RATIONAL POINTS ON KUMMER VARIETIES AND SWINNERTON-DYER'S METHOD

COURSE: ADAM MORGAN
NOTES: ROSS PATERSON

DISCLAIMER. These notes were taken live during lectures. In particular, any mistakes are the fault of the transcriber and not of the lecturer. I only started taking notes 15 minutes into the first lecture, so there is some excellent motivation and definitions missing from the starts.

LECTURE 1

The Cassels–Tate pairing is a bilinear pairing

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

and the left (reps. right) kernel is the maximal divisable subgroup of $Ш(A)$ (res $Ш(A^\vee)$)

1. THE OBSTRUCTION TO THE CT PAIRING PEING ALTERNATING

Let us assume for now that A is principally polarised with $\lambda : A \to A^\vee$ such a polarisation. Then we have a pairing

$$\langle , \rangle_{\mathrm{CT}} : Ш(A) \times Ш(A) \to \mathbb{Q}/\mathbb{Z}$$
$$\langle x, y \rangle_\lambda = \langle x, \lambda(y) \rangle_{\mathrm{CT}}$$

Flach showed that this is antisymmetric.

Question 1. *Is this in fact an alternating pairing? i.e. is* $\langle x, x \rangle_\lambda = 0$*?*

Seems people thought yes but hadn't written a proof, until Poonen–Stoll looked at this. Why would we want to know? Well if M is a finite abelian group with a non-degenerate alternating pairing $P : M \times M \to \mathbb{Q}/\mathbb{Z}$ then $M \cong T \times T$ for some abelian group T. In particular, $\#M$ is a square.

Answer 2 (Poonen–Stoll)**.** *In general, if P is only antisymmetric then $x \mapsto P(x,x) \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ may be 2-torsion. In particular, there exists an element $c \in M[2]$ such that $P(x,x) = P(x,c)$ for all $x \in M$. Then we have*

$$M \cong \begin{cases} T \times T & \text{if } P(c,c) = 0 \\ \mathbb{Z}/2\mathbb{Z} \times T \times T & \text{if } P(c,c) \neq 0 \end{cases}$$

We have a short exact sequence

$$0 \to A^\vee(\overline{k}) \to \mathrm{Pic}(A_{\overline{K}}) \xrightarrow{\mathcal{L} \mapsto \phi_{\mathcal{L}}} \mathrm{NS}(A_{\overline{K}}) \to 0.$$

where $\phi_{\mathcal{L}}$ is the map $x \mapsto \tau_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$ which goes $A_{\overline{K}} \to A^\vee_{\overline{K}}$. This induces

$$H^0(k, \mathrm{NS}(A_{\overline{K}})) \to H^1(k, A^\vee)$$

where $\lambda \mapsto c_\lambda$.

Theorem 3 (Poonen–Stoll)**.** *Let $c := \lambda^{-1}c_\lambda \in H^1(k, A)$. Then $c \in Ш(A)[2]$ and*

$$\langle x, x\rangle_\lambda = \langle x, c\rangle_\lambda$$

for all $x \in Ш(A)$. In particular, if $\#Ш(A) < \infty$ then we have

(i) $\langle , \rangle_\lambda$ is alternating if and only if $\lambda = \phi_{\mathcal{L}}$ for some $\mathcal{L} \in \mathrm{Pic}(A)$.
(ii) $\dim_{\mathbb{F}_2} Ш(A)[2]$ is even if and only if $\langle c, c\rangle_\lambda = 0$.

This is a very satisfying answer to the question, all coming from the geometry.

Hint of proof. Let $x = [X] \in Ш(A)$, then we want $c_\lambda - \lambda(x) \in H^1(k, A^\vee)$ to map to 0 in $\mathrm{Br}_1(X)/\mathrm{Br}_0(X) \cong H^1(K, \mathrm{Pic}(X_{\overline{K}}))$. We have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^\vee(\overline{K}) & \longrightarrow & \mathrm{Pic}(A_{\overline{K}}) & \longrightarrow & \mathrm{NS}(A_{\overline{K}}) & \longrightarrow & 0 \\ & & \| & & & & \| & & \\ 0 & \longrightarrow & \mathrm{Pic}^0(X_{\overline{K}}) & \longrightarrow & \mathrm{Pic}(X_{\overline{K}}) & \longrightarrow & \mathrm{NS}(X_{\overline{K}}) & \longrightarrow & 0, \end{array}$$

but the middle two groups are not necessarily isomorphic – there's not necessarily a Galois equivariant map between them! Comparing Galois actions in the middle we get $\lambda \mapsto c_\lambda - \lambda(x)$ under the connecting map for the bottom sequence. □

