QUADRATIC TWISTS OF ABELIAN VARIETIES AND DISPARITY IN SELMER RANKS

ADAM MORGAN

Abstract. We study the parity of 2-Selmer ranks in the family of quadratic twists of a fixed principally polarised abelian variety over a number field. Specifically, we determine the proportion of twists having odd (respectively even) 2-Selmer rank. This generalises work of Klagsbrun–Mazur–Rubin for elliptic curves and Yu for Jacobians of hyperelliptic curves. Several differences in the statistics arise due to the possibility that the Shafarevich–Tate group (if finite) may have order twice a square. In particular, the statistics for parities of 2-Selmer ranks and 2-infinity Selmer ranks need no longer agree and we describe both.

Contents

1. Introduction

In this paper we study how various invariants of principally polarised abelian varieties behave under quadratic twist.

Our first result determines the distribution of the parities of 2-Selmer ranks in the quadratic twist family of an arbitrary principally polarised abelian variety. Specifically, for a number field K (with absolute Galois group G_K) and real number $X > 0$ set

$$\mathcal{C}(K, X) = \{\chi \in \mathrm{Hom}_{\mathrm{cnt}}(G_K, \{\pm 1\}) \ : \ \mathrm{Norm}(\mathfrak{p}) < X \text{ for all primes } \mathfrak{p} \text{ at which } \chi \text{ ramifies}\}.$$

Theorem 1.1. *Let A/K be a principally polarised abelian variety and let*

$$\epsilon : \mathrm{Gal}(K(A[2])/K) \to \{\pm 1\}$$

be the map

$$\sigma \mapsto (-1)^{\dim_{\mathbb{F}_2} A[2]^\sigma}.$$

(i) *If ϵ is a homomorphism then, for all sufficiently large X,*

$$\frac{|\{\chi \in \mathcal{C}(K,X) \ : \ \dim_{\mathbb{F}_2}\mathrm{Sel}_2(A^\chi/K) \text{ is even}\}|}{|\mathcal{C}(K,X)|} = \frac{1+(-1)^{\dim_{\mathbb{F}_2}\mathrm{Sel}_2(A/K)}\cdot\delta}{2}$$

where δ is a finite product of explicit local terms δ_v (see the statement of Theorem 10.13 for their definition).

(ii) *If ϵ fails to be a homomorphism then, for all sufficiently large X,*

$$\frac{|\{\chi \in \mathcal{C}(K,X) \ : \ \dim_{\mathbb{F}_2}\mathrm{Sel}_2(A^\chi/K) \text{ is even}\}|}{|\mathcal{C}(K,X)|} = 1/2.$$

(Here for $\chi \in \mathrm{Hom}_{\mathrm{cnt}}(\mathrm{Gal}(\bar{K}/K),\{\pm 1\})$ we let A^χ/K denote the quadratic twist of A by χ.)

Theorem 1.1 is known for elliptic curves by work of Klagsbrun–Mazur–Rubin [KMR13, Theorem A] and, more generally, for Jacobians of odd degree hyperelliptic curves by work of Yu [Yu16, Theorem 1]. These previous results both fall into Case (i) of Theorem 1.1, thus the failure of ϵ to be a homomorphism forcing parity in the distribution is a phenomenon new to this work. Despite this, Case (ii) of Theorem 1.1 is in some sense the 'generic' case since if $\mathrm{Gal}(K(A[2])/K)$ is the full symplectic group $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ for $g = \dim A \geq 3$ then the simplicity of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ prevents ϵ from being a homomorphism. For a discussion of when ϵ is or is not a homomorphism for various families of abelian varieties, see §10.3.

In the two previously known cases above, finiteness of the 2-primary subgroup of the Shafarevich–Tate group is known to imply that the parity of the 2-Selmer rank agrees with that of the Mordell–Weil rank, so that Theorem 1.1 is conjecturally satisfied by Mordell–Weil ranks also. For general principally polarised abelian varieties, however, this need not be true due to a phenomenon first observed by Poonen–Stoll (see [PS99]): the 2-primary subgroup of the Shafarevich–Tate group, if finite, need not have square order. Thus to see how one expects the parity of Mordell–Weil ranks to behave in quadratic twist families we also prove a version of Theorem 1.1 for 2^∞-Selmer ranks (by definition the 2^∞-Selmer rank, denoted rk_2, is equal to the sum of the Mordell–Weil rank and the (conjecturally trivial) $\mathbb{Z}_2$-corank of the 2-primary subgroup of the Shafarevich–Tate group).

Theorem 1.2. *Let A/K be a principally polarised abelian variety. Then, for all sufficiently large $X > 0$,*

$$\frac{|\{\chi \in \mathcal{C}(K,X) \ : \ \mathrm{rk}_2(A^\chi/K) \text{ is even}\}|}{|\mathcal{C}(K,X)|} = \frac{1+(-1)^{\mathrm{rk}_2(A/K)}\cdot\kappa}{2}$$

where κ is an explicit finite product of local terms κ_v given in Definition 10.21.

We remark that if $\dim A$ is odd and K has a real place then $\kappa = 0$. In general however κ is often non-zero: see [KMR13, Example 7.11] for an example of an elliptic curve for which κ is dense in $[-1,1]$ as the base field K varies, and [Yu16, Proposition 8.1] for an example of an abelian surface over $\mathbb{Q}$ for which $\kappa = 1$.

Combining Theorems 1.1 and 1.2 we see that the distribution of parities of 2-Selmer ranks and 2^∞-Selmer ranks in general behave quite differently, as the following example illustrates.

Example 1.3 (See Example 10.24)**.** Let $J/\mathbb{Q}$ be the Jacobian of the genus 2 hyperelliptic curve $C : y^2 = x^6 + x^4 + x + 3$. Then the function ϵ is not a homomorphism for $J/\mathbb{Q}$ so that half of the 2-Selmer ranks of the quadratic twists of J are even and are half odd. On the other hand, J has $\kappa = \frac{3}{16}$ and odd 2^∞-Selmer rank, so that 19/32 of the twists of J have even 2^∞-Selmer rank and 13/32 have odd 2^∞-Selmer rank.

In fact, in the case where ϵ fails to be a homomorphism we show that the parity of the 2^∞-Selmer ranks behaves in some sense independently of the parity of the 2-Selmer ranks. See Remark 10.26 for the proof of this statement and Corollary 10.29 for a description of the joint distribution of the parities of 2-Selmer ranks and 2-infinity Selmer ranks in all cases.

A key step in passing between Theorem 1.1 and Theorem 1.2 is the study of how the 'non-square order Shafarevich–Tate group' phenomenon behaves under quadratic twist. Our main result here is:

Theorem 1.4. *Let A/K be an abelian variety equipped with a principal polarisation λ defined over K and let $\chi \in \mathrm{Hom}_{\mathrm{cnt}}(G_K, \{\pm 1\})$ correspond to a quadratic extension L/K.*

Then $\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A/K)[2] + \dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A^\chi/K)[2] \equiv 0 \pmod 2$ if and only if

$$\sum_{v \text{ non-split in } L/K} \mathrm{inv}_v\ \mathfrak{g}(A/K_v, \lambda, \chi_v) = 0 \ \text{ in } \ \mathbb{Q}/\mathbb{Z}$$

where the local terms $\mathfrak{g}(A/K_v, \lambda, \chi_v) \in \mathrm{Br}(K_v)[2]$ are given in Definition 5.15. (Here χ_v denotes the restriction of χ to the completion K_v and $Ш_{\mathrm{nd}}(A/K)$ denotes the quotient of the Shafarevich–Tate group of A/K by its maximal divisible subgroup.)

In particular, Theorem 1.4 shows that the sum

$$\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A/K)[2] + \dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A^\chi/K)[2] \qquad (\mathrm{mod}\ 2)$$

is controlled by purely local behaviour. In the case where A/K is the Jacobian of a curve, it is a result of Poonen–Stoll [PS99, Corollary 12] that this is in fact true for the parity of $\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A/K)[2]$ itself, but whether or not this holds for an arbitrary principally polarised abelian variety remains open.

In general, the definition of the local terms $\mathfrak{g}(A/K_v, \lambda, \chi_v)$ appearing in Theorem 1.4 is somewhat involved but if the principal polarisation λ on A/K_v is induced by a K_v-rational symmetric line bundle $\mathcal{L}_v$ then they take a simple form. Specifically, associated to $\mathcal{L}_v$ is a $\mathrm{Gal}(\bar{K}_v/K_v)$-invariant quadratic refinement q of the Weil pairing on $A[2]$ (we review this classical construction in §4.2). As a consequence, $\mathrm{Gal}(\bar{K}_v/K_v)$ acts on $A[2]$ through the orthogonal group $O(q)$. In particular we obtain a quadratic character ψ_v of K_v as the composition

$$\psi_v : \mathrm{Gal}(\bar{K}_v/K_v) \to O(q)/SO(q) \cong \{\pm 1\}.$$

We then have

$$\mathfrak{g}(A/K_v, \lambda, \chi_v) = \chi_v \cup \psi_v \in \mathrm{Br}(K_v).$$

This allows the explicit evaluation of $\mathfrak{g}(A/K_v, \lambda, \chi_v)$ for archimedean places and for nonarchimedean places $v \nmid 2$ at which A has good reduction (Proposition 5.16). The implications for arithmetic of the difference in characteristic 2 between quadratic forms and symmetric bilinear pairings will be a recurring theme throughout this paper.

Theorem 1.4 may also be used to prove the analogue of Theorem 1.1 for the parity of the dimension of the 2-torsion of the Shafarevich–Tate group in the family of quadratic twists of a principally polarised abelian variety. This quantifies the failure of the Shafarevich–Tate group to have square order in the family of quadratic twists. See Theorem 10.27 for the precise statement.

To expain the remaining results of the paper we briefly indicate how we prove Theorem 1.1. As in [KMR13], which proves the elliptic curve case, we deduce Theorem 1.1 from a more general theorem that determines the distribution of parities of ranks of certain Selmer groups

$\mathrm{Sel}(T,\chi)$ associated to a finite dimensional $\mathbb{F}_p$-vector space T equipped with a $\mathrm{Gal}(\bar{K}/K)$-action, an alternating pairing, and abstract 'twisting data'. The general result is Theorem 7.4, the case $\dim T = 2$ of which combines Theorem 7.6 and Theorem 8.2 of op. cit. Taking $T = A[2]$ along with the Weil pairing and the twisting data detailed in §10 recovers Theorem 1.1.

On the other hand, taking $p > 2$ and $T = A[p]$ for a principally polarised abelian variety A/K, along with the twisting data described in § 11, enables us to prove an analogue of Theorem 1.1 which applies to Selmer groups of certain p-cyclic twists of A^{p-1} (again, the case where A is an elliptic curve is shown by Klagsbrun–Mazur–Rubin in [KMR13]). To state the result, let $\mathcal{C}(K)$ and $\mathcal{C}(K,X)$ for $p > 2$ be defined in the identical way to $p = 2$, replacing $\mathrm{Hom}_{\mathrm{cnt}}(\mathrm{Gal}(\bar{K}/K),\{\pm 1\})$ (the group of quadratic characters) with the group $\mathrm{Hom}_{\mathrm{cnt}}(\mathrm{Gal}(\bar{K}/K),\boldsymbol{\mu}_p)$ (of p-cyclic characters). For $\chi \in \mathcal{C}(K)$ non-trivial, let $L = \bar{K}^{\ker(\chi)}$ and denote by A^χ/K the $p-1$-dimensional abelian variety defined as the kernel of the norm homomorphism $\mathrm{Res}_{L/K}A \to A$ (here $\mathrm{Res}_{L/K}$ denotes the restriction of scalars from L to K). There is a natural inclusion of $\mathbb{Z}[\boldsymbol{\mu}_p]$ into $\mathrm{End}_K(A^\chi)$ and, in this way, any generator π of the unique prime of $\mathbb{Z}[\boldsymbol{\mu}_p]$ lying over p yields a self-isogeny of A^χ. Denote by $\mathrm{Sel}_\pi(A^\chi/K)$ the associated π-Selmer group which may be shown to be independent of the choice of π (see §11 for more details of the above constructions). We then have:

Theorem 1.5. *Let p be an odd prime, K a number field, A/K a principally polarised abelian variety, and Σ the set consisting of all archimedean places of K, all places of bad reduction for A, and all places dividing p. Define $\epsilon : \mathrm{Gal}(K(A[p])/K) \to \{\pm 1\}$ by $\sigma \mapsto (-1)^{\dim_{\mathbb{F}_p} A[p]^\sigma}$.*

(i) *Suppose ϵ is trivial when restricted to $\mathrm{Gal}(K(A[p])/K(\boldsymbol{\mu}_p))$. Then for all sufficiently large X,*

$$\frac{|\{\chi \in \mathcal{C}(K,X) \ : \ \dim_{\mathbb{F}_p}\mathrm{Sel}_\pi(A^\chi/K) \text{ is even}\}|}{|\mathcal{C}(K,X)|} = \frac{1+(-1)^{\dim_{\mathbb{F}_p}\mathrm{Sel}_p(A/K)}\cdot\delta}{2}$$

where δ is an explicit finite product of local terms δ_v (see the statement of Corollary 11.6 for their definition). Moreover (unlike the case $p = 2$) δ is always non-zero.

(ii) *If ϵ is non-trival when restricted to $\mathrm{Gal}(K(A[p])/K(\boldsymbol{\mu}_p))$ then*

$$\lim_{X\to\infty} \frac{|\{\chi \in \mathcal{C}(K,X) \ : \ \dim_{\mathbb{F}_p}\mathrm{Sel}_\pi(A^\chi/K) \text{ is even}\}|}{|\mathcal{C}(K,X)|} = 1/2.$$

When A is an elliptic curve yet $p > 2$, ϵ is non-trivial when restricted to $\mathrm{Gal}(K(A[p])/K(\boldsymbol{\mu}_p))$ if and only if p divides $[K(A[p]) : K]$ (see [KMR13, Lemma 4.3]), so that now both cases Theorem 1.5 can occur. In particular, we see that allowing the dimension of A to be arbitrary uncovers a more uniform picture between $p = 2$ and $p > 2$ than was visible for elliptic curves. See Remark 11.8 for a discussion on conditions on the $\mathrm{Gal}(\bar{K}/K)$-action on $A[p]$ which result in Case (i) (resp. (ii)) of Theorem 1.5. We simply note here that if the Galois action on $A[p]$ is as large as possible, so that $\mathrm{Gal}(K(A[p])/K)$ is isomorphic to the general symplectic group $\mathrm{GSp}_{2g}(\mathbb{F}_p)$ for $g = \dim A$, then Case (ii) applies.

Finally, we remark that a key step in proving Theorem 7.4 (the version of Theorems 1.1 and 1.5 for general T) is, for a character χ, to describe the quantity

$$\dim_{\mathbb{F}_p}\mathrm{Sel}(T,\chi) - \dim_{\mathbb{F}_p}\mathrm{Sel}(T,\mathbb{1}) \qquad (\mathrm{mod}\ 2)$$

as a sum of local terms (see Theorem 6.12). Upon taking $T = A[2]$ for a principally polarised abelian variety A/K one obtains (Theorem 10.12) a local formula for the difference between the parity of the 2-Selmer rank of A/K and the 2-Selmer rank of the quadratic twist A^χ/K. This

generalises a theorem of Kramer [Kra81, Theorem 1] for elliptic curves, and Yu [Yu16, Theorem 5.11] for Jacobians of odd degree hyperelliptic curves. Combining this with Theorem 1.4, one obtains (Theorem 10.20) a purely local formula for the parity of the 2^∞-Selmer rank of A over the quadratic extension cut out by χ. Such local formulae for (the parity of) 2^∞-Selmer ranks have applications to the 2-parity conjecture and we plan to examine this in future work.

Layout of the paper. In §2 we review some standard results in group cohomology which will be used in the seqeuel. In §3 we review and study quadratic forms on finite dimensional $\mathbb{F}_2$-vector spaces. The main result is Proposition 3.9 which forms a key technical step in the proof of Theorem 1.4. §4 recalls the constructions of certain quadratic forms associated to abelian varieties and examines how these behave under quadratic twist. Of particular importance is Lemma 4.20 which plays a crucial role in associating twisting data to the group of 2-torsion points of a principally polarised abelian variety. Theorem 1.4 is proven in §4. The analogue of Theorems 1.1 and 1.5 for general T is proven in §6-§9 which broadly follow the layout and strategy of [KMR13, §3–4 and §6–8]. Specifically, in §6 we recall the notions of metabolic structure and twisting data from op. cit. and generalise them to arbitrary (finite) dimensional $\mathbb{F}_p$-vector spaces, as well as defining the associated Selmer groups. §7 states the main result (Theorem 7.4) and proves the anlogue of Case (i) of Theorems 1.1 and 1.5 in this setting. §8 uses class field theory to produce certain global characters with specified local behaviour and is a more or less direct generalisation of [KMR13, §6], albeit with different proofs. The results of §8 are then applied in §9 to prove the remaining cases of Theorem 7.4. §10 associates a metabolic structure and twisting data to the 2-torsion in a principally polarised abelian variety and deduces Theorems 1.1 and 1.2. Finally, §11 associates a metabolic structure and twisting data to the p-torsion in a principally polarised abelian variety for p odd and deduces Theorem 1.5.

Notation. For a group G acting on an abelian group M, for $\sigma \in G$ we write

$$M^\sigma := \{m \in M \ : \ \sigma(m) = m\}.$$

For a field F we denote its separable closure by $\bar{F}$, its absolute Galois group by G_F and, for p different from the characteristic of F, we denote by $\boldsymbol{\mu}_p$ the G_F-module of p-th roots of unity in $\bar{F}$. We denote by $\mathrm{Br}(F)$ the Brauer group of F.

For an abelian variety A/F we write $A^\vee/F$ for the dual of A. A *principally polarised abelian variety* over F is a pair $(A/F, \lambda)$ consisting of an abelian variety A/F and a principal polarisation $\lambda : A \to A^\vee$ defined over F. For a quadratic character $\chi \in \mathrm{Hom}_{\mathrm{cnt}}(G_F, \{\pm 1\})$ the *quadratic twist* of A by χ is the pair (A^χ, ψ) consisting of an abelian variety A^χ/F and an $\bar{F}$-isomorphism $\psi : A \to A^\chi$ such that $\psi^{-1}\psi^\sigma = [\chi(\sigma)]$ for all $\sigma \in G_F$.

For a number field K we denote by M_K the set of places of K and write K_v for the completion of K at $v \in M_K$. We denote by $\mathrm{inv}_v : \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$ the local invariant map and, if v is nonarchimedean, denote by K_v^{ur} the maximal unramified extension of K_v. We implicitly fix embeddings $\bar{K} \hookrightarrow \bar{K}_v$ for each $v \in M_K$ and view G_{K_v} as a subgroup of G_K for each v. In particular, for a (finite) Galois extension L/K of number fields and a non-archimedean place $v \in M_K$ unramified in L/K we have a well defined Frobenius element Frob_v in $\mathrm{Gal}(L/K)$.

For a G_K-module M, the injections $G_{K_v} \hookrightarrow G_K$ induce restriction maps on cohomology $H^i(K, M) \to H^i(K_v, M)$ for each $i \geq 0$ and $v \in M_K$. For a cocycle ξ we write ξ_v for its restriction to K_v (see §2 for our notation and conventions concerning group cohomology). We

define, for v a non-archimedean place of K,

$$H^i_{\mathrm{ur}}(K_v, M) := \ker\left(H^i(K_v, M) \xrightarrow{\mathrm{res}} H^i(K_v^{\mathrm{ur}}, M)\right).$$

1.1. **Acknowledgements.** We thank Kęstutis Česnavičius for many useful conversations and comments, and for correspondence regarding the material in §4. We thank Tim Dokchitser, Vladimir Dokchitser, Céline Maistret and Jeremy Rickard for helpful conversations, and the anonymous referee for pointing out Corollary 10.29. We would like to thank the University of Warwick and King's College London where parts of this research were carried out. This research is supported by EPSRC grant EP/M016846.

2. Group cohomology and group extensions

In the following sections we will make several computations involving group cohomology. Here we set up the relevant notation and review some basic results. All material in this section is standard: see e.g. [AW67].

2.1. **Group cohomology.** Let G be a finite group and M a G-module. For $i \geq 0$ we write $C^i(G, M)$ for the group of i-cochains with values in M and $d : C^i(G, M) \to C^{i+1}(G, M)$ for the usual differential. When $i = 0$ we have $(dm)(g) = gm - m$ for $m \in M = C^0(G, M)$ and $g \in G$, and when $i = 1$ we have

$$(df)(g, h) = f(g) + gf(h) - f(gh)$$

for $f \in C^1(G, M)$ and $g, h \in G$. We write $Z^i(G, M)$ (resp. $B^i(G, M)$) for the group of i-cocycles (resp. i-coboundaries) with values in M. We will always think of the i'th-cohomology group $H^i(G, M)$ as the quotient $Z^i(G, M)/B^i(G, M)$. When making computations involving group cohomology, we'll make the convention that Fraktur letters such as $\mathfrak{a}, \mathfrak{b}$ etc. denote cohomology classes and that the corresponding lower case Roman letters a, b etc., denote cocycles representing these cohomology classes. More generally, if G is a profinite group we consider continuous cochains, cocycles and coboundaries, using the same notation and conventions to talk about them.

2.2. **Cup product on cochains.** Let G be a finite (or profinite) group and let M and N be G-modules. Then for $i, j \geq 0$ the *cup-product* map

$$\cup : C^i(G, M) \times C^j(G, N) \longrightarrow C^{i+j}(G, M \otimes N)$$

is defined by

$$(a \cup b)(g_1, ..., g_{i+j}) = a(g_1, ..., g_i) \otimes g_1 ... g_i b(g_{i+1}, ..., g_{i+j}).$$

For $a \in C^i(G, M)$ and $b \in C^j(G, N)$ we have the equality

$$d(a \cup b) = da \cup b + (-1)^i a \cup db \tag{2.1}$$

inside $C^{i+j+1}(G, M \otimes N)$.

For $i, j \geq 0$ the cup product map above induces a cup product map on cohomology

$$\cup : H^i(G, M) \times H^j(G, N) \to H^{i+j}(G, M \otimes N)$$

which satisfies $\mathfrak{a} \cup \mathfrak{b} = (-1)^{ij} \mathfrak{b} \cup \mathfrak{a}$.

2.3. **Group extensions.** Let G be a finite group and M an abelian group with trivial G-action. In what follows we write the group law on G multiplicatively and the group law on M additively. Let $\mathfrak{a} \in H^2(G, M)$ and a be a 2-cocycle representing $\mathfrak{a}$. Define a group structure on the set $G \times M$ by the rule

$$(g, m) \cdot (g', m') = (gg', m + m' + a(g, g'))$$

and let E_a denote the resulting group. The maps $\alpha : M \to E_a$ and $\beta : E_a \to G$ defined by $m \mapsto (1, m - a(1, 1))$ and $(g, m) \mapsto g$ respectively give rise to the short exact sequence

$$0 \to M \xrightarrow{\alpha} E_a \xrightarrow{\beta} G \to 0$$

realising E_a as a central extension of G by M. The isomorphism class of this extension is independent of the choice of cocycle representing $\mathfrak{a}$ and the sequence splits if and only if $\mathfrak{a}$ is the trivial class in $H^2(G, M)$. More specifically, let $s : G \to E_a$ denote the set section $g \mapsto (g, 0)$ to β. Then if $\phi : E_a \to M$ is a homomorphism splitting the exact sequence (i.e. giving a section to α) then the function $f = \phi \circ s \in C^1(G, M)$ is a 1-cochain satisfying $df = a$.

Remark 2.2. The above correspondence in fact gives rise to a bijection between elements of $H^2(G, M)$ and the set of isomorphism classes of central extensions of G by M, and one can generalise this correspondence to include the case where the action of G on M is non-trivial (though now the relevant extensions are, in general, no longer central). See [AW67, §2] for more details.

3. Quadratic forms on finite dimensional $\mathbb{F}_2$-vector spaces

The aim of this section is to prove Propositions 3.9 and 3.10 which are needed for the proof of Theorem 1.4. In §3.1, §3.2 and §3.3 we review the theory of quadratic forms on finite dimensional $\mathbb{F}_2$-vector spaces. The material in §3.1 and §3.2 is standard, see e.g. [Sch85, Section 9.4]. In §3.3 we review a construction due to Pollatsek (given in the discussion preceeding [Pol71, Theorem 1.11]) which we use in the proof of Proposition 3.9.

For the rest of this section fix a finite dimensional $\mathbb{F}_2$-vector space V equipped with a non-degenerate alternating pairing

$$\langle\ ,\ \rangle : V \times V \longrightarrow \mathbb{F}_2$$

(so in particular $\dim V$ is even). We denote by $\mathrm{Sp}(V)$ the symplectic group of linear automorphisms of V preserving the pairing.

3.1. Quadratic refinements and the class $\mathfrak{c} \in H^1(\mathrm{Sp}(V), V)$.

Definition 3.1 (Quadratic refinement)**.** A function $q : V \to \mathbb{F}_2$ is called a *quadratic refinement* of $\langle\ ,\ \rangle$ if we have

$$q(v + v') + q(v) + q(v') = \langle v, v' \rangle$$

for all $v, v' \in V$.

Let $\mathcal{Q}$ denote the set of all quadratic refinements of $\langle\ ,\ \rangle$. It is a principal homogeneous space for V where, for $v \in V$, we define $q + v \in \mathcal{Q}$ by setting

$$(q + v)(v') = q(v') + \langle v, v' \rangle$$

for $v' \in V$. The symplectic group $\mathrm{Sp}(V)$ acts on the set of quadratic refinements via $q \mapsto q \circ \sigma^{-1}$ (for $\sigma \in \mathrm{Sp}(V)$). This action is compatible with addition by elements of V and so associated to $\mathcal{Q}$ is a class

$$\mathfrak{c} \in H^1(\mathrm{Sp}(V), V).$$

Explicitly, picking a quadratic refinement q and defining $\lambda : V \to V^* := \mathrm{Hom}(V, \mathbb{F}_2)$ to be the map $v \mapsto \langle v, - \rangle$, the function $c_q : \mathrm{Sp}(V) \to V$ given by setting

$$c_q(\sigma) = \lambda^{-1}(q \circ \sigma^{-1} - q)$$

is a 1-cocycle representing $\mathfrak{c}$.

Remark 3.2. Let $\mathcal{A}lt$ denote the group of (possibly degenerate) alternating pairings on V under addition. It has an action of $\mathrm{Sp}(V)$ given by $\sigma \cdot \langle\langle\ ,\ \rangle\rangle = \big\langle\big\langle \sigma^{-1}(\ ), \sigma^{-1}(\ )\big\rangle\big\rangle$. Similarly, let $\mathcal{Q}uad$ denote the group of quadratic forms on V under addition which also carries an action of $\mathrm{Sp}(V)$ via $\sigma \cdot q = q \circ \sigma^{-1}$. Then we have a short exact sequence of $\mathrm{Sp}(V)$-modules

$$0 \to V^* \longrightarrow \mathcal{Q}uad \longrightarrow \mathcal{A}lt \longrightarrow 0 \tag{3.3}$$

where the map $V^* \to \mathcal{Q}uad$ is inclusion and the map $\mathcal{Q}uad \to \mathcal{A}lt$ sends a quadratic form to its associated pairing. The associated long exact sequence for cohomology gives a map

$$\delta : H^0(\mathrm{Sp}(V), \mathcal{A}lt) \to H^1(\mathrm{Sp}(V), V^*).$$

Our pairing $\langle\ ,\ \rangle$ is an element of $H^0(\mathrm{Sp}(V), \mathcal{A}lt)$ and the class $\mathfrak{c} \in H^1(\mathrm{Sp}(V), V)$ constructed above is the image of $\langle\ ,\ \rangle$ under δ, once we use the map λ above to identify $H^1(\mathrm{Sp}(V), V)$ with $H^1(\mathrm{Sp}(V), V^*)$.

Remark 3.4. It is shown in [Pol71, Theorems 4.1 and 4.4] that if $\dim(V) \geq 4$ then $H^1(\mathrm{Sp}(V), V) \cong \mathbb{Z}/2\mathbb{Z}$, generated by $\mathfrak{c}$.

3.2. **Orthogonal groups, Special orthogonal groups and the Dickson homomorphism.** For a given quadratic refinement q, denote by $O(q)$ the corresponding orthogonal group of linear automorphisms preserving q rather than just the pairing. The orthogonal group $O(q)$ has an index 2 subgroup $SO(q)$ which is by definition the kernel of the Dickson homomorphism, whose definition we now recall. Let $C(q)$ denote the Clifford algebra associated to q (see [Sch85, Definition 9.2.1]), $C^0(q)$ its even graded sub-algebra and $Z(q)$ the centre of $C^0(q)$. Then $Z(q)$ is a rank 2 étale algebra over $\mathbb{F}_2$ (see Theorem 9.4.8 of op. cit.). Since $O(q)$ acts naturally on $C(q)$ and preserves the grading, it acts on $Z(q)$ by $\mathbb{F}_2$-algebra homomorphisms. Noting that the automorphism group of any rank 2 étale algebra over $\mathbb{F}_2$ (or indeed any field) is canonically isomorphic to $\mathbb{Z}/2\mathbb{Z}$, we obtain a homomorphism $d_q : O(q) \to \mathbb{Z}/2\mathbb{Z}$, the *Dickson homomorphism*.

We will also need the following alternative characterisation of the Dickson homomorphism.

