JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Sebastian PETERSEN

The rank of hyperelliptic Jacobians in families of quadratic twists

Tome 18, n° 3 (2006), p. 653-676.

<http://jtnb.cedram.org/item?id=JTNB_2006__18_3_653_0>

Journal de Théorie des Nombres
de Bordeaux **18** (2006), 653-676

The rank of hyperelliptic Jacobians in families of quadratic twists

par Sebastian PETERSEN

Résumé. La variation du rang des courbes elliptiques sur $\mathbb{Q}$ dans des familles de "twists" quadratiques a été étudiée de façon détaillée par Gouvêa, Mazur, Stewart, Top, Rubin et Silverberg. On sait par exemple que chaque courbe elliptique sur $\mathbb{Q}$ admet une infinité de twists quadratiques de rang au moins 1. Presque toutes les courbes elliptiques admettent même une infinité de twists de rang ≥ 2 et on connaît des exemples pour lesquels on trouve une infinité de twists ayant rang ≥ 4. On dispose pareillement de quelques résultats de densité. Cet article étudie la variation du rang des jacobiennes hyperelliptiques dans des familles de twists quadratiques, d'une manière analogue.

Abstract. The variation of the rank of elliptic curves over $\mathbb{Q}$ in families of quadratic twists has been extensively studied by Gouvêa, Mazur, Stewart, Top, Rubin and Silverberg. It is known, for example, that any elliptic curve over $\mathbb{Q}$ admits infinitely many quadratic twists of rank ≥ 1. Most elliptic curves have even infinitely many twists of rank ≥ 2 and examples of elliptic curves with infinitely many twists of rank ≥ 4 are known. There are also certain density results. This paper studies the variation of the rank of hyperelliptic Jacobian varieties in families of quadratic twists in an analogous way.

1. Introduction

The behavior of the Mordell-Weil-rank of elliptic curves over $\mathbb{Q}$ in families of quadratic twists has been extensively studied by Gouvêa and Mazur [3], Stewart and Top [21] and in the series of papers [15], [16], [17] by Rubin and Silverberg. See [18] for an up-to-date survey. We briefly summarize some of the main results:

Manuscrit reçu le 20 février 2006.

(1) Any elliptic curve over $\mathbb{Q}$ has infinitely many quadratic twists of rank ≥ 1.
(2) If E is an elliptic curve over $\mathbb{Q}$ with $j_E \notin \{0, 1728\}$, then E has infinitely many quadratic twists of rank ≥ 2.
(3) Examples of elliptic curves with infinitely many quadratic twists of rank ≥ 4 are known.

If the parity conjecture holds true, then somewhat better conditional results were shown. In case of the first two statements certain density results were obtained - see [15] for the details. The aim of this paper is to study the rank in families of quadratic twists of hyperelliptic Jacobians in a similar way.

Let k be a field. Throughout this note a k-variety will be a separated, algebraic, geometrically integral k-scheme and a k-curve will be a k-variety of dimension 1. A **hyperelliptic curve** H over k will be a geometrically regular k-curve together with a distinguished k-morphism $p : H \to \mathbb{P}_1$ of degree 2.

In [15, Section 6] Rubin and Silverberg pose the following problem: Find an elliptic curve $E/\mathbb{Q}$ and a hyperelliptic curve $S/\mathbb{Q}$ such that the Jacobian J_S of S is $\mathbb{Q}$-isogenous to $E^r \times B$ for some abelian variety $B/\mathbb{Q}$ and with $r \geq 4$. Solutions (E, S, r, B) to this problem were obtained for $r = 2$ and $r = 3$ in [15] (see also [8]). If (E, S, r, B) is a solution to this problem, then E will have infinitely many quadratic twists of rank $\geq r$ by the arguments in [15] or by applying the following more general theorem in the special case $A = E$.

Theorem 1.1. *Let k be a number field and A/k an abelian variety (for example A an elliptic curve or $A = J_H$ the Jacobian of a certain hyperelliptic curve).*

(1) *Suppose that there is a hyperelliptic curve S/k such that $\mathrm{Hom}(J_S, A) \neq 0$. Then A admits infinitely many quadratic twists of rank $\geq \mathrm{rk}(\mathrm{Hom}(J_S, A))$.*
(2) *Let S be an arbitrary hyperelliptic curve. If there is a k-isogeny $J_S \sim A^r \times B$ for some abelian variety B/k, then*

$$\mathrm{rk}(\mathrm{Hom}_k(J_S, A)) \geq r \cdot \mathrm{rk}(\mathrm{End}_k(A)).$$

The proof of this theorem is based on the specialization theorem of Silverman. In fact, Theorem 4.2 below gives a more detailed statement. Our general result on the rank in families of quadratic twists of hyperelliptic Jacobians is:

(1) Any hyperelliptic curve H over k admits infinitely many quadratic twists of rank $\geq \mathrm{rk}(\mathrm{End}_k(J_H))$. (Use the above theorem with $S = H$ and $A = J_H$ to see this.)
(2) We remark that for any R there is a hyperelliptic curve H over k with $\mathrm{rk}(\mathrm{End}_k(J_H)) \geq R$ and thus with infinitely many quadratic twists of rank $\geq R$. Unfortunately we always have $\mathrm{rk}(\mathrm{End}_k(J_H)) \leq 4g_H^2$ where $g_H = \dim(J_H)$ is the genus of H. Thus we cannot observe arbitrarily large endomorphism rings, if we pin down the genus at the same time.

Let k be a number field. We will then be interested in the following problem: Construct a hyperelliptic curve H/k and a hyperelliptic curve S/k such that there is a k-isogeny $J_S \sim J_H^r \times B$ for some abelian variety B/k. (Compare the problem of Rubin and Silverberg above). If (H, S, r, B) is a solution to this problem, then J_H will have infinitely many quadratic twists of rank $\geq r \cdot \mathrm{rk}(\mathrm{End}_k(J_H))$ by Theorem 1.1. We think it is too ambitious to try to prove the following statement: "For any hyperelliptic curve H there exists another hyperelliptic curve S such that there is a k-isogeny $J_S \sim J_H^2 \times B$ for some B", since this statement *would* imply that any hyperelliptic Jacobian (and in particular any elliptic curve) *would* have quadratic twists of arbitrarily high rank. A conjecture[1] of Honda [6] (see also [16, 7.9]) implies to the contrary that the rank should be bounded in the family of quadratic twists of an elliptic curve $E/\mathbb{Q}$. Nevertheless we can prove:

(1) There are certain quite special hyperelliptic curves H/k (but still infinitely many for each genus) for which there exists a hyperelliptic curve S/k such that $J_S \sim J_H^2 \times B$ for some B/k. Each such H admits infinitely many quadratic twists of rank $\geq 2 \cdot \mathrm{rk}(\mathrm{End}_k(J_H))$.
(2) There are certain very special hyperelliptic curves H/k for which there is a hyperelliptic curve S/k such that $J_S \sim J_H^3 \times B$. Each such H admits infinitely many quadratic twists of rank $\geq 3 \cdot \mathrm{rk}(\mathrm{End}_k(J_H))$.

Furthermore, in the special case $k = \mathbb{Q}$, we can sharpen all our theorems on the rank in families of quadratic twist by providing density results similar to the density results in [15], [16], [17]. The proof of these density results is based on strong results of Stewart and Top [21] on squarefree values of polynomials.

Acknowledgement

Most of this article is based on the author's Ph.D. thesis. The author wishes to heartily thank his supervisor Prof. Greither for many very helpful

[1] Today many people think that this conjecture of Honda could be false.

discussions on the subject. Furthermore he wants to thank Prof. B. Conrad for providing him with his preprint [2]. Finally the author wants to mention that most of this paper is built on ideas which are already present in the papers [15], [16], [17] of Rubin and Silverberg on ranks of elliptic curves.

Notation

Let k be a field. If X and Y are k-schemes, then $\mathrm{Mor}_k(X,Y)$ stands for the set of k-morphisms $X \to Y$. We write AbVar_k for the category of abelian varieties over k. If A and B are abelian varieties over k, then $\mathrm{Hom}_k(A,B)$ denotes the abelian group of AbVar_k-morphisms $A \to B$. Furthermore $\mathrm{Aut}_k(A)$ means the group of AbVar_k-automorphisms $A \to A$. Note that $\mathrm{Aut}_k(A)$ does not contain non-trivial translations. We denote by $\mathrm{IsAb}_k := \mathrm{AbVar}_k \otimes \mathbb{Q}$ the isogeny category of AbVar_k and by

$$\mathrm{Hom}_k^0(A,B) := \mathrm{Hom}_k(A,B) \otimes_{\mathbb{Z}} \mathbb{Q}$$

the $\mathbb{Q}$-vector space of IsAb_k-morphisms $A \to B$. If there is a k-isogeny $A \to B$, then we shall write $A \sim B$ and call A and B isogenous. We denote by k^s the separable closure of k. The Galois group G_k operates on the left on $\mathrm{Spec}(k^s)$ and on the right on k^s. Finally, if C is a smooth, projective curve over k, then J_C stands for the Jacobian of C and g_C for the genus of C.