Remark 4. $c \in Ш(A)[2]$ admits a natural lift to a class $\tilde{c} \in \mathrm{Sel}_2(A) \subseteq H^1(K, A[2])$ due to the sequence

$$0 \longrightarrow A^\vee[2] \longrightarrow \mathrm{Pic}^{\mathrm{Sym}}(A_{\overline{K}}) \longrightarrow \mathrm{NS}(A_{\overline{K}}) \longrightarrow 0.$$

Here, $\mathrm{Pic}^{\mathrm{Sym}}(A_{\overline{K}})$ is the subspace of $\mathrm{Pic}(A_{\overline{K}})$ fixed by inversion.

Alternatively, $\tilde{c}$ can be described as the G_K-set of quadratic refinements of the Weil pairing $A[2] \times A[2] \to \mu_2$. Here a quadratic refinement is a quadratic function $q : A[2] \to \mu_2$ such that $q(x+y)q(x)^{-1}q(y)^{-1} = e_2(x, y)$ for e_2 the Weil pairing.

Corollary 5. *If $A[2] \subseteq A(K)$, then $\#Ш(A) < \infty$ implies that $\#Ш(A)$ is a square.*

2. Kummer Varieties

Let A/K be a principally polarised abelian variety, with $\dim(A) \geq 2$. This gives rise to a Kummer variety

$$X = \mathrm{desing}(A/\{\pm 1\}).$$

If $\dim(A) = 2$ then this will give you a K3 surface.

For $\alpha \in H^1(K, A[2])$, we have a pair (Y_α, ι) where Y_α is the associated A-torsor in $H^1(K, A)$ and ι is an involution compatible with -1 from A. We define

$$X_\alpha := \mathrm{desing}\left(Y_\alpha/\langle \iota \rangle\right)$$

to be the generalised Kummer variety associated to α. We have

$$\begin{array}{c} \tilde{Y_\alpha}/\iota \\ \big\downarrow \\ X_\alpha \end{array}$$

where $\tilde{A}_\alpha$ is the blow-up of Y_α at the fixed points of ι. In particular, Y_α is birational to a torsor.

2.1. **Quadratic twist construction.** Given a quadratic character $\chi : G_K \to \{\pm 1\}$, view χ as a 1-cocycle with values in $\mathrm{Aut}_{\overline{K}} A$. Then you get a quadratic twist A^χ/K. Note that there is an isomorphism $\phi : A^\chi \cong A$ over the quadratic extension associated to χ, so that $\phi^{-1\sigma}\phi = \chi(\sigma)$ for all $\sigma \in G_K$.

Note that $A[2] \cong A^\chi[2]$ over K: -1 does not change elements of order 2. In fact for $\alpha \in H^1(K, A[2]) \cong H^1(K, A^\chi[2])$ we get the same Kummer variety on either side, but $\tilde{Y_\alpha}$ changes to $\tilde{Y_\alpha}^\chi$.

We have

$$X_\alpha(K) \neq \emptyset \iff \exists \chi \text{ s.t. } Y_\alpha^\chi(K) \neq \emptyset.$$

The natural strategy for proving Hasse principle for X_α conditional on $\#Ш$ being finite is as follows. Suppose $X_\alpha(\mathbb{A}_K) \neq \emptyset$, then equivalently for every place v of K we have $\chi_v : G_K \to \{\pm 1\}$ such that $Y_\alpha^{\chi_v}(K_v) \neq \emptyset$.

(1) Find a global character χ_0 such that $Y_\alpha^{\chi_0} \neq \emptyset(\mathbb{A}_K)$ if and only if $\alpha \in \mathrm{Sel}_2(A^\chi)$.
(2) Construct sequence $\chi_0, \chi_1, \chi_2, \ldots, \chi_n$ with
$$\mathrm{Sel}_2(A^{\chi_0}) \supset \mathrm{Sel}_2(A^{\chi_1}) \supset \mathrm{Sel}_2(A^{\chi_2}) \supset \cdots \supset \mathrm{Sel}_2(A^{\chi_n}) = \langle \alpha \rangle .$$
(3) If $\#Ш(A^{\chi_n}) < \infty$ and we're in a situation where this implies that
$$\dim Ш(A^{\chi_n})[2] \equiv 0 \mod 2$$
then conclude that $X_\alpha(K) \neq \emptyset$. Indeed, we have
$$0 \to A(K)/2A(K) \to \mathrm{Sel}_2(A^{\chi_n}) \to Ш(A^{\chi_n}) \to 0$$
and since $Ш(A^{\chi_n})$ is even dimensional and surjected on by the 1-dimensional selmer group $\mathrm{Sel}_2(A^{\chi_n})$, it must be trivial. In particular, $Y_\alpha^{\chi_n}(K) \neq \emptyset$ and hence $X_\alpha(K) \neq \emptyset$ by just mapping a point down to X_α.