Proposition 3.5. *Let q be a quadratic refinement of $\langle\ ,\ \rangle$ and $\sigma \in O(q)$. Then*

$$d_q(\sigma) = \dim V^\sigma \pmod 2.$$

Proof. This is [Dye77, Theorem 3]. □

3.3. **An extension of the Dickson homomorphism to the full symplectic group.** The following is a version of a construction due to Pollatsek ([Pol71]) which gives an extension of the Dickson homomorpism to the whole of $\mathrm{Sp}(V)$. We caution however that the resulting function $\mathrm{Sp}(V) \to \mathbb{Z}/2\mathbb{Z}$ is not a homomorphism (we cannot ask for this since for $\dim V \geq 6$ the group $\mathrm{Sp}(V)$ is simple).

Construction 3.6 (Pollatsek)**.** Fix a quadratic refinement q of $\langle\ ,\ \rangle$. Set $U = \mathbb{F}_2^2$ equipped with its unique non-degenerate alternating form $\langle\ ,\ \rangle_U$. Further, let q_U denote the unique quadratic refinement of $\langle\ ,\ \rangle_U$ with Arf invariant 1. Thus for $(\lambda, \lambda') \in U$ we have

$$q_U((\lambda, \lambda')) = \lambda + \lambda' + \lambda\lambda'.$$

Let $x = (1,0)$ and $y = (0,1)$ so that $q_U(x) = 1 = q_U(y)$ and $\langle x, y\rangle_U = 1$. Now let $W := V \oplus U$ be the orthogonal direct sum of V and U, so that W comes equipped with the quadratic form $q_W := q + q_U$, whose associated (non-degenerate, alternating) pairing is $\langle\ ,\ \rangle_W := \langle\ ,\ \rangle + \langle\ ,\ \rangle_U$.

Now given $g = (\sigma, \alpha) \in \mathrm{Sp}(V) \times \mathbb{F}_2$, define the linear automorphism $\phi_q(g)$ of W by setting

$$\phi_q(g)(x) = x,$$

$$\phi_q(g)(y) = \alpha x + c_q(\sigma) + y,$$

and for $v \in V$,

$$\phi_q(g)(v) = \sigma(v) + \langle c_q(\sigma), \sigma(v)\rangle\, x$$

and extending linearly.

A key property of this construction, as shown in the discussion preceeding [Pol71, Theorem 1.11], is that for each $g \in \mathrm{Sp}(V)\times\mathbb{F}_2$ we have $\phi_q(g) \in O(q_W)$. Moreover, Pollatsek shows in loc. cit. that for each $\sigma \in \mathrm{Sp}(V)$, there is a unique $\alpha(\sigma) \in \mathbb{F}_2$ such that $\phi_q((\sigma, \alpha(\sigma))) \in SO(q_W)$. One has $\alpha(\sigma) = d_q(\sigma)$ for all $\sigma \in O(q)$, so the map $\sigma \mapsto \alpha(\sigma)$ gives an extension of the Dickson homomorphism to the full symplectic group $\mathrm{Sp}(V)$.

3.4. **Triviality of $\mathfrak{c} \cup \mathfrak{c}$.** The pairing $\langle\ ,\ \rangle$ induces a cup-product map

$$\cup : H^1(\mathrm{Sp}(V), V) \times H^1(\mathrm{Sp}(V), V) \longrightarrow H^2(\mathrm{Sp}(V), \mathbb{F}_2).$$

We now use the construction of the previous subsection to analyse the element $\mathfrak{c} \cup \mathfrak{c} \in H^2(\mathrm{Sp}(V), \mathbb{F}_2)$.

Notation 3.7. Given a quadratic refinement $q \in \mathcal{Q}$, let E_q denote the central extension of $\mathrm{Sp}(V)$ by $\mathbb{F}_2$ corresponding to the 2-cocycle $c_q \cup c_q$, so that as a set $E_q = \mathrm{Sp}(V) \times \mathbb{F}_2$, and is equipped with the group structure

$$(\sigma, \alpha) \cdot (\sigma', \alpha') = (\sigma\sigma', \alpha + \alpha' + (c_q \cup c_q)(\sigma, \sigma')).$$

We then have:

Lemma 3.8. *The function ϕ_q of 3.6 is a homomorphism $E_q \to O(q_W)$.*

Proof. As above, ϕ_q gives a map from E_q into $O(q_W)$. An easy computation shows additionally that it is a homomorphism. □

We may now prove the main result of the section.

Proposition 3.9. *For each quadratic refinement $q \in \mathcal{Q}$ there is a unique function $f_q : \mathrm{Sp}(V) \to \mathbb{F}_2$ such that $df_q = c_q \cup c_q \in Z^2(\mathrm{Sp}(V), \mathbb{F}_2)$ and such that the restriction of f_q to the orthogonal group $O(q)$ is the Dickson homomorphism. In particular, we have*

$$\mathfrak{c} \cup \mathfrak{c} = 0 \in H^2(\mathrm{Sp}(V), \mathbb{F}_2).$$

Proof. We first show uniqueness. If f_q' is another function with $df_q' = c_q \cup c_q$ then the difference $f_q - f_q'$ is a homomorphism from $\mathrm{Sp}(V)$ to $\mathbb{F}_2$. If $\dim V \geq 6$ then $\mathrm{Sp}(V)$ is simple and hence $f_q = f_q'$. If $\dim V$ (which is necessarily even) is 2 or 4 then $\mathrm{Sp}(V)$ has a unique index 2 subgroup and hence a unique non-trivial homomorphism to $\mathbb{F}_2$. In each case this homomorphism is non-trivial when restricted to $O(q)$ for each quadratic refinement q, whence the result.

In the notation of 3.6, associated to q_W is the Dickson homomorphism

$$d_{q_W} : O(q_W) \longrightarrow \mathbb{F}_2.$$

We claim that $d_{q_W} \circ \phi_q : E_q \to \mathbb{F}_2$ gives a section to the map $\mathbb{F}_2 \to E_q$ sending α to $(1, \alpha)$, thus splitting the extension E_q. Indeed, let $\alpha \in \mathbb{F}_2$. Then $\phi_q((1, \alpha)) = \mathrm{id}_V \oplus m_\alpha$ where $m_\alpha \in O(q_U)$ is defined by $m_\alpha(x) = x$, $m_\alpha(y) = \alpha x + y$. One sees (either using the definition in terms of Clifford algebras, or by applying Proposition 3.5) that $\mathrm{id}_V \oplus m_\alpha$ is in $SO(q_W)$ if and only if $\alpha = 0$, whence $d_{q_W}((1, \alpha)) = \alpha$ as desired.

It now follows that the function $f_q : \mathrm{Sp}(V) \to \mathbb{F}_2$ defined by $f_q(\sigma) = (d_{q_W} \circ \phi_q)((\sigma, 0))$ satisfies $df_q = c_q \cup c_q$ (see §2.3 and note that $(c_q \cup c_q)(1, 1) = 0$).

It remains to show that the restriction of f_q to $O(q)$ is the Dickson homomorphism d_q. To see this note that for any $\sigma \in O(q)$ we have $c_q(\sigma) = 0$ and so

$$\phi_q((\sigma, 0)) = \sigma \oplus \mathrm{id}_U.$$

Since this is in $SO(q_W)$ if and only if σ is in $SO(q)$ (again by looking at Clifford algebras or using Proposition 3.5), we have the claim. □

We now describe how f_q changes upon changing the quadratic refinement q.

Proposition 3.10. *Let q and q' be two quadratic refinements of $\langle\ ,\ \rangle$ and let $v \in V$ be such that $q' = q + v$, so that $c_{q'} = c_q + dv$. Then we have*

$$f_{q'} = f_q + c_q \cup v + v \cup c_q + v \cup dv$$

as cochains in $C^1(\mathrm{Sp}(V), \mathbb{F}_2)$.

Proof. One readily computes

$$d(f_q + c_q \cup v + v \cup c_q + v \cup dv) = c_{q'} \cup c_{q'},$$

so it remains to show that the restriction of $f_q + c_q \cup v + v \cup c_q + v \cup dv$ to $O(q')$ is the Dickson homomorphism $d_{q'}$. To do this we'll use the characterisation of the Dickson homomorphism given in Proposition 3.5.

Fix $\sigma \in O(q')$. Then $c_q(\sigma) = (dv)(\sigma)$. In the notation of 3.6, given $w \in W$ and writing $w = z + \epsilon_1 x + \epsilon_2 y$ with $z \in V$ and $\epsilon_1, \epsilon_2 \in \mathbb{F}_2$, one sees that w is fixed by $\phi_q((\sigma, 0))$ if and only if

$$\sigma(z) - z = \epsilon_2 (dv)(\sigma) \tag{3.11}$$

and

$$\langle (dv)(\sigma), \sigma(z) \rangle = 0. \tag{3.12}$$

Now (3.11) is equivalent to $z = z' + \epsilon_2 v$ for some $z' \in V^\sigma$. If z has this form, then using invariance of z' under σ one computes

$$\langle (dv)(\sigma), \sigma(z) \rangle = \epsilon_2 \langle \sigma(v), v \rangle .$$

Thus if $\langle \sigma(v), v \rangle = 0$ then the second condition (3.12) is redundant, whilst if $\langle \sigma(v), v \rangle = 1$ then it may be replaced with the condition $\epsilon_2 = 0$. We conclude that

$$\mathrm{dim} W^{\phi_q((\sigma,0))} \equiv \mathrm{dim} V^\sigma + \langle \sigma(v), v \rangle \pmod 2$$

and hence (using Proposition 3.5)

$$f_q(\sigma) = d_{q'}(\sigma) + \langle \sigma(v), v \rangle = d_{q'}(\sigma) + (v \cup dv)(\sigma).$$

Thus the restriction of f_q to $O(q')$ is equal to $d_{q'} + v \cup dv$. Noting also that the restriction of c_q to $O(q')$ is equal to dv the result follows easily. □

Remark 3.13. Let $\tilde{V}$ denote the group whose underlying set is $V \times \mathbb{F}_2$, endowed with the group law

$$(v, \alpha) \cdot (v', \alpha') = (v + v', \alpha + \alpha' + \langle v, v' \rangle).$$

Then $\tilde{V}$ sits in a short exact sequence

$$0 \to \mathbb{F}_2 \longrightarrow \tilde{V} \longrightarrow V \to 0, \tag{3.14}$$

the map $\mathbb{F}_2 \to \tilde{V}$ sending α to $(0, \alpha)$ and the map $\tilde{V} \to V$ being projection onto the first factor. Making $\mathrm{Sp}(V)$ act trivially on $\mathbb{F}_2$ and diagonally on $\tilde{V}$ this sequence becomes an exact sequence of $\mathrm{Sp}(V)$-modules. Using the relation $df_q = c_q \cup c_q$ one can show that for each quadratic refinement q the function $\tilde{c}_q : \mathrm{Sp}(V) \to \tilde{V}$ defined by

$$\tilde{c}_q(\sigma) = (c_q(\sigma), f_q(\sigma))$$

is a 1-cocycle. One may then use the relationship between f_q and f'_q given in Proposition 3.10 to show that the class $\tilde{\mathfrak{c}}$ of $\tilde{c}_q$ in $H^1(\mathrm{Sp}(V), \tilde{V})$ does not depend on q so that the results of this section prove that $\mathfrak{c} \in H^1(\mathrm{Sp}(V), V)$ admits a canonical lift to $H^1(\mathrm{Sp}(V), \tilde{V})$. (It is shown in [PR11, Corollary 2.8(b)] that the connecting homomorphism $H^1(\mathrm{Sp}(V), V) \to H^2(\mathrm{Sp}(V), \mathbb{F}_2)$ arising from (3.14) sends $\mathfrak{a} \in H^1(\mathrm{Sp}(V), V)$ to $\mathfrak{a} \cup \mathfrak{a}$, so that the triviality of $\mathfrak{c} \cup \mathfrak{c}$ is equivalent to the existence of some lift of $\mathfrak{c}$ to $H^1(\mathrm{Sp}(V), \tilde{V})$.)

4. Quadratic forms associated to abelian varieties

In this section we study the behaviour under quadratic twist of certain quadratic forms associated to abelian varieties. Though several results in this section will be used in what follows, the most important is Lemma 4.20 which provides the technical input required to generalise [Yu16, Theorem 5.10] to the case of arbitrary principally polarised abelian varieties (this is done in Lemma 10.6). §4.1–4.3 review some standard results in the theory of abelian varieties as can be found, for example, in [Mum66].

For the rest of this section, fix a field F of characteristic 0 (which for applications will be either a number field or the completion of one). Let A/F be an abelian variety. For $x \in A(\bar{F})$ denote by τ_x the translation-by-x map $\tau_x : A \to A$.

4.1. Line bundles and self-dual homomorphisms.

Let $\mathcal{L}$ be a line bundle on $A/\bar{F}$. We denote by $\phi_{\mathcal{L}}$ the homomorphism $A \to A^\vee$ sending $x \in A(\bar{F})$ to the element of $A^\vee(\bar{F})$ corresponding to the line bundle $\tau_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$. We write $K(\mathcal{L})$ for the kernel of $\phi_{\mathcal{L}}$. If $\mathcal{L}$ is ample then $K(\mathcal{L})$ is a finite subgroup of A.

We have a short exact sequence of G_F-modules

$$0 \longrightarrow A^\vee(\bar{F}) \longrightarrow \mathrm{Pic} A_{\bar{F}} \longrightarrow \mathrm{Hom}_{\text{self-dual}}(A_{\bar{F}}, A^\vee_{\bar{F}}) \longrightarrow 0, \tag{4.1}$$

the map $A^\vee(\bar{F}) \to \mathrm{Pic} A_{\bar{F}}$ being the natural inclusion and the map $\mathrm{Pic} A_{\bar{F}} \to \mathrm{Hom}_{\text{self-dual}}(A_{\bar{F}}, A^\vee_{\bar{F}})$ sending a line bundle $\mathcal{L}$ to $\phi_{\mathcal{L}}$. As in [PR11, §3.2], (4.1) induces a short exact sequence of G_F-modules

$$0 \longrightarrow A^\vee[2] \longrightarrow \mathrm{Pic}^{\mathrm{sym}} A_{\bar{F}} \longrightarrow \mathrm{Hom}_{\text{self-dual}}(A_{\bar{F}}, A^\vee_{\bar{F}}) \longrightarrow 0, \tag{4.2}$$

where here $\mathrm{Pic}^{\mathrm{sym}} A_{\bar{F}}$ denotes the group of symmetric line bundles on A (i.e. those satisfying $[-1]^*\mathcal{L} \cong \mathcal{L}$).

4.2. **Quadratic refinements of the Weil pairing on $A[2]$.** Let $(\ ,\ )_{e_2} : A[2]\times A^\vee[2] \longrightarrow \boldsymbol{\mu}_2$ denote the Weil pairing. It is bilinear, non-degenerate and G_F-equivariant. If $\lambda : A \to A^\vee$ is a self-dual homomorphism then it induces an alternating pairing

$$(\ ,\ )_\lambda : A[2] \times A[2] \longrightarrow \boldsymbol{\mu}_2$$

defined by $(a,b)_\lambda = (a, \lambda(b))_{e_2}$ for $a, b \in A[2]$. If λ is defined over F then $(\ ,\ )_\lambda$ is G_F-invariant. In general, for a line bundle $\mathcal{L}$ on A set $(\ ,\ )_\mathcal{L} := (\ ,\ )_{\phi_\mathcal{L}}$.

Definition 4.3. Let $\mathcal{L}$ be a symmetric line bundle on A. Define the map $q_\mathcal{L} : A[2] \to \boldsymbol{\mu}_2$ as follows. Given $x \in A[2]$, we have $x^*[-1]^*\mathcal{L} = x^*\mathcal{L}$. In particular, the restriction of the normalised[1] isomorphism $\tau : \mathcal{L} \xrightarrow{\sim} [-1]^*\mathcal{L}$ to x is multiplication by an element $\eta_x \in \bar{F}^\times$ on $x^*\mathcal{L}$. One in fact has $\eta_x \in \boldsymbol{\mu}_2$ and we set $q_\mathcal{L}(x) := \eta_x$.

Remark 4.4. The map $q_\mathcal{L}$ defined above is denoted $e_*^\mathcal{L}$ in [Mum66] (fourth definition in §2).

The following well known lemma summarises the properties of $q_\mathcal{L}$.

Lemma 4.5. *Let $\mathcal{L}$ be a symmetric line bundle on A. Then we have*

(i) *if $\mathcal{L} \cong \mathcal{L}'$ then $q_\mathcal{L} = q_{\mathcal{L}'}$,*
(ii) *the function $q_\mathcal{L}$ is a quadratic form on $A[2]$ (valued in $\boldsymbol{\mu}_2$) whose associated bilinear pairing is $(\ ,\ )_\mathcal{L}$,*
(iii) *if $\mathcal{M}$ is another symmetric line bundle then $q_{\mathcal{L}\otimes\mathcal{M}} = q_\mathcal{L} \cdot q_\mathcal{M}$.*

Proof. Part (i) is immediate. For parts (ii) and (iii) see e.g. [Mum66, §2] or [PR11, Proposition 3.2]. □

For a principal polarisation $\lambda : A \to A^\vee$ defined over F, we can use Lemma 4.5 to give a geometric interpretation of the principal homogeneous space for $A[2]$ associated to the set of quadratic refinements of the Weil pairing $(\ ,\ )_\lambda$ on $A[2]$.

Definition 4.6. Let $\lambda : A \to A^\vee$ be a self-dual homomorphism defined over F. We define $\mathfrak{c}_\lambda \in H^1(F, A^\vee[2])$ to be the image of λ under the connecting homomorphism in the long exact for Galois cohomology associated to (4.2). If λ is a principal polarisation we will also, by an abuse of notation, write $\mathfrak{c}_\lambda$ for the element $\lambda^{-1}(\mathfrak{c}_\lambda) \in H^1(F, A[2])$.

Lemma 4.7. *Let $\lambda : A \to A^\vee$ be a principal polarisation defined over F, so that $(\ ,\ )_\lambda$ is a non-degenerate, G_F-equivariant, alternating pairing on $A[2]$. Then G_F acts on $A[2]$ through the symplectic group $\mathrm{Sp}(A[2])$ associated to the pairing $(\ ,\ )_\lambda$. Let $\mathfrak{c} \in H^1(F, A[2])$ be the cohomology class associated to the set of quadratic refinements of $(\ ,\ )_\lambda$ as in §3.1.*

Then we have the equality $\mathfrak{c} = \mathfrak{c}_\lambda$ inside $H^1(F, A[2])$.

Proof. We remark that this is implicit in [PR11, §3]. First note that by Lemma 4.5(ii), for any symmetric line bundle $\mathcal{L}$ for which $\lambda = \phi_\mathcal{L}$, the function $q_\mathcal{L}$ is a quadratic refinement of $(\ ,\ )_\lambda$. The result now follows either by an explict computation using the association $\mathcal{L} \mapsto q_\mathcal{L}$ or, more conceptually, from the long exact sequences for cohomology associated to the commutative diagram (16) of [PR11, §3.4], the top row of which is our sequence (4.2) and the bottom row of which is the exact sequence (3.3) of Remark 3.2. □

[1] Writing $e \in A(\bar{F})$ for the identity section, an isomorphism $\tau : \mathcal{L} \xrightarrow{\sim} [-1]^*\mathcal{L}$ is called *normalised* if

$$e^*(\tau) : e^*\mathcal{L} \xrightarrow{\sim} e^*[-1]^*\mathcal{L} = e^*\mathcal{L}$$

is the identity. There is a unique such τ for each symmetric line bundle (see [Mum66, §2]).

4.3. **Theta groups.** In this subsection we suppose that $\mathcal{L}$ is an ample line bundle on A so that $K(\mathcal{L})$ is finite. We recall the definition of the Theta group associated to $\mathcal{L}$ (see [Mum66] for more details of what follows).

Definition 4.8. The *Theta group* $\mathscr{G}(\mathcal{L})$ associated to $\mathcal{L}$ is the set of pairs (x, φ) where $x \in K(\mathcal{L})$ and φ is an isomorphism $\varphi : \mathcal{L} \xrightarrow{\sim} \tau_x^*\mathcal{L}$ (over $\bar{F}$). The group operation is given by

$$(x, \varphi) \cdot (x', \varphi') = (x + x', \tau_{x'}^*(\varphi) \circ \varphi').$$

Remark 4.9. If $\mathcal{L} \cong \mathcal{L}'$ then fixing an isomorphism $\alpha : \mathcal{L} \xrightarrow{\sim} \mathcal{L}'$ we obtain an isomorphism $\mathscr{G}(\mathcal{L}) \xrightarrow{\sim} \mathscr{G}(\mathcal{L}')$ given by

$$(x, \varphi) \longmapsto (x, \tau_x^*(\alpha) \circ \varphi \circ \alpha^{-1})$$

which is independent of α (since any two choices differ by a scalar). As such, $\mathscr{G}(\mathcal{L})$ is canonically isomorphic to $\mathscr{G}(\mathcal{L}')$.

Remark 4.10. The group $\mathscr{G}(\mathcal{L})$ sits in a short exact sequence

$$0 \to \bar{F}^\times \longrightarrow \mathscr{G}(\mathcal{L}) \longrightarrow K(\mathcal{L}) \to 0, \tag{4.11}$$

the map $\mathscr{G}(\mathcal{L}) \to K(\mathcal{L})$ being projection onto the first factor and the map $\bar{F}^\times \to \mathscr{G}(\mathcal{L})$ sending $\eta \in \bar{F}^\times$ to the pair $(0, \text{mult. by } \eta)$.

Lemma 4.12. *We have the following functorial properties of $\mathscr{G}$:*

(i) *let A/F and B/F be abelian varieties, let $\mathcal{L}$ be an ample line bundle on B and let $f : A \to B$ be an isomorphism. Then the map $\tilde{f} : \mathscr{G}(f^*\mathcal{L}) \xrightarrow{\sim} \mathscr{G}(\mathcal{L})$ given by*

$$(x, \varphi) \mapsto \big(f(x), (f^{-1})^*(\varphi)\big)$$

is an isomorphism making the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \bar{F}^\times & \longrightarrow & \mathscr{G}(f^*\mathcal{L}) & \longrightarrow & K(f^*\mathcal{L}) & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \tilde{f}} & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & \bar{F}^\times & \longrightarrow & \mathscr{G}(\mathcal{L}) & \longrightarrow & K(\mathcal{L}) & \longrightarrow & 0 \end{array}$$

commute,

(ii) *given abelian varieties $A/F, B/F$ and C/F, isomorphisms $f_1 : A \to B$ and $f_2 : B \to C$ and an ample line bundle $\mathcal{L}$ on C, we have*

$$\widetilde{f_2 \circ f_1} = \tilde{f}_2 \circ \tilde{f}_1 : \mathscr{G}(f_1^* f_2^* \mathcal{L}) \xrightarrow{\sim} \mathscr{G}(\mathcal{L}).$$

Proof. In both cases this is a simple computation. We remark that we crucially require that f is an isomorphism in (i), the situation for a general homomorphism being more subtle. See, for example, [Mum66, Proposition 2] and the surrounding discussion. □

4.4. **Theta groups in the main case of interest.** Suppose that A is equipped with a fixed principal polarisation $\lambda : A \to A^\vee$ defined over F and take $\mathcal{L} = (1, \lambda)^*\mathcal{P}$ where $\mathcal{P}$ is the Poincaré line bundle on $A \times A^\vee$ (here, for a homomorphism $\mu : A \to A^\vee$ we denote by $(1, \mu) : A \to A \times A^\vee$ the composition of the diagonal morphism $\Delta : A \to A \times A$ with the morphism $1 \times \mu : A \times A \to A \times A^\vee$). Then $\mathcal{L}$ is an F-rational, ample, symmetric line bundle on A such that $\phi_{\mathcal{L}} = 2\lambda$ (see [PR12, Remark 4.5]). In particular, we have $K(\mathcal{L}) = \ker(2\lambda) = A[2]$.

Since $[-1]^*\mathcal{L} \cong \mathcal{L}$ we have an induced isomorphism $\widetilde{[-1]}$ of $\mathscr{G}(\mathcal{L})$ as in Lemma 4.12.

Lemma 4.13. *With $\mathcal{L} = (1, \lambda)^*\mathcal{P}$ as above, the automorphism $\widetilde{[-1]}$ of $\mathscr{G}(\mathcal{L})$ is trivial.*

Proof. By [Mum66, Proposition 3], if $\mathcal{F}$ is any ample symmetric line bundle on A and $(x,\varphi) \in \mathscr{G}(\mathcal{F})$ is such that $x \in A[2]$, then the automorphism $\widetilde{[-1]}$ of $\mathscr{G}(\mathcal{F})$ sends (x,φ) to $(x, q_{\mathcal{F}}(x)\varphi)$.

In particular, since $K(\mathcal{L}) = A[2]$ in our case, it suffices to show that $q_{\mathcal{L}}$ is trivial. Pick a symmetric line bundle $\mathcal{M}$ such that $\lambda = \phi_{\mathcal{M}}$ (whilst it may not be possible to choose an F-rational such $\mathcal{M}$, this is always possible over $\bar{F}$). By standard properties of the Poincaré line bundle we have $(1 \times \phi_{\mathcal{M}})^*\mathcal{P} \cong m^*\mathcal{M} \otimes p_1^*\mathcal{M}^{-1} \otimes p_2^*\mathcal{M}^{-1}$, where $m : A \times A \to A$ is addition and p_1 (resp. p_2) denotes projection onto the first (resp. second) factor. Pulling back along the diagonal morphism $\Delta : A \to A \times A$ we obtain

$$\mathcal{L} \cong [2]^*\mathcal{M} \otimes \mathcal{M}^{-2} \cong \mathcal{M}^2$$

where for the second isomorphism above we use the symmetry of $\mathcal{M}$ along with the fact that for any line bundle $\mathcal{F}$ on A we have $[2]^*\mathcal{F} \cong \mathcal{F}^3 \otimes [-1]^*\mathcal{F}$ (see e.g. [Mil86, Corollary 6.6]). By Lemma 4.5(iii) we conclude that $q_{\mathcal{L}} = (q_{\mathcal{M}})^2 = 1$ as desired. □

Remark 4.14. As $\mathcal{L}$ is F-rational, the group $\mathscr{G}(\mathcal{L})$ carries a natural G_F-action. Explicitly, for $\sigma \in G_F$ and $(x,\varphi) \in \mathscr{G}(\mathcal{L})$, we have

$$\sigma \cdot (x,\varphi) = (\sigma(x), \sigma^*(\varphi)) \in \mathscr{G}(\sigma^*\mathcal{L}) = \mathscr{G}(\mathcal{L})$$

where for the equality $\mathscr{G}(\sigma^*\mathcal{L}) = \mathscr{G}(\mathcal{L})$ we combine Remark 4.9 with the assumption that $\mathcal{L}$ is F-rational. In particular, the exact sequence of Remark 4.10 becomes a short exact sequence of G_F-modules

$$0 \to \bar{F}^\times \longrightarrow \mathscr{G}(\mathcal{L}) \longrightarrow A[2] \to 0 \tag{4.15}$$

(we caution here that $\mathscr{G}(\mathcal{L})$ is nonabelian). This short exact sequence will be important in what follows. More specifically, as in [PR12, Corollary 4.7], the associated connecting map $H^1(F, A[2]) \to H^2(F, \bar{F}^\times)$ is a quadratic form whose associated bilinear pairing is that arising from cup-product and the Weil pairing $(\ ,\ )_\lambda : A[2] \times A[2] \to \boldsymbol{\mu}_2 \hookrightarrow \bar{F}^\times$.

4.5. **Quadratic twists.** Maintaining the notation of §4.4 (so in particular $\mathcal{L} = (1,\lambda)^*\mathcal{P}$) let $\chi : G_F \to \boldsymbol{\mu}_2$ be a quadratic character. Write (A^χ, ψ) for the quadratic twist of A by χ (so that $\psi : A \to A^\chi$ is an $\bar{F}$-isomorphism with $\psi^{-1} \circ \psi^\sigma = [\chi(\sigma)]$ for all $\sigma \in G_F$). We now consider the effect of quadratic twisting on the constructions appearing earlier in this section. Note that ψ restricts to a G_F-equivariant isomorphism $A[2] \xrightarrow{\sim} A^\chi[2]$.

Lemma 4.16. *The morphism $\lambda_\chi := (\psi^\vee)^{-1}\lambda\psi^{-1} : A^\chi \to A^{\chi\vee}$ is a principal polarisation defined over F.*

Proof. This is a manifestation of the fact that $[-1]^*$ acts trivially on the Néron–Severi group. More precisely, one computes immediately that λ_χ is defined over F, and it's a polarisation since if $\mathcal{M}$ is a line bundle on A (not necessarily F-rational) such that $\lambda = \phi_{\mathcal{M}}$ then one has $\lambda_\chi = \phi_{\mathcal{M}_\chi}$ where $\mathcal{M}_\chi = (\psi^{-1})^*\mathcal{M}$. □

More generally, we have:

Lemma 4.17. *We have a commutative diagram of G_F-modules*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A^{\chi\vee}[2] & \longrightarrow & \mathrm{Pic}^{\mathrm{sym}} A^\chi_{\bar{F}} & \longrightarrow & \mathrm{Hom}_{\text{self-dual}}(A^\chi_{\bar{F}}, A^{\chi\vee}_{\bar{F}}) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \psi^\vee} & & \downarrow{\scriptstyle \psi^*} & & \downarrow & & \\
0 & \longrightarrow & A^\vee[2] & \longrightarrow & \mathrm{Pic}^{\mathrm{sym}} A_{\bar{F}} & \longrightarrow & \mathrm{Hom}_{\text{self-dual}}(A_{\bar{F}}, A^\vee_{\bar{F}}) & \longrightarrow & 0,
\end{array}$$

where the rightmost vertical map sends μ to $\psi\mu\psi^\vee$.

