Forum of Mathematics, Sigma (2020), **Vol. 8**:e60, 1–4
doi:10.1017/fms.2020.42

CAMBRIDGE
UNIVERSITY PRESS

RESEARCH ARTICLE

Corrigendum: Abelian *n*-division fields of elliptic curves and Brauer groups of product Kummer & abelian surfaces

Anthony Várilly-Alvarado[1] and Bianca Viray[2]

[1]Department of Mathematics MS 136, Rice University, Houston, TX 77005, USA; E-mail: varilly@rice.edu.
[2]University of Washington, Department of Mathematics, Box 354350, Seattle, WA 98195, USA; E-mail: bviray@uw.edu.

Received: 20 February 2020; **Revised:** 17 April 2020; **Accepted:** 15 May 2020

There is an error in the statement and proof of [VAV17, Proposition 5.1] that affects the statements of [VAV17, Corollaries 5.2 and 5.3]. In this note, we correct the statement of [VAV17, Proposition 5.1] and explain how to rectify subsequent statements. In brief, for a statement about abelian Galois representations of a *fixed* level, 'abelian' should be replaced with 'liftable abelian' (Definition 1). Statements about abelian Galois representations of arbitrarily high level, however, remain unchanged because such representations give rise to liftable abelian Galois representations of smaller, but still arbitrarily high, level. Hence the main theorems of the paper remain unchanged.

Definition 1. Let n be a positive integer. A subgroup H of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is liftable abelian if there exists an abelian subgroup $\widehat{H} < \mathrm{GL}_2(\widehat{\mathbb{Z}}))$ such that $\widehat{H}$ surjects onto H under the natural quotient map $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. (In particular, a liftable abelian subgroup is abelian.)

For a positive integer n and an elliptic curve E over a field k of characteristic 0, let $\rho_{E,n}\colon \Gamma_k \to \mathrm{Aut}(E_n) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ denote the representation arising from the action of Galois on the n-torsion of E. If $m \mid n$, then we write $\iota_{m,n}\colon E_m \hookrightarrow E_n$ for the natural inclusion; the image of the multiplication map

$$\left[\frac{n}{m}\right]\colon \mathrm{End}(E_m) \longrightarrow \mathrm{End}(E_n), \qquad \varphi \mapsto \iota_{m,n} \circ \varphi \circ \left[\frac{n}{m}\right]$$

is $\mathrm{End}(E_n) \cap M_2(\frac{n}{m}\mathbb{Z}/n\mathbb{Z})$. This map is also compatible with the homomorphisms $\rho_{E,n}$ and $\rho_{E,m}$. These two observations together yield the following lemma, where we have written $\mathrm{End}_k(E_m) \circ \left[\frac{n}{m}\right]$ in place of $\left[\frac{n}{m}\right](\mathrm{End}_k(E_m))$, to match the notation in [VAV17].

Lemma 2. *If* $m \mid n$ *then* $\mathrm{End}_k(E_m) \circ \left[\frac{n}{m}\right] = \mathrm{End}_k(E_n) \cap M_2(\frac{n}{m}\mathbb{Z}/n\mathbb{Z})$. □

Write $G_{E,n}$ for the quotient of $\mathrm{im}\,\rho_{E,n}$ by the subgroup of scalar matrices. The following proposition and corollaries replace [VAV17, Proposition 5.1 and Corollaries 5.2 and 5.3].

Proposition 3. *Let* ℓ *be a prime, let* s *be a positive integer, and let* E *be an elliptic curve over a field* k *of characteristic* 0. *Then*

$$\dim_{\mathbb{F}_\ell} \frac{\mathrm{End}_k(E_{\ell^s})}{\mathrm{End}_k(E_{\ell^{s-1}}) \circ [\ell]} = \begin{cases} 4 & \text{if } G_{E,\ell^s} = \{1\}, \\ 2 & \text{if } G_{E,\ell^s} \neq \{1\} \text{ and } \mathrm{im}(\rho_{E,\ell^s}) \text{ is liftable abelian, and} \\ 1 & \text{if } \mathrm{im}(\rho_{E,\ell^s}) \text{ is not liftable abelian.} \end{cases}$$

https://doi.org/10.1017/fms.2020.42 Published online by Cambridge University Press