2. Hyperelliptic curves and quadratic twists

In this section we collect basic material on hyperelliptic curves and on their quadratic twists.

Let k be a field of characteristic 0 and $K = k(X)$ the function field of $\mathbb{P}_1$. In the introduction we defined a hyperelliptic curve H/k to be a smooth k-curve together with a distinguished degree 2 morphism $H \to \mathbb{P}_1$. Sometimes we want to give a hyperelliptic curve by an explicit equation. We define $\mathrm{Adm}(k) := K^\times - k^\times K^{\times 2}$, Adm standing for admissible, and for $f \in \mathrm{Adm}(k)$ we denote by $H_{f,k}$ (or simply H_f if the ground field is understood) the normalization of $\mathbb{P}_1$ in the function field

$$k(X, \sqrt{f(X)}) := k(X)[Y]/(Y^2 - f(X)).$$

One may think of $H_{f,k}$ as the smooth, projective model for the equation

$$Y^2 = f(X).$$

There is a canonical degree 2 morphism $H_{f,k} \to \mathbb{P}_1$, thus $H_{f,k}$ is a hyperelliptic curve. $J_{f,k}$ stands for the Jacobian of $H_{f,k}$. If $E|k$ is a field extension and $f \in \mathrm{Adm}(k)$, then $f \in \mathrm{Adm}(E)$ and $H_{f,E} = H_{f,k} \otimes_k E$. Let $D \in E^\times$.

We denote by $H^D_{f,E} := H_{D^{-1}f,E}$ the E-curve which is the smooth projective model for the equation

$$DY^2 = f(X).$$

Note that there is an obvious $E(\sqrt{D})$-isomorphism

$$H^D_{f,E} \otimes E(\sqrt{D}) \cong H_{f,E} \otimes E(\sqrt{D}),$$

that is $H^D_{f,E}$ is an $E(\sqrt{D})|E$-twist of $H_{f,E}$.

We will be concerned with twists of an arbitrary abelian variety A/k in several places of this paper. Let $E|k$ be a field extension (usually $E = k$ or $E = k(T)$ in our applications) and $L|E$ be a Galois extension. An $L|E$-**twist** of A is an abelian variety B/E, for which there is an L-isomorphism $B_L \to A_L$.

Let B be an $L|E$-twist of A and $f : B_L \to A_L$ an L-isomorphism. Then $\xi : G_{L|E} \to \mathrm{Aut}_L(A_L), \sigma \mapsto f^\sigma f^{-1}$ is a cocycle in $Z^1(G_{L|E}, \mathrm{Aut}_L(A_L))$ whose cohomology class neither depends on the choice of f nor on the E-isomorphism class of B. It is well-known, that this sets up a bijection of pointed sets

$$\alpha : T_{L|E}(A) \to H^1(G_{L|E}, \mathrm{Aut}_L(A_L)).$$

Here $T_{L|E}(X)$ stands for the set of E-isomorphism classes of $L|E$-twists of A.

We shall be mainly concerned with quadratic twists. For any abelian variety A/k we can identify μ_2 with a subgroup of $\mathrm{Aut}_{E^s}(A_{E^s})$. We obtain maps

$$E^\times \to H^1(G_E, \mu_2) \to H^1(G_E, \mathrm{Aut}_{E^s}(A_{E^s})) \to T_{E^s|E}(A),$$

where the left hand map $D \mapsto (\sigma \mapsto \sqrt{D}^{\sigma-1})$ comes from Kummer theory, the middle map is induced by the inclusion $\mu_2 \subset \mathrm{Aut}_{E^s}(A_{E^s})$ and the right hand map is the inverse of the map α described above. For $D \in E^\times$ denote by A^D_E (or simply by A^D) the image of $D \in E^\times$ under this sequence of maps. The abelian varieties[2] A^D_E are called the **quadratic twists** of A_E. Clearly A^D_E depends only on the residue class of D in $E^\times/E^{\times 2}$. If $f \in \mathrm{Adm}(k)$ and $D \in E^\times$, then $J^D_{f,E}$ turns out to be the Jacobian of $H^D_{f,E}$.

We recall a convenient description of the Mordell-Weil group of a quadratic twist A^D. If G is a profinite group, M is a discrete G-module and $\xi \in \mathrm{Hom}(G, \mu_2)$, then we denote by

$$M^\xi := \{a \in M \mid a^\sigma = \xi(\sigma)a \,\forall \sigma \in G\}$$

the eigenspace of ξ in the sequel.

[2]In fact, A^D_E is an E-isomorphism class of abelian varieties rather than an abelian variety.

Remark 2.1. *Let A/k be an abelian variety, $E|k$ an extension field and $D \in E^\times$. Let $L|E$ be a Galois extension field containing $\sqrt{D}$. We define $\xi \in \mathrm{Hom}(G_{L|E}, \mu_2)$ by $\xi(\sigma) := \sqrt{D}^{\sigma-1}$ for $\sigma \in G_{L|E}$. Then there is an isomorphism $A^D(E) \cong A(L)^\xi$.*

Proof. By the constructions above, there is an L-isomorphism $f : A^D_L \cong A_L$ such that $\xi(\sigma) = f^\sigma f^{-1}$ for all $\sigma \in G_{L|E}$. One checks easily, that the isomorphism $f : A^D(L) \to A(L)$, which needs not be $G_{L|E}$-equivariant, induces an isomorphism $A^D(E) \cong A(L)^\xi$, as desired. □

We conclude this section by an important remark on the Mordell-Weil group of an abelian variety in a Kummer extension of exponent 2. If G is a 2-group, then we shall write $\hat{G} := \mathrm{Hom}(G, \mu_2)$ for its character group in the sequel. Furthermore, for abelian groups M and N, we shall use the notation $M \sim N$ if there is a $\mathbb{Q}$-isomorphism $M \otimes \mathbb{Q} \cong N \otimes \mathbb{Q}$.

Proposition 2.2. *Let $E|k$ be an extension field and $L|E$ a* finite Kummer extension of exponent 2. *Let A/k be an abelian variety. Let $\Delta := (L^{\times 2} \cap E^\times)/E^{\times 2}$. Then*

$$\bigoplus_{D \in \Delta} A^D(E) \cong \bigoplus_{\xi \in \hat{G}_{L|E}} A(L)^\xi \sim A(L).$$

In particular $A(E(\sqrt{D})) \sim A(E) \oplus A^D(E)$ for $D \in E^\times \setminus E^{\times 2}$. One may rewrite this as $A(E(\sqrt{D}))/A(E) \sim A^D(E)$.

Proof. This is a consequence of 2.1 and a well-known purely algebraic theorem on modules over 2-groups (see [14, 15.5] for example). □

3. Specialization of generic twists

Let k be a number field and A/k an abelian variety. Let T be an indeterminate and $K := k(T)$. The quadratic twists of A_K are called **generic twists** of A in the sequel. One may think of such a generic twist $A^{D(T)}_K$, $D(T) \in K^\times$ as a 1-parameter family of abelian varieties. Specializing the variable T to a value $t \in \mathbb{P}_1(k)$ which is neither a pole nor a zero of $D(T)$ leads to a usual abelian variety $A^{D(t)}_k$ over k which is a quadratic twist of A. The following Theorem 3.1 is a quite immediate consequence of the specialization theorem of Silverman [20] (see also [9] and the account [2] of B. Conrad.).

Theorem 3.1. (Silverman, Conrad) *Suppose that $D(T) \in \mathrm{Adm}(k)$. Then there is a finite set $S \subset \mathbb{P}_1(k)$ which contains the zeros and poles of $D(T)$ such that*

$$\mathrm{rk}(A^{D(T)}(K)) \leq \mathrm{rk}(A^{D(t)}(k))$$

for all $t \in \mathbb{P}_1(k) \setminus S$. □

The main case of interest is the case where A is a hyperelliptic Jacobian.

Let A/k be an abelian variety and $D(T) \in \mathrm{Adm}(k)$. We will now give a description for the number $\mathrm{rk}(A^{D(T)}(K))$. Recall that the k-curve H_D is the smooth, projective model for the equation $Y^2 = D(T)$. The function field $R(H_D)$ of H_D is $K(\sqrt{D(T)})$.

