RANDOM MAXIMAL ISOTROPIC SUBSPACES AND SELMER GROUPS

BJORN POONEN AND ERIC RAINS

Abstract. We first develop a notion of quadratic form on a locally compact abelian group. Under suitable hypotheses, we construct a probability measure on the set of closed maximal isotropic subspaces of a locally compact quadratic space over $\mathbb{F}_p$. A random subspace chosen with respect to this measure is discrete with probability 1, and the dimension of its intersection with a fixed compact open maximal isotropic subspace is a certain nonnegative-integer-valued random variable.

We then prove that the p-Selmer group of an elliptic curve is naturally the intersection of a discrete maximal isotropic subspace with a compact open maximal isotropic subspace in a locally compact quadratic space over $\mathbb{F}_p$. By modeling the first subspace as being random, we can explain the known phenomena regarding distribution of Selmer ranks, such as the theorems of Heath-Brown and Swinnerton-Dyer for 2-Selmer groups in certain families of quadratic twists, and the average size of 2- and 3-Selmer groups as computed by Bhargava and Shankar. The only distribution on Mordell-Weil ranks compatible with both our random model and Delaunay's heuristics for p-torsion in Shafarevich-Tate groups is the distribution in which 50% of elliptic curves have rank 0, and 50% have rank 1.

We generalize many of our results to abelian varieties over global fields. Along the way, we give a general formula relating self cup products in cohomology to connecting maps in nonabelian cohomology, and apply it to obtain a formula for the self cup product associated to the Weil pairing.

1. Introduction

1.1. **Selmer groups.** D. R. Heath-Brown [HB93, HB94] and P. Swinnerton-Dyer [SD08] obtained the distribution for the nonnegative integer $s(E)$ defined as the $\mathbb{F}_2$-dimension of the 2-Selmer group $\operatorname{Sel}_2(E)$ minus the dimension of the rational 2-torsion group $E(\mathbb{Q})[2]$, as E varies over quadratic twists of certain elliptic curves over $\mathbb{Q}$. The distribution was the one for which

$$\operatorname{Prob}(s(E)=d) = \left(\prod_{j\ge 0}(1+2^{-j})^{-1}\right)\left(\prod_{j=1}^{d}\frac{2}{2^j-1}\right).$$

In [HB94], it was reconstructed from the moments of $2^{s(E)}$; in [SD08], it arose as the stationary distribution for a Markov process.

Our work begins with the observation that this distribution coincides with a distribution arising naturally in combinatorics, namely, the limit as $n\to\infty$ of the distribution of $\dim(Z\cap W)$ where Z and W are random maximal isotropic subspaces inside a hyperbolic

Date: September 21, 2010.

2000 *Mathematics Subject Classification.* Primary 11G10; Secondary 11G05, 11G30, 14G25, 14K15.

Key words and phrases. Selmer group, Shafarevich-Tate group, maximal isotropic, quadratic space, Weil pairing, theta characteristic, self cup product.

B. P. was partially supported by NSF grant DMS-0841321.

quadratic space of dimension $2n$ over $\mathbb{F}_2$. Here it is essential that the maximal isotropic subspaces be isotropic not only for the associated symmetric bilinear pairing, but also for the quadratic form; otherwise, one would obtain the wrong distribution. That such a quadratic space might be relevant is suggested already by the combinatorial calculations in [HB94].

Is it just a coincidence, or is there some direct relation between Selmer groups and intersections of maximal isotropic subgroups? Our answer is that $\operatorname{Sel}_2(E)$ is naturally the intersection of two maximal isotropic subspaces in an *infinite-dimensional* quadratic space V over $\mathbb{F}_2$. The fact that it could be obtained as an intersection of two subspaces that were maximal isotropic for a pairing induced by a Weil pairing is implicit in standard arithmetic duality theorems.

To make sense of our answer, we develop a theory of quadratic forms on locally compact abelian groups. The locally compact abelian group V in the application is the restricted direct product of the groups $\mathrm{H}^1(\mathbb{Q}_p, E[2])$ for $p \leq \infty$ with respect to the subgroups of unramified classes. The quadratic form Q is built out of D. Mumford's Heisenberg group construction. The arithmetic duality theorems are applied to show that the images of the compact group $\prod_{p\leq\infty} E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$ and the discrete group $\mathrm{H}^1(\mathbb{Q}, E[2])$ are maximal isotropic in (V, Q). Their intersection is $\operatorname{Sel}_2(E)$.

In fact, we work in a more general context, with $[2]\colon E \to E$ replaced by any self-dual isogeny $\lambda\colon A \to \widehat{A}$ coming from a line sheaf on an abelian variety A over a global field k. (See Theorem 6.8.) In this setting, we have a surprise: it is not $\operatorname{Sel}_\lambda(A)$ itself that is the intersection of maximal isotropic subgroups, but its quotient by $\text{Ш}^1(k, A[\lambda])$, and the latter group is sometimes nonzero.

The resulting prediction for $\dim_{\mathbb{F}_p} \operatorname{Sel}_p(E)$ does not duplicate C. Delaunay's prediction for $\dim_{\mathbb{F}_p} \text{Ш}(E)[p]$ [Del01, Del07]. Instead the predictions complement each other: we prove that the only distribution on $\operatorname{rk} E(\mathbb{Q})$ compatible with both predictions is that for which $\operatorname{rk} E(\mathbb{Q})$ is 0 or 1, with probability 1/2 each. (A related result, that for $p = 2$ the Sel_2 prediction and the rank prediction together imply the $\text{Ш}[2]$ predictions for rank 0 and 1, had been observed at the end of [Del07].)

1.2. **Self cup product of the Weil pairing.** A secondary goal of our paper is to answer a question of B. Gross about the self cup product associated to the Weil pairing on the 2-torsion of the Jacobian $A := \operatorname{Jac} X$ of a curve X. The Weil pairing

$$e_2\colon A[2] \times A[2] \to \mathbb{G}_m$$

induces a symmetric bilinear pairing

$$\langle\ ,\ \rangle\colon \mathrm{H}^1(A[2]) \times \mathrm{H}^1(A[2]) \to \mathrm{H}^2(\mathbb{G}_m).$$

We prove the identity $\langle x, x\rangle = \langle x, c_{\mathcal{T}}\rangle$, where $c_{\mathcal{T}}$ is a particular canonical element of $\mathrm{H}^1(A[2])$. Namely, $c_{\mathcal{T}}$ is the class of the torsor under $A[2]$ parametrizing the theta characteristics on X.

We have been vague about the field of definition of our curve; in fact, it is not too much harder to work over an arbitrary base scheme. (See Theorem 5.9.) Moreover, we prove a version with Jacobians replaced by arbitrary abelian schemes. (See Theorem 5.4.)

1.3. **Other results.** One ingredient common to the proofs of Theorems 6.8 and 5.4 is a general result about cohomology, Theorem 3.5, which reinterprets the self cup product map $H^1(M) \to H^2(M \otimes M)$ as the connecting map for a canonical central extension of M

by $M \otimes M$. Its proof can be read with group cohomology in mind, but we prove it for an arbitrary site since later we need it for fppf cohomology. Its application towards Theorem 6.8 goes through another cohomological result, Proposition 3.9, which shows that the connecting homomorphism $\mathrm{H}^1(C) \to \mathrm{H}^2(A)$ for a central extension is quadratic, and which computes the associated bilinear pairing.

We also prove some results that help us apply Theorems 6.8 and 5.4: Section 4 proves results about Shafarevich-Tate groups of finite group schemes that are relevant to both theorems, and Section 5.5 gives criteria for the vanishing of $c_{\mathcal{T}}$.

The two main threads of our article come together in Remark 6.10 and Example 6.14, in which we predict the distribution of the 2-Selmer group of a 2-dimensional Jacobian.

2. Random maximal isotropic subspaces

2.1. **Quadratic modules.** See [Sch85, 1.§6 and 5.§1] for the definitions of this section. Let V and T be abelian groups. Call a function $Q\colon V \to T$ a (T-valued) quadratic form if Q is a quadratic map (i.e., the symmetric pairing $\langle\ ,\ \rangle\colon V \times V \to T$ sending (x,y) to $Q(x+y) - Q(x) - Q(y)$ is bilinear) and $Q(av) = a^2 Q(v)$ for every $a \in \mathbb{Z}$ and $v \in V$. Then (V,Q) is called a quadratic module.

Remark 2.1. A quadratic map Q satisfying the identity $Q(-v) = Q(v)$ is a quadratic form. (Taking $x = y = 0$ shows that $Q(0) = 0$, and then $Q(av + (-v)) - Q(av) - Q(-v) = a(Q(0) - Q(v) - Q(-v))$ computes $Q(av)$ for other $a \in \mathbb{Z}$ by induction.)

Lemma 2.2. *Let (V,Q) be a quadratic module. Suppose that $v \in V$ and $\ell \in \mathbb{Z}$ are such that $\ell v = 0$. If ℓ is odd, then $\ell Q(v) = 0$. If ℓ is even, then $2\ell Q(v) = 0$.*

Proof. We have $\ell^2 Q(v) = Q(\ell v) = 0$, and $2\ell Q(v) = \ell\langle v, v\rangle = \langle \ell v, v\rangle = 0$. □

Given a subgroup $W \subseteq V$, let $W^\perp := \{v \in V : \langle v, w\rangle = 0 \text{ for all } w \in W\}$. Call W a maximal isotropic subgroup of (V,Q) if $W^\perp = W$ and $Q|_W = 0$. Let $\mathcal{I}_V$ be the set of maximal isotropic subgroups of (V,Q).

Remark 2.3. Say that W is maximal isotropic *for the pairing* $\langle\ ,\ \rangle$ if $W^\perp = W$. If $W = 2W$ or $T[2] = 0$, then $W^\perp = W$ implies $Q|_W = 0$, but in general $Q|_W = 0$ is a nonvacuous extra condition.

Call a quadratic module (V,Q) nondegenerate if Q is $\mathbb{R}/\mathbb{Z}$-valued and V is finite (we will relax this condition in Section 2.4) and the homomorphism $V \to V^* := \operatorname{Hom}(V, \mathbb{R}/\mathbb{Z})$ defined by $v \mapsto (w \mapsto \langle v, w\rangle)$ is an isomorphism. Call (V,Q) weakly metabolic if it is nondegenerate and contains a maximal isotropic subgroup. (Metabolic entails the additional condition that the subgroup be a direct summand.)

Remark 2.4. Suppose that (V,Q) is a nondegenerate quadratic module, and X is an isotropic subgroup of (V,Q). Then

(a) The quotient $X^\perp/X$ is a nondegenerate quadratic module under the quadratic form Q_X induced by Q.
(b) If $W \in \mathcal{I}_V$, then $(W \cap X^\perp) + X \in \mathcal{I}_V$, and $((W \cap X^\perp) + X)/X \in \mathcal{I}_{X^\perp/X}$. Let $\pi^{V, X^\perp/X}(W)$ denote this last subgroup, which is the image of $W \cap X^\perp$ in $X^\perp/X$.

Remark 2.5. If (V, Q) is a nondegenerate quadratic module with $\#V < \infty$, the obstruction to V being weakly metabolic is measured by an abelian group $\mathrm{WQ} \simeq \bigoplus_p \mathrm{WQ}(p)$ called the Witt group of nondegenerate quadratic forms on finite abelian groups [Sch85, 5.§1]. The obstruction for (V, Q) equals the obstruction for $X^\perp/X$ for any isotropic subgroup X of (V, Q) (cf. [Sch85, Lemma 5.1.3]).

2.2. **Counting subspaces.**

Proposition 2.6. *Let (V, Q) be a $2n$-dimensional weakly metabolic quadratic space over $F := \mathbb{F}_p$, with Q taking values in $\frac{1}{p}\mathbb{Z}/\mathbb{Z} \simeq F$.*

(a) *All fibers of $\pi^{V, X^\perp/X} \colon \mathcal{I}_V \to \mathcal{I}_{X^\perp/X}$ have size $\prod_{i=1}^{\dim X}(p^{n-i}+1)$.*
(b) *We have $\#\mathcal{I}_V = \prod_{j=0}^{n-1}(p^j+1)$.*
(c) *Let W be a fixed maximal isotropic subspace of V. Let X_n be the random variable $\dim(Z \cap W)$, where Z is chosen uniformly at random from $\mathcal{I}_V$. Then X_n is a sum of independent Bernoulli random variables $B_1, \ldots, B_n$ where B_i is 1 with probability $1/(p^{i-1}+1)$ and 0 otherwise.*
(d) *For $0 \le d \le n$, let $a_{d,n} := \operatorname{Prob}(X_n = d)$, and let $a_d := \lim_{n\to\infty} a_{d,n}$. Then*
$$\sum_{d \ge 0} a_{d,n} z^d = \prod_{i=0}^{n-1} \frac{z+p^i}{1+p^i} = \prod_{i=0}^{n-1} \frac{1+p^{-i}z}{1+p^{-i}}.$$
$$\sum_{d \ge 0} a_d z^d = \prod_{i=0}^{\infty} \frac{1+p^{-i}z}{1+p^{-i}}.$$

(e) *For $0 \le d \le n$, we have*
$$a_{d,n} = \prod_{j=0}^{n-1}(1+p^{-j})^{-1} \prod_{j=1}^{d} \frac{p}{p^j-1} \prod_{j=0}^{d-1}(1-p^{j-n}).$$
(f) *For $d \ge 0$, we have*
$$a_d = c \prod_{j=1}^{d} \frac{p}{p^j-1},$$
where
$$c := \prod_{j \ge 0}(1+p^{-j})^{-1} = \frac{1}{2}\prod_{i \ge 0}(1-p^{-(2i+1)}).$$

Proof.

(a) Choose a full flag in X; then $\pi^{V, X^\perp/X}$ factors into $\dim X$ maps of the same type, so we reduce to the case $\dim X = 1$. Write $X = Fv$ with $v \in V$. For $Z \in \mathcal{I}_V$, let $\overline{Z}$ be its image in $\mathcal{I}_{X^\perp/X}$. There is a bijection $\{Z \in \mathcal{I}_V : v \in Z\} \to \mathcal{I}_{X^\perp/X}$ defined by $Z \mapsto \overline{Z} = Z/X$.

Fix $\overline{W} \in \mathcal{I}_{X^\perp/X}$, and let $W \in \mathcal{I}_V$ be such that $\overline{W} = W/X$. We want to show that $\#\{Z \in \mathcal{I}_V : \overline{Z} = \overline{W}\} = p^{n-1}+1$. This follows once we show that the map
$$\{Z \in \mathcal{I}_V : \overline{Z} = \overline{W}\} \to \{\text{codimension 1 subspaces of } W\} \cup \{W\}$$
$$Z \mapsto Z \cap W$$

is a bijection. If $v \in Z$, then $\overline{Z} = \overline{W}$ implies that $Z = W$. If $v \notin Z$, then $\overline{Z} = \overline{W}$ implies that $Z \cap W$ has codimension 1 in W. Conversely, for a given W_1 of codimension 1 in W, the $Z \in \mathcal{I}_V$ containing W_1 are in bijection with the maximal isotropic subspaces of the weakly metabolic 2-dimensional space $W_1^\perp/W_1$, which is isomorphic to (F^2, xy), so there are two such Z: one of them is W, and the other satisfies $Z \cap W = W_1$ and $\overline{Z} = \overline{W}$. Thus we have the bijection.