Proof. As with Lemma 4.16 this follows from an explicit computation, and results from the fact that $[-1]$ acts trivially on each group appearing. □

Corollary 4.18. *Let $\bar{\psi}^{-1}$ denote the isomorphism $H^1(F, A^\chi[2]) \to H^1(F, A[2])$ induced by ψ^{-1} and let $\mathfrak{c}_\lambda \in H^1(F, A[2])$ (resp. $\mathfrak{c}_{\lambda_\chi} \in H^1(F, A^\chi[2])$) be the cohomology class associated to λ (resp. λ_χ) as in Definition 4.6. Then we have $\bar{\psi}^{-1}(\mathfrak{c}_{\lambda_\chi}) = \mathfrak{c}_\lambda$.*

Proof. This follows immediately from the long exact sequences for cohomology associated to the commutative diagram of Lemma 4.17. □

We now consider the effect of quadratic twisting on the Theta group associated to $\mathcal{L} = (1, \lambda)^*\mathcal{P}$.

Lemma 4.19. *Let $\mathcal{L} = (1, \lambda)^*\mathcal{P}$, write $\mathcal{P}_\chi$ for the Poincaré line bundle on $A^\chi \times A^{\chi\vee}$ and define $\mathcal{L}_\chi := (1, \lambda_\chi)^*\mathcal{P}_\chi$. Then $\psi^*\mathcal{L}_\chi \cong \mathcal{L}$.*

Proof. Standard properties of the Poincaré line bundle (see e.g. [Mil86, §11]) give

$$(1 \times \psi^\vee)^*\mathcal{P} \cong (\psi \times 1)^*\mathcal{P}_\chi$$

as line bundles on $A \times A^{\chi\vee}$. Since $\psi^\vee$ is an isomorphism we obtain

$$\mathcal{L} = (1, \lambda)^*\mathcal{P} \cong (1, \lambda)^*(1 \times (\psi^\vee)^{-1})^*(\psi \times 1)^*\mathcal{P}_\chi.$$

The right hand side of the above expression is easily seen to be equal to

$$\psi^*\Delta^*(1 \times \lambda_\chi)^*\mathcal{P}_\chi = \psi^*\mathcal{L}_\chi$$

as desired (here $\Delta : A \to A \times A$ is the diagonal morphism). □

Lemma 4.20. *The isomorphism $\tilde{\psi} : \mathscr{G}(\mathcal{L}) \to \mathscr{G}(\mathcal{L}_\chi)$ (arising from Lemma 4.12 and Lemma 4.19) is Galois equivariant. In particular, $\tilde{\psi}$ fits into a commutative diagram of G_F-modules*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \bar{F}^\times & \longrightarrow & \mathscr{G}(\mathcal{L}) & \longrightarrow & A[2] & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \tilde{\psi}} & & \downarrow{\scriptstyle \psi} & & \\ 0 & \longrightarrow & \bar{F}^\times & \longrightarrow & \mathscr{G}(\mathcal{L}_\chi) & \longrightarrow & A^\chi[2] & \longrightarrow & 0, \end{array}$$

where all vertical maps are isomorphisms.

Proof. Write $\mathrm{Isom}_{\mathcal{L},\mathcal{L}_\chi}(A, A^\chi)$ for the set of $\bar{F}$-isomorphisms $f : A \to A^\chi$ for which $f^*\mathcal{L}_\chi \cong \mathcal{L}$. Then using the explicit Galois action given in Remark 4.14 one sees that the map $\mathrm{Isom}_{\mathcal{L},\mathcal{L}_\chi}(A, A^\chi) \to \mathrm{Isom}\,(\mathscr{G}(\mathcal{L}), \mathscr{G}(\mathcal{L}_\chi))$ given by $f \mapsto \tilde{f}$ is Galois equivariant. It then follows from Lemma 4.12 that we have, for all $\sigma \in G_F$,

$$(\widetilde{\psi})^\sigma = \widetilde{\psi^\sigma} = \psi \circ \widetilde{[\chi(\sigma)]} = \widetilde{\psi} \circ \widetilde{[\chi(\sigma)]} = \tilde{\psi}$$

where the last equality follows from Lemma 4.13. □

5. Controlling the parity of $\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A/K)[2]$ under quadratic twist

In this section we prove Theorem 1.4 concerning the behaviour under quadratic twist of the Shafarevich–Tate group of a principally polarised abelian variety.

For the rest of the section, fix a number field K and and let $(A/K, \lambda)$ be a principally polarised abelian variety. To fix notation, we briefly recall the definition of the 2-Selmer and Shafarevich–Tate groups of A/K.

5.1. **The 2-Selmer group and the Shafarevich–Tate group.** For a place v of K we denote by $\delta_v : A(K_v)/2A(K_v) \hookrightarrow H^1(K_v, A[2])$ the connecting homomorphism associated to the multiplication-by-two Kummer sequence

$$0 \to A[2] \longrightarrow A(\bar{K_v}) \xrightarrow{[2]} A(\bar{K_v}) \to 0 \tag{5.1}$$

over the completion K_v of K at v.

The 2-Selmer group of A/K is the group

$$\mathrm{Sel}_2(A/K) := \{\xi \in H^1(K, A[2]) \ : \ \xi_v \in \mathrm{im}(\delta_v) \ \forall v \in M_K\}.$$

It sits in a short exact sequence

$$0 \to A(K)/2A(K) \longrightarrow \mathrm{Sel}_2(A/K) \longrightarrow Ш(A/K)[2] \to 0 \tag{5.2}$$

where

$$Ш(A/K) := \ker(H^1(K, A) \to \prod_{v \in M_K} H^1(K_v, A))$$

is the Shafarevich–Tate group of A/K.

5.2. **The Cassels–Tate pairing.** Denote by $Ш_{\mathrm{nd}}(A/K)$ the quotient of $Ш(A/K)$ by its maximal divisible subgroup. The Cassels–Tate pairing is a bilinear pairing

$$\langle \ , \ \rangle_{\mathrm{CT}} : Ш(A/K) \times Ш(A^\vee/K) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

the left (resp. right) kernel of which is $Ш_{\mathrm{nd}}(A/K)$ (resp. $Ш_{\mathrm{nd}}(A^\vee/K)$). The principal polarisation $\lambda : A \to A^\vee$ induces a non-degenerate bilinear pairing

$$\langle \ , \ \rangle_{\mathrm{CT},\lambda} : Ш_{\mathrm{nd}}(A/K) \times Ш_{\mathrm{nd}}(A/K) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

defined by $\langle a, b\rangle_{\mathrm{CT},\lambda} = \langle a, \lambda(b)\rangle_{\mathrm{CT}}$ for $a, b \in Ш(A/K)$. This pairing is antisymmetric ([Fla90, Theorem 2], see also [PS99, Corollary 6]).

Via the map $\mathrm{Sel}_2(A/K) \to Ш(A/K)[2]$ of (5.2) the Cassels–Tate pairing $\langle \ , \ \rangle_{\mathrm{CT},\lambda}$ induces an antisymmetric pairing on $\mathrm{Sel}_2(A/K)$ (though this is no longer non-degenerate). By an abuse of notation we denote this by $\langle \ , \ \rangle_{\mathrm{CT},\lambda}$ also.

5.3. **Description of the Cassels–Tate pairing on $\mathrm{Sel}_2(A/K)$.** We will need an explicit description of the Cassels–Tate pairing $\langle \ , \ \rangle_{\mathrm{CT},\lambda}$ on $\mathrm{Sel}_2(A/K)$. We use the 'Weil pairing' definition as in [PS99, §12.2] which we copy almost verbatim and to which we refer for more details.

Definition 5.3 (Cassels–Tate pairing)**.** Let $\mathfrak{a}$, $\mathfrak{b} \in \mathrm{Sel}_2(A/K)$. There will be several choices involved in the definition of $\langle \mathfrak{a}, \mathfrak{b}\rangle_{\mathrm{CT},\lambda}$. We begin with the global choices.

Pick cocycles a and b representing $\mathfrak{a}$ and $\mathfrak{b}$ respectively. Next, pick $\sigma \in C^1(K, A[4])$ such that $2\sigma = a$. Then $d\sigma$ is a 2-cocycle with values in $A[2]$, i.e. an element of $Z^2(K, A[2])$. The Weil pairing $(\ , \ )_\lambda : A[2] \times A[2] \to \boldsymbol{\mu}_2 \hookrightarrow \bar{K}^\times$ induces a cup-product map $\cup : Z^2(K, A[2]) \times Z^1(K, A[2]) \to Z^3(K, \bar{K}^\times)$. As K is a number field $H^3(K, \bar{K}^\times) = 0$, so we may choose $\epsilon \in C^2(K, \bar{K}^\times)$ such that $d\sigma \cup b = d\epsilon$.

Now for the local choices. Fix a place v of K. The class of a_v is trivial in $H^1(K_v, A(\bar{K_v}))$ so we may choose $P_v \in A(\bar{K_v})$ with $a_v = dP_v$. Pick $Q_v \in A(\bar{K_v})$ with $2Q_v = P_v$. Then $\rho_v := dQ_v$ is an element of $Z^1(K_v, A[4])$ and $\sigma_v - \rho_v$ takes values in $A[2]$, i.e. is an element of $C^1(K_v, A[2])$. Then we may form the element $(\sigma_v - \rho_v) \cup b_v$ of $C^2(K_v, \bar{K_v}^\times)$ (again defining the cup-product map using the Weil pairing on $A[2]$). The difference $(\sigma_v - \rho_v) \cup b_v - \epsilon_v$ is

a 2-cocycle with values in $\bar{K_v}^\times$. Let $\mathfrak{d}_v$ denote its class in $H^2(K_v, \bar{K_v}^\times) = \mathrm{Br}(K_v)$. Then $\langle \mathfrak{a}, \mathfrak{b} \rangle_{\mathrm{CT},\lambda}$ is defined as

$$\langle \mathfrak{a}, \mathfrak{b} \rangle_{\mathrm{CT},\lambda} := \sum_{v \in M_K} \mathrm{inv}_v(\mathfrak{d}_v) \ \in \mathbb{Q}/\mathbb{Z}.$$

The value of the sum above is independent of all choices made.

5.4. **Controlling the parity of $\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A/K)[2]$ globally.** If A is an elliptic curve and λ its canonical principal polarisation then it is well known that $\langle\ ,\ \rangle_{\mathrm{CT},\lambda}$ is in fact alternating and it follows that $\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A/K)[2]$ is even. For general principally polarised abelian varieties however, Poonen and Stoll showed in [PS99] that $\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A/K)[2]$ need not be even and gave a criterion for determining whether or not this is the case. Specificaly, let $\mathfrak{c}_\lambda \in H^1(K, A[2])$ be the cohomology class associated to λ as in Definition 4.6. By [PS99, Lemma 1] we in fact have $\mathfrak{c}_\lambda \in \mathrm{Sel}_2(A/K)$.

We then have the following theorem of Poonen–Stoll.

Theorem 5.4. *The group $Ш_{\mathrm{nd}}(A/K)[2]$ has even $\mathbb{F}_2$-dimension if and only if*

$$\langle \mathfrak{c}_\lambda, \mathfrak{c}_\lambda \rangle_{\mathrm{CT},\lambda} = 0 \in \mathbb{Q}/\mathbb{Z}.$$

Proof. The image of $\mathfrak{c}_\lambda$ in $Ш(A/K)[2]$ is the homogeneous space associated to λ as in [PS99, §2]. Theorem 8 of op. cit. now gives the result. □

Remark 5.5. Since the image of $\mathfrak{c}_\lambda$ in $Ш(A/K)$ is annihilated by 2 we have $\langle \mathfrak{c}_\lambda, \mathfrak{c}_\lambda \rangle_{\mathrm{CT},\lambda} \in \{0, \frac{1}{2}\}$.

5.5. **Quadratic twists.** For the rest of the section fix a quadratic character χ and let (A^χ, ψ) be the quadratic twist of A by χ. We now set up the notation which we will use when computing with A^χ in what follows. We endow A^χ with the K-rational principal polarisation $\lambda_\chi := (\psi^\vee)^{-1}\lambda\psi^{-1}$ (see §4.5). Associated to λ_χ is the Weil pairing

$$(\ ,\ )_{\lambda_\chi} : A^\chi[2] \times A^\chi[2] \to \boldsymbol{\mu}_2$$

and the Cassels–Tate pairing

$$\langle\ ,\ \rangle_{\mathrm{CT},\lambda_\chi} : Ш(A^\chi/K)[2] \times Ш(A^\chi/K)[2] \to \mathbb{Q}/\mathbb{Z}$$

(which we also view as a pairing on $\mathrm{Sel}_2(A^\chi/K)$). Using the isomorphism ψ we identify $A^\chi[2]$ and $A[2]$ as G_K-modules. Note that this identification also respects the Weil pairing (i.e. identifies $(\ ,\ )_{\lambda_\chi}$ with $(\ ,\ )_\lambda$; to see this e.g. combine Lemma 4.5(ii) and Lemma 4.17). In this way, we identify $H^1(K, A^\chi[2])$ with $H^1(K, A[2])$ and thus view the 2-Selmer group $\mathrm{Sel}_2(A^\chi/K)$ inside $H^1(K, A[2])$. In particular, we may talk about the intersection of $\mathrm{Sel}_2(A/K)$ and $\mathrm{Sel}_2(A^\chi/K)$.

We also use ψ to identify $A[4](\bar{K})$ with $A^\chi[4](\bar{K})$. This last identification does not respect the G_K-action. Thus for each i, we have identified $C^i(K, A^\chi[4])$ with $C^i(K, A[4])$ but the differential $d : C^i(K, A^\chi[4]) \to C^{i+1}(K, A^\chi[4])$ is not identified with the usual differential on $C^i(K, A[4])$; we write d_χ for the map $C^i(K, A[4]) \to C^{i+1}(K, A[4])$ to which is does correspond. For example, the map $d : C^1(K, A^\chi[4]) \to C^2(K, A^\chi[4])$ corresponds to the map $d_\chi : C^1(K, A[4]) \to C^2(K, A[4])$ defined by

$$(d_\chi f)(\sigma, \tau) = f(\sigma) + \chi(\sigma)\sigma f(\tau) - f(\sigma\tau).$$

Similarly, we use ψ to identify $C^i(K, A^\chi(\bar{K}))$ and $C^i(K, A(\bar{K}))$ for each i, and define differentials d_χ on $C^i(K, A(\bar{K}))$ similarly.

5.6. **Strategy of the proof of Theorem 1.4.** To motivate what follows, we briefly sketch the proof of Theorem 1.4.

For $\mathfrak{a}, \mathfrak{b} \in Ш(A/K)$, in the definition of $\langle \mathfrak{a}, \mathfrak{b} \rangle_{\mathrm{CT},\lambda}$ the local terms $\mathfrak{d}_v$ (in the notation of Definition 5.3) depend on the global choices. In particular, it is not clear that $\langle \mathfrak{c}_\lambda, \mathfrak{c}_\lambda \rangle_{\mathrm{CT},\lambda}$, and hence the parity of $\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A/K)[2]$, may be expressed as a sum of local terms whose definition requires no global choices (this is, however, known to be true if A/K is the Jacobian of a curve: see [PS99, Corollary 12]).

When considering A along with its quadratic twist A^χ, we eliminate the global choices as follows. Associated to λ_χ is the class $\mathfrak{c}_{\lambda_\chi} \in \mathrm{Sel}_2(A^\chi/K)$ (viewed inside $H^1(K, A[2])$ as in §5.5). By Corollary 4.18 we have $\mathfrak{c}_{\lambda_\chi} = \mathfrak{c}_\lambda$ and in particular, $\mathfrak{c}_\lambda$ lies in $\mathrm{Sel}_2(A/K) \cap \mathrm{Sel}_2(A^\chi/K)$. Now the sum of the pairings $\langle\ ,\ \rangle_{\mathrm{CT},\lambda}$ and $\langle\ ,\ \rangle_{\mathrm{CT},\lambda_\chi}$ gives a new pairing on $\mathrm{Sel}_2(A/K) \cap \mathrm{Sel}_2(A^\chi/K)$. By Theorem 5.4, $\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A/K)[2] + \dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A^\chi/K)[2]$ is even if and only if $\mathfrak{c}_\lambda$ pairs trivially with itself under this new pairing.

We show in Lemma 5.8 that the global choices involved in computing the sum of the two Cassels–Tate pairings are milder than those for the individual pairings (we remark that this simplification of the Cassels–Tate pairing under quadratic twist has also been observed in the recent preprint of Smith [Smi16, Proof of Theorem 3.2]). Specifically, the global choices involved in computing

$$\langle \mathfrak{c}_\lambda, \mathfrak{c}_\lambda \rangle_{\mathrm{CT},\lambda} + \langle \mathfrak{c}_\lambda, \mathfrak{c}_\lambda \rangle_{\mathrm{CT},\lambda_\chi}$$

are: a choice of cocycle $c_\lambda \in Z^1(K, A[2])$ representing $\mathfrak{c}_\lambda$, and a choice of cochain $F : G_K \to \boldsymbol{\mu}_2$ such that $dF = c_\lambda \cup c_\lambda \in Z^2(K, \boldsymbol{\mu}_2)$.

By Lemma 4.7, $\mathfrak{c}_\lambda \in H^1(K, A[2])$ is the cohomology class parameterizing quadratic refinements of the Weil pairing. In particular, a choice of cocycle representing $\mathfrak{c}_\lambda$ amounts to a choice of quadratic refinement q. For each such q we have already constructed a canonical choice for the function F above, namely that given by Proposition 3.9. Thus the only global choice remaining is that of q. Proposition 3.10 shows how this choice for F changes upon changing q, allowing us to prove that the local terms then arising do not, in fact, depend on the choice of quadratic refinement either.

5.7. **Pairings on $\mathbf{Sel}_2(A/K) \cap \mathbf{Sel}_2(A^\chi/K)$.** Define $\mathcal{S}_\chi := \mathrm{Sel}_2(A/K) \cap \mathrm{Sel}_2(A^\chi/K)$. Here we define a pairing $\langle\ ,\ \rangle_{S_\chi}$ on $\mathcal{S}_\chi$ with values in $\mathbb{Q}/\mathbb{Z}$ which we shall see is the sum of the Cassels–Tate pairings for A and its twist A^χ. However, for clarity when using this pairing later, we define it separately.

Definition 5.6 (The pairing $\langle\ ,\ \rangle_{S_\chi}$)**.** Let $\mathfrak{a}$,$\mathfrak{b} \in \mathcal{S}_\chi = \mathrm{Sel}_2(A/K) \cap \mathrm{Sel}_2(A^\chi/K)$. As with the definition of the Cassels–Tate pairing, we begin with the global choices. We first claim that $\mathfrak{a} \cup \mathfrak{b} = 0 \in H^2(K, \boldsymbol{\mu}_2) = \mathrm{Br}(K)[2]$. Indeed, for each place v of K both $\mathfrak{a}_v$ and $\mathfrak{b}_v$ are in the image of $A(K_v)/2A(K_v)$ under the connecting homomorphism associated to the multiplication-by-2 Kummer sequence. Since this image is its own orthogonal complement under the cup-product pairing

$$H^1(K_v, A[2]) \times H^1(K_v, A[2]) \to H^2(K_v, \bar{K_v}^\times) = \mathrm{Br}(K_v)$$

(this results from Tate local duality, see e.g. [Mil06, I.3.4]) we have $(\mathfrak{a} \cup \mathfrak{b})_v = 0 \in \mathrm{Br}(K_v)$ for each place v of K. Reciprocity for the Brauer group now gives the claim.

Now represent $\mathfrak{a}$ and $\mathfrak{b}$ by cocycles a and b respectively and, as is possible by the above discussion, pick $f \in C^1(K, \boldsymbol{\mu}_2)$ with $df = a \cup b \in \mathrm{Z}^2(K, \boldsymbol{\mu}_2)$.

We now turn to the local choices. Fix a place v of K. Since $\mathfrak{a} \in \mathrm{Sel}_2(A/K)$ there is $P_v \in A(\bar{K}_v)$ with $dP_v = a_v$. Pick $Q_v \in A(\bar{K}_v)$ with $2Q_v = P_v$. Then $\rho_v := dQ_v$ is an element of $Z^1(K_v, A[4])$. Since $\mathfrak{a}$ is also in $\mathrm{Sel}_2(A^\chi/K)$ we can similarly (i.e. by replacing d by d_χ throughout) define $P_{v,\chi}$, $Q_{v,\chi}$ and $\rho_{v,\chi} = d_\chi Q_{v,\chi} \in C^1(K_v, A[4])$. Then $\rho_v + \rho_{v,\chi}$ takes values in $A[2]$. One checks that $d(\rho_v + \rho_{v,\chi}) = \chi_v \cup a_v \in Z^2(K_v, A[2])$. Thus the difference

$$(\rho_v + \rho_{v,\chi}) \cup b_v \ - \ \chi_v \cup f_v$$

is a 2-cocycle with values in $\boldsymbol{\mu}_2$. Denote by $\mathfrak{d}_v$ its class in $\mathrm{Br}(K_v)[2]$.

Now define

$$\langle a, b \rangle_{S_\chi} := \sum_{v \in M_K} \mathrm{inv}_v(\mathfrak{d}_v) \in \mathbb{Q}/\mathbb{Z}.$$

One easily checks that once the initial global choices are made the cocycle class $\mathfrak{d}_v \in \mathrm{Br}(K_v)$ is independent of the local choices. That the resulting sum is independent of all choices follows from reciprocity for the Brauer group.

Remark 5.7. If a place v of K splits in the quadratic extension L/K associated to χ then χ_v is trivial and ψ gives an isomorphism between A and A^χ over K_v. It follows easily that the local terms $\mathrm{inv}_v(\mathfrak{d}_v)$ are trivial at all such v. Thus in the definition of $\langle\ ,\ \rangle_{S_\chi}$ we may replace the sum over all places of K by the sum over all places of K non-split in L/K.

Lemma 5.8. *The pairing $\langle\ ,\ \rangle_{S_\chi}$ is the sum of the Cassels–Tate pairings for A and A^χ:*

$$\langle\ ,\ \rangle_{S_\chi} = \langle\ ,\ \rangle_{CT,\lambda} + \langle\ ,\ \rangle_{CT,\lambda_\chi}.$$

In particular, it is (anti-)symmetric.

Remark 5.9. This lemma is implicit in the recent preprint of Smith [Smi16, Proof of Theorem 3.2].

Proof. Fix $\mathfrak{a}, \mathfrak{b} \in S_\chi$. We begin by making the global choices involved in computing $\langle \mathfrak{a}, \mathfrak{b} \rangle_{CT,\lambda}$. We pick cocycles a and b representing $\mathfrak{a}$ and $\mathfrak{b}$ respectively and pick $\sigma \in C^1(K, A[4])$ with $2\sigma = a$. Next, we pick $\epsilon \in C^2(K, \bar{K}^\times)$ with $d\epsilon = d\sigma \cup b$.

We now make the corresponding choices involved in computing $\langle \mathfrak{a}, \mathfrak{b} \rangle_{CT,\lambda_\chi}$. As we are at liberty to do, we pick the same cocycle representitves a and b chosen above. We similarly pick the same element σ of $C^1(K, A[4])$ satisfying $2\sigma = a$ (here using the identification of $A[4]$ with $A^\chi[4]$ via ψ as discussed). We then pick $\epsilon_\chi \in C^2(K, \bar{K}^\times)$ such that $d\epsilon_\chi = d_\chi\sigma \cup b$. Note that we cannot chose $\epsilon = \epsilon_\chi$ in general due to the difference between the differentials d and d_χ. However, we have

$$d(\epsilon + \epsilon_\chi) = (d\sigma + d_\chi\sigma) \cup b = (\chi \cup a) \cup b,$$

the last equality following from the definition of d_χ and a simple computation.

Now let $f \in C^1(K, \boldsymbol{\mu}_2)$ be such that $df = a \cup b$. By (2.1) and associativity of the cup-product we have $d(\chi \cup f) = d(\epsilon + \epsilon_\chi)$ whence $\chi \cup f = \epsilon + \epsilon_\chi + \nu$ for some cocycle $\nu \in Z^2(K, \bar{K}^\times)$.

We now make the local choices involved in computing $\langle \mathfrak{a}, \mathfrak{b} \rangle_{CT,\lambda}$. We choose $P_v \in A(\bar{K}_v)$ with $dP_v = a_v$ and then pick $Q_v \in A(\bar{K}_v)$ with $2Q_v = P_v$. Next, set $\rho_v := dQ_v \in C^1(K_v, A[4])$ and define $\mathfrak{d}_v$ to be the class of $(\sigma_v - \rho_v) \cup b_v - \epsilon_v$ in $H^2(K_v, \bar{K}_v{}^\times)$.

Finally, we make the local choices involved in computing $\langle \mathfrak{a}, \mathfrak{b} \rangle_{CT,\lambda_\chi}$. Thus we pick $P_{v,\chi}$ with $d_\chi P_{v,\chi} = a_v$, $Q_{v,\chi}$ with $2Q_{v,\chi} = P_{v,\chi}$, set $\rho_{v,\chi} = d_\chi Q_{v,\chi}$ and define $\mathfrak{d}_{v,\chi}$ to be the class of $(\sigma_v - \rho_{v,\chi}) \cup b_v - \epsilon_{\chi,v}$ in $H^2(K_v, \bar{K}_v{}^\times)$.

With these choices in place $\mathfrak{d}_v + \mathfrak{d}_{v,\chi}$ is the class in $\mathrm{Br}(K_v)$ of

$$(a_v - (\rho_v + \rho_{v,\chi})) \cup b_v - \chi_v \cup f_v + \nu_v.$$

Noting that $\rho_v + \rho_{v,\chi}$ takes values in $A[2]$ and that $\mathfrak{a}_v \cup \mathfrak{b}_v = 0$ (as discussed previously) we see that

$$\mathrm{inv}_v(\mathfrak{d}_v) + \mathrm{inv}_v(\mathfrak{d}_{v,\chi}) = \mathrm{inv}_v\left((\rho_v + \rho_{v,\chi}) \cup b_v - \chi_v \cup f_v\right) + \mathrm{inv}_v(\nu_v).$$

Summing over all places and noting that by reciprocity for the Brauer group we have

$$\sum_{v \in M_K} \mathrm{inv}_v(\nu_v) = 0 \in \mathbb{Q}/\mathbb{Z},$$

we have

$$\langle \mathfrak{a}, \mathfrak{b} \rangle_{CT} + \langle \mathfrak{a}, \mathfrak{b} \rangle_{CT,\chi} = \sum_{v \in M_K} \mathrm{inv}_v\left((\rho_v + \rho_{v,\chi}) \cup b_v - \chi_v \cup f_v\right).$$

But this is precisely how the quantity $\langle \mathfrak{a}, \mathfrak{b} \rangle_{S_\chi}$ was defined. □

5.8. **The local terms $\mathfrak{g}(A, \lambda, \chi)$.** In this subsection we study the local terms which arise in computing $\langle \mathfrak{c}_\lambda, \mathfrak{c}_\lambda \rangle_{\mathcal{S}_\chi}$, and show in particular that they are independent of certain choices involved. We work purely locally and take F to be a local field of characteristic 0. Let $(A/F, \lambda)$ be a principally polarised abelian variety. Let $\chi \in \mathrm{Hom}_{\mathrm{cnt}}(G_F, \boldsymbol{\mu}_2)$ be a quadratic character of F and $(A^\chi/F, \psi)$ be the quadratic twist of A by χ. We use the same conventions and notation as in §5.5 when talking about objects associated to A^χ. We will need to identify $\boldsymbol{\mu}_2$ with the additive group of $\mathbb{F}_2$ in the following, and we write the group law on $\boldsymbol{\mu}_2$ additively to avoid confusion when doing this.

Denote by $\mathfrak{c}_\lambda \in H^1(F, A[2])$ the cohomology class associated to λ as in Definition 4.6. By [PS99, Lemma 1] its image in $H^1(F, A)[2]$ is trivial. By Corollary 4.18, it follows also that the image of $\mathfrak{c}_\lambda$ in $H^1(F, A^\chi)[2]$ is trivial too (here the map $H^1(F, A[2]) \to H^1(F, A^\chi)[2]$ comes from identifying $A[2]$ with $A^\chi[2]$ via ψ).

Remark 5.10. By Lemma 4.7 $\mathfrak{c}_\lambda$ is equal to the cohomology class associated to the set of quadratic refinements of the Weil pairing $(\ ,\ )_\lambda$ on $A[2]$. In particular, for each quadratic refinement q of $(\ ,\ )_\lambda$, the function $c_q : G_F \to A[2]$ sending $\sigma \in G_F$ to the unique element $c_q(\sigma) \in A[2]$ such that

$$q(\sigma^{-1}v) - q(v) = (v, c_q(\sigma))_\lambda$$

for all $v \in A[2]$, is a cocycle in $Z^1(F, A[2])$ representing the class $\mathfrak{c}_\lambda$.