Remark 3.2. *We have*

$$\begin{aligned} A^{D(T)}(K) &\sim A(R(H_D))/A(K) = A(R(H_D))/A(k) \cong \\ &\cong \mathrm{Mor}_k(H_D, A)/A(k) \sim \mathrm{Hom}_k(J_D, A) \end{aligned}$$

by 2.2, the fact [10, 3.8] *that $A(K) = A(k)$, the canonical isomorphism $A(R(H_D)) \cong \mathrm{Mor}_k(H_D, A)$ (recall that any rational map from a smooth curve C to an abelian variety B is defined on the whole of C) and Lemma 3.3 below. The case $A = J_f$, $f \in \mathrm{Adm}(k)$ is of particular importance.*

Lemma 3.3. *Let A/k be an abelian variety and C/k a geometrically regular, projective curve. Then* $\mathrm{Mor}_k(C, A)/A(k) \sim \mathrm{Hom}_k(J_C, A)$.

Proof. Note that $C(k)$ can be empty. Nevertheless $C(k^s) \neq \emptyset$. Hence, by the universal mapping property of J_C as Albanese variety of C (see [11, 6.1] and also [11, Section 1]), there is a G_k-linear epimorphism $\mathrm{Mor}_{k^s}(C_{k^s}, A_{k^s}) \to \mathrm{Hom}_{k^s}(J_{C,k^s}, A_{k^s})$ with kernel $A(k^s)$. Taking G_k-invariants one obtains an isomorphism

$$\varphi : (\mathrm{Mor}_{k^s}(J_{C,k^s}, A_{k^s})/A(k^s))^{G_k} \to \mathrm{Hom}_k(J_C, A).$$

Furthermore there is an exact Galois cohomology sequence

$$0 \to \mathrm{Mor}_k(C, A)/A(k) \xrightarrow{i} (\mathrm{Mor}_{k^s}(C_{k^s}, A_{k^s})/A(k^s))^{G_k} \to H^1(G_k, A(k^s))$$

and $H^1(G_k, A(k^s)) \otimes_{\mathbb{Z}} \mathbb{Q} = 0$. Hence $\varphi \circ i$ becomes an isomorphism when tensored with $\mathbb{Q}$. □

The main case of interest is the case where $A = J_f$, $f \in \mathrm{Adm}(k)$ is a hyperelliptic Jacobian. We will be interested in generic twists of high rank. The next remark gives some a priori information in this direction. Let $f \in \mathrm{Adm}(k)$. The generic twist $H_{f,K}^{f(T)}$ of H_f by $f(T)$ will be called the **generic eigentwist** of H_f. Note that the hyperelliptic curve $H_f^{f(T)}$ over

$K = k(T)$ is the smooth, projective model of the equation $f(T)Y^2 = f(X)$ and $J_f^{f(T)}$ is its Jacobian.

Remark 3.4. *It follows from Remark 3.2 that* $\mathrm{rk}(J_f^{f(T)}(K)) = \mathrm{rk}(\mathrm{End}_k(J_f))$ *for all* $f \in \mathrm{Adm}(k)$. *Furthermore* $\mathrm{rk}(\mathrm{End}_k(J_f)) \geq 1$ *provided* $g(H_f) \geq 1$.

The next remark suggests that one should search for useful twist polynomials for J_f among expressions of the form $f \circ g(T)$. For $f(X) \in \mathrm{Adm}(k)$ we define

$$\mathrm{Adm}_f(k) := \{g \in k(X)^\times - k^\times | f \circ g \in \mathrm{Adm}(k)\}.$$

Remark 3.5. *Let* $f \in \mathrm{Adm}(k)$ *and* $g \in \mathrm{Adm}_f(k)$. *Then there is an abelian variety* B/k *such that* $J_{f\circ g} \sim J_f \times B$ *and* $\mathrm{rk}(J_f^{f\circ g}(K)) \geq \mathrm{rk}(J_f^f(K))$.

Proof. The obvious k-algebra monomorphism

$$\alpha : k(X, \sqrt{f(X)}) \to k(X, \sqrt{f \circ g(X)})$$

induces a finite morphism $H_{f\circ g} \to H_f$. Hence there is a splitting $J_{f\circ g} \sim J_f \times B$. Thus

$$\mathrm{rk}(J_f^{f\circ g}(K)) = \mathrm{rk}(\mathrm{Hom}_k(J_{f\circ g}, J_f)) \geq \mathrm{rk}(\mathrm{End}_k(J_f)) = \mathrm{rk}(J_f^{f(T)}(K)),$$

by 3.2 and 3.4. □

4. Counting functions

Let k be a number field and A/k an abelian variety. For $d, a \in k^\times$ we have $A^d \cong A^{da^2}$ (compare the definition of A^d). Hence for $D \in k^\times/k^{\times 2}$ the expression A^D is well-defined (at least as an isomorphism class). Let $\Delta_k := k^\times/k^{\times 2}$. The main object of interest in this note is the question whether the subset

$$\Delta_{k,R}(A) := \{D \in \Delta_k | \mathrm{rk}(A^D(k)) \geq R\}$$

of Δ_k is infinite. Throughout this note we use the following terminology:

We shall say that A *has infinitely many quadratic twists of rank* $\geq R$ *if and only if* $\Delta_{k,R}(A)$ *is an infinite set. Similarly, for a hyperelliptic curve* H/k, *we say that* H *has infinitely many quadratic twists of rank* $\geq R$ *iff* $\Delta_{k,R}(J_H)$ *is infinite.*

Note that obviously isomorphic twists A^d and A^{da^2} are only counted once in the sequel. It will be important to study the following image modulo

$k^{\times 2}$ of a function $D(T) \in \mathrm{Adm}(k)$

$$B(D) := \{\overline{D(x)} | x \in \mathbb{P}_1(k) \text{ neither a pole nor a zero of } D\} \subset \Delta_k.$$

Here we write $\overline{a}$ for the image of $a \in k^\times$ in Δ_k.

Lemma 4.1. *The set $B(D)$ is infinite.*

Proof. This uses a standard argument which is built on the Hilbert irreducibility theorem (see [9] and [13, 2.5]). □

In the special case $k = \mathbb{Q}$ we can define a counting function which can be used to measure the size of a subset of $\Delta_\mathbb{Q}$. Denote by $\mathcal{S} \subset \mathbb{Z} \setminus \{0\}$ the set of squarefree integers and define $\mathcal{S}(x) = \{s \in \mathcal{S} : \ |s| \leq x\}$ for $x \in \mathbb{R}$. Note that $\mathcal{S}$ is a system of representatives for $\Delta_\mathbb{Q} = \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. If $\Delta' \subset \Delta_\mathbb{Q}$ is an arbitrary subset, then we use the counting function

$$\nu(\Delta', x) := |\{s \in \mathcal{S}(x) | \overline{s} \in \Delta'\}|$$

to measure the size of Δ'. For non-negative functions h_1, h_2 on $[0, \infty)$ we shall write $h_1 \ll h_2$ if there are constants $C, D > 0$ such that $h_1(x) \leq Ch_2(x)$ for all $x \geq D$. Furthermore we shall write $h_1 \sim h_2$ provided $|h_1 - h_2|$ is bounded.

Let $A/\mathbb{Q}$ be an abelian variety. We are mainly interested in the counting function

$$\delta_R(A, x) := \nu(\Delta_{\mathbb{Q},R}(A), x) = |\{d \in \mathcal{S}(x) | \mathrm{rk}(A^d(\mathbb{Q})) \geq R\}|.$$

If A has infinitely many quadratic twists of rank $\geq R$, then $\lim\limits_{x \to \infty} \delta_R(A, x) = \infty$ and we will look for asymptotic lower bounds of $\delta_R(A, x)$ as $x \to \infty$. In the derivation of these lower bounds the counting function

$$b(D(T), x) := \nu(B(D), x),$$

$D(T) \in \mathrm{Adm}(k)$ will play a key role.

Note that the question on asymptotic lower bounds $b(D, x)$ more or less comes down to a difficult question in elementary number theory not involving curves, Jacobians, ranks and so forth. The question is simply: How many different classes mod $\mathbb{Q}^{\times 2}$ occur in the image of the rational function $D(T)$?

Theorem 4.2. *Let A/k be an abelian variety and $D(T) \in \mathrm{Adm}(k)$. Let $R := \mathrm{rk}(A^{D(T)}(k(T)))$ be the rank of the corresponding generic twist of A. (Recall from 3.2 that $R = \mathrm{rk}(\mathrm{Hom}_k(J_D, A))$.)*

(1) *If $J_D \sim A^r \times B$ for some abelian variety B/k then $R \geq r \cdot \mathrm{rk}(\mathrm{End}_k(A))$.*

(2) *The abelian variety A has infinitely many quadratic twists of rank $\geq R$.*
(3) *If $k = \mathbb{Q}$, then $\delta_R(A, x) \gg b(D, x)$ as $x \to \infty$.*

The case where $A = J_f$, $f \in \mathrm{Adm}(k)$ is a hyperelliptic Jacobian is of particular interest.

