ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 45, Number 6, 2015

TRANSITION FORMULAE FOR RANKS OF ABELIAN VARIETIES

DANIEL DELBOURGO AND ANTONIO LEI

ABSTRACT. Let $A_{/k}$ denote an abelian variety defined over a number field k with good ordinary reduction at all primes above p, and let $K_\infty = \bigcup_{n\geq 1} K_n$ be a p-adic Lie extension of k containing the cyclotomic $\mathbb{Z}_p$-extension. We use K-theory to find recurrence relations for the λ-invariant at each σ-component of the Selmer group over K_∞, where $\sigma : G_k \to \mathrm{GL}\,(V)$. This provides upper bounds on the Mordell-Weil rank for $A(K_n)$ as $n \to \infty$ whenever $G_\infty = \mathrm{Gal}\,(K_\infty/k)$ has dimension at most 3.

1. Introduction. Let E be an elliptic curve defined over a number field k, and suppose that E has good ordinary reduction at all places lying above a prime $p \neq 2$. Assuming E has no complex multiplication (and under extra hypotheses), Coates and Howson [**3,** Proposition 6.9] showed

$$\mathrm{rank}_{\mathbb{Z}}\big(E(K_n)\big) \leq c \times p^{3n} \quad \text{for some constant } c = c(E,p) > 0,$$

where $K_n = K(E[p^n])$ are the fields generated by p^n-division points on E. In this article, we address the following

Question 1.1. *If one replaces the* $\mathrm{GL}\,(2,\mathbb{Z}_p)$*-extension above by an arbitrary Lie extension* $K_\infty = \bigcup_{n\geq 1} K_n$*, and the elliptic curve by a* g*-dimensional abelian variety* A *defined over* k*, then can one obtain similar bounds?*

Conjecture 1.2. *If* $k(\mu_{p^\infty}) \subset K_\infty$*, the rank of* $A(K_n)$ *is* $O(p^{n\times(d-1)})$*, where* $d = \dim\,(\mathrm{Gal}(K_\infty/k))$*.*

2010 AMS *Mathematics subject classification.* Primary 11G10, 11R23, 20F05, 22E20.

Keywords and phrases. Mordell-Weil ranks, abelian varieties, non-commutative Iwasawa theory, representations of pro-p groups, K-theory.

Received by the editors on May 24, 2012, and in revised form on March 17, 2014.

DOI:10.1216/RMJ-2015-45-6-1807 Copyright ©2015 Rocky Mountain Mathematics Consortium

We shall prove a stronger form of this conjecture in the special case where our p-adic Lie extension K_∞ of k is of dimension ≤ 3, and satisfies:

(a) K_∞ contains the cyclotomic $\mathbb{Z}_p$-extension k_∞ of k;
(b) $H := \mathrm{Gal}(K_\infty/k_\infty)$ is a pro-p group with no p-torsion.

In particular, we remark that the group $G_\infty := \mathrm{Gal}(K_\infty/k)$ must be without any p-torsion, so its Iwasawa algebra $\Lambda(G_\infty) = \varprojlim_U \mathbb{Z}_p[G_\infty/U]$ contains no zero-divisors. Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$, and set $\Gamma_k = G_\infty/H \cong \mathbb{Z}_p$. Given a compact finitely-generated $\mathcal{O}[\![\Gamma_k]\!]$-torsion module $\mathcal{J}$, we shall write $\lambda_{\mathcal{O}[\![\Gamma_k]\!]}(\mathcal{J})$ for its cyclotomic λ-invariant, which equals the number of zeros of a generator for the characteristic ideal $\mathrm{char}_{\mathcal{O}[\![\Gamma_k]\!]}(\mathcal{J})$ for $\mathcal{J}$.

Theorem 1.3. *Suppose that $M = \mathrm{Sel}_{K_\infty}(A)^\vee$ is a $\Lambda(G_\infty)$-torsion module which belongs to the category $\mathfrak{M}_H(G_\infty)$. Then for every p-adic Artin representation $\sigma : G_\infty \to \mathrm{GL}_{\mathcal{O}}(V_\sigma)$, one has a transition formula*

$$\lambda_{\mathcal{O}[\![\Gamma_k]\!]}\big(\mathrm{tw}_{\hat{\sigma}}(M)\big) = \sum_i n_i(\sigma) \times \lambda_{\mathcal{O}[\![\Gamma_k]\!]}\big(\mathrm{tw}_{\hat{\rho}_i} M\big),$$

where the sum runs over a finite set of irreducible representations of G_∞, and the constants $n_i(\sigma)$ are defined via the decomposition

$$\psi_p \circ \mathrm{Tr}(\sigma) = \sum_i n_i(\sigma) \cdot \mathrm{Tr}(\rho_i)$$

under the action of the pth Adams operator ψ_p.

We refer the reader to Section 2 for full notation. The proof of this theorem is based upon a series of K_1-congruences derived by Ritter and Weiss **[14]** which relate Akashi series of big Selmer groups, specialized at those Artin characters factoring through K_∞/k. In particular, these allow us to find recurrence relations for their λ-invariants. Because the growth rate of these λ-invariants at the trace of the regular representation for K_n/k is $O(p^{dn})$ where $d = \dim(G_\infty)$, we obtain the following as a consequence.

Corollary 1.4. *Under the same hypotheses and assuming $d = \dim(G_\infty) \leq 3$, there exists a filtration $k \subset K_1 \subset \cdots \subset K_n \subset \cdots \subset K_\infty$ with*

$[K_n : k] = p^{dn}$ *and a natural number* $n_0 \leq 2$, *such that*

$$\operatorname{rank}_{\mathbb{Z}}\big(A(K_n)\big) \leq C_{A,G_\infty} \times p^{(d-1)n} + (2g)^2 \quad \textit{for all } n \geq n_0,$$

where $C_{A,G_\infty} = p^{-(d-1)n_0} \times \lambda_{\mathbb{Z}_p[\![\Gamma_{K_{n_0}}]\!]}(\mathrm{Sel}_{K_\infty}(A)^\vee_{H\cap \mathrm{Gal}(K_\infty/K_{n_0})}) \geq 0.$

Let $G_\infty = \Sigma_0 \supset \Sigma_1 \supset \cdots \supset \Sigma_n \supset \cdots$ be a filtration of normal subgroups such that $[G : \Sigma_n] = p^{dn}$, and set K_n to be the fixed field of Σ_n. We apply our main theorem to the regular representation on G_∞/Σ_n, and deduce a *sufficient* condition for the asymptotic formula (in the corollary) to hold is

$$\Sigma_n = \Sigma_{n-1}^p, \tag{1.1}$$

for all $n \geq n_0 + 1$. We then construct such a filtration using the theory of González-Sánchez and Klopsch [**8**], which classifies all analytic pro-p groups of dimension smaller than or equal to 3.

The two-dimensional cases are easily disposed of (one need only study subgroups of $\mathbb{Z}_p^2$ or $\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$). For the three-dimensional case, note G_∞ is isomorphic to $\langle x, y_1, y_2\rangle/\mathcal{R}$ where x, y_1, y_2 are distinguished generators for G_∞, and $\mathcal{R}$ is a set of relations involving commutators of these generators. We define Σ_n to be the subgroup generated by $x^{p^n}, y_1^{p^n}$ and $y_2^{p^n}$, and establish that (1.1) holds for $n \geq 3$ through a detailed study of commutators.

Remarks. (i) It should be mentioned that the techniques in this paper do not yield any lower bounds on the growth of $\operatorname{rank}_{\mathbb{Z}}\big(A(K_n)\big)$ as n increases. To obtain such lower bounds, one should input parity information over K_n in the manner of Harris, Matsuno, Mazur-Rubin, Coates et al., and others; see also [**5**].

(ii) Whenever the constant term C_{A,G_∞} is zero, one immediately deduces from the corollary that $A(K_\infty)$ has finite $\mathbb{Z}$-rank, bounded above by $(2g)^2$.

(iii) Provided one has a concrete realization of the Galois group in terms of an explicit tower of numbers fields, in many cases it is possible to sharpen the upper bounds considerably; for example, if $\dim(G_\infty) = 2$, then the $(2g)^2$-term above may be removed altogether (see Theorem 3.5).

(iv) As John Coates pointed out to us, there is a quicker way to obtain the asymptotic bound in the above corollary (if one does not care too much about the precise constants C_{A,G_∞} and n_0); one instead directly studies the growth of the $H \cap \Sigma_n$-coinvariants for the large Selmer group. We refer the reader to **[1]** for a more succinct argument when $\dim(G_\infty) = 2$.

(v) In the first appendix we show that (1.1) holds for $n \geq 1$ in a large number of cases. We include in the second appendix alternative proofs of our main result for both the Heisenberg and false-Tate curve extensions; whilst these are undoubtedly lengthier, they nicely illustrate the scaling effect which the pth Adams operator induces on the regular representations.

2. Generalities on λ-invariants. We begin by explaining how the Ritter-Weiss K_1-congruences can be used to derive some explicit upper bounds on the Mordell-Weil rank; in essence, we need to gain control over the cyclotomic λ-invariant over K_n as $n \to \infty$.

2.1. Preliminary results on p-adic Lie extensions. Let G_∞ and H be p-adic Lie groups as in the introduction. Let M denote a compact, finitely-generated torsion $\Lambda(G_\infty)$-module; henceforth, we shall impose:

Hypothesis ($\mu = 0$)**.** The module M is in the $\mathfrak{M}_H(G_\infty)$-category, i.e., the quotient $M/M[p^\infty]$ is of finite-type over $\Lambda(H)$.

This is equivalent to assuming the total vanishing of the μ-invariants for M, over each of the finite normal extensions of k inside K_∞.

Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$, and fix a uniformizer π of $\mathcal{O}$. Let $\sigma^\dagger : \Lambda(G_\infty) \to \mathrm{Mat}_{n\times n}(\mathcal{O})$ be the ring homomorphism induced from an Artin representation $\sigma : G_\infty \to \mathrm{GL}\,(n, \mathcal{O})$. The continuous group homomorphism $G_\infty \to \mathrm{Mat}_{n\times n}(\mathcal{O}[\![\Gamma_k]\!])$ that sends $g \in G_\infty$ to $\sigma^\dagger(g) \otimes (g \bmod H)$ extends to a (localized) algebra homomorphism

$$\Phi_\sigma : \Lambda(G_\infty)_{S^*} \longrightarrow \mathrm{Mat}_{n\times n}\big(Q_{\mathcal{O}}(\Gamma_k)\big),$$

where S^* is an Ore set, and $Q_{\mathcal{O}}(\Gamma_k)$ is the skew-field of quotients of $\mathcal{O}[\![\Gamma_k]\!]$ (see **[2,** Lemma 3.3] for details).

For a ring R, let $\mathrm{K}_j(R)$ denote its jth K-group; then on the level of K-groups, we have

$$\Phi'_\sigma : \mathrm{K}_1\big(\Lambda(G_\infty)_{S^*}\big) \longrightarrow \mathrm{K}_1\Big(\mathrm{Mat}_{n\times n}\big(Q_{\mathcal{O}}(\Gamma_k)\big)\Big) \cong Q_{\mathcal{O}}(\Gamma_k)^\times,$$

where the last isomorphism arises by Morita invariance. Returning to our module M, its class $[M]$ inside the Grothendieck group $\mathrm{K}_0(\mathfrak{M}_H(G_\infty))$ lifts to an element ξ_M under the connecting homomorphism $\partial_{G_\infty} : \mathrm{K}_1(\Lambda(G_\infty)_{S^*}) \twoheadrightarrow \mathrm{K}_0(\mathfrak{M}_H(G_\infty))$—the surjectivity of ∂ follows directly from [**2,** Proposition 3.4], provided the group G_∞ has no element of order p. Any such lift ξ_M is referred to as a *characteristic element* for M.

In preparation for the main result of this section we shall first introduce some common notation and then prove an elementary but useful lemma.

Notation. (i) For a topological group G, let $R_p(G)$ indicate the additive group generated by the $\overline{\mathbb{Q}}_p$-valued characters χ with open kernel; we also write $\mathrm{Irr}\,(G)$ for the subset of characters from irreducible G-representations.