3. Variation of 2-Selmer groups in quadratic twist failies

Again take A/K a principally polarised abelian variety. Consider the sequence

$$0 \to A[2] \to A \to A \to 0.$$

Then we take Galois cohomology globally and locally to get

$$\begin{array}{ccccccc} 0 & \longrightarrow & A(K)/2A(K) & \longrightarrow & H^1(K, A[2]) & \longrightarrow & H^1(K, A) \\ & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \mathrm{res}_v} & & \\ 0 & \longrightarrow & \prod_v A(K_v)/2A(K_v) & \xrightarrow{\delta_v} & \prod_v H^1(K_v, A[2]) & \longrightarrow & \prod_v H^1(K_v, A) \end{array}$$

Now for some facts!

(1) If $v \nmid 2N_A\infty$, where N_A is the conductor of A, then $\mathrm{im}(\delta_v) = H^1_{\mathrm{nr}}(K_v, A[2]) = \ker(H^1(K_v, A[2]) \to H^1(K_v^{\mathrm{nr}}, A[2]))$
(2) If $v \nmid 2\infty$ then
$$\dim \mathrm{im}(\delta_v) = \dim A(K_v)/2A(K_v) = \dim A(K_v)[2]$$
(3) We have a local Tate pairing
$$\langle , \rangle : H^1(K_v, A[2]) \times H^1(K_v, A[2]) \xrightarrow{\cup} H^2(K_v, \mu_2) \xrightarrow{\mathrm{inv}_v} \mathbb{Q}/\mathbb{Z},$$
which is non-degenerate and the image $\mathrm{im}(\delta)$ is its own orthogonal complement (i.e. is maximal isotropic for the pairing).

Remark 6. These unramified classes are very explicit! Let's say that $v \nmid 2N_A\infty$, we know that $A[2]$ is unramified and cocycles representing classes in $H^1_{\mathrm{nr}}(K_v, A[2])$ can be evaluated at Frobenius to obtain an isomorphism

$$H^1_{\mathrm{nr}}(K_v, A[2] \xrightarrow{\sim} A[2]/(\mathrm{Frob}_v - 1)A[2],$$

where Frob_v is Frobenius.

Let $\chi : G_K \to \{\pm 1\}$ be a quadratic character then, since $A[2] = A^\chi[2]$, we can view $\mathrm{Sel}_2(A^\chi)$ as a subgroup of $H^1(K, A[2])$.

Definition 7. Let $\delta_v^\chi : A^\chi(K_v)/2A^\chi(K_v) \to H^1(K, A[2])$ be the corresponding injection for a quadratic character χ.

Note that

$$\mathrm{Sel}_2(A^\chi) = \left\{a \in H^1(K, A[2]) \ : \ \mathrm{res}_v(a) \in \mathrm{im}(\delta_v^\chi)\right\}$$

Lemma 8. *Let $v \nmid 2\infty N_A$, then*

(1) If χ is unramified at v then $\mathrm{im}(\delta_v) = H^1_{\mathrm{nr}}(K_v, A[2]) = \mathrm{im}(\delta_v^\chi)$.
(2) If χ ramifies at v then $\mathrm{im}(\delta_v^\chi) \cap \mathrm{im}(\delta_v) = 0$.

Proof. Let us prove the claims.