Proof. The first statement is obvious - we just recalled it because of its importance.

By 3.1 there is a finite subset $S \subset \Delta_k$ such that $B(D) \setminus S \subset \Delta_{k,R}(A)$. Now $B(D)$ is infinite by the Lemma 4.1 above. Hence A has infinitely many quadradic twists of rank $\geq R$.

Now suppose that $k = \mathbb{Q}$. It follows that

$$b(D, x) \sim \nu(B(D) \setminus S, x) \ll \delta_R(A, x),$$

as desired. □

Of course the theorem is of use only if $\mathrm{rk}(A^{D(T)}(K)) > 0$. Consider the important special case where $A = J_f$, $f \in \mathrm{Adm}(k)$. One can then apply the theorem with $D = f$, that is, in the case of the generic eigentwist. The following corollary is an immediate consequence of Corollary 3.4 and Theorem 4.2.

Corollary 4.3. *Let $f(X) \in \mathrm{Adm}(k)$. Suppose that $g(H_f) \geq 1$. Let $R := \mathrm{rk}(\mathrm{End}_k(J_f))$. Then $R \geq 1$ and H_f has infinitely many quadratic twists of rank $\geq R$. Furthermore*

$$\delta_R(J_f, x) \gg b(f, x)$$

as $x \to \infty$, provided $k = \mathbb{Q}$.

In 4.2 and 4.3 above and in the forthcoming Theorems 5.2, 7.4, 8.4, 8.8 a function of the form $b(D, x)$, $D \in \mathrm{Adm}(\mathbb{Q})$ occurs as an asymptotic lower bound for a function $\delta_R(A, x)$ we are really interested in. Thus information on the asymptotic behavior of $b(D, x)$ is interesting in connection with these theorems. There is a vast literature on the asymptotic behavior of $b(D, x)$, see [7], [5] and [21]. We quote a strong theorem[3] due to Stewart and Top from their paper [21] in order to make Theorems 4.2, 4.3, 5.2, 7.4, 8.4, 8.8 more explicit.

[3]For simplicity we do not restate the result in the sharpest form possible.

Let $D(T) \in \mathrm{Adm}(\mathbb{Q})$ be a squarefree polynomial of degree $d \geq 3$. Let

$$\varepsilon(D) := \min(\{a \,|\, a \in \mathbb{N}, 2a \geq d\})^{-1}.$$

Theorem 4.4. (Stewart and Top)

(1) *We have* $b(D,x) \gg x^{\varepsilon(D)} \log(x)^{-2}$ *as* $x \to \infty$.
(2) *If* $D(T)$ *splits into linear factors, then* $b(D,x) \gg x^{\varepsilon(D)}$ *as* $x \to \infty$.

Proof. This is an immediate consequence of Theorems 1 and 2 of [21]. □

5. The generic eigentwist

Let k be a number field. In the light of 4.3 it is interesting to construct $f \in \mathrm{Adm}(k)$ for which the rank of the generic eigentwist $\mathrm{rk}(J_f^{f(T)}(k(T))) = \mathrm{rk}(\mathrm{End}_k(J_f))$ is large. Note that there is a natural upper bound for the rank of the generic eigentwist in terms of the genus g_f of H_f as $\mathrm{rk}(\mathrm{End}_k(J_f)) \leq 4g_f^2$ by [10, 12.5].

Let $h(X) \in \mathrm{Adm}(k)$ be a monic, squarefree polynomial of degree 3. Suppose that $h(0) \neq 0$. (We can take $h(X) = X^3 - 1$ for example.) Let $f_r(X) := h(X^{2^r})$. Let $C_r := H_{f_r}$ and $A_r := J_{f_r}$. Note that C_0 is an elliptic curve. Clearly f_r is a monic, squarefree polynomial of degree $2^r \cdot 3$. For $r \geq 1$ the genus of C_r satisfies $g(C_r) = 2^{r-1} \cdot 3 - 1$. (One computes the ramification of $C_r(\overline{k}) \to \mathbb{P}_1(\overline{k})$ and applies the Hurwitz genus formula to see this. Compare 6.6 below.)

Proposition 5.1. *There are abelian varieties* B_i *over* k *with the following properties.*

(1) *The dimensions are given by* $\dim(B_0) = \dim(B_1) = 1$ *and* $\dim(B_r) = 2^{r-2} \cdot 3$ *for* $r \geq 2$.
(2) *There is an isogeny* $A_r \sim B_0 \times B_1 \times \cdots \times B_r$ *for all* r.

Proof. Let $B_0 = A_0$. Obviously $f_{r+1}(X) = f_r(X^2)$. By 3.4 there is a finite morphism $C_{r+1} \to C_r$. Hence there is a decomposition $A_{r+1} \sim A_r \times B_{r+1}$ with some abelian variety B_{r+1}, and B_{r+1} must have dimension $g(C_{r+1}) - g(C_r)$. The two assertions are immediate from that. □

Theorem 5.2. *The rank of the generic eigentwist of* C_r *is*

$$\mathrm{rk}(A_r^{f_r}(k(T))) = \mathrm{rk}(\mathrm{End}_k(A_r)) \geq r + 1.$$

Hence $C_r = H_{f_r}$ *has infinitely many twists of rank* $\geq r + 1$. *Furthermore, if* $k = \mathbb{Q}$, *then* $\delta_{r+1}(A_r, x) \gg b(f_r, x)$ *and* $b(f_r, x) \to \infty$.

See Theorem 4.4 for information on the asymptotic behavior of $b(f_r, x)$.

Proof. It follows from the decomposition $A_r \sim B_0 \times B_1 \times \cdots \times B_r$ that $\mathrm{rk}(\mathrm{End}_k(J_r)) \geq r+1$. The rest is a consequence of 4.3. □

By the above result, there is a hyperelliptic curve C_r for any r which admits infinitely many quadratic twists of rank $\geq r+1$. Unfortunately in our example the genus $g(C_r)$ grows exponentially with r.

6. Kummer extensions of $\mathbb{P}_1$

Let k be a number field. In view of Theorem 4.2 it seems natural to study the following question: Given (possibly equal) hyperelliptic curves $C_1, C_2, \cdots, C_s$ over k, is there a hyperelliptic curve C/k such that $J_C \sim J_{C_1} \times \cdots \times J_{C_s} \times B$ for some abelian variety B/k? As mentioned in the introduction, this seems to be a very difficult question. Nevertheless it is quite easy to construct a Kummer extension $T \to \mathbb{P}_1$ of exponent 2 and degree 2^s such that $J_T \sim J_{C_1} \times \cdots \times J_{C_s} \times B$ for some B/k. Under certain very restrictive hypotheses one can show that this Kummer extension T, to be constructed below, is hyperelliptic again (that is admits a degree 2 morphism to $\mathbb{P}_1$.)

Let $K = k(X)$ be the function field of $\mathbb{P}_1$ and consider a finite subgroup $\Delta \subset K^\times/K^{\times 2}$. Suppose that $K(\sqrt{\Delta})|k$ is a regular extension. Such subgroups will be called **admissible** in the sequel. Denote by $H_{\Delta,k}$ (or by H_Δ) the normalization of $\mathbb{P}_1$ in $K(\sqrt{\Delta})$. Then H_Δ is a geometrically regular k-curve. There is a canonical map $p : H_\Delta \to \mathbb{P}_1$ of degree $|\Delta|$ and this map is a Galois cover with Galois group isomorphic to Δ. Furthermore J_Δ stands for the Jacobian variety of H_Δ. Note that these definitions are in a sense compatible with the definitions in Section 2: If $f \in \mathrm{Adm}(k)$, then the group $\langle \overline{f} \rangle \subset K^\times/K^{\times 2}$ genenrated by $\overline{f}$ is admissible, $H_f = H_{\langle \overline{f} \rangle}$ is the smooth projective model of $Y^2 = f(X)$ and $J_f = J_{\langle \overline{f} \rangle}$ is the Jacobian of H_f. For an abelian variety A/k and $D \in k^\times$ the definiton of A^D from Section 2 is still in force.

