Torsion Points of Low Order on Elliptic Curves and Drinfeld Modules

by

Lisa Marie Redekop

B.Sc., University of Ottawa, 2002.

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in the Department
of
Mathematics

SIMON FRASER UNIVERSITY
Spring 2006

APPROVAL

Name: Lisa Marie Redekop

Degree: Master of Science

Title of thesis: Torsion Points of Low Order on Elliptic Curves and Drinfeld Modules

Examining Committee: Dr. Ladislav Stacho
Chair

Dr. Imin Chen
Senior Supervisor

Dr. Nils Bruin
Supervisor

Dr. Alistair Lachlan
Internal Examiner

Date Approved: April 7, 2006

Abstract

In this thesis, we calculate the Galois groups of extensions generated by torsion points of low order on elliptic curves and Drinfeld modules through their corresponding division polynomials. We investigate division polynomials of degree up to and including four, which correspond to 2-torsion and 3-torsion points on elliptic curves and $(T+a)$-torsion and (T^2+aT+b)-torsion points on Drinfeld modules of rank 1 and 2. These calculations depend on the invariants that classify elliptic curves and Drinfeld modules up to an isomorphism.

Dedication

This thesis is dedicated to my parents, Gloria and Vern, who have loved and supported me to no end my entire life, and who have taught me the meaning of perseverance.

Acknowledgements

First and foremost I thank my supervisor, Dr. Imin Chen, for his genuine feedback and guidance throughout this thesis writing process. His keen eye for clarity and preciseness has taught me a great deal - thank you.

I thank my friends and family who have helped me along the way by giving me the support I needed to carry on.

Most importantly, I thank my husband Jonathan for his love and patience. His unconditional support has fueled me enumerable times and I thank you.

Contents

List of Tables

Chapter 1

Introduction

The primary motivation of this thesis is to calculate the Galois groups of extensions generated by torsion points of low order on elliptic curves and Drinfeld modules. In particular, we calculate the Galois groups of splitting fields of division polynomials of low degree on elliptic curves and Drinfeld modules. The determination of these Galois groups depend on the invariants that classify the elliptic curves or Drinfeld modules up to isomorphism.

The field extensions generated by torsion points on elliptic curves and on Drinfeld modules have recently played an important role in the study of the arithmetic of number fields and function fields. They play a central role for instance in the proof of the Modularity Conjecture for elliptic curves over $\mathbb{Q}$ [BCDT01] and Fermat's Last Theorem [Wil95].

The study of torsion points on elliptic curves or Drinfeld modules is equivalent to the study of rational points on modular curves and on Drinfeld modular curves. In essence, we are giving parametrizations of these modular curves for torsion points of low order by directly using field theory. Such parametrizations have been determined in the literature, by primarily using complex function theory (cf. [Bir72] for instance).

This introductory chapter contains background information that is used throughout this thesis. This includes methods for determining the Galois groups of cubic and quartic polynomials, and an introduction to elliptic curves and Drinfeld modules; their

structure and isomorphism classes. Following this background information, Chapter 3 gives pertinent information on torsion points on elliptic curves and on Drinfeld modules, and gives methods used to determine their respective Galois groups. Chapter 4 studies the Galois groups of cubic and quartic division polynomials of elliptic curves, while Chapter 5 studies the Galois groups of division polynomials both of rank 1 and 2 Drinfeld modules that give rise to cubic and quartic division polynomials.

1.1 Usage of Magma and Maple

We use Magma [BCP97] and Maple [GGC81] throughout this thesis for simple algebraic calculations. Magma is used to determine the factorization of a polynomial over a given field. Maple is used to aid the process of solving a system of equations by substitution and is used to calculate the discriminant of a polynomial over a field of characteristic $p \neq 2$. We also use Maple to find Möbius transformations of one variable so that a given expression is of a particular form, which is illustrated by the following example.

Example 1.1 *Let k be a field and consider $u \in k$ given by*

$$u = \frac{t^2}{(2t+1)(t+1)}, \tag{1.1}$$

for some $t \in k$. Suppose we would like u to be of the form

$$u = \frac{s^2}{s+1}, \tag{1.2}$$

for some $s \in k$. Then we proceed as follows. Using Maple, substitute $t = (as + b)/(cs + d)$, where $a, b, c, d \in k$, into (1.1) to get

$$u = \frac{(as+b)^2}{(cs+d)^2(2s+1)(s+1)}. \tag{1.3}$$

By equating (1.2) with (1.3) and using Maple to cross multiply and collect terms, we get

$$\begin{aligned}(a+c)(2a+c)s^4 + (-a^2 + (b+d)(2a+c) + (a+c)(2b+d))s^3 \\ +(-a(2b+a) + (b+d)(2b+d))s^2 - b(b+2a)s - b^2 = 0.\end{aligned}$$

Setting the coefficient of s equal to 0 gives the solution

$$a = d, \qquad b = 0, \qquad c = -d, \qquad \text{and} \qquad d = d.$$

Therefore, if we set $t = s/(-s+1)$ then u in terms of s is of the desired form, namely

$$u = \frac{s^2}{s+1}.$$

To recapitulate, in example 1.1, we use Maple for substitution, cross multiplication, and collecting like terms. Throughout this thesis, we assume that Magma or Maple is being used when factoring, substituting, and finding a Möbius transformation to get a an expression in a particular form.

