ERRATA FOR A LOCAL-GLOBAL PRINCIPLE FOR ISOGENIES OF COMPOSITE DEGREE

ISABEL VOGT

This document corrects some statements in:

[1] Isabel Vogt, *A local-global principle for isogenies of composite degree*, Proc. Lond. Math. Soc. (3) **121** (2020), no. 6, 1496–1530, DOI 10.1112/plms.12378. MR4144369

The "equivalently all" part of Lemma 3.2 does not hold if the isogeny class $\mathscr{C}(E)$ contains curves with full (projective) level ℓ-structure. This necessitates several changes to the definition of exceptional and hence some changes to statements of results. First, we give the correct "equivalently all" statement for an isogeny class $\mathscr{C}$ to contain an ℓ^n-isogeny globally. The following holds in that case:

Lemma 1. *Suppose that E/K is ℓ^a-isogenous to a curve E'/K which has independent ℓ^b- and ℓ^c-isogenies (which are also independent from the dual of the ℓ^a-isogeny) with $b+c=n$, and $0 \leqslant a \leqslant c \leqslant b$. Then, up to conjugacy, the mod ℓ^n Galois representation $G_E(\ell^n)$ is contained in the group*

$$A(\ell^n) = A_{a,c,b}(\ell^n) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \gamma \equiv 0 \pmod{\ell^{a+b}}, \delta \equiv \alpha - \ell^a \beta \pmod{\ell^c} \right\}.$$

Remark. Notice that when $a = 0$, this recovers the result that $G_{E'}(\ell^n)$ is contained in a Cartan subgroup modulo ℓ^c and a Borel subgroup modulo ℓ^b for $b + c = n$.

Proof Sketch of Lemma 1. Choose a basis e_1, e_2 for ℓ-adic Tate module $T_\ell E'$ of E' so that, modulo ℓ^b and ℓ^c, the vectors e_1, e_2 correspond to the given independent ℓ^b- and ℓ^c-isogenies. Since E' also has an independent ℓ^a-isogeny (and $a \leqslant c, b$), the projectivization of the ℓ^a-torsion is a trivial Galois module. Hence,

$$G_{E'}(\ell^n) \subset \left\{ \begin{pmatrix} x & \ell^c y \\ \ell^b z & x + \ell^a w \end{pmatrix} : x, y, z, w \in \mathbb{Z}/\ell^n\mathbb{Z} \right\}.$$

By the ℓ^a-isogeny, the ℓ-adic Tate module $T_\ell E$ of E injects into $T_\ell E'$ as an index ℓ^a-sublattice $\mathbb{Z}_\ell v + \ell^a \mathbb{Z}_\ell^2$ for some $v \in \mathbb{Z}_\ell^2$. Since v, e_1, e_2 are all distinct modulo ℓ, by acting by PGL_2, we may assume that $v = e_1 + e_2$. To obtain the Galois action on the lattice spanned by $\ell^a e_1$ and $e_1 + e_2$, we conjugate

$$\ell^{-a} \begin{pmatrix} 1 & -1 \\ 0 & \ell^a \end{pmatrix} \begin{pmatrix} x & \ell^c y \\ \ell^b z & x + \ell^a w \end{pmatrix} \begin{pmatrix} \ell^a & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x - \ell^b z & \ell^{c-a} y - \ell^{b-a} z - w \\ \ell^{a+b} z & \ell^b z + x + \ell^a w \end{pmatrix}.$$

The group of matrices of this shape is exactly $A(\ell^n)$. □

The paragraph after Lemma 3.2 should read that an isogeny class $\mathscr{C}$ has an ℓ^n-isogeny if and only if every element $E \in \mathscr{C}$ has $G_E(\ell^n)$ conjugate to a subgroup of $A_{a,c,b}(\ell^n)$ for some choice of $0 \leqslant a \leqslant c \leqslant b$. Definitions 3 and 4 also need to be suitably modified:

Definition 2 (Definition 3 from [1])**.** A subgroup $G \subset \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ is exceptional if

(i) for every element $g \in G$, the characteristic polynomial $\chi_g(t)$ has a root in $\mathbb{Z}/\ell^n\mathbb{Z}$; equivalently, if $\ell \neq 2$, for all $g \in G$, $\Delta(g) = \mathrm{tr}(g)^2 - 4\det(g)$ is a square in $\mathbb{Z}/\ell^n\mathbb{Z}$;
(ii) there do not exist $0 \leqslant a \leqslant c \leqslant b$ such that G is conjugate to a subgroup of $A_{a,c,b}(\ell^n)$.

Definition 3 (Definition 4 from [1])**.** We will say that a subgroup $G \subset \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ is lift-exceptional (at step n) if

(i) $G(\ell^n)$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$;

Date: May 5, 2022.

