. In this case we may choose D_0 as D_1.

Otherwise, $\dim(D_1) \leq 2$. Then, the dimension of the solvable subgroup $E = ZD_1$ of $\mathrm{GL}_2(\mathbb{Z}_l)$ is at most 3. If $\dim(E) = 3$, then by Lemma 3.4 again, E is $\mathrm{GL}_2(\mathbb{Z}_l)$-conjugate to a subgroup of B. Hence, D_1 is also $\mathrm{GL}_2(\mathbb{Z}_l)$-conjugate to a subgroup of B. Again, we may choose $D_0 = D_1$.

If $\dim(E) = 2$, then by Lemma 3.5(c), E has an open subgroup $E_0 = \langle z, h\rangle$ with $z \in Z$. By Theorem 2.5, there exists $H \in \mathcal{H}$ and there exists $g \in \mathrm{GL}_2(\mathbb{Z}_l)$ such that $h^g \in H$. Since z commutes with g and belongs to H, we have $E_0^g = \langle z, h^g\rangle \leq H$. Then, the open subgroup $D_0 = E_0 \cap D$ of D satisfies $D_0^g \leq H$.

Finally, if $\dim(E) \leq 1$, then Z is an open subgroup of E. Hence, $D_0 = D \cap Z$ is an open subgroup of D which is contained e.g. in the group B that belongs to $\mathcal{H}$, as desired. ∎

LEMMA 3.7: *Let U be an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_l)$ and let H be one of the groups $H_{d,n}$ introduced in Notation 1.2. Then, $(U \cap H) \smallsetminus (B^G \cup \mathrm{SL}_2(\mathbb{Z}_l)) \neq \emptyset$.*

Proof: Suppose $H = H_{d,n}$. By Notation 1.2, the matrix $\mathbf{a} = \left(\begin{smallmatrix} 1 & l^i \\ l^{2n+i}d & 1 \end{smallmatrix}\right)$ belongs to H. If i is large, then $\mathbf{a} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) + l^i \left(\begin{smallmatrix} 0 & 1 \\ l^{2n}d & 0 \end{smallmatrix}\right)$ is l-adically close to the unit matrix, so $\mathbf{a}$ is in the open subgroup U of $\mathrm{GL}_2(\mathbb{Z}_l)$. On the other hand, since $\mathbf{a}$ is not a scalar

matrix, $\mathbf{a} \notin B^G$ (Theorem 2.5). In addition, $\det(\mathbf{a}) = 1 - l^{2n+2i}d \neq 1$, so $\mathbf{a} \notin \mathrm{SL}_2(\mathbb{Z}_l)$, as desired. ∎

PROPOSITION 3.8: *Let U be an open subgroup of $G = \mathrm{GL}_2(\mathbb{Z}_l)$ and let $\mathcal{H}_0$ be a proper subset of $\mathcal{H}$. Then, $U \not\subseteq \mathrm{SL}_2(\mathbb{Z}_l) \cup \bigcup_{H\in\mathcal{H}_0} H^G$.*

Proof: First we consider the case where there exists $(d, j) \in \{l, \zeta, l\zeta\} \times \{0, 1, 2, \ldots\}$ such that $H_{d,j} \notin \mathcal{H}_0$. By Lemma 3.7, there exists $u \in (U \cap H_{d,j}) \smallsetminus (B^G \cup \mathrm{SL}_2(\mathbb{Z}_l))$. Since $Z \leq B$, we have $u \notin Z$. If $H' = H_{d',j'}$ with $(d', j') \neq (d, j)$, then $H_{d,j} \cap H^G_{d',j'} = Z$ (Lemma 1.9). Hence, $u \notin H^G_{d',j'}$. It follows that $u \notin \mathrm{SL}_2(\mathbb{Z}_l) \cup \bigcup_{H\in\mathcal{H}_0} H^G$.