Chapter 2

Background

This chapter contains background information on Galois theory, elliptic curves, and Drinfeld modules.

2.1 Field theory

Let k be a field and consider a polynomial $f \in k[x]$. We say that f *splits* over k if f has only linear factors over k. Let K be a field such that k is a subfield of K. Then we say K is a *field extension* of k, denoted by $K|k$. If f does not split over k, we can then construct such an extension K of k so that f splits over K.

Definition 2.1 *Let f be a polynomial over a field k. The extension $K|k$ is called a splitting field extension for f over k if f splits over K and there is no proper subfield L of K containing k such that f splits over L.*

Any two splitting field extensions for a given polynomial f over k are isomorphic. We say f has distinct roots if the roots of f are distinct in a splitting field extension of k, which is indeed independent of the splitting field. We would like to have criteria to determine whether the irreducible factors of f over k have repeated roots in a splitting field extension for f. It turns out if char $k = 0$ then the irreducible factors of any polynomial over k have distinct roots.

Definition 2.2 *Let f be an irreducible polynomial of degree n over a field k and let K be a splitting field extension for f over k. We say that f is separable over k if f has n distinct roots in K. A polynomial f over a field k is separable if all of its irreducible factors are separable over k.*

Lemma 2.3 ([Gar86], p.86) *Let f be an irreducible polynomial over a field k. Then f is not separable if and only if char $k = p > 0$ and f has the form*

$$f = a_0 + a_1 x^p + a_2 x^{2p} + \cdots + a_n x^{np}, \text{ for some } a_i \in k.$$

Let $K|k$ be an extension of fields, then the set of automorphisms of K which fix k is

$$\Gamma(K|k) = \{\sigma \in Aut\, K \mid \sigma(g) = g \text{ for all } g \in k\}.$$

The group $\Gamma(K|k)$ is a subgroup of $Aut\ K$ called the *Galois group* of K over k. If $K|k$ is a splitting field extension for $f \in k[x]$, then $\Gamma(K|k)$ is called the Galois group of f over k.

Theorem 2.4 ([Gar86], p.95) *Let f be a polynomial over a field k and suppose that $K|k$ is a splitting field extension for f over k. Let S denote the set of roots of f in K. Then each $\sigma \in \Gamma(K|k)$ defines a permutation of S, so that we have a mapping, denoted by Φ, from $\Gamma(K|k)$ to the group Σ_S of permutations of S. Moreover, Φ is a group monomorphism.*

Proof: *([Gar86], p.95)* Let $G = \Gamma(K|k)$. An element of G acts on f by acting on each of its coefficients. Hence, $\sigma(f) = f$ as f has its coefficients in k. For $\alpha \in S$,

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0,$$

hence σ maps S into S. Since σ is injective and S is finite, $\sigma|_S$ is a permutation. Therefore we have a mapping, denoted by Φ, from G into the group Σ_S of permutations of S. If $\sigma, \tau \in G$ then by definition $(\sigma\tau)(\alpha) = \sigma(\tau(\alpha))$ whence Φ is a group homomorphism. Furthermore, if $\sigma(\alpha) = \tau(\alpha)$ for all $\alpha \in S$, then $\tau^{-1}\sigma(\alpha) = \alpha$ for all $\alpha \in S$. It follows that $\tau^{-1}\sigma$ fixes K, giving $\tau = \sigma$. Consequently Φ is a group monomorphism.

■

Lemma 2.5 ([Gar86], p.66) *Suppose $f \in k[x]$ is irreducible and that $K|k$ is a splitting field extension for f. If α and β are roots of f in K, then there is an automorphism $\sigma : K \to K$ such that $\sigma(\alpha) = \beta$ and σ fixes k.*

Let f be a polynomial over k of degree n with distinct roots and with Galois group G and let S_n denote the group of permutations of $\{1, 2, ..., n\}$. From Theorem 2.4, G is isomorphic to a subgroup of S_n. Furthermore, if f is an irreducible polynomial over k, then G is transitive.