(ii) Recall that, at each prime number p, the pth Adams operator ψ_p acts on $\chi \in R_p(G)$ by sending it to the virtual character $\psi_p\chi : g \mapsto \chi(g^p)$.

(iii) On choosing a topological generator, we may identify $\mathcal{O}[\![\Gamma_k]\!]$ with the power series ring $\mathcal{O}[\![X]\!]$. We define $\varphi : \mathcal{O}[\![\Gamma_k]\!]_{(\pi)} \to \mathcal{O}[\![\Gamma_k]\!]_{(\pi)}$ to be the map extending $X \mapsto (1+X)^p - 1$ linearly and continuously.

(iv) For a non-zero element $\mathcal{F} \in \mathcal{O}[\![\Gamma_k]\!]_{(\pi)}$, we write $\lambda(\mathcal{F})$ for the λ-invariant of $\mathcal{F}$, which is the number of zeros minus the number of poles (counted with multiplicity) that $\mathcal{F}$ has as a function on the open unit disk. Similarly, we write $\mu(\mathcal{F})$ for the μ-invariant of $\mathcal{F}$, which is the unique integer n satisfying

$$\pi^{-n}\mathcal{F} \in \mathcal{O}[\![\Gamma_k]\!]_{(\pi)} \setminus \pi\mathcal{O}[\![\Gamma_k]\!]_{(\pi)}.$$

Lemma 2.1. *Let $\mathcal{F}_1$ and $\mathcal{F}_2$ be non-zero elements of $\mathcal{O}[\![\Gamma_k]\!]_{(\pi)}$ such that both $\mu(\mathcal{F}_1) = \mu(\mathcal{F}_2) = 0$ and*

$$\mathcal{F}_1 \equiv \mathcal{F}_2 \mod \pi\mathcal{O}[\![\Gamma_k]\!]_{(\pi)}.$$

Then $\lambda(\mathcal{F}_1) = \lambda(\mathcal{F}_2)$.

Proof. For each $i = 1, 2$, we can express $\mathcal{F}_i$ as a power series quotient f_i/g_i where $f_i, g_i \in \mathcal{O}[\![\Gamma_k]\!]$ and $\mu(f_i) = \mu(g_i) = 0$. Then $\lambda(\mathcal{F}_i) = \lambda(f_i) - \lambda(g_i)$, and, from the above congruence,

$$f_1 g_2 \equiv f_2 g_1 \mod \pi\mathcal{O}[\![\Gamma_k]\!]. \tag{2.1}$$

In general, if $\mathcal{F} \in \mathcal{O}[\![\Gamma_k]\!] \setminus \pi\mathcal{O}[\![\Gamma_k]\!]$, then

$$\lambda(\mathcal{F}) = \dim_{\mathcal{O}/\pi}\Big(\mathcal{O}[\![\Gamma_k]\!]/\langle \pi, \mathcal{F}\rangle\Big).$$

However, equation (2.1) implies $\langle \pi, f_1 g_2\rangle$ and $\langle \pi, f_2 g_1\rangle$ represent the same ideal, in which case $\lambda(f_1 g_2)$ equals $\lambda(f_2 g_1)$; as a direct consequence,

$$\lambda(\mathcal{F}_1) = \lambda(f_1) - \lambda(g_1) = \lambda(f_2) - \lambda(g_2) = \lambda(\mathcal{F}_2),$$

and the required equality is proved. □

Theorem 2.2. *If $\xi_M \in \mathrm{K}_1(\Lambda(G_\infty)_{S^*})$ denotes a characteristic element for M and $\sigma : G_\infty \to \mathrm{Aut}_{\mathcal{O}}(V_\sigma)$ is any Artin representation which satisfies the condition $\Phi'_\sigma(\xi_M) \in \mathcal{O}[\![\Gamma_k]\!]_{(\pi)}$, then*

$$\lambda\big(\Phi'_\sigma(\xi_M)\big) = \sum_{\chi_i \in \mathrm{Irr}\,(G_\infty)} n_i(\sigma) \times \lambda\big(\Phi'_{\rho_i}(\xi_M)\big),$$

where the constants $n_i(\sigma)$ are defined by the decomposition

$$\psi_p \circ \mathrm{Tr}(\sigma) = \sum_{\chi_i \in \mathrm{Irr}\,(G_\infty)} n_i(\sigma) \cdot \chi_i$$

with each $\chi_i = \mathrm{Tr}\,(\rho_i)$. (See also **[15,** Theorem 4.1.6]*.)*

Proof. The congruences of Ritter and Weiss are derived in terms of p-adic Lie groups of dimension 1; therefore, we must first explain how to descend from G_∞ to a suitable one-dimensional quotient $G^{(1)}_{\infty,\sigma}$ as follows.

Let $K_{\infty,\sigma} = \overline{\mathbb{Q}}^{\mathrm{Ker}\,(\sigma)} \cdot k_\infty$ be the compositum of the field cut out by $\mathrm{Ker}\,(\sigma)$ together with the cyclotomic $\mathbb{Z}_p$-extension of k. In particular, one can decompose

$$G^{(1)}_{\infty,\sigma} := \mathrm{Gal}\big(K_{\infty,\sigma}/k\big) \cong \Gamma_k \ltimes H^{(1)}_\sigma,$$

where $H_\sigma^{(1)}$ is obtained as a quotient of H. Furthermore, $H_\sigma^{(1)}$ must be a finite p-group because $\mathrm{Im}\,(\sigma)$ is finite, so $\dim\,(G_{\infty,\sigma}^{(1)}) = 1$.

We now recall the definition of the Det-homomorphism from **[13]**. Let $x \in Q(G_{\infty,\sigma}^{(1)})^\times$ and $\chi \in R_p(G_{\infty,\sigma}^{(1)})$. The action of x gives rise to an automorphism on the $Q_{\overline{\mathbb{Q}}_p}(\Gamma_k)$-vector space $\mathrm{Hom}_{\overline{\mathbb{Q}}_p[H_\sigma^{(1)}]}(V_\chi, \overline{\mathbb{Q}}_p \otimes_{\mathbb{Q}_p} Q(G_{\infty,\sigma}^{(1)}))$. If one writes $\mathrm{Det}_\chi(x) \in Q_{\overline{\mathbb{Q}}_p}(\Gamma_k)^\times$ for the determinant of this action, this allows us to define a map

$$\begin{aligned} Q\big(G_{\infty,\sigma}^{(1)}\big)^\times &\longrightarrow \mathrm{Hom}\Big(R_p\big(G_{\infty,\sigma}^{(1)}\big), Q_{\overline{\mathbb{Q}}_p}(\Gamma_k)^\times\Big) \\ x &\longmapsto [\chi \longmapsto \mathrm{Det}_\chi(x)]. \end{aligned}$$

From **[13,** Section 3], the map defined in this way is a group homomorphism, and it factors through the projection $Q(G_{\infty,\sigma}^{(1)})^\times \twoheadrightarrow \mathrm{K}_1(Q(G_{\infty,\sigma}^{(1)}))$. Its image lies inside a certain subgroup $\mathrm{Hom}^* \subset \mathrm{Hom}$, which is described explicitly in **[13,** Theorem 8]. We shall write

$$\mathrm{Det} : \mathrm{K}_1\Big(Q\big(G_{\infty,\sigma}^{(1)}\big)\Big) \longrightarrow \mathrm{Hom}^*\Big(R_p\big(G_{\infty,\sigma}^{(1)}\big), Q_{\overline{\mathbb{Q}}_p}(\Gamma_k)^\times\Big)$$

for the Det-homomorphism given above. Note that, if $x \in \Lambda(G_{\infty,\sigma}^{(1)})_{(p)}$ and $\chi \in R_p(G_{\infty,\sigma}^{(1)})$ take values in $\mathcal{O}$, the determinant $(\mathrm{Det}x)(\chi)$ will in fact belong to $\mathcal{O}[\![\Gamma_k]\!]_{(\pi)}$ by **[14,** Proof of Lemma 2].

The crux of our argument is that, for x and χ as above, and enlarging the scalars $\mathcal{O}$ if necessary, one has the modulo p congruence

$$(\mathrm{Det}x)(\chi)^p \equiv \varphi\big(\mathrm{Det}(\mathrm{Frob}_p x)\big)(\psi_p \circ \chi) \mod p \cdot \mathcal{O}[\![\Gamma_k]\!]_{(\pi)},$$

which was proven by Ritter and Weiss **[14,** Proposition 8].

Remarks. (i) If we take $\mathcal{F}_1 = (\mathrm{Det}\,x)(\chi)^p$ and $\mathcal{F}_2 = \varphi(\mathrm{Det}\,(\mathrm{Frob}_p x))(\psi_p\chi)$ with $\mu(\mathcal{F}_1) = \mu(\mathcal{F}_2) = 0$, then Lemma 2.1 implies

$$\begin{aligned} p \times \lambda\big((\mathrm{Det}\,x)(\chi)\big) &= \lambda\big(\varphi\big(\mathrm{Det}\,(\mathrm{Frob}_p x)\big)(\psi_p \circ \chi)\big) \\ &= p \times \lambda\big((\mathrm{Det}\,x)(\psi_p \circ \chi)\big), \end{aligned}$$

since the effect of the map φ is to multiply the λ-invariant by p, whilst the Frobenius action on the coefficients does not change the λ-invariant.

(ii) Moreover, if $\chi = \mathrm{Tr}\,(\sigma)$ and $\psi_p \circ \chi = \sum_{\chi_i \in \mathrm{Irr}\,(G_\infty)} n_i(\sigma) \cdot \chi_i$, then by explicit Brauer induction

$$\lambda\Big((\mathrm{Det}\, x)(\psi_p \circ \chi)\Big) = \lambda\Bigg(\prod_{\chi_i \in \mathrm{Irr}\,(G_\infty)} (\mathrm{Det}\, x)(\chi_i)^{n_i(\sigma)}\Bigg).$$

(iii) Combining the previous two comments, we immediately see that both $\lambda((\mathrm{Det}\, x)(\chi))$ and $\lambda(\prod_{\chi_i \in \mathrm{Irr}\,(G_\infty)} (\mathrm{Det}\, x)(\chi_i)^{n_i(\sigma)})$ are equal.

To complete the proof of the theorem, we must connect the Hom-description with the characteristic element of M. From the definition of the map Φ_σ, clearly it factorizes through the first K-group for the localization of $\Lambda(G^{(1)}_{\infty,\sigma})$. In fact, there is a commutative diagram

$$\begin{array}{ccccc}
\Phi'_\sigma : \mathrm{K}_1\Big(\Lambda\big(G_\infty\big)_{S^*}\Big) & \xrightarrow{\mathrm{pr}_*} & \mathrm{K}_1\Big(\Lambda\big(G^{(1)}_{\infty,\sigma}\big)_{\overline{S}^*}\Big) & \xrightarrow{\left(\Phi^{(1)}_\sigma\right)'} & Q_{\overline{\mathbb{Q}}_p}(\Gamma_k)^\times \\
 & & \Big\downarrow \iota_* & & \Big\uparrow h \mapsto h\big(\mathrm{Tr}(\sigma)\big) \\
 & & \mathrm{K}_1\Big(Q\big(G^{(1)}_{\infty,\sigma}\big)\Big) & \xrightarrow{\mathrm{Det}} & \mathrm{Hom}^*\Big(R_p\big(G^{(1)}_{\infty,\sigma}\big), Q_{\overline{\mathbb{Q}}_p}(\Gamma_k)^\times\Big),
\end{array}$$

where ι denotes the mapping of an algebra Λ into its skew-field of quotients; the homomorphism $\Phi^{(1)}_\sigma : \Lambda(G^{(1)}_{\infty,\sigma})_{\overline{S}^*} \to \mathrm{Mat}_{n\times n}(Q_{\mathcal{O}}(\Gamma_k))$ is constructed in an identical way to Φ_σ, with the Lie group G_∞ replaced by its one-dimensional quotient.