Theorem 6.1. *There is a k-isogeny $J_\Delta \sim \prod_{d \in \Delta} J_d$ for any admissible subgroup $\Delta \subset K^\times/K^{\times 2}$.*

Proof. Let A be an arbitrary abelian variety. Then the homomorphism

$$\bigoplus_{d \in \Delta} A(K(\sqrt{d}))/A(K) \to A(K(\sqrt{\Delta}))/A(K)$$

becomes an isomorphism when tensored with $\mathbb{Q}$ by 2.2. Furthermore the canonical map

$$A(K(\sqrt{\Delta}))/A(K) \to \mathrm{Hom}(J_\Delta, A)$$

becomes an isomorphism when tensored with $\mathbb{Q}$. (Indeed, the left hand side is isomorphic to $\mathrm{Mor}_k(H_\Delta, A)/A(k)$ as every rational map from a smooth variety V to an abelian variety is defined on the whole of V. Furthermore $\mathrm{Mor}_k(H_\Delta, A)/A(k) \sim \mathrm{Hom}(J_\Delta, A)$ by 3.3.) This shows that the canonical homomorphism

$$\bigoplus_{d\in\Delta} \mathrm{Hom}_k(J_d, A) \to \mathrm{Hom}_k(J_\Delta, A)$$

becomes an isomorphism when tensored with $\mathbb{Q}$. Furthermore

$$\bigoplus_{d\in\Delta} \mathrm{Hom}_k(J_d, A) \cong \mathrm{Hom}_k(\prod_{d\in\Delta} J_d, A).$$

Hence there is a natural isomorphism between the functors $\mathrm{Hom}_k^0(J_\Delta, -)$ and $\mathrm{Hom}_k^0(\prod_{d\in\Delta} J_d, -)$ from IsAb_k to the category of $\mathbb{Q}$-vector spaces. By Yoneda's Lemma, J_Δ and $\prod_{d\in\Delta} J_d$ must be isomorphic as objects of IsAb_k. □

Remark 6.2. *In the situation of Theorem 6.1, let* Γ *be a subgroup of* Δ *of index* 2. *Let* $f \in \Delta \setminus \Gamma$.

(1) *The field inclusion* $K(\sqrt{\Gamma}) \subset K(\sqrt{\Delta})$ *induces a degree* 2 *morphism* $H_\Delta \to H_\Gamma$.
(2) *Suppose that* $K(\sqrt{\Gamma}) = k(U)$ *is a rational function field. (Unfortunately this happens only very rarely.) Then* $H_\Gamma \cong \mathbb{P}_1$ *and* H_Δ *is a hyperelliptic curve. Furthermore there is a rational expression* $r(U)$ *such that* $X = r(U)$ *(recall* $K = k(X)$*) and*

$$K(\sqrt{\Delta}) = K(\sqrt{\Gamma}, \sqrt{f}) = k(U, \sqrt{f \circ r(U)}).$$

In particular there is a k*-isomorphism* $H_{f\circ r} \cong H_\Delta$ *and a* k*-isogeny* $J_{f\circ r} \sim \prod_{d\in\Delta} J_d$. *(*$J_d = 0$ *for* $d \in \Gamma$.*)*

We are naturally led to the following question: Under which (restrictive) hypothesis is $K(\sqrt{\Gamma})$ a rational function field? There is the following general criterion.

Remark 6.3. *Let* C/k *be a geometrically regular, projective curve. Then the following statements are equivalent.*

(1) *The function field* $R(C)$ *is a rational function field.*
(2) *There is a* k*-isomorphism* $C \cong \mathbb{P}_1$.

(3) *The genus of C is zero and $C(k) \neq \emptyset$.*

We thus need a formula for the genus of a curve H_Δ where $\Delta \subset K^\times/K^{\times 2}$ is an admissible subgroup. We will now briefly describe the ramification behavior of the projection $p : H_\Delta \to \mathbb{P}_1$ and then compute the genus of H_Δ by the Hurwitz formula. For $P \in \mathbb{P}_1(\overline{k})$, the valuation $v_P : \overline{k}(X)^\times \to \mathbb{Z}$ induces a homomorphism $\overline{v}_P : k(X)^\times/k(X)^{\times 2} \to \mathbb{Z}/2$. Let

$$S(\Delta) := \{P \in \mathbb{P}_1(\overline{k}) \,|\, \exists d \in \Delta : \overline{v}_P(d) \neq 0\}$$

and $s(\Delta) := |S(\Delta)|$.

Proposition 6.4. *Let $P \in \mathbb{P}_1(\overline{k})$. Then*

$$|\{Q \in H_\Delta(\overline{k}) \,|\, p(Q) = P\}| = \begin{cases} |\Delta| & P \notin S(\Delta), \\ |\Delta|/2 & P \in S(\Delta). \end{cases}$$

Thus $S(\Delta)$ is the ramification locus of p and each $P \in S(\Delta)$ has ramification index 2.

Proof. Note that $2 \in k^\times$ is a unit in each local ring of $\mathbb{P}_1$. The proposition hence follows from general facts on the ramification behavior of a discrete valuation ring in an exponent 2 Kummer extension of its quotient field. □

Corollary 6.5. *The genus of H_Δ is given by $g(H_\Delta) = 1 + |\Delta|(\frac{s(\Delta)}{4} - 1)$.*

Proof. By 6.4 the ramification divisor $R \in \mathrm{Div}(H_{\Delta,\overline{k}})$ has degree $s(\Delta)\frac{|\Delta|}{2}$. The Corollary is now immediate from the Hurwitz formula. □

Corollary 6.6. *We have $g(H_f) = \frac{1}{2}s(\langle f \rangle) - 1$ for $f \in \mathrm{Adm}(k)$.*

Remark 6.7.

(1) *If $l(X) = aX + b \in k[X]$ is a linear polynomial and $U = \sqrt{l}$, then $k(X, \sqrt{l}) = k(U)$ is a rational function field and $X = \frac{U^2 - b}{a}$.*

(2) *Let $l_1(X), l_2(X) \in k[X]$ be linear polynomials which are k-linearly independent. Then the subgroup $\Delta \subset K^\times/K^{\times 2}$ generated by l_1 and l_2 is admissible and of order 4. Furthermore $S(\Delta) = \{\infty, a_1, a_2\}$ where a_i is the root of l_i. Thus $s(\Delta) = 3$ and $g(H_\Delta) = 0$. If there is a solution $(t, s_1, s_2) \in k^3$ of the equations $l_1(t) = s_1^2$, $l_2(t) = s_2^2$, then the function*

$$U := \frac{\sqrt{l_1(X)} - s_1}{\sqrt{l_2(X)} - s_2} \in R(H_\Delta) = k(X, \sqrt{l_1}, \sqrt{l_2})$$

has a simple pole and a simple zero and hence defines an isomorphism $H_\Delta \to \mathbb{P}_1$. Then $k(X, \sqrt{l_1}, \sqrt{l_2}) = k(U)$ and there is a rational expression r_{l_1,l_2} such that $X = r_{l_1,l_2}(U)$.

(3) *Let* $\Delta \subset k(X)^\times/k(X)^{\times 2}$ *be an admissible subgroup. If* $|\Delta| \geq 8$ *or if* Δ *contains the class of a squarefree polynomial of degree* ≥ 3*, then* $s(\Delta) > 4$ *and* $g(H_\Delta) \geq 1$.

7. Construction of useful generic twists: rank 2.

Let k be a number field and $K = k(T)$. If $f \in \mathrm{Adm}(k)$ and $H_f(k) \neq \emptyset$, then the generic eigentwist has rank

$$\mathrm{rk}(J_f^{f(T)}(K)) = \mathrm{rk}(\mathrm{End}_k(J_f)) \geq 1.$$

(Recall 3.2.) Sometimes one can achieve better results when considering other generic twists. In this section we construct examples of $f(X), D(T) \in \mathrm{Adm}(k)$ such that $J_D \sim J_f^2 \times B$ for some abelian variety B/k and consequently

$$\mathrm{rk}(J_f^{D(T)}(K)) \geq 2 \cdot \mathrm{rk}(\mathrm{End}_k(J_f)).$$

The author learned the main ideas used in this construction from the papers [15], [16], [17] of Rubin and Silverberg.

Theorem 7.1. *Let* $f \in \mathrm{Adm}(k)$ *and* $g_1, \cdots, g_s \in \mathrm{Adm}_f(k)$*. Let* $k_1, \cdots, k_s \in \mathrm{Adm}(k)$*. Suppose that*

$$f(g_i(T)) \cdot f(T) \in k_i(T)K^{\times 2}$$

for all i*. Let* $\Delta \subset K^\times/K^{\times 2}$ *be the subgroup generated by* $\{f(T), k_1(T), \cdots, k_s(T)\}$ *and* Γ *the subgroup of* Δ *generated by* $\{k_1(T), \cdots, k_s(T)\}$*. Suppose that* Δ *is admissible of order* 2^{s+1}*.*

(1) *There is an abelian variety* B/k *such that* $J_\Delta \sim J_f^{s+1} \times B$.
(2) *Furthermore* $\mathrm{rk}(J_f^{f(T)}(K(\sqrt{\Gamma}))) \geq (s+1)\mathrm{rk}(\mathrm{End}_k(J_f))$.