(1) if χ is unramified, then this is immediately clear since A^χ still has good reduction so we can appeal to our previous fact now for A^χ.
(2) We claim that $A^\chi(K_v^{\mathrm{nr}})[4] \subseteq A[2]$. Indeed, take any $\sigma \in I_v$ where I_v is the inertia subgroup. Since χ is ramified, such a thing exists. Since A had good reduction at v we must have that $A[4] = A(K_v^{\mathrm{nr}})[4]$ by Néron–Ogg–Shafarevich. But σ acts on $A^\chi[4]$ as multiplication by $\chi(\sigma) = -1$, and hence
$$A^\chi(K_v^{\mathrm{nr}})[4] \subseteq \{x \in A^\chi[4] \ : \ -x = x\} = A[2],$$
as required.
Now consider
$$0 \to A[2] \to A^\chi[4] \to A[2] \to 0$$
Then as $A(K_v)[2] \subseteq A(K_v^{\mathrm{nr}})[2]$ and δ_v^χ is injective to $H^1(K_v, A[2])$, we must have that the image $\mathrm{im}(\delta_v^\chi) = \delta_v^\chi(A(K_v)[2])$ by counting the dimension and applying this injectivity, and again via this injectivity $\delta_v^\chi(A(K_v)[2]) \cap H^1_{\mathrm{nr}}(K_v, A[2]) = 0$ as required.

□

Proposition 9 (Mazur–Rubin)**.** *Let $\chi : G_K \to \{\pm 1\}$ and $\Sigma = \{v \mid 2N_A\infty\}$. Suppose that $\mathrm{im}(\delta_v) = \mathrm{im}(\delta_v^\chi)$ for all $v \in \Sigma$ (e.g. if $\mathrm{res}_v(\chi)$ is trivial $\forall v \in \Sigma$). Let $S = \{v \notin \Sigma \ : \ \chi$ ramified at $v\}$. Moreover define*

$$V_S := \mathrm{im}\left(\mathrm{Sel}_2(A) \to \bigoplus_{v \in S} H^1(K_v, A[2])\right)$$
$$V_S^\chi := \mathrm{im}\left(\mathrm{Sel}_2(A^\chi) \to \bigoplus_{v \in S} H^1(K_v, A[2])\right)$$

Then

$$\dim \mathrm{Sel}_2(A^\chi) = \dim \mathrm{Sel}_2(A) + \dim V_S^\chi - \dim V_S.$$

Moreover we have

(1) $\dim V_S + \dim V_S^\chi \leq t = \sum_{v\in S} \dim A(K_v)[2]$
(2) $\dim V_S + \dim V_S^\chi \equiv t \mod 2$

Proof. Let $M = \{x \in \mathrm{Sel}_2(A) \ : \ \mathrm{res}_v(x) = 0 \ \forall v \in S\}$. By definition we have exact sequences

$$0 \longrightarrow M \longrightarrow \mathrm{Sel}_2(A) \longrightarrow V_S \longrightarrow 0$$

$$0 \longrightarrow M \longrightarrow \mathrm{Sel}_2(A^\chi) \longrightarrow V_S^\chi \longrightarrow 0.$$

Taking dimensions gives the first claim.

We now show point (1). firstly since $\mathrm{im}(\delta_v) \cap \mathrm{im}(\delta_v^\chi) = 0$ and are both maximal isotropic, we must have that the restriction of the local Tate pairing

$$\langle , \rangle_v : \mathrm{im}(\delta_v) \times \mathrm{im}(\delta_v^\chi) \to \mathbb{Q}/\mathbb{Z}$$

is non-degenerate. Summing over S, we now have a pairing

$$\sum_v \langle , \rangle_v : \bigoplus_{v\in S} \mathrm{im}(\delta_v) \times \bigoplus_{v\in S} \mathrm{im}(\delta_v^\chi) \to \mathbb{Q}/\mathbb{Z}$$

where V_S is contained in the left and V_S^χ in the right domains. Reciprocity for the Brauer group $\mathrm{Br}(K)$ gives us that

$$0 = \sum_v \mathrm{inv}_v(a \cup b) = \sum_{v\in S} \mathrm{inv}_v(a \cup b)$$

so V_S, V_S^χ are orthogonal with respect to this pairing. Hence

$$\dim V_S + \dim V_S^\chi \leq \sum_{v\in S} \dim \mathrm{im}(\delta_v) = \sum_{v\in S} A(K_v)[2].$$

Point (2) is more subtle, and uses existence of quadratic refinements for the local Tate pairing coming from Mumford theta groups. □

Lecture 2

Let K be a number field and A/K a principally polarised abelian variety. We recall Proposition 9, and that the maps here are

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

Let's take a step back and recap the strategy so that we're on the same page. We're interested in the existence of rational points on generalised Kummer varieties. For A/K, and $\alpha \in H^1(K, A[2])$, we can associate (Y_α, ι) where ι is an involution, and $X_\alpha = \mathrm{desing}(Y_\alpha/\iota)$ is the Kummer variety of interest. For each $\chi : G_K \to \{\pm 1\}$ we have a map $\widetilde{Y}_\alpha^\chi \to X_\alpha$. Suppose that $X(\mathbb{A}_K) \neq \emptyset$, so that equivalently for every v, we have $\chi_v : G_{K_v} \to \{\pm 1\}$ with $Y_\alpha^{\chi_v}(K_v) \neq \emptyset$. Our steps are then.