The other possibility is that $B \notin \mathcal{H}_0$. We choose in this case $\beta \in \mathbb{Z}_l^\times$ which is not a root of unity and set $b_0 = \left(\begin{smallmatrix} \beta & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $m = (G : U)$. Then, $b = b_0^{m!} = \left(\begin{smallmatrix} \beta^{m!} & 0 \\ 0 & 1 \end{smallmatrix}\right)$ belongs to $(U \cap B) \smallsetminus (\mathrm{SL}_2(\mathbb{Z}_l) \cap Z)$.

Finally, for each pair $(d, j) \in \{l, \zeta, l\zeta\} \times \{0, 1, 2, \ldots\}$ we have, by Lemma 1.9, that $B \cap H^G_{d,j} = Z$. Hence, $b \notin H^G_{d,j}$. Therefore, $b \in U \smallsetminus (\mathrm{SL}_2(\mathbb{Z}_l) \cup \bigcup_{H\in\mathcal{H}_0} H^G)$, as desired. ∎

Remark 3.9: We can not replace $\mathcal{H}$ in Proposition 3.8 by $\mathcal{H} \cup \{\mathrm{SL}_2(\mathbb{Z}_l)\}$. Indeed, by Theorem 2.5, $\mathrm{GL}_2(\mathbb{Z}_l) = \bigcup_{H\in\mathcal{H}} H^G$, where $G = \mathrm{GL}_2(\mathbb{Z}_l)$. ∎

THEOREM 3.10: *Let U be an open subgroup of $G = \mathrm{GL}_2(\mathbb{Z}_l)$. Then U is not finitely sliceable.*

Proof: We assume toward contradiction that G has closed subgroups $E_1, \ldots, E_n$ of infinite index such that $U \subseteq \bigcup_{i=1}^n E_i^G$. In particular, $n \geq 1$. By Proposition 3.6, each E_i has an open subgroup $E_{i,0}$ which is G-conjugate to a subgroup of a group H_i that belongs to $\mathcal{H} \cup \{\mathrm{SL}_2(\mathbb{Z}_l)\}$. We choose an open normal subgroup N of G which is contained in U such that $E_i \cap N \leq E_{i,0}$. Then, $N \subseteq \bigcup_{i=1}^n (E_i^G \cap N) = \bigcup_{i=1}^n (E_i \cap N)^G \subseteq \bigcup_{i=1}^n E_{i,0}^G \subseteq \bigcup_{i=1}^n H_i^G$. Thus, we may replace U by N and E_i by H_i for $i = 1, \ldots, n$, if necessary, to assume that

(4) $U \subseteq \bigcup_{i=1}^n E_i^G$ and each E_i belongs to $\mathcal{H} \cup \{\mathrm{SL}_2(\mathbb{Z}_l)\}$.

But then, $\mathcal{H}_0 = \{E_1, \ldots, E_n\} \smallsetminus \{\mathrm{SL}_2(\mathbb{Z}_l)\}$ is a proper subset of $\mathcal{H}$ (because $\mathcal{H}$ is infinite) and $U \subseteq \mathrm{SL}_2(\mathbb{Z}_l) \cup \bigcup_{H\in\mathcal{H}_0} H^G$, in contrast to Proposition 3.8. This concludes the proof of the theorem. ∎

4. Central Division Algebras over l-adic Fields

Division algebras of finite dimension over finite extensions of the fields $\mathbb{Q}_l$ give rise to another family of l-adic analytic groups. However, in contrast to the groups $\mathrm{GL}_2(\mathbb{Z}_l)$, each member of the new family admits a finite slicing. Unfortunately, we do not know if any of those groups occurs as a Galois group of a Galois extension of any number field [LaR15].

We recall basic facts about division algebras, which will be used in the sequel.

Remark 4.1: On division algebras. Recall that a **central division algebra over a field** K is a K-algebra D in which each of the elements of $D^\times = D \setminus \{0\}$ is invertible and K is the center of D. We denote the dimension of D over K by $[D : K]$ and assume that $[D : K] < \infty$. Then, $[D : K] = d^2$ for some positive integer d, which is called the **degree** of D [FaD93, p. 90, Thm. 3.10].