Corollary 4. *Let E be an elliptic curve over k, and let n be a positive integer. Then we have an isomorphism of abelian groups*

$$\operatorname{End}_k(E_n) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z} \times (\mathbb{Z}/n_2\mathbb{Z})^2$$

for positive integers $n_2 \mid n_1 \mid n$. Furthermore, n_1 is the largest integer dividing n such that $\operatorname{Gal}(k(E_{n_1})/k)$ is liftable abelian, and n_2 is the largest integer dividing n such that $\operatorname{Gal}(k(E_{n_2})/k) \subset (\mathbb{Z}/n_2\mathbb{Z})^\times$, where $a \in (\mathbb{Z}/n_2\mathbb{Z})^\times$ acts by $P \mapsto aP$. If E is non-CM, then $(\operatorname{End}(\overline{E})/n)^\Gamma \cong \mathbb{Z}/n\mathbb{Z}$, and hence

$$\frac{\operatorname{End}_k(E_n)}{(\operatorname{End}(\overline{E})/n)^\Gamma} \cong \mathbb{Z}/n_1\mathbb{Z} \times (\mathbb{Z}/n_2\mathbb{Z})^2 .$$

Remark 5. The proofs of Proposition 3 and Corollary 4 prove a stronger statement, namely that if $n_1 = n_2$, then $\operatorname{End}_k(E_n) = \mathbb{Z}/n\mathbb{Z} \cdot I + \mathrm{M}_2(\frac{n}{n_2}\mathbb{Z}/n\mathbb{Z})$; and if $n_1 \neq n_2$, then

$$\operatorname{End}_k(E_n) = \left\{aI + b\tfrac{n}{n_1}A : a, b \in \mathbb{Z}/n\mathbb{Z}\right\} + \mathrm{M}_2(\tfrac{n}{n_2}\mathbb{Z}/n\mathbb{Z}) \subset \mathrm{M}_2(\mathbb{Z}/n\mathbb{Z}),$$

where $A \in \operatorname{im}\rho_{E,n_1}$ is a matrix such that $A \bmod \ell \notin \langle I \rangle$, for any $\ell \mid n_1$, as given by Lemma 7.

Corollary 6. *Let E be an elliptic curve over k, and let n be a positive integer. Let k'/k be a field extension. There is an isomorphism of abelian groups*

$$\frac{\operatorname{End}_{k'}(E_n)}{\operatorname{End}_k(E_n)} \cong \mathbb{Z}/\tfrac{n_1'}{n_1}\mathbb{Z} \times \left(\mathbb{Z}/\tfrac{n_2'}{n_2}\mathbb{Z}\right)^2 ,$$

where n_1' (respectively, n_1) is the largest integer dividing n such that $\operatorname{Gal}(k'(E_{n_1})/k')$ (respectively, $\operatorname{Gal}(k(E_{n_1})/k)$) is liftable abelian and n_2' (respectively, n_2) is the largest integer dividing n such that $\operatorname{Gal}(k'(E_{n_2})/k') \subset (\mathbb{Z}/n_2'\mathbb{Z})^\times$ (respectively, $\operatorname{Gal}(k(E_{n_2})/k) \subset (\mathbb{Z}/n_2\mathbb{Z})^\times$).

The proof of Corollary 4 proceeds as in [VAV17, proof of Corollary 5.2], almost verbatim, after replacing the word ‘abelian’ with the phrase ‘liftable abelian’, and references to [VAV17, Proposition 5.1] with references to Proposition 3. Corollary 6 is more easily deduced from Remark 5.

Characterizing liftable abelian groups is essential in the proof of Proposition 3:

Lemma 7. *Let n be a positive integer, and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be a subgroup. Then H is liftable abelian if and only if H is contained in a subring of $\mathrm{M}_2(\mathbb{Z}/n\mathbb{Z})$ generated by I and A, for some matrix A such that $A \bmod \ell \notin \langle I \rangle$ for any prime $\ell \mid n$.*

Proof. By the Sun Tzu Remainder Theorem, it suffices to prove the lemma in the case where $n = \ell^s$, so we restrict to this case for the remainder of the proof.

If H is liftable abelian, then there is an abelian subgroup $\widehat{H} < \mathrm{GL}_2(\mathbb{Z}_\ell)$ that surjects onto H. Applying [VAV17, Proposition 5.5] to $\widehat{H} \bmod \ell^{2s}$, we conclude that there is an $A' \in M_2(\mathbb{Z}/\ell^{2s}\mathbb{Z})$ with $A' \bmod \ell \notin \langle I \rangle$ such that $\widehat{H} \bmod \ell^s = H \subseteq \langle I, A' \bmod \ell^s \rangle$.