(ii) for every $g \in G$, the characteristic polynomial $\chi_g(t)$ has a root in $\mathbb{Z}/\ell^{n-1}\mathbb{Z}$;
(iii) $G(\ell)$ is not contained in a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$;
(iv) G is not contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$;
(v) there does not exist $0 \leqslant a \leqslant \lfloor (n-1)/2 \rfloor$ such that G is conjugate to a subgroup of $A_{a,a+1,n-a-1}(\ell^n)$.

The first sentence Lemma 4.4 needs to be changed accordingly:

Lemma 4 (Lemma 4.4 of [1])**.** *Assume that $G(\ell)$ is not contained in split Cartan, and $G(\ell^n)$ is not conjugate to a subgroup of $A_{a,a+1,n-a-1}(\ell^n)$ for any $0 \leqslant a \leqslant \lfloor (n-1)/2 \rfloor$, and $G(\ell^{n-1})$ is contained in a Borel B, and every element of $G(\ell^n)$ has square discriminant. Let...*

In the proof of Lemma 4.4, in both the case that n is even and the case that n is odd, we must consider the possibility that "$\ell \mid b$" for all elements of $A \in K(\ell^n)$. We treat this in the following way:

Lemma 5. *With the setup from Lemma 4.4 of* [1]*, suppose that $K(\ell^n) \pmod{\ell}$ is contained in a split Cartan subgroup. Then either*

(a) $G(\ell)$ is contained in a split Cartan subgroup (in particular, $G(\ell^n)$ is not lift-exceptional), or
(b) $G(\ell^n)$ is contained in a Borel subgroup (in particular, $G(\ell^n)$ is not lift-exceptional), or
(c) $G(\ell^n)$ is conjugate to a subgroup of $A_{a,a+1,n-a-1}(\ell^n)$ for some $0 \leqslant a \leqslant \lfloor (n-1)/2 \rfloor$ (in particular, $G(\ell^n)$ is not lift-exceptional), or
(d) $n = 2m+1$ and $G(\ell^{2m+1}) \subset \mathbb{K}(\ell^{2m+1}) \subset R(\ell^{2m+1})$ (in particular, the conclusions of Lemma 4.4 hold).

Proof. Working in the basis in which B is upper-triangular, notice that $K(\ell^n)$ is contained in every subgroup $A_{a,a+1,n-a-1}(\ell^n)$ for $a \leqslant n-2$ by construction. We may therefore assume that the image of ϕ is nontrivial mod ℓ^{n-1}, or else we are done. Notice also that $K(\ell^n) \pmod{\ell}$ is scalar, and hence contained in *every* split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Recall that $G(\ell^n)$ is generated by $K(\ell^n)$ and one preimage X of a generator of the image of ϕ. If the image of ϕ is nontrivial modulo ℓ, then $X \bmod \ell$ is uppertriangular with distinct diagonal entries. Therefore, $X \bmod \ell$ is contained in *some* split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$; together with $K(\ell^n) \pmod{\ell}$, we see that all of $G(\ell)$ is contained in a split Cartan subgroup.

We may therefore assume that the image of ϕ is trivial modulo some power ℓ^a and nontrivial modulo ℓ^{a+1} for some $1 \leqslant a \leqslant n-2$. If $a > \lfloor (n-1)/2 \rfloor$, then we may apply the proof of Lemma 4.4 to all of $G(\ell^n)$ instead of the normal subgroup $K(\ell^n)$. The case "$b \equiv 0 \pmod{\ell}$" is not an issue since it implies that $G(\ell)$ is contained in a Cartan subgroup.

It remains to treat the case $a \leqslant \lfloor (n-1)/2 \rfloor$. The element X is of the form

$$X = \begin{pmatrix} x & y \\ \ell^n z & x + \ell^a w \end{pmatrix}.$$

If $y \equiv 0 \pmod{\ell}$, then X, and hence all of $G(\ell)$, is contained in a Cartan subgroup. We therefore assume that $\ell \nmid y$. Let $\nu = -w/y$ (which is nonzero by our assumption that the diagonal entries of X are distinct modulo ℓ^{a+1}). Conjugating $A_{a,a+1,n-a-1}(\ell^n)$ by the element $\left(\begin{smallmatrix} 1 & \\ & \nu \end{smallmatrix}\right)$ yields the group

$$A^{\nu}_{a,a+1,n-a-1}(\ell^n) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \gamma \equiv 0 \pmod{\ell^{n-1}}, \delta \equiv \alpha - \ell^a \nu \beta \pmod{\ell^{a+1}} \right\},$$

to which X evidently belongs. Since we assumed that $K(\ell^n) \bmod \ell$ is contained in a split Cartan subgroup, we also have that $K(\ell^n) \subset A^{\nu}_{a,a+1,n-a-1}(\ell^n)$, and so the same is true for $G(\ell^n)$. □