Proof. We have $J_\Delta \sim \prod_{d \in \Delta} J_d$ by 6.1. Δ contains the set $\{f, f \circ g_1, f \circ g_2, \cdots f \circ g_s\}$ of order $s+1$, as $k_i(T)f(T) \in f \circ g_i(T)K^{\times 2}$ by hypothesis. Hence J_Δ must contain $J_f \times \prod_{i=1}^s J_{f \circ g_i}$ as an isogeny factor. Furthermore $J_{f \circ g_i}$ contains J_f as an isogeny factor, because there is a finite morphism $H_{f \circ g_i} \to H_f$ by 3.5. The first assertion follows readily from that.

To prove the second assertion we use 2.2 and 3.5 to compute

$$\begin{aligned}\mathrm{rk}(J_f^{f(T)}(K(\sqrt{\Gamma}))) &\geq \mathrm{rk}(J_f^{f(T)}(K)) + \sum_{i=1}^{s} \mathrm{rk}(J_f^{f(T)k_i(T)}(K) = \\ &= \mathrm{rk}(J_f^{f(T)}(K)) + \sum_{i=1}^{s} \mathrm{rk}(J_f^{f(g_i(T))}(K) \geq \\ &\geq (s+1)\cdot \mathrm{rk}(J_f^{f(T)}(K))\end{aligned}$$

and use $\mathrm{rk}(J_f^{f(T)}(K)) = \mathrm{rk}(\mathrm{End}_k(J_f))$. □

Corollary 7.2. *Suppose in addition that $K(\sqrt{\Gamma}) = k(U)$ is a rational function field*[4]*. Then there is a rational expression r such that $r(U) = T$. (Recall $K = k(T)$.)*

(1) *There is an abelian variety B/k such that $J_{f\circ r} \sim J_\Delta \sim J_f^{s+1} \times B$.*
(2) *Furthermore* $\mathrm{rk}(J_f^{f(r(U))}(k(U)) \geq (s+1)\mathrm{rk}(\mathrm{End}_k(J_f))$.

Proof. The first statement follows from Theorem 7.1 and Remark 6.2.

The second statement follows from the first and the fact 3.2 that

$$J_f^{f(r(U))}(k(U)) \sim \mathrm{Hom}_k(J_{f\circ r}, J_f).$$

Alternatively one can use part (2) of 7.1 to prove the second statement. □

We need to produce relations of the form $f(g(T)) \in k(T)K^{\times 2}$ with $k(T)$ a linear polynomial in order to apply the above results. We will identify $\mathrm{PGL}(k) := \mathrm{GL}_2(k)/k^\times$ with the automorphism group of $\mathbb{P}_1$ in the sequel. The matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ corresponds to the automorphism $X \mapsto \frac{aX+b}{cX+d}$. Thus $\mathrm{PGL}(k)$ operates on $\mathbb{P}_1(k)$ and also on $\mathbb{P}_1(\overline{k})$.

Lemma 7.3. *Let $f(T) \in k[T]$ be a monic, squarefree polynomial of odd degree d. Let $\sigma(T) \in \mathrm{PGL}(k)$ be an automorphism which permutes the roots of f. Suppose that $\sigma(T)$ does not have a pole at ∞. Then there is a linear polynomial $l(T) = f(\sigma(\infty))(T - \sigma^{-1}(\infty))$ such that*

$$f(\sigma(T)) \cdot f(T) \in l(T)K^{\times 2}.$$

Proof. We claim that

$$f(\sigma(T)) = f(\sigma(\infty))(T - \sigma^{-1}(\infty)))^{-d} f(T).$$

[4]As mentioned before, this rarely happens.

To see this, note that both sides of the equation have the same divisor and evaluate to $f(\sigma(\infty))$ at ∞. This implies $f(\sigma(T)) \cdot f(T) \in l(T)K^{\times 2}$ as d is odd. □

Theorem 7.4. *Let $f(X) \in k[X]$ be a monic, squarefree polynomial of odd degree d. Suppose that there is an automorphism $\sigma(X) \in \mathrm{PGL}(k)$ which permutes the roots of f. Suppose furthermore that $\sigma(X)$ does not have a pole at ∞. Let $D(T) = f(\frac{T^2}{f(\sigma(\infty))} + \sigma^{-1}(\infty))$.*

(1) *There is a k-isogeny $J_D \sim J_f \times J_f$.*
(2) *We have $\mathrm{rk}(J_f^{D(T)}(K)) = 2 \cdot \mathrm{rk}(\mathrm{End}_k(J_f))$.*
(3) *Let $R = 2 \cdot \mathrm{rk}(\mathrm{End}_k(J_f))$. Then H_f has infinitely many quadratic twists of rank $\geq R$. Furthermore, if $k = \mathbb{Q}$, then $\delta_R(J_f, x) \gg b(D, x)$. See Theorem 4.4 for information on the asymptotic behavior of $b(D, x)$.*

Proof. Let $l(T) = f(\sigma(\infty))(T - \sigma^{-1}(\infty))$. Then $f(T) \cdot f(\sigma(T)) \in l(T)K^{\times 2}$ by 7.3. The subgroup $\Delta \subset K^\times$ generated by $f(T)$ and $l(T)$ is admissible of order 4. Let Γ be the subgroup of Δ generated by $l(T)$. If we let $U := \sqrt{l(T)}$, then $K(\sqrt{\Gamma}) = k(U)$ is a rational function field and $T = \frac{U^2}{f(\sigma(\infty))} + \sigma^{-1}(\infty)$ by 6.7. By 7.2 there is an isogeny $J_D \sim J_f^2 \times B$ with an abelian variety B/k. By 6.6 we have $\dim(J_f) = \frac{d-1}{2}$. Furthermore $D(T)$ is of degree $2d$ and thus $\dim(J_D) = d - 1$. This shows that $\dim(B) = 0$. The first statement is clear from that. The second statement follows from the first. The rest is an immediate consequence of 4.2. □

Remark 7.5. *One can explicitly construct polynomials $f(X) \in \mathrm{Adm}(k)$ which meet the hypothesis of the theorem as follows: Start with an automorphism $\sigma \in \mathrm{PGL}(k)$ of finite order which has a k-rational fixed point and which does not have a pole at ∞. There are plenty of choices for such σ. Then choose pairwise different orbits $B_1, \cdots, B_s \subset \mathbb{P}_1(k)$ of σ such that no B_i contains ∞ and such that $\sum |B_i|$ is odd. This is possible as there is an orbit of order 1. Then the polynomial*

$$f(X) = \prod_{i=1}^{s} \prod_{a \in B_i} (X - a)$$

is monic, squarefree and of odd degree and σ permutes the roots of f.

We go through an explicit example.

Example. Suppose that k is a number field. We shall work with the automorphism $\sigma(X) = 1/X$ in this example. It is of order 2, has a zero

at ∞ and a pole at zero and its fixed points are 1 and -1. Let $s \in \mathbb{N}$ and $s \geq 2$. Then σ permutes the roots of the monic, squarefree polynomial

$$f(X) = (X+1)(X-2)(X-\frac{1}{2})(X-3)(X-\frac{1}{3})\cdots(X-s)(X-\frac{1}{s}).$$

The degree of f is visibly odd. Furthermore $f(\sigma(\infty)) = f(0) = 1$. Hence, by the theorem,

$$\mathrm{rk}(J_f^{f(T^2)}(k(T)) = 2 \cdot \mathrm{rk}(\mathrm{End}_k(J_f)).$$

In particular H_f has infinitely many quadratic twists of rank $\geq 2 \cdot \mathrm{rk}(\mathrm{End}_k(J_f))$. Moreover $J_{f(T^2)} \sim J_f \times J_f$. The author speculates that $\mathrm{End}_k(J_f))$ is $\mathbb{Z}$, but he has not checked it. □

8. Construction of useful generic twists: rank 3.

Let k be a number field and $K = k(T)$. In this section we construct examples of $f(X), D(T) \in \mathrm{Adm}(k)$ such that $J_D \sim J_f^3 \times B$ for some abelian variety B and

$$\mathrm{rk}(J_f^D(k(T))) \geq 3 \cdot \mathrm{rk}(\mathrm{End}_k(J_f)).$$

The construction is analoguous to the construction of Rubin and Silverberg in [15, Section 4].

Let $G \subset \mathrm{PGL}(k)$ be a *finite* subgroup. If $b \in \mathbb{P}_1(k)$ and $b \notin G \cdot \infty$, then we define

$$f_{G,b}(X) = \prod_{\sigma \in G} (X - \sigma(b)).$$

Note that $f_{G,b}$ is squarefree iff $|G \cdot b| = |G|$. Furthermore we define

$$f^-_{G,b}(X) = \prod_{c \in Gb} (X - c).$$

Note that $f^-_{G,b}(X)$ is a squarefree divisor of $f_{G,b}(X)$ and that $f^-_{G,b}(X) = f_{G,b}(X)$ iff $|G \cdot b| = |G|$. One can show that $|G \cdot b| < |G|$ only for finitely many b.