Now assume that $H \subset \langle I, A \rangle$ for some matrix A such that $A \bmod \ell \notin \langle I \rangle$. By [VAV17, proof of Corollary 5.6] (starting from the second line, taking $s' = s$), any such H is conjugate to a subgroup of $C_s(\ell^s)$, $C_{ns}^{t,\overline{\varepsilon}}(\ell^s)$, or $B_{ab}^t(\ell^s)$. Any subgroup of a liftable abelian subgroup is itself liftable abelian, so it suffices to show that the groups $C_s(\ell^k)$, $C_{ns}^{t,\overline{\varepsilon}}(\ell^k)$, and $B_{ab}^t(\ell^k)$ appearing in [VAV17, Corollary 5.6] are liftable abelian.

For the split Cartan group $C_s(\ell^k)$ and the Borel groups $B_{ab}^t(\ell^k)$, the inverse limits

$$\varprojlim_n C_s(\ell^n) \quad \text{and} \quad \varprojlim_n B_{ab}^t(\ell^n)$$

in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ are abelian and surject onto $C_s(\ell^k)$ and $B_{ab}^t(\ell^k)$, respectively, proving the claim.

https://doi.org/10.1017/fms.2020.42 Published online by Cambridge University Press

For the group $C_{ns}^{t,\overline{\varepsilon}}(\ell^k)$, one can construct a surjective system

$$C_{ns}^{t,\overline{\varepsilon_{k+1}}}(\ell^{k+1}) \twoheadrightarrow C_{ns}^{t,\overline{\varepsilon_k}}(\ell^k)$$

by taking $\overline{\varepsilon_{k+1}} \in (\mathbb{Z}/\ell^{k+1-t})^\times/(\mathbb{Z}/\ell^{k+1-t})^{\times 2}$ a lift of $\overline{\varepsilon_k} \in (\mathbb{Z}/\ell^{k-t})^\times/(\mathbb{Z}/\ell^{k-t})^{\times 2}$ compatibly up through the system. The inverse limit of this system demonstrates that $C_{ns}^{t,\overline{\varepsilon}}(\ell^k)$ is liftable abelian. □

Proof of Proposition 3. If $G_{E,\ell^s} = \{1\}$, then the claim is immediate; thus we may assume that $G_{E,\ell^s} \neq 1$. Now assume further that $\operatorname{im}\rho_{E,\ell^s}$ is liftable abelian. By Lemma 7, there is an $A' \in M_2(\mathbb{Z}/\ell^s\mathbb{Z})$ with $A' \bmod \ell \notin \langle I \rangle$ such that $\operatorname{im}\rho_{E,\ell^s} \subseteq \langle I, A' \rangle$. Let t be the maximal integer such that $\operatorname{im}\rho_{E,\ell^s} \subseteq \langle I, \ell^t A' \rangle$. Note that since $G_{E,\ell^s} \neq \{1\}$, t must be strictly less than s; or equivalently, $s - t \geq 1$. Then

$$\begin{aligned}\operatorname{End}_k(E_{\ell^s}) &= \{M : A'M \equiv MA' \bmod \ell^{s-t}\}\\ &= \{aI + bA' + \ell^{s-t}M' : a, b \in \mathbb{Z}/\ell^s\mathbb{Z}, M' \in \mathrm{M}_2(\mathbb{Z}/\ell^s\mathbb{Z})\},\end{aligned}$$

where the second equality comes from [VAV17, Lemma 5.4] applied to A'. Together with Lemma 2, we deduce that for $M' \in \mathrm{M}_2(\mathbb{Z}/\ell^s\mathbb{Z})$, we have $\ell^{s-t-1} \cdot (\ell M') \in \operatorname{End}_k(E_{\ell^{s-1}}) \circ [\ell]$. Hence, $\operatorname{End}_k(E_{\ell^s})/\operatorname{End}_k(E_{\ell^{s-1}}) \circ [\ell]$ is generated by I and A' and so is 2-dimensional.

To complete the proof, we claim that if $\dim_{\mathbb{F}_\ell}(\operatorname{End}_k(E_{\ell^s}))/(\operatorname{End}_k(E_{\ell^{s-1}}) \circ [\ell]) \geq 2$, then $\operatorname{im}\rho_{E,\ell^s}$ is liftable abelian. The identity endomorphism always generates a one-dimensional subspace of this quotient, so if the inequality holds, then by Lemma 2, there exists an $A \in \operatorname{End}_k(E_{\ell^s})$ that is not a scalar modulo ℓ. Since every element of $\operatorname{im}\rho_{E,\ell^s}$ commutes with A, by [VAV17, Lemma 5.4], we have $\operatorname{im}\rho_{E,\ell^s} \subset \langle I, A \rangle$. Lemma 7 then shows that $\operatorname{im}\rho_{E,\ell^s}$ is liftable abelian. □

Corrections for subsequent statements in [VAV17].