- Find a global χ_0 such that $Y_\alpha^{\chi_0} \neq \emptyset$. Equivalently, that $\alpha \in \mathrm{Sel}_2(A^\chi)$.
- Construct a succession of such characters $\chi_1, \ldots, \chi_n$ such that $\mathrm{Sel}_2(A^{\chi_i}) \supsetneq \mathrm{Sel}_2(A^{\chi_{i+1}})$, and the last has $\mathrm{Sel}_2(A^{\chi_n}) = \langle \alpha \rangle$.
- Under finiteness of Ш(A^{χ_n}), we must have our claim.

Corollary 10. *Suppose*

- $\mathrm{res}_v(\chi)$ *is trivial for all* $v \in \Sigma$,
- χ *ramifies in a unique place* $w \notin \Sigma$ *such that*

$$\mathrm{Sel}_2(A) \xrightarrow{\mathrm{res}_w} H^1_{\mathrm{nr}}(K_w, A[2]) \cong A[2]/(\mathrm{Frob}_w - 1)A[2],$$

which is $\varphi \mapsto \varphi(\mathrm{Frob}_w)$*, is surjective.*

Then $\dim \mathrm{Sel}_2(A^\chi) = \dim \mathrm{Sel}_2(A) - \dim A(K_w)[2]$.

Proof. Apply Proposition 9, then our assumption gives $V_S = \dim A(K_2)[2]$ and $V_S^\chi = 0$. □

It's worth noting and incorporating into our proof that if this strategy is to work, then α will represent a rank point on $A^{\chi_n}(K)$, which will be rank 1. In particular, the parity of the rank will be odd, and this is something we expect to be able to control under finiteness of Ш via local root numbers.

Theorem 11 (M)**.** *Assume that* $\#Ш(A^\chi) < \infty$ *for all* χ*. Then* $\mathrm{rank}(A)^\chi \mod 2$ *is determined by* $\{\mathrm{res}_v(\chi)\}_{v\in\Sigma}$*. This is unconditional if we replace* $\mathrm{rk}(A)$ *with* $\mathrm{rk}_2(A)$ *the* 2^∞ *Selmer rank.*

Ideas in proof. This uses variant of part (ii) of Proposition 9 and then an understanding of the Poonen–Stoll class under quadratic twist. □

Remark 12. The rank statement follows easily from the parity conjecture:

$$(-1)^{\mathrm{rk}(A)} = \omega(A) = \prod_{v|N_A\infty} \omega_v(A),$$

where ω (resp. ω_v) is the global (resp. local) root number. Say χ corresponds to a quadratic extension F/K. Then we have

$$(-1)^{\mathrm{rk}(A^\chi)} = (-1)^{\mathrm{rk}(A)}(-1)^{\mathrm{rk}(A/F)} = (-1)^{\mathrm{rk}(A)} \prod_{w|N_A\infty} w_v(A).$$

It is known for elliptic curves that finiteness of Ш implies parity, but this is not known for general abelian varieties.

An example: Jacobians of genus 2 curves. Let $f(x) \in K[x]$ be a separable degree 5 or 6 polynomial and consider $C : y^2 = f(x)$ the associated genus 2 curve. Let $A = \mathrm{Jac}(C)$ be the corresponding principally polarised abelian surface. If $\chi : G_K \to \{\pm 1\}$ and $K(\sqrt{d})/K$ be the associated quadratic extension. Then

$$A^\chi = \mathrm{Jac}(y^2 = df(x)).$$

Let

$$W = \begin{cases} \langle (r,0) \ : \ f(r) = 0 \rangle & \text{if } \deg(f) = 6 \\ \langle (r,0) \ : \ f(r) = 0 \rangle \cup \{\infty\} & \text{if } \deg(f) = 5. \end{cases}$$

given $P, Q \in W$ we have $[P - Q] \in A[2]$. In fact there is an isomorphism of G_K-modules