Let us now take $x = \iota_*(\mathrm{pr}_*\xi_M)$. Applying this factorization to x yields

$$\Phi'_\sigma(\xi_M) = \big(\Phi^{(1)}_\sigma\big)' \circ \mathrm{pr}_*(\xi_M) = (\mathrm{Det}\, x)\Big|_{\mathrm{Tr}\,(\sigma)} = (\mathrm{Det}\, x)(\chi)$$

and, by similar reasoning,

$$\Phi'_{\rho_i}(\xi_M) = \big(\Phi^{(1)}_{\rho_i}\big)' \circ \mathrm{pr}_*(\xi_M) = (\mathrm{Det}\, x)\Big|_{\mathrm{Tr}\,(\rho_i)} = (\mathrm{Det}\, x)(\chi_i).$$

Finally, our hypothesis on the μ-invariants of M ensures the vanishing condition in remark (i) is satisfied; hence, we obtain

$$\begin{aligned}
\lambda\big(\Phi'_\sigma(\xi_M)\big) = \lambda\big((\mathrm{Det}\, x)(\chi)\big) &\overset{\text{by (iii)}}{=} \lambda\Bigg(\prod_{\chi_i \in \mathrm{Irr}\,(G_\infty)} (\mathrm{Det}\, x)(\chi_i)^{n_i(\sigma)}\Bigg) \\
&= \sum_{\chi_i} n_i(\sigma) \times \lambda\big((\mathrm{Det}\, x)(\chi_i)\big) = \sum_{\chi_i} n_i(\sigma) \times \lambda\big(\Phi'_{\rho_i}(\xi_M)\big),
\end{aligned}$$

and the desired equality follows. ☐

2.2. Bounding Mordell-Weil ranks. Let K_∞/k denote a p-adic Lie extension given as in the introduction, and write k_n for the nth layer in the $\mathbb{Z}_p$-extension k_∞ of degree $[k_n : k] = p^n$. Suppose A is an abelian variety of dimension g defined over k, such that:

(A) A has good ordinary reduction at all the primes of k lying above p;
(B) $\mathrm{Sel}_{K_\infty}(A)^\vee := \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Sel}_{K_\infty}(A), \mathbb{Q}_p/\mathbb{Z}_p)$ is a torsion $\Lambda(G_\infty)$-module;
(C) As a $\mathbb{Z}_p[\![X]\!]$-module, $\mathrm{Sel}_{K_n \cdot k_\infty}(A)^\vee$ has trivial μ-invariant for all $n \geq 1$.

The second condition is now a standard conjecture in the non-commutative Iwasawa theory of abelian varieties.

Lemma 2.3. *Assume that G_∞ has dimension ≤ 3 (as a p-adic Lie group). Then, $H_i(H', \mathrm{Sel}_{K_\infty}(A)^\vee) = 0$ for $i \geq 1$ where H' is any open subgroup of H.*

Proof. By Pontryagin duality, it is equivalent to show the statement that $H^i(H', \mathrm{Sel}_{K_\infty}(A)) = 0$ for $i \geq 1$.

By assumption, H' is of dimension ≤ 2, so the assertion is clear for $i \geq 3$. Likewise, the statement for $i = 2$ follows from that for $i = 1$ by the same argument as [**4,** Proposition 2.9]. For $i = 1$, it is enough to show that

(a) The maps $\gamma_w : J_v(k_\infty) \to J_w(K_\infty)^H$ are surjective for all $v \in S$, $w|v$, where the set S includes the primes at which A has bad reduction, and also the primes above p;
(b) $H^m(G_S(K_\infty), H^1(G_\infty, A[p^\infty])) = 0$ for $m \geq 1$.

Here $J_v(k_\infty) = H^1(k_{\infty,v}, A)(p)$, with a similar definition for $J_w(K_\infty)$.

We first prove (a). As in [**4,** Proof of Lemma 2.3], we have

$$\mathrm{coker}(\gamma_w) = H^2(D_{w/v}, A[p^\infty]) = 0,$$

by Tate local duality when $v \nmid p$, where $D_{w/v}$ is the decomposition group of w over v. For finite places $v \mid p$,

$$\operatorname{coker}(\gamma_w) = H^2(D_{w/v}, \widetilde{A}_w[p^\infty]);$$

with $\widetilde{A}_w$ indicating the reduction of the abelian variety at w. If $\widehat{A}$ denotes the formal group associated to A at w, there is an exact sequence

$$\begin{aligned}\cdots \longrightarrow H^2(D_{w/v}, A[p^\infty]) &\longrightarrow H^2(D_{w/v}, \widetilde{A}_w[p^\infty]) \\ &\longrightarrow H^3(D_{w/v}, \widehat{A}[p^\infty]) \longrightarrow \cdots,\end{aligned}$$

and $H^2(D_{w/v}, A[p^\infty]) = H^3(D_{w/v}, \widehat{A}[p^\infty])$; however, $H^3(D_{w/v}, \widehat{A}[p^\infty]) = 0$ as $D_{w/v}$ has p-cohomological dimension ≤ 2, thence (a) follows.

We may prove (b) in the same way as [**4,** Lemma 2.4]. $\square$

Lemma 2.4. *Let $M = \mathrm{Sel}_{K_\infty}(A)^\vee$, and let K be a finite subextension of K_∞/k with Galois group $G = \mathrm{Gal}(K/k)$. If M_K denotes the $\mathrm{Gal}(K_\infty/K \cdot k_\infty)$-coinvariants of M, then*

$$\lambda_{\mathbb{Z}_p[\![\Gamma_k]\!]}\big(\Phi'_{\mathrm{reg}_G}(\xi_M)\big) = [K \cap k_\infty : k] \times \lambda_{\mathbb{Z}_p[\![\Gamma_K]\!]}(M_K)$$

where reg_G is the regular representation of G, and Γ_K indicates the Galois group $\mathrm{Gal}(K \cdot k_\infty/K)$.

Proof. Recall, from [**2,** Lemma 3.7], there is a commutative diagram

$$\begin{array}{ccc} \mathrm{K}_1\big(\Lambda(G_\infty)_{S^*}\big) & \xrightarrow{\partial_{G_\infty}} & \mathrm{K}_0\big(\mathfrak{M}_H(G_\infty)\big) \\ \big\downarrow{\scriptstyle \Phi'_\rho} & & \big\downarrow{\scriptstyle \mathrm{Ak}_{\mathcal{O}} \circ \mathrm{tw}_{\widehat{\rho}}} \\ Q_{\mathcal{O}}(\Gamma_k)^\times & \overset{\mathrm{proj}}{\twoheadrightarrow} & Q_{\mathcal{O}}(\Gamma_k)^\times/\mathcal{O}[\![\Gamma_k]\!]^\times. \end{array}$$

Here $\rho : G_\infty \to \mathrm{Aut}_{\mathcal{O}}(V)$ denotes any fixed Artin representation. The Akashi series is given by the alternating product

$$\mathrm{Ak}_{\mathcal{O}}(\mathcal{P}) := \prod_{i \geq 0} \mathrm{char}_{\Lambda_{\mathcal{O}}(\Gamma_k)}\Big(H_i\big(H, \mathcal{P}\big)\Big)^{(-1)^i} \mod \mathcal{O}[\![\Gamma_k]\!]^\times,$$

while $\mathrm{tw}_{\widehat{\rho}} : \mathfrak{M}_H(G_\infty) \to \mathfrak{M}_H(G_\infty)$ is the (contragredient) ρ-twist operator.

Let us now take ρ to be reg_G (with $\mathcal{O} = \mathbb{Z}_p$), and set

$$H' = H \cap \mathrm{Gal}(K_\infty/K) = \mathrm{Gal}(K_\infty/K \cdot k_\infty).$$

By Lemma 2.3, we have, for all $i \geq 1$, that $H_i(H', \mathrm{Sel}_{K_\infty}(A)^\vee) = 0$, which implies $H_i(H', \mathrm{tw}_{\widehat{\rho}}(M)) = 0$. Therefore, $H_i(H, \mathrm{tw}_{\widehat{\rho}}(M))$ is a p-group of exponent dividing $[H : H']$, and its characteristic power series must be of the form $p^{\mu_i} \times$ (a unit of $\Lambda(\Gamma_k)$) with $\mu_i \in \mathbb{Z}_{\geq 0}$. Thus,

$$\begin{aligned}\Phi'_\rho(\xi_M) &\equiv \mathrm{Ak}_{\mathbb{Z}_p}\big(\mathrm{tw}_{\widehat{\rho}}(M)\big)\\ &\equiv p^{\sum_i (-1)^i \mu_i}\\ &\times \mathrm{char}_{\mathbb{Z}_p[\![\Gamma_k]\!]}\big(H_0(H, \mathrm{tw}_{\widehat{\rho}}(M))\big) \mod \mathbb{Z}_p[\![\Gamma_k]\!]^\times.\end{aligned}$$

If $\Gamma' = \mathrm{Gal}(K \cap k_\infty/k)$, then since $G_\infty \cong \Gamma_k \ltimes H$, one has $G \cong \Gamma' \ltimes H/H'$. Using Frobenius reciprocity and Shapiro's lemma:

$$\begin{aligned}H_0\left(H, M \otimes \mathrm{reg}_G\right) &\cong H_0\Big(H, M \otimes \mathrm{Ind}_{H'}^{H}\left(\mathrm{reg}_{\Gamma'}\right)\Big)\\ &\cong H_0\Big(H, \mathrm{Ind}_{H'}^{H}(M \otimes \mathrm{reg}_{\Gamma'})\Big)\\ &\cong H_0(H', M) \otimes \mathrm{reg}_{\Gamma'}.\end{aligned}$$

Therefore, one can deduce

$$\lambda_{\mathbb{Z}_p[\![\Gamma_k]\!]}\big(H_0\big(H, \mathrm{tw}_{\widehat{\rho}}(M)\big)\big) = \#\Gamma' \times \lambda_{\mathbb{Z}_p[\![\Gamma_{K_n}]\!]}\big(M_{H'}\big),$$

and it follows that

$$\lambda_{\mathbb{Z}_p[\![\Gamma_k]\!]}\big(\Phi'_\rho(\xi_M)\big) = \#\Gamma' \times \lambda_{\mathbb{Z}_p[\![\Gamma_K]\!]}(M_K),$$

as required. □

We now assume that there exists a filtration of normal subgroups

$$G_\infty = \Sigma_0 \supset \Sigma_1 \supset \cdots \supset \Sigma_n \supset \cdots \tag{2.2}$$

such that $\#G_n = p^{dn}$ and $K_n \cap k_\infty = k_n$ for all $n \geq 0$, where G_n and K_n are defined as G_∞/Σ_n and $K_\infty^{\Sigma_n}$, respectively.

Lemma 2.5. *If $\Sigma_n = \Sigma_{n-1}^p$ for some $n \geq 1$, then*

$$\psi_p \circ \mathrm{Tr}(\mathrm{reg}_{G_n}) = p^d \times \mathrm{Tr}(\mathrm{reg}_{G_{n-1}}).$$

Proof. Recall that, if G is a finite group, then

$$\mathrm{Tr}(\mathrm{reg}_G)(g) = \begin{cases} 0 & \text{if } g \neq 1 \\ \#G & \text{if } g = 1. \end{cases}$$

In particular, for $g \in G_\infty$,

$$\psi_p \circ \mathrm{Tr}(\mathrm{reg}_{G_n})(g) = \mathrm{Tr}(\mathrm{reg}_{G_n})(g^p) = \begin{cases} 0 & \text{if } g^p \notin \Sigma_n \\ \#G_n & \text{if } g^p \in \Sigma_n, \end{cases}$$

whereas

$$\mathrm{Tr}(\mathrm{reg}_{G_{n-1}})(g) = \begin{cases} 0 & \text{if } g \notin \Sigma_{n-1} \\ \#G_{n-1} & \text{if } g \in \Sigma_{n-1}. \end{cases}$$

The result follows from the fact $p^d \times \#G_{n-1} = \#G_n$. $\square$

Theorem 2.6. *Assume that G_∞ is a p-adic Lie group of dimension $d \leq 3$ with no p-torsion, and that the filtration (2.2) exists. If K_∞ is as above and there exists an integer n_0 such that $\Sigma_n = \Sigma_{n-1}^p$ for all $n \geq n_0 + 1$, then*

$$\mathrm{rank}_{\mathbb{Z}}\left(A(K_n)\right) \leq C_{A,G_\infty} \times p^{(d-1)n} + \delta_{A,G_\infty},$$

where $C_{A,G_\infty} = p^{-(d-1)n_0} \times \lambda_{\mathbb{Z}_p[\![\Gamma_{K_{n_0}}]\!]}(\mathrm{Sel}_{K_\infty}(A)^\vee_{H\cap\Sigma_{n_0}})$ and $\delta_{A,G_\infty} \leq (2g)^2$ are both constants independent of n.