Corollary 5.2 of [VAV17] is used in the proof of [VAV17, Theorems 6.5 and 6.9]. In turn, [VAV17, Theorem 6.5] is used in the proofs of [VAV17, Theorem 1.3, **(EC)** ⇒ **(Ab):**, Theorem 1.5, and Theorem 1.8], while [VAV17, Theorem 6.9] is used in the proof of [VAV17, Theorem 1.3, **(Ab)** ⇒ **(EC):**, and Corollary 6.10.]

Using Corollary 4 in place of [VAV17, Corollary 5.2] in the proof of [VAV17, Theorem 6.5] yields a *stronger* version of the theorem. Namely, Corollary 4 allows one to deduce that the Galois group $\operatorname{Gal}(\tilde{L}(\sqrt{\delta}, E'_{n/c})/\tilde{L}(\sqrt{\delta}))$ is *liftable* abelian. In particular, the proofs of [VAV17, Theorem 1.3, **(EC)** ⇒ **(Ab):**, Theorem 1.5, and Theorem 1.8] go through unchanged.

On the other hand, using Corollary 4 in place of [VAV17, Corollary 5.2] in the proof of [VAV17, Theorem 6.9] yields the following weaker version of the theorem and its corollary; however, this version still suffices for the proof of [VAV17, Theorem 1.3, **(Ab)** ⇒ **(EC):**].

Theorem 8. *Let n be a positive integer, let E' be a non-CM elliptic curve over a field k of characteristic* 0*, with a k-rational cyclic subgroup C of order d, and let $E = E'/C$. Let W and W' be principal homogeneous spaces of E and E', respectively, with periods coprime to n, and let $Y = W \times W'$. If* $\operatorname{Gal}(k(E'_n)/k)$ *is liftable abelian, then* $\operatorname{Br} Y/\operatorname{Br}_1 Y$ *has an element of order* $n/\gcd(d, n)$*.*

Remark 9. With the weaker assumption that $\operatorname{Gal}(k(E'_n)/k)$ is abelian, then one can prove that $\operatorname{Br} Y/\operatorname{Br}_1 Y$ has an element of order $m/\gcd(d, m)$, where $m := \prod_{p|n} p^{\lceil v_p(n)/2 \rceil}$.

Corollary 10. *Let n, E, E', W, W' be as in Theorem 8. Suppose further that W and W' have period dividing* 2*, so that we may define* $X := \operatorname{Kum}(W \times W')$*. If* $\operatorname{Gal}(k(E'_n)/k)$ *is liftable abelian, then* $\operatorname{Br} X/\operatorname{Br}_1 X$ *has an element of order* $n_{\mathrm{odd}}/\gcd(d, n_{\mathrm{odd}})$*.*

Finally, [VAV17, Theorem 6.9] is used in the proof of the implication **(Ab)** ⇒ **(EC)** in [VAV17, Theorem 1.3].

Corrected proof of [VAV17], Theorem 1.3, ***(Ab)*** $\Rightarrow$ ***(EC):*** Let r'' be a positive integer, let k''/F be an extension of degree at most r'', let E/k'' be an elliptic curve with a k''-rational cyclic subgroup C of order d, and let $E' := E/C$. Let n be a positive integer such that $k''(E'_n)/k''$ is abelian. Then Lemma 7 and [VAV17, Proposition 5.5] together imply that $\mathrm{Gal}(k(E'_m)/k)$ is liftable abelian, where $m := \prod_{p|n} p^{\lceil v_p(n)/2\rceil}$. Hence, Theorem 8 implies that there exists $Y/k'' \in \mathscr{A}^2_d$ with an element of order $m/\gcd(d,m)$ in $\mathrm{Br}\,Y/\mathrm{Br}_1\,Y$, where $m = \prod_{p|n} p^{\lceil v_p(n)/2\rceil}$. Thus, by assumption, $m_{\mathrm{odd}} \le B'(r'',d)\gcd(d,m) \le B'(r'',d)d$. Since $n \mid m^2$, we may take $B'' := (B'(r'',d)d)^2$. $\square$

Acknowledgements. We are grateful to Francesca Balestrieri, Alexis Johnson, and Rachel Newton for alerting us to the error in the proof of [VAV17, Proposition 5.1] and for an insightful counterexample that led us to a corrected statement. We also thank the referee for a careful reading of the Corrigendum and for their valuable suggestions.

Reference

[VAV17] Anthony Várilly-Alvarado and Bianca Viray, *Abeliann-division fields of elliptic curves and Brauer groups of product Kummer & abelian surfaces*, Forum Math. Sigma **5** (2017), e 26, 42, DOI 10.1017/fms.2017.16. MR3731278

https://doi.org/10.1017/fms.2020.42 Published online by Cambridge University Press