Definition 5.11. Let $q : A[2] \to \boldsymbol{\mu}_2$ be a quadratic refinement of the Weil pairing $(\ ,\ )_\lambda$. Then we define the function $F_q : G_F \to \boldsymbol{\mu}_2$ as the composition

$$F_q : G_F \longrightarrow \mathrm{Sp}(A[2]) \xrightarrow{f_q} \mathbb{F}_2 \cong \boldsymbol{\mu}_2,$$

where the map $G_F \to \mathrm{Sp}(A[2])$ is the homomorphism coming from the action of G_F on $A[2]$ and $f_q : \mathrm{Sp}(A[2]) \to \mathbb{F}_2$ is the map afforded by Proposition 3.9.

Remark 5.12. For each quadratic refinement q of $(\ ,\ )_\lambda$ it follows from Proposition 3.9 that we have $dF_q = c_q \cup c_q \in Z^2(F, \boldsymbol{\mu}_2)$.

Definition 5.13. Let $\chi \in \mathrm{Hom}_{\mathrm{cnt}}(G_F, \boldsymbol{\mu}_2)$ be a quadratic character, let q be a quadratic refinement of $(\ ,\ )_\lambda$ and let c_q be the associated cocycle representing $\mathfrak{c}_\lambda$. As in the definition of the local choices for the pairing $\langle\ ,\ \rangle_{S_\chi}$, pick $P_q \in A(\bar{F})$ with $dP_q = c_q$, let $Q_q \in A(\bar{F})$

be such that $2Q_q = P_q$ and set $\rho_q = dQ_q$. Similarly, pick $P_{\chi,q} \in A(\bar{F})$ with $d_\chi P_{\chi,q} = c_q$, let $Q_{\chi,q} \in A(\bar{F})$ be such that $2Q_{\chi,q} = P_{\chi,q}$ and set $\rho_{\chi,q} = d_\chi Q_{\chi,q}$.

We then define $\mathfrak{g}(A, \lambda, \chi, q)$ to be the class of the cocycle

$$g(A, \lambda, \chi, q) := (\rho_q + \rho_{\chi,q}) \cup c_q - \chi \cup F_q$$

in $\mathrm{Br}(F)[2]$. As in §5.7, $\mathfrak{g}(A, \lambda, \chi, q)$ does not depend on the choices of $P_q, Q_q, P_{\chi,q}$ or $Q_{\chi,q}$.

The following lemma is key to the proof of Theorem 1.4.

Lemma 5.14. *The quantity $\mathfrak{g}(A, \lambda, \chi, q) \in \mathrm{Br}(F)[2]$ is independent of the choice of quadratic refinement q.*

Proof. Keep the notation of Definition 5.13 in what follows. Let q and q' be two quadratic refinements. Then $q - q' = (-, v)_\lambda$ for some $v \in A[2]$ and $c_{q'} = c_q + dv$. By Proposition 3.10 we have

$$F_{q'} = F_q + c_q \cup v + v \cup c_q + v \cup dv.$$

Now fix choices for $P_q, Q_q, P_{\chi,q}$ and $Q_{\chi,q}$ as in Definition 5.13. Then we may take $P_{q'} = P_q + v$ and $P_{\chi,q'} = P_{\chi,q} + v$. Pick $T \in A[4]$ with $2T = v$. Then we may take $Q_{q'} = Q_q + T$ and $Q_{\chi,q'} = Q_{\chi,q} + T$. Thus

$$\rho_{q'} + \rho_{\chi,q'} = \rho_q + \rho_{\chi,q} + dT + d_\chi T.$$

An easy computation gives $dT + d_\chi T = dv + \chi \cup v$. Combining this with the expressions for $F_{q'}$ and $c_{q'}$ in terms of F_q and c_q respectively, we see that we have an equality of cocycles

$$g(A, \lambda, \chi, q') = g(A, \lambda, \chi, q) + (\rho_q + \rho_{\chi,q}) \cup dv + (dv + \chi \cup v) \cup (c_q + dv) - \chi \cup (c_q \cup v + v \cup c_q + v \cup dv)$$

inside $Z^2(F, \boldsymbol{\mu}_2)$.

Now $c_q + dv \in C^1(F, A[2])$ is a cocycle whilst $dv \in C^1(F, A[2])$ is a coboundary. Thus the class of $dv \cup (c_q + dv)$ is trivial in $\mathrm{Br}(F)[2]$. Using this observation, cancelling like terms in the previous expression, and passing to classes in the Brauer group, one has

$$\mathfrak{g}(A, \lambda, \chi, q') = \mathfrak{g}(A, \lambda, \chi, q) + [(\rho_q + \rho_{\chi,q}) \cup dv - \chi \cup c_q \cup v]$$

(where here '[ ]' denotes the operation of taking classes in the Brauer group).

Now, as remarked in the definition of the pairing $\langle\ ,\ \rangle_{S_\chi}$, we have $d(\rho_q + \rho_{\chi,q}) = \chi \cup c_q$. Thus by standard properties of cup product on cochains (see §2.2) we have

$$d\left((\rho_q + \rho_{\chi,q}) \cup v\right) = (\rho_q + \rho_{\chi,q}) \cup dv - \chi \cup c_q \cup v.$$

In particular, the class of $(\rho_q + \rho_{\chi,q}) \cup dv - \chi \cup c_q \cup v$ is trivial in $\mathrm{Br}(F)$, whence $\mathfrak{g}(A, \lambda, \chi, q') = \mathfrak{g}(A, \lambda, \chi, q)$ as desired. □

Lemma 5.14 allows us to make the folllowing refinement of Definition 5.13.

Definition 5.15. Define $\mathfrak{g}(A, \lambda, \chi) \in \mathrm{Br}(F)[2]$ to be the quantity $\mathfrak{g}(A, \lambda, \chi, q)$ for any choice of quadratic refinement q of $(\ ,\ )_\lambda$.

The following proposition computes explicitly the terms $\mathfrak{g}(A, \lambda, \chi)$ in certain cases.

Proposition 5.16. *Let $\mathfrak{g}(A, \lambda, \chi) \in \mathrm{Br}(F)[2]$ be as in Definition 5.15.*

(i) *We have $\mathfrak{g}(A, \lambda, \mathbb{1}) = 0$ where $\mathbb{1}$ is the trivial character of F.*

(ii) *Suppose that q is a G_F-invariant quadratic refinement of the Weil pairing $(\ ,\ )_\lambda$ on $A[2]$ and let $\alpha : G_F \to \boldsymbol{\mu}_2$ be the quadratic character corresponding to the homomorphism*

$$G_F \longrightarrow O(q)/SO(q) \cong \mathbb{Z}/2\mathbb{Z} \cong \boldsymbol{\mu}_2$$

coming from the action of G_F on $A[2]$. Then

$$\mathfrak{g}(A, \lambda, \chi) = \alpha \cup \chi \in \mathrm{Br}(F)[2].$$

(iii) *Suppose that F is nonarchimedean with odd residue characteristic and that A has good reduction. Then we have*

$$\mathrm{inv}_F\ \mathfrak{g}(A, \lambda, \chi) = \begin{cases} 0 & \chi \text{ unramified} \\ \frac{1}{2} \dim_{\mathbb{F}_2} A(F)[2] \in \mathbb{Q}/\mathbb{Z} & \chi \text{ ramified.} \end{cases}$$

(iv) *Suppose that F is archimedean. Then we have*

$$\mathrm{inv}_F\ \mathfrak{g}(A, \lambda, \chi) = \begin{cases} 0 & F = \mathbb{C} \text{ or } \chi \text{ trivial,} \\ \frac{1}{2} \dim_{\mathbb{F}_2} A(F)[2] \in \mathbb{Q}/\mathbb{Z} & F = \mathbb{R} \text{ and } \chi \text{ non-trivial.} \end{cases}$$

Proof. (i): Clear.

(ii): If there is an F-rational quadratic refinement q then c_q is identically zero and it follows immediately from Lemma 5.14 and the definition of $\mathfrak{g}(A, \lambda, \chi, q)$ that

$$\mathfrak{g}(A, \lambda, \chi) = \mathfrak{g}(A, \lambda, \chi, q) = -\chi \cup F_q = \chi \cup \alpha$$

where for the last equality we use that the restriction of F_q to elements of $O(q)$ agrees with the Dickson homomorphism d_q (see Proposition 3.9).

(iii): By [PR11, Proposition 3.6 (d)], our assumptions on F and the reduction of A imply that there is a G_F-invariant quadratic refinement q of the Weil pairing on $A[2]$. Let α be the associated quadratic character so that $\mathfrak{g}(A, \lambda, \chi) = \alpha \cup \chi$ by (ii). Now by definition, α factors through $\mathrm{Gal}(F(A[2])/F)$ and our assumptions on F and A mean that $F(A[2])/F$ is unramified. Consequently, α is unramified. In fact, let σ denote the Frobenius element in $F(A[2])/F$. Then by Proposition 3.5 we have

$$\alpha(\sigma) = (-1)^{\dim_{\mathbb{F}_2} A[2]^\sigma} = (-1)^{\dim_{\mathbb{F}_2} A(F)[2]}.$$

In particular, we see that if $\dim_{\mathbb{F}_2} A(F)[2]$ is even then α is the trivial character, whilst if $\dim_{\mathbb{F}_2} A(F)[2]$ is odd then α is the unique non-trivial unramified quadratic character of F. Since F is assumed to have odd residue characteristic, standard properties of the cup-product of two quadratic characters gives the result (we review these later in §8.1: see, in particular, Lemma 8.4).

(iv): The argument here is similar to that of (iii). First note that if χ is trivial then $\mathfrak{g}(A, \lambda, \chi) = 0$ by (i). In particular, the only case we have not already covered is when $F = \mathbb{R}$ and χ is the quadratic character corresponding to the extension $\mathbb{C}/\mathbb{R}$. By [PR11, Proposition 3.6 (d)] there is an $\mathbb{R}$-rational quadratic refinement q of the Weil pairing $(\ ,\ )_\lambda$. Let α be the associated quadratic character and write σ for the unique non-trivial element of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. By Proposition 3.5 we see that α is trivial if $\dim_{\mathbb{F}_2} A[2]^\sigma = \dim_{\mathbb{F}_2} A(\mathbb{R})[2]$ is even, and is the quadratic character corresponding to $\mathbb{C}/\mathbb{R}$ otherwise. The result now follows from (ii). □

Remark 5.17. As in Lemma 4.5, if the polarisation λ is of the form $\phi_{\mathcal{L}}$ for an F-rational symmetric line bundle $\mathcal{L}$ then there is an associated G_F-invariant quadratic refinement of the Weil pairing on $A[2]$. Thus combined with Proposition 5.16 (ii) this gives a geometric condition for when the local terms $\mathfrak{g}(A, \lambda, \chi)$ may be evaluated.

Remark 5.18. It is natural to ask if the terms $\mathfrak{g}(A,\lambda,\chi)$ are independent of the choice of principal polarisation λ. The above proposition shows that this is true when χ is trivial, when A/F has good reduction and F has odd residue characteristic, or when F is archimedean. We have been unable to prove this in general however.

Remark 5.19. Write $L = F(A[2])$ and let χ be any quadratic character. Since for any quadratic refinement q the cocycle c_q factors through $\mathrm{Gal}(L/F)$, the points P_q and $P_{\chi,q}$ of Definition 5.13 lie in $A(L)$ and $A^\chi(L)$ respectively. In particular, it follows that the cocycle $\mathfrak{g}(A,\lambda,\chi)$ factors through $\mathrm{Gal}(L'/F)$, where L' is the compositum of all the (finitely many) quadratic extensions of $F(A[2])$.

5.9. **Controlling the parity of $\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A/K)[2] + \dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A^\chi/K)[2]$ via local contributions.** We return to the notation of §5.1-§5.7 so that, in particular, K is a number field and $(A/K,\lambda)$ a principally polarised abelian variety.

Theorem 5.20 (=Theorem 1.4)**.** *Let χ be a quadratic character of K and for each place v of K write χ_v for the restriction of χ to G_{K_v}, A/K_v for the base change of A to K_v, and λ_v for the principal polarisation on A/K_v corresponding to λ.*

Then $\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A/K)[2] + \dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A^\chi/K)[2] \equiv 0 \pmod 2$ *if and only if*

$$\sum_{v\in M_K} \mathrm{inv}_v\ \mathfrak{g}(A/K_v,\lambda_v,\chi_v) = 0 \in \mathbb{Q}/\mathbb{Z}.$$

Remark 5.21. Before proving Theorem 5.20 we remark that if v is a nonarchimedean place of K, not dividing 2 and such that both A has good reduction and χ is unramified at v, then $\mathfrak{g}(A/K_v,\lambda_v,\chi_v) = 0$ by Proposition 5.16 (iii). In particular, the sum in the statement of Theorem 5.20 is finite.

Proof of Theorem 5.20. By Corollary 4.18, Theorem 5.4 applied to both A and A^χ (along with their principal polarisations λ and λ_χ), and Lemma 5.8, we see that $\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A/K)[2] + \dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A_\chi/K)[2]$ is even if and only if $\langle \mathfrak{c}_\lambda, \mathfrak{c}_\lambda\rangle_{\mathcal{S}_\chi} = 0$.

We now follow Definition 5.6 to compute $\langle \mathfrak{c}_\lambda, \mathfrak{c}_\lambda\rangle_{\mathcal{S}_\chi}$. For the global choices, fix a quadratic refinement q of the Weil pairing $(\ ,\ )_\lambda$ on $A[2]$. Then as in the local case (Remark 5.10) the function $c_q : G_K \to A[2]$ sending $\sigma \in G_K$ to the unique element $c_q(\sigma) \in A[2]$ such that

$$q(\sigma^{-1}v) - q(v) = (v, c_q(\sigma))_\lambda$$

for all $v \in A[2]$, is a cocycle in $Z^1(F, A[2])$ representing the class $\mathfrak{c}_\lambda$. Similarly, the function $F_q : G_K \to \boldsymbol{\mu}_2$ defined as the composition

$$F_q : G_K \longrightarrow \mathrm{Sp}(A[2]) \xrightarrow{f_q} \mathbb{F}_2 \cong \boldsymbol{\mu}_2,$$

(where the map $G_K \to \mathrm{Sp}(A[2])$ is the homomorphism coming from the action of G_K on $A[2]$ and $f_q : \mathrm{Sp}(A[2]) \to \mathbb{F}_2$ is the map afforded by Proposition 3.9) is an element of $C^1(K, \boldsymbol{\mu}_2)$ satisfying $dF_q = c_q \cup c_q \in Z^2(K, \bar{K}^\times)$.

With these global choices in place, the local terms arising in the definition of $\langle \mathfrak{c}_\lambda, \mathfrak{c}_\lambda\rangle_{\mathcal{S}_\chi}$ are precisely the terms $\mathfrak{g}(A/K_v,\lambda_v,\chi_v,q)$ of Definition 5.13. By Lemma 5.14 (for fixed v) they are independent of q, their common value being by definition $\mathfrak{g}(A/K_v,\lambda_v,\chi_v)$.

Thus

$$\langle \mathfrak{c}_\lambda, \mathfrak{c}_\lambda\rangle_{\mathcal{S}_\chi} = \sum_{v\in M_K} \mathrm{inv}_v\ \mathfrak{g}(A/K_v,\lambda_v,\chi_v)$$

and the result follows. □

6. Disparity in Selmer ranks: definitions and recollections

The next four sections are devoted to proving Theorem 7.4 concerning the parity of certain Selmer groups defined in terms of abstract twisting data. Our aproach follows closely the strategy of [KMR13], which proves the result for Galois modules of dimension 2 (whilst we handle arbitrary (even) dimension). Many of the statements of op. cit. go through with some minor changes however in order to highlight the diferences it is necessary to recall much of their setup and basic results. Thus in this section we recall the setup of [KMR13]. Where notions need to be generalised or slightly adapted we state the differences in a remark immediately following the definition.

6.1. **Notation.** Here we fix some notation which will remain in place for the entirety of §6-§9. Fix first a prime p and number field K. Following [KMR13], for a field L (either K or K_v for some $v \in M_K$) we define $\mathcal{C}(L) := \mathrm{Hom}_{\mathrm{cnt}}(G_L, \boldsymbol{\mu}_p)$, the group of characters of order dividing p. We denote the trivial character by $\mathbb{1}_L$. Further, we define $\mathcal{F}(L)$ to be the quotient of $\mathcal{C}(L)$ by the action of $\mathrm{Aut}(\boldsymbol{\mu}_p)$ (the action given by post-composition). The set $\mathcal{F}(L)$ is naturally identified with the set of cyclic extensions of L of degree dividing p, the map being given by sending the equivalence class of $\chi \in \mathcal{C}(L)$ to the fixed field $\bar{K}^{\ker(\chi)}$. When L is a nonarchimedean local field we write $\mathcal{C}_{\mathrm{ram}}(L)$ (resp. $\mathcal{C}_{\mathrm{ur}}(L)$) for the subset of $\mathcal{C}(L)$ consisting of ramified (resp. unramified) characters, and similarly write $\mathcal{F}_{\mathrm{ram}}(L)$ (resp. $\mathcal{F}_{\mathrm{ur}}(L)$) for the subset of $\mathcal{F}(L)$ corresponding to ramified (resp. unramified) extensions. Note that if L has residue characteristic coprime to p then $\mathcal{C}_{\mathrm{ram}}(L)$ (and hence also $\mathcal{F}_{\mathrm{ram}}(L)$) is non-empty if and only if $\boldsymbol{\mu}_p \subseteq L$.

For an finite dimensional $\mathbb{F}_p$-vector space M we say that a map $q : M \to \mathbb{Q}/\mathbb{Z}$ is a *quadratic form* if $q(nx) = n^2 q(x)$ for all $n \in \mathbb{Z}$ and $x \in M$, and if the map $(x, y) \mapsto q(x+y) - q(x) - q(y)$ is a symmetric bilinear pairing on M. We say that q is *non-degenerate* if the associated pairing is (i.e. if it has trivial kernel). If q is a quadratic form on M with associated pairing $\langle\ ,\ \rangle$ then for a subspace W of M we write

$$W^{\perp} = \{m \in M\ :\ \langle w, m\rangle = 0\ \forall w \in W\}$$

for the orthogonal complement of W and say that W is a *Lagrangian* subspace of (M, q) if $W = W^{\perp}$ and $q(W) = 0$. We call (M, q) a *metabolic space* if q is non-degenerate and if M has a Lagrangian subspace.

6.2. **The module T and the finite set of places Σ.** Fix, for the remainder of §6-§9, a finite dimensional $\mathbb{F}_p$-vector space T equipped with a continuous G_K-action and a non-degenerate G_K-equivariant alternating pairing

$$(\ ,\ ) : T \times T \longrightarrow \boldsymbol{\mu}_p$$

(so that, in particular, $\dim_{\mathbb{F}_p} T$ is necessarily even). For $v \in M_K$, if the inertia subgroup of G_{K_v} acts trivially on T then we say that T is *unramified* at v, and *ramified* at v otherwise. We denote by $K(T)$ the field of definition of the elements of T, i.e. the fixed field of the kernel of the action of G_K on T. Note that the presence of the pairing forces $K(\boldsymbol{\mu}_p) \subseteq K(T)$.

We also fix a finite set Σ of places of K containing all archimedean places, all places over p, and all places where T is ramified (and possibly some more to be specified later).

6.3. **The Local Tate Pairing and Tate quadratic forms.** For each place $v \in M_K$ write $\langle\ ,\ \rangle_v$ for the local Tate pairing

$$H^1(K_v, T) \times H^1(K_v, T) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

given by the composition

$$H^1(K_v,T)\times H^1(K_v,T)\xrightarrow{\cup} H^2(K_v,\boldsymbol{\mu}_p)\xrightarrow{\mathrm{inv}_v}\mathbb{Q}/\mathbb{Z},$$

where the first map is induced by cup-product and the pairing $(\ ,\ )$. It is non-degenerate, bilinear and symmetric.

Definition 6.1. Let v be a place of K. We say a quadratic form $q_v : H^1(K_v,T)\to\mathbb{Q}/\mathbb{Z}$ is a *Tate quadratic form* if its associated bilinear form is the local Tate pairing $\langle\ ,\ \rangle_v$. If $v\notin\Sigma$ then we say that q_v is *unramified* if it vanishes on $H^1_{\mathrm{ur}}(K_v,T)$ (in which case $H^1_{\mathrm{ur}}(K_v,T)$ is a Lagrangian subspace for q_v).

Remark 6.2. If $p=2$ then our definition differs slightly from [KMR13, Definition 3.2] of Klagsbrun–Mazur–Rubin since it allows quadratic forms valued in $\frac{1}{4}\mathbb{Z}/\mathbb{Z}$ whilst their definition only allows quadratic forms taking values in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$. This extra generality is necessary when $\dim_{\mathbb{F}_p}T>2$ in order to allow $T=A[2]$ for a principally polarised abelian variety A/K (see Remark 10.4).

As in [KMR13, Lemma 3.4], if $p>2$ then there is a unique Tate quadratic form q_v on $H^1(K_v,T)$ given by

$$q_v=\frac{1}{2}\langle\ ,\ \rangle_v.$$

6.4. **Global metabolic structures.** With our slightly modified definition of a Tate quadratic form in hand we can define a global metabolic structure on T in an identical way to [KMR13, Definition 3.3].

Definition 6.3. A *global metabolic structure* $\mathbf{q}$ on T consists of a collection $\mathbf{q}=(q_v)_v$ ($v\in M_K$) of Tate quadratic forms such that

(i) for each $v\in M_K$ the pair $\big(H^1(K_v,T),q_v\big)$ is a metabolic space,
(ii) the quadratic form q_v is unramified at each place $v\notin\Sigma$,
(iii) if $c\in H^1(K,T)$ then $\sum_v q_v(c_v)=0$.

As in [KMR13, Lemma 3.4], if $p>2$ then the unique Tate quadratic forms on $H^1(K_v,T)$ defined above do indeed give a global metabolic structure on T, so specifying a global metabolic structure is only necessary when $p=2$.

6.5. **Selmer structures and Selmer groups.** We define Selmer structures for $(T,\mathbf{q})$, along with the associated Selmer groups, as in [KMR13, Definition 3.8].

Definition 6.4. A Selmer structure $\mathcal{S}$ for $(T,\mathbf{q})$ is the data of

(i) a finite set $\Sigma_{\mathcal{S}}$ of places of K containing Σ,
(ii) for each $v\in\Sigma_{\mathcal{S}}$ a Lagrangian subspace $H_{\mathcal{S}}(K_v,T)$ of $\big(H^1(K_v,T),q_v\big)$.

Definition 6.5. Let $\mathcal{S}$ be a Selmer structure for $(T,\mathbf{q})$. For each $v\notin\Sigma_{\mathcal{S}}$ we set $H^1_{\mathcal{S}}(K_v,T)=H^1_{\mathrm{ur}}(K_v,T)$ and define the *Selmer group* associated to $\mathcal{S}$ as

$$H^1_{\mathcal{S}}(K,T):=\ker\left(H^1(K,T)\longrightarrow\bigoplus_{v\in M_K}H^1(K_v,T)/H^1_{\mathcal{S}}(K_v,T)\right).$$

The following theorem, which is a very slight generalisation of [KMR13, Theorem 3.9], allows us to compare the dimensions of two Selmer groups modulo 2.

Theorem 6.6. *Let $\mathcal{S}$ and $\mathcal{S}'$ be two Selmer structures for $(T, \boldsymbol{q})$. Then*

$$\dim_{\mathbb{F}_p} H^1_{\mathcal{S}}(K,T) - \dim_{\mathbb{F}_p} H^1_{\mathcal{S}'}(K,T) \equiv$$

$$\sum_{\Sigma_{\mathcal{S}} \cup \Sigma_{\mathcal{S}'}} \dim_{\mathbb{F}_p} H^1_{\mathcal{S}}(K_v,T)/(H^1_{\mathcal{S}}(K_v,T) \cap H^1_{\mathcal{S}'}(K_v,T)) \pmod 2.$$

Proof. This is proven for $\dim_{\mathbb{F}_p} T = 2$ in [KMR13, Theorem 3.9] and the proof generalises verbatim to the case where T has arbitrary (even) dimension with one subtlety: their proof relies on [KMR13, Proposition 2.4] which is a general result concerning the dimension of the intersection of Lagrangian subspaces of a finite dimensional metabolic space. The one difference from the case there is that now our quadratic forms (in general) take values in $\mathbb{Q}/\mathbb{Z}$ rather than just $\mathbb{F}_p$ as they assume. However, one readily verifies that this assumption is not used in the proof of the cited result. Alternatively, see [Čes18, Theorem 5.9] which gives a further generalisation of [KMR13, Theorem 3.9] which includes our case. □

6.6. **Twisting data and twisted Selmer groups.** Fix from now on a global metabolic structure $\mathbf{q}$ on T.

Definition 6.7. For each place $v \in M_K$, write $\mathcal{H}(q_v)$ for the set of Lagrangian subspaces for q_v and, for $v \notin \Sigma$, write $\mathcal{H}_{\mathrm{ram}}(q_v)$ for the subset of $\mathcal{H}(q_v)$ consisting of Lagrangian subspaces X for which $X \cap H^1_{\mathrm{ur}}(K_v,T) = 0$.

Definition 6.8 (Twisting data)**.** We define *twisting data* $\boldsymbol{\alpha}$ for $(T, \mathbf{q}, \Sigma)$ to consist of

(i) for each $v \in \Sigma$ a map

$$\alpha_v : \mathcal{F}(K_v) \longrightarrow \mathcal{H}(q_v),$$

(ii) for each $v \notin \Sigma$ for which $\boldsymbol{\mu}_p \subseteq K_v$, a map

$$\alpha_v : \mathcal{F}_{\mathrm{ram}}(K_v) \longrightarrow \mathcal{H}_{\mathrm{ram}}(q_v).$$

Remark 6.9. Our definition of twisting data is slightly different to that of [KMR13, Definition 4.4]. In their case, since T has dimension 2, for $v \notin \Sigma$ and with $\boldsymbol{\mu}_p \subseteq K_v$, $\mathcal{H}_{\mathrm{ram}}(q_v)$ has cardinality 0,1, or p according to $\dim T^{G_{K_v}} = 0, 1$ or 2 respectively. In the first two cases they do not specify a map α_v as there is a unique such. In the final case they additionally insist that α_v is a bijection, as is possible since $\mathcal{F}_{\mathrm{ram}}(K_v)$ has order p.

Since for us T is allowed to have dimension greater that 2 we in general have $|\mathcal{H}_{\mathrm{ram}}(q_v)| > p$ and thus cannot insist that α_v is a bijection once it ceases to be unique. Although omitting this condition does not impact what follows, and is in fact not used in the main results of [KMR13], we remark that it is used crucially in a follow up paper to op. cit. ([KMR14]).

Definition 6.10 (Twisted Selmer groups)**.** Let $(T,\ \mathbf{q},\ \Sigma,\ \boldsymbol{\alpha})$ as above be fixed, and let $\chi \in \mathcal{C}(K)$. Let P_χ denote the set of primes of K for which χ ramifies. Then we define a Selmer structure $\mathcal{S}(\chi)$ by taking $\Sigma_{\mathcal{S}(\chi)}$ to be $\Sigma \cup P_\chi$ and setting $H^1_{\mathcal{S}(\chi)}(K_v,T) := \alpha_v(\chi_v)$ for $v \in \Sigma \cup P_\chi$. We write $\mathrm{Sel}(T,\chi)$ for the associated Selmer group:

$$\mathrm{Sel}(T,\chi) := H^1_{\mathcal{S}(\chi)}(K,T).$$

6.7. **Comparing the parity of dimensions of twisted Selmer groups.** From now on we fix T, the set of places Σ, a global metabolic structure $\mathbf{q}$, and twisting data $\boldsymbol{\alpha}$.

The following theorem, which is a slight variant of [KMR13, Theorem 4.11] allows us to compare the parity of the dimensions of the Selmer groups $\mathrm{Sel}(T,\chi)$ as we vary χ. We first make one further definition.

Definition 6.11. Let v be a place of K and χ_1 and χ_2 be elements of $\mathcal{C}(K_v)$. Then we set

$$h_v(\chi_1,\chi_2) := \dim_{\mathbb{F}_p}\left(\alpha_v(\chi_1)/(\alpha_v(\chi_1)\cap\alpha_v(\chi_2))\right).$$

Note that since any two Lagrangian subspaces of $H^1(K_v,T)$ have the same dimension this is symmetric in χ_1 and χ_2.

Theorem 6.12. *For any $\chi\in\mathcal{C}(K)$ we have*

$$\dim_{\mathbb{F}_p}\mathrm{Sel}(T,\chi)-\dim_{\mathbb{F}_p}\mathrm{Sel}(T,\mathbb{1}_K)\equiv\sum_{v\in\Sigma}h_v(\mathbb{1}_{K_v},\chi_v)+\sum_{v\notin\Sigma,\chi_v\ \mathrm{ram}}\dim_{\mathbb{F}_p}T^{G_{K_v}}\pmod 2$$

(here the second sum is taken over places $v\notin\Sigma$ for which the character χ_v is ramified).