Proof. Let $M = \mathrm{Sel}_{K_\infty}(A)^\vee$, and write $M_n = M_{H\cap\Sigma_n}$. From Theorem 2.2 and Lemma 2.5, it follows that

$$\lambda_{\mathbb{Z}_p[\![\Gamma_k]\!]}\big(\Phi'_{\mathrm{reg}_{G_n}}(\xi_M)\big) = p^d \times \lambda_{\mathbb{Z}_p[\![\Gamma_k]\!]}\big(\Phi'_{\mathrm{reg}_{G_{n-1}}}(\xi_M)\big).$$

Now, taking K to be K_n and K_{n-1} in Lemma 2.4 respectively, one deduces

$$p^n \times \lambda_{\mathbb{Z}_p[\![\Gamma_{K_n}]\!]}(M_n) = p^d \times p^{n-1} \times \lambda_{\mathbb{Z}_p[\![\Gamma_{K_{n-1}}]\!]}(M_{n-1});$$

thence, for $n \geq n_0$,

$$\lambda_{\mathbb{Z}_p[\![\Gamma_{K_n}]\!]}(M_n) = p^{d-1} \times \lambda_{\mathbb{Z}_p[\![\Gamma_{K_{n-1}}]\!]}(M_{n-1}).$$

As a direct corollary, we obtain the upper bound

$$\lambda_{\mathbb{Z}_p[\![\Gamma_{K_n}]\!]}(M_n) \leq C_{A,G_\infty} \times p^{(d-1)n}.$$

The kernel of the natural restriction map

$$H^1\big(K_n \cdot k_\infty, A[p^\infty]\big) \xrightarrow{\delta_n} H^1\big(K_\infty, A[p^\infty]\big)^{\mathrm{Gal}(K_\infty/K_n \cdot k_\infty)}$$

is equal to $H^1(K_\infty/K_n \cdot k_\infty, A(K_\infty)[p^\infty])$. We claim that its $\mathbb{Z}_p$-corank is bounded by some constant $\delta_{A,G_\infty} \leq (2g)^2$, independent of n. (This follows from the fact that $\mathrm{Gal}(K_\infty/K_n \cdot k_\infty)$ is either abelian or isomorphic to a subgroup of $\langle x, y : [x,y] = y^{p^s}\rangle$ where $s \in \mathbb{N}$ by [**8,** Proposition 7.1]; hence, it contains a normal subgroup of dimension 1; also, the $\mathbb{Z}_p$-corank of $A(K_\infty)[p^\infty]$ is at most $2g$.) Therefore, the $\mathbb{Z}_p$-corank of the kernel of the homomorphism

$$\mathrm{Sel}_{K_n \cdot k_\infty}(A) \xrightarrow{\mathrm{res}} \mathrm{Sel}_{K_\infty}(A)^{\mathrm{Gal}(K_\infty/K_n \cdot k_\infty)}$$

is also bounded by δ_{A,G_∞}. Moreover, by Mazur's control theorem [**12**],

$$\begin{aligned}\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{K_n}(A) &= \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{K_n \cdot k_\infty}(A)^{\Gamma_{K_n}} \\ &\leq \lambda_{\mathbb{Z}_p[\![\Gamma_{K_n}]\!]}\big(\mathrm{Sel}_{K_n \cdot k_\infty}(A)\big)\end{aligned}$$

so one can deduce

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{K_n}(A) \leq C_{A,G_\infty} \times p^{(d-1)n} + \delta_{A,G_\infty}.$$

Lastly if $Ш(A/K_n)$ denotes the Tate-Shafarevich group of A over K_n, then

$$\begin{aligned}\mathrm{rank}_{\mathbb{Z}}\big(A(K_n)\big) &\leq \mathrm{rank}_{\mathbb{Z}}\big(A(K_n)\big) + \mathrm{corank}_{\mathbb{Z}_p}\Big(Ш(A/K_n)[p^\infty]\Big) \\ &= \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{K_n}(A) \\ &\leq C_{A,G_\infty} \times p^{(d-1)n} + \delta_{A,G_\infty},\end{aligned}$$

as required. □

3. The two-dimensional case. Let A/k be an abelian variety satisfying conditions (A)–(C) in subsection 2.2, with the dimension of G_∞ equal to 2. We shall show that the filtration as specified in (2.2), with the property that $\Sigma_n = \Sigma_{n-1}^p$ for all $n \geq 1$, exists. We recall that one has the following result from [**8,** Proposition 7.1] and [**10,** subsection 7.3].

Theorem 3.1. *If G_∞ is two-dimensional, then G_∞ is isomorphic either to $\mathbb{Z}_p \times \mathbb{Z}_p$, or instead to*

$$G(s) := \begin{pmatrix} 1 & \mathbb{Z}_p \\ 0 & 1 + p^s\mathbb{Z}_p \end{pmatrix},$$

for some integer $s \in \mathbb{N}$.

When $G_\infty \cong \mathbb{Z}_p^2$, we may simply take Σ_n to be the subgroup corresponding to $(p^n\mathbb{Z}_p)^2$ for $n \geq 0$. We shall therefore concentrate on the non-abelian case. Note that $G(s)$ is an open subgroup of $G(1)$ for all $s \in \mathbb{N}$. Therefore, without loss of generality, we may assume that $G_\infty \cong G(1)$; in this case, one may realize K_∞ as a Lie subextension of the false-Tate curve extension $k(\mu_{p^\infty}, m^{1/p^\infty})$ where $m > 0$ is some p-power-free integer.

Remark 3.2. A bound on the Mordell-Weil rank for the false-Tate extension (when A is an elliptic curve) was first obtained by Hachimori and Venjakob [**9,** Corollary 2.9] who applied results of Matsuno [**11**] on finite Λ-submodules in Selmer groups, albeit without explicitly determining C_{A,K_∞} below. The proof we present here is based purely on the 'algebraic shape' of $\mathrm{K}_1(\Lambda(G_\infty)_{S^*})$, and instead uses the finite-dimensional representation theory of the underlying Galois group.

We now identify G_∞ with $G(1)$, and define

$$\Sigma_n = \begin{pmatrix} 1 & p^n\mathbb{Z}_p \\ 0 & 1 + p^{n+1}\mathbb{Z}_p \end{pmatrix}$$

at each $n \geq 0$. Then $[\Sigma_{n-1} : \Sigma_n] = p^2$ for every $n \geq 1$, and it can be checked that Σ_n is a normal subgroup of G_∞.

Lemma 3.3. *For $n \geq 1$, we have $\Sigma_n = \Sigma_{n-1}^p$.*

Proof. Writing $g = \begin{pmatrix} 1 & b \\ 0 & a \end{pmatrix} \in G_\infty$, one computes

$$g^p = \begin{pmatrix} 1 & (a^{p-1} + \cdots + a + 1)b \\ 0 & a^p \end{pmatrix}.$$

If $g \in \Sigma_{n-1}$, then $a \in 1 + p^n\mathbb{Z}_p$ and $b \in p^{n-1}\mathbb{Z}_p$. In particular, $a \equiv 1 \mod p$, so $a^{p-1} + \cdots + a + 1 \equiv 0 \mod p$; therefore, $g^p \in \Sigma_n$.

Conversely, if $g \in \Sigma_n$, we have $a \in 1 + p^{n+1}\mathbb{Z}_p$, and we may find $a_0 \in 1 + p^n\mathbb{Z}_p$ such that $a_0^p = a$. Moreover, $a_0^{p-1} + \cdots + 1 \equiv p \mod p^2$, so we may find $b_0 \in p^{n-1}\mathbb{Z}_p$ such that $(a_0^{p-1} + \cdots + 1)b_0 = b$. In other words,

$$g_0 = \begin{pmatrix} 1 & b_0 \\ 0 & a_0 \end{pmatrix} \in \Sigma_{n-1} \quad \text{and} \quad g_0^p = g.$$

□

Recall from the previous section that K_n is the fixed field of K_∞ under Σ_n.

Lemma 3.4. *For all $n \geq 0$, one has $K_n \cap k_\infty = k_n$.*

Proof. Via the semi-direct product $G_\infty = \Gamma_k \ltimes H$, we can identify Γ_k as a subgroup of G_∞. The assertion in the lemma is then equivalent to the equality $[\Gamma_k : \Gamma_k \cap \Sigma_n] = p^n$. By Lemma 3.3, one has $\Sigma_n = G_\infty^{p^n}$; therefore,

$$\Gamma_k \cap \Sigma_n = \Gamma_k^{p^n},$$

which clearly has index p^n in Γ_k. □

Theorem 3.5. *There is an asymptotic bound*

$$\mathrm{rank}_{\mathbb{Z}}\big(A(K_n)\big) \leq C_{A,K_\infty} \times p^n \quad \textit{at all integers } n \geq 0,$$

for the given constant $C_{A,K_\infty} = \lambda_{\mathbb{Z}_p[\![\Gamma_k]\!]}(\mathrm{Sel}_{K_\infty}(A)_H^\vee)$.

Proof. By Lemmas 3.3 and 3.4, it is enough to show the term δ_{A,G_∞} in Theorem 2.6 vanishes in this setting. Recall, from the proof of the theorem, that δ_{A,G_∞} is the $\mathbb{Z}_p$-corank of $H^1(K_\infty/k_\infty, A(K_\infty)[p^\infty])$, and the latter group turns out to be finite by a natural generalization of **[9,** Lemma 3.3]. □

4. The three-dimensional case. Let A/k be an abelian variety satisfying conditions (A)–(C) in subsection 2.2, with the dimension of G_∞ equaling 3. We remark that G_∞ is soluble (because $G_\infty/H \cong \Gamma$ and

H is of dimension 2, which is soluble using Theorem 3.1); in particular, this excludes $\mathrm{SL}(2, \mathbb{Z}_p)$ and $\mathrm{SL}(1, \mathbb{D}_p)$ from appearing.

Let us review the classification of such soluble groups, as is discussed at length in [**8,** Theorem 7.4]. We shall write $\mathbb{N}_0$ for the set of non-negative integers $\mathbb{Z}_{\geq 0}$.

Theorem 4.1. *If G_∞ is soluble and torsion-free, then G_∞ is isomorphic to one of the following groups*:

(i) *the abelian group $\mathbb{Z}_p^3$;*
(ii) *an open subgroup of the Heisenberg group, i.e., a group represented by $\langle x, y_1, y_2 : [y_1, y_2] = 1, [y_1, x] = 1, [y_2, x] = y_1^{p^s} \rangle$ for some $s \in \mathbb{N}_0$;*
(iii) $\langle x, y_1, y_2 : [y_1, y_2] = 1, [y_1, x] = y_1^{p^s}, [y_2, x] = y_2^{p^s} \rangle$ *for some $s \in \mathbb{N}$;*
(iv) $\langle x, y_1, y_2 : [y_1, y_2] = 1, [y_1, x] = y_1^{p^s} y_2^{p^{s+r} d}, [y_2, x] = y_1^{p^{s+r}} y_2^{p^s} \rangle$ *for some $s, r \in \mathbb{N}$ and $d \in \mathbb{Z}_p$;*
(v) $\langle x, y_1, y_2 : [y_1, y_2] = 1, [y_1, x] = y_2^{p^s d}, [y_2, x] = y_1^{p^s} y_2^{p^{s+r}} \rangle$ *where $s, r \in \mathbb{N}_0$ and $d \in \mathbb{Z}_p$, such that either $s \geq 1$, or $r \geq 1$ and $d \in p\mathbb{Z}_p$;*
(vi) *either one of $\langle x, y_1, y_2 : [y_1, y_2] = 1, [y_1, x] = y_2^{p^{s+r}}, [y_2, x] = y_1^{p^s} \rangle$ or $\langle x, y_1, y_2 : [y_1, y_2] = 1, [y_1, x] = y_2^{p^{s+r} t}, [y_2, x] = y_1^{p^s} \rangle$ where $s, r \in \mathbb{N}_0$ with $s + r \geq 1$ and $t \in \mathbb{Z}_p^\times$ is not a square modulo p.*

As an illustration, in case (3), if k contains the pth roots of unity, then K_∞ may be realized as an extension of the type

$$k\big(\mu_{p^\infty}, m_1^{1/p^\infty}, m_2^{1/p^\infty}\big),$$

where p, m_1, m_2 are pairwise coprime as integers. Since the abelian case is well understood, we only consider cases (2)–(6) here. Let

$$\Sigma_n = \left\langle x^{p^n}, y_1^{p^n}, y_2^{p^n} \right\rangle.$$

Our main goal is to show that these subgroups satisfy the condition given by Lemma 2.5, namely,

Theorem 4.2. *For $n \geq 3$, we have $\Sigma_{n-1}^p = \Sigma_n$ and $[\Sigma_{n-1} : \Sigma_n] = p^3$. Moreover, $K_n \cap k_\infty = k_n$.*

In particular, this would give us the required asymptotic bounds on the $\mathbb{Z}$-rank of $A(K_n)$ by Theorem 2.6:

Theorem 4.3. *There is an asymptotic bound*

$$\mathrm{rank}_{\mathbb{Z}}\big(A(K_n)\big) \leq C_{A,G_\infty} \times p^{2n} + \delta_{A,G_\infty} \quad \textit{at all integers } n \geq 2,$$

where $\delta_{A,G_\infty} \leq (2g)^2$ *and* $C_{A,G_\infty} \geq 0$.

