Journal of Number Theory 166 (2016) 85–92

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Optimal quotients and surjections of Mordell–Weil groups

Everett W. Howe

Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121-1967, USA

A R T I C L E   I N F O

Article history:
Received 26 July 2015
Received in revised form 7 February 2016
Accepted 7 February 2016
Available online 1 April 2016
Communicated by Steven J. Miller

MSC:
11G10
11G05
11G30
11G35

Keywords:
Jacobian
Mordell–Weil group
Automorphism

A B S T R A C T

Answering a question of Ed Schaefer, we show that if J is the Jacobian of a curve C over a number field, if s is an automorphism of J coming from an automorphism of C, and if u lies in $\mathbf{Z}[s] \subseteq \operatorname{End} J$ and has connected kernel, then it is not necessarily the case that u gives a surjective map from the Mordell–Weil group of J to the Mordell–Weil group of its image.

1. Introduction

Let J be the Jacobian of a curve C over a number field. If the automorphism group G of J is nontrivial, one can use idempotents of the group algebra $\mathbf{Q}[G]$ to decompose J (up to isogeny) as a direct sum of abelian subvarieties. This decomposition can be useful, for example, if one would like to compute the rational points on C, because one of the

E-mail address: however@alumni.caltech.edu.

http://dx.doi.org/10.1016/j.jnt.2016.02.013
0022-314X/

subvarieties may satisfy the conditions necessary for Chabauty's method even when J itself does not.

In this context, Ed Schaefer asked the following question in an online discussion:

Question 1. *Let C be a curve over a number field k, let σ be a nontrivial automorphism of C, let s be the associated automorphism of the Jacobian J of C, and let u be an element of $\mathbf{Z}[s] \subseteq \operatorname{End} J$. Let $A \subseteq J$ be the image of u, and suppose the kernel of u is connected. Is it always true that map of Mordell–Weil groups $J(k) \to A(k)$ induced by u is surjective*?

An *optimal quotient* of an abelian variety A is a surjective morphism $A \to A'$ of abelian varieties whose kernel is connected (see [1, §3]), so Schaefer's question asks whether an optimal quotient of a curve's Jacobian "coming from" an automorphism of the curve necessarily induces a surjection of Mordell–Weil groups.

The purpose of this paper is to show by explicit example that the answer to Schaefer's question is *no*. In Section 2 we show that if $\varphi\colon C \to E$ is a degree-2 map from a genus-2 curve to an elliptic curve, and if σ is the involution of C that fixes E, then the endomorphism $1 + s$ of J has connected kernel and its image is isomorphic to E. In fact, the map $J \to E$ determined by $1 + s$ is isomorphic to the push-forward $\varphi_*\colon J \to E$. To show that the answer to Question 1 is *no*, it therefore suffices to find a double cover $\varphi\colon C \to E$ of an elliptic curve by a genus-2 curve such that φ_* is not surjective on Mordell–Weil groups. We provide one such example in Section 3, and show in Section 4 that there are in fact infinitely many examples.

2. Genus-2 double covers of elliptic curves

In this section we review some facts about genus-2 double covers of elliptic curves over an arbitrary field of characteristic not 2. In Section 3 we will return to the case where the base field is a number field.

The general theory of degree-n maps from genus-2 curves to elliptic curves is explained by Frey and Kani [2]. Over the complex numbers, the complete two-parameter family of genus-2 double covers of elliptic curves was given in 1832 by Jacobi ([4, pp. 416–417], [5, pp. 380–382]) as a postscript to his review of Legendre's *Traité des fonctions elliptiques* [6]; Legendre had himself given a one-parameter family of genus-2 double covers of elliptic curves (see Remark 3, below). In [3, §3.2], Jacobi's construction is modified so that it works rationally over any base field of characteristic not 2, as follows:

Let k be an arbitrary field of characteristic not 2 and let K be a separable closure of k. Suppose we are given equations $y^2 = f$ and $y^2 = g$ for two elliptic curves E and F over k, where f and g are separable cubics in $k[x]$, and suppose further that we are given an isomorphism $\psi\colon E[2](K) \to F[2](K)$ of Galois modules such that ψ is not the restriction to $E[2]$ of a geometric isomorphism $E_K \to F_K$. Then [3, Proposition 4, p. 324] gives an explicit equation for a genus-2 curve C/k such that the Jacobian J of C is isomorphic