Journal of Algebra 509 (2018) 535–565

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Torsion subgroups of rational elliptic curves over the compositum of all D_4 extensions of the rational numbers

Harris B. Daniels

Department of Mathematics and Statistics, Amherst College, Amherst, MA 01002, USA

A R T I C L E   I N F O

Article history:
Received 14 October 2017
Available online 23 March 2018
Communicated by Gerhard Hiss

MSC:
primary 11G05
secondary 11R21, 12F10, 14H52

Keywords:
Elliptic curve
Torsion points
Galois theory

A B S T R A C T

Let $E/\mathbb{Q}$ be an elliptic curve and let $\mathbb{Q}(D_4^\infty)$ be the compositum of all extensions of $\mathbb{Q}$ whose Galois closure has Galois group isomorphic to a quotient of a subdirect product of a finite number of transitive subgroups of D_4. In this article we first show that $\mathbb{Q}(D_4^\infty)$ is in fact the compositum of all D_4 extensions of $\mathbb{Q}$ and then we prove that the torsion subgroup of $E(\mathbb{Q}(D_4^\infty))$ is finite and determine the 24 possibilities for its structure. We also give a complete classification of the elliptic curves that have each possible torsion structure in terms of their j-invariants.

1. Introduction

A fundamental theorem in arithmetic geometry known as the Mordell–Weil theorem says that the rational points on an elliptic curve defined over a number field can be given the algebraic structure of a finitely generated abelian group. More specifically, if K is a number field and E/K is an elliptic curve then the set of K-rational points $E(K)$ is

E-mail address: hdaniels@amherst.edu.
URL: http://hdaniels.people.amherst.edu.

https://doi.org/10.1016/j.jalgebra.2018.02.038
0021-8693/

isomorphic to a group of the form $\mathbb{Z}^r \oplus E(K)_{\text{tors}}$ where r is a nonnegative integer and $E(K)_{\text{tors}}$ is a finite abelian group called the *torsion subgroup of E over K*. In fact, as long as the base field K is a number field, the torsion subgroup of an elliptic curve is always isomorphic to a group of the form $\mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/ab\mathbb{Z}$ for some positive integers a and b. Merel, in [27] proved the existence of a uniform bound on the size of $E(K)_{\text{tors}}$ that depends only on the degree of the extension $K/\mathbb{Q}$. In light of this result it is natural to ask the following question.

Question 1.1. For a fixed $d \geq 1$, what groups (up to isomorphism) arise as the torsion subgroup of an elliptic curve over a number field of degree d?

The following theorems give a complete answer to Question 1.1 when $d = 1$ and 2.

Theorem 1.2 *(Mazur [25]). Let $E/\mathbb{Q}$ be an elliptic curve. Then*

$$E(\mathbb{Q})_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & 1 \leq M \leq 10 \textit{ or } M = 12, \textit{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & 1 \leq M \leq 4. \end{cases}$$

Theorem 1.3 *(Kenku, Momose [19], Kamienny [13]). Let E/F be an elliptic curve over a quadratic number field F. Then*

$$E(F)_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \textit{with } 1 \leq M \leq 16 \textit{ or } M = 18, \textit{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \textit{with } 1 \leq M \leq 6, \textit{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3M\mathbb{Z} & \textit{with } M = 1 \textit{ or } 2, \textit{ only if } F = \mathbb{Q}(\sqrt{-3}), \textit{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \textit{only if } F = \mathbb{Q}(\sqrt{-1}). \end{cases}$$

Recently, Etropolski, Morrow, and Zureick-Brown, (and independently Derickx) announced that they have found a complete classification of the torsion structures that occur for elliptic curves over cubic fields, giving an answer to Question 1.1 in the case when $d = 3$. This answer comes after the work of Jeon, Kim, Lee, and Schweizer [11,12] classifying all of the torsion structures of elliptic curves defined over cubic fields that occur infinitely often.

One way to simplify Question 1.1 is to restrict to the torsion subgroups of elliptic curves defined over $\mathbb{Q}$ that have been base-extended to degree d number fields. There are many results related to this question and below we present a few of them.

Theorem 1.4. *[24, Thm. 2] Let $E/\mathbb{Q}$ be an elliptic curve and let F be a quadratic number field. Then*