Proof. This is essentially [KMR13, Theorem 4.11]. Let $\mathcal{S}(\chi)$ and $\mathcal{S}(\mathbb{1}_K)$ be the Selmer structures associated to the characters χ and $\mathbb{1}_K$ respectively. Then

$$\Sigma_{\mathcal{S}(\chi)}\cup\Sigma_{\mathcal{S}(\mathbb{1}_K)}=\Sigma\sqcup\{v\notin\Sigma\ :\ \chi_v\text{ ramified}\}.$$

Applying Theorem 6.6 to $\mathcal{S}(\chi)$ and $\mathcal{S}(\mathbb{1}_K)$ and noting that, by the definition of the twisting data, $H^1_{\mathrm{ur}}(K_v,T)\cap\alpha_v(\chi_v)=0$ for all $v\notin\Sigma$ for which χ_v is ramified, we obtain

$$\dim_{\mathbb{F}_p}\mathrm{Sel}(T,\chi)-\dim_{\mathbb{F}_p}\mathrm{Sel}(T,\mathbb{1}_K)\equiv\sum_{v\in\Sigma}h_v(\mathbb{1}_{K_v},\chi_v)+\sum_{v\notin\Sigma,\chi_v\ \mathrm{ram}}\dim_{\mathbb{F}_p}H^1_{\mathrm{ur}}(K_v,T)\pmod 2.$$

The result now follows since for each $v\notin\Sigma$ we have $\dim_{\mathbb{F}_p}H^1_{\mathrm{ur}}(K_v,T)=\dim_{\mathbb{F}_p}T^{G_{K_v}}$. This is shown in (the proof of) [KMR13, Lemma 3.7] in the case that T has dimension 2. The general case is identical. □

7. Disparity in Selmer ranks: statement and first cases

In this section we fix $(T,\Sigma,\mathbf{q},\boldsymbol{\alpha})$ as in the previous section and consider the proportion of characters χ for which the associated Selmer groups $\mathrm{Sel}(T,\chi)$ have odd (resp. even) $\mathbb{F}_p$-dimension. To make this precise, one has to order the elements of $\mathcal{C}(K)$.

7.1. **Ordering twists.** We use the same ordering as in [KMR13, Definition 7.3].

Definition 7.1. For $\chi\in\mathcal{C}(K)$, set

$$||\chi|| = \max\{N(\mathfrak{p})\ :\ \chi\text{ is ramified at }\mathfrak{p}\}$$

(where here for a prime $\mathfrak{p}\lhd\mathcal{O}_K$, $N(\mathfrak{p})$ denotes the norm of $\mathfrak{p}$). If this set is empty, our convention is that $||\chi||=1$. Now for each $X>0$ define

$$\mathcal{C}(K,X)=\{\chi\in\mathcal{C}(K)\ :\ ||\chi||<X\}.$$

For each $X\geq 1$ this is a finite subgroup of $\mathcal{C}(K)$ and each element of $\mathcal{C}(K)$ appears in $\mathcal{C}(K,X)$ for some X. We will make crucial use of the group structure on the $\mathcal{C}(K,X)$ to facilitate with counting problems.

We will repeatedly use the following fact.

Lemma 7.2. *For all sufficiently large $X > 0$ the restriction homomorphism*

$$\mathcal{C}(K, X) \longrightarrow \prod_{v \in \Sigma} \mathcal{C}(K_v)$$

sending χ to $(\chi_v)_{v \in \Sigma}$ is surjective.

Proof. This follows immediately from the Grunwald–Wang theorem. See for example [NSW08, Theorem 9.2.3(ii)]. See also [KMR13, Proposition 6.8 (i)] but note that they have a running hypothesis on the set of places Σ which we do not wish to impose at this stage. □

7.2. **Statement of the result.** The proportion of characters for which $\dim_{\mathbb{F}_p} \mathrm{Sel}(T, \chi)$ is even (resp. odd) will depend heavily on the action of G_K on T. More specifically, it will depend on the behaviour of the following function. Recall that $K(T)$ denotes the field of definition of the elements of T.

Definition 7.3. Write $G := \mathrm{Gal}(K(T)/K)$ and define the function

$$\epsilon : G \to \{\pm 1\}$$

by

$$\sigma \mapsto (-1)^{\dim_{\mathbb{F}_p} T^\sigma}.$$

The result is then the following.

Theorem 7.4. *We have:*

(i) *if either $p = 2$ and ϵ fails to be a homomorphism, or $p > 2$ and ϵ is non-trivial when restricted to $\mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$, then*

$$\lim_{X \to \infty} \frac{|\{\chi \in \mathcal{C}(K, X) \ : \ \dim_{\mathbb{F}_p} \mathrm{Sel}(T, \chi) \text{ is even}\}|}{|\mathcal{C}(K, X)|} = 1/2.$$

Moreover, if $p = 2$ then it suffices to take X sufficiently large as opposed to taking the limit $X \to \infty$.

(ii) *if either $p = 2$ and ϵ is a homomorphism, or $p > 2$ and ϵ is trivial when restricted to $\mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$, then for all sufficiently large X we have*

$$\frac{|\{\chi \in \mathcal{C}(K, X) \ : \ \dim_{\mathbb{F}_p} \mathrm{Sel}(T, \chi) \text{ is even}\}|}{|\mathcal{C}(K, X)|} = \frac{1 + (-1)^{\dim_{\mathbb{F}_p} \mathrm{Sel}(T, \mathbb{1}_K)} \cdot \delta}{2}$$

with $\delta = \prod_{v \in \Sigma} \delta_v$ given in Definition 7.8.

The proof of Theorem 7.4, which is a combination of Theorems 7.10 and 9.5, will occupy the remainder of §7-§9.

Remark 7.5. Here we briefly discuss the function ϵ. For convenience we identify $\boldsymbol{\mu}_p$ with the additive group of $\mathbb{F}_p$ and think of the pairing $(\ ,\ )$ as landing in $\mathbb{F}_p$. Due to this pairing, the group $G = \mathrm{Gal}(K(T)/K)$ is a subgroup of the general symplectic group

$$\mathrm{GSp}(T) = \{g \in \mathrm{GL}(V) \ : \ \forall v, w \in T, \ (gv, gw) = \lambda(g)(v, w) \text{ for some } \lambda(g) \in \mathbb{F}_p^\times\}.$$

First suppose $p = 2$ so that $\mathrm{GSp}(T) = \mathrm{Sp}(T)$ is the symplectic group associated to $(\ ,\ )$. If $\dim_{\mathbb{F}_2} T > 4$ then $\mathrm{Sp}(T)$ is simple and since any symplectic transvection σ (i.e. element of $\mathrm{Sp}(T)$ of the form $v \mapsto v + (v, w)w$ for fixed $0 \neq w \in T$) has $\dim_{\mathbb{F}_2} T^\sigma$ odd, if G is isomorphic to $\mathrm{Sp}(T)$ (i.e. is as large as possible) then ϵ is not a homomorphism. Thus Case (i) of Theorem 7.4 is, in some sense, the 'generic' case. When $\dim_{\mathbb{F}_2} T = 2$ one can check that ϵ

is always a homomorphism, whilst if $\dim_{\mathbb{F}_2} T = 4$ then $\mathrm{Sp}(T)$ is isomorphic to the symmetric group S_6. One can check (see Example 10.17 later) that when G is either the whole of S_6 or the alternating group A_6 then ϵ is not a homomorphism, so again Case (i) of Theorem 7.4 holds for G 'large enough'. On the other hand, Proposition 3.5 gives a supply of examples where ϵ is a homomorphism. Namely, if G fixes a quadratic refinement q of $(\ ,\ )$ then G is a subgroup of the orthogonal group $O(q)$, in which case ϵ is the Dickson homomorphism.

Now suppose that $p > 2$. The subgroup $\mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$ consists of those elements $g \in G$ for which $\lambda(g) = 1$. That is, it is the intersection of G with the symplectic group $\mathrm{Sp}(T)$. If G contains a symplectic transvection σ (which as now $p > 2$ is an element of $\mathrm{Sp}(T)$ of the form $v \mapsto v + \beta \cdot (v, w)w$ for $\beta \in \mathbb{F}_p^\times, 0 \neq w \in T$) then one sees easily that $\epsilon(\sigma) = -1$, so that ϵ is non-trivial when restricted to $\mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$. Thus again Case (i) of Theorem 7.4 holds for G 'large enough'.

7.3. **The cases $p = 2$ and ϵ a homomorphism, and $p > 2$ and ϵ trivial when restricted to $\mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$.** Suppose now that either $p = 2$ and ϵ is a homomorphism, or $p > 2$ and ϵ is trivial for all $\sigma \in \mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$.

Definition 7.6. Let $v \in \Sigma$ and $\chi \in \mathcal{C}(K_v)$. If $p > 2$ we define

$$\omega_v(\chi) := (-1)^{h_v(\mathbb{1}_{K_v}, \chi)}.$$

If $p = 2$ view ϵ as a quadratic character of K and let $\Delta \in K^\times/K^{\times 2}$ be such that the corresponding quadratic extension is given by $K(\sqrt{\Delta})/K$. We then define

$$\omega_v(\chi) := \chi(\Delta)(-1)^{h_v(\mathbb{1}_{K_v}, \chi)}$$

where here for a place v of K we evaluate χ_v at Δ via local class field theory.

Lemma 7.7. *For any $\chi \in \mathcal{C}(K)$ we have*

$$(-1)^{\dim_{\mathbb{F}_p} \mathrm{Sel}(T,\chi)} = (-1)^{\dim_{\mathbb{F}_p} \mathrm{Sel}(T,\mathbb{1}_K)} \prod_{v \in \Sigma} \omega_v(\chi_v).$$

Proof. Fix $v \notin \Sigma$ with $\boldsymbol{\mu}_p \subseteq K_v$, and let $\mathrm{Frob}_v \in G$ denote the Frobenius element at v in $K(T)/K$. Then as T is unramified at v we have

$$(-1)^{\dim_{\mathbb{F}_p} T^{G_{K_v}}} = \epsilon(\mathrm{Frob}_v).$$

If $p > 2$ then $\epsilon(\mathrm{Frob}_v) = 1$ for all $v \notin \Sigma$ by assumption, whence the result follows from Theorem 6.12.

Now suppose that $p = 2$. As above, view ϵ as a quadratic character of K. Since ϵ factors through $\mathrm{Gal}(K(T)/K)$ it is unramified outside Σ. In particular, if $v \notin \Sigma$ is such that χ_v is unramified, then both ϵ_v and χ_v are unramified at v and so $\chi_v(\Delta) = 1$. On the other hand, if $v \notin \Sigma$ is such that χ_v ramifies at v then since K_v has odd residue characteristic, we have $\chi_v(\Delta) = \epsilon(\mathrm{Frob}_v)$ (see Lemma 8.4 (ii)). Global class field theory gives $\prod_{v \in M_K} \chi_v(\Delta) = 1$ from which it follows that

$$\prod_{v \notin \Sigma,\ \chi_v \text{ ram}} (-1)^{\dim_{\mathbb{F}_p} T^{G_{K_v}}} = \prod_{v \in \Sigma} \chi_v(\Delta).$$

We now conclude by Theorem 6.12. □

The proof of Theorem 7.4 (ii) now proceeds as in [KMR13, §7].

Definition 7.8. For each $v \in \Sigma$ define

$$\delta_v := \frac{1}{|\mathcal{C}(K_v)|} \sum_{\chi \in \mathcal{C}(K_v)} \omega_v(\chi) \qquad \text{and} \qquad \delta := \prod_{v \in \Sigma} \delta_v.$$

Remark 7.9. We have decided to define δ slightly differently to [KMR13, §7] so that it is a product of local terms. Our definition of the δ_v is consistent with theirs however.

Theorem 7.10. *Suppose that either $p = 2$ and ϵ is a homomorphism, or $p > 2$ and ϵ is trivial when restricted to $\mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$. Then for all sufficiently large $X > 0$ we have*

$$\frac{|\{\chi \in \mathcal{C}(K, X) \ : \ \dim_{\mathbb{F}_p} \mathrm{Sel}(T, \chi) \text{ is even}\}|}{|\mathcal{C}(K, X)|} = \frac{1 + (-1)^{\dim_{\mathbb{F}_p} \mathrm{Sel}(T, \mathbb{1}_K)} \delta}{2}.$$

Proof. The argument is the same as in [KMR13, Theorem 7.6]. We repeat it for convenience. Write $\Gamma = \prod_{v \in \Sigma} \mathcal{C}(K_v)$ and for $\chi \in \mathcal{C}(K)$, write $\chi|_\Gamma$ for the image of χ under the natural restriction homomorphism $\mathcal{C}(K) \to \Gamma$ sending χ to $(\chi_v)_{v \in \Sigma}$. From Lemma 7.7 we see that the parity of $\dim_{\mathbb{F}_p} \mathrm{Sel}(T, \chi)$ depends only on $\chi|_\Gamma$ and that $\dim_{\mathbb{F}_p} \mathrm{Sel}(T, \chi)$ is even if and only if

$$\prod_{v \in \Sigma} \omega(\chi_v) = (-1)^{\dim_{\mathbb{F}_p} \mathrm{Sel}(T, \mathbb{1}_K)}.$$

As if possible by Lemma 7.2, take X sufficiently large that $\mathcal{C}(K, X)$ surjects onto Γ under restriction. Since restriction is a group homomorphism, its fibres all have the same size (being cosets of the kernel) and, in particular, we have

$$\frac{|\{\chi \in \mathcal{C}(K, X) \ : \ \dim_{\mathbb{F}_p} \mathrm{Sel}(T, \chi) \text{ is even}\}|}{|\mathcal{C}(K, X)|} = \frac{|\{\gamma \in \Gamma \ : \ \prod_{v \in \Sigma} \omega(\gamma_v) = (-1)^{\dim_{\mathbb{F}_p} \mathrm{Sel}(T, \mathbb{1}_K)}\}|}{|\Gamma|}$$

where here, for $\gamma \in \Gamma$ we denote by γ_v its projection onto $\mathcal{C}(K_v)$.

To evaluate the right hand side of the above expression, define

$$N := |\{\gamma \in \Gamma \ : \ \prod_{v \in \Sigma} \omega(\gamma_v) = 1\}|.$$

Then we have

$$N - (|\Gamma| - N) = \sum_{\gamma \in \Gamma} \prod_{v \in \Sigma} \omega(\gamma_v) = \prod_{v \in \Sigma} \sum_{\chi_v \in \mathcal{C}(K_v)} \omega(\chi_v).$$

Dividing the above expression through by $2|\Gamma|$ gives

$$\frac{|\{\gamma \in \Gamma \ : \ \prod_{v \in \Sigma} \omega(\gamma_v) = 1\}|}{|\Gamma|} = \frac{1 + \delta}{2}$$

and the result follows immediately. □

8. Disparity in Selmer ranks: local symbols and global characters

In order to prove the remaining cases of Theorem 7.4 we now recall and slightly generalise (as well as rephrase for convenience in §9) the results of [KMR13, §6], which uses class field theory to analyse which collections of local characters arise from a global character.

8.1. **Local symbols.** For each nonarchimedean place v of K, Tate local duality gives a non-degenerate pairing

$$H^1(K_v, \boldsymbol{\mu}_p) \times H^1(K_v, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \mathbb{Q}/\mathbb{Z}, \tag{8.1}$$

defined as the composition

$$H^1(K_v, \boldsymbol{\mu}_p) \times H^1(K_v, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\cup} H^2(K, \boldsymbol{\mu}_p) \hookrightarrow \mathrm{Br}(K_v) \xrightarrow{\mathrm{inv}_v} \mathbb{Q}/\mathbb{Z}$$

(here the map '$\cup$' is the cup product map on cohomology combined with the canonical isomorphism $\mathbb{Z}/p\mathbb{Z} \otimes \boldsymbol{\mu}_p \cong \boldsymbol{\mu}_p$).

We now slightly modify this pairing. As the Galois action on $\mathbb{Z}/p\mathbb{Z}$ is trivial we have $H^1(K_v, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}_{\mathrm{cnt}}(G_{K_v}, \mathbb{Z}/p\mathbb{Z})$. Picking an isomorphism of abstract groups $\theta : \boldsymbol{\mu}_p \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}$ induces isommorphisms

$$\mathcal{C}(K_v) \cong H^1(K_v, \mathbb{Z}/p\mathbb{Z}) \qquad \text{and} \qquad \frac{1}{p}\mathbb{Z}/\mathbb{Z} \cong \boldsymbol{\mu}_p \tag{8.2}$$

where for the latter we identify $\mathbb{Z}/p\mathbb{Z}$ with $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$ by sending $1 \in \mathbb{Z}/p\mathbb{Z}$ to $\frac{1}{p}$. Noting that $H^2(K_v, \boldsymbol{\mu}_p) \subseteq \mathrm{Br}(K_v)$ is mapped by inv_v into $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$, combining the pairing (8.1) with the isomorphisms of (8.2) yields a non-degenerate pairing

$$[\ ,\ ]_v : H^1(K_v, \boldsymbol{\mu}_p) \times \mathcal{C}(K_v) \longrightarrow \boldsymbol{\mu}_p \tag{8.3}$$

which is easily seen to be independent of the choice of θ.

The following well known lemma summarises the properties of this local pairing.

Lemma 8.4. *Let v be a nonarchimedean place of K. Then*

(i) *if $v \nmid p$ then the groups $H^1_{\mathrm{ur}}(K_v, \boldsymbol{\mu}_p)$ and $\mathcal{C}_{\mathrm{ur}}(K_v)$ are orthogonal complements with respect to the pairing $[\ ,\ ]_v$.*

(ii) *let $x \in K_v^\times$ and write $\phi_x \in H^1(K_v, \boldsymbol{\mu}_p)$ for the image of x under the boundary map associated to the Kummer sequence*

$$1 \to \boldsymbol{\mu}_p \longrightarrow \bar{K}_v^\times \xrightarrow{x \mapsto x^p} \bar{K}_v^\times \to 1.$$

Then for any $\chi \in \mathcal{C}(K_v)$ we have

$$[\phi_x, \chi]_v = \chi(\mathrm{Art}_{K_v}(x))^{-1},$$

where here $\mathrm{Art}_{K_v} : K_v^\times \to G_{K_v}^{\mathrm{ab}}$ denotes the local Artin map.

(iii) *suppose v is such that $\boldsymbol{\mu}_p \subseteq K_v$ so that $H^1(K_v, \boldsymbol{\mu}_p) = \mathcal{C}(K_v)$. Then the resulting pairing*

$$[\ ,\ ]_v : \mathcal{C}(K_v) \times \mathcal{C}(K_v) \longrightarrow \boldsymbol{\mu}_p$$

is antisymmetric.

Proof. Part (i) is [NSW08, Theorem 7.2.15] whilst part (ii) is Corollary 7.2.13 of op cit. (The cited results are stated for the pairing of (8.1) rather than the altered pairing $[\ ,\ ]_v$ but in each case they immediately imply the claimed results.) Finally, antisymmetry of the cup product

$$H^1(K_v, \mathbb{Z}/p\mathbb{Z}) \times H^1(K_v, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^2(K_v, \mathbb{Z}/p\mathbb{Z} \otimes \mathbb{Z}/p\mathbb{Z})$$

gives part (iii). □

8.2. **Existence of global characters with specified restriction and ramification.** We will need the following lemma which is the analogue of [KMR13, Proposition 6.8 (iii)] in the case that the dimension of T is allowed to be larger than 2.

Notation 8.5. Writing $\Gamma := \prod_{v\in\Sigma}\mathcal{C}(K_v)$, we denote by $[\ ,\ ]_\Sigma$ the non-degenerate bilinear pairing

$$[\ ,\ ]_\Sigma : \left(\prod_{v\in\Sigma} H^1(K_v,\boldsymbol{\mu}_p)\right)\times\Gamma \longrightarrow \boldsymbol{\mu}_p$$

defined as the sum (or rather product) over $v\in\Sigma$ of the pairings $[\ ,\ ]_v$ of (8.3).

Lemma 8.6. *Let P denote the set of primes of K not in Σ which split completely in $K(T)/K$, and fix $\gamma\in\Gamma$. Then there is a character $\chi\in\mathcal{C}(K)$ unramified outside $\Sigma\cup P$ and with $\chi|_\Gamma=\gamma$, if and only if $[c,\gamma]_\Sigma=0$ for each c in the image of the restriction homomorphism*

$$H^1(K(T)/K,\boldsymbol{\mu}_p)\longrightarrow\prod_{v\in\Sigma}H^1(K_v,\boldsymbol{\mu}_p).$$

Proof. Exactness at the middle term of the Poitou–Tate exact sequence (see, for example, [Mil06, Theorem I.4.10]) applied to the set $\Sigma\cup P$ of places and the G_K-module $\mathbb{Z}/p\mathbb{Z}$ (and its dual $\boldsymbol{\mu}_p$), shows that

$$\mathrm{im}\left(H^1(K_{\Sigma\cup P}/K,\mathbb{Z}/p\mathbb{Z})\longrightarrow\prod_{v\in\Sigma\cup P}{}'H^1(K_v,\mathbb{Z}/p\mathbb{Z})\right)$$

is the orthogonal complement of

$$\mathrm{im}\left(H^1(K_{\Sigma\cup P}/K,\boldsymbol{\mu}_p)\longrightarrow\prod_{v\in\Sigma\cup P}{}'H^1(K_v,\boldsymbol{\mu}_p)\right)$$

under the sum of the local pairings of (8.1), where here $K_{\Sigma\cup P}$ denotes the maximal extension of K unramified outside $\Sigma\cup P$ and the restricted direct products are taken with respect to unramified classes.

Now fix any choice of isomorphism $\boldsymbol{\mu}_p\cong\mathbb{Z}/p\mathbb{Z}$ and use it to identify $\mathcal{C}(K)$ with $H^1(K,\mathbb{Z}/p\mathbb{Z})$, and $\mathcal{C}(K_v)$ with $H^1(K_v,\mathbb{Z}/p\mathbb{Z})$ for each v similarly. Then the group $H^1(K_{\Sigma\cup P}/K,\mathbb{Z}/p\mathbb{Z})$ corresponds to the group of characters unramified outside $\Sigma\cup P$, which we denote by $\mathcal{C}(K)_{\Sigma\cup P}$. Making these identifications and projecting onto $\prod_{v\in\Sigma}\mathcal{C}(K_v)$, it follows formally that the image of $\mathcal{C}(K)_{\Sigma\cup P}$ in $\prod_{v\in\Sigma}\mathcal{C}(K_v)$ is the orthogonal complement with respect to the pairing $[\ .\ ]_\Sigma$ of the image of

$$\ker\left(H^1(K_{\Sigma\cup P}/K,\boldsymbol{\mu}_p)\longrightarrow\prod_{v\in P}{}'H^1(K_v,\boldsymbol{\mu}_p)\right)$$

in $\prod_{v\in\Sigma}H^1(K_v,\boldsymbol{\mu}_p)$. We now conclude by the following lemma. □

Lemma 8.7. *Let P denote the set of primes of K not in Σ and which split completely in $K(T)/K$, and let $K_{\Sigma\cup P}$ denote the maximal extension of K unramified outside $\Sigma\cup P$. Then we have*

$$H^1(K(T)/K,\boldsymbol{\mu}_p)=\ker\left(H^1(K_{\Sigma\cup P}/K,\boldsymbol{\mu}_p)\longrightarrow\prod_{v\in P}{}'H^1(K_v,\boldsymbol{\mu}_p)\right),$$

the groups being compared inside $H^1(K,\boldsymbol{\mu}_p)$ (and the restricted direct product being taken with respect to unramified classes as above).

Proof. Since $K(T)$ is unramified outside Σ we have $K(T) \subseteq K_{\Sigma \cup P}$. Thus it suffices to show that we have

$$H^1(K(T)/K, \boldsymbol{\mu}_p) = \ker\left(H^1(K, \boldsymbol{\mu}_p) \xrightarrow{\text{res}} \prod_{v \in P}{}' H^1(K_v, \boldsymbol{\mu}_p) \right).$$

Since each prime in P splits completely in $K(T)/K$ the restriction map above factors as

$$H^1(K, \boldsymbol{\mu}_p) \xrightarrow{f_1} H^1(K(T), \boldsymbol{\mu}_p) \xrightarrow{f_2} \prod_{v \in \mathcal{P}}{}' H^1(K_v, \boldsymbol{\mu}_p),$$

both maps being given by restriction. Since the inflation-restriction exact sequence identifies $H^1(K(T)/K, \boldsymbol{\mu}_p)$ with $\ker(f_1)$, it suffices to show that f_2 is injective. Since $K(T)$ and each K_v ($v \in P$) contain $\boldsymbol{\mu}_p$, we may reinterpret f_2 as the restriction map on characters

$$\mathcal{C}(K(T)) \longrightarrow \prod_{v \in P}{}' \mathcal{C}(K_v).$$

Suppose $\chi \in \mathcal{C}(K(T))$ is a character of $K(T)$ which is trivial in $\mathcal{C}(K_v)$ for each $v \in P$, let $L/K(T)$ denote the extension corresponding to the fixed field of the kernel of χ, and let L'/K denote the Galois closure of L/K. Then our assumption on χ means that every prime $v \in \mathcal{P}$ splits completely in L'/K. By the Chebotarev density theorem this gives $[L' : K] \leq [K(T) : K]$. Since we already know that $K(T) \subseteq L'$ we must have $L' = K(T)$ whence χ is the trivial character. □

8.3. **Assumptions on the set of places Σ.** We now impose conditions on the finite set of places Σ (in addition to containing all archimedean places, all primes over p and all places for which T is ramified) which will be necessary for the proof of the remaining cases of Theorem 7.4.

Assumption 8.8. We henceforth impose the following conditions on the finite set of places Σ:

(i) the restriction homomorphism

$$H^1(K(T)/K, \boldsymbol{\mu}_p) \longrightarrow \prod_{v \in \Sigma} H^1(K_v, \boldsymbol{\mu}_p)$$

is injective,

(ii) $\mathrm{Pic}(\mathcal{O}_{K,\Sigma}) = 0$,

(iii) the natural map

$$\mathcal{O}_{K,\Sigma}^\times / (\mathcal{O}_{K,\Sigma}^\times)^p \longrightarrow \prod_{v \in \Sigma} K_v^\times / (K_v^\times)^p$$

is injective.

(In (ii) and (iii), $\mathcal{O}_{K,\Sigma}$ denotes the elements of K integral outside Σ.)

Lemma 8.9. *A set of places Σ satisfying 8.8 exists.*

Proof. We begin by taking Σ large enough that it contains all archimedean places, all primes over p and all places where T ramifies. By the Grunwald–Wang theorem [NSW08, Theorem 9.1.9(ii)] the map

$$H^1(K, \boldsymbol{\mu}_p) \longrightarrow \prod_{v \in M_K} H^1(K_v, \boldsymbol{\mu}_p)$$

is injective. In particular, as $H^1(K(T)/K, \boldsymbol{\mu}_p)$ is a finite subgroup of $H^1(K, \boldsymbol{\mu}_p)$, we see that by enlarging Σ if necessary we may additionally ensure that (i) holds.

Finally, [KMR13, Lemma 6.1] shows that any finite set of places may be further enlarged so that (ii) and (iii) hold. □

Lemma 8.10. *Suppose 8.8 is satisfied and let $\mathfrak{p}$ be a prime of K with $\mathfrak{p} \notin \Sigma$ and $\boldsymbol{\mu}_p \subseteq K_\mathfrak{p}^\times$. Write*

$$\delta_\mathfrak{p} : K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times p} \xrightarrow{\sim} \mathcal{C}(K_\mathfrak{p})$$

for the isomorphism (coming from the Kummer sequence) sending $x \in K_\mathfrak{p}^\times$ to the character $\sigma \mapsto \sigma(y)/y$ where $y \in \bar{K}_\mathfrak{p}^\times$ is such that $y^p = x$ (any two choices for y yield the same character since $\boldsymbol{\mu}_p \subseteq K_\mathfrak{p}$).

Then there is a (global) character $\varphi(\mathfrak{p}) \in \mathcal{C}(K)$ satisfying the following three conditions:

$$\begin{aligned} &\varphi(\mathfrak{p}) \text{ ramifies at } \mathfrak{p}, \\ &\varphi(\mathfrak{p}) \text{ is unramified outside } \Sigma \cup \{\mathfrak{p}\}, \\ &\text{the restriction of } \varphi(\mathfrak{p}) \text{ to } \mathcal{C}(K_\mathfrak{p}) \text{ is equal to } \delta_\mathfrak{p}(\varpi) \text{ for some uniformiser } \varpi \text{ of } K_\mathfrak{p}. \end{aligned} \tag{8.11}$$

Proof. Given the assmuptions on Σ, the existence of a character $\varphi(\mathfrak{p})$ which ramifies at $\mathfrak{p}$ and is unramified outside $\Sigma \cup \{\mathfrak{p}\}$ follows from [KMR13, Proposition 6.8 (ii)]. Fix one such and pick $x \in K_\mathfrak{p}^\times$ such that the restriction of $\varphi(\mathfrak{p})$ is equal to $\delta_\mathfrak{p}(x)$. Since $\varphi(\mathfrak{p})$ ramifies at $\mathfrak{p}$ the extension of $K_\mathfrak{p}^\times$ obtained by adjoining a p-th root of x ramifies. In particular, since $K_\mathfrak{p}$ has residue characteristic coprime to p (as $\mathfrak{p} \notin \Sigma$), the valuation $v_\mathfrak{p}(x)$ of x is coprime to p. Noting that replacing $\varphi(\mathfrak{p})$ with $\varphi(\mathfrak{p})^m$ for any m coprime to p yields another character which ramifies at $\mathfrak{p}$ and is unramified outside $\Sigma \cup \{\mathfrak{p}\}$, we may suppose that $v_\mathfrak{p}(x)$ is congruent to 1 modulo p. Finally, since $K_\mathfrak{p}^{\times p}$ is in the kernel of $\delta_\mathfrak{p}$ we may now shift x by a p-th power of a uniformiser to suppose that x has valuation 1 as desired. □

The following lemma evaluates the pairing $[\ ,\ ]_\Sigma$ of 8.5 between the characters $\varphi(\mathfrak{p})$ of Lemma 8.10 and elements of $H^1(K(T)/K, \boldsymbol{\mu}_p)$.