$$A[2] \cong \frac{\mathbb{F}_2[W]_{\mathrm{sum}=0}}{\sum_{w\in W} w}.$$

Thinking of the right hand size as even sized subsets of W modulo the equivalence relation identifying a subset with its complement, the Weil pairing becomes

$$e_2(T_1, T_2) = (-1)^{\#T_1 \cap T_2}$$

and a bijection

$$\left\{\begin{smallmatrix}\text{odd sized}\\ \text{subsets of}\\ W\end{smallmatrix}\right\} \leftrightarrow \left\{\begin{smallmatrix}\text{quadratic}\\ \text{refinements of}\\ we_2\end{smallmatrix}\right\}.$$

under the map $T \mapsto q_T$ where $q_T(T') = (-1)^{\frac{\#T'}{2}+\#T'\cap T}$. This gives an explicit description of the lift $\tilde{c} \in H^1(K, A[2])$ of the Poonen–Stoll class.

We have $G := \mathrm{Gal}(K(A[2])/K \cong \mathrm{Gal}(f) \subseteq S_{\deg(f)}$. We can then show the following.

Lemma 13. *Suppose that $G \cong S_{\deg(f)}$ then $A[2]$ is a simple G-module and $\mathrm{End}_{\mathbb{Z}G}(A[2]) = \mathbb{F}_2$. Then*

$$H^1(G, A[2]) = \begin{cases} 0 & \text{if } \deg(f) = 5, \\ \langle \tilde{c} \rangle & \text{if } \deg(f) = 6, \end{cases}$$

where $\tilde{c}$ is the lift of the Poonen–Stoll class as before.

4. Extensions defined by 1-cocycles

Let $T = \{\alpha_1, \ldots, \alpha_t\} \subseteq H^1(K, A[2])$, $G = \mathrm{Gal}(K(A[2])/K)$ and $L = K(A[2])$. Represent the α_i by 1-cocycles $\tilde{\alpha_i}$, then

$$\begin{aligned} \varphi_T : G_K &\to A[2]^t \rtimes G \\ \sigma &\mapsto (\tilde{\alpha_1}(\sigma), \ldots, \tilde{\alpha_t}(\sigma), \overline{\sigma}) \end{aligned}$$

is a homomorphism. Let K_T be the fixed field of $\ker(\varphi_T)$ so that the factored map $\varphi_T : \mathrm{Gal}(K_T/K) \to A[2]^t \rtimes G$ is injective.

Lemma 14. *Suppose that:*

- *$A[2]$ is a simple G-module, and $\mathrm{End}_G(A[2]) = \mathbb{F}_2$,*
- *the image of T in $H^1(L, A[2])$ is $\mathbb{F}_2$-linearly independent (automatic if true in T and $H^1(G, A[2]) = 0$).*

Then $\varphi_T : \mathrm{Gal}(K_T/K) \to A[2]^t \rtimes G$ is an isomorphism. Moreover, the maximal abelian subextension of K_t/K is contained in $K(A[2])/K$

Proof sketch. We have

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(K_t/L) & \longrightarrow & \mathrm{Gal}(K_T/K) & \longrightarrow & \mathrm{Gal}(L/K) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \varphi_T|_L} & & \downarrow{\scriptstyle \varphi_T} & & \| & & \\ 1 & \longrightarrow & A[2]^t & \longrightarrow & A[2]^t \rtimes G & \longrightarrow & G & \longrightarrow & 1. \end{array}$$

It suffices to show that $\varphi_T|_L$ is surjective. Note that by construction, this is G-equivariant where G acts on $\mathrm{Gal}(K_T/L)$ via the conjugation action of $\mathrm{Gal}(L/K)$ in the larger group.

$\mathrm{im}(\varphi_T|_L) \leq A[2]^t$ is a G-submodule, and since $A[2]$ is simple we must have that $\mathrm{Gal}(K_T/L) \cong A[2]^r$ for some $r \leq t$. Hence

$$\mathrm{Hom}_G(\mathrm{Gal}(K_T/L), A[2]) \cong \mathrm{Hom}_G(A[2]^r, A[2]) \cong \mathbb{F}_2^r.$$

Now we know that the span of $\mathrm{res}_L(T)$ inside of this group is of dimension t by the $\mathbb{F}_2$-linear independence, so $t \leq r$ and we conclude. □

Theorem 15 (Harpaz–Skorobogatov)**.** *Take $f(x) \in \mathcal{O}_K[x]$ to be a separable monic polynomial of degree 5, let $C : y^2 = f(x)$ be the corresponding hyperelliptic curve and $A = \mathrm{Jac}(C)$ the Jacobian. Let $\alpha \in H^1(K, A[2])$ and suppose:*

- $\mathrm{Gal}(F) \cong S_5$
- *Suppose that there is a prime $\mathfrak{p} \nmid 2$ such that*

$$v_{\mathfrak{p}}(\mathrm{disc}(f)) = 1,$$

  and α is unramified at $\mathfrak{p}$.