(b) Apply (a) to a maximal isotropic X.

(c) If $n > 0$, fix a nonzero v in W, and define $\overline{Z}$ as in the proof of (a). Then

$$\dim Z \cap W = \dim \overline{Z} \cap \overline{W} + \delta_{v \in Z},$$

where $\delta_{v \in W}$ is 1 if $v \in Z$ and 0 otherwise. The term $\dim \overline{Z} \cap \overline{W}$ has the distribution X_{n-1}. Conditioned on the value of $\overline{Z}$, the term $\delta_{v \in Z}$ is 1 with probability $1/(p^{n-1}+1)$ and 0 otherwise, since there are $p^{n-1}+1$ subspaces $Z \in \mathcal{I}_V$ with the given $\overline{Z}$, and only one of them (namely, the preimage of $\overline{Z}$ under $V \to V/Fv$) contains v. Thus X_n is the sum of X_{n-1} and the independent Bernoulli random variable B_n, so we are done by induction on n.

(d) The generating function for X_n is the product of the generating functions for $B_1, \ldots, B_n$; this gives the first identity. The second follows from the first.

(e) This follows from (d) and Cauchy's q-binomial theorem (which actually goes back to [Rot11] and is related to earlier formulas of Euler). Namely, set $t = 1/p$ in formula (18) of [Cau43], and divide by $\prod_{j=0}^{n-1}(1+p^{-j})$.

(f) Take the limit of (e) as $n \to \infty$. The alternative formula for c follows from substituting

$$1 + p^{-j} = \frac{1-p^{-2j}}{1-p^{-j}}$$

for $j \neq 0$ and cancelling common factors. □

Remark 2.7. There is a variant for finite-dimensional vector spaces V over a finite field F of non-prime order. One can define the notion of weakly metabolic quadratic form $Q\colon V \to F$, and then prove Proposition 2.6 with q in place of p.

If we consider only even-dimensional nondegenerate quadratic spaces over F, then the obstruction analogous to that in Remark 2.5 takes values in a group of order 2. The obstruction is the discriminant in $F^\times/F^{\times 2}$ if $\operatorname{char} F \neq 2$, and the Arf invariant (see [Sch85]9.§4) if $\operatorname{char} F = 2$.

Remark 2.8. By Lemma 2.2, a quadratic form on a 2-torsion module will in general take values in the *4-torsion* of the image group. Thus we need an analogue of Proposition 2.6(c) for a $\frac{1}{4}\mathbb{Z}/\mathbb{Z}$-valued quadratic form Q on a $2n$-dimensional $\mathbb{F}_2$-vector space V such that $Q(V) \not\subset \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, or equivalently such that $\langle x, x\rangle = -2Q(x)$ is not identically 0.

The map $x \mapsto \langle x, x\rangle$ is a linear functional $V \to \frac{1}{2}\mathbb{Z}/\mathbb{Z} \simeq \mathbb{F}_2$ since

$$\langle x+y, x+y\rangle = \langle x, x\rangle + 2\langle x, y\rangle + \langle y, y\rangle = \langle x, x\rangle + \langle y, y\rangle.$$

Hence there exists a nonzero $c \in V$ such that $\langle x, x\rangle = \langle x, c\rangle$ for all $x \in V$. This equation shows that for any maximal isotropic subspace W of V, we have $c \in W^\perp = W$. The map $W \mapsto W/\mathbb{F}_2 c$ defines a bijection between the set of maximal isotropic subspaces of V and the set of maximal isotropic subspaces of $(\mathbb{F}_2 c)^\perp/\mathbb{F}_2 c$, which is a $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$-valued quadratic space.

So the random variable $\dim(Z \cap W)$ for V is 1 plus the corresponding random variable for the $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$-valued quadratic space of dimension $\dim V - 2$.

Definition 2.9. Given a prime p, let X_{Sel_p} be a $\mathbb{Z}_{\geq 0}$-valued random variable such that for any $d \in \mathbb{Z}_{\geq 0}$, the probability $\operatorname{Prob}(X_{\mathrm{Sel}_p} = d)$ equals the a_d in Proposition 2.6(d).

In the notation of Proposition 2.6(c), we can also write

$$X_{\mathrm{Sel}_p} = \lim_{n\to\infty} X_n = \sum_{n=1}^{\infty} B_n.$$

Remark 2.10. The distribution of X_{Sel_2} agrees with the distribution of $s(E)$ mentioned at the beginning of Section 1.1.

2.3. **Some topology.** To interpret a_r as a probability and not only a limit of probabilities, we are led to consider infinite-dimensional quadratic spaces. The naïve dual of such a space V is too large to be isomorphic to V, so we consider spaces with a locally compact topology and use the Pontryagin dual. In order to define a probability measure on the set of maximal isotropic subspaces, we need additional countability constraints. This section proves the equivalence of several such countability constraints.

For a locally compact abelian group G, define the Pontryagin dual $G^* := \operatorname{Hom}_{\mathrm{conts}}(G, \mathbb{R}/\mathbb{Z})$. Recall that a topological space is σ-compact if it is expressible as a union of countably many compact subspaces, first-countable if each point has a countable basis of neighborhoods, second-countable if the topology admits a countable basis, and separable if it has a countable dense subset.

Proposition 2.11. *Let G be a locally compact abelian group. The following are equivalent:*
(a) *G^* is σ-compact.*
(b) *G is first-countable.*
(c) *G is metrizable.*

Moreover, G is second-countable if and only if G and G^* are both σ-compact.

Proof. After peeling off a direct factor $\mathbb{R}^n$ from G, we may assume that G contains a compact open subgroup K, by the Pontryagin–van Kampen structure theorem [vK35, Theorem 2]. Each of (a), (b), (c) holds for G if and only if it holds for K, and for K the three conditions are equivalent to second-countability by [Kak43, Theorem 2 and the bottom of page 366]. To prove the final statement, observe that G is second-countable if and only if K is second-countable and G/K is countable. By the above, K is second-countable if and only G^* is σ-compact; on the other hand, G/K is countable if and only if G is σ-compact. □

Corollary 2.12. *Let G be a locally compact abelian group such that $G \simeq G^*$. Then the following are equivalent:*

(a) *G is σ-compact.*
(b) *G is first-countable.*
(c) *G is metrizable.*
(d) *G is second-countable.*
(e) *G is separable.*

Proof. Proposition 2.11 formally implies the equivalence of (a), (b), (c), (d). To obtain (d) $\Longrightarrow$ (e), choose one point from each nonempty set in a countable basis. To prove (e) $\Longrightarrow$ (a), reduce to the case that G contains a compact open subgroup K; then separability implies that G/K is finite, so G is σ-compact. ☐

2.4. Quadratic forms on locally compact abelian groups.

Definition 2.13. A locally compact quadratic module (V, Q) is a locally compact abelian group V equipped with a continuous quadratic form $Q\colon V \to \mathbb{R}/\mathbb{Z}$.

The definitions of maximal isotropic and nondegenerate extend to this setting.

Definition 2.14. Call a nondegenerate locally compact quadratic module (V, Q) weakly metabolic if it contains a *compact open* maximal isotropic subgroup W; we then say also that (V, Q, W) is weakly metabolic.

Remark 2.15. In Definition 2.14, it would perhaps be more natural to require the subgroup W to be only closed, not necessarily compact and open. Here we explain that the two definitions are equivalent when V contains a compact open subgroup, which is not a strong hypothesis, since by the Pontryagin–van Kampen structure theorem, if V is a locally compact abelian group, then $V \simeq \mathbb{R}^n \oplus V'$ as topological groups, where V' contains a compact open subgroup.

If (V, Q) is a nondegenerate locally compact quadratic module containing a compact open subgroup K, then $X := K \cap K^\perp$ is an compact open *isotropic* subgroup. Next, if W is *any* closed maximal isotropic subgroup of (V, Q), then $(W \cap X^\perp) + X$ is a compact open maximal isotropic subgroup of (V, Q) (cf. Remark 2.4(b)).

Remark 2.16. If (V, Q) is a nondegenerate locally compact quadratic module containing a compact open subgroup X, then the obstruction to (V, Q) containing a maximal isotropic closed subgroup is the same as that for $X^\perp/X$, so the obstruction is measured by an element of WQ that is independent of X (cf. Remark 2.5).

Example 2.17. If W is a locally compact abelian group, then $V := W \times W^*$ may be equipped with the quadratic form $Q((w, f)) := f(w)$. If W contains a compact open subgroup Y, then its annihilator in W^* is a compact open subgroup Y' of W^*, and $X := Y \times Y'$ is a compact open subgroup of V, so Remark 2.15 shows that (V, Q) is weakly metabolic.

Example 2.18 (cf. [Bra48, Théorème 1])**.** Suppose that (V_i, Q_i, W_i) for $i \in I$ are weakly metabolic. Define the restricted direct product

$$V := \prod_{i\in I}{}^{'}(V_i, W_i) := \left\{ (v_i)_{i\in I} \in \prod_{i \in I} V_i : v_i \in W_i \text{ for all but finitely many } i \right\}.$$

Let $W := \prod_{i \in I} W_i$. As usual, equip V with the topology for which W is open and has the product topology. For $v := (v_i) \in V$, define $Q(v) = \sum_{i\in I} Q_i(v_i)$, which makes sense since $Q_i(v_i) = 0$ for all but finitely many i. Then (V, Q, W) is another weakly metabolic locally compact quadratic module.

Moreover, if I is countable and each V_i is second-countable, then V is second-countable too. (*Proof:* Use Corollary 2.12 to replace second-countable by σ-compact. If each V_i is σ-compact, then each V_i/W_i is countable, so $V/W \simeq \bigoplus_{i\in I} V_i/W_i$ is countable, so V is σ-compact.)

Let (V,Q) be a locally compact quadratic module. Let $\mathcal{I}_V$ be the set of maximal isotropic closed subgroups of (V,Q). Let $\mathcal{X}_V$ be the poset of compact open isotropic subgroups of (V,Q), ordered by (reverse) inclusion.

Theorem 2.19. *Let (V,Q,W) be a second-countable weakly metabolic locally compact quadratic module.*

(a) *The set $\mathcal{X}_V$ is a countable directed poset.*
(b) *The finite sets $\mathcal{I}_{X^\perp/X}$ for $X \in \mathcal{X}_V$ with the maps $\pi^{X_1^\perp/X_1, X_2^\perp/X_2}$ for $X_1 \subseteq X_2$ (cf. Remark 2.4(b)) form an inverse system.*
(c) *If $\bigcap_{X\in\mathcal{X}_V} X = 0$, then the collection of maps $\pi^{V,X^\perp/X}$ induce a bijection*

$$\mathcal{I}_V \to \varprojlim_{X\in\mathcal{X}_V} \mathcal{I}_{X^\perp/X}.$$

Equip $\mathcal{I}_V$ with the inverse limit topology.
(d) *In the remaining parts of this theorem, assume that p is a prime such that $pV = 0$. Then there exists a unique probability measure μ on the Borel σ-algebra of $\mathcal{I}_V$ such that for every compact open isotropic subgroup X of (V,Q), the push-forward $\pi_*^{V,X^\perp/X}\mu$ is the uniform probability measure on the finite set $\mathcal{I}_{X^\perp/X}$.*
(e) *The measure μ is invariant under the orthogonal group* $\operatorname{Aut}(V,Q)$.
(f) *If Z is distributed according to μ, then* $\operatorname{Prob}(Z \text{ is discrete}) = 1$ *and* $\operatorname{Prob}(Z\cap W \text{ is finite}) = 1$. *If moreover $\dim_{\mathbb{F}_p} V$ is infinite, then the distribution of $\dim(Z\cap W)$ is given by X_{Sel_p} (see Definition 2.9).*

Proof.

(a) The intersection of two compact open isotropic subgroups of V is another one, so $\mathcal{X}_V$ is a directed poset. To prove that $\mathcal{X}_V$ is countable, first consider the bijection

$$\begin{aligned}\{\text{compact open subgroups of } W\} &\to \{\text{finite subgroups of } V/W\} \\ X &\mapsto X^\perp/W.\end{aligned} \tag{1}$$

Since V/W is a countable discrete group, both sets above are countable. The map

$$\begin{aligned}\mathcal{X}_V &\to \{\text{compact open subgroups of } W\} \\ X &\mapsto X\cap W\end{aligned}$$

has finite fibers, since the $X\in\mathcal{X}_V$ containing a given compact open subgroup Y of W are in bijection with the isotropic subgroups of the finite group $Y^\perp/Y$. Thus $\mathcal{X}_V$ is countable.
(b) Given $X_1 \subseteq X_2 \subseteq X_3$ the maps $\pi^{X_i^\perp/X_i, X_j^\perp/X_j}$ for $i<j$ behave as expected under composition.
(c) The same computation proving (b) yields the map. The inverse map $(Z_X) \mapsto Z$ is constructed as follows: given $(Z_x) \in \varprojlim_{X\in\mathcal{X}_V} \mathcal{I}_{X^\perp/X}$, let $\tilde{Z}_X$ be the preimage of Z_X

under $X^\perp \twoheadrightarrow X^\perp/X$, and let

$$\tilde{Z}_X := \varprojlim_{\substack{Y\in\mathcal{X}_V\\ Y\subseteq X}} \left(Z_Y \cap \frac{X^\perp}{Y} \right) \subseteq \varprojlim_{\substack{Y\in\mathcal{X}_V\\ Y\subseteq X}} \frac{X^\perp}{Y} = X^\perp$$
$$Z := \bigcup_{X\in\mathcal{X}_V} \tilde{Z}_X.$$

The maps in the inverse system are surjections, so the image of $\tilde{Z}_X$ in $X^\perp/X$ equals Z_X. If $X, X' \in \mathcal{X}_V$ and $X' \subseteq X$, then $\tilde{Z}_X = \tilde{Z}_{X'} \cap X^\perp$, so $Z \cap X^\perp = \tilde{Z}_X$. Since each Z_Y is isotropic in $Y^\perp/Y$, the group $\tilde{Z}_X$ is isotropic, so Z is isotropic. If $z \in Z^\perp$, then we have $z \in X^\perp$ for some X, and then for any $Y \subseteq X$, the element $z \bmod Y \in Y^\perp/Y$ is perpendicular to $\pi^{V,Y^\perp/Y}(Z) = Z_Y$, but $Z_Y^\perp = Z_Y$, so $z \bmod Y \in Z_Y$, and also $z \bmod Y \in X^\perp/Y$; this holds for all $Y \subseteq X$, so $z \in Z$. Thus $Z^\perp = Z$; i.e., $Z \in \mathcal{I}_V$.

Now we show that the two constructions are inverse to each other. If we start with (Z_X), then the Z produced by the inverse map satisfies $\pi^{V,X^\perp/X}(Z) = Z_X$. Conversely, if we start with Z, and define $Z_X := \pi^{V,X^\perp/X}(Z)$, then the inverse map applied to (Z_X) produces Z' such that $Z \cap X^\perp \subseteq Z'$ for all X, so $Z \subseteq Z'$, but Z and Z' are both maximal isotropic, so $Z = Z'$.