4.1. Preliminary results on commutators. We write $Y = \langle y_1, y_2 \rangle \cong \mathbb{Z}_p^{\oplus 2}$ (since $[y_1, y_2] = 1$), so that

$$[x, y_i] \in Y \quad \text{at each } i = 1, 2. \tag{4.1}$$

Lemma 4.4. *For* $i = 1, 2$ *and* $\alpha \in \mathbb{Z}_p$, *we have* $[x^\alpha, y_i] \in Y$. *Moreover,*

$$[x^\alpha, y_i^\beta] = [x^\alpha, y_i]^\beta \quad \textit{for all } \beta \in \mathbb{Z}_p.$$

Proof. By (4.1), we have $xYx^{-1} = Y$. This implies $x^n Y x^{-n} = Y$ for all $n \in \mathbb{Z}$; hence, the first statement follows by continuity.

Let $x^\alpha y_i x^{-\alpha} = y \in Y$. Then $[x^\alpha, y_i] = yy_i^{-1} \in Y$, but Y is abelian so

$$x^\alpha y_i^\beta x^{-\alpha} = y^\beta \quad \text{and} \quad [x^\alpha, y_i^\beta] = y^\beta y_i^{-\beta} = [x^\alpha, y_i]^\beta,$$

and the second statement is true. □

In particular, we see that Y^{p^n} is a normal subgroup of G_∞ for all $n \geq 0$. For $\alpha \in \mathbb{Z}_p$, there exist $a_n, b_n, c_n, d_n \in \mathbb{Z}_p$ (depending on α) such that

$$[x^{n\alpha}, y_1] = y_1^{a_n} y_2^{b_n}, \qquad [x^{n\alpha}, y_2] = y_1^{c_n} y_2^{d_n}$$

for all integers $n \in \mathbb{N}$. We have the following recurrence relations.

Lemma 4.5. *For all integers* $n \geq 1$,

$$a_{n+1} = (a_1+1)a_n + c_1 b_n + a_1; \qquad b_{n+1} = (d_1+1)b_n + b_1 a_n + b_1;$$
$$c_{n+1} = (a_1+1)c_n + c_1 d_n + c_1; \qquad d_{n+1} = (d_1+1)d_n + b_1 c_n + d_1.$$

Proof. One computes, via Lemma 4.4,

$$[x^{(n+1)\alpha}, y_1] = x^{(n+1)\alpha} y_1 x^{-(n+1)\alpha} y_1^{-1} = x[x^{n\alpha}, y_1]x^{-1}[x, y_1]$$

$$= xy_1^{a_n}y_2^{b_n}x^{-1}[x,y_1] = [x,y_1^{a_n}]y_1^{a_n}[x,y_2^{b_n}]y_2^{b_n}[x,y_1]$$
$$= [x,y_1]^{a_n}y_1^{a_n}[x,y_2]^{b_n}y_2^{b_n}[x,y_1],$$

which implies the first two equations. The last two can be obtained similarly. □

Corollary 4.6. *For all $n \in \mathbb{N}$, $a_n, b_n, d_n \equiv 0 \mod p$ and $c_n \equiv nc_1 \mod p$.*

Proof. By definition, $a_1, b_1, d_1 \equiv 0 \mod p$. Thus, we deduce by induction that $a_n, b_n, d_n \equiv 0$ and $c_{n+1} \equiv c_n + c_1 \mod p$. □

Lemma 4.7. *If $\alpha \in p\mathbb{Z}_p$, then $[x^\alpha, y_i] \in Y^p$ at each $i = 1, 2$.*

Proof. By Corollary 4.6,

$$[x^n, y_1] \in Y^p \quad \text{and} \quad [x^n, y_2] \in \langle y_1^p, y_2^p\rangle = Y^p \quad \text{at every } n \in p\mathbb{N}.$$

Hence, using continuity arguments again, one obtains

$$[x^\alpha, y_1] \in Y^p \quad \text{and} \quad [x^\alpha, y_2] \in Y^p,$$

for all $\alpha \in p\mathbb{Z}_p$; the result now follows. □

Lemma 4.8. *If $\alpha, \beta, \gamma \in \mathbb{Z}_p$ and $n \in \mathbb{N}$, then*

$$\left(x^\alpha y_1^\beta y_2^\gamma\right)^n = x^{n\alpha}y_1^{n\beta}y_2^{n\gamma}\prod_{i=1}^{n-1}\left([y_1^{-\beta}, x^{-i\alpha}][y_2^{-\gamma}, x^{-i\alpha}]\right);$$
$$\left(y_1^\beta y_2^\gamma x^\alpha\right)^n = \prod_{i=1}^{n-1}\left([x^{i\alpha}, y_1^\beta][x^{i\alpha}, y_2^\gamma]\right)y_1^{n\beta}y_2^{n\gamma}x^{n\alpha}.$$

Proof. One calculates that

$$x^\alpha y_1^\beta y_2^\gamma x^{n\alpha} = x^\alpha y_1^\beta x^{n\alpha}y_2^\gamma[y_2^{-\gamma}, x^{-n\alpha}]$$
$$= x^{(n+1)\alpha}y_1^\beta[y_1^{-\beta}, x^{-n\alpha}]y_2^\gamma[y_2^{-\gamma}, x^{-n\alpha}].$$

Therefore, upon applying Lemma 4.4,

$$\left(x^{\alpha}y_1^{\beta}y_2^{\gamma}\right)x^{n\alpha}y_1^{n\beta}y_2^{n\gamma}\prod_{i=1}^{n-1}\left([y_1^{-\beta},x^{-i\alpha}][y_2^{-\gamma},x^{-i\alpha}]\right)$$
$$=x^{(n+1)\alpha}y_1^{(n+1)\beta}y_2^{(n+1)\gamma}\prod_{i=1}^{n}\left([y_1^{-\beta},x^{-i\alpha}][y_2^{-\gamma},x^{-i\alpha}]\right),$$

and the first equation follows inductively. The second one can be proved similarly. □

Lemma 4.9. *Let $n \geq 0$ be an integer. If $\alpha \in p^n\mathbb{Z}_p$, then*

$$[x^{\alpha}, y_i] \in Y^{p^n} \quad \textit{for both } i = 1, 2.$$

Proof. We prove this by induction. When $n = 0$, there is nothing to prove and the case $n = 1$ is given by Lemma 4.7.

Assume that the statement is true for $n - 1$ where $n \geq 2$, and let $\alpha \in p^n\mathbb{Z}_p$. From the inductive hypothesis, there exists $y = y_1^{\beta}y_2^{\gamma} \in Y^{p^{n-2}}$ such that $[x^{\alpha/p}, y_i] = y^p$, so $y_i^{-1}x^{\alpha/p}y_i = y^p x^{\alpha/p}$. As a straight consequence,

$$\begin{aligned} y_i^{-1}x^{\alpha}y_i &= \left(y_1^{p\beta}y_2^{p\gamma}x^{\alpha/p}\right)^p \\ &= \prod_{n=1}^{p-1}\left([x^{n\alpha/p}, y_1^{p\beta}][x^{n\alpha/p}, y_2^{p\gamma}]\right)y_1^{p^2\beta}y_2^{p^2\gamma}x^{\alpha} \\ &= \left(\prod_{n=1}^{p-1}[x^{n\alpha/p}, y_1^{\beta}][x^{n\alpha/p}, y_2^{\gamma}]\right)^p y^{p^2}x^{\alpha} \end{aligned}$$

upon using Lemmas 4.8 and 4.4. Furthermore, the inductive hypothesis implies

$$[x^{n\alpha/p}, y_1^{\beta}], [x^{n\alpha/p}, y_2^{\gamma}] \in Y^{p^{n-1}} \quad \text{for all } n \in \mathbb{Z};$$

therefore, there exists $y' \in Y^{p^{n-2}}$ such that

$$y_i^{-1}x^{\alpha}y_i = (y'y)^{p^2}x^{\alpha}.$$

One concludes $[x^{\alpha}, y_i] \in Y^{p^n}$, so the statement of the lemma is true. □

Corollary 4.10. *For all $n \geq 0$, Σ_n is a normal subgroup of G_∞.*

Proof. Let $i \in \{1,2\}$. Lemma 4.4 tells us that $xy_i^{p^n}x^{-1} \in \Sigma_n$, whereas Lemma 4.9 implies $y_i x^{p^n} y_i^{-1} \in \Sigma_n$, from which the result follows. □

4.2. Proof of Theorem 4.2. Let us first give an explicit description for the elements of Σ_n.

Lemma 4.11. *For all integers $n \geq 0$, the group Σ_n coincides with the set*

$$\left\{ x^\alpha y_1^\beta y_2^\gamma : \alpha, \beta, \gamma \in p^n \mathbb{Z}_p \right\}.$$

Proof. Let $\alpha, \beta \in p^n\mathbb{Z}_p$ and $i \in \{1,2\}$. Then, by Lemma 4.4, we have

$$y_i^\beta x^\alpha = x^\alpha y_i^\beta [y_i^{-\beta}, x^{-\alpha}] = x^\alpha y_i^\beta [x^{-\alpha}, y_i]^{-\beta} \in x^\alpha Y^{p^n}.$$

Thus, every word in x^{p^n} and $y_i^{p^n}$ can be written as $x^\alpha y$, for some $\alpha \in p^n\mathbb{Z}_p$ and $y \in Y^{p^n}$. □

This clearly implies $[\Sigma_{n-1} : \Sigma_n] = p^3$. It remains to show that $\Sigma_{n-1}^p = \Sigma_n$. Let $\alpha, \beta, \gamma \in p^{n-1}\mathbb{Z}_p$; using Lemmas 4.4 and 4.8 in tandem,

$$(x^\alpha y_1^\beta y_2^\gamma)^p = x^{p\alpha} y_1^{p\beta} y_2^{p\gamma} (y_1^a y_2^b)^\beta (y_1^c y_2^d)^\gamma$$

for some $a, b, c, d \in \mathbb{Z}_p$, which only depend on α. From Lemma 4.9, if $\alpha \in p^2\mathbb{Z}_p$, then $a, b, c, d \in p^2\mathbb{Z}_p$; furthermore, $\Sigma_{n-1}^p \subset \Sigma_n$ for every $n \geq 3$ upon applying Lemma 4.11.