For each $x \in D^\times$ there exists a positive integer n such that $1, x, \ldots, x^n$ are linearly dependent over K. Hence, $K[x]$ is a subfield of D. Since $[D : K] < \infty$, $K[x]$ is contained in a maximal subfield of D.

If L is an arbitrary maximal subfield of D that contains K, then $[L : K] = d$ and $D \otimes_K L$ is isomorphic to the L-algebra $M_d(L)$ [FaD93, p. 96, Cor. 3.17].

Let L and L' be two field extensions of K in D and $\tau\colon L \to L'$ a K-isomorphism. By Skolem-Noether, there exists $\delta \in D^\times$ such that $\tau(x) = \delta^{-1} x \delta$ for each $x \in L$. Thus, $L^\times$ and $(L')^\times$ are conjugate in $D^\times$. ∎

THEOREM 4.2: *Let l be a prime number, K a finite extension of $\mathbb{Q}_l$, and D a finite dimensional central division algebra over K with $d = \deg(D) \geq 2$. Then, $G = D^\times / K^\times$ is a profinite group with finitely many closed subgroups $H_1, \ldots, H_n$ of infinite index such that $G = \bigcup_{i=1}^n H_i^G$.*

Proof: We consider G as the projective space $\mathbb{P}(D) = D^\times / K^\times$ of the finitely generated vector space D over the l-adic field K. Thus, G is a Hausdorff, compact, and totally disconnected group in the l-adic topology. Hence, G is profinite [RiZ00, p. 11, Thm. 1.1.12].

By Remark 4.1, every element of $D^\times$ is contained in a maximal field extension

L in D and $[L : K] = d$. By [Lan70, p. 54, Prop. 14], K has only finitely many field extensions of degree d in its algebraic closure $\tilde{K}$. Thus, K has finitely many field extensions $L_1, \ldots, L_n$ of degree d in D such that every maximal field extension L of K in D is K-isomorphic to L_i for some i between 1 and n. By Remark 4.1, there exist $1 \leq i \leq n$ and $\delta \in D^\times$ such that $(L^\times)^\delta = L_i^\times$. Hence, $H = L^\times/K^\times$ is G-conjugate to $H_i = L_i^\times/K^\times$ in $G = D^\times/K^\times$. It follows that $G = \bigcup_{i=1}^n H_i^G$.

Since L is a finite extension of K, it is complete under the l-adic topology of D. Therefore, L is closed in D. It follows that $L^\times$ is closed in $D^\times$.

Next, we consider $L^\times$ and $D^\times$ as l-adic analytic submanifolds of L and D, respectively, to conclude that $\dim(L^\times) = \dim(L) = [K : \mathbb{Q}_l]d$ and $\dim(D^\times) = \dim(D) = [K : \mathbb{Q}_l]d^2$. Hence, $\dim(D^\times/L^\times) = \dim(D^\times) - \dim(L^\times) = [K : \mathbb{Q}_l](d^2 - d) > 0$. In particular, $L^\times$ is a closed non-open subgroup of $D^\times$ (by (3b) of Section 3).

Given an i between 1 and n, we apply the preceding two paragraphs to L_i rather than to L and conclude that $H_i = L_i^\times/K^\times$ is closed in $G = D^\times/K^\times$. Also, $(G : H_i) = (D^\times/K^\times : L_i^\times/K^\times) = (D^\times : L_i^\times) = \infty$, as claimed. ∎