(d) Since V/W is a discrete $\mathbb{F}_p$-vector space of dimension $\aleph_0$, we may choose a cofinal increasing sequence of finite-dimensional subspaces of V/W, and this corresponds under (1) to a cofinal decreasing sequence $Y_1, Y_2, \ldots$ of compact open subgroups of W whose intersection is 0. Thus (c) applies. Each map in the inverse system has fibers of constant size, by Proposition 2.6(a), so the uniform measures on these finite sets are compatible. By [Bou04, III.§4.5, Proposition 8(iv)], the inverse limit measure exists.

(e) The construction is functorial with respect to isomorphisms $(V, Q) \to (V', Q')$.

(f) Since $\sum_{r=0}^\infty a_r = 1$, it suffices to prove the last statement, that $\operatorname{Prob}(\dim(Z \cap W) = r) = a_r$. Let Y_i be as in the proof of (d). Then $\dim(Z \cap W)$ is the limit of the increasing sequence of nonnegative integers $\dim(\pi^{V,Y_i^\perp/Y_i}(Z) \cap \pi^{V,Y_i^\perp/Y_i}(W))$. By Proposition2.6(c) and its proof, the difference of consecutive integers in this sequence is a sum of independent Bernoulli random variables. Since $\sum_{j\ge1} \operatorname{Prob}(B_j = 1)$ converges, the Borel-Cantelli lemma implies that

$$\operatorname{Prob}\Big(\dim(Z \cap W) \neq \dim(\pi^{V,Y_i^\perp/Y_i}(Z) \cap \pi^{V,Y_i^\perp/Y_i}(W))\Big) \to 0$$

as $i \to \infty$. In particular, $\operatorname{Prob}(\dim(Z \cap W) = \infty)$ is 0. On the other hand, $\dim Y_i^\perp/Y_i \to \infty$ as $i \to \infty$, so

$$\operatorname{Prob}(\dim(Z \cap W) = d) = \lim_{n\to\infty} a_{d,n} = a_d = \operatorname{Prob}\left(X_{\mathrm{Sel}_p} = d\right). \qquad \square$$

2.5. **Moments.** Given a random variable X, let $\mathbb{E}(X)$ be its expectation. So if $m \in \mathbb{Z}_{\ge0}$, then $\mathbb{E}(X^m)$ is its m^{th} moment.

Proposition 2.20. *Fix a prime p, $d \in \mathbb{Z}_{\geq 0}$, and $m \in \mathbb{Z}_{\geq 0}$. Let X_n be as in Proposition 2.6*(c)*, and let X_{Sel_p} be as in Definition 2.9. Then*

$$\mathbb{E}\left(\left(p^{X_n}\right)^m\right) = \prod_{i=1}^{m} \frac{p^i+1}{1+p^{-(n-i)}}$$

$$\mathbb{E}\left(\left(p^{X_{\mathrm{Sel}_p}}\right)^m\right) = \prod_{i=1}^{m} (p^i+1).$$

In particular, $\mathbb{E}(p^{X_{\mathrm{Sel}_p}}) = p+1$.

Proof. Substitute $z = p^m$ in Proposition 2.6(d). The products telescope. $\square$

3. Some homological algebra

3.1. **A tensor algebra construction.** We will define a functor U from the category of $\mathbb{Z}$-modules to the category of groups, the goal being Theorem 3.5. Let M be a $\mathbb{Z}$-module. Let $TM = \bigoplus_{i\geq 0} T^i M$ be the tensor algebra. Then $T^{\geq n}M = \bigoplus_{i\geq n} T^i M$ is a 2-sided ideal of TM. Let $T^{<n}M$ be the quotient ring $TM/T^{\geq n}M$. Let UM be the kernel of $(T^{<3}M)^\times \to (T^{<1}M)^\times = \mathbb{Z}^\times = \{\pm 1\}$. The grading on TM gives rise to a filtration of UM, which yields the following central extension of groups

$$1 \to M \otimes M \to UM \xrightarrow{\pi} M \to 1. \tag{2}$$

Elements of UM may be written as $1+m+t$ where $m \in M$ and $t \in M \otimes M$, and should be multiplied as follows:

$$(1+m+t)(1+m'+t') = 1 + (m+m') + ((m \otimes m') + t + t').$$

The surjection $UM \to M$ admits a set-theoretic section $s\colon M \to UM$ sending m to $1+m$. If $m, m' \in M$, then

$$s(m)\, s(m')\, s(m+m')^{-1} = m \otimes m' \tag{3}$$

in $M \otimes M \subseteq UM$.

A simple computation verifies the following universal property of UM:

Proposition 3.1. *The map $s\colon M \to UM$ is universal for set maps $\sigma\colon M \to G$ to a group G such that $(m,m') \mapsto \sigma(m)\sigma(m')\sigma(m+m')^{-1}$ is a bilinear function from $M \times M$ to an abelian subgroup of G.*

A quadratic map $q\colon M \to G$ is a set map between abelian groups such that $(m,m') \mapsto q(m+m') - q(m) - q(m')$ is bilinear. (Perhaps "*pointed* quadratic map" would be better terminology; for instance, the quadratic maps $q\colon \mathbb{Q} \to \mathbb{Q}$ are the polynomial functions of degree at most 2 sending 0 to 0.) Proposition 3.1 implies:

Corollary 3.2. *The map $M \to (UM)^{\mathrm{ab}}$ is universal for quadratic maps from M to an abelian group.*

Remark 3.3.

(a) The commutator $[1+m+t, 1+m'+t]$ equals $m \otimes m' - m' \otimes m$, so we have an exact sequence of abelian groups

$$0 \to S^2 M \to (UM)^{\mathrm{ab}} \to M \to 0,$$

where $SM = \bigoplus_{n \geq 0} S^n M$ is the symmetric algebra. In particular,

$$(UM)^{\mathrm{ab}} \simeq \ker\left((S^{<3}M)^\times \to (S^{<1}M)^\times\right).$$

(b) Similarly, if $2M = 0$, then $(1+m+t)^2 = 1 + m \otimes m$, so we obtain an exact sequence of $\mathbb{F}_2$-vector spaces

$$0 \to \bigwedge^2 M \to (UM)^{\mathrm{ab}} \otimes \mathbb{F}_2 \to M \to 0,$$

and

$$(UM)^{\mathrm{ab}} \otimes \mathbb{F}_2 \simeq \ker\left((\bigwedge^{<3} M)^\times \to (\bigwedge^{<1} M)^\times\right).$$

3.2. **Sheaves of groups.** In the rest of Section 3, $\mathcal{C}$ is a site. Let $\mathfrak{Gp}_{\mathcal{C}}$ be the category of sheaves of groups on $\mathcal{C}$, and let $\mathfrak{Ab}_{\mathcal{C}}$ be the category of sheaves of abelian groups on $\mathcal{C}$. For $M \in \mathfrak{Ab}_{\mathcal{C}}$, write $\mathrm{H}^i(M)$ for $\mathrm{Ext}^i(\mathbb{Z}, M)$, where $\mathbb{Z}$ is the constant sheaf; in other words, $\mathrm{H}^i(-)$ is the i^{th} right derived functor of $\mathrm{Hom}(\mathbb{Z}, -)$ on $\mathfrak{Ab}_{\mathcal{C}}$. For $M \in \mathfrak{Gp}_{\mathcal{C}}$, define $\mathrm{H}^0(M)$ as $\mathrm{Hom}(\mathbb{Z}, M)$ and define $\mathrm{H}^1(M)$ in terms of torsors as in [Gir71, §III.2.4]. The definitions are compatible for $M \in \mathfrak{Ab}_{\mathcal{C}}$ and $i = 0, 1$ [Gir71, Remarque III.3.5.4].

Remark 3.4. The reader may prefer to imagine the case for which sheaves are G-sets for some group G, abelian sheaves are $\mathbb{Z}G$-modules, and $\mathrm{H}^i(M)$ is just group cohomology.

All the constructions and results of Section 3.1 have sheaf analogues. In particular, for $M \in \mathfrak{Ab}_{\mathcal{C}}$ we obtain $\mathscr{U}M \in \mathfrak{Gp}_{\mathcal{C}}$ fitting in exact sequences

$$1 \to M \otimes M \to \mathscr{U}M \to M \to 1 \tag{4}$$

$$0 \to S^2 M \to (\mathscr{U}M)^{\mathrm{ab}} \to M \to 0, \tag{5}$$

and, if $2M = 0$,

$$0 \to \bigwedge^2 M \to (\mathscr{U}M)^{\mathrm{ab}} \otimes \mathbb{F}_2 \to M \to 0. \tag{6}$$

3.3. **Self cup products.**

Theorem 3.5. *For $M \in \mathfrak{Ab}_{\mathcal{C}}$, the connecting map $\mathrm{H}^1(M) \to \mathrm{H}^2(M \otimes M)$ induced by* (4) *(see* [Gir71, §IV.3.4.1]*) maps each x to $x \cup x$.*

Proof. Let $x \in \mathrm{H}^1(M) = \mathrm{Ext}^1(\mathbb{Z}, M)$. Let

$$0 \to M \to X \xrightarrow{\alpha} \mathbb{Z} \to 0 \tag{7}$$

be the corresponding extension. Let $X_1 := \alpha^{-1}(1)$, which is a sheaf of torsors under M.

We will construct a commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & M \otimes M & \longrightarrow & \mathscr{U}M & \xrightarrow{\pi} & M & \longrightarrow & 1 \\
 & & \| & & \uparrow & & \uparrow & & \\
1 & \longrightarrow & M \otimes M & \longrightarrow & G & \xrightarrow{\delta} & G' & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M \otimes M & \longrightarrow & X \otimes M & \xrightarrow{\epsilon} & M & \longrightarrow & 0
\end{array} \tag{8}$$

of sheaves of groups, with exact rows. The first row is (4). The last row, obtained by tensoring (7) with M, is exact since $\mathbb{Z}$ is flat. Let G be the sheaf of $(u, t) \in \mathscr{U}M \oplus (X \otimes M)$ such that $\pi(u) = \epsilon(t)$ in M. The vertical homomorphisms emanating from G are the two projections. Let $\delta\colon G \to \mathscr{U}X$ send (u,t) to $u-t$. Then $\ker\delta = M\otimes M$, embedded diagonally in G. Let $G' = \delta(G)$. Explicitly, if e is a section of X_1, then G' consists of sections of $\mathscr{U}X$ of the form $1+m-e\otimes m+t$ with $m\in M$ and $t\in M\otimes M$. The vertical homomorphisms emanating from G' are induced by the map $G\to M$ sending (u,t) to $\pi(u)=\epsilon(t)$.

A calculation shows that $1+X_1+M\otimes M$ is a right torsor X' under G', corresponding to some $x'\in \mathrm{H}^1(G')$. Moreover, $\mathscr{U}X\to X$ restricts to a *torsor* map $X'\to X_1$ compatible with $G'\to M$, so $\mathrm{H}^1(G')\to\mathrm{H}^1(M)$ sends x' to x.

By [Gir71, §IV.3.4.1.1], the commutativity of (8) shows that the image of x under the connecting map $\mathrm{H}^1(M)\to\mathrm{H}^2(M\otimes M)$ from the first row, equals the image of x' under the connecting map $\mathrm{H}^1(G')\to\mathrm{H}^2(M\otimes M)$ from the second row, which equals the image of x under the connecting homomorphism $\mathrm{H}^1(M)\to\mathrm{H}^2(M\otimes M)$ from the third row. This last homomorphism is $y\mapsto x\cup y$, so it maps x to $x\cup x$ (cf. [Yon58], which explains this definition of $x\cup y$ for extensions of modules over a ring). □

Example 3.6. If $M=\mathbb{Z}/2\mathbb{Z}$, then (4) is the sequence of constant sheaves

$$0\to\mathbb{Z}/2\mathbb{Z}\to\mathbb{Z}/4\mathbb{Z}\to\mathbb{Z}/2\mathbb{Z}\to 0,$$

which induces the Bockstein morphism $\mathrm{H}^1(X,\mathbb{Z}/2\mathbb{Z})\to\mathrm{H}^2(X,\mathbb{Z}/2\mathbb{Z})$. So Theorem 3.5 recovers the known result that for any topological space X, the self-cup-product $\mathrm{H}^1(X,\mathbb{Z}/2\mathbb{Z})\to\mathrm{H}^2(X,\mathbb{Z}/2\mathbb{Z})$ is the Bockstein morphism. (See properties (5) and (7) of Steenrod squares in Section 4.L of [Hat10].)

Remark 3.7. In group cohomology, if we represent a class in $\mathrm{H}^1(M)$ by a cochain ζ, then one can check that the coboundary of $s\circ\zeta$ equals the difference of $\zeta\cup\zeta$ and the image of ζ under the connecting map. A similar argument using Čech cochains gives an alternate proof of the general case of Theorem 3.5, as we now explain.

By [Gir71, Théorème 0.2.6], we may replace $\mathcal{C}$ by a site with one with an equivalent topos in order to assume that $\mathcal{C}$ has finite fiber products, and in particular, a final object S. Then the natural map $\check{\mathrm{H}}^1(M)\to\mathrm{H}^1(M)$ is an isomorphism [Gir71, Remarque III.3.6.5(5)], so any $x\in\mathrm{H}^1(M)$ is represented by a 1-cocycle m for some covering $(S'_i\to S)_{i\in I}$. For simplicity, let us assume that the covering consists of *one* morphism $S'\to S$ (the general case is similar). Let $S''=S'\times_S S'$, and $S'''=S'\times_S S'\times_S S'$. Let $\pi_{23},\pi_{13},\pi_{12}\colon S'''\to S''$ be the projections. So $m\in M(S'')$ satisfies $\pi_{13}^*m=\pi_{12}^*m+\pi_{23}^*m$. Applying the section $M\to\mathscr{U}M$ yields a 1-cochain $1+m\in(\mathscr{U}M)(S'')$. Its 2-coboundary in $(M\otimes M)(S''')\subseteq(\mathscr{U}M)(S''')$ represents the image of x under the connecting map $\mathrm{H}^1(M)\to\mathrm{H}^2(M\otimes M)$ [Gir71, Corollaire IV.3.5.4(ii)]. On the other hand, the definition of the 2-coboundary given in [Gir71, Corollaire IV.3.5.4] together with (3) shows that it is $\pi_{12}^*m\otimes\pi_{23}^*m\in(M\otimes M)(S''')$, whose class in $\mathrm{H}^2(M\otimes M)$ represents $x\cup x$, by definition.

Let $M,N\in\mathfrak{Ab}_{\mathcal{C}}$. Let $\beta\in\mathrm{H}^0(\mathbf{Hom}(M\otimes M,N))$. (The bold face in **Hom**, **Ext**, etc., indicates that we mean the sheaf versions.) Using β, construct an exact sequence

$$0\to N\to\mathscr{U}_\beta\to M\to 0 \tag{9}$$

as the pushout of (4) by $\beta\colon M\otimes M\to N$.