Let $g = x^\alpha y_1^\beta y_2^\gamma \in \Sigma_n$ with $\alpha, \beta, \gamma \in p^n\mathbb{Z}_p$, and set $\alpha_0 = \alpha/p \in p^{n-1}\mathbb{Z}_p$. We may then associate to α_0 these constants a, b, c, d as described above. Consider the simultaneous equations

$$\beta_0 + \frac{a}{p}\beta_0 + \frac{c}{p}\gamma_0 = \frac{\beta}{p};$$
$$\gamma_0 + \frac{b}{p}\beta_0 + \frac{d}{p}\gamma_0 = \frac{\gamma}{p}.$$

Since $n \geq 3$, we have $a, b, c, d \in p^2\mathbb{Z}_p$. Therefore, all coefficients above are in $\mathbb{Z}_p$, and the determinant of the equations is congruent to 1 modulo p. Therefore, we may solve $\beta_0, \gamma_0 \in p^{n-1}\mathbb{Z}_p$. In other words, if $g_0 = x^{\alpha_0} y_1^{\beta_0} y_2^{\gamma_0}$, then $g_0 \in \Sigma_{n-1}$ and $g_0^p = g$; hence, $\Sigma_n \subset \Sigma_{n-1}^p$ as required.

Finally, the proof for the statement $k_\infty \cap K_n = k_n$ follows from the same argument as that for Lemma 3.4 on replacing Lemma 3.3 by Lemma 4.11.

Remarks. (i) Recall that a pro-p group G is *powerful* if $G/\overline{G^p}$ is abelian. In particular, as G is finitely generated, G^p coincides with its Frattini subgroup. Note further that G_∞ always contains an open subgroup which is powerful (see **[6,** Corollary 4.3]); therefore, after a finite base-change of k, one may assume that G_∞ is powerful.

(ii) If we take $\Sigma_n = P_n(G_\infty)$ to be the lower p-series of G_∞, i.e.,

$$P_1(G_\infty) = G_\infty$$

and

$$P_{i+1}(G_\infty) = \overline{P_i(G_\infty)^p [P_i(G_\infty), G_\infty]} \quad \text{for } i \geq 1,$$

then $\Sigma_{n-1}^p = \Sigma_n$ (from **[6,** Theorem 3.6]) and $[\Sigma_{n-1} : \Sigma_n] = p^3$ if $n \gg 1$, since Σ_n is uniform whenever $n \gg 1$ (see **[6,** Theorem 4.2]). In particular, this yields an alternative method to obtain the asymptotic bound on $\mathrm{rank}_{\mathbb{Z}}(A(K_n))$.

APPENDIX

A. An improvement on Theorem 4.2. In this appendix, we show that Theorem 4.2 in fact holds for $n \geq 1$ if the constants a_1, b_1, d_1 are congruent to 0 modulo p^2. Under this additional assumption, one has the following:

Lemma A.1. *Let $\alpha \in \mathbb{Z}_p$, then*

$$\prod_{n=1}^{p-1} [x^{n\alpha}, y_1] \in Y^{p^2} \quad \textit{and} \quad \prod_{n=1}^{p-1} [x^{n\alpha}, y_2] \in \left\langle y_1^p, y_2^{p^2} \right\rangle.$$

Proof. Upon replacing p by p^2, the proof of Corollary 4.6 implies

$$[x^n, y_1] \in Y^{p^2} \quad \text{and} \quad [x^n, y_2] \equiv y_1^{nc_1} \mod Y^{p^2}$$

at each $n \in \mathbb{N}$. By continuity, one knows that

$$[x^\alpha, y_1] \in Y^{p^2} \quad \text{and} \quad [x^\alpha, y_2] \equiv y_1^{\alpha c_1} \mod Y^{p^2}$$

for all $\alpha \in \mathbb{Z}_p$, which gives the first part of the lemma. For the second part,

$$\prod_{n=1}^{p-1} [x^{n\alpha}, y_2] \equiv \prod_{n=1}^{p-1} y_1^{n\alpha c_1} \equiv y_1^{p(p-1)\alpha c_1/2} \mod Y^{p^2},$$

as required. □

Proposition A.2. *For all $n \geq 1$, $\Sigma_{n-1}^p = \Sigma_n$.*

Proof. As in subsection 4.2, for $n \geq 1$ and $\alpha, \beta, \gamma \in p^{n-1}\mathbb{Z}_p$, we have

$$(x^\alpha y_1^\beta y_2^\gamma)^p \;=\; x^{p\alpha} y_1^{p\beta} y_2^{p\gamma} (y_1^a y_2^b)^\beta (y_1^c y_2^d)^\gamma$$

for some $a, b, c, d \in \mathbb{Z}_p$. But Lemma 4.2 implies that $a, b, d \equiv 0 \mod p^2$ and $c \equiv 0 \mod p$; therefore, $\Sigma_{n-1}^p \subset \Sigma_n^p$.

Let $g = x^\alpha y_1^\beta y_2^\gamma \in \Sigma_n$ with $\alpha, \beta, \gamma \in p^n\mathbb{Z}_p$; as in subsection 4.2, we need to solve

$$\begin{aligned} \beta_0 + \frac{a}{p}\beta_0 + \frac{c}{p}\gamma_0 &= \frac{\beta}{p}; \\ \gamma_0 + \frac{b}{p}\beta_0 + \frac{d}{p}\gamma_0 &= \frac{\gamma}{p}, \end{aligned}$$

where a, b, c, d are constants associated to $\alpha_0 = \alpha/p$. But $a, b, d \equiv 0 \mod p^2$ and $c \equiv 0 \mod p$. By Lemma 4.2, all coefficients above are in $\mathbb{Z}_p$, and the determinant of the equations is congruent to 1 modulo p. Therefore, we may solve for β_0 and γ_0 and proceed as before. □

Remark. One can give a more explicit proof for Proposition 4.2 when G_∞ is the full Heisenberg group (namely for case (ii) of Theorem 4.1, with $s = 0$). In this situation, G_∞ will be isomorphic to the matrix group $\begin{pmatrix} 1 & \mathbb{Z}_p & \mathbb{Z}_p \\ 0 & 1 & \mathbb{Z}_p \\ 0 & 0 & 1 \end{pmatrix}$; hence, Σ_n may be identified with $\begin{pmatrix} 1 & p^n\mathbb{Z}_p & p^n\mathbb{Z}_p \\ 0 & 1 & p^n\mathbb{Z}_p \\ 0 & 0 & 1 \end{pmatrix}$.

Let $g = \left(\begin{smallmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{smallmatrix}\right) \in G_\infty$, so that

$$g^p = \begin{pmatrix} 1 & pa & pc + \binom{p}{2}ab \\ 0 & 1 & pb \\ 0 & 0 & 1 \end{pmatrix}.$$

As a corollary, $g \in \Sigma_{n-1}$ implies that $g^p \in \Sigma_n$ as $p \neq 2$.

Conversely if $g \in \Sigma_n$, there exist $a_0, b_0 \in p^{n-1}\mathbb{Z}_p$ such that $pa_0 = a$ and $pb_0 = b$. As $p \neq 2$, we have $c - \binom{p}{2}a_0b_0 \in p^n\mathbb{Z}_p$; consequently, there exists $c_0 \in p^{n-1}\mathbb{Z}_p$ such that $pc_0 + \binom{p}{2}a_0b_0 = c$. Then

$$g_0 := \begin{pmatrix} 1 & a_0 & c_0 \\ 0 & 1 & b_0 \\ 0 & 0 & 1 \end{pmatrix} \in \Sigma_{n-1} \quad \text{and} \quad g_0^p = g,$$

and the proposition follows.

B. Explicit calculations of representations. The proofs of both Theorems 3.5 and 4.3 rely on constructing a filtration as given by (2.2) with the property that $\Sigma_n = \Sigma_{n-1}^p$ when n is large enough, which is sufficient because of Lemma 2.5. In this appendix, we show that the conclusion on traces of regular representations given in Lemma 2.5 may be obtained directly, when G_∞ is either non-abelian of dimension 2 or a Heisenberg group; this involves us undertaking a low-brow study of the Adams operator ψ_p acting on the regular representation.

B.1. Representations of the false-Tate curve tower. We first study how the ψ_p-operator acts on $R_p(G_n)$, where the group

$$G_n = H_n \rtimes \Upsilon_n \quad \text{such that } H_n = \mathbb{Z}_p/p^n\mathbb{Z}_p \text{ and } \Upsilon_n = \Delta \times \frac{1+p\mathbb{Z}_p}{1+p^n\mathbb{Z}_p}$$

with $\Delta \lhd \mu_{p-1} \subset \mathbb{Z}_p^\times$.

For each positive integer $m \le n$, we shall write $\eta_m : \mathbb{Z}_p/p^n\mathbb{Z}_p \to \mu_{p^m}$ for the multiplicative character sending $x \mapsto \exp(2\pi i x/p^m)$ at every $x \in H_n$ (clearly one can equally well view η_m as a character of H_k if $m \le k \le n$). By [**7,** Lemma 15], the irreducible representations of G_n of dimension > 1 are of the form

$$\mathrm{Ind}_{H_m}^{G_m}(\eta_m) \otimes \beta \quad \text{where } m \le n, \text{ and } \beta : \Upsilon_n \longrightarrow \overline{\mathbb{Q}}_p^\times \text{ multiplicatively.}$$

N.B. Any representation of G_m for $m < n$ is automatically a representation of the larger group G_n, courtesy of the projection maps $G_n \twoheadrightarrow G_m$.

Proposition B.1. *If the additive character* $\chi^{(n,\beta)} = \mathrm{Tr}\,(\mathrm{Ind}_{H_n}^{G_n}(\eta_n) \otimes \beta)$, *then one has an equality*

$$\psi_p \circ \chi^{(n,\beta)} = p \cdot \mathrm{Tr}\left(\mathrm{Ind}_{H_{n-1}}^{G_{n-1}}(\eta_{n-1}) \otimes \beta^p\right)$$

inside the virtual ring $R_p(G_n)$.

Proof. We begin by making two simplifying assumptions:

- The group $G_n = \mathbb{Z}/p^n\mathbb{Z} \rtimes (\mathbb{Z}/p^n\mathbb{Z})^\times$, i.e., Δ is the whole of $\mathbb{F}_p^\times$;
- The character β is trivial on $\Upsilon_n = (\mathbb{Z}/p^n\mathbb{Z})^\times$.

Therefore, our task is to show for all $g \in G_n$,

$$\mathrm{Tr}\left(\mathrm{Ind}_{H_n}^{G_n}(\eta_n)(g^p)\right) = p \times \mathrm{Tr}\left(\mathrm{Ind}_{H_{n-1}}^{G_{n-1}}(\eta_{n-1})(g)\right).$$

We again proceed by undertaking a low-brow computation. Observe that

$$G_n \cong \begin{pmatrix} \Upsilon_n & H_n \\ 0 & 1 \end{pmatrix} \lhd \mathrm{GL}\left(2, \mathbb{Z}_p/p^n\mathbb{Z}_p\right),$$

and let us write $g_x = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$ at each $x \in \Upsilon_n$. ☐

Remarks. (a) If $g = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G_n$, then $g_x \cdot g \cdot g_x^{-1} = \begin{pmatrix} a & xb \\ 0 & 1 \end{pmatrix}$; hence,

$$\mathrm{Tr}\left(\mathrm{Ind}_{H_n}^{G_n}(\eta_n)(g)\right) = \sum_{\substack{x \in G_n/H_n \text{ with} \\ g_x \cdot g \cdot g_x^{-1} \in H_n}} \eta_n \begin{pmatrix} a & xb \\ 0 & 1 \end{pmatrix}.$$

(b) Certainly, when $a \neq 1$ the sum is empty, thus $\mathrm{Tr}\,(\mathrm{Ind}_{H_n}^{G_n}(\eta_n)(g)) = 0$.

(c) Alternatively, if $a = 1$, then

$$\operatorname{Tr}\Big(\operatorname{Ind}_{H_n}^{G_n}\big(\eta_n\big)(g)\Big) = \sum_{x\in\Upsilon_n} \exp\big(2\pi i x b/p^n\big)$$
$$= \begin{cases} p^n - p^{n-1} & \text{if } p^n \big| b \\ -p^{n-1} & \text{if } p^{n-1} \big\| b \\ 0 & \text{otherwise.} \end{cases}$$

Recall that $g = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$; it is then an easy exercise to show

- If $g^p = 1$, then $a^p = 1$ and $p^{n-1}\big|b$;
- If $g^p = \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix}$ with $p^{n-1}\big|b'$, then $a^p = 1$ and $p^{n-2}\big|b$.