Lemma 8.12. *Let $\mathfrak{p}$ be a prime of K not in Σ, let $\varphi(\mathfrak{p})$ satisfy (8.11), and let $c \in H^1(K(T)/K, \boldsymbol{\mu}_p)$. Then writing $\mathrm{Frob}_\mathfrak{p}$ for the Frobenius element at $\mathfrak{p}$ in $\mathrm{Gal}(K(T)/K)$ we have*

$$[c, \varphi(\mathfrak{p})]_\Sigma = c(\mathrm{Frob}_\mathfrak{p}).$$

Proof. By global class field theory the product of $[c, \varphi(\mathfrak{p})]_v$ over all places of K is equal to 1. In particular, we have

$$[c, \varphi(\mathfrak{p})]_\Sigma = \prod_{v \notin \Sigma} [c, \varphi(\mathfrak{p})]_v.$$

If $\mathfrak{q}$ is a prime of K not in Σ then $\mathfrak{q} \nmid p$ and, additionally, $K(T)/K$ is unramified at $\mathfrak{q}$ whence the restriction of c to $H^1(K_\mathfrak{q}, \boldsymbol{\mu}_p)$ is in the unramified subgroup $H^1_{\mathrm{ur}}(K_\mathfrak{q}, \boldsymbol{\mu}_p)$. If $\mathfrak{q} \neq \mathfrak{p}$ then $\varphi(\mathfrak{p})$ is also unramified at $\mathfrak{q}$ whence $[c, \varphi(\mathfrak{p})]_\mathfrak{q} = 1$ by Lemma 8.4 (i).

It now follows that $[c, \varphi(\mathfrak{p})]_\Sigma = [c, \varphi(\mathfrak{p})]_\mathfrak{p}$ and to conclude we must show that $[c, \varphi(\mathfrak{p})]_\mathfrak{p} = c(\mathrm{Frob}_\mathfrak{p})$. Since $\boldsymbol{\mu}_p \subseteq K_\mathfrak{p}$ and we've chosen $\varphi(\mathfrak{p})$ so that its restriction to $\mathcal{C}(K_\mathfrak{p})$ agrees with $\delta_\mathfrak{p}(\varpi)$ for some uniformiser ϖ of $K_\mathfrak{p}$, parts (ii) and (iii) of Lemma 8.4 combine to give

$$[c, \varphi(\mathfrak{p})]_\mathfrak{p} = c(\mathrm{Art}_{K_\mathfrak{p}}(\varpi)).$$

Now c is unramified at $\mathfrak{p}$ and by standard properties of the local Artin map we have $\mathrm{Art}_{K_\mathfrak{p}}(\varpi)|_{K_\mathfrak{p}^{\mathrm{nr}}} = \mathrm{Frob}_{K_\mathfrak{p}}$. On the other hand, since c came from $H^1(K(T)/K, \boldsymbol{\mu}_p)$, its restriction to $H^1(K_\mathfrak{p}, \boldsymbol{\mu}_p)$

factors through $\mathrm{Gal}(K_{\mathfrak{p}}(T)/K_{\mathfrak{p}})$. As the restriction of $\mathrm{Frob}_{K_{\mathfrak{p}}}$ to $\mathrm{Gal}(K_{\mathfrak{p}}(T)/K_{\mathfrak{p}})$ is precisely $\mathrm{Frob}_{\mathfrak{p}}$, we have the result. □

9. Disparity in Selmer ranks: remaining cases

We now treat the remaining cases of Theorem 7.4, namely when $p = 2$ and ϵ fails to be a homomorphism, or when $p > 2$ and ϵ is non-trivial when restricted to $\mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$. Our strategy is broadly based on that of [KMR13, §8], although the arguments are more involved.

We begin by fixing a finite set of places Σ satisfying 8.8. As before let G denote the Galois group of $K(T)/K$ and write $\Gamma := \prod_{v\in\Sigma} \mathcal{C}(K_v)$. For $\chi \in \mathcal{C}(K)$ we denote by $\chi|_\Gamma$ the image of χ in Γ under the (product of the) natural restriction map(s).

Definition 9.1. Define a map $w : \mathcal{C}(K) \to \{\pm 1\}$ by

$$w(\chi) := \prod_{v\notin\Sigma,\ \chi_v \text{ ram}} (-1)^{\dim_{\mathbb{F}_p} T^{G_{K_v}}} = \prod_{v\notin\Sigma,\ \chi_v \text{ ram}} \epsilon(\mathrm{Frob}_v),$$

where here $\mathrm{Frob}_v \in G$ denotes the Frobenius element at v in $K(T)/K$.

Remark 9.2. By Theorem 6.12, for each $\chi \in \mathcal{C}(K)$ we have

$$(-1)^{\dim_{\mathbb{F}_2} \mathrm{Sel}(T,\chi)} = w(\chi)(-1)^{\dim_{\mathbb{F}_2} \mathrm{Sel}(T,\mathbb{1}_K)} \prod_{v\in\Sigma} (-1)^{h_v(\mathbb{1}_K,\chi_v)}.$$

We now examine the extent to which $w(\chi)$ behaves 'independently' of the restriction of χ to Γ. To this end, we make the following definition.

Definition 9.3. For each $X \geq 1$ and $\gamma \in \Gamma$, define

$$s_X(\gamma) = \frac{|\{\chi \in \mathcal{C}(K,X) \ :\ \chi|_\Gamma = \gamma,\ w(\chi) = 1\}|}{|\{\chi \in \mathcal{C}(K,X) \ :\ \chi|_\Gamma = \gamma\}|}.$$

The rest of the section is occupied with the proof of the following Theorem.

Theorem 9.4. *We have*

(i) *if $p = 2$ and ϵ fails to be a homomorphism then, for all sufficiently large X, $s_X(\gamma) = \frac{1}{2}$ for all $\gamma \in \Gamma$,*
(ii) *if $p > 2$ and ϵ is non-trivial when restricted to $\mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$ then $\lim_{X\to\infty} s_X(\gamma) = \frac{1}{2}$ for all $\gamma \in \Gamma$.*

Assuming this for the moment we get as a corollary the remaining cases of Theorem 7.4.

Theorem 9.5. *We have*

(i) *if $p = 2$ and ϵ fails to be a homomorphism then, for all sufficiently large X,*

$$\frac{|\{\chi \in \mathcal{C}(K,X) \ :\ \dim_{\mathbb{F}_p} \mathrm{Sel}(T,\chi) \text{ is even}\}|}{|\mathcal{C}(K,X)|} = \frac{1}{2},$$

(ii) *if $p > 2$ and ϵ is non-trivial when restricted to $\mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$ then*

$$\lim_{X\to\infty} \frac{|\{\chi \in \mathcal{C}(K,X) \ :\ \dim_{\mathbb{F}_p} \mathrm{Sel}(T,\chi) \text{ is even}\}|}{|\mathcal{C}(K,X)|} = \frac{1}{2}.$$

Proof. Fix $\gamma \in \Gamma$ and suppose that $\chi \in \mathcal{C}(K,X)$ is such that $\chi|_\Gamma = \gamma$. Then by Remark 9.2 we have

$$\dim_{\mathbb{F}_2}\mathrm{Sel}(T,\chi) \text{ is even } \Leftrightarrow\ w(\chi) = (-1)^{\dim_{\mathbb{F}_2}\mathrm{Sel}(T,\mathbb{1}_K)}\prod_{v\in\Sigma}(-1)^{h_v(\mathbb{1}_K,\gamma_v)},$$

and the right hand side depends only on γ. In particular, by Theorem 9.4 we have

$$\lim_{X\to\infty}\frac{|\{\chi\in\mathcal{C}(K,X)\ :\ \chi|_\Gamma=\gamma \text{ and } \dim_{\mathbb{F}_2}\mathrm{Sel}(T,\chi) \text{ is even}\}|}{|\{\chi\in\mathcal{C}(K,X)\ :\ \chi|_\Gamma=\gamma\}|} = \frac{1}{2},$$

and if $p=2$ then this is in fact an equality for all sufficiently large X rather than a limit. Averaging over all $\gamma\in\Gamma$ gives the result (note that the sets $\{\chi\in\mathcal{C}(K,X)\ :\ \chi|_\Gamma=\gamma\}$ all have the same size for sufficiently large X as the restriction map $\chi\mapsto\chi|_\Gamma$ is a homomorphism and is surjective for X sufficiently large by Lemma 7.2). □

We now turn to the proof of Theorem 9.4.

Definition 9.6. Fix an $\mathbb{F}_p$-basis $\{\phi_1,...,\phi_r\}$ for $H^1(K(T)/K,\boldsymbol{\mu}_p)$. Further, define the homomorphism $f:\Gamma\to\boldsymbol{\mu}_p^r$ by setting

$$f(\gamma) = ([\phi_i,\gamma]_\Sigma)_{i=1}^r$$

where here we view the ϕ_i inside $\prod_{v\in\Sigma}H^1(K_v,\boldsymbol{\mu}_p)$ via the product of the natural restriction maps, and $[\ ,\ ]_\Sigma$ is the pairing of 8.5 (we allow the case $r=0$ in which case $\boldsymbol{\mu}_p^r$ is the trivial group).

Remark 9.7. Since we have taken Σ large enough that the map

$$H^1(K(T)/K,\boldsymbol{\mu}_p)\longrightarrow\prod_{v\in\Sigma}H^1(K_v,\boldsymbol{\mu}_p)$$

is injective, it follows from the non-degeneracy of the pairing $[\ ,\ ]_\Sigma$ that f is surjective.

Definition 9.8. For each $n\geq 1$ and $\eta\in\boldsymbol{\mu}_p^r$, define

$$t_X(\eta) = \frac{|\{\chi\in\mathcal{C}(K,X)\ :\ f(\chi|_\Gamma)=\eta,\ w(\chi)=1\}|}{|\{\chi\in\mathcal{C}(K,X)\ :\ f(\chi|_\Gamma)=\eta\}|}.$$

The following lemma reduces the problem of understanding $s_X(\gamma)$ as γ ranges over the elements of Γ, to understanding $t_X(\eta)$ as η ranges over the elements of $\boldsymbol{\mu}_p^r$.

Lemma 9.9. (c.f. [KMR13, Lemma 8.4]) *Let $\gamma\in\Gamma$. Then for X sufficiently large we have*

$$s_X(\gamma) = t_X(f(\gamma)).$$

Proof. Let P denote the set of primes of K not in Σ and which split completely in $K(T)/K$, and let $\gamma'\in\Gamma$ be such that $f(\gamma')=f(\gamma)$. Then $\gamma'\gamma^{-1}$ is in the kernel of f so by Lemma 8.6 there is $\chi_{\gamma,\gamma'}\in\mathcal{C}(K)$ with $\chi_{\gamma,\gamma'}|_\Gamma=\gamma'\gamma^{-1}$ and such that $\chi_{\gamma,\gamma'}$ is unramified outside $\Sigma\cup P$. Now for any $\chi\in\mathcal{C}(K)$ we have $w(\chi)=w(\chi\chi_{\gamma,\gamma'})$ since the sets of primes not in Σ where χ and $\chi_{\gamma,\gamma'}$ ramify differ only at primes $\mathfrak{p}\in P$, and at such primes we have

$$\epsilon(\mathrm{Frob}_\mathfrak{p}) = \epsilon(1) = (-1)^{\dim T} = 1$$

(where as usual $\mathrm{Frob}_\mathfrak{p}$ denotes the Frobenius element at $\mathfrak{p}$ in $K(T)/K$). Thus if X is sufficiently large that $\chi_{\gamma,\gamma'}$ is in $\mathcal{C}(K,X)$, multiplication by $\chi_{\gamma,\gamma'}$ gives a bijection between the set

$$\{\chi\in\mathcal{C}(K,X)\ :\ \chi|_\Gamma=\gamma,\ w(\chi)=1\}$$

and the set

$$\{\chi \in \mathcal{C}(K,X) \ : \ \chi|_\Gamma = \gamma',\ w(\chi) = 1\},$$

as well as between the same two sets with the conditions on $w(\chi)$ removed.

Writing $\eta = f(\gamma)$, it follows that for X sufficiently large we have

$$t_X(\eta) = \frac{\sum_{\gamma' \in f^{-1}(\{\eta\})} |\{\chi \in \mathcal{C}(K,X) \ : \ \chi|_\Gamma = \gamma',\ w(\chi) = 1\}|}{\sum_{\gamma' \in f^{-1}(\{\eta\})} |\{\chi \in \mathcal{C}(K,X) \ : \ \chi|_\Gamma = \gamma'\}|}$$

$$= \frac{|f^{-1}(\{\eta\})| \cdot |\{\chi \in \mathcal{C}(K,X) \ : \ \chi|_\Gamma = \gamma,\ w(\chi) = 1\}|}{|f^{-1}(\{\eta\})| \cdot |\{\chi \in \mathcal{C}(K,X) \ : \ \chi|_\Gamma = \gamma\}|} = s_X(\gamma)$$

as desired. □

We now study the quantities $t_X(\eta)$ as η ranges over $\boldsymbol{\mu}_p^r$, splitting into cases according to $p = 2$ or $p > 2$.

9.1. **The case where $p = 2$ and ϵ fails to be a homomorphism.** Suppose now that $p = 2$ and ϵ fails to be a homomorphism.

Definition 9.10. Define the map $\theta : \mathcal{C}(K) \to \boldsymbol{\mu}_2^r \times \{\pm 1\}$ by setting

$$\theta(\chi) := (f(\chi|_\Gamma), w(\chi)).$$

The following observation will be crucial to our method. We remark that it fails for $p > 2$.

Lemma 9.11. *The map θ is a homomorphism.*

Proof. Since both the restriction map $\mathcal{C}(K) \to \Gamma$ and the map $f : \Gamma \to \boldsymbol{\mu}_2^r$ are homomorphisms, it suffices to show that $w : \mathcal{C}(K) \to \{\pm 1\}$ is a homomorphism.

For each $v \notin \Sigma$, define a map $w_v : \mathcal{C}(K_v) \to \{\pm 1\}$ by

$$w_v(\chi) = \begin{cases} (-1)^{\dim_{\mathbb{F}_2} T^{G_{K_v}}} & \chi \text{ ramified} \\ 1 & \text{else.} \end{cases}$$

Since w is the product of the w_v over $v \notin \Sigma$, it suffices to show that each w_v is a homomorphism. To see this, note that as $v \notin \Sigma$, K_v has odd residue characteristic. In particular, the product of any two ramified characters of K_v is unramified, and the product of a ramified character with an unramified character is again ramified. □

Remark 9.12. For $X > 0$ write θ_X for the restriction of θ to $\mathcal{C}(K,X)$. Then for each $\eta \in \boldsymbol{\mu}_2^r$ we have

$$t_X(\eta) = \frac{|\theta_X^{-1}((\eta,1))|}{|\theta_X^{-1}((\eta,1))| + |\theta_X^{-1}((\eta,-1))|}.$$

Now (for $X > 1$), $\mathcal{C}(K,X)$ is a group and θ_X is a homomorphism. Thus the fibres over points in the image of θ_X have the same size, being cosets of the kernel. In light of Lemma 9.9, Theorem 9.4 (i) is equivalent to the statement that, if ϵ fails to be a homomorphism, then θ_X is surjective for sufficiently large $X > 0$. Since $\boldsymbol{\mu}_2^r \times \{\pm 1\}$ is a finite group this is, in turn, equivalent to the statement that if ϵ fails to be a homomorphism then θ is surjective. This is the statement we now study, and prove in Proposition 9.14.

We now fix a collection of global characters $\{\varphi(\mathfrak{p})\}_{\mathfrak{p} \notin \Sigma}$ satisfying (8.11). Each $\varphi(\mathfrak{p})$ is ramified at $\mathfrak{p}$, yet unramified outside $\Sigma \cup \{\mathfrak{p}\}$. Lemma 8.12 allows us to evaluate the map θ on the $\varphi(\mathfrak{p})$.

Lemma 9.13. *For each $\mathfrak{p} \notin \Sigma$ we have*

$$\theta(\varphi(\mathfrak{p})) = \left((\phi_i(\mathrm{Frob}_\mathfrak{p}))_{i=1}^r, \epsilon(\mathrm{Frob}_\mathfrak{p})\right)$$

where here $\mathrm{Frob}_\mathfrak{p} \in G$ *denotes the Frobenius element at* $\mathfrak{p}$ *in* $K(T)/K$.

Proof. Since amongst the primes not in Σ the character $\varphi(\mathfrak{p})$ only ramifies at $\mathfrak{p}$, we have $w(\varphi(\mathfrak{p})) = \epsilon(\mathrm{Frob}_\mathfrak{p})$ by definition. We have $f(\varphi(\mathfrak{p})|_\Gamma) = (\phi_i(\mathrm{Frob}_\mathfrak{p}))_{i=1}^r$ by Lemma 8.12. □

Proposition 9.14. *The map $\theta : \mathcal{C}(K) \longrightarrow \boldsymbol{\mu}_2^r \times \{\pm 1\}$ is surjective if and only if ϵ fails to be a homomorphism.*

Proof. Note that the subgroup $\mathcal{U}$ of $\mathcal{C}(K)$ consisting of characters unramified outside Σ is in the kernel of θ, and the quotient $\mathcal{C}(K)/\mathcal{U}$ is generated by the $\varphi(\mathfrak{p})$ as $\mathfrak{p}$ ranges over primes not in Σ.

By the Chebotarev density theorem, each conjugacy class in $G = \mathrm{Gal}(K(T)/K)$ arises as $\mathrm{Frob}_\mathfrak{p}$ for some $\mathfrak{p} \notin \Sigma$ and so by Lemma 9.13 it follows that the image of θ is the subgroup of $\boldsymbol{\mu}_2^r \times \{\pm 1\}$ generated by the set

$$\{((\phi_i(\sigma))_{i=1}^r, \epsilon(\sigma)) \ : \ \sigma \in G\}$$

(note that for $\sigma \in G$, both $\epsilon(\sigma)$ and the $\phi_i(\sigma)$ depend only on the conjugacy class of σ in G).

Recall that the set $\{\phi_i : 1 \leq i \leq r\}$ is a basis for $H^1(K(T)/K, \boldsymbol{\mu}_2) = \mathrm{Hom}(G, \boldsymbol{\mu}_2)$. To make this more explicit denote by G^2 the subgroup of G generated by the squares of all the elements of G. It's a normal subgroup and the quotient G/G^2 is an abelian group of exponent 2. That is, G/G^2 is a finite dimensional $\mathbb{F}_2$-vector space. Since every homomorphism from G to $\boldsymbol{\mu}_2$ factors through G/G^2 we have

$$\mathrm{Hom}(G, \boldsymbol{\mu}_2) = \mathrm{Hom}(G/G^2, \boldsymbol{\mu}_2)$$

and the right hand group is just the dual of G/G^2 as an $\mathbb{F}_2$-vector space. In particular, the map $G/G^2 \to \boldsymbol{\mu}_2^r$ sending σ to $(\phi_i(\sigma))_{i=1}^r$ is an isomorphism.

Combining the above we arrive at a purely group theoretic criterion: θ is surjective if and only if the set

$$S := \{(\bar{\sigma}, \epsilon(\sigma)) \ : \ \sigma \in G\}$$

generates $G/G^2 \times \{\pm 1\}$, where here for $\sigma \in G$ we write $\bar{\sigma}$ for the image of σ in G/G^2.

Suppose now that ϵ is a homomorphism. Then ϵ necessarily factors through G/G^2 and we see that S generates an index 2 subgroup of $G/G^2 \times \{\pm 1\}$, so that θ is not surjective in this case.

Conversely, suppose that ϵ fails to be a homomorphism and write H for the subgroup of $G/G^2 \times \{\pm 1\}$ generated by S. By assumption, we may find σ and τ in G with $\epsilon(\sigma\tau) = -\epsilon(\sigma)\epsilon(\tau)$. Then

$$(\bar{\sigma}, \epsilon(\sigma)) \cdot (\bar{\tau}, \epsilon(\tau)) \cdot (\overline{\sigma\tau}, \epsilon(\sigma\tau)) = \left(\overline{(\sigma\tau)^2}, -1\right) = (1, -1)$$

is in H (here the first 1 denotes the identity in G/G^2). Then for any $\sigma \in G$, both $(\bar{\sigma}, \epsilon(\sigma))$ and

$$(\bar{\sigma}, -\epsilon(\sigma)) = (1, -1) \cdot (\bar{\sigma}, \epsilon(\sigma))$$

are in H. Thus $H = G/G^2 \times \{\pm 1\}$ and θ is surjective. □

Proof of Theorem 9.4 (i). By Remark 9.12 we see that Theorem 9.4 (i) holds if and only if θ is surjective whenever ϵ fails to be a homomorphism. The result now follows from Proposition 9.14. □

9.2. **The case where $p > 2$ and ϵ is non-trivial when restricted to $\mathbf{Gal}(K(T)/K(\boldsymbol{\mu}_p))$.** Suppose now that $p > 2$ and that the restriction of ϵ to $\mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$ is non-trivial.

We begin by defining a slight refinement of the quantity $t_X(\eta)$.

Definition 9.15. Fix an enumeration of the primes $\mathfrak{p} \notin \Sigma$ such that if $i \leq j$ then $N(\mathfrak{p}_i) \leq N(\mathfrak{p}_j)$, and for each $n \geq 1$ define the subgroup $\mathcal{C}_n(K)$ of $\mathcal{C}(K)$ by

$$\mathcal{C}_n(K) := \{\chi \in \mathcal{C}(K) \ : \ \chi \text{ is unramified outside } \Sigma \cup \{\mathfrak{p}_1, ..., \mathfrak{p}_n\}\}.$$

Further, for each $n \geq 1$ and $\eta \in \boldsymbol{\mu}_p^r$, define

$$\hat{t}_n(\eta) := \frac{|\{\chi \in \mathcal{C}_n(K) \ : \ f(\chi|_\Gamma) = \eta, \ w(\chi) = 1\}|}{|\{\chi \in \mathcal{C}_n(K) \ : \ f(\chi|_\Gamma) = \eta\}|} - \frac{1}{2}.$$

Remark 9.16. Note that we subtract $1/2$ in the definition of $\hat{t}_n(\eta)$ whilst we did not in the definition of $t_X(\eta)$. This will neaten the statement of some results in the rest of the section. Clearly for any $\eta \in \boldsymbol{\mu}_p^r$, to show that $\lim_{X\to\infty} t_X(\eta) = \frac{1}{2}$ it suffices to show that $\lim_{n\to\infty} \hat{t}_n(\eta) = 0$.

As in the case $p = 2$ we now fix a collection of global characters $\{\varphi(\mathfrak{p})\}_{\mathfrak{p}\notin\Sigma,\ \boldsymbol{\mu}_p \subseteq K_\mathfrak{p}}$ satisfying (8.11).

Lemma 9.17. *Fix $n \geq 1$. Then if $\boldsymbol{\mu}_p \subsetneq K_{\mathfrak{p}_{n+1}}$ we have $\mathcal{C}_{n+1}(K) = \mathcal{C}_n(K)$. On the other hand, if $\boldsymbol{\mu}_p \subseteq K_{\mathfrak{p}_{n+1}}$ then we have*

$$\mathcal{C}_{n+1}(K) = \bigsqcup_{i=0}^{p-1} \varphi(\mathfrak{p}_{n+1})^i \cdot \mathcal{C}_n(K).$$

Proof. In each case this follows from the structure of $\mathcal{C}(K_{\mathfrak{p}_{n+1}})$; see [KMR13, Lemma 8.3]. □

Definition 9.18. Let V be the regular representation of $\boldsymbol{\mu}_p^r$ over $\mathbb{C}$, so that V has basis $\{e_\eta \ : \ \eta \in \boldsymbol{\mu}_p^r\}$ on which $\boldsymbol{\mu}_p^r$ acts via $\eta' \cdot e_\eta = e_{\eta'\eta}$. For each $n \geq 1$ define

$$\hat{\mathbf{t}}_n := \sum_{\eta \in \boldsymbol{\mu}_p^r} \hat{t}_n(\eta) e_\eta \in V.$$

Further, for $\sigma \in \mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$, define $\rho(\sigma) := (\phi_i(\sigma))_{i=1}^r \in \boldsymbol{\mu}_p^r$ and

$$M(\sigma) := \frac{1}{p}\left(1 + \epsilon(\sigma) \sum_{i=1}^{p-1} \rho(\sigma)^i\right) \in \mathrm{End}(V).$$

Remark 9.19. For $\sigma \in \mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$ the element $M(\sigma)$ depends only on the conjugacy class of σ in G. Indeed, for each $1 \leq i \leq r$ and $g \in G$, the cocycle relation for ϕ_i gives $\phi_i(g\sigma g^{-1}) = g\phi_i(\sigma)$. It now follows that for each i, $\sum_{j=1}^{p-1} \phi_i(\sigma)^j$ depends only on the conjugacy class of σ in G. Since the same is true for $\epsilon(\sigma)$ we are done.

Lemma 9.20. *Fix $n \geq 1$. If $\boldsymbol{\mu}_p \subsetneq K_{\mathfrak{p}_{n+1}}$ then we have $\hat{\mathbf{t}}_{n+1} = \hat{\mathbf{t}}_n$. On the other hand, if $\boldsymbol{\mu}_p \subseteq K_{\mathfrak{p}_{n+1}}$ then we have the following recurrence relation for $\hat{\mathbf{t}}_n$:*

$$\hat{\mathbf{t}}_{n+1} = M(\mathrm{Frob}_{\mathfrak{p}_{n+1}})\hat{\mathbf{t}}_n,$$

where here $\mathrm{Frob}_{\mathfrak{p}_{n+1}} \in G$ denotes the Frobenius element at $\mathfrak{p}_{n+1}$ in $K(T)/K$.

Proof. If $\boldsymbol{\mu}_p \subsetneq K_{\mathfrak{p}_{n+1}}$ then $\mathcal{C}_{n+1}(K) = \mathcal{C}_n(K)$ and the result is clear.

Suppose now that $\boldsymbol{\mu}_p \subseteq K_{\mathfrak{p}_{n+1}}$ and define the map $\theta : \mathcal{C}(K) \to \boldsymbol{\mu}_p^r \times \{\pm 1\}$ by

$$\theta(\chi) := (f(\chi|_\Gamma), w(\chi))$$

(note that, unlike the case $p = 2$ this is not a homomorphism). Then Lemma 8.12 gives

$$\theta(\varphi(\mathfrak{p}_n)) = (\rho(\mathrm{Frob}_{\mathfrak{p}_n}), \epsilon(\mathrm{Frob}_{\mathfrak{p}_n}))\,.$$

Moreover, if $\chi_0 \in \mathcal{C}_n(K)$ then we have

$$\theta(\chi_0 \cdot \varphi(\mathfrak{p}_{n+1})^i) = \theta(\chi_0) \cdot \theta(\varphi(\mathfrak{p}_{n+1})^i)$$

since the sets of primes not in Σ at which χ_0 and $\varphi(\mathfrak{p}_{n+1})^i$ ramify are disjoint. Writing σ for $\mathrm{Frob}_{\mathfrak{p}_{n+1}}$, this gives

$$\theta(\chi_0 \cdot \varphi(\mathfrak{p}_{n+1})^i) = \begin{cases} \theta(\chi_0) & i = 0 \\ \theta(\chi_0) \cdot \left(\rho(\sigma)^i, \epsilon(\sigma)\right) & 1 \leq i \leq p-1. \end{cases}$$

It now follows from Lemma 9.17 that for each $\eta \in \boldsymbol{\mu}_p^r$ we have

$$\begin{aligned} |\{\chi \in \mathcal{C}_{n+1}(K) \ : \ \theta(\chi) = (\eta, 1)\}| \ &= \ \sum_{i=0}^{p-1} \left|\{\chi \in \varphi(\mathfrak{p}_{n+1})^i \cdot \mathcal{C}_n(K) \ : \ \theta(\chi) = (\eta, 1)\}\right| \\ &= |\{\chi_0 \in \mathcal{C}_n(K) \ : \ \theta(\chi_0) = (\eta, 1)\}| \\ &+ \sum_{i=1}^{p-1} \left|\left\{\chi_0 \in \mathcal{C}_n(K) \ : \ \theta(\chi_0) = \left(\eta \cdot \rho(\sigma)^{-i}, \epsilon(\sigma)\right)\right\}\right|. \end{aligned}$$

Dividing through by $|\mathcal{C}_{n+1}(K)| = p|\mathcal{C}_n(K)|$ gives

$$\hat{t}_{n+1}(\eta) = \frac{1}{p}\left(\hat{t}_n(\eta) + \epsilon(\sigma) \sum_{i=1}^{p-1} \hat{t}_n\left(\rho(\sigma)^{-i} \cdot \eta\right)\right)$$

and the result now follows from the definition of $M(\sigma)$. □

Lemma 9.21. *For any $m \geq 1$ and $\sigma \in \mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$ we have*

$$M(\sigma)^m = \begin{cases} M(\sigma) & \epsilon(\sigma) = 1, \\ \left(\frac{2}{p}\left(\frac{2-p}{p}\right)^m - \frac{2-p}{p}\left(\frac{2}{p}\right)^m\right)\mathrm{id}_V + \left(\left(\frac{2}{p}\right)^m - \left(\frac{2-p}{p}\right)^m\right) M(\sigma) & \epsilon(\sigma) = -1. \end{cases}$$

In particular, for $p > 2$ and writing $||\cdot||$ for the operator norm on $\mathrm{End}(V)$, we have

$$\lim_{m\to\infty} ||M(\sigma)^m|| = \begin{cases} ||M(\sigma)|| & \epsilon(\sigma) = 1, \\ 0 & \epsilon(\sigma) = -1. \end{cases}$$

Proof. Fix $\sigma \in \mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$ and define

$$T(\sigma) := \frac{1}{p}\sum_{i=0}^{p-1} \rho(\sigma)^i.$$

Then $T(\sigma)$ is an idempotent in $\mathrm{End}(V)$ (e.g. by orthogonality of characters of $\boldsymbol{\mu}_p$ or by explicit computation) so that $T(\sigma)^m = T(\sigma)$ for each $m \geq 1$. Note that we have

$$M(\sigma) = \begin{cases} T(\sigma) & \epsilon(\sigma) = 1 \\ \frac{2}{p} - T(\sigma) & \epsilon(\sigma) = -1. \end{cases}$$

If $\epsilon(\sigma) = 1$ this immediately gives $M(\sigma)^m = M(\sigma)$, whilst if $\epsilon(\sigma) = -1$ the result now follows easily either by induction on m or by expanding $(\frac{2}{p} - T(\sigma))^m$ with the binomial theorem.