If β is symmetric, then $\mathscr{U}_\beta$ is abelian, and we let ϵ_β be the class of (9) in $\mathrm{Ext}^1(M,N)$. If β is symmetric and $\mathbf{Ext}^1(M,N)=0$, then applying $\mathbf{Hom}(-,N)$ to (5) yields

$$0\to\mathbf{Hom}(M,N)\to\mathbf{Hom}((\mathscr{U}M)^{\mathrm{ab}},N)\to\mathbf{Hom}(S^2M,N)\to 0$$

and a connecting homomorphism sends $\beta \in \mathrm{H}^0(\mathbf{Hom}(S^2M, N))$ to an element $c_\beta \in \mathrm{H}^1(\mathbf{Hom}(M, N))$.

Corollary 3.8. *Then the following maps $\mathrm{H}^1(M) \to \mathrm{H}^2(N)$ are the same, when defined:*
(a) *The composition*

$$\mathrm{H}^1(M) \xrightarrow{\Delta} \mathrm{H}^1(M) \times \mathrm{H}^1(M) \xrightarrow{\cup} \mathrm{H}^2(M \otimes M) \xrightarrow{\beta} \mathrm{H}^2(N).$$

(b) *The connecting homomorphism $\mathrm{H}^1(M) \to \mathrm{H}^2(N)$ associated to* (9).
(c) *The pairing with ϵ_β under the Yoneda product*

$$\mathrm{Ext}^1(M, N) \times \mathrm{H}^1(M) \to \mathrm{H}^2(N)$$

(if β is symmetric).
(d) *The pairing with c_β under the evaluation cup product*

$$\mathrm{H}^1(\mathbf{Hom}(M, N)) \times \mathrm{H}^1(M) \to \mathrm{H}^2(N)$$

(if β is symmetric and $\mathbf{Ext}^1(M, N) = 0$).

Proof. Theorem 3.5 and functoriality implies the equality of (a) and (b). Standard homological algebra gives equality of (b), (c), and (d). □

3.4. **Commutator pairings.**

Proposition 3.9. *Let $1 \to A \to B \xrightarrow{\rho} C \to 1$ be an exact sequence in $\mathfrak{Gp}_{\mathcal{C}}$, with A central in B, and C abelian. Let $q \colon \mathrm{H}^1(C) \to \mathrm{H}^2(A)$ be the connecting map. Given $c_1, c_2 \in C$, we can lift them locally to b_1, b_2 and form their commutator $[b_1, b_2] := b_1 b_2 b_1^{-1} b_2^{-1} \in A$; this induces a homomorphism $[\ ,\ ] \colon C \otimes C \to A$. For $\gamma_1, \gamma_2 \in \mathrm{H}^1(C)$, we have that $q(\gamma_1+\gamma_2) - q(\gamma_1) - q(\gamma_2)$ equals the image of $-\gamma_1 \cup \gamma_2$ under the homomorphism $\mathrm{H}^2(C \otimes C) \to \mathrm{H}^2(A)$ induced by $[\ ,\ ]$.*

Proof. That the commutator induces a homomorphism is a well-known simple computation. Pulling back $1 \to A^3 \to B^3 \to C^3 \to 1$ by the homomorphism $C^2 \to C^3$ sending (c_1, c_2) to $(c_1, c_2, c_1 + c_2)$ and then pushing out by the homomorphism $A^3 \to A$ sending (a_1, a_2, a_3) to $a_3 - a_2 - a_1$ yields an exact sequence $1 \to A \to Q \to C^2 \to 1$. Here $Q = B'/B''$ where B' is the subgroup sheaf of $(b_1, b_2, b_3) \in B^3$ satisfying $\rho(b_3) = \rho(b_1) + \rho(b_2)$, and B'' is the subgroup sheaf of B^3 generated by sections $(a_1, a_2, a_3) \in A^3$ with $a_3 = a_1 + a_2$. The surjection $Q \to C^2$ admits a section $\sigma \colon C^2 \to Q$ defined locally as follows: given (c_1, c_2) lifting to $(b_1, b_2) \in B^2$, send it to the image of $(b_1, b_2, b_1 b_2)$ in Q (this is independent of the choice of lifts, since we work modulo B''). A calculation shows that

$$\sigma((c_1', c_2'))\, \sigma((c_1, c_2) + (c_1', c_2'))^{-1}\, \sigma((c_1, c_2)) = [c_1', c_2^{-1}] = -[c_1', c_2] \tag{10}$$

in A, and the three factors on the left may be rotated since the right hand side is central in Q. Proposition 3.1 and (10) yield the middle vertical map in the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C^2 \otimes C^2 & \longrightarrow & \mathscr{U}(C^2) & \longrightarrow & C^2 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & A & \longrightarrow & Q & \longrightarrow & C^2 & \longrightarrow & 1 \end{array} \tag{11}$$

with exact rows, and the left vertical map sends $(c_1, c_2) \otimes (c_1', c_2')$ to $-[c_1', c_2]$. The connecting map for the first row sends $(\gamma_1, \gamma_2) \in \mathrm{H}^1(C^2)$ to $(\gamma_1, \gamma_2) \cup (\gamma_1, \gamma_2) \in \mathrm{H}^2(C^2 \otimes C^2)$, by Theorem 3.5. The connecting map for the second row is a composition $\mathrm{H}^1(C^2) \to \mathrm{H}^1(C^3) \to$

$\mathrm{H}^2(A^3) \to \mathrm{H}^2(A)$, so it maps (γ_1, γ_2) to $q(\gamma_1+\gamma_2) - q(\gamma_1) - q(\gamma_2)$. Finally, the left vertical map sends $(\gamma_1,\gamma_2) \cup (\gamma_1,\gamma_2) \in \mathrm{H}^2(C^2 \otimes C^2)$ to the image of $-\gamma_1 \cup \gamma_2$ under the commutator pairing $\mathrm{H}^2(C \otimes C) \to \mathrm{H}^2(A)$. So compatibility of the connecting maps yields the result. □

4. Shafarevich-Tate groups of finite group schemes

For each field k, choose an algebraic closure $\overline{k}$ and a separable closure $k_s \subseteq \overline{k}$, and let $G_k := \mathrm{Gal}(k_s/k)$.

A local field is a nondiscrete locally compact topological field; each such field is a finite extension of one of $\mathbb{R}$, $\mathbb{Q}_p$, or $\mathbb{F}_p((t))$ for some prime p. A global field is a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p(t)$ for some prime p. Let Ω be the set of nontrivial places of k. For $v \in \Omega$, let k_v be the completion of k at v, so k_v is a local field; if v is nonarchimedean, let $\mathcal{O}_v$ be the valuation ring in k_v.

For a sheaf of abelian groups M on the big fppf site of $\operatorname{Spec} k$, define

$$Ш^1(k, M) := \ker\left(\mathrm{H}^1(k,M) \to \prod_{v\in\Omega} \mathrm{H}^1(k_v, M)\right). \tag{12}$$

The following criteria for vanishing of $Ш^1(k,M)$ will be especially relevant for Theorem 6.8(b).

Proposition 4.1. *Suppose that M is a finite étale group scheme over k, so we identify M with the finite G_k-module $M(k_s)$.*

(a) *If $M = \mathbb{Z}/n\mathbb{Z}$, then $Ш^1(k,M) = 0$.*
(b) *If M is a direct summand of a direct sum of permutation $\mathbb{Z}/n\mathbb{Z}$-modules arising from finite separable extensions of k, then $Ш^1(k,M) = 0$.*
(c) *Let G be the image of G_k in $\operatorname{Aut} M(k_s)$. Identify $\mathrm{H}^1(G,M)$ with its image under the injection $\mathrm{H}^1(G,M) \hookrightarrow \mathrm{H}^1(k,M)$. Then*

$$Ш^1(k,M) \subseteq \bigcap_{\text{cyclic } H \leq G} \ker\left(\mathrm{H}^1(G,M) \to \mathrm{H}^1(H,M)\right).$$

(d) *If p is a prime such that $pM = 0$ and the Sylow p-subgroups of $\operatorname{Aut} M(k_s)$ are cyclic, then $Ш^1(k,M) = 0$.*
(e) *If E is an elliptic curve, and $p \neq \operatorname{char} k$, then $Ш^1(k, E[p]) = 0$.*
(f) *If $\operatorname{char} k \neq 2$, and A is the Jacobian of the smooth projective model of $y^2 = f(x)$, where $f \in k[x]$ is separable of odd degree, then $Ш^1(k, A[2]) = 0$.*

Proof.

(a) See [Mil06, Example I.4.11(i)].
(b) Combine (a) with Shapiro's lemma [AW67, §4, Proposition 2] to obtain the result for a finite permutation module $(\mathbb{Z}/n\mathbb{Z})[G_k/G_L]$ for a finite separable extension L of k. The result for direct summands of direct sums of these follows.
(c) This is a consequence of the Chebotarev density theorem: see [BPS10].
(d) Let G be the image of $G_k \to \operatorname{Aut} M(k_s)$. Then any Sylow p-subgroup P of G is cyclic. But the restriction $\mathrm{H}^1(G,M) \to \mathrm{H}^1(P,M)$ is injective [AW67, §6, Corollary 3], so (c) shows that $Ш^1(k,M) = 0$.
(e) Any Sylow-p-subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ is conjugate to the group of upper triangular unipotent matrices, which is cyclic. Apply (d).

(f) The group $A[2]$ is a direct summand of the permutation $\mathbb{Z}/2\mathbb{Z}$-module on the set of zeros of f. Apply (b). □

See Example 5.12(b) for a 2-dimensional Jacobian A with $\text{Ш}^1(\mathbb{Q}, A[2]) \neq 0$. Such examples are rare: Example 5.12(c) shows that asymptotically 100% of 2-dimensional Jacobians A over $\mathbb{Q}$ have $\text{Ш}^1(\mathbb{Q}, A[2]) = 0$.

5. Abelian schemes

5.1. **The relative Picard functor.** Let $A \to S$ be an abelian scheme. Let $\mathbf{Pic}_{A/S}$ be its relative Picard functor on the big fppf site of S. Trivialization along the identity section shows that $\mathbf{Pic}_{A/S}(T) \simeq \operatorname{Pic}(A \times_S T)/\operatorname{Pic} T$ for each S-scheme T (see Proposition 4 on page 204 of [BLR90]). We generally identify line sheaves with their classes in $\mathbf{Pic}$. For an S-scheme T and $a \in A(T)$, let

$$\begin{aligned} \tau_a \colon A_T &\to A_T \\ x &\mapsto a + x \end{aligned}$$

be the translation-by-a morphism. Given a line sheaf $\mathscr{L}$ on A, the theorem of the square implies that

$$\begin{aligned} \phi_{\mathscr{L}} \colon A &\to \mathbf{Pic}_{A/S} \\ a &\mapsto \tau_a^* \mathscr{L} \otimes \mathscr{L}^{-1} \end{aligned} \tag{13}$$

is a homomorphism. If we vary the base and vary $\mathscr{L}$, we obtain a homomorphism of fppf-sheaves

$$\begin{aligned} \mathbf{Pic}_{A/S} &\to \mathbf{Hom}(A, \mathbf{Pic}_{A/S}) \\ \mathscr{L} &\mapsto \phi_{\mathscr{L}}. \end{aligned}$$

Its kernel is denoted $\mathbf{Pic}^0_{A/S}$. Using the fact that $\mathbf{Pic}_{A/S}$ is an algebraic space, and the fact that $\mathbf{Pic}^0_{A/S}$ is an open subfunctor of $\mathbf{Pic}_{A/S}$ (which follows from [SGA 6, Exposé XIII, Théorème 4.7]), one can show that $\mathbf{Pic}^0_{A/S}$ is another abelian scheme $\widehat{A}$ over S [FC90, p. 3]. The image of $\phi_{\mathscr{L}}$ is contained in $\widehat{A}$, so we may view $\phi_{\mathscr{L}}$ as a homomorphism $A \to \widehat{A}$. Moreover, $\phi_{\mathscr{L}}$ equals its dual homomorphism $\widehat{\phi_{\mathscr{L}}}$. In fact, we have an exact sequence of fppf-sheaves

$$0 \to \widehat{A} \to \mathbf{Pic}_{A/S} \to \mathbf{Hom}_{\text{self-dual}}(A, \widehat{A}) \to 0. \tag{14}$$

Remark 5.1. For an abelian variety A over a field k, the group $\operatorname{Hom}_{\text{self-dual}}(A, \widehat{A})$ of global sections of $\mathbf{Hom}_{\text{self-dual}}(A, \widehat{A})$ may be identified with the G_k-invariant subgroup of the Néron-Severi group $\operatorname{NS} A_{k_s}$. (For the case $k = \overline{k}$ see [Mum70], in particular Corollary 2 on page 178 and Theorem 2 on page 188 and the remark following it. The general case follows because any homomorphism defined over $\overline{k}$ is in fact defined over k_s, since it maps the Zariski-dense set of prime-to-$(\operatorname{char} k)$ torsion points in $A(k_s)$ to points in $\widehat{A}(k_s)$.)

For any homomorphism of abelian schemes $\lambda \colon A \to B$, let $A[\lambda] := \ker \lambda$.

5.2. **Symmetric line sheaves.** Multiplication by an integer n on A induces a pullback homomorphism $[n]^*\colon \mathbf{Pic}_{A/S} \to \mathbf{Pic}_{A/S}$. Let $\mathbf{Pic}^{\mathrm{Sym}}_{A/S}$ be the kernel of $[-1]^* - [1]^*$ on $\mathbf{Pic}_{A/S}$. More concretely, because $A \to S$ has a section, we have $\mathbf{Pic}^{\mathrm{Sym}}_{A/S}(T) = \mathrm{Pic}^{\mathrm{Sym}}(A \times_S T)/\operatorname{Pic} T$ for each S-scheme T, where $\mathrm{Pic}^{\mathrm{Sym}}(A \times_S T)$ is the group of isomorphism classes of symmetric line sheaves on $A \times_S T$. Since $[-1]^*$ acts as -1 on $\widehat{A}$ and as $+1$ on $\mathbf{Hom}_{\text{self-dual}}(A, \widehat{A})$, and since multiplication-by-2 on $\widehat{A}$ is surjective, the snake lemma applied to $[-1]^* - [1]^*$ acting on (14) yields an exact sequence

$$0 \to \widehat{A}[2] \to \mathbf{Pic}^{\mathrm{Sym}}_{A/S} \to \mathbf{Hom}_{\text{self-dual}}(A, \widehat{A}) \to 0. \tag{15}$$

5.3. **The Weil pairing.** We recall some facts and definitions that can be found in [Pol03, §10.4], for example. (In that book, S is $\operatorname{Spec} k$ for a field k, but the same arguments apply over an arbitrary base scheme.) Given an isogeny $\lambda\colon A \to B$ of abelian schemes over S, there is a Weil pairing

$$e_\lambda\colon A[\lambda] \times \widehat{B}[\widehat{\lambda}] \to \mathbb{G}_m \tag{16}$$

identifying $A[\lambda]$ with the Cartier dual of $\widehat{B}[\widehat{\lambda}]$. In particular, if $n \in \mathbb{Z}_{\geq 1}$, then $[n]\colon A \to A$ gives rise to

$$e_n\colon A[n] \times \widehat{A}[n] \to \mathbb{G}_m.$$

If $\lambda\colon A \to \widehat{A}$ is a self-dual isogeny, then

$$e_\lambda\colon A[\lambda] \times A[\lambda] \to \mathbb{G}_m$$

is alternating.