Then assuming that $\#Ш(A) < \infty$ the Kummer variety X_α satisfies the Hasse principle.

Proof. Assume that $\#Ш(A) < \infty$ throughout. Note that $\tilde{c} \in H^1(K, A[2])$ is trivial, and without loss of generality we assume that $\alpha \neq 0$ and $X_\alpha(\mathbb{A}_K) \neq \emptyset$. Let $\Sigma = \{v \mid 2N_A\infty\} \cup \{v \ : \ \alpha \text{ ramified at } v\}$. We have that there is a system $\{\chi_v\}_{v\in\Sigma}$ such that

- $Y_\alpha^{\chi_v}(K_v) \neq \emptyset$
- if $\chi : G_K \to \{\pm 1\}$ is such that $\mathrm{res}_v(\chi) = \chi_v$ for all $v \in \Sigma$, then $\mathrm{rk}(A^\chi)$ is odd (and hence $\dim \mathrm{Sel}_2(A^\chi)$ odd)

This second step really uses the existence of $\mathfrak{p}$ to move from even to odd.

Step 1: We construct the global character $\chi = \chi_0 : G_K \to \{\pm 1\}$ such that

- $\mathrm{res}_v(\chi_0) = \chi_v$ for all $v \in \Sigma$.
- If χ_0 ramifies at $v \notin \Sigma$ then $\mathrm{res}_v(\alpha) = 0$.

We will not explain this in the interests of time. Essentially this can be lifted off the shelf from the fibration method literature, or you can just show it using some class field theory and Poitou–Tate duality. It uses the maximality of the Galois action.

As a consequence we have $\alpha \in \mathrm{Sel}_2(A^{\chi_0})$ and $\mathrm{Sel}_2(A^{\chi_0})$ is odd.

Step 2: Let χ be a character as constructed in step 1, so that $\alpha \in \mathrm{Sel}_2(A^{\chi_0})$ and $\mathrm{Sel}_2(A^{\chi_0})$ is odd and *dimension at least* 3. Then we claim that there exists a new character χ' such that $\alpha \in \mathrm{Sel}_2(A^{\chi'})$ and $\dim(\mathrm{Sel}_2(A^{\chi'})) = \dim \mathrm{Sel}_2(A^\chi) - 2$.

Given this claim, we apply inductively, reduce to selmer rank 1 and then use finiteness of Ш as required.

Proof of claim: Extend $\alpha = \alpha_1$ to a basis $T = \{\alpha_1, \dots, \alpha_t\}$ for $\mathrm{Sel}_2(A^\chi)$. Using Lemma 14 and the example we wrote earlier about such hyperelliptic curves, we know we have this extension K_T/K with

$$\begin{aligned} \mathrm{Gal}(K_T/K) &\cong A[2]^t \rtimes S_5 \\ \sigma &\mapsto (\alpha_1(\sigma), \dots, \alpha_t(\sigma), \overline{\sigma}) \end{aligned}$$

Let $\tilde{\Sigma} = \Sigma \cup \{v \ : \ \chi \text{ is ramified at } v\}$, and $\mathfrak{m} = 8\prod_{v\in\tilde{\Sigma}} v$ be a modulus and $K_\mathfrak{m}/K$ be the corresponding ray class field. Then there exists $\sigma \in \mathrm{Gal}(K_\mathfrak{m}K_T/K)$ such that

(1) $\sigma|_{K_\mathfrak{m}} = 1$
(2) $\varphi_T(\sigma|_{K_T}) = (0, P_1, P_2, *, \dots, *, \tau)$

where τ is a double transposition and P_1, P_2 is a basis for the 2-dimensional module $A[2]/(\tau - 1)A[2]$.