As an immediate consequence,

$$\operatorname{Tr}\big(\operatorname{Ind}_{H_n}^{G_n}(\eta_n)(g^p)\big) = \begin{cases} p^n - p^{n-1} & \text{if } a^p = 1 \text{ and } p^{n-1}\big|b \\ -p^{n-1} & \text{if } a^p = 1 \text{ and } p^{n-2}\big\|b \\ 0 & \text{otherwise.} \end{cases}$$

On the other hand, putting $W_n = \operatorname{Ker}\left(G_n \twoheadrightarrow G_{n-1}\right)$, one calculates

$$\operatorname{Tr}\left(\operatorname{Ind}_{H_{n-1}}^{G_{n-1}}(\eta_{n-1})(g)\right)$$
$$= \begin{cases} p^{n-1} - p^{n-2} & \text{if } g \in W_n \\ -p^{n-2} & \text{if } gW_n = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \text{ with } p^{n-2}\big\|b \\ 0 & \text{otherwise;} \end{cases}$$

this is numerically equal to the previous trace divided by p, so we are done.

Remarks. (i) The general case where $\Delta \subset \mathbb{F}_p^\times$ can be treated as follows. Using the notation $G_n^{(\Delta)} = H_n \rtimes \Upsilon_n^{(\Delta)}$ with $\Upsilon_n^{(\Delta)} =$

$\Delta \times (1+p\mathbb{Z}_p)/(1+p^n\mathbb{Z}_p)$, the square

$$\begin{array}{ccc} \underline{\mathrm{Rep}}\left(G_n^{(\Delta)}\right) & \overset{\mathrm{Ind}_{\Delta}^{\mathbb{F}_p^\times}}{\longrightarrow} & \underline{\mathrm{Rep}}\left(G_n^{(\mathbb{F}_p^\times)}\right) \\ \big\downarrow \mathrm{Tr} & & \big\downarrow \mathrm{Tr} \\ R_p\left(G_n^{(\Delta)}\right) & \overset{\left(\mathrm{Ind}_{\Delta}^{\mathbb{F}_p^\times}\right)_*}{\longrightarrow} & R_p\left(G_n^{(\mathbb{F}_p^\times)}\right) \end{array}$$

is commutative, since $G_n^{(\Delta)}$ is normal inside $G_n^{(\mathbb{F}_p^\times)}$ with quotient $\cong \mathbb{F}_p^\times/\Delta$.

(ii) However, $\mathrm{Ind}_{H_m}^{G_m^{(\mathbb{F}_p^\times)}}(\eta_m) = \mathrm{Ind}_{\Delta}^{\mathbb{F}_p^\times}(\mathrm{Ind}_{H_m}^{G_m^{(\Delta)}}(\eta_m))$ for $m=n$ and $m=n-1$; thus, the assertion in $R_p\left(G_n^{(\Delta)}\right)$ can be deduced from its cousin in $R_p(G_n^{(\mathbb{F}_p^\times)})$.

(iii) Finally, if β is a non-trivial character on Υ_n then, amongst the virtual characters, one has $\psi_p \circ \mathrm{Tr}\,(\sigma\otimes\beta)(g) = \mathrm{Tr}\,(\sigma\otimes\beta)(g^p) = \beta(g)^p \times \psi_p \circ \mathrm{Tr}\,(\sigma)(g)$; in particular, this allows us to incorporate β into our previous formulae.

Corollary B.2. *For all $n \geq 2$, one has $\psi_p \circ \mathrm{Tr}\left(\mathrm{reg}_{G_n}\right) = p^2 \times \mathrm{Tr}\left(\mathrm{reg}_{G_{n-1}}\right)$.*

Proof. We show it first for $G_n = \mathbb{Z}_p/p^n\mathbb{Z}_p \rtimes (\mathbb{Z}_p/p^n\mathbb{Z}_p)^\times$, i.e., for $\Delta = \mathbb{F}_p^\times$. The regular representation on G_n decomposes into

$$\mathrm{reg}_{G_n} \cong \mathrm{reg}_{\Upsilon_n} \oplus \bigoplus_{k=1}^{n} \bigoplus_{\beta\in\mathfrak{X}(\Upsilon_n/\Upsilon_k)} \left(\mathrm{Ind}_{H_k}^{G_k}(\eta_k)\otimes\beta\right)^{p^k-p^{k-1}},$$

where $\mathfrak{X}(-)$ denotes the character group $\mathrm{Hom}_{\mathrm{cont}}(-,\mathbb{G}_m)$; it follows that

$$\mathrm{Tr}\left(\mathrm{reg}_{G_n}\right) = \sum_{\alpha\in\mathfrak{X}(\Upsilon_n)} \alpha + \sum_{k=1}^{n} \sum_{\beta\in\mathfrak{X}(\Upsilon_n/\Upsilon_k)} (p^k-p^{k-1}) \times \mathrm{Tr}\left(\mathrm{Ind}_{H_k}^{G_k}(\eta_k)\otimes\beta\right).$$

Upon applying the previous proposition, $\psi_p \circ \mathrm{Tr}\left(\mathrm{reg}_{G_n}\right)$ must then equal

$$\sum_{\alpha\in\mathfrak{X}(\Upsilon_n)}\alpha^p+\sum_{k=1}^{n}\sum_{\beta\in\mathfrak{X}(\Upsilon_n/\Upsilon_k)}(p^k-p^{k-1})\times p\cdot\mathrm{Tr}\left(\mathrm{Ind}_{H_{k-1}}^{G_{k-1}}(\eta_{k-1})\otimes\beta^p\right).$$

Clearly, $\sum_{\alpha\in\mathfrak{X}(\Upsilon_n)}\alpha^p=p\cdot\sum_{\alpha\in\mathfrak{X}(\Upsilon_{n-1})}\alpha=p\cdot\mathrm{Tr}(\mathrm{reg}_{\Upsilon_{n-1}})$, whilst

$$\sum_{\beta\in\mathfrak{X}(\Upsilon_n/\Upsilon_1)}(p-1)\times p\cdot\mathrm{Tr}\left(\mathrm{Ind}_{H_0}^{G_0}(\eta_0)\otimes\beta^p\right)=(p^2-p)\times\mathrm{Tr}\big(\mathrm{reg}_{\Upsilon_{n-1}}\big).$$

As a direct consequence, plugging these numbers back into our formula:

$$\begin{aligned}\psi_p\circ\mathrm{Tr}\left(\mathrm{reg}_{G_n}\right)&=p^2\times\mathrm{Tr}\left(\mathrm{reg}_{\Upsilon_{n-1}}\right)\\&\quad+\sum_{k=2}^{n}\sum_{\beta\in\mathfrak{X}(\Upsilon_n/\Upsilon_k)}(p^{k+1}-p^k)\times\mathrm{Tr}\left(\mathrm{Ind}_{H_{k-1}}^{G_{k-1}}(\eta_{k-1})\otimes\beta^p\right)\\=p^2\Bigg(\mathrm{Tr}\left(\mathrm{reg}_{\Upsilon_{n-1}}\right)&+\sum_{k=1}^{n-1}\sum_{\beta\in\mathfrak{X}(\Upsilon_n/\Upsilon_{k+1})}(p^k-p^{k-1})\times\mathrm{Tr}\left(\mathrm{Ind}_{H_k}^{G_k}(\eta_k)\otimes\beta^p\right)\Bigg).\end{aligned}$$

However,

$$\sum_{\beta\in\mathfrak{X}(\Upsilon_n/\Upsilon_{k+1})}\mathrm{Tr}\left(\sigma\otimes\beta^p\right)=\sum_{\beta\in\mathfrak{X}(\Upsilon_{n-1}/\Upsilon_k)}\mathrm{Tr}\left(\sigma\otimes\beta\right);$$

thence,

$$\psi_p\circ\mathrm{Tr}\left(\mathrm{reg}_{G_n}\right)=p^2\left(\mathrm{Tr}\big(\mathrm{reg}_{\Upsilon_{n-1}}\big)+\cdots\right)=p^2\times\mathrm{Tr}\big(\mathrm{reg}_{G_{n-1}}\big).\quad\square$$

Remark. When Δ is a proper subgroup of $\mathbb{F}_p^\times$, we use the commutativity of

$$\begin{array}{ccc}\underline{\mathrm{Rep}}\big(G_n^{(\Delta)}\big) & \xrightarrow{\mathrm{Ind}_\Delta^{\mathbb{F}_p^\times}} & \underline{\mathrm{Rep}}\big(G_n^{(\mathbb{F}_p^\times)}\big)\\ \big\downarrow{\scriptstyle\mathrm{Tr}} & & \big\downarrow{\scriptstyle\mathrm{Tr}}\\ R_p\big(G_n^{(\Delta)}\big) & \xrightarrow{\left(\mathrm{Ind}_\Delta^{\mathbb{F}_p^\times}\right)_*} & R_p\big(G_n^{(\mathbb{F}_p^\times)}\big)\end{array}$$

together with the fact $\mathrm{reg}_{G_n^{(\Delta)}}$ occurs as a direct summand in $\mathrm{reg}_{G_n^{(\mathbb{F}_p^\times)}}$.

B.2. Representations of the Heisenberg group. Consider the group $\mathcal{H}_n = \mathrm{GL}\,(3, \mathbb{Z}/p^n\mathbb{Z}) \cap \begin{pmatrix} 1 & \star & \star \\ 0 & 1 & \star \\ 0 & 0 & 1 \end{pmatrix}$ of order $\#\mathcal{H}_n = p^{3n}$. For each integer m in the range $0 \leq m \leq n$, one defines subgroups

$$\mathcal{U}_n^{(m)} := \begin{pmatrix} 1 & \star & \star \\ 0 & 1 & p^m\mathbb{Z}/p^n \\ 0 & 0 & 1 \end{pmatrix},$$

$$\mathcal{V}_n^{(m)} := \left[\mathcal{U}_n^{(m)}, \mathcal{U}_n^{(m)}\right] = \begin{pmatrix} 1 & 0 & p^m\mathbb{Z}/p^n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

In particular, if we fix a character $\chi : \mathcal{U}_n^{(m)} \to \mathbb{C}^\times$, then $\rho_n^{(m,\chi)} := \mathrm{Ind}_{\mathcal{U}_n^{(m)}}^{\mathcal{H}_n}(\chi)$ furnishes us with an $\mathcal{H}_n$-representation, of degree equal to $[\mathcal{H}_n : \mathcal{U}_n^{(m)}] = p^m$. Furthermore, assuming that

$$\chi : \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \longmapsto \zeta,$$

where $\zeta \in \mu_{p^m} - \mu_{p^{m-1}}$ is a primitive p^mth root of unity, it follows from an application of Mackey's irreducibility criterion for characters that $\rho_n^{(m,\chi)}$ is irreducible.

Proposition B.3. If $0 \leq m \leq n$ and $\chi : \mathcal{U}_n^{(m)} \to \mathbb{C}^\times$ is as above, then

$$\psi_p \circ \mathrm{Tr}\left(\mathrm{Ind}_{\mathcal{U}_n^{(m)}}^{\mathcal{H}_n}(\chi)\right) = p \cdot \mathrm{Tr}\left(\mathrm{Ind}_{\mathcal{U}_{n-1}^{(m-1)}}^{\mathcal{H}_{n-1}}(\chi^p)\right)$$

inside the virtual ring $R_p(\mathcal{H}_n)$.

Proof. If

$$g = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

with $a, b, c \in \mathbb{Z}/p^n\mathbb{Z}$, we just write $g = (a, b, c)$. The conjugacy classes of $\mathcal{H}_n$ are given by $(a, b, \mathbb{Z}/p^n\mathbb{Z})$ with $a \neq 0$ or $b \neq 0$, and also by

$(0,0,c)$ for $c \in \mathbb{Z}/p^n\mathbb{Z}$. The individual elements $x_i = (0,i,0)$ with $i \in \{0,1,\dots,p^m-1\}$ form a set of coset representatives for $\mathcal{H}_n/\mathcal{U}_n^{(m)}$.

Sub-case (i). The element $x \in (a,b,\mathbb{Z}/p^n\mathbb{Z})$ is such that $b \notin p^m\mathbb{Z}/p^n\mathbb{Z}$; here $x_i x x_i^{-1} \notin \mathcal{U}_n^{(m)}$ for all i, so $\operatorname{Tr}(\rho_n^{(m,\chi)}(x)) = 0$.