For any homomorphism $\lambda\colon A \to \widehat{A}$, define $e_2^\lambda\colon A[2] \times A[2] \to \mathbb{G}_m$ by $e_2^\lambda(x, y) = e_2(x, \lambda y)$. If $\mathscr{L} \in \mathbf{Pic}_{A/S}(S)$, let $e_2^{\mathscr{L}} = e_2^{\phi_{\mathscr{L}}}$; this is an alternating bilinear pairing, and hence is also symmetric.

5.4. **Quadratic refinements of the Weil pairing.**

Proposition 5.2. *There is a (not necessarily bilinear) pairing of fppf sheaves*

$$\mathfrak{q}\colon A[2] \times \mathbf{Pic}^{\mathrm{Sym}}_{A/S} \to \boldsymbol{\mu}_2 \subset \mathbb{G}_m$$

such that:

(a) *The pairing is additive in the second argument:* $\mathfrak{q}(x, \mathscr{L} \otimes \mathscr{L}') = \mathfrak{q}(x, \mathscr{L})\mathfrak{q}(x, \mathscr{L}')$.
(b) *The restriction of* $\mathfrak{q}$ *to a pairing*

$$\mathfrak{q}\colon A[2] \times \widehat{A}[2] \to \mathbb{G}_m$$

is the Weil pairing e_2. *In particular, this restriction is bilinear.*
(c) *In general,* $\mathfrak{q}(x + y, \mathscr{L}) = \mathfrak{q}(x, \mathscr{L})\mathfrak{q}(y, \mathscr{L})e_2^{\mathscr{L}}(x, y)$.

Proof. See [Pol03, §13.1]. □

We can summarize Proposition 5.2 in the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \widehat{A}[2] & \longrightarrow & \mathbf{Pic}^{\mathrm{Sym}}_{A/S} & \longrightarrow & \mathbf{Hom}_{\text{self-dual}}(A,\widehat{A}) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle e_2}\,\wr & & \downarrow{\scriptstyle \mathfrak{q}} & & \downarrow{\scriptstyle e_2^{\bullet}} & & \\
0 & \longrightarrow & \mathbf{Hom}(A[2],\mathbb{G}_m) & \longrightarrow & \mathbf{Hom}((\mathscr{U} A[2])^{\mathrm{ab}} \otimes \mathbb{F}_2, \mathbb{G}_m) & \longrightarrow & \mathbf{Hom}(\bigwedge^2 A[2], \mathbb{G}_m) & \longrightarrow & 0,
\end{array} \tag{17}$$

which we now explain. The top row is (15). The bottom row is obtained by applying $\mathbf{Hom}(-,\mathbb{G}_m)$ to (6) for $M = A[2]$, and using $\mathbf{Ext}^1(A[2],\mathbb{G}_m) = 0$ (a special case of [Wat71, Theorem 1, with the argument of §3 to change fpqc to fppf]). The vertical maps are the map $y \mapsto e_2(-,y)$, the map sending $\mathscr{L}$ to the homomorphism $(\mathscr{U} A[2])^{\mathrm{ab}} \otimes \mathbb{F}_2 \to \mathbb{G}_m$ corresponding to $\mathfrak{q}(-,\mathscr{L})$ (see Corollary 3.2), and the map $[\mathscr{L}] \mapsto e_2^{\mathscr{L}}$, respectively. Commutativity of the two squares are given by (b) and (c) in Proposition 5.2, respectively.

The top row of (17) gives a homomorphism

$$\begin{aligned} \mathrm{Hom}_{\text{self-dual}}(A,\widehat{A}) &\to \mathrm{H}^1(\widehat{A}[2]) \\ \lambda &\mapsto c_\lambda. \end{aligned} \tag{18}$$

We may interpret c_λ geometrically as the class of the torsor under $\widehat{A}[2]$ that parametrizes symmetric line sheaves $\mathscr{L}$ with $\phi_{\mathscr{L}} = \lambda$ (cf. [Pol03, §13.5]). Thus c_λ is the obstruction to finding $\mathscr{L} \in \mathrm{Pic}^{\mathrm{Sym}} A$ with $\phi_{\mathscr{L}} = \lambda$.

Remark 5.3. The map $\mathrm{H}^1(\widehat{A}[2]) \to \mathrm{H}^1(\widehat{A})$ sends c_λ to the element called c_λ in [PS99, §4].

Theorem 5.4. *For any $\lambda \in \mathrm{Hom}_{\text{self-dual}}(A,\widehat{A})$. and any $x \in \mathrm{H}^1(A[2])$, we have*

$$x \underset{e_2^\lambda}{\cup} x = x \underset{e_2}{\cup} c_\lambda \tag{19}$$

in $\mathrm{H}^2(\mathbb{G}_m)$, where the cup products are induced by the pairings underneath.

Proof. The rightmost vertical map in (17) maps λ to e_2^λ. These are mapped by the horizontal connecting homomorphisms to $c_\lambda \in \mathrm{H}^1(\widehat{A}[2])$ and $c_{e_2^\lambda} \in \mathrm{H}^1(\mathbf{Hom}(A[2],\mathbb{G}_m))$, which are identified by the leftmost vertical map e_2. Apply Corollary 3.8 with $M = A[2]$, $N = \mathbb{G}_m$, and $\beta = e_2^\lambda$, using $\mathbf{Ext}^1(A[2],\mathbb{G}_m) = 0$: map (a) gives the left hand side of (19) and map (d) gives the right hand side of (19) (written backwards) because of the identification of c_λ with c_{e^λ} via e_2. □

5.5. **Criteria for triviality of the obstruction.** The following lemma serves only to prove Proposition 5.6(a) below.

Lemma 5.5. *Let k be a field, and let G be a finite cyclic group.*

(a) *Let A be a finite-dimensional kG-module. Let $A^* := \mathrm{Hom}_k(A,k)$ be the dual representation, and let A^G be the subspace of G-invariant vectors. Then $\dim A^G = \dim(A^*)^G$.*

(b) *If $0 \to A \to B \to C \to 0$ is an exact sequence of finite-dimensional kG-modules, and the surjection $B^* \to A^*$ admits a section as G-sets, then the connecting homomorphism $C^G \to \mathrm{H}^1(G,A)$ is 0.*

Proof.

(a) Let g be a generator of G. If M is a matrix representing the action of g on A, the action of g^{-1} on A^* is given by the transpose M^t. Then $\dim A^G = \dim\ker(M-1) = \dim\ker(M^t-1) = \dim(A^*)^G$, where the middle equality follows from Jordan canonical form (after extending scalars to $\overline{k}$).

(b) The section gives the 0 at the right in

$$0 \to (C^*)^G \to (B^*)^G \to (A^*)^G \to 0.$$

Taking dimensions and applying (a) yields $\dim B^G = \dim A^G + \dim C^G$. This together with the exactness of

$$0 \to A^G \to B^G \to C^G \to \mathrm{H}^1(G,A)$$

implies that the connecting homomorphism $C^G \to \mathrm{H}^1(G,A)$ is 0. □

Proposition 5.6. *Let $\lambda\colon A \to \widehat{A}$ be a self-dual homomorphism of abelian varieties over a field k. Suppose that at least one of the following hypotheses holds:*

(a) $\operatorname{char} k \neq 2$ *and the image G of $G_k \to \operatorname{Aut} A[2](k_s)$ is cyclic.*

(b) *k is a perfect field of characteristic 2.*

(c) *k is $\mathbb{R}$ or $\mathbb{C}$.*

(d) *k is a nonarchimedean local field of residue characteristic not 2, and A has* good reduction *(i.e., extends to an abelian scheme over the valuation ring of k).*

(e) *k is a finite field.*

Then $c_\lambda = 0$.

Proof.

(a) Apply Lemma 5.5(b) to the bottom row of (17), viewed as a sequence of $\mathbb{F}_2 G$-modules; it applies since the dual sequence is (6) for $M := A[2]$, and the section s of Section 3.1 yields a G-set section $A[2] \to (\mathscr{U} A[2])^{\mathrm{ab}} \otimes \mathbb{F}_2$. Thus the top horizontal map in

$$\begin{array}{ccc} \mathrm{H}^0(G, \mathbf{Hom}(\bigwedge^2 A[2], \mathbb{G}_m)) & \longrightarrow & \mathrm{H}^1(G, \widehat{A}[2]) \\ \| & & \downarrow \\ \mathrm{H}^0(G_k, \mathbf{Hom}(\bigwedge^2 A[2], \mathbb{G}_m)) & \xrightarrow{\delta} & \mathrm{H}^1(G_k, \widehat{A}[2]) \end{array}$$

is 0. Thus $\delta = 0$. Now (17) shows that $c_\lambda = \delta(e_2^\lambda) = 0$.

(b) Let $M := A[2]$, and let $M^\vee := \mathbf{Hom}(M, \mathbb{G}_m) = \widehat{A}[2]$ be its Cartier dual. The bottom row of (17) yields an exact sequence

$$\mathrm{H}^0(\mathbf{Hom}((\mathscr{U} M)^{\mathrm{ab}} \otimes \mathbb{F}_2, \mathbb{G}_m)) \to \mathrm{H}^0(\mathbf{Hom}(\bigwedge^2 M, \mathbb{G}_m)) \xrightarrow{\delta} \mathrm{H}^1(M^\vee). \tag{20}$$

It suffices to prove that $\delta = 0$, or that the first map is surjective. Equivalently, by the universal property of $(\mathscr{U} M)^{\mathrm{ab}} \otimes \mathbb{F}_2$, we need each alternating pairing $b\colon M \times M \to \boldsymbol{\mu}_2$ to be $q(x+y) - q(x) - q(y)$ for some quadratic map $q\colon M \to \boldsymbol{\mu}_2$.

In fact, we will prove this for *every* finite commutative group scheme M over k with $2M = 0$. Since k is perfect, there is a canonical decomposition $M = M_{el} \oplus M_{le} \oplus M_{ll}$ into étale-local, local-étale, and local-local subgroup schemes. Then $M^\vee = (M_{le})^\vee \oplus (M_{el})^\vee \oplus (M_{ll})^\vee$. The homomorphism $M \to M^\vee$ induced by the alternating pairing must map M_{el} to $(M_{le})^\vee$, and M_{le} to $(M_{el})^\vee$, and M_{ll} to $(M_{ll})^\vee$. In particular, $b = b_e + b_{ll}$ where b_e and

b_{ll} are alternating pairings on $M_{el} \oplus M_{le}$ and M_{ll}, respectively. The pairing b_e necessarily has the form

$$(m_{el}, m_{le}), (m'_{el}, m'_{le}) \mapsto B(m_{el}, m'_{le})B(m'_{el}, m_{le})$$

for some bilinear pairing $B\colon M_{el} \times M_{le} \to \boldsymbol{\mu}_2$. Then b_e comes from the quadratic map $(m_{el}, m_{le}) \mapsto B(m_{el}, m_{le})$.

It remains to consider the case $M = M_{ll}$. Then $M^\vee(k_s) = 0$. By [Mil06, Theorem III.6.1 and the paragraph preceding it], $\mathrm{H}^1(M^\vee) = \mathrm{H}^1(G_k, M^\vee(k_s)) = \mathrm{H}^1(G_k, 0) = 0$, so $\delta = 0$.

(c) Follows from (a).
(d) The assumptions imply $k(A[2])$ is unramified over k (see [ST68, Theorem 1], for example), so (a) applies.
(e) Follows from (a) and (b). □

5.6. **Formula for the obstruction in the case of a line sheaf on a torsor.** Let P be a torsor under A. For $a \in A(S)$, let $\tau_a\colon P \to P$ be the translation. Also, for $x \in P(S)$, let $\tau_x\colon A \to P$ be the torsor action. The maps τ_x^* for local choices of sections x induce a well-defined isomorphism $\mathbf{Pic}^0_{P/S} \simeq \mathbf{Pic}^0_{A/S}$ since any τ_a^* is the identity on $\mathbf{Pic}^0_{A/S}$. Let $\mathscr{L} \in \mathbf{Pic}_{P/S}(S)$. Generalizing (13), we define

$$\begin{aligned} \phi_{\mathscr{L}}\colon A &\to \mathbf{Pic}_{P/S} \simeq \mathbf{Pic}_{A/S} \\ a &\mapsto \tau_a^*\mathscr{L} \otimes \mathscr{L}^{-1}. \end{aligned}$$

We may view $\phi_{\mathscr{L}}$ as an element of $\operatorname{Hom}_{\text{self-dual}}(A, \widehat{A})$. If $x \in P(S)$, then $\phi_{\tau_x^*\mathscr{L}} = \phi_{\mathscr{L}}$.

Proposition 5.7. *Let P be a torsor under A, equipped with an order-2 automorphism $\iota\colon P \to P$ compatible with $[-1]\colon A \to A$. The fixed locus P^ι of ι is a torsor under $A[2]$; let $c \in \mathrm{H}^1(A[2])$ be its class. Let $\mathscr{L} \in \mathbf{Pic}_{P/S}(S)$ be such that $\iota^*\mathscr{L} \simeq \mathscr{L}$, and let $\lambda = \phi_{\mathscr{L}}\colon A \to \widehat{A}$. Then $c_\lambda = \lambda(c)$ in $\mathrm{H}^1(\widehat{A}[2])$.*

Proof. If x is a section of P^ι, then $[-1]^*\tau_x^*\mathscr{L} \simeq \tau_x^*\iota^*\mathscr{L} \simeq \tau_x^*\mathscr{L}$, so we obtain a map

$$\begin{aligned} \gamma\colon P^\iota &\to \mathbf{Pic}^{\mathrm{Sym}}_{A/S} \\ x &\to \tau_x^*\mathscr{L}. \end{aligned}$$

For sections $a \in A[2]$ and $x \in P^\iota$, we have

$$\gamma(a + x) = \tau_{a+x}^*\mathscr{L} = \tau_a^*(\tau_x^*\mathscr{L}) = \phi_{\tau_x^*\mathscr{L}}(a) \otimes \tau_x^*\mathscr{L} = \lambda(a) \otimes \gamma(x)$$

in $\mathbf{Pic}^{\mathrm{Sym}}_{A/S}$. In other words, γ is a torsor map (with respect to $\lambda\colon A[2] \to \widehat{A}[2]$) from the torsor P^ι (under $A[2]$) to the torsor (under $\widehat{A}[2]$) of line sheaves in $\mathbf{Pic}^{\mathrm{Sym}}_{A/S}$ with Néron-Severi class λ. Taking classes of these torsors yields $\lambda(c) = c_\lambda$. □

5.7. **Application to Jacobians.** Let $X \to S$ be a family of genus-g curves, by which we mean a smooth proper morphism whose geometric fibers are integral curves of genus g. (If $g \neq 1$, then the relative canonical sheaf or its inverse makes $X \to S$ projective: see Remark 2 on page 252 of [BLR90].) By the statement and proof of Proposition 4 on page 260 of [BLR90],

(1) There is a decomposition of functors $\mathbf{Pic}_{X/S} \simeq \coprod_{n \in \mathbb{Z}} \mathbf{Pic}^n_{X/S}$.
(2) The subfunctor $\mathbf{Pic}^0_{X/S}$ is (represented by) a projective abelian scheme A over S.