Remark 4.3: The argument in the second paragraph of the proof of Theorem 4.2 fails for local fields of positive characteristic p. Indeed, in this case each of these fields has the form $K = \mathbb{F}_q((t))$, where q is a power of p [CaF67, p. 129, 2.]. Consider for example the field $K = \mathbb{F}_p((t))$. Then, K has infinitely many extensions of degree p. To this end let I be the set of all negative integers that are not divisible by p. Let $i < j$ be in I. Then, there exists no $x \in K$ such that $t^i - t^j = x^p - x$. Otherwise, $x = \sum_{k=m}^\infty a_k t^k$ for some integer m with $a_k \in \mathbb{F}_p$ and $a_m \neq 0$. Then, $t^i - t^j = \sum_{k=m}^\infty a_k(t^{kp} - t^k)$. Since $i, j < 0$, the smallest exponent of t in the right hand side is mp, and since p divides neither i nor j, we have $a_m = 0$, which is a contradiction (see also [Art67, Sec. 10.4]). By Artin-Schreier [Bou90, p. A.V.92, Thm. 5] (see also [Lan93, p. 290, Thm. 6.4]), the field extensions $K(t^{i/p})$ of K of degree p with $i \in I$ are distinct. ∎

5. Towers of Tuples of Polynomials

We give an arithmetic interpretation to the slicing of a profinite group G which can be realized over a number field as a Galois group. Using a theorem of Serre, we apply this interpretation to the group $\mathrm{GL}_2(\mathbb{Z}_l)$ for each large prime number l.

We denote the ring of integers of a number field K by O_K and the set of non-zero prime ideals of O_K by $P(K)$. We choose an algebraic closure $\tilde{K}$ of K and set $\mathrm{Gal}(K) = \mathrm{Gal}(\tilde{K}/K)$. For each $\tau \in \mathrm{Gal}(K)$ let $\tilde{K}(\tau)$ be the fixed field of τ in $\tilde{K}$. We say that $\tilde{K}(\tau)$ has a certain property **P** for **almost all** $\tau \in \mathrm{Gal}(K)$ if the set of $\tau \in \mathrm{Gal}(K)$ for which **P** is false in $\tilde{K}(\tau)$ has Haar measure 0. Likewise we use the expression "for almost all $\mathfrak{p} \in P(K)$" instead of "for all but finitely many $\mathfrak{p} \in P(K)$". Given $\mathfrak{p} \in P(K)$, we write $\bar{K}_\mathfrak{p}$ for the residue field $O_K/\mathfrak{p}$. This field is a finite extension of $\mathbb{F}_p$, where p is the prime number that lies under $\mathfrak{p}$. If L is a finite extension of K and $\mathfrak{P} \in P(L)$ **lies over** $\mathfrak{p}$ (i.e. $\mathfrak{P} \cap O_K = \mathfrak{p}$), then $\bar{L}_\mathfrak{P}$ can be considered as a finite extension of $\bar{K}_\mathfrak{p}$. We say that $\mathfrak{P}$ has **degree** 1 **over** K if $\bar{L}_\mathfrak{P} = \bar{K}_\mathfrak{p}$.

We use these concepts in the following consequence of the transfer theorem [FrJ08, p. 447, Thm. 20.9.3. See also Proposition 20.9.5 for the special case when $K = \mathbb{Q}$.]. In that theorem we write $\mathcal{L}(\mathrm{ring}, O_K)$ for the first order language of the theory of rings with a constant symbol for each element of O_K [FrJ08, p. 135, Example 7.3.1].

PROPOSITION 5.1: *A sentence θ in $\mathcal{L}(\mathrm{ring}, O_K)$ is true in $\bar{K}_\mathfrak{p}$ for almost all $\mathfrak{p} \in P(K)$ if and only if θ is true in $\tilde{K}(\tau)$ for almost all $\tau \in \mathrm{Gal}(K)$.*

LEMMA 5.2: *Let K be a number field and let $f_1, \ldots, f_n$ be polynomials in $O_K[X]$ which are irreducible over K. For each i between 1 and n let x_i be a root of $f_i(X)$ in $\tilde{K}$. Then the following statements are equivalent:*

(1a) *For almost all $\mathfrak{p} \in P(K)$ there exist i and a prime ideal $\mathfrak{P} \in P(K(x_i))$ of degree 1 over K that lies over $\mathfrak{p}$.*