In particular, using Lemma 5, we may assume in the proof of Theorem 3.6 of [1] that

$$K(\ell^{2m+1}) \subset \mathbb{K}(\ell^{2m+1}) = \left\{ \begin{pmatrix} r & s \\ \ell^{2m} s & t \end{pmatrix} : r \equiv t \pmod{\ell^{2m}} \right\},$$

is not contained in the subgroup where s is 0 modulo ℓ. It is easy to verify that the map $\psi \colon \mathbb{K}(\ell^{2m+1}) \to \mathbb{F}_\ell$ extracting the value of s/r modulo ℓ is a group homomorphism. In particular, our assumption guarantees that $K(\ell^{2m+1})$ surjects onto $\mathbb{F}_\ell$ under ψ, and we use this for the remainder of the paper.

In Lemmas 4.8 and 4.9 of [1], the conclusions can be strengthened by replacing $\mathbb{K}$ with any subgroup K of $\mathbb{K}$ surjecting onto $\mathbb{F}_\ell$ under ψ. Similarly, Proposition 4.10 can be strengthened to say that for such K with ψ surjective, $X \cdot K$ is lift-exceptional only if the diagonal characters of X are opposite modulo ℓ^{m+1}. This strengthening guarantees that what is checked in the proof of Theorem 3.6 is, in fact, sufficient.

Notice that the entire group $\mathbb{K}(\ell^{2m+1})$ is not conjugate to any subgroup of $A_{a,a+1,n-a-1}(\ell^n)$ for any $0 \leqslant a < m$. The group $\mathbb{K}(\ell^{2m+1})$ is also not contained in a split Cartan subgroup modulo ℓ. For this reason, to check that the group denoted $X \cdot \mathbb{K}$ in Section 4.2 of [1] satisfies Definition 3 (iii)-(v), it suffices to check that it is not contained in a Borel subgroup. The altered definition of lift-exceptional therefore does not affect the relevance of the calculation in Lemma 4.7 and the "if" part of Proposition 4.10.

The computer calculations in Section 5, while correct for the definition of exceptional given in [1], must be updated to test for the correct definition of exceptional subgroup. The new `python` files can be found at the `GitHub` repository: `https://github.com/ivogt161/isogeny`. The file `verify_Proposition_5-1.py` finds all exceptional subgroups of $\mathrm{GL}_2(\mathbb{Z}/2^n\mathbb{Z})$ for $n \leqslant 6$. All exceptional subgroups by the correct Definition 2 given above are also exceptional by the old definition, but the converse is not true. The groups labeled 27445 ($n = 4$), and 189900 ($n = 5$), and $891738, 893327$ ($n = 6$) in Table A.1 in [1] are **not** exceptional by this correct definition.

These changes strengthen the results given in the introduction of [1] in the following way:

- (Theorem 1 of [1]) This can be strengthened by removing "16" from the finite list of integers N outside of which $\Sigma(K, N)$ is finite.
- (Theorem 5 of [1]) The infinite family with $\ell = 2$ and $n = 4$ corresponding to the group labeled 27445 is *not* exceptional by the correct definition. The theorem should therefore read:

  Theorem 6 (Theorem 5 of [1])**.** *Let $\mathscr{C}(E/\mathbb{Q})$ have an ℓ^n-isogeny locally almost everywhere. If E is not $\mathbb{Q}$-isogenous to a curve with an ℓ^n-isogeny over $\mathbb{Q}$, then $\ell = 7$, $n = 1$ or 2, and $j(E) = 2268945/128$.*

The results in Section 8 (for elliptic curves with geometric complex multiplication) still hold, and the proofs go through with only one very minor change: the first sentence of the first complete paragraph at the top of page 1525 should note "If we assume that $r < \lfloor n/2 \rfloor$, then there do not exist $0 \leqslant a \leqslant c \leqslant b$ with $b + c = n$ such that $\rho_{E,\ell^n}(G_K)$ is conjugate to a subgroup of $A_{a,c,b}(\ell^n)$, since $a + b < \lfloor n/2 \rfloor$ implies $b + c < n$."

Acknowledgements. Thank you to Ariel Weiss and Amit Ophir for pointing out that the "equivalently all" characterization in Lemma 3.2 of [1] is incorrect and for drawing my attention to the fact that the case $K(\ell^n)$ contained in a split Cartan mod ℓ required special attention.

Department of Mathematics, Brown University, Providence, RI USA
Email address: `ivogt.math@gmail.com`