(3) The subfunctor $\mathbf{Pic}^{g-1}_{X/S}$ is (represented by) a smooth projective scheme P over S, a torsor under A. (If $g = 1$, then $P = A$.)
(4) The scheme-theoretic image of the "summing" map $X^{g-1} \to P$ is an effective relative Cartier divisor on P (take this to be empty if $g = 0$). Let Θ be the associated line sheaf on P.
(5) The homomorphism $\lambda := \phi_\Theta \colon A \to \widehat{A}$ is an isomorphism.
(6) Define $\iota \colon P \to P$ by $\mathscr{F} \mapsto \omega_{X/S} \otimes \mathscr{F}^{-1}$; then $\iota^*\Theta \simeq \Theta$. (To prove this, one can reduce to the case where S is a moduli scheme of curves with level structure, and then to the case where S is the spectrum of a field, in which case it is a consequence of the Riemann-Roch theorem.)

Definition 5.8. The theta characteristic torsor $\mathcal{T}$ is the closed subscheme of $P = \mathbf{Pic}^{g-1}_{X/S}$ parametrizing classes whose square is the canonical class $\omega_{X/S} \in \mathbf{Pic}^{2g-2}_{X/S}(S)$.

Equivalently, $\mathcal{T} = P^\iota$. Let $c_\mathcal{T} \in \mathrm{H}^1(A[2])$ be the class of this torsor.

Theorem 5.9. *Let $X \to S$ be a family of genus-g curves, and let $A, \lambda, c_\mathcal{T}$ be as above. Then $c_\lambda = \lambda(c_\mathcal{T})$ in $\mathrm{H}^1(\widehat{A}[2])$, and for any $x \in \mathrm{H}^1(A[2])$ we have*

$$x \underset{e_2^\lambda}{\cup} x = x \underset{e_2^\lambda}{\cup} c_\mathcal{T} \tag{21}$$

in $\mathrm{H}^2(\mathbb{G}_m)$.

Proof. Proposition 5.7 with $P = \mathbf{Pic}^{g-1}_{X/S}$ and $\mathscr{L} = \Theta$ yields $c_\lambda = \lambda(c_\mathcal{T})$. So (19) in Theorem 5.4 becomes (21). ☐

Remark 5.10. If $S = \operatorname{Spec} k$ for a perfect field k of characteristic 2, then Proposition 5.6(b) gives $c_\lambda = 0$, so $c_\mathcal{T} = 0$. In fact, the proof produces a canonical k-point of $\mathcal{T}$. This generalizes an observation of D. Mumford [Mum71, p. 191] that a curve over an algebraically closed field of characteristic 2 has a canonical theta characteristic.

5.8. **Hyperelliptic Jacobians.**

Proposition 5.11. *If E is an elliptic curve, then $x \underset{e_2^\lambda}{\cup} x = 0$ for all $x \in \mathrm{H}^1(E[2])$. The same holds for the Jacobian of any hyperelliptic curve X if it has a rational Weierstrass point or its genus is odd. In particular, this applies to $y^2 = f(x)$ with f separable of degree $n \not\equiv 2 \pmod 4$ over a field of characteristic not 2.*

Proof. For an elliptic curve E, the trivial line sheaf $\mathscr{O}_E$ is a theta characteristic defined over k. Now suppose that X is a hyperelliptic curve of genus g, so it is a degree-2 cover of a genus-0 curve Y. The class of a point in $Y(k_s)$ pulls back to a k-point of $\mathbf{Pic}^2_{X/k}$, and if g is odd, multiplying by $(g-1)/2$ gives a k-point of $\mathcal{T}$. On the other hand, if X has a rational Weierstrass point P, then $\mathscr{O}((g-1)P)$ is a theta characteristic defined over k. So $\mathcal{T}$ is trivial in all these cases. Now apply Theorem 5.9. ☐

Example 5.12. Fix $g \in 1$. Suppose that X is (the smooth projective model of) the curve $y^2 = f(x)$ where f is a degree-$2g+2$ separable polynomial over a field k of characteristic not 2. Let $\mathfrak{a} \in \mathbf{Pic}^2_{X/k}(k)$ be the point in the proof of Proposition 5.11. Let Δ be the set of zeros of f in k_s, so $\#\Delta = 2g+2$. Fix $m \in \mathbb{Z}$. Let Δ_m be the set of unordered partitions of Δ into two subsets whose size has the same parity as m, so $\#\Delta_m = 2^{2g}$. For each $\{A, B\} \in \Delta_m$, take the class of the sum of the points in A and add an integer multiple of to get a class in $\operatorname{Pic}^m(X_{k_s})$. The set of such classes is a torsor $\mathcal{W}_m$ of $A[2]$. Moreover, $\mathcal{T} \simeq \mathcal{W}_{g-1}$ (cf. [Mum71, p. 191]). Using this, one can show:

(a) For $f(x) = (x^2+1)(x^2-3)(x^2+3)$ over $\mathbb{Q}_3$, we have $c_{\mathcal{T}} \neq 0$.
(b) For $f(x) = x^6+x+6$ over $\mathbb{Q}$, we have $0 \neq c_{\mathcal{T}} \in Ш^1(\mathbb{Q}, A[2])$, where $Ш^1$ is defined in (12). (*Proof:* The discriminant of f is $-\ell$, where ℓ is the prime 362793931. For $p \notin \{2, \ell\}$, the element $c_{\mathcal{T}}$ maps to 0 in $\mathrm{H}^1(\mathbb{Q}_p, A[2])$ by Proposition 5.6(c,d), and $f(x)$ has a zero in each of $\mathbb{Q}_2$ and $\mathbb{Q}_\ell$, so the same is true at those places. On the other hand, the Galois group of f over $\mathbb{Q}$ is S_6, so $c_{\mathcal{T}} \neq 0$.)
(c) For random $f(x) \in \mathbb{Z}[x]$ of degree $2g+2$ with coefficients in $[-B, B]^{2g+3}$, the probability that $Ш^1(\mathbb{Q}, A[2]) = 0$ tends to 1 as $B \to \infty$. (*Sketch of proof:* By Proposition 4.1(e) we may assume $g \geq 2$. By the Hilbert irreducibility theorem, the group $\operatorname{Gal}(\mathbb{Q}(A[2])/\mathbb{Q}) \simeq \operatorname{Gal}(f)$ is as large as possible, i.e., equal to S_{2g+2}, with probability tending to 1. The G_k-module $A[2]$ may be identified with the sum-0 part of the permutation module $\mathbb{F}_2^{2g+2}$ modulo the diagonal image of $\mathbb{F}_2$; let $\mathbb{F}_2^{2g}$ be this quotient. By Proposition 4.1(c), $Ш^1(\mathbb{Q}, A[2]) \subseteq \mathrm{H}^1(S_{2g+2}, \mathbb{F}_2^{2g}) \subset \mathrm{H}^1(\mathbb{Q}, A[2])$. The group $\mathrm{H}^1(S_{2g+2}, \mathbb{F}_2^{2g})$ is of order 2, generated by the class $c_{\mathcal{W}_1} \in \mathrm{H}^1(\mathbb{Q}, A[2])$ of $\mathcal{W}_1$ [Pol71, Theorem 5.2]. Computations as in [PS99, §9.2] show that for each prime p, the probability that $f(x)$ factors over $\mathbb{Z}_p$ into irreducible polynomials of degree $2g$ and 2 defining unramified and ramified extensions of $\mathbb{Q}_p$, respectively, is of order $1/p$ (not smaller) as $p \to \infty$, and in this case no point in $\mathcal{W}_1$ is $G_{\mathbb{Q}_p}$-invariant, $c_{\mathcal{W}_1}$ has nonzero image in $\mathrm{H}^1(\mathbb{Q}_p, A[2])$. Since the conditions at finitely many p are asymptotically independent as $B \to \infty$, and since $\sum 1/p$ diverges, there will exist such a prime p for almost all f, and in this case $c_{\mathcal{W}_1} \notin Ш^1(\mathbb{Q}, A[2])$, so $Ш^1(\mathbb{Q}, A[2]) = 0$.)

Part (c) can be extended to an arbitrary global field of characteristic not 2.

5.9. **Jacobians with generic 2-torsion.** Suppose that X is a curve of genus $g \geq 2$ over a field of characteristic not 2 such that the image G of $G_k \to \operatorname{Aut} A[2]$ is as large as possible, i.e., $\mathrm{Sp}_{2g}(\mathbb{F}_2)$. (This forces X to be non-hyperelliptic if $g \geq 3$.) By [Pol71, Theorems 4,1 and 4.8], the group $\mathrm{H}^1(G, A[2]) \subseteq \mathrm{H}^1(G_k, A[2])$ is of order 2, generated by $c_{\mathcal{T}}$. So Proposition 4.1(c) shows that $Ш^1(k, A[2])$ is of order 2 or 1, according to whether the nonzero class $c_{\mathcal{T}}$ lies in $Ш^1(k, A[2])$ or not.

6. Selmer groups as intersections of two maximal isotropic subgroups

6.1. **Quadratic form arising from the Heisenberg group.** Let $A \to S$ be an abelian scheme. Let $\mathscr{L}$ be a symmetric line sheaf on A such that the homomorphism $\lambda := \phi_{\mathscr{L}}$ is an isogeny.

Example 6.1. For any self-dual isogeny $\mu\colon A \to \widehat{A}$, the isogeny $\lambda := 2\mu$ is of the form $\phi_{\mathscr{L}}$ as above. Namely, take $\mathscr{L} := (1, \mu)^*\mathscr{P}$, where $\mathscr{P}$ is the Poincaré line sheaf on $A \times \widehat{A}$ (see [Mum70, §20, proof of Theorem 2]). Alternatively, the existence of $\mathscr{L}$ follows from $c_{2\mu} = 2c_\mu = 0$.

The pairs (x,ϕ) where $x \in A(S)$ and ϕ is an isomorphism from $\mathscr{L}$ to $\tau_x^*\mathscr{L}$ form a (usually nonabelian) group under the operation

$$(x,\phi)(x',\phi') = (x+x', (\tau_{x'}\phi)\phi').$$

The same can be done after base extension, so we get a group functor. Automorphisms of $\mathscr{L}$ induce the identity on this group functor, so it depends only on the class of $\mathscr{L}$ in $\operatorname{Pic} A$.

Proposition 6.2 (Mumford)**.**

(a) *This functor is representable by an fppf group scheme $\mathcal{H}(\mathscr{L})$, called the* Heisenberg group *(or* theta group *or* Mumford group*).*

(b) *It fits in an exact sequence*

$$1 \to \mathbb{G}_m \to \mathcal{H}(\mathscr{L}) \to A[\lambda] \to 1, \tag{22}$$

where the two maps in the middle are given by $t \mapsto (0, \text{multiplication by } t)$ and (x,ϕ) to x. This exhibits $\mathcal{H}(\mathscr{L})$ as a central extension of fppf group schemes.

(c) *The induced commutator pairing*

$$A[\lambda] \times A[\lambda] \to \mathbb{G}_m$$

is the Weil pairing e_λ.

Proof. See [Mum91, pp. 44–46]. ☐

Corollary 6.3. *The connecting homomorphism $q\colon \mathrm{H}^1(A[\lambda]) \to \mathrm{H}^2(\mathbb{G}_m)$ induced by (22) is a quadratic form whose associated bilinear pairing $\mathrm{H}^1(A[\lambda]) \times \mathrm{H}^1(A[\lambda]) \to \mathrm{H}^2(\mathbb{G}_m)$ sends (x,y) to $-x \underset{e_\lambda}{\cup} y$.*

Proof. Proposition 3.9 applied to (22) shows that q is a quadratic *map* giving rise to the bilinear pairing claimed. By Remark 2.1, it remains to prove the identity $q(-v) = q(v)$. Functoriality of (22) with respect to the automorphism $[-1]$ of A gives a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathcal{H}(\mathscr{L}) & \longrightarrow & A[\lambda] & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow{\scriptstyle -1} & & \\ 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathcal{H}([-1]^*\mathscr{L}) & \longrightarrow & A[\lambda] & \longrightarrow & 1 \end{array}$$

But $[-1]^*\mathscr{L} \simeq \mathscr{L}$, so both rows give rise to q. Functoriality of the connecting homomorphism gives $q(-v) = q(v)$ for any $v \in \mathrm{H}^1(A[\lambda])$. ☐

The exact sequence

$$0 \to A[\lambda] \to A \xrightarrow{\lambda} \widehat{A} \to 0$$

gives rise to the "descent sequence"

$$0 \to \frac{\widehat{A}(S)}{\lambda A(S)} \xrightarrow{\delta} \mathrm{H}^1(A[\lambda]) \to \mathrm{H}^1(A)[\lambda] \to 0, \tag{23}$$

where $\mathrm{H}^1(A)[\lambda]$ is the kernel of the homomorphism $\mathrm{H}^1(A) \to \mathrm{H}^1(\widehat{A})$ induced functorially by λ.

Proposition 6.4. *Identify $\widehat{A}(S)/\lambda A(S)$ with its image W under δ in (23). Then $q|_W = 0$.*

Proof. Let $\mathscr{P}$ be the Poincaré line sheaf on $A \times \widehat{A}$. For $y \in \widehat{A}(S)$, let $\mathscr{P}_y$ be the line sheaf on A obtained by restricting $\mathscr{P}$ to $A \times \{y\}$. For any $y_1, y_2 \in \widehat{A}(S)$, there is a canonical isomorphism $\iota_{y_1,y_2} \colon \mathscr{P}_{y_1} \otimes \mathscr{P}_{y_2} \to \mathscr{P}_{y_1+y_2}$, satisfying a cocycle condition [Pol03, §10.3].