Since $p > 2$ we have both

$$\lim_{m\to\infty} \left(\frac{2}{p}\right)^m = 0 \quad \text{and} \quad \lim_{m\to\infty} \left(\frac{2-p}{p}\right)^m = 0,$$

from which the statement about $\lim_{m\to\infty} ||M(\sigma)^m||$ follows immediately. □

Proposition 9.22. *Suppose that $p > 2$ and ϵ is non-trivial when restricted to $\mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$. Then for each $\eta \in \boldsymbol{\mu}_p^r$ we have*

$$\lim_{n\to\infty} \hat{t}_n(\eta) = 0.$$

Proof. Write $H := \mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$, and note that this is a normal subgroup of G. For each $n \geq 1$ we have $\boldsymbol{\mu}_p \subseteq K_{\mathfrak{p}_n}$ if and only if $\mathrm{Frob}_{\mathfrak{p}_n} \in H$. By Lemma 9.20, for each $n \geq 1$ we have

$$\hat{\mathbf{t}}_n = \left(\prod_{\substack{i=2 \\ \mathrm{Frob}_{\mathfrak{p}_i} \in H}}^{n} M(\mathrm{Frob}_{\mathfrak{p}_i}) \right) \hat{\mathbf{t}}_1. \tag{9.23}$$

Write $C_1, ..., C_l$ for the conjugacy classes in G that are contained in H and, for each i, fix a representative σ_i for C_i. Further, for each $1 \leq i \leq l$, define

$$m_i(n) := |\{2 \leq j \leq n \ : \ \mathrm{Frob}_{\mathfrak{p}_j} \in C_i\}|.$$

Since the group ring $\mathbb{C}[\boldsymbol{\mu}_p^r]$ is commutative, the matrices $M(\sigma_i)$ all mutually commute and we may group like terms in (9.23) to obtain (cf. Remark 9.19)

$$\hat{\mathbf{t}}_n = \left(\prod_{i=1}^{l} M(\sigma_i)^{m_i(n)} \right) \hat{\mathbf{t}}_1.$$

Writing $||\cdot||$ for the usual Euclidean norm on V (with respect to the basis $\{e_\eta : \eta \in \boldsymbol{\mu}_p^r\}$), we have

$$||\hat{\mathbf{t}}_n|| = \left\| \left(\prod_{i=1}^{l} M(\sigma_i)^{m_i(n)} \right) \hat{\mathbf{t}}_1 \right\| \leq \left(\prod_{i=1}^{l} \|M(\sigma_i)\|^{m_i(n)} \right) ||\hat{\mathbf{t}}_1||.$$

By the Chebotarev density theorem each of the $m_i(n)$ tend to infinity with n and, since we have assumed there is at least one i with $\epsilon(\sigma_i) = -1$, it follows from Lemma 9.21 that

$$\lim_{n\to\infty} ||\hat{\mathbf{t}}_n|| = 0.$$

That is, $\lim_{n\to\infty} \hat{t}_n(\eta) = 0$ for each $\eta \in \boldsymbol{\mu}_p^r$. □

Proof of Theorem 9.4 (ii). Fix $\gamma \in \Gamma$ and write $\eta = f(\gamma)$. Then by Lemma 9.9, for all X sufficiently large we have $s_X(\gamma) = t_X(\eta)$. It follows from Proposition 9.22 that $\lim_{X\to\infty} t_X(\eta) = \frac{1}{2}$, from which the result follows. □

10. Twisting data for abelian varieties ($p = 2$)

In this section let K be a number field and $(A/K, \lambda)$ a principally polarised abelian variety. In the notation of §6-§9 we take $p = 2$ and $T = A[2]$ endowed with the Weil pairing $(\ ,\ )_\lambda$. Let Σ be a finite set of places of K containing all archimedean places, all places dividing 2, and all places at which A has bad reduction. Then T is unramified outside Σ.

We now endow T with a global metabolic structure and twisting data in such a way that for $\chi \in \mathcal{C}(K)$ the associated Selmer group $\mathrm{Sel}(A[2], \chi)$ agrees with the 2-Selmer group $\mathrm{Sel}_2(A^\chi/K)$ of the quadratic twist of A by χ. For elliptic curves this is done in [KMR13, §5]. Our definition of the global metabolic structure and twisting data will be a direct generalisation of theirs. The main difficulty is establishing Lemma 10.6 which for elliptic curves is [KMR13, Lemma 5.2 (ii)] and for Jacobians of odd degree hyperelliptic curves is [Yu16, Theorem 5.10]. We will deduce the general case from the results of §4.5 concerning the behaviour of certain Theta groups under quadratic twist.

10.1. **A global metabolic structure on $A[2]$.** For a place v of K write

$$\delta_v : A(K_v)/2A(K_v) \hookrightarrow H^1(K_v, A[2])$$

for the connecting homomorphism in the multiplication-by-2 Kummer sequence.

Definition 10.1. Let $\mathcal{P}$ denote the Poincare line bundle on $A \times A^\vee$. For each place v of K write $\mathcal{L}_v$ for the pull back of $\mathcal{L} = (1, \lambda)^*\mathcal{P}$ to a line bundle on A/K_v and let $\mathscr{G}(\mathcal{L}_v)$ denote the associated Theta group. Then we define $q_{A,\lambda,v}$ to be the map

$$q_{A,\lambda,v} : H^1(K_v, A[2]) \longrightarrow H^2(K_v, \bar{K}_v^\times) = \mathrm{Br}(K_v) \xrightarrow{\mathrm{inv}_v} \mathbb{Q}/\mathbb{Z}$$

where the first map is the connecting map associated to the short exact sequence of G_{K_v}-modules

$$0 \to \bar{K}_v^\times \longrightarrow \mathscr{G}(\mathcal{L}_v) \longrightarrow A[2] \to 0 \tag{10.2}$$

of Remark 4.14.

Lemma 10.3. *Let v be a place of K. Then*

(i) *$q_{A,\lambda,v}$ is a quadratic form on $H^1(K_v, A[2])$ whose associated bilinear pairing is the local Tate pairing corresponding to $(\ ,\ )_\lambda$,*
(ii) *the image of $A(K_v)/2A(K_v)$ under δ_v is a Lagrangian subspace of $H^1(K_v, A[2])$ with respect to $q_{A,\lambda,v}$.*

In particular, $q_{A,\lambda,v}$ is a Tate quadratic form on $H^1(K_v, A[2])$ in the sense of Definition 6.1.

Proof. Part (i) is [PR12, Corollary 4.7] whilst Proposition 4.9 of op. cit. gives (ii). □

Remark 10.4. In contrast to the case of elliptic curves the quadratic form $q_{A,\lambda,v}$ in general takes values in $\frac{1}{4}\mathbb{Z}/\mathbb{Z}$ rather than just $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$, which is the reason for allowing $\mathbb{Q}/\mathbb{Z}$-valued quadratic forms in Definition 6.1 rather than just those valued in $\mathbb{F}_2$. See [PR12, Remark 4.16] for an example of this phenomenon.

Corollary 10.5. *The collection $\mathbf{q} = (q_{A,\lambda,v})_v$ defines a global metabolic structure on $A[2]$.*

Proof. By Lemma 10.3 (ii) $q_{A,\lambda,v}$ admits a Lagrangian subspace making $\big(H^1(K_v, T), q_{A,\lambda,v}\big)$ into a metabolic space for each place v of K. Moreover, if $v \notin \Sigma$ then $\mathrm{im}(\delta_v) = H^1_{\mathrm{ur}}(K_v, A[2])$ (see e.g. [PR12, Proposition 4.12] and the preceeding remark). In particular, by Lemma 10.3 (ii), $q_{A,\lambda,v}$ is unramified at each such place.

Finally, let $\mathfrak{a} \in H^1(K, A[2])$. Write

$$q : H^1(K, A[2]) \to H^2(K, \bar{K}^\times) = \mathrm{Br}(K)$$

for the connecting homomorphism associated to the sequence (10.2) viewed over K instead of K_v (with $\mathcal{L}_v$ replaced by $\mathcal{L} := (1, \lambda)^*\mathcal{P}$). Then $q(\mathfrak{a}) \in \mathrm{Br}(K)$ and we have

$$\sum_{v \in M_K} q_v(\mathfrak{a}_v) = \sum_{v \in M_K} \mathrm{inv}_v q(\mathfrak{a}) = 0,$$

the last equality following from reciprocity for the Brauer group of K. □

10.2. **Twisting data associated to A/K.** We now define the twisting data $\boldsymbol{\alpha}$.

Fix a place v of K and $\chi \in \mathcal{C}(K_v)$, and let (A^χ, ψ) denote the quadratic twist of A by χ. By Lemma 4.16 $\lambda_\chi := (\psi^\vee)^{-1}\lambda\psi^{-1}$ is a principal polarisation on A^χ, defined over K_v. In particular, associated to the pair (A^χ, λ_χ) we have a quadratic form $q_{A^\chi,\lambda_\chi,v}$ on $H^1(K_v, A^\chi[2])$.

Lemma 10.6. *The isomorphism $H^1(K_v, A^\chi[2]) \cong H^1(K_v, A[2])$ induced by ψ identifies the quadratic forms $q_{A,\lambda,v}$ and $q_{A^\chi,\lambda_\chi,v}$.*

Proof. Take the long exact sequences for Galois cohomology associated to the commutative diagram of Lemma 4.20. □

Definition 10.7. For $\chi \in \mathcal{C}(K_v)$ define $\alpha_v(\chi) \subseteq H^1(K_v, A[2])$ to be the image of the map

$$A^\chi(K_v)/2A^\chi(K_v) \hookrightarrow H^1(K_v, A^\chi[2]) \xrightarrow{\sim} H^1(K_v, A[2])$$

the first map arising from the multiplication-by-2 Kummer sequence for A^χ and the latter being induced by ψ^{-1}. Note that by combining Lemma 10.6 with Lemma 10.3 (ii) applied to A^χ/K_v we see that $\alpha_v(\chi)$ is a Lagrangian subspace of $H^1(K_v, A[2])$.

As in Definition 6.11, for χ_1 and χ_2 elements of $\mathcal{C}(K_v)$ we set

$$h_v(\chi_1, \chi_2) = \dim_{\mathbb{F}_p} \left(\alpha_v(\chi_1)/(\alpha_v(\chi_1) \cap \alpha_v(\chi_2))\right).$$

Lemma 10.8. *For each quadratic character $\chi \in \mathcal{C}(K_v)$, let L_χ denote the extension of K_v cut out by χ. Then*

$$h_v(\mathbb{1}, \chi_v) = \dim_{\mathbb{F}_2} A(K_v)/N_{L_\chi/K_v}A(L_\chi)$$

where here $N_{L_\chi/K_v} : A(L_\chi) \to A(K_v)$ is the 'local norm map' sending $P \in A(L_\chi)$ to

$$N_{L_\chi/K_v}(P) := \sum_{\sigma \in \mathrm{Gal}(L_\chi/K_v)} \sigma(P).$$

Proof. This is shown in [MR07, Proposition 5.2]. Whilst loc. cit. is stated for the case of elliptic curves and for twists by characters of order $p > 2$, the proof carries over unchanged to our case. See also [Kra81, Proposition 7]. □

The following Lemma evaluates the cokernel of the local norm map in certain cases.

Lemma 10.9. *Let v be a place of K and $\chi \in \mathcal{C}(K_v)$. As above, let L_χ denote the extension of K_v cut out by χ.*

(i) *Suppose $v \nmid 2$ is nonarchimedean and that A has good reduction at v. If χ is unramified then*

$$\dim_{\mathbb{F}_2} A(K_v)/N_{L_\chi/K_v}A(L_\chi) = 0.$$

On the other hand, if χ is ramified then $N_{L_\chi/K_v}A(L_\chi) = 2A(K_v)$ and, in particular, we have

$$\dim_{\mathbb{F}_2} A(K_v)/N_{L_\chi/K_v}A(L_\chi) = \dim_{\mathbb{F}_2} A(K_v)[2].$$

(ii) *Suppose v is archimedean and χ non-trivial. Then*

$$\dim_{\mathbb{F}_2} A(K_v)/N_{L_\chi/K_v}A(L_\chi) = \dim_{\mathbb{F}_2} A(K_v)[2] - g$$

where $g = \dim A$ is the dimension of A.

Proof. (i). The case where χ is unramified is a result of Mazur [Maz72, Corollary 4.4]. For χ ramified the case where A is an elliptic curve is [MR07, Lemma 5.5 (ii)] and the argument for general abelian varieties is identical.

(ii). By assumption L_χ/K_v is the extension $\mathbb{C}/\mathbb{R}$. Since A/K_v is an abelian variety of dimension g over the reals we have an isomorphism of real Lie groups

$$A(K_v) \cong (\mathbb{R}/\mathbb{Z})^g \times (\mathbb{Z}/2\mathbb{Z})^m \tag{10.10}$$

for some $0 \leq m \leq g$ (see, for example, [Sil89, Proposition 1.9 and Remark 1.12]). Now N_{L_χ/K_v} is a continuous map from the connected group $A(L_\chi)$ to $A(K_v)$ (for the complex and real topologies respectively) and it follows that the image of N_{L_χ/K_v} is contained in the connected component of the identity in $A(K_v)$, which we denote $A^0(K_v)$. Under the isomorphism (10.10), $A^0(K_v)$ is the factor corresponding to $(\mathbb{R}/\mathbb{Z})^g$. On the other hand, we have $2A(K_v) \subseteq N_{L_\chi/K_v}A(L_\chi)$ and we see again from (10.10) that multiplication by 2 is surjective on $A^0(K_v)$. Thus $N_{L_\chi/K_v}A(L_\chi) = A^0(K_v)$. Appealing to (10.10) one last time we obtain $|A(K_v)/N_{L_\chi/K_v}A(L_\chi)| = 2^{-g}|A(K_v)[2]|$. □

Proposition 10.11. *The collection of maps $\boldsymbol{\alpha} = (\alpha_v)_v$ defines twisting data with respect to $(A[2], \boldsymbol{q}, \Sigma)$. Moreover, we have*

$$\mathrm{Sel}(A[2], \chi) \cong \mathrm{Sel}_2(A^\chi/K)$$

where $\mathrm{Sel}(A[2], \chi)$ is defined with respect to $(A[2], \boldsymbol{q}, \Sigma, \boldsymbol{\alpha})$ as in Definition 6.10.

Proof. Note that since $p = 2$ the group $\mathcal{F}(K_v)$ appearing in the definition of twisting data (Definition 6.8) is equal to $\mathcal{C}(K_v)$. For each place v of K and $\chi_v \in \mathcal{C}(K_v)$, the subspace $\alpha_v(\chi_v)$ of $H^1(K_v, A[2])$ is Lagrangian by Lemma 10.6 and Lemma 10.3 (ii) applied to A^χ/K_v. Moreover, if $v \notin \Sigma$ and χ_v is ramified then $\alpha_v(\chi_v)$ is an element of $\mathcal{H}_{\mathrm{ram}}(q_v)$. Indeed, by definition we need to show that $\alpha_v(\chi_v) \cap H^1_{\mathrm{ur}}(K_v, A[2]) = 0$. As before, as $v \notin \Sigma$ we have

$$H^1_{\mathrm{ur}}(K_v, A[2]) = \delta_v(A(K_v)/2A(K_v)) = \alpha_v(\mathbb{1}_v).$$

Combining Lemma 10.8 with Lemma 10.9 gives

$$\dim_{\mathbb{F}_2} (\alpha(\mathbb{1}_v)/\alpha_v(\chi_v) \cap \alpha_v(\mathbb{1}_v)) = \dim_{\mathbb{F}_2} A(K_v)/2A(K_v) = \dim_{\mathbb{F}_2} \alpha(\mathbb{1}_v)$$

whence $\alpha_v(\chi_v) \cap \alpha_v(\mathbb{1}_v) = 0$ as desired. Thus $\boldsymbol{\alpha}$ defines twisting data.

Finally, we will show that for $\chi \in \mathcal{C}(K)$ the associated Selmer group $\mathrm{Sel}(A[2], \chi)$ agrees with the classical Selmer group $\mathrm{Sel}_2(A^\chi/K)$. By the definition of $\mathrm{Sel}_2(A^\chi/K)$ and the maps α_v we have

$$\mathrm{Sel}_2(A^\chi/K) = \{\mathfrak{a} \in H^1(K, A[2]) \ : \ \mathfrak{a}_v \in \alpha_v(\chi_v) \text{ for all } v \in M_K\}.$$

On the other hand, we have

$$\mathrm{Sel}(A[2], \chi) = \{\mathfrak{a} \in H^1(K, A[2]) \ : \ \mathfrak{a}_v \in H^1_{\mathcal{S}(\chi)}(K_v, A[2]) \text{ for all } v \in M_K\}$$

where, as in Definition 6.10, $H^1_{\mathcal{S}(\chi)}(K_v, A[2]) = \alpha(\chi_v)$ if $v \in \Sigma$ or χ_v is ramified at v, and is equal to $H^1_{\mathrm{ur}}(K_v, A[2])$ otherwise.

In particular, to show that $\mathrm{Sel}(A[2], \chi) = \mathrm{Sel}_2(A^\chi/K)$ it suffices to show that $\alpha(\chi_v) = H^1_{\mathrm{ur}}(K_v, A[2])$ whenever $v \notin \Sigma$ and χ_v is unramified. But for such places we have $\alpha(\mathbb{1}_v) = H^1_{\mathrm{ur}}(K_v, A[2])$ and since χ_v is unramified Lemma 10.9 (i) gives $h(\mathbb{1}_v, \chi_v) = 0$. It now follows immediately that $\alpha(\chi_v) = H^1_{\mathrm{ur}}(K_v, A[2])$ as desired. □

10.3. **Main theorems for 2-Selmer ranks.** Having interpreted the groups $\mathrm{Sel}_2(A^\chi/K)$ as those arising from twisting data we apply the results of the previous sections to deduce results about abelian varieties.

The following generalises a theorem of Kramer [Kra81, Theorem 1] for elliptic curves and Yu [Yu16, Theorem 5.11] for odd degree hyperelliptic curves.

Theorem 10.12. *Let K be a number field, χ a quadratic character of K corresponding to the extension L/K, and A/K a principally polarised abelian variety. Then*

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(A^\chi/K) \equiv \dim_{\mathbb{F}_2} \mathrm{Sel}_2(A/K) + \sum_{v \in M_K} \dim_{\mathbb{F}_2} A(K_v)/N_{L_w/K_v} A(L_w) \pmod 2$$

(here w denotes any place of L extending v).

Proof. Combine Theorem 6.12, Proposition 10.11 and Lemma 10.8. □

Theorem 10.13 (Theorem 1.1)**.** *Let K be a number field, A/K a principally polarised abelian variety, and Σ the set consisting of all archimedean places of K, all places of bad reduction for A, and all places dividing 2. Define $\epsilon : \mathrm{Gal}(K(A[2])/K) \to \{\pm 1\}$ by $\sigma \mapsto (-1)^{\dim_{\mathbb{F}_2} A[2]^\sigma}$.*

(i) *If ϵ fails to be a homomorphism then for all sufficiently large X*

$$\frac{|\{\chi \in \mathcal{C}(K, X) \ : \ \dim_{\mathbb{F}_2} \mathrm{Sel}_2(A^\chi/K) \text{ is even}\}|}{|\mathcal{C}(K, X)|} = 1/2.$$

(ii) *If ϵ is a homomorphism, let $K(\sqrt{\Delta})/K$ be the fixed field of the kernel of ϵ. For each $v \in \Sigma$ and quadratic character $\chi \in \mathcal{C}(K_v)$ write L_χ/K_v for the extension cut out by χ and define*

$$\omega_v(\chi) := \chi(\Delta)(-1)^{\dim_{\mathbb{F}_2} A(L_\chi)/N_{L_\chi/K_v} A(L_\chi)}.$$

Finally, define

$$\delta_v := \frac{1}{|\mathcal{C}(K_v)|} \sum_{\chi \in \mathcal{C}(K_v)} \omega(\chi) \qquad \text{and} \qquad \delta := \prod_{v \in \Sigma} \delta_v.$$

Then for all sufficiently large X,

$$\frac{|\{\chi \in \mathcal{C}(K, X) \ : \ \dim_{\mathbb{F}_2} \mathrm{Sel}_2(A^\chi/K) \text{ is even}\}|}{|\mathcal{C}(K, X)|} = \frac{1 + (-1)^{\dim_{\mathbb{F}_2} \mathrm{Sel}_2(A/K)} \cdot \delta}{2}.$$

Proof. Combine Proposition 10.11, Theorem 7.4 and Lemma 10.8. □

Remark 10.14. Lemma 10.9 (ii) enables one to evaluate the local terms δ_v for archimedean places. For nonarchimedean places of odd residue characteristic, the dimension of the cokernel of the norm map may be expressed in terms of Tamagawa numbers: see [Mor15, Lemma 2.5].

In the following examples we examine when ϵ is (resp. is not) a homomorphism for certain families of abelian varieties.

Example 10.15 (Generic 2-torsion)**.** For any principally polarised abelian variety A/K of dimension g, $\mathrm{Gal}(K(A[2])/K)$ is a subgroup of the symplectic group $\mathrm{Sp}_{2g}(\mathbb{F}_2)$. As in Remark 7.5, if $g \geq 2$ and $\mathrm{Gal}(K(A[2])/K) \cong \mathrm{Sp}_{2g}(\mathbb{F}_2)$ then ϵ is not a homomorphism.

Example 10.16 (Elliptic curves)**.** Suppose that A/K is an elliptic curve, say given by a Weierstrass equation of the form $y^2 = f(x)$ for some monic (separable) cubic polynomial $f(x)$. Then $\mathrm{Gal}(K(A[2])/K) = \mathrm{Gal}(f)$ is the Galois group of the splitting field of $f(x)$ and as such may be viewed as a subgroup of the symmetric group S_3. One readily checks that the map $\sigma \mapsto (-1)^{\dim_{\mathbb{F}_2} A[2]^\sigma}$ is the sign homomorphism. Thus ϵ is always a homomorphism and we may take Δ to be the discriminant of the elliptic curve. Thus Theorem 10.13 recovers [KMR13, Theorem A]. See Proposition 7.9 of op. cit. for a table computing the local terms δ_v as a function of the reduction of the elliptic curve.

Example 10.17 (Hyperelliptic curves)**.** Let C/K be a hyperelliptic curve of genus $g \geq 2$, say given by a Weierstrass equation $y^2 = f(x)$ for a (separable, not necessarily monic) polynomial $f(x)$ with $\deg(f) \in \{2g+1, 2g+2\}$. Take A/K to be the Jacobian of C so that A/K is a principally polarised abelian variety of dimension g. Then again $\mathrm{Gal}(K(A[2])/K) = \mathrm{Gal}(f)$ which we view as a subgroup of the symmetric group $S_{\deg(f)}$. Write $\mathrm{sgn} : \mathrm{S}_n \to \{\pm 1\}$ for the sign homomorphism and fix $\sigma \in \mathrm{Gal}(f)$ with cycle type $(d_1 \ ... \ d_s)$. Then we have

$$\epsilon(\sigma) = \begin{cases} -\mathrm{sgn}(\sigma) & \text{all } d_i \text{ even and } \deg(f) \equiv 2 \pmod 4, \\ \mathrm{sgn}(\sigma) & \text{else.} \end{cases} \tag{10.18}$$

Indeed, this follows from [Cor01, Theorem 1.4] (whilst loc. cit. is stated for hyperelliptic curves over finite fields of odd residue characteristic, the proof yields the above statement for all fields of characteristic not 2; note also the erratum [Cor05]).

Suppose now that either g is odd or $\deg(f)$ is odd. Then by (10.18) ϵ is always a homomorphism and again we may take Δ to be the discriminant of the hyperelliptic curve C. In particular, the case $\deg(f)$ odd recovers [Yu16, Theorem 1].

Now suppose that both g and $\deg(f)$ are even, or equivalently $\deg(f) \equiv 2 \pmod 4$. Suppose further that either $\mathrm{Gal}(f) \cong S_{2g+2}$ or $\mathrm{Gal}(f) \cong A_{2g+2}$. Then by (10.18) we see that ϵ is not a homomorphism (indeed, the only non-trivial homomorphism from S_{2g+2} to $\{\pm 1\}$ is sgn yet (10.18) shows that ϵ is non-trivial when restricted to A_{2g+2}).

Example 10.19 (Abelian varieties with principal polarisation induced by a rational symmetric line bundle)**.** Suppose that $(A/K, \lambda)$ is a principally polarised abelian variety and that the polarisation λ is induced by a rational (i.e. G_K-invariant) symmetric line bundle $\mathcal{L}$. Then the associated quadratic refinement $q_{\mathcal{L}}$ of the Weil-pairing $(\ ,\ )_\lambda$ on $A[2]$ (as in Definition 4.3) is G_K-invariant also, whence $\mathrm{Gal}(K(A[2])/K)$ acts on $A[2]$ through the orthogonal group $O(q_{\mathcal{L}})$. Then ϵ is the Dickson homomorphism $d_{q_{\mathcal{L}}}$ (Proposition 3.5). We remark that this case includes both elliptic curves and Jacobians of hyperelliptic curves of either odd degree or odd genus: see [PR11, Proposition 3.11].

10.4. **Main theorems for 2^∞-Selmer ranks.** We now incorporate the results of §5 to move from 2-Selmer ranks to 2^∞-Selmer ranks.

Theorem 10.20. *Let K be a number field and $(A/K, \lambda)$ a principally polarised abelian variety. Let Σ be the set consisting of all archimedean places of K, all places of bad reduction for A, and all places dividing 2, and let L/K be a quadratic extension with associated quadratic character χ. Then*

$$\mathrm{rk}_2(A/L) \equiv \sum_{\substack{v\in\Sigma \\ v \text{ non-split in } L/K}} \left(2\ \mathrm{inv}_v\ \mathfrak{g}(A/K_v,\lambda_v,\chi_v) + \dim_{\mathbb{F}_2} A(K_v)/N_{L_w/K_v}A(L_w)\right) \pmod 2$$

where the local terms[2] $\mathfrak{g}(A/K_v,\lambda_v,\chi_v)\in \mathrm{Br}(K_v)[2]$ *are given in Definition 5.15, and* w *denotes any place of* L *extending* v*.*

Proof. First note that $\mathrm{rk}_2(A/L) = \mathrm{rk}_2(A/K) + \mathrm{rk}_2(A^\chi/K)$. Moreover, we have

$$\dim_{\mathbb{F}_2}\mathrm{Sel}_2(A/K) = \mathrm{rk}_2(A/K) + \dim_{\mathbb{F}_2}A(K)[2] + \dim_{\mathbb{F}_2}Ш_{\mathrm{nd}}(A/K)[2]$$

and the analagous equality for A^χ/K. Noting that $\dim_{\mathbb{F}_2}A(K)[2] = \dim_{\mathbb{F}_2}A^\chi(K)[2]$ the above observations combine to give

$$\begin{aligned}\mathrm{rk}_2(A/L) \ \equiv\ & \dim_{\mathbb{F}_2}\mathrm{Sel}_2(A/K) + \dim_{\mathbb{F}_2}\mathrm{Sel}_2(A^\chi/K) \\ & + \dim_{\mathbb{F}_2}Ш_{\mathrm{nd}}(A/K)[2] + \dim_{\mathbb{F}_2}Ш_{\mathrm{nd}}(A^\chi/K)[2] \pmod 2.\end{aligned}$$

Combining Theorem 10.12 with Theorem 5.20 then gives

$$\mathrm{rk}_2(A/L) \equiv \sum_{v\in M_K} \left(2\ \mathrm{inv}_v\mathfrak{g}(A/K_v,\lambda_v,\chi_v) + \dim_{\mathbb{F}_2} A(K_v)/N_{L_w/K_v}A(L_w)\right) \pmod 2.$$

Finally, combining Proposition 5.16 with Lemma 10.9 shows that

$$2\ \mathrm{inv}_v\mathfrak{g}(A/K_v,\lambda_v,\chi_v) + \dim_{\mathbb{F}_2} A(K_v)/N_{L_w/K_v}A(L_w) \equiv 0 \pmod 2$$

for each place $v\notin\Sigma$, and similarly for each place $v\in\Sigma$ which split in L/K. □

We now prove Theorem 1.2, after first defining the local terms appearing in the statement.