(1b) *For almost all $\mathfrak{p} \in P(K)$ there exist i and $x \in \bar{K}_\mathfrak{p}$ such that $f_i(x) = 0$.*

(1c) *For almost all $\tau \in \mathrm{Gal}(K)$ there exist i and $x \in \tilde{K}(\tau)$ such that $f_i(x) = 0$.*

(1d) *There exists a finite Galois extension N of K that contains $x_1, \ldots, x_n$ such that*

$$(*) \qquad \mathrm{Gal}(N/K) = \bigcup_{i=1}^{n} \bigcup_{\sigma \in \mathrm{Gal}(N/K)} \mathrm{Gal}(N/K(x_i))^{\sigma}.$$

(1e) *Equality (*) holds for each Galois extension N of K that contains $x_1, \ldots, x_n$.*

(1f) *For each $\tau \in \mathrm{Gal}(K)$ there exist i and $x \in \tilde{K}(\tau)$ such that $f_i(x) = 0$.*

Proof: The equivalence of (1a) and (1b) follows from a theorem of Dedekind and Kummer (see [Jan73, p. 32, Thm. 7.6, and p. 33, Prop. 7.7] or [Lan70, p. 27, Prop. 25 and the remark on p. 29]).

The equivalence of (1b) and (1c) is a special case of Proposition 5.1 applied to the sentence $\bigvee_{i=1}^{n} \exists X\colon f_i(X) = 0$.

If (1d) is true, then for each $\tau \in \mathrm{Gal}(K)$ there exist i between 1 and n and $\sigma \in \mathrm{Gal}(N/K)$ such that $x_i^{\sigma\tau} = x_i^{\sigma}$. Hence, $x = x_i^{\sigma}$ is a root of f_i that belongs to $\tilde{K}(\tau)$. Therefore, (1f) holds, so also (1c) is true.

If (1d) is false, then there exists $\bar{\tau} \in \mathrm{Gal}(N/K)$ such that $x_i^{\sigma\bar{\tau}} \neq x_i^{\sigma}$ for all i and σ. The set of all $\tau \in \mathrm{Gal}(K)$ whose restriction to N is $\bar{\tau}$ has a positive measure. For each τ in this set none of the polynomials $f_1, \cdots, f_n$ has a root in $\tilde{K}(\tau)$. Hence, (1c) is false, so (1f) is also false.

We leave the proof of the equivalence between (1d) and (1e) to the reader. ∎

Definition 5.3: Let K be a number field. We say that an n-tuple $(f_1, \ldots, f_n)$ of polynomials in $O_K[X]$ which are irreducible over K are **exhausting** if it satisfies each of the equivalent conditions (1a)–(1f) of Lemma 5.2.

For each $1 \leq i \leq n$ we choose a zero x_i of f_i in $\tilde{K}$ and let $L_i = K(x_i)$. Then, the n-tuple $(L_1, \ldots, L_n)$ is **exhausting over** K if (1a) holds, that is if the n-tuple $(f_1, \ldots, f_n)$ is exhausting.

Let N be a Galois extension of K. We say that N/K is **n-sliceable** if there exists a sequence $(L_{i1}, \ldots, L_{in})_{i=1,2,3,\ldots}$ of exhausting n-tuples of finite extensions of K in N such that $L_{ij} \subseteq L_{i+1,j}$ for all i, j, and $L_j = \bigcup_{i=1}^{\infty} L_{ij}$ is an infinite extension of K for $j = 1, \ldots, n$. The above sequence of n-tuples of extensions of K may be called an **n-sliceable infinite Kronecker tower between K and N**.