The group $\mathcal{H}(\mathscr{L})(S)$ acts on the left on the set of triples (x, y, ϕ) where $x \in A(S)$, $y \in \widehat{A}(S)$, and $\phi \colon \mathscr{L} \otimes \mathscr{P}_y \to (\tau_x^* \mathscr{L})$ as follows:

$$(x, \phi)(x', y', \phi') = (x + x', y', (\tau_{x'}\phi)\phi').$$

The same holds after base extension, and we get a sheaf of sets $\mathcal{G}(\mathscr{L})$ on which $\mathcal{H}(\mathscr{L})$ acts freely. There is a morphism $\mathcal{G}(\mathscr{L}) \to \widehat{A}$ sending (x, y, ϕ) to y, and this identifies $\widehat{A}$ with the quotient sheaf $\mathcal{H}(\mathscr{L})\backslash\mathcal{G}(\mathscr{L})$. There is also a morphism $\mathcal{G}(\mathscr{L}) \to A$ sending (x, y, ϕ) to x, and the action of $\mathcal{H}(\mathscr{L})$ on $\mathcal{G}(\mathscr{L})$ is compatible with the action of its quotient $A[\lambda]$ on A. Thus we have the following compatible diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathcal{H}(\mathscr{L}) & \dashrightarrow & \mathcal{G}(\mathscr{L}) & \longrightarrow & \widehat{A} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A[\lambda] & \longrightarrow & A & \xrightarrow{\lambda} & \widehat{A} & \longrightarrow & 0
\end{array}$$

where the first row indicates only that $\mathcal{H}(\mathscr{L})$ acts freely on $\mathcal{G}(\mathscr{L})$ with quotient being $\widehat{A}$. This is enough to give a commutative square of pointed sets

$$\begin{array}{ccc}
\mathrm{H}^0(\widehat{A}) & \longrightarrow & \mathrm{H}^1(\mathcal{H}(\mathscr{L})) \\
\| & & \downarrow \\
\mathrm{H}^0(\widehat{A}) & \longrightarrow & \mathrm{H}^1(A[\lambda]),
\end{array}$$

so $\mathrm{H}^0(\widehat{A}) \to \mathrm{H}^1(A[\lambda])$ factors through $\mathrm{H}^1(\mathcal{H}(\mathscr{L}))$. But the sequence $\mathrm{H}^1(\mathcal{H}(\mathscr{L})) \to \mathrm{H}^1(A[\lambda]) \to \mathrm{H}^2(\mathbb{G}_m)$ from (22) is exact, so the composition $\mathrm{H}^0(\widehat{A}) \to \mathrm{H}^1(A[\lambda]) \to \mathrm{H}^2(\mathbb{G}_m)$ is 0. □

6.2. **Local fields.** Let k_v be a local field. The group $\mathrm{H}^1(k_v, A[\lambda])$ has a topology making it locally compact, the group $\mathrm{H}^2(k_v, \mathbb{G}_m)$ may be identified with a subgroup of $\mathbb{Q}/\mathbb{Z}$ and given the discrete topology, and the quadratic form $q \colon \mathrm{H}^1(k_v, A[\lambda]) \to \mathrm{H}^2(k_v, \mathbb{G}_m)$ is continuous (cf. [Mil06, III.6.5]; the same arguments work even though (22) has a nonabelian group in the middle). The composition

$$\mathrm{H}^1(k_v, A[\lambda]) \xrightarrow{q} \mathrm{H}^2(k_v, \mathbb{G}_m) \hookrightarrow \mathbb{Q}/\mathbb{Z}.$$

is a quadratic form q_v. By local duality [Mil06, I.2.3, I.2.13(a), III.6.10], q_v is nondegenerate. Moreover, $\mathrm{H}^1(k_v, A[\lambda])$ is finite if $\operatorname{char} k_v \neq 0$ [Mil06, I.2.3, I.2.13(a)], and σ-compact in general [Mil06, III.6.5(a)], so it is second-countable by Corollary 2.12.

Proposition 6.5. *Let k_v be a local field. In* (23) *for $S = \operatorname{Spec} k_v$, the group $W \simeq \widehat{A}(k_v)/\lambda A(k_v)$ is a compact open maximal isotropic subgroup of* $(\mathrm{H}^1(k_v, A[\lambda]), q_v)$, *which is therefore weakly metabolic.*

Proof. By Proposition 6.4, q_v restricts to 0 on W, so it suffices to show that $W^\perp = W$. Let $A(k_v)_\bullet$ be $A(k_v)$ modulo its connected component (which is nonzero only if k_v is $\mathbb{R}$ or $\mathbb{C}$). Then W is the image of $\widehat{A}(k_v)_\bullet \to \mathrm{H}^1(k_v, A[\lambda])$, so $W^\perp$ is the kernel of the dual map, which by Tate local duality [Mil06, I.3.4, I.3.7, III.7.8] is $\mathrm{H}^1(k_v, A[\lambda]) \to \mathrm{H}^1(k_v, A)$. This kernel is W, by exactness of (23). $\square$

Proposition 6.6. *Suppose that k_v is nonarchimedean and that $\mathcal{O}_v$ is its valuation ring. Suppose that A extends to an abelian scheme (again denoted A) over $\mathcal{O}_v$. Then the subgroup $W \simeq \widehat{A}(k_v)/\lambda A(k_v)$ equals the open subgroup $\mathrm{H}^1(\mathcal{O}_v, A[\lambda])$ of $\mathrm{H}^1(k_v, A[\lambda])$. In particular, $\mathrm{H}^1(\mathcal{O}_v, A[\lambda])$ is a maximal isotropic subgroup.*

Proof. Let $\mathbb{F}_v$ be the residue field of $\mathcal{O}_v$. By [Mil80, III.3.11(a)] and [Lan56], respectively, $\mathrm{H}^1(\mathcal{O}_v, A) \simeq \mathrm{H}^1(\mathbb{F}_v, A) = 0$. The valuative criterion for properness [Har77, II.4.7] yields $A(\mathcal{O}_v) = A(k_v)$ and $\widehat{A}(\mathcal{O}_v) = \widehat{A}(k_v)$. So taking cohomology of (23) over $\mathcal{O}_v$ gives the result. $\square$

6.3. **Global fields.** Let k be a global field. For any nonempty subset $\mathcal{S}$ of Ω containing the archimedean places, define the ring of $\mathcal{S}$-integers $\mathcal{O}_{\mathcal{S}} := \{x \in k : v(x) \geq 0 \text{ for all } v \notin \mathcal{S}\}$.

Let A be an abelian variety over k, As in Section 6.1, let $\mathscr{L}$ be a symmetric line sheaf on A be such that the homomorphism $\lambda := \phi_{\mathscr{L}}$ is an isogeny. Choose a nonempty finite $\mathcal{S}$ containing all bad places, by which we mean that $\mathcal{S}$ contains all archimedean places and A extends to an abelian scheme A over $\mathcal{O}_{\mathcal{S}}$. In Example 2.18 take $I = \Omega$, $V_i = \mathrm{H}^1(k_v, A[\lambda])$, $Q_i = q_v$, and $W_i = \widehat{A}(k_v)/\lambda A(k_v)$, which is valid by Proposition 6.5. The resulting restricted direct product

$$V := \prod_{v\in\Omega}{}' \left(\mathrm{H}^1(k_v, A[\lambda]), \frac{\widehat{A}(k_v)}{\lambda A(k_v)} \right)$$

equipped with the quadratic form

$$Q\colon \prod_{v\in\Omega}{}' \left(\mathrm{H}^1(k_v, A[\lambda]), \frac{\widehat{A}(k_v)}{\lambda A(k_v)} \right) \to \mathbb{Q}/\mathbb{Z}$$

$$(\xi_v)_{v\in\Omega} \mapsto \sum_v q_v(\xi_v).$$

is a second-countable weakly metabolic locally compact quadratic module. Proposition 6.6, which applies for all but finitely many v, shows that

$$V = \prod_{v\in\Omega}{}' \left(\mathrm{H}^1(k_v, A[\lambda]), \mathrm{H}^1(\mathcal{O}_v, A[\lambda]) \right).$$

(The subgroup $\mathrm{H}^1(\mathcal{O}_v, A[\lambda])$ is defined and equal to $\widehat{A}(k_v)/\lambda A(k_v)$ only for $v \notin \mathcal{S}$, but that is enough.)

As usual, define the Selmer group

$$\mathrm{Sel}_\lambda(A) := \ker \left(\mathrm{H}^1(k, A[\lambda]) \to \prod_{v\in\Omega} \mathrm{H}^1(k_v, A) \right).$$

Example 6.7. By Remark 5.3 and [PS99, Corollary 2], the element of $c_\lambda \in \mathrm{H}^1(\widehat{A}[2])$ of (18) belongs to $\mathrm{Sel}_2(\widehat{A})$.

Below will appear $Ш^1(k, A[\lambda])$, which is a subgroup of $\mathrm{Sel}_\lambda(A)$, and is not to be confused with the Shafarevich-Tate group $Ш^1(k, A)$.

Theorem 6.8.

(a) *The images of the homomorphisms*

$$\begin{array}{ccc} & & \mathrm{H}^1(k, A[\lambda]) \\ & & \downarrow \\ \prod_{v\in\Omega} \frac{\widehat{A}(k_v)}{\lambda A(k_v)} & \longrightarrow & \prod'_{v\in\Omega} (\mathrm{H}^1(k_v, A[\lambda]), \mathrm{H}^1(\mathcal{O}_v, A[\lambda])) \end{array}$$

are maximal isotropic subgroups with respect to Q.

(b) *The vertical map induces an isomorphism from* $\mathrm{Sel}_\lambda(A)/\text{Ш}^1(k, A[\lambda])$ *to the intersection of these two images. (See Section 4 for information about* $\text{Ш}^1(k, A[\lambda])$*, which is often* 0.*)*

Proof.

(a) The subgroup $\prod_{v\in\Omega} \widehat{A}(k_v)/\lambda A(k_v)$ (or rather its image W under the horizontal injection) is maximal isotropic by construction.

The vertical homomorphism $\mathrm{H}^1(k, A[\lambda]) \to \prod'_{v\in\Omega}(\mathrm{H}^1(k_v, A[\lambda]), \mathrm{H}^1(\mathcal{O}_v, A[\lambda]))$ is well-defined since each element of $\mathrm{H}^1(k, A[\lambda])$ belongs to the subgroup $\mathrm{H}^1(\mathcal{O}_\mathcal{T}, A[\lambda])$ for some finite $\mathcal{T} \subseteq \Omega$ containing $\mathcal{S}$, and $\mathcal{O}_\mathcal{T} \subseteq \mathcal{O}_v$ for all $v \notin \mathcal{T}$. Let W be the image. Suppose that $s \in \mathrm{H}^1(k, A[\lambda])$, and let $w \in W$ be its image. The construction of the quadratic form of Corollary 6.3 is functorial with respect to base extension, so $Q(w)$ can be computed by evaluating the global quadratic form

$$q\colon \mathrm{H}^1(k, A[\lambda]) \to \mathrm{H}^2(k, \mathbb{G}_m)$$

on s, and afterwards summing the local invariants. Exactness of

$$0 \to \mathrm{H}^2(k, \mathbb{G}_m) \to \bigoplus_{v\in\Omega} \mathrm{H}^2(k_v, \mathbb{G}_m) \xrightarrow{\sum \mathrm{inv}} \mathbb{Q}/\mathbb{Z} \to 0$$

in the middle (the reciprocity law for the Brauer group: see [GS06, Remark 6.5.6] for references) implies that the sum of the local invariants of our global class is 0. Thus $Q|_W = 0$.

It remains to show that W is its own annihilator. Since e_λ identifies $A[\lambda]$ with its own Cartier dual, the middle three terms of the 9-term Poitou-Tate exact sequence ([Mil06, I.4.10(c)] and [GA09, 4.11]) give the self-dual exact sequence

$$\mathrm{H}^1(k, A[\lambda]) \xrightarrow{\beta_1} \prod'_{v\in\Omega}(\mathrm{H}^1(k_v, A[\lambda]), \mathrm{H}^1(\mathcal{O}_v, A[\lambda])) \xrightarrow{\gamma_1} \mathrm{H}^1(k, A[\lambda])^*,$$

where $*$ denotes Pontryagin dual. Since $W = \mathrm{im}(\beta_1)$ and the dual of β_1 is γ_1,

$$W^\perp = \ker(\gamma_1) = \mathrm{im}(\beta_1) = W.$$

(b) This follows from the exactness of (23) for $S = \mathrm{Spec}\, k_v$ for each $v \in \Omega$. □

Remark 6.9. There is a variant of Theorem 6.8 in which the infinite restricted direct product is taken over only a *subset* $\mathcal{S}$ of Ω containing all bad places and all places of residue characteristic dividing $\deg \lambda$. If $\mathcal{S}$ is finite, then the restricted direct product becomes a finite direct product. The same proof as before shows that the images of $\prod_{v\in\mathcal{S}} \widehat{A}(k_v)/\lambda A(k_v)$

and $\mathrm{H}^1(\mathcal{O}_{\mathcal{S}}, A[\lambda])$ are maximal isotropic. The intersection of the images equals the image of $\mathrm{Sel}_\lambda(A)$.

Remark 6.10. Suppose that $A = \mathrm{Jac}\, X$ and λ is multiplication-by-2, with $\mathscr{L}$ as in Example 6.1. Then, as in Remark 2.8, q_v takes values in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ (instead of just $\frac{1}{4}\mathbb{Z}/\mathbb{Z}$) if and only if the element $c_{\mathcal{T},v} \in \mathrm{H}^1(k_v, A[2])$ in Theorem 5.9 for X_{k_v} is 0. Thus Q takes values in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ if and only if $c_{\mathcal{T}} \in Ш^1(k, A[2])$.

Remark 6.11. Suppose that we are considering a family of abelian varieties with a systematic subgroup G of $\mathrm{Sel}_\lambda(A)$ coming from rational points (e.g., a family of elliptic curves with rational 2-torsion). Let X be the image of G in $\prod'_{v\in\Omega}(\mathrm{H}^1(k_v, A[\lambda]), \mathrm{H}^1(\mathcal{O}_v, A[\lambda]))$. Then our model for $\mathrm{Sel}_\lambda(A)$ should be that its image in $X^\perp/X$ is an intersection of random maximal isotropic subgroups. In particular, the size of $\mathrm{Sel}_\lambda(A)/Ш^1(k, A[\lambda])$ should be distributed as $\#X$ times the size of the random intersection.

Example 6.12. Suppose that $\mathrm{char}\, k \neq p$ and A is an elliptic curve $E\colon y^2 = f(x)$. The theta divisor Θ on E is the identity point with multiplicity 1. Let $\mathscr{L} = \mathscr{O}(p\Theta)$. Then λ is $E \xrightarrow{p} E$, and $\mathrm{Sel}_\lambda(A)$ is the p-Selmer group $\mathrm{Sel}_p(E)$. Moreover, $Ш^1(k, E[p]) = 0$ by Proposition 4.1(e). Thus Theorem 6.8 identifies $\mathrm{Sel}_p(E)$ as an intersection of maximal isotropic subspaces in an $\mathbb{F}_p$-vector space, even when $p = 2$, by Remark 6.10, because $c_{\mathcal{T}} = 0$ as in Proposition 5.11.

In particular, $\dim \mathrm{Sel}_p(E)$ should be expected to be distributed according to X_{Sel_p}, with the adjustment given by Remark 6.11 when necessary. When $p = 2$, this is known for the family of quadratic twists of $y^2 = x^3 - x$ over $\mathbb{Q}$ [HB94, Theorem 2], and for families of quadratic twists of other elliptic curves with rational 2-torsion over $\mathbb{Q}$ [SD08]. For the family of all elliptic curves over $\mathbb{Q}$, it is known that the average size of Sel_2 is 3 [BS10a] and the average size of Sel_3 is 4 [BS10b] (cf. Proposition 2.20). See [dJ02] for some earlier related investigations in the function field case. Other evidence is provided in [MR10], which, for an elliptic curve E over a number field k, gives lower bounds on the number of quadratic twists (up to a bound) with a prescribed value of $\dim \mathrm{Sel}_2$.