Sub-case (ii). The element $x \in (a,b,\mathbb{Z}/p^n\mathbb{Z})$ is such that $b \in p^m\mathbb{Z}/p^n\mathbb{Z}$ but $a \notin p^m\mathbb{Z}/p^n\mathbb{Z}$; if we write $x = (a,b,c)$, then $x_i x x_i^{-1} = (a,b,c)(0,0,-ai)$ in which case

$$\operatorname{Tr}\left(\rho_n^{(m,\chi)}(x)\right) = \chi(a,b,c) \times \sum_{i=0}^{p^m-1} \chi(0,0,i)^a = 0.$$

Sub-case (iii). The element $x \in (a,b,\mathbb{Z}/p^n\mathbb{Z})$ with $a,b \in p^m\mathbb{Z}/p^n\mathbb{Z}$; if we again write $x = (a,b,c)$, as before, $x_i x x_i^{-1} = (a,b,c)(0,0,-ai)$; thence,

$$\operatorname{Tr}\left(\rho_n^{(m,\chi)}(x)\right) = \chi(a,b,c) \times \sum_{i=0}^{p^m-1} \chi(0,0,i)^a = p^m \times \chi(a,b,c).$$

Sub-case (iv). The element $x \in Z(\mathcal{H}_n) = (0,0,\mathbb{Z}/p^n\mathbb{Z})$, so $x_i x x_i^{-1} = x$, and consequently, $\operatorname{Tr}(\rho_n^{(m,\chi)}(x)) = p^m \times \chi(x)$.

In summary, we have thus far established

$$\operatorname{Tr}\left(\rho_n^{(m,\chi)}(a,b,c)\right) = \begin{cases} 0 & \text{if either } a \text{ or } b \notin p^m\mathbb{Z}/p^n\mathbb{Z} \\ p^m\chi(a,b,c) & \text{otherwise.} \end{cases}$$

However, χ^p will determine a one-dimensional character on $\mathcal{U}_{n-1}^{(m-1)}/\mathcal{V}_{n-1}^{(m-1)}$, and certainly $\chi^p(0,0,1) \in \mu_{p^{m-1}} - \mu_{p^{m-2}}$. By the previous discussion,

$$\psi_p \circ \operatorname{Tr}\left(\rho_n^{(m,\chi)}(a,b,c)\right) = \begin{cases} 0 & \text{if either } a \text{ or } b \notin p^{m-1}\mathbb{Z}/p^n\mathbb{Z} \\ p^m\chi^p(a,b,c) & \textit{otherwise,} \end{cases}$$

and the result now follows. $\square$

Corollary B.4. *For all $n \geq 2$, one has $\psi_p \circ \operatorname{Tr}\left(\operatorname{reg}_{\mathcal{H}_n}\right) = p^3 \times \operatorname{Tr}\left(\operatorname{reg}_{\mathcal{H}_{n-1}}\right)$.*

Proof. Let $\overline{\mathcal{U}}^{(m)}_{n,\mathrm{conj}}$ be a set of representative characters χ on the group $\mathcal{U}^{(m)}_n$, which yield irreducible (pairwise) non-isomorphic $\rho_n^{(m,\chi)}$'s. We have $\#\overline{\mathcal{U}}^{(m)}_{n,\mathrm{conj}} = \phi(p^{n-m}) \times p^n$. Moreover, the map sending $\chi \mapsto \chi^p$, induces a degree p covering $\overline{\mathcal{U}}^{(m)}_{n,\mathrm{conj}} \twoheadrightarrow \overline{\mathcal{U}}^{(m-1)}_{n-1,\mathrm{conj}}$ on these representative character sets.

Since $\mathrm{reg}_{\mathcal{H}_n} \cong \mathrm{reg}_{\mathcal{H}_n^{\mathrm{ab}}} \oplus \bigoplus_{m=1}^n \bigoplus_{\chi\in\overline{\mathcal{U}}^{(m)}_{n,\mathrm{conj}}} (\mathrm{Ind}^{\mathcal{H}_n}_{\mathcal{U}_n^{(m)}}(\chi))^{p^m}$, its trace equals

$$\mathrm{Tr}\left(\mathrm{reg}_{\mathcal{H}_n}\right) = \sum_{\psi\in\widehat{\mathcal{H}_n^{\mathrm{ab}}}} \psi + \sum_{m=1}^{n} \sum_{\chi\in\overline{\mathcal{U}}^{(m)}_{n,\mathrm{conj}}} p^m \times \mathrm{Tr}\left(\mathrm{Ind}^{\mathcal{H}_n}_{\mathcal{U}_n^{(m)}}(\chi)\right). \tag{B.1}$$

Hitting this with the pth Adams operator, and applying Proposition 4.2,

$$\begin{aligned}
\psi_p \circ \mathrm{Tr}\left(\mathrm{reg}_{\mathcal{H}_n}\right) &= \sum_{\psi\in\widehat{\mathcal{H}_n^{\mathrm{ab}}}} \psi^p + \sum_{m=1}^{n} \sum_{\chi\in\overline{\mathcal{U}}^{(m)}_{n,\mathrm{conj}}} p^m \times p\cdot \mathrm{Tr}\left(\mathrm{Ind}^{\mathcal{H}_{n-1}}_{\mathcal{U}_{n-1}^{(m-1)}}(\chi^p)\right)\\
&= \frac{\#\mathcal{H}_n^{\mathrm{ab}}}{\#\mathcal{H}_{n-1}^{\mathrm{ab}}} \times \sum_{\psi'\in\widehat{\mathcal{H}_{n-1}^{\mathrm{ab}}}} \psi' + p^2 \times \frac{\#\overline{\mathcal{U}}^{(1)}_{n,\mathrm{conj}}}{\#\mathcal{H}_{n-1}^{\mathrm{ab}}} \times \mathrm{Tr}\big(\mathrm{reg}_{\mathcal{H}_{n-1}^{\mathrm{ab}}}\big)\\
&\quad + \sum_{m'=1}^{n-1} \sum_{\chi\in\overline{\mathcal{U}}^{(m'+1)}_{n,\mathrm{conj}}} p^{m'+2} \times \mathrm{Tr}\left(\mathrm{Ind}^{\mathcal{H}_{n-1}}_{\mathcal{U}_{n-1}^{(m')}}(\chi^p)\right).
\end{aligned}$$

The following identities are straightforward to derive:

- $\#\mathcal{H}_n^{\mathrm{ab}} = \big[\mathcal{U}_n^{(0)} : \mathcal{V}_n^{(0)}\big] = p^{2n} = p^2 \times \big[\mathcal{U}_{n-1}^{(0)} : \mathcal{V}_{n-1}^{(0)}\big] = p^2 \times \#\mathcal{H}_{n-1}^{\mathrm{ab}}$;
- $\#\overline{\mathcal{U}}^{(1)}_{n,\mathrm{conj}} = \phi(p^{n-1}) \times p^n = (p-1) \times \#\mathcal{H}_{n-1}^{\mathrm{ab}}$;
- $\#\overline{\mathcal{U}}^{(m'+1)}_{n,\mathrm{conj}} = \phi(p^{n-m'-1}) \times p^n = p \times \#\overline{\mathcal{U}}^{(m')}_{n-1,\mathrm{conj}}$.

Substituting these back into our previous expression, one concludes that

$$\begin{aligned}
&\psi_p \circ \mathrm{Tr}\left(\mathrm{reg}_{\mathcal{H}_n}\right)\\
&\qquad = p^2 \times \sum_{\psi'\in\widehat{\mathcal{H}_{n-1}^{\mathrm{ab}}}} \psi' + p^2 \times \big(p-1\big) \times \mathrm{Tr}\big(\mathrm{reg}_{\mathcal{H}_{n-1}^{\mathrm{ab}}}\big)
\end{aligned}$$

$$+\sum_{m'=1}^{n-1}\sum_{\chi'\in\overline{\mathcal{U}}_{n-1,\mathrm{conj}}^{(m')}} p^{m'+2}\times\frac{\#\overline{\mathcal{U}}_{n,\mathrm{conj}}^{(m'+1)}}{\#\overline{\mathcal{U}}_{n-1,\mathrm{conj}}^{(m')}}\times\mathrm{Tr}\left(\mathrm{Ind}_{\mathcal{U}_{n-1}^{(m')}}^{\mathcal{H}_{n-1}}(\chi')\right)$$

$$=p^2\times\big(1+(p-1)\big)\sum_{\psi'\in\widehat{\mathcal{H}_{n-1}^{\mathrm{ab}}}}\psi'+\sum_{m'=1}^{n-1}\sum_{\chi'\in\overline{\mathcal{U}}_{n-1,\mathrm{conj}}^{(m')}} p^{m'+3}\times\mathrm{Tr}\left(\mathrm{Ind}_{\mathcal{U}_{n-1}^{(m')}}^{\mathcal{H}_{n-1}}(\chi')\right),$$

which coincides with $p^3\times\mathrm{Tr}\,(\mathrm{reg}_{\mathcal{H}_{n-1}})$ by (B.1). □

Acknowledgments. Both authors are extremely grateful to the Australian Research Council for their support, as part of an ARC-DP1092496 grant. They are also indebted to the hospitality of University of Warwick (where the work was completed), and especially to David Loeffler and John Cremona. They are also thankful to the anonymous referee for the corrections and comments on an earlier version of the paper.

REFERENCES

1. John Coates, Takako Fukaya, Kazuya Kato and Ramdorai Sujatha, *Root numbers, Selmer groups, and non-commutative Iwasawa theory*, J. Alg. Geom. **19** (2010), 19–97.

2. John Coates, Takako Fukaya, Kazuya Kato, Ramdorai Sujatha and Otmar Venjakob, *The* GL_2 *main conjecture for elliptic curves without complex multiplication*, Publ. Math. Inst. Sci. **101** (2005), 163–208.

3. John Coates and Susan Howson, *Euler characteristics and elliptic curves*, II, J. Math. Soc. Japan **53** (2001), 175–235.

4. John Coates, Peter Schneider and Ramdorai Sujatha, *Links between cyclotomic and* GL_2 *Iwasawa theory*, Doc. Math. (2003), 187–215 (electronic).

5. D. Delbourgo and A. Lei, *Estimating the growth in Mordell-Weil ranks and Shafarevich-Tate groups over Lie extensions*, Ramanujan J., to appear.

6. John Dixon, Marcus du Sautoy, Avinoam Mann and Dan Segal, *Analytic pro-p groups*, Second edition, Cambr. Stud. Adv. Math. **61**, Cambridge University Press, Cambridge, 1999.

7. Vladimir Dokchitser, *Root numbers of non-abelian twists of elliptic curves*, Proc. Lond. Math. Soc. **91** (2005), 300–324.

8. Jon González-Sánchez and Benjamin Klopsch, *Analytic pro-p groups of small dimensions*, J. Group Theory **12** (2009), 711–734.

9. Yoshitaka Hachimori and Otmar Venjakob, *Completely faithful Selmer groups over Kummer extensions*, Doc. Math. (2003), 443–478 (electronic).

10. Benjamin Klopsch, *Pro-p groups with linear subgroup growth*, Math. Z. **245** (2003), 335–370.

11. Kazuo Matsuno, *Finite Λ-submodules of Selmer groups of abelian varieties over cyclotomic $\mathbb{Z}_p$-extensions*, J. Num. Theor. **99** (2003), 415–443.

12. Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

13. Jürgen Ritter and Alfred Weiss, *Toward equivariant Iwasawa theory. II*, Indag. Math. **15** (2004), 549–572.

14. ______, *Toward equivariant Iwasawa theory*, III, Math. Ann. **336** (2006), 27–49.

15. Victor Snaith, *Explicit Brauer induction, with applications to algebra and number theory*, Cambr. Stud. Adv. Math. **40**, Cambridge University Press, Cambridge, 1994.

The Department of Mathematics, University of Waikato, Private Bag 3105, Hamilton 3240, New Zealand
Email address: **delbourg@waikato.ac.nz**

Département de mathématiques et de statistique, Université Laval, Pavillon Alexandre-Vachon, 1045 avenue de la Médecine, Québec QC, Canada G1V 0A6
Email address: **antonio.lei@mat.ulaval.ca**