Proposition 8.1. *Let $\eta \in G$. Suppose that $\eta(\infty) \neq \infty$.*

1. *The quantity $f_{G,b}(\eta(\infty))$ does not depend on b.*
2. *If there is a $c \in \mathbb{P}_1(k) \setminus G \cdot \infty$ whose orbit $G \cdot c$ has length $|G|/m$, then $f_{G,b}(\eta(\infty)) \in k^{\times m}$ is an m-th power.*

Proof. We view

$$f_{G,b}(\eta(\infty)) = \prod_{\sigma\in G} (\eta(\infty) - \sigma(b)) \in k(b)$$

as a rational function in a variable b. Its divisor

$$\sum_{\sigma\in G} (\sigma^{-1}\eta(\infty) - \sigma^{-1}(\infty)) = 0$$

is zero. Hence $f_{G,b}(\eta(\infty))$ does not depend on b.

Suppose that there is a $c \in \mathbb{P}_1(k) \setminus G\cdot\infty$ whose orbit $G\cdot c$ has length $|G|/m$. Then

$$f_{G,b}(\eta(\infty)) = f_{G,c}(\eta(\infty)) = \prod_{\sigma\in G} (\eta(\infty) - \sigma(c))$$

is an m-th power as any factor occurs m times in the product. □

We will now specialize to a subgroup $G \cong S_3$ of $\mathrm{PGL}(k)$. Let $\lambda \in k\setminus\{0,1\}$ and consider the automorphisms

$$\sigma(X) = \frac{\lambda^2 X - \lambda^2}{(2\lambda-1)X - \lambda^2} \quad \text{and} \quad \eta(X) = \frac{-X+\lambda}{(\lambda-2)X+1}.$$

The map σ switches 0 and 1 and has λ as a fixed point. η swiches 0 and λ and has 1 as a fixed point. Let G be the subgroup of $\mathrm{PGL}(k)$ generated by η and σ. Then G is isomorphic to the symmetric group S_3. Let $b_1, \cdots, b_s \in \mathbb{P}_1(k) \setminus G\cdot\infty$ and assume $|G\cdot b_i| = 6$ for all i. Suppose that $G\cdot b_i \neq G\cdot b_j$ for $i \neq j$. Consider the squarefree polynomial

$$f(X) = f^-_{G,\lambda}(X) f_{G,b_1}(X)\cdots f_{G,b_s}(X).$$

Lemma 8.2. (1) *Let* $l_\sigma(X) := \lambda(1-\lambda)((2\lambda-1)X - \lambda^2)$. *Then*

$$f(X)f(\sigma(X)) \in l_\sigma(X)k(X)^{\times 2}.$$

(2) *Let* $l_\eta(X) := (1-\lambda)((\lambda-2)X+1)$. *Then* $f(X)f(\eta(X)) \in l_\eta(X)k(X)^{\times 2}$. *Note that* $l_\sigma(X)$ *and* $l_\eta(X)$ *do not depend on the* b_i. *But they do depend on* λ.

Proof. We have $f^-_{G,\lambda}(X) = X(X-1)(X-\lambda)$ and a straightforward computation yields

$$f^-_{G,\lambda}(\sigma(\infty)) = f^-_{G,\lambda}\left(\frac{\lambda^2}{2\lambda-1}\right) = \lambda(1-\lambda)(2\lambda-1) \bmod k^{\times 2}$$

and

$$f^-_{G,\lambda}(\eta(\infty)) = f^-_{G,\lambda}\left(-\frac{1}{\lambda-2}\right) = (1-\lambda)(\lambda-2) \bmod k^{\times 2}.$$

Furthermore we have

$$f(\tau(\infty)) = f^-_{G,\lambda}(\tau(\infty)) \cdot \prod_{i=1}^{s} f_{G,b_i}(\tau(\infty)) = f^-_{G,\lambda}(\tau(\infty)) \bmod k^{\times 2}$$

for all $\tau \in G$ which do not have a pole at ∞. Indeed, any factor $f_{G,b_i}(\tau(\infty))$ is a square by 8.1, as G has an orbit $\{0, 1, \lambda\}$ of order 3.

Clearly $f(X)$ is of odd degree and the elements of G permute the roots of f. Hence, by 7.3, we obtain

$$f(X) \cdot f(\tau(X)) \in f(\tau(\infty))(X - \tau^{-1}(\infty))k(X)^{\times 2}$$

for all $\tau \in G$ which do not have a pole at ∞. Putting these equations together we compute

$$f(X)f(\sigma(X)) = \lambda(1-\lambda)(2\lambda-1)\left(X - \frac{\lambda^2}{2\lambda-2}\right) = l_\sigma(X) \bmod k(X)^{\times 2}$$

and

$$f(X)f(\eta(X)) = (1-\lambda)(\lambda-2)\left(X - \frac{1}{\lambda-2}\right) = l_\eta(X) \bmod k(X)^{\times 2},$$

as desired. □

Lemma 8.3. *Suppose that there is an $a \in k^\times$ such that $\lambda = -2a^2$. Let*

$$U := \frac{\sqrt{l_\sigma(T)} - a(\lambda-1)}{\sqrt{l_\eta(T)} - a(\lambda-1)}$$

Then $k(T, \sqrt{l_\sigma(T)}, \sqrt{l_\eta(T)}) = k(U)$ is a rational function field. In particular there is a rational expression r_{l_σ,l_η} such that $T = r_{l_\sigma,l_\eta}(U)$.

Proof. Note that $l_\sigma(\frac{\lambda+1}{2}) = a^2(\lambda-1)^2$ is a square and $l_\eta(\frac{\lambda+1}{2}) = a^2(\lambda-1)^2$ is a square as well. The assertion follows from Remark 6.7. □

We want to mention that the statement of the above Lemma 8.3 is included in the proof of [15, Theorem 4.1, p. 7]. In this paper Rubin and Silverberg even determine the rational expression r_{l_σ,l_η} explicitly.

Theorem 8.4. *Suppose that there is an $a \in k^\times$ such that $\lambda = -2a^2$. Let $D(U) = f(r_{l_\sigma,l_\eta}(U))$.*

(1) *There is an abelian variety B/k such that $J_D \sim J_f^3 \times B$.*
(2) *We have* $\mathrm{rk}(J_f^{D(U)}(k(U))) \geq 3 \cdot \mathrm{rk}(\mathrm{End}_k(J_f))$.

(3) *Let* $R := 3 \cdot \mathrm{rk}(\mathrm{End}_k(J_f))$. *Then* H_f *has infinitely many quadratic twists of rank* $\geq R$. *Furthermore, if* $k = \mathbb{Q}$, *then* $\delta_R(J_f, x) \gg b(D, x)$ *and* $b(D, x) \to \infty$. *See Theorem 4.4 for information on the asymptotic behavior of* $b(D, x)$.

Proof. The subgroup $\Delta \subset K^\times/K^{\times 2}$ generated by f, l_σ and l_η is admissible of order 8. The subgroup Γ of Δ generated by l_σ and l_η is of order 4 and $K(\sqrt{\Gamma}) = k(U)$ is a rational function field by Lemma 8.3 above. Furthermore $T = r_{l_\sigma, l_\eta}(U)$. The first two statements follow by 8.2 and 7.2. The third statement is then an immediate consequence of 4.2. □

We give an explicit example.

Example. We shall work with $\lambda = -2$. Then

$$\sigma(X) = \frac{4X - 4}{-5X - 4} \quad \text{and} \quad \eta(X) = \frac{-X - 2}{-4X + 1}.$$

Consider the polynomial

$$f(X) := f_{\overline{G},-2}(X) f_{G,-1}(X) = X(X-1)(X+2)\cdot \\ \cdot (X+1)(X+8)(X+\frac{1}{5})(X-\frac{8}{5})(X-\frac{2}{11})(X-\frac{2}{3}).$$

Then, by Theorem 8.4 above, H_f has infinitely many quadratic twists of rank $\geq 3 \cdot \mathrm{rk}(\mathrm{End}_k(H_f)))$. Furthermore there is a $D \in \mathrm{Adm}(k)$ such that $J_D = J_f^3 \times B$ for some abelian variety B/k. The author speculates that $\mathrm{End}_k(J_f)$ is no larger than $\mathbb{Z}$ in this example. □

We will now consider certain cyclic subgroups $G \cong \mathbb{Z}/3$ of $\mathrm{PGL}(k)$ in order to obtain further examples. Let $a, b, c, d \in k^\times$ and assume that $a+d = -1$ and $ad - bc = 1$. Consider the automorphism

$$\sigma(X) = \frac{aX + b}{cX + d}$$

of $\mathbb{P}_1$.

Remark 8.5. *The order of* σ *in* $\mathrm{PGL}(k)$ *is* 3.