One can infer a prediction for the behavior of $\mathrm{Sel}_n(E)$ for any squarefree n, since the $\mathrm{Sel}_p(E)$ for different p should vary independently. For example, the average size of $\mathrm{Sel}_n(E)$ should be $\prod_{p|n}(p+1)$, the sum of the divisors of n, a suggestion put forth also by M. Bhargava.

Example 6.13. A similar argument suggests the distribution X_{Sel_2} for the 2-Selmer group of the Jacobian of a hyperelliptic curve $y^2 = f(x)$ with f separable of *odd* degree over a global field of characteristic not 2. (Apply Proposition 4.1(f).)

Example 6.14. Consider $y^2 = f(x)$ over $\mathbb{Q}$ with $\deg f = 2g + 2$ for even $g \geq 2$. Example 5.12(c) shows that $Ш^1(\mathbb{Q}, A[2])$ is 0 with probability 1. But the Hilbert irreducibility theorem shows that $c_{\mathcal{T}} \neq 0$ with probability 1, so Remarks 6.10 and 2.8 suggest that $\dim \mathrm{Sel}_2(A)$ now has the distribution $X_{\mathrm{Sel}_2} + 1$. In particular, this suggests that the average size of $\mathrm{Sel}_2(A)$ should be $\mathbb{E}\left(2^{X_{\mathrm{Sel}_2}+1}\right) = 6$ instead of 3.

In the analogous situation with g odd, it is less clear what to predict since it may be that the behavior of $c_{\mathcal{W}_1}$ invalidates the random model.

7. Relation to heuristics for Ш and rank

The Hilbert irreducibility theorem shows that asymptotically 100% of elliptic curves (ordered by naïve height) have $E(\mathbb{Q})[p] = 0$. (For much stronger results, see [Duk97] and

[Jon10].) So for statistical purposes, when letting E run over all elliptic curves, we may ignore contributions of torsion to the p-Selmer group.

In analogy with the Cohen-Lenstra heuristics [CL84], Delaunay has formulated a conjecture describing the distribution of Shafarevich-Tate groups of random elliptic curves over $\mathbb{Q}$. We now explain his conjectures for $\dim_{\mathbb{F}_p} Ш[p]$. For each prime p and $r \in \mathbb{Z}_{\geq 0}$, let $X_{Ш[p],r}$ be a random variable taking values in $2\mathbb{Z}_{\geq 0}$ such that

$$\operatorname{Prob}\left(X_{Ш[p],r} = 2n\right) \;=\; p^{-n(2r+2n-1)} \frac{\prod_{i=n+1}^{\infty}(1-p^{-(2r+2i-1)})}{\prod_{i=1}^{n}(1-p^{-2i})}.$$

The following conjecture is as in [Del01, Example F and Heuristic Assumption], with the correction that $u/2$ in the Heuristic Assumption is replaced by u (his u is our r). This correction was suggested explicitly in [Del07, §3.2] for rank 1, and it seems natural to make the correction for higher rank too.

Conjecture 7.1 (Delaunay)**.** *Let $r, n \in \mathbb{Z}_{\geq 0}$. If E ranges over elliptic curves over $\mathbb{Q}$ of rank r, up to isomorphism, ordered by conductor, then the fraction with* $\dim_{\mathbb{F}_p} Ш(E)[p] = 2n$ *equals* $\operatorname{Prob}\left(X_{Ш[p],r} = 2n\right)$.

If the "rank" r itself is a random variable R, viewed as a prior distribution, then the distribution of $\dim \operatorname{Sel}_p(E)$ should be given by $R + X_{Ш[p],R}$. On the other hand, Theorem 6.8 suggests that $\dim \operatorname{Sel}_p(E)$ should be distributed according to X_{Sel_p}. Let $R_{\text{conjectured}}$ be the random variable taking values 0 and 1 with probability 1/2 each.

Theorem 7.2. *For each prime p, the unique $\mathbb{Z}_{\geq 0}$-valued random variable R such that X_{Sel_p} and $R + X_{Ш[p],R}$ have the same distribution is $R_{\text{conjectured}}$.*

Proof. First we show that $R_{\text{conjectured}}$ has the claimed property. This follows from the following identities for $n \in \mathbb{Z}_{\geq 0}$:

$$\begin{aligned}
\operatorname{Prob}\left(X_{\operatorname{Sel}_p} = 2n\right) &= c \prod_{j=1}^{2n} \frac{p}{p^j - 1} \\
&= \frac{1}{2} \prod_{i \geq 0} (1 - p^{-(2i+1)}) \cdot p^{-n(2n-1)} \prod_{j=1}^{2n} (1 - p^{-j})^{-1} \\
&= \frac{1}{2} p^{-n(2n-1)} \prod_{i \geq n+1} (1 - p^{-(2i-1)}) \prod_{i=1}^{n} (1 - p^{-2i})^{-1} \\
&= \frac{1}{2} \operatorname{Prob}\left(X_{Ш[p],0} = 2n\right)
\end{aligned}$$

$$\begin{aligned}
\operatorname{Prob}\left(X_{\mathrm{Sel}_p} = 2n+1\right) &= c \prod_{j=1}^{2n+1} \frac{p}{p^j - 1} \\
&= \frac{1}{2} \prod_{i \geq 0} (1 - p^{-(2i+1)}) \cdot p^{-n(2n+1)} \prod_{j=1}^{2n+1} (1 - p^{-j})^{-1} \\
&= \frac{1}{2} p^{-n(2n+1)} \prod_{i \geq n+1} (1 - p^{-(2i+1)}) \prod_{i=1}^{n} (1 - p^{-2i})^{-1} \\
&= \frac{1}{2} \operatorname{Prob}\left(X_{\text{Ш}[p],1} = 2n\right).
\end{aligned}$$

Next we show that any random variable R with the property has the same distribution as $R_{\text{conjectured}}$. For $r \in \mathbb{Z}_{\geq 0}$, define a function $f_r \colon \mathbb{Z}_{\geq 0} \to \mathbb{R}$ by $f_r(s) := \operatorname{Prob}(X_{\text{Ш}[p],r} = s - r)$. The assumption on R implies that

$$\sum_{r=0}^{\infty} \operatorname{Prob}(R = r) f_r(s) = \sum_{r=0}^{\infty} \operatorname{Prob}\left(R_{\text{conjectured}} = r\right) f_r(s).$$

Thus to prove that R and $R_{\text{conjectured}}$ have the same distribution, it will suffice to prove that the functions f_r are linearly independent in the sense that for any sequence of real numbers $(\alpha_r)_{r \geq 0}$ with $\sum_{r \geq 0} |\alpha_r| < \infty$ the equality $\sum_{r=0}^{\infty} \alpha_r f_r = 0$ implies that $\alpha_r = 0$ for all $r \in \mathbb{Z}_{\geq 0}$. In fact, $\alpha_r = 0$ by induction on r, since $f_r(s) = 0$ for all $s > r$, and $f(r, r) > 0$. $\square$

Acknowledgements

We thank Benedict Gross for the suggestion to look at the self cup product on $\mathrm{H}^1(k, A[2])$ induced by the Weil pairing e_2 on a Jacobian, and for other comments. We also thank Brian Conrad, Christophe Delaunay, and Robert Guralnick.

References

[AW67] M. F. Atiyah and C. T. C. Wall, *Cohomology of groups*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 94–115. MR 0219512 (36 #2593) ↑b, d

[BS10a] Manjul Bhargava and Arul Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, June 9, 2010. Preprint, arXiv:1006.1002. ↑6.12

[BS10b] ———, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank* 0, July 1, 2010. Preprint, arXiv:1007.0052. ↑6.12

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR **1045822 (91i:**14034) ↑5.1, 5.7

[Bou04] Nicolas Bourbaki, *Integration. I. Chapters 1–6*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 2004. Translated from the 1959, 1965 and 1967 French originals by Sterling K. Berberian. MR **2018901 (2004i:**28001) ↑d

[Bra48] Jean Braconnier, *Sur les groupes topologiques localement compacts*, J. Math. Pures Appl. (9) **27** (1948), 1–85 (French). MR 0025473 (10,11c) ↑2.18

[BPS10] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus* 3, July 24, 2010. Preprint. ↑c

[Cau43] A. Cauchy, *Mémoire sur les fonctions dont plusieurs valeurs sont liées entre elles par une équation linéaire, et sur diverses transformations de produits composés d'un nombre indéfini de facteurs*, C. R. Acad. Sci. Paris **17** (1843), 523–531 (French). Reprinted in *Oeuvres*, Ser. 1, Vol. 8, Gauthier-Villars, Paris, 1893, 42–50. ↑e

[CL84] H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62, DOI 10.1007/BFb0099440, (to appear in print). MR **756082 (85j:**11144) ↑7

[dJ02] A. J. de Jong, *Counting elliptic surfaces over finite fields*, Mosc. Math. J. **2** (2002), no. 2, 281–311. Dedicated to Yuri I. Manin on the occasion of his 65th birthday. MR **1944508 (2003m:**11080) ↑6.12

[Del01] Christophe Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over* $\mathbb{Q}$, Experiment. Math. **10** (2001), no. 2, 191–196. MR **1837670 (2003a:**11065) ↑1.1, 7

[Del07] ———, *Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics*, Ranks of elliptic curves and random matrix theory, London Math. Soc. Lecture Note Ser., vol. 341, Cambridge Univ. Press, Cambridge, 2007, pp. 323–340. MR **2322355 (2008i:**11089) ↑1.1, 7

[Duk97] William Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 8, 813–818, DOI 10.1016/S0764-4442(97)80118-8 (English, with English and French summaries). MR **1485897 (99b:**11059) ↑7

[FC90] Gerd Faltings and Ching-Li Chai, *Degeneration of abelian varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 22, Springer-Verlag, Berlin, 1990. With an appendix by David Mumford. MR **1083353 (92d:**14036) ↑5.1

[GS06] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, Cambridge, 2006. MR **2266528 (2007k:**16033) ↑a

[Gir71] Jean Giraud, *Cohomologie non abélienne*, Springer-Verlag, Berlin, 1971 (French). Die Grundlehren der mathematischen Wissenschaften, Band 179. MR 0344253 (49 #8992) ↑3.2, 3.5, 3.3, 3.7

[GA09] Cristian D. González-Avilés, *Arithmetic duality theorems for 1-motives over function fields*, J. Reine Angew. Math. **632** (2009), 203–231, DOI 10.1515/CRELLE.2009.055. MR **2544149 (2010i:**11169) ↑a

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52. MR 0463157 (57 #3116) ↑6.2

[Hat10] Allen Hatcher, *Algebraic topology*, June 30, 2010. Downloaded from `http://www.math.cornell.edu/~hatcher/AT/ATpage.html` . ↑3.6

[HB93] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem*, Invent. Math. **111** (1993), no. 1, 171–195, DOI 10.1007/BF01231285. MR **1193603 (93j:**11038) ↑1.1

[HB94] ———, *The size of Selmer groups for the congruent number problem. II*, Invent. Math. **118** (1994), no. 2, 331–370, DOI 10.1007/BF01231536. With an appendix by P. Monsky. MR **1292115 (95h:**11064) ↑1.1, 6.12

[Jon10] Nathan Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), no. 3, 1547–1570, DOI 10.1090/S0002-9947-09-04804-1. MR 2563740 ↑7

[Kak43] Shizuo Kakutani, *On cardinal numbers related with a compact Abelian group*, Proc. Imp. Acad. Tokyo **19** (1943), 366–372. MR 0015124 (7,375a) ↑2.3

[Lan56] Serge Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563. MR 0086367 (19,174a) ↑6.2

[MR10] Barry Mazur and Karl Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), 541–575. ↑6.12

[Mil80] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980. MR **559531 (81j:**14002) ↑6.2

[Mil06] ———, *Arithmetic duality theorems*, second, BookSurge, LLC, 2006. MR **881804 (88e:**14028) ↑a, b, 6.2, 6.2, a

[Mum70] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay, 1970. MR 0282985 (44 #219) ↑5.1, 6.1

[Mum71] ———, *Theta characteristics of an algebraic curve*, Ann. Sci. École Norm. Sup. (4) **4** (1971), 181–192. MR 0292836 (45 #1918) ↑5.10, 5.12

[Mum91] ———, *Tata lectures on theta. III*, Progress in Mathematics, vol. 97, Birkhäuser Boston Inc., Boston, MA, 1991. With the collaboration of Madhav Nori and Peter Norman. MR **1116553 (93d:**14065) ↑6.1

[Pol03] Alexander Polishchuk, *Abelian varieties, theta functions and the Fourier transform*, Cambridge Tracts in Mathematics, vol. 153, Cambridge University Press, Cambridge, 2003. MR **1987784 (2004m:**14094) ↑5.3, 5.4, 5.4, 6.1

[Pol71] Harriet Pollatsek, *First cohomology groups of some linear groups over fields of characteristic two*, Illinois J. Math. **15** (1971), 393–417. MR 0280596 (43 #6316) ↑c, 5.9

[PS99] Bjorn Poonen and Michael Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149. MR **1740984 (2000m:**11048) ↑5.3, c, 6.7

[Rot11] H. A. Rothe, *Systematisches Lehrbuch der Arithmetik*, Barth, Leipzig, 1811. ↑e

[Sch85] Winfried Scharlau, *Quadratic and Hermitian forms*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 270, Springer-Verlag, Berlin, 1985. MR **770063 (86k:**11022) ↑2.1, 2.5, 2.7

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. MR 0236190 (38 #4488) ↑d

[SGA 6] *Théorie des intersections et théorème de Riemann-Roch*, Lecture Notes in Mathematics, Vol. 225, Springer-Verlag, Berlin, 1971 (French). Séminaire de Géométrie Algébrique du Bois-Marie 1966–1967 (SGA 6); Dirigé par P. Berthelot, A. Grothendieck et L. Illusie. Avec la collaboration de D. Ferrand, J. P. Jouanolou, O. Jussila, S. Kleiman, M. Raynaud et J. P. Serre. MR 0354655 (50 #7133) ↑5.1

[SD08] Peter Swinnerton-Dyer, *The effect of twisting on the 2-Selmer group*, Math. Proc. Cambridge Philos. Soc. **145** (2008), no. 3, 513–526, DOI 10.1017/S0305004108001588. MR **2464773 (2010d:**11059) ↑1.1, 6.12

[vK35] E. R. van Kampen, *Locally bicompact abelian groups and their character groups*, Ann. of Math. (2) **36** (1935), no. 2, 448–463, DOI 10.2307/1968582. MR 1503234 ↑2.3

[Wat71] William C. Waterhouse, *Principal homogeneous spaces and group scheme extensions*, Trans. Amer. Math. Soc. **153** (1971), 181–189. MR 0269659 (42 #4554) ↑5.4

[Yon58] Nobuo Yoneda, *Note on products in* Ext, Proc. Amer. Math. Soc. **9** (1958), 873–875. MR 0175957 (31 #233) ↑3.3

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

E-mail address: poonen@math.mit.edu

URL: http://math.mit.edu/~poonen/

Department of Mathematics, California Institute of Technology, Pasadena, CA 91125

E-mail address: rains@caltech.edu