We say that the Galois extension N/K is **finitely sliceable** if N/K is n-sliceable for some positive integer n. ∎

PROPOSITION 5.4: *Let K be a number field, N a Galois extension of K with $G = \mathrm{Gal}(N/K)$, and n a positive integer. Then, the profinite group G is n-sliceable if and only if the Galois extension N/K is n-sliceable.*

Proof: First suppose that G is n-sliceable. Then, G has closed subgroups $H_1, \ldots, H_n$ of infinite index such that $G = \bigcup_{j=1}^{n} H_j^G$. For each j between 1 and n let L_j be the fixed field in N of H_j. Then,

$$\mathrm{Gal}(N/K) = \bigcup_{j=1}^{n} \bigcup_{\sigma \in \mathrm{Gal}(N/K)} \mathrm{Gal}(N/L_j)^{\sigma}. \tag{2}$$

Since $(G : H_j) = \infty$, the field L_j is an infinite extension of K. Choose a sequence of finite Galois extensions $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$ of K in N whose union is N. For each i let $L_{ij} = N_i \cap L_j$. Then, we choose a primitive element x_{ij} for L_{ij}/K which is integral over O_K and let $f_{ij} \in O_K[X]$ be the monic irreducible polynomial of x_{ij} over K. By (2),

$$\mathrm{Gal}(N_i/K) = \bigcup_{j=1}^{n} \bigcup_{\sigma \in \mathrm{Gal}(N_i/K)} \mathrm{Gal}(N_i/K(x_{ij}))^{\sigma}.$$

Thus, $f_{i1}, \ldots, , f_{in}$ satisfy Condition (1d), so the n-tuple $(f_{i1}, \ldots, f_{in})$ is exhausting. Hence, the n-tuples $(L_{i,1}, \ldots, L_{i,n})$ are exhausting over K (Definition 5.3). By construction $L_{ij} \subseteq L_{i+1,j}$ and $L_j = \bigcup_{i=1}^{\infty} L_{ij}$ for all i and j. It follows that N/K is n-sliceable.

Conversely, suppose that N/K is n-sliceable. Arguing backwards, Galois correspondence gives a sequence $(G_1, G_2, G_3, \ldots)$ of open normal subgroups of G with a trivial intersection, and for each positive integer i an n-tuple $(H_{i1}, \ldots, H_{in})$ of open subgroups of G that contain G_i such that $G/G_i = \bigcup_{j=1}^{n} (H_{ij}/G_i)^{G/G_i}$, $H_{i+1,j} \leq H_{ij}$, and $H_j = \bigcap_{i'=1}^{\infty} H_{i'j}$ is of infinite index in G for all j. Using compactness we find an n-slicing $G = \bigcup_{j=1}^{n} H_j^G$ of G, as desired. ∎

Elliptic curves over $\mathbb{Q}$ without complex multiplication supply an interesting application of Theorem 3.10.

PROPOSITION 5.5 (Serre): *Let E be an elliptic curve without complex multiplication defined over $\mathbb{Q}$. For each prime l let N_{l^∞} be the field generated over $\mathbb{Q}$ by all points of E having an l-power order. Then, for almost all l we have* $\mathrm{Gal}(N_{l^\infty}/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}_l)$.

The condition about E not to have complex multiplication is satisfied if the j-invariant of E is non-integral. In particular, this is the case if E is defined by the equation $Y^2 + Y = X^3 - X$, where $j = \frac{2^{12}3^3}{37}$. In this case, $\mathrm{Gal}(N_{l^\infty}/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}_l)$ *for all l.*

Proof: The first statement is a reformulation of [Ser72, Statement (6) on p. 2].

A proof that j is integral if E has complex multiplication can be found for example in [Lan73, p. 57].

The example of the elliptic curve defined by $Y^2 + Y = X^3 - X$ appears in [Ser72, p. 310, Subsection 5.5.6]. That $\mathrm{Gal}(N_{l^\infty}/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}_l)$ for all l is mentioned (without proof) on page 311 at the end of Subsection 5.5 of [Ser72]. ∎

THEOREM 5.6: *Each of the groups* $\mathrm{GL}_2(\mathbb{Z}_l)$ *can be realized over $\mathbb{Q}$ as a Galois group. However, there exists no triple (l, N, K), where l is an odd prime number, N is a Galois extension of $\mathbb{Q}$, and K is a finite extension of $\mathbb{Q}$ in N, such that* $\mathrm{Gal}(N/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}_l)$ *and N/K is finitely sliceable.*