Proof. The matrix $A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has characteristic polynomial $X^2 + X + 1 = (X - \zeta_3)(X - \overline{\zeta_3})$, where $\zeta_3 \in \overline{k}^\times$ is a primitive third root of unity. Thus the matrix A is diagonalizable and this suffices. □

Let G be the subgroup of $\mathrm{PGL}(k)$ generated by σ. Let $v_1, \cdots, v_{2s+1} \in \mathbb{P}_1(k) \backslash G \cdot \infty$ and assume that $|G \cdot v_i| = 3$ for all i. Suppose that $G \cdot v_i \neq G \cdot v_j$

for $i \neq j$. Consider the squarefree polynomial

$$f(X) = f_{G,v_1}(X) \cdots f_{G,v_{2s+1}}(X).$$

Lemma 8.6. *Let $l_1(X) = cX + d$ and $l_2(X) = -cX + a$.*

(1) *Then $f(X)f(\sigma(X)) \in l_1(X)k(X)^{\times 2}$.*
(2) *Furthermore $f(X)f(\sigma^2(X)) \in l_2(X)k(X)^{\times 2}$.*

Proof. We make use of 8.1 and the relations $a + d = -1$, $ad - cb = 1$ to compute

$$\begin{aligned} f_{G,v_i}(\sigma(\infty)) &= f_{G,0}(\frac{a}{c}) = \frac{a}{c}(\frac{a}{c} - \frac{b}{d})(\frac{a}{c} + \frac{b}{a}) = \\ &= \frac{a}{c}\frac{ad - cb}{cd}\frac{a^2 + bc}{ca} = \frac{a^2 + bc}{c^3 d} = \\ &= \frac{a^2 + ad - 1}{c^3 d} = \frac{a(a + d) - 1}{c^3 d} = \frac{-(a + 1)}{c^3 d} = c^{-3} \end{aligned}$$

and similarly

$$\begin{aligned} f_{G,v_i}(\sigma^2(\infty)) &= f_{G,0}(-\frac{d}{c}) = -\frac{d}{c}(-\frac{d}{c} - \frac{b}{d})(-\frac{d}{c} + \frac{b}{a}) = \\ &= \frac{d}{c}\frac{d^2 + bc}{cd}\frac{-ad + bc}{ca} = -\frac{d^2 + bc}{c^3 a} = \\ &= -\frac{d^2 + ad - 1}{c^3 a} = \frac{d(a + d) - 1}{c^3 a} = \frac{-d - 1}{c^3 a} = -c^{-3}. \end{aligned}$$

Hence $f(\sigma(\infty)) \in ck^{\times 2}$ and $f(\sigma^2(\infty)) \in -ck^{\times 2}$. Obviously f is of odd degree and the elements of G permute the roots of f. Furthermore σ and σ^2 do not have a pole at ∞. Otherwise σ or σ^2 would be a translation, but a translation cannot have order 3 in $\mathrm{PGL}(k)$. Lemma 7.3 implies

$$f(X)f(\sigma(X)) = c\left(X + \frac{d}{c}\right) = (cX + d) \bmod k(X)^{\times 2}$$

and

$$f(X)f(\sigma^2(X)) = -c\left(X - \frac{a}{c}\right) = (-cX + a) \bmod k(X)^{\times 2}$$

as desired. □

Lemma 8.7. *Suppose that $k^\times$ contains a fourth root of unity ζ_4. Let $U = \frac{\sqrt{cX+d}}{\sqrt{-cX+a}-\zeta_4}$. Then $k(X, \sqrt{l_1(X)}, \sqrt{l_2(X)}) = k(U)$ is a rational function field. In particular there is a rational expression r_{l_1,l_2} such that $T = r_{l_1,l_2}(U)$.*

Proof. Let $x_0 := -\frac{d}{c}$. Then $(x_0, 0, \zeta_4)$ is a solution to the equations $l_1(X) = Y^2$, $l_2(X) = Z^2$ and the assertion follows by 6.7. □

Theorem 8.8. *Suppose that $k^\times$ contains a fourth root of unity. Let $D(U) = f(r_{l_1,l_2}(U))$.*

(1) *There is an abelian variety B/k such that $J_D \sim J_f^3 \times B$.*
(2) *We have* $\mathrm{rk}(J_f^{D(U)}(k(U))) \geq 3 \cdot \mathrm{rk}(\mathrm{End}_k(J_f))$.
(3) *The hyperelliptic curve H_f has infinitely many quadratic twists of rank* $\geq 3 \cdot \mathrm{rk}(\mathrm{End}_k(J_f))$.

Proof. The subgroup $\Delta \subset K^\times/K^{\times 2}$ generated by f, l_1 and l_2 is admissible of order 8. The subgroup Γ of Δ generated by l_1 and l_2 is of order 4 and $K(\sqrt{\Gamma}) = k(U)$ is a rational function field by Lemma 8.7 above. Furthermore $T = r_{l_1,l_2}(U)$. The first two statements follow by 8.6 and 7.2. The third statement is then an immediate consequence of 4.2. □

Example. We shall work with $\sigma(X) = \frac{X+3}{-X-2}$ that is, with $a = 1$, $b = 3$, $c = -1$ and $d = -2$, to obtain an explicit example. Consider the polynomial

$$\begin{aligned} f(X) := f_{G,0}(X) f_{G,1}(X) f_{G,2}(X) &= X(X + \frac{3}{2})(X + 3) \cdot \\ &\cdot (X - 1)(X + \frac{4}{3})(X + \frac{5}{2}) \cdot \\ &\cdot (X - 2)(X + \frac{5}{4})(X + \frac{7}{3}). \end{aligned}$$

Then, by Theorem 8.8 above, H_f has infinitely many quadratic twists of rank $\geq 3 \cdot \mathrm{rk}(\mathrm{End}_k(J_f)))$. Furthermore there is a $D \in \mathrm{Adm}(k)$ such that $J_D \sim J_f^3 \times B$ for some B. Again, the author speculates that $\mathrm{End}_k(J_f)$ is no larger than $\mathbb{Z}$, but he has not checked it. □

References

[1] L. Brünjes, *Über die Zetafunktion von Formen von Fermatgleichungen*. Ph.D. Thesis, Regensburg (2002).
[2] B. Conrad, *Silverman's specialization theorem revisited*. Preprint (2004).
[3] F. Gouvêa, B. Mazur, *The squarefree sieve and the rank of elliptic curves*. J. Amer. Math. Soc. **4** (1991), no. 1, 1–23.
[4] A. Grothendieck et al., *Eléments de Géometrie Algébrique*. Publ. Math. IHES, **4, 8, 17, 20, 24, 28, 32**.
[5] H. Helfgott, *On the square-free sieve*. Acta. Arith. **115** (2004), 349–402.
[6] T. Honda, *Isogenies, rational points and section points of group varieties*. Japan J. Math. **30** (1960), 84–101.
[7] C. Hooley, *Application of sieve methods to the theory of numbers*. Cambridge University Press 1976.

[8] E. Howe, F. Leprévost, B. Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*. Forum Math. **12** (2000), 315–364.
[9] S. Lang, *Fundamentals of Diophantine Geometry*. Springer (1983).
[10] J. Milne, *Abelian Varieties*. In: Arithmetic Geometry, edited by G. Cornell and J. Silverman, Springer 1986.
[11] J. Milne, *Jacobian Varieties*. In: Arithmetic Geometry, edited by G. Cornell and J. Silverman, Springer 1986.
[12] D. Mumford, *Abelian Varieties*. Oxford University Press (1970).
[13] S. Petersen, *On a Question of Frey and Jarden about the Rank of Abelian Varieties*. Journal of Number Theory **120** (2006), 287–302.
[14] M. Rosen, *Number Theory in Function Fields*. Springer **GTM 210** (2002).
[15] K. Rubin, A. Silverberg, *Rank Frequencies for Quadratic Twists of Elliptic Curves*. Experimental Mathematics **10**, no. 4 (2001), 559–569.
[16] K. Rubin, A. Silverberg, *Ranks of Elliptic Curves*. Bulletin of the AMS **39** (2002), 455–474.
[17] K. Rubin, A. Silverberg, *Twists of elliptic curves of rank at least four*. Preprint (2004).
[18] A. Silverberg, *The distribution of ranks in families of quadratic twists of elliptic curves*. Preprint (2004).
[19] J. Silverman, *The Arithmetic of Elliptic Curves*. Springer, **GTM 106** (1986).
[20] J. Silverman, *Heights and the specialization map for families of abelian varieties*. J. Reine Angew. Mathematik **342** (1983), 197–211.
[21] C.L. Stewart, J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*. J. Amer. Math. Soc. **8** (1995), 943–973.

Sebastian Petersen
Universität der Bundeswehr München
Institut für Theoretische Informatik und Mathematik
D-85577 Neubiberg
E-mail: sebastian.petersen@unibw.de