Let $\mathfrak{p} \notin \tilde{\Sigma}$ be a prime such that $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(K_\mathfrak{m}K_T/K)$ is in the conjugacy class of σ (by Chebotarev). Then by class field theory

- $\mathfrak{p} = \langle \pi \rangle$ for some $\pi \in \mathcal{O}_K$ which is totally positive and congruent to 1 modulo $\mathfrak{m}$. If χ corresponds to $K(\sqrt{d})/K$ then let χ' be the character corresponding to $K(\sqrt{\pi d})/K$. Note that $\mathrm{res}_v(\chi') = \mathrm{res}_v(\chi)$ for all $v \in \Sigma$ by construction. Moreover it is unramified away from Σ and $\mathfrak{p}$.
- $\mathrm{Sel}_2(A^\chi) \xrightarrow{\mathrm{res}_\mathfrak{p}} H^1_{\mathrm{nr}}(K_\mathfrak{p}, A[2])$ the map given by evaluation on cocycles is surjective since $\alpha_2(\mathrm{Frob}_\mathfrak{p}), \alpha_3(\mathrm{Frob}_\mathfrak{p})$ span $A[2]/(\mathrm{Frob}_\mathfrak{p} - 1)A[2]$
- $\alpha(\mathrm{Frob}_\mathfrak{p}) = 0$.

We then apply Corollary 10 and conclude. □

Remark 16. We can prove variants of this theorem for $\mathrm{Gal}(f) \in \{A_5, F_{20}, D_{10}\}$ via this method. This has been shown by Morgan–Skorobogatov.

Theorem 17 (M.)**.** *The same result as in Theorem 15 holds when* $\deg(f) = 6$ *and* $\mathrm{Gal}(f) = S_6$

There are various problems with the original strategy here.

(1) $\tilde{c}$ is nontrivial and generates $H^1(\mathrm{Gal}(f), A[2])$. So it lives in $\mathrm{Sel}_2(A^\chi)$ for every χ. So we can never get $\mathrm{Sel}_2(A^\chi) = \langle \alpha \rangle$.
(2) Even overcoming this, $\#Ш < \infty$ no longer implies that $\dim Ш(A^\chi)[2]$ is even.

Our alternative strategy is to do a second descent step using the Cassels–Tate pairing.

$$Ш(A^\chi) \times Ш(A^\chi) \to \mathbb{Q}/\mathbb{Z}.$$

This lifts back to a pairing

$$\mathrm{CTP}_\chi : \mathrm{Sel}_2(A^\chi) \times \mathrm{Sel}_2(A^\chi) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$$

where the left (and right) kernel is the image under the map induced by $E[4] \to E[2]$ by multiplication by 2 of the group $\mathrm{Sel}_4(A^\chi)$.

Suppose, using finiteness of $Ш(A^\chi)$, that we can arrange that

- $\mathrm{rk}(A^\chi)$ is odd,
- $\ker(\mathrm{CTP}_\chi) = \langle \alpha \rangle$.

Then again we can conclude that $X_\alpha(K) \neq \emptyset$. So we need to study variation of the Cassels–Tate pairing under quadratic twist.

5. Variation of the Cassels–Tate pairing under quadratic twist

Let A/K be a principally polarised abelian variety and $G = \mathrm{Gal}(K(A[2])/K)$. Let $\tilde{c} \in \mathrm{Sel}_2(A)$ be the lift of the Poonen–Stoll class as before.

Definition 18. Call a $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$-valued pairing P on $\mathrm{Sel}_2(A)$ *admissible* if

- $P(x, x) = P(x, \tilde{c})$ for all $x \in \mathrm{Sel}_2(A)$,
- $P(c, c) = 0 \iff \dim(Ш/Ш_{\mathrm{div}})[2] \equiv 0 \mod 2$.

Theorem 19 (M.)**.** *Suppose that* $A[2]$ *is a simple* G *-module and* $\mathrm{End}_G(A[2]) = \mathbb{F}_2$*. Suppose there exists* $g \in G$ *such that* $A[2]^g = 0$ *and* $H^1(G, A[2]) = \langle \tilde{c} \rangle$*.*

Then there exists $\chi : G_K \to \pm\{\pm 1\}$ *such that*

- $\mathrm{rk}_2(A) \equiv \mathrm{rk}_2(A^\chi) \mod 2$
- $\mathrm{Sel}_2(A^\chi) = \mathrm{Sel}_2(A)$ *inside of* $H^1(K, A[2])$*,*
- *For all* $x, y \in \mathrm{Sel}_2(A^\chi)$*,*

$$\mathrm{CTP}_\chi(x, y) = P(x, y).$$