Proof: By Proposition 5.5, $G = \mathrm{GL}_2(\mathbb{Z}_l)$ can be realized over $\mathbb{Q}$, for each l. On the other hand, let l be an odd prime number, $N/\mathbb{Q}$ a Galois extension with Galois group $\mathrm{GL}_2(\mathbb{Z}_l)$, and K a finite extension of $\mathbb{Q}$ in N. Then, $\mathrm{Gal}(N/K)$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_l)$. By Theorem 3.10, $\mathrm{Gal}(N/K)$ admits no finite slicing. Hence, by Proposition 5.4, N/K admits no finite slicing. ∎

Remark 5.7: Let D be a central division algebra of finite degree ≥ 2 over a finite extension K of $\mathbb{Q}_l$. Suppose that U is an open subgroup of $G = D^\times/K^\times$ and there exists a Galois extension N of $\mathbb{Q}$ with Galois group U. By Theorem 4.2, G is finitely sliceable, hence by the subsection "Open subgroups" of the introduction, also U is finitely sliceable.

However, it seems to be unknown, if any open subgroup of G can be realized as a Galois group over $\mathbb{Q}$. ∎

References

[Art67] E. Artin, *Algebraic Numbers and Algebraic Functions,* Gordon and Breach, New York, 1967.

[Bor91] A. Borel, *Linear Algebraic Groups (second enlarged edition),* Graduate Texts in Mathematics **126**, Springer-Verlag, New York, 1991.

[Bou89] N. Bourbaki, *Lie Groups and Lie Algebras, Chapter 1–3.* Springer, Berlin, 1989.

[Bou90] N. Bourbaki, *Algebra II, Chapters 4–7,* Springer, Berlin, 1990.

[CaF67] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory,* Academic Press, London, 1967.

[DDMS99] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, *Analytic pro-p Groups,* Second Edition, Cambridge Studies in Advanced Mathematices **61**, Cambridge University Press, Cambridge, 1999.

[FaD93] B. Farb and R. K. Dennis, *Noncommutative Algebra,* Graduate texts in mathematics 144, Springer, New York, 1993.

[FrJ08] M. D. Fried and M. Jarden, *Field Arithmetic, third edition, revised by Moshe Jarden,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2008.

[Jan73] G.J. Janusz, *Algebraic Number Fields,* Academic Press, New York, 1973.

[Jeh77] W. Jehne, *Kronecker classes of algebraic number fields,* Journal of Number Theory **9** (1977), 279–320.

[KLS14] W. M. Kantor, A. Lubotzky, and A. Shalev, *Invariable generation of infinite groups,* Journal of Algebra (2014), http://dx.doi.org/10.1016/j.algebra.2014.08.030

[Koc70] H. Koch, *Galoissche Theorie der p-Erweiterungen,* Mathematische Monographien **10**, Berlin 1970.

[Lan70] S. Lang, *Algebraic Number Theory,* Addison-Wesley, Reading, 1970.

[Lan73] S. Lang, *Elliptic Functions,* Addison-Wesley, Reading, 1973.

[Lan93] S. Lang, *Algebra, third edition,* Addison-Wesley, Reading, 1993.

[LaR15] M. Larsen, R. Ramakrishna, *The inverse Galois problem for p-adic Lie algebras,* work in progress.

[RiZ00] L. Ribes and P. Zalesskii, *Profinite Groups,* Ergebnisse der Mathematik (3) **40**, Springer, Berlin, 2000.

[Ser72] J.-P. Serre, *Propriétés galoisiennes des points d'ordere fini des courbes elliptiques,* Inventiones mathematicae **15** (1972), 259–331.

[Ser92] J.-P. Serre, *Lie Algebras and Lie Groups,* Lectures Notes in Mathematics **1500**, Springer-Verlag, New York, 1992.