Definition 10.21. Let K be a number field, $(A/K,\lambda)$ a principally polarised abelian variety, and let Σ denote the set consisting of all archimedean places of K, all places of bad reduction for A, and all places dividing 2.

For each $v\in\Sigma$ and $\chi\in\mathcal{C}(K_v)$ define

$$\Omega_v(\chi) := (-1)^{2\ \mathrm{inv}_v\mathfrak{g}(A/K_v,\lambda_v,\chi)+\dim_{\mathbb{F}_2}A(K_v)/N_{L_\chi/K_v}A(L_\chi)}$$

where here L_χ is the extension of K_v cut out by χ. Further, we define (for each $v\in\Sigma$)

$$\kappa_v = \frac{1}{|\mathcal{C}(K_v)|}\sum_{\chi\in\mathcal{C}(K_v)}\Omega_v(\chi) \qquad \text{and} \qquad \kappa = \prod_{v\in\Sigma}\kappa_v.$$

Remark 10.22. If v is archimedean then by Theorem 10.20 we have

$$\Omega_v(\chi_v) = \begin{cases} 1 & \chi_v \text{ trivial} \\ (-1)^{\dim A} & \text{else.}\end{cases}$$

In particular, if v is a real place and $\dim A$ is odd then $\kappa_v = 0$ (hence also $\kappa = 0$), whilst if v is complex or $\dim A$ is even, we have $\kappa_v = 1$.

Theorem 10.23. *Let* A/K *be a principally polarised abelian variety. Then for all sufficiently large* $X > 0$*,*

$$\frac{|\{\chi\in\mathcal{C}(K,X)\ :\ \mathrm{rk}_2(A^\chi/K) \text{ is even}\}|}{|\mathcal{C}(K,X)|} = \frac{1+(-1)^{\mathrm{rk}_2(A/K)}\cdot\kappa}{2}.$$

[2]Here and in Definition 10.21 we think of $\mathrm{inv}_v\ \mathfrak{g}(A/K_v,\lambda_v,\chi_v)$ as being equal to 0 or 1/2 (as opposed to the class of this in $\mathbb{Q}/\mathbb{Z}$) so that $2\ \mathrm{inv}_v\ \mathfrak{g}(A/K_v,\lambda_v,\chi_v)$ is either 0 or 1 accordingly.

Proof. As noted previously, for any $\chi \in \mathcal{C}(K)$ corresponding to the quadratic extension L/K, we have

$$\mathrm{rk}_2(A/L) = \mathrm{rk}_2(A/K) + \mathrm{rk}_2(A^\chi/K).$$

Thus for each $\chi \in \mathcal{C}(K)$, Theorem 10.20 gives

$$(-1)^{\mathrm{rk}_2(A^\chi/K)} = (-1)^{\mathrm{rk}_2(A/K)} \prod_{v\in\Sigma} \Omega(\chi_v)$$

with $\Omega(\chi_v) \in \{\pm 1\}$ depending only on the restriction of χ to K_v. The argument is now identical to that in the proof of Theorem 7.10. As is the case there, 'sufficiently large $X > 0$' means that we require only that X is large enough that the restriction homomorphism from $\mathcal{C}(K, X)$ to $\prod_{v\in\Sigma} \mathcal{C}(K_v)$ is surjective. □

The following example shows that the proportion of twists having even 2-Selmer rank can differ from the proportion having even 2^∞-Selmer rank.

Example 10.24. Consider the genus 2 hyperelliptic curve $C : y^2 = x^6 + x^4 + x + 3$ over $\mathbb{Q}$. The polynomial $f(x) = x^6 + x^4 + x + 3$ has Galois group S_6. By Theorem 10.13 (see also Example 10.17) the 2-Selmer ranks are distributed 1/2-1/2 amongst even/odd in the quadratic twist family of the Jacobian J/K of C.

On the other hand, we claim that $\kappa = 3/16$ so that 19/32 of the twists of J have even 2^∞-Selmer rank whilst 13/32 have odd 2^∞-Selmer rank. The discriminant of $f(x)$ is $-5 \cdot 2670719$, so J/K has good reduction away from $2, 5$ and 2670719. Thus we have $\Sigma = \{2, 5, 2670719, \infty\}$. Using the computer algebra package MAGMA ([BCP97]), one computes that $\mathrm{rk}_2(J/K)$ is odd. By Remark 10.22, $\kappa_\infty = 1$. To compute κ_2, κ_5 and $\kappa_{2670719}$, one may use the following trick. By Theorem 10.20 and the above discussion, for a quadratic character χ of $\mathbb{Q}$ corresponding to the extension $L/\mathbb{Q}$, one has

$$(-1)^{\mathrm{rk}_2(J^\chi/\mathbb{Q})} = - \prod_{\substack{v\in\{2,5,2670719\} \\ v \text{ non-split in } L}} \Omega_v(\chi_v). \tag{10.25}$$

Now for $0 \neq n \in \mathbb{Z}$, the quadratic twist of J by $\mathbb{Q}(\sqrt{n})/\mathbb{Q}$ is the Jacobian of the hyperelliptic curve $y^2 = nf(x)$. Thus one may use MAGMA to compute $(-1)^{\mathrm{rk}_2(J^\chi/\mathbb{Q})}$ for various (finitely many) quadratic characters χ, from which one may then determine all the $\Omega_v(\chi_v)$ by (10.25). Upon doing this one obtains $\kappa_2 = 3/4, \kappa_5 = -1/2$ and $\kappa_{2670719} = 1/2$ and the claim follows.

Remark 10.26. Since by Theorem 10.20 the parity of $\mathrm{rk}_2(A^\chi/K)$ depends only on the restriction of χ to the archimedean places, the places of bad reduction for A, and the places over 2, it follows from Theorem 9.4 (i) (along with Proposition 10.11) that when ϵ fails to be a homomorphism we in fact have

$$\frac{|\{\chi \in \mathcal{C}(K, X) \ : \ \dim_{\mathbb{F}_2} \mathrm{Sel}_2(A^\chi/K) \text{ is even and } \mathrm{rk}_2(A^\chi/K) \text{ is even}\}|}{|\{\chi \in \mathcal{C}(K, X) \ : \ \mathrm{rk}_2(A^\chi/K) \text{ is even}\}|} = 1/2$$

for all sufficiently large X (assuming the denominator is non-zero) and that the same holds when we condition on $\mathrm{rk}_2(A^\chi/K)$ being odd also. Thus when ϵ fails to be a homomoprhism the parities of Selmer ranks and the parities of 2-infinity Selmer ranks behave 'independently'.

10.5. **The proportion of twists having non-square Shafarevich–Tate group.** We now prove an analogue of Theorem 1.1 for $\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A/K)[2]$ rather than for $\dim_{\mathbb{F}_2}\mathrm{Sel}_2(A/K)$. Since the Shafarevich–Tate group of a principally polarised abelian variety, if finite, has square order if and only if $\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A/K)[2]$ is even (see e.g. [PS99, Theorem 8]), this may be viewed as quantiftying the failure of the Shafarevich–Tate group to have square order in quadratic twist families. The proof of the theorem is identical to its analogue for 2-Selmer ranks, so we only sketch the proof.

Theorem 10.27. *Let K be a number field, $(A/K,\lambda)$ a principally polarised abelian variety, and Σ the set consisting of all archimedean places of K, all places of bad reduction for A, and all places dividing 2. Define $\epsilon : \mathrm{Gal}(K(A[2])/K) \to \{\pm 1\}$ by $\sigma \mapsto (-1)^{\dim_{\mathbb{F}_2} A[2]^\sigma}$.*

(i) *If ϵ fails to be a homomorphism then for all sufficiently large X*

$$\frac{|\{\chi \in \mathcal{C}(K,X) \ : \ \dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A^\chi/K)[2] \text{ is even}\}|}{|\mathcal{C}(K,X)|} = 1/2.$$

(ii) *If ϵ is a homomorphism, let $K(\sqrt{\Delta})/K$ be the fixed field of the kernel of ϵ. For each $v \in \Sigma$ and quadratic character $\chi \in \mathcal{C}(K_v)$ write L_χ/K_v for the extension cut out by χ and define*

$$\Upsilon_v(\chi) := \chi(\Delta)(-1)^{2\ \mathrm{inv}_v \mathfrak{g}(A/K_v,\lambda_v,\chi_v)}.$$

Finally, define

$$\rho_v := \frac{1}{|\mathcal{C}(K_v)|}\sum_{\chi\in\mathcal{C}(K_v)} \Upsilon(\chi) \qquad \text{and} \qquad \rho := \prod_{v\in\Sigma}\rho_v.$$

Then for all sufficiently large X,

$$\frac{|\{\chi \in \mathcal{C}(K,X) \ : \ \dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A^\chi/K)[2] \text{ is even}\}|}{|\mathcal{C}(K,X)|} = \frac{1+(-1)^{\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A/K)[2]}\cdot\rho}{2}.$$

Proof. Fix a quadratic character χ of K. As in Definition 9.1, set

$$w(\chi) := \prod_{v\notin\Sigma,\ \chi_v \text{ ram}} (-1)^{\dim_{\mathbb{F}_p} A(K_v)[2]} = \prod_{v\notin\Sigma,\ \chi_v \text{ ram}} \epsilon(\mathrm{Frob}_v).$$

Combining Theorem 5.20 with Proposition 5.16 we obtain

$$(-1)^{\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A^\chi/K)[2]} = w(\chi)(-1)^{\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A/K)[2]}\prod_{v\in\Sigma}(-1)^{2\ \mathrm{inv}_v\mathfrak{g}(A/K_v,\lambda_v,\chi_v)}. \tag{10.28}$$

If ϵ is a homomorphism then, as in the proof of Lemma 7.7, we have $w(\chi) = \prod_{v\in\Sigma}\chi_v(\Delta)$, whence

$$(-1)^{\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A^\chi/K)[2]} = (-1)^{\dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A/K)[2]}\prod_{v\in\Sigma}\Upsilon_v(\chi)$$

and the same argument as in the proof of Theorem 7.10 gives the result.

On the other hand, suppose that ϵ is a homomorphism and enlarge Σ if neccesary so that 8.8 holds, noting that (10.28) still remains true. The result now follows from Theorem 9.4 (cf. proof of Theorem 9.5). □

10.6. **The joint distribution of parities of 2-Selmer ranks and 2-infinity Selmer ranks.** By combining Theorem 10.27 with Theorems 10.13 and 10.23 we are able to push Remark 10.26 further to determine the 'joint distribution' of parities of 2-Selmer ranks and 2-infinity Selmer ranks.

Corollary 10.29 (of Theorem 10.27)**.** *Let K be a number field, A/K a principally polarised abelian variety, and $\epsilon : \mathrm{Gal}(K(A[2])/K) \to \{\pm 1\}$ the map $\sigma \mapsto (-1)^{\dim_{\mathbb{F}_2} A[2]^\sigma}$. Let the constants δ, κ and ρ be as in Theorem 10.13, Definition 10.21 and Theorem 10.27 respectively. Then for $m, n \in \{0,1\}$ we have, for all sufficiently large X,*

$$\frac{|\{\chi \in \mathcal{C}(K,X) \ : \ \mathrm{rk}_2(A^\chi/K) \ \equiv m \ (\mathrm{mod}\ 2),\ \dim_{\mathbb{F}_2}\mathrm{Sel}_2(A^\chi/K) \ \equiv n \ (\mathrm{mod}\ 2)\}|}{|\mathcal{C}(K,X)|}$$

$$= \frac{1}{4} + (-1)^m a_1 + (-1)^n a_2 + (-1)^{m+n} a_3$$

where

$$a_1 = \frac{1}{4}(-1)^{\mathrm{rk}_2(A/K)}\kappa,$$

and $a_2 = a_3 = 0$ if ϵ fails to be a homomorphism whilst

$$a_2 = \frac{1}{4}(-1)^{\dim_{\mathbb{F}_2}\mathrm{Sel}_2(A/K)}\delta \quad \text{and} \quad a_3 = \frac{1}{4}(-1)^{\dim_{\mathbb{F}_2}\mathrm{Sel}_2(A/K)+\mathrm{rk}_2(A/K)}\rho$$

otherwise.

Proof. Follows from Theorems 10.13, 10.23 and 10.27 upon noting that, for any $\chi \in \mathcal{C}(K)$, we have

$$\dim_{\mathbb{F}_2}\mathrm{Sel}_2(A^\chi/K) = \mathrm{rk}_2(A^\chi/K) + \dim_{\mathbb{F}_2} A(K)[2] + \dim_{\mathbb{F}_2} Ш_{\mathrm{nd}}(A^\chi/K)[2].$$

□

11. Twisting data for abelian varieties ($p > 2$)

As in the previous section, let K be a number field and $(A/K, \lambda)$ a principally polarised abelian variety. This time we take p to be an odd prime and $T = A[p]$. As with $A[2]$ in the previous section, we endow T with a canonical global metabolic structure and twisting data so that the resulting Selmer groups have a classical interpretation. For elliptic curves this is done by Klagsbrun–Mazur–Rubin in [KMR13, §5]. This time the case of an arbitrary principally polarised abelian variety is almost identical to that of loc. cit., though to fix notation we repeat the relevant material.

11.1. **The global metabolic structure on $A[p]$.** As with the case $p = 2$, the polarisation λ along with the Weil-pairing

$$(\ ,\ )_{e_p} : A[p] \times A^\vee[p]$$

provides the desired (non-degenerate, alternating, G_K-equivariant) bilinear pairing

$$(\ ,\ )_\lambda : T \times T \to \boldsymbol{\mu}_p$$

(defined by setting $(x,y)_\lambda = (x, \lambda(y))_{e_p}$ for $x, y \in T$). We take Σ to be a finite set of places of K containing all archimedean places, all primes over p, and all primes at which A has bad reduction. Then T is unramified outside Σ.

Since p is odd, the quadratic forms $q_v = \frac{1}{2}\langle\ ,\ \rangle_v$ (here v a place of K and $\langle\ ,\ \rangle_v$ denotes the local Tate pairing associated to $(\ ,\ )_\lambda$) are Tate quadratic forms which endow T with a global metabolic structure $\mathbf{q}$ (cf. §6.3).

11.2. **Twisting data associated to $A[p]$.** Here we associate canonical twisting data to $(A[p], \Sigma, \mathbf{q})$.

Definition 11.1. Let $\chi \in \mathcal{C}(K)$ be non-trivial and let L denote the associated cyclic p-extension $L = \bar{K}^{\ker(\chi)}$ of K. We write A^χ for the abelian variety denoted A_L in [MRS07, Definition 5.1], so that A^χ/K is an abelian variety of dimension $(p-1)\dim A$ which may be defined as the kernel of the 'norm' homomorphism $\mathrm{Res}_{L/K}A \to A$ (here $\mathrm{Res}_{L/K}A$ denotes the restriction of scalars of A from L to K).

By [MRS07, Theorem 5.5 (iv)], χ induces an inclusion of $\mathbb{Z}[\boldsymbol{\mu}_p]$ into $\mathrm{End}_K(A^\chi)$. Moreover, by Theorem 2.2 (iii) of op. cit. we have a canonical isomorphism $\psi : A[p] \xrightarrow{\sim} A^\chi[\mathfrak{p}]$ where $\mathfrak{p}$ denotes the unique prime of $\mathbb{Z}[\boldsymbol{\mu}_p]$ lying over p.

If $\mathbb{1}_{K_v} \neq \chi \in \mathcal{C}(K_v)$ for some place of K then we define A^χ/K_v similarly.

Remark 11.2. Fix $\chi \in \mathcal{C}(K)$ non-trivial, and let π be a generator of the prime $\mathfrak{p}$ of $\mathbb{Z}[\boldsymbol{\mu}_p]$ lying over p. View π inside $\mathrm{End}_K(A^\chi)$ as above. Then π is an isogeny and we have an associated π-Selmer group

$$\mathrm{Sel}_\pi(A^\chi/K) = \{\mathfrak{a} \in H^1(K, A^\chi[\mathfrak{p}]) \ : \ \mathfrak{a}_v \in \mathrm{im}(\delta_v)\ \forall v \in M_K\},$$

where here for each place v of K, $\delta_v : A^\chi(K_v)/\pi A^\chi(K_v) \hookrightarrow H^1(K_v, A^\chi[\mathfrak{p}])$ is the connecting homomorphism associated to the multiplication-by-π Kummer sequence for A^χ/K_v.

One checks that $\mathrm{Sel}_\pi(A^\chi/K)$ does not depend on the choice of generator π for $\mathfrak{p}$.

We now define the twisting data.

Definition 11.3. Let v be a place of K and $\chi \in \mathcal{C}(K_v)$. Define $\alpha_v(\chi) \subseteq H^1(K_v, A[p])$ as follows:

(i) If χ is trivial, define $\alpha_v(\chi)$ to be the image of $A(K)/pA(K)$ under the connecting homomorphism assoicated to the multiplication-by-p Kummer sequence for A/K_v,

(ii) If χ is non-trivial, let π be a generator of the prime $\mathfrak{p}$ of $\mathbb{Z}[\boldsymbol{\mu}_p]$ lying over p. Then we define $\alpha_v(\chi)$ to be the image of $A^\chi(K_v)/\pi A^\chi(K_v)$ under the composition

$$A^\chi(K_v)/\pi A^\chi(K_v) \xrightarrow{\delta_v} H^1(K_v, A^\chi[\mathfrak{p}]) \xrightarrow{\sim} H^1(K_v, A[p]),$$

where the rightmost map is induced by the isomorphism $\psi : A[p] \xrightarrow{\sim} A[\mathfrak{p}]$ of Definition 11.1. One sees easily that $\alpha_v(\chi)$ does not depend on the choice of π, and depends only on the extension cut out by χ.

As usual, for v a place of K and $\chi_1, \chi_2 \in \mathcal{C}(K_v)$, write

$$h_v(\chi_1, \chi_2) = \dim_{\mathbb{F}_p} \left(\alpha_v(\chi_1)/(\alpha_v(\chi_1) \cap \alpha_v(\chi_2))\right).$$

As in the case $p = 2$, we have.

Lemma 11.4. *Let v be a place of K, $\chi \in \mathcal{C}(K_v)$ and L_χ the extension of K_v cut out by χ. Then*

$$h_v(\mathbb{1}_{K_v}, \chi) = \dim_{\mathbb{F}_p} A(K_v)/N_{L_\chi/K_v}A(L_\chi)$$

where $N_{L_\chi/K_v} : A(L_\chi) \to A(K_v)$ is the norm map.

Moreover, if $v \nmid p$ is a nonarchimedean place of K at which A has good reduction then

(i) *if χ is unramified, we have*

$$h_v(\mathbb{1}_{K_v}, \chi) = \dim_{\mathbb{F}_p} A(K_v)/N_{L_\chi/K_v}A(L_\chi) = 0,$$

(ii) *if χ is ramified, we have*

$$h_v(\mathbb{1}_{K_v}, \chi) = \dim_{\mathbb{F}_p} A(K_v)/N_{L_\chi/K_v} A(L_\chi) = \dim_{\mathbb{F}_p} A(K_v)[p].$$

Proof. As in the case $p = 2$ the first claim is shown for elliptic curves in [MR07, Proposition 5.2] and the argument is identical. The evaluation of the cokernel of the local norm map is [Maz72, Corollary 4.4] for χ unramified, and for χ ramified the case where A is an elliptic curve is [MR07, Lemma 5.5 (ii)] and the same agument works in general. □

Proposition 11.5. *The maps $\boldsymbol{\alpha} = (\alpha_v)_v$ define twisting data for $T = (A[p], \boldsymbol{q}, \Sigma)$ and the associated Selmer groups* $\mathrm{Sel}(A[p], \chi)$ *satisfy*

$$\mathrm{Sel}(A[p], \chi) \cong \mathrm{Sel}_\pi(A^\chi/K).$$

Proof. We first claim that for each place v of K and $\chi \in \mathcal{C}(K_v)$, we have $\alpha_v(\chi) \in \mathcal{H}(q_v)$ (i.e. $\alpha_v(\chi)$ is Lagrangian). That is (since p is odd), that $\alpha_v(\chi) \subseteq H^1(K_v, A[p])$ is its own orthogonal complement under the Tate pairing. For χ trivial, that (the image in $H^1(K_v, A[p])$ of) $A(K_v)/pA(K_v)$ is its own orthogonal complement is a well known consequence of Tate local duality, see e.g. [Mil06, I.3.4]. For χ non-trivial this is shown for A an elliptic curve in [MR07, Proposition A.7] and the argument for a general principally polarised abelian variety is identical (with the Weil pairing associated to the principal polarisation λ providing the pairing on the p-adic Tate-module $T_p(A)$ required for Definition A.5 of op. cit.). We remark that in the above, unlike the case $p = 2$, the twist A^χ need not possess a principal polarisation (see [How01, Theorem 1.1]) so one cannot deduce the result by just applying Tate duality to A^χ/K_v, as one does not have an approporiate Weil-pairing on $A[\mathfrak{p}]$.

To show that $\boldsymbol{\alpha}$ defines twisting data, it remains to show that for each place $v \notin \Sigma$ with $\boldsymbol{\mu}_p \subseteq K_v$, we have $\alpha_v(\chi) \in \mathcal{H}_{\mathrm{ram}}(q_v)$. That is, that $\alpha_v(\chi) \cap H^1_{\mathrm{ur}}(K_v, A[p]) = 0$. Again, the agrument is the same as in the case $p = 2$. Indeed, for such places we have $\alpha_v(\mathbb{1}_{K_v}) = H^1_{\mathrm{ur}}(K_v, A[p])$ (again, see e.g. [PR12, Proposition 4.12] and the preceeding remark) and we conclude by Lemma 11.4 (ii).

The isomorphism $\mathrm{Sel}(A[p], \chi) \cong \mathrm{Sel}_\pi(A^\chi/K)$ is also proven identically to the case $p = 2$ by comparing the local conditions defining the two Selmer groups. □

Corollary 11.6 (Theorem 1.5)**.** *Let p be an odd prime, K a number field, A/K a principally polarised abelian variety, and Σ the set consisting of all archimedean places of K, all places of bad reduction for A, and all places dividing p. Define $\epsilon : \mathrm{Gal}(K(A[p])/K) \to \{\pm 1\}$ by $\sigma \mapsto (-1)^{\dim_{\mathbb{F}_p} A[p]^\sigma}$.*

(i) *If ϵ is non-trival when restricted to* $\mathrm{Gal}(K(A[p])/K(\boldsymbol{\mu}_p))$ *then*

$$\lim_{X\to\infty} \frac{|\{\chi \in \mathcal{C}(K, X) \ : \ \dim_{\mathbb{F}_p} \mathrm{Sel}_\pi(A^\chi/K) \text{ is even}\}|}{|\mathcal{C}(K, X)|} = 1/2.$$

(ii) *Suppose ϵ is trivial when restricted to* $\mathrm{Gal}(K(A[p])/K(\boldsymbol{\mu}_p))$. *For each $v \in \Sigma$ and character $\chi \in \mathcal{C}(K_v)$, write L_χ/K_v for the extension cut out by χ and define*

$$\omega_v(\chi) := (-1)^{\dim_{\mathbb{F}_p} A(L_\chi)/N_{L_\chi/K_v} A(L_\chi)}.$$

Finally, define

$$\delta_v := \frac{1}{|\mathcal{C}(K_v)|} \sum_{\chi \in \mathcal{C}(K_v)} \omega(\chi) \qquad \text{and} \qquad \delta := \prod_{v \in \Sigma} \delta_v.$$

Then for all sufficiently large X,

$$\frac{|\{\chi \in \mathcal{C}(K,X) \ : \ \dim_{\mathbb{F}_p}\mathrm{Sel}_\pi(A^\chi/K) \text{ is even}\}|}{|\mathcal{C}(K,X)|} = \frac{1+(-1)^{\dim_{\mathbb{F}_p}\mathrm{Sel}_p(A/K)}\cdot\delta}{2}.$$

Proof. Combine Theorem 7.4 with Proposition 11.5 and Lemma 11.4. □

Remark 11.7. As observed by Klagsbrun–Mazur–Rubin immediately before the statement of [KMR13, Theorem 8.2], as each $|\mathcal{C}(K_v)|$ has odd size we cannot have $\delta = 0$ in Case (ii) above.

Remark 11.8. As in Remark 7.5, a sufficient condition to ensure that ϵ is non-trival when restricted to $\mathrm{Gal}(K(A[p])/K(\boldsymbol{\mu}_p))$ is that $\mathrm{Gal}(K(A[p])/K)$ (viewed as a subgroup of $\mathrm{GSp}_{2g}(\mathbb{F}_p)$ for $g = \dim A$) contains a symplectic transvection. In particular, if the Galois action on $A[p]$ is as large as possible, so that $\mathrm{Gal}(K(A[p])/K) \cong \mathrm{GSp}_{2g}(\mathbb{F}_p)$, then Case (i) of Corollary 11.6 applies. It is also known that $\mathrm{Gal}(K(A[p])/K)$ contains a transvection if there is a place v of K, not dividing p, such that A has semistable reduction of toric dimension 1 at v, and such that the order of the Néron component group of A/K_v is coprime to p (see [LD98, Proposition 1.3]).

References

[AW67] M. F. Atiyah and C. T. C. Wall, *Cohomology of groups*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), 1967, pp. 94–115. MR0219512

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). MR1484478

[Čes18] Kęstutis Česnavičius, *The ℓ-parity conjecture over the constant quadratic extension*, Math. Proc. Cambridge Philos. Soc. **165** (2018), no. 3, 385–409. MR3860395

[Cor01] Gunther Cornelissen, *Two-torsion in the Jacobian of hyperelliptic curves over finite fields*, Arch. Math. (Basel) **77** (2001), no. 3, 241–246. MR1865865 (2002g:11082)

[Cor05] ———, *Erratum to: 'Two-torsion in the Jacobian of hyperelliptic curves over finite fields'*, Arch. Math. (Basel) **85** (2005), no. 6, loose erratum.

[Dye77] R. H. Dye, *A geometric characterization of the special orthogonal groups and the Dickson invariant*, J. London Math. Soc. (2) **15** (1977), no. 3, 472–476. MR0453639

[Fla90] Matthias Flach, *A generalisation of the Cassels-Tate pairing*, J. Reine Angew. Math. **412** (1990), 113–127. MR1079004

[How01] Everett W. Howe, *Isogeny classes of abelian varieties with no principal polarizations*, Moduli of abelian varieties (Texel Island, 1999), 2001, pp. 203–216. MR1827021 (2002g:11079)

[KMR13] Zev Klagsbrun, Barry Mazur, and Karl Rubin, *Disparity in Selmer ranks of quadratic twists of elliptic curves*, Ann. of Math. (2) **178** (2013), no. 1, 287–320. MR3043582

[KMR14] ———, *A markov model for selmer ranks in families of twists*, Compositio Mathematica **150** (2014Jul), no. 7, 1077–1106.

[Kra81] Kenneth Kramer, *Arithmetic of elliptic curves upon quadratic extension*, Trans. Amer. Math. Soc. **264** (1981), no. 1, 121–135. MR597871 (82g:14028)

[LD98] Pierre Le Duff, *Représentations galoisiennes associées aux points d'ordre l des jacobiennes de certaines courbes de genre 2*, Bull. Soc. Math. France **126** (1998), no. 4, 507–524. MR1693445

[Maz72] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266. MR0444670 (56 #3020)

[Mil06] J. S. Milne, *Arithmetic duality theorems*, Second, BookSurge, LLC, Charleston, SC, 2006. MR2261462 (2007e:14029)

[Mil86] ———, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 103–150. MR861974

[Mor15] Adam Morgan, *2-selmer parity for hyperelliptic curves in quadratic extensions*, Preprint, arXiv:1504.01960 (2015).

[MR07] Barry Mazur and Karl Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), no. 2, 579–612. MR2373150 (2009a:11127)

[MRS07] B. Mazur, K. Rubin, and A. Silverberg, *Twisting commutative algebraic groups*, J. Algebra **314** (2007), no. 1, 419–438. MR2331769

[Mum66] D. Mumford, *On the equations defining abelian varieties. i.*, Inventiones mathematicae **1** (1966), 287–354.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, Second, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR2392026

[Pol71] Harriet Pollatsek, *First cohomology groups of some linear groups over fields of characteristic two*, Illinois J. Math. **15** (1971), 393–417. MR0280596

[PR11] Bjorn Poonen and Eric Rains, *Self cup products and the theta characteristic torsor*, Math. Res. Lett. **18** (2011), no. 6, 1305–1318. MR2915483

[PR12] ———, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245–269. MR2833483

[PS99] Bjorn Poonen and Michael Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149. MR1740984 (2000m:11048)

[Sch85] Winfried Scharlau, *Quadratic and Hermitian forms*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 270, Springer-Verlag, Berlin, 1985. MR770063

[Sil89] Robert Silhol, *Digression on real abelian varieties and classification of real abelian surfaces*, Real algebraic surfaces, 1989, pp. 75–94.

[Smi16] Alexander Smith, *Governing fields and statistics for 4-selmer groups and 8-class groups*, Preprint, arXiv:1607.07860 (2016).

[Yu16] Myungjun Yu, *Selmer ranks of twists of hyperelliptic curves and superelliptic curves*, J. Number Theory **160** (2016), 148–185. MR3425203

School of Mathematics and Statistics, University of Glasgow, University Place, Glasgow, G12 8QQ.

Email address: adam.morgan@glasgow.ac.uk