2.2 Projective Varieties

Let k be a field with algebraic closure $\bar{k}$ and let the projective n-space over $\bar{k}$ be denoted by $\mathbb{P}^n(\bar{k})$ (or simply $\mathbb{P}^n$). If f is a homogeneous polynomial in $S = \bar{k}[x_0, ..., x_n]$, then the zeros of f are given by $Z(f) = \{P \in \mathbb{P}^n : f(P) = 0\}$. Furthermore, if T is a set of homogeneous polynomials in S, we define the zero set of T to be

$$Z(T) = \{P \in \mathbb{P}^n : f(P) = 0 \text{ for all } f \in T\}.$$

A subset V of $\mathbb{P}^n$ is called a *projective algebraic set* if there exists a set T of homogeneous elements of S such that $Z(T) = V$. Furthermore, the ideal of V, denoted by $I(V)$, is the ideal in S generated by

$$\{f \in S : f \text{ is homogeneous and } f(P) = 0 \text{ for all} P \in V\}.$$

We can now define the Zariski topology on $\mathbb{P}^n$ by taking open sets to be the compliments of projective algebraic sets. A nonempty subset Y of a topological space is *irreducible* if it cannot be expressed as the union of two proper subsets, each one of which is closed in Y ([Har77], p.3). A *projective variety* is then an irreducible algebraic set in $\mathbb{P}^n$ ([Har77], p.10). A projective variety defined over k is an irreducible projective algebraic set V such that there exists a set T of homogeneous polynomials in $k[x_0, ..., x_n]$ and $Z(T) = V$.

The function field of $\mathbb{P}^n$ is the subfield of $\bar{k}(X_0, \ldots, X_n)$ consisting of all rational functions $F(X) = f(X)/g(X)$ for which f and g have the same degree. Then the function field of a projective variety V, denoted by $\bar{k}(V)$, is the field of rational functions $F(X) = f(X)/g(X) \in \bar{k}(X_0, \ldots, X_n)$ such that:

(i) f and g are homogeneous of the same degree;

(ii) $g \notin I(V)$;

(iii) two functions f/g and f'/g' are identified (or equal) if $fg' - f'g \in I(V)$ ([Sil86], p.15).

The function field $k(V)$ is then the field of rational functions $F(X) \in k(X_0, \ldots, X_n)$ satisfying (i), (ii), and (iii) given above.

Definition 2.6 ([Sil86], p.15) *Let k be a field with algebraic closure $\bar{k}$. Suppose V_1, $V_2 \subset \mathbb{P}^n$ are projective varieties. A rational map $\theta : V_1 \to V_2$ is a map of the form $\theta = [f_0, ..., f_n]$, where $f_0, \ldots, f_n \in \bar{k}(V_1)$ have the property that for every point $P \in V_1$ at which $f_0, \ldots, f_n$ are all defined,*

$$\theta(P) = [f_0(P), \ldots, f_n(P)] \in V_2.$$

Furthermore, we say that θ is defined over k if there is some $\lambda \in \bar{k}^*$ so that $\lambda f_0, \ldots, \lambda f_n \in k(V_1)$.

Definition 2.7 ([Sil86], p.16) *Let k be a field with algebraic closure $\bar{k}$. Suppose V_1, $V_2 \subset \mathbb{P}^n$ are projective varieties. A rational map*

$$\theta = [f_0, ..., f_n] : V_1 \to V_2$$

is called regular (or defined) at $P \in V_1$ if there is a function $g \in \bar{k}(V_1)$ such that $gf_0, \ldots, gf_n$ are all regular at P, and $(gf_i)(P) \neq 0$ for some i. A rational map is called a morphism if it is regular for every $P \in V_1(\bar{k})$.

Example 2.8 *Let k be a field of characteristic $p \neq 2$ and let V be a projective variety in $\mathbb{P}^2$ given by*

$$V : \ X^2 + Y^2 = Z^2.$$

Consider the map θ_1 given by

$$\theta_1 : V \to \mathbb{P}^1$$

$$\theta_1([X,Y,Z]) \mapsto [-Y/(X+Z) : 1].$$

Then θ_1 is regular at every point in $V(\bar{k})$. This is clear, except possibly at the point $P = [1,0,-1]$. Let $f = -Y/(X+Z)$. We must then find a $g \in \bar{k}(V)$ such that gf and g are regular at P and one of $g(P)f(P)$ or $g(P)$ is nonzero. Let $g = Y/(X-Z)$, then $g(P)f(P) = 1$ and $g(P) = 0$ are regular at $P = [1,0,-1]$. Hence, θ_1 is in fact regular at every point of V. Therefore, θ_1 is a morphism defined over k.

One can define the notion of the dimension of a projective variety ([Har77], p.10). A *curve* is then a projective variety of dimension 1. Another invariant is the genus of a curve ([Har77], p.294). Curves of genus 0 defined over k with a k-rational point are isomorphic to $\mathbb{P}^1$, whereas curves of genus 1 with a k-rational point are isomorphic to an elliptic curve.

2.2.1 Curves of Genus 0

Theorem 2.9 ([HS91], p.75) *Let C be a smooth projective curve of genus 0 defined over a field k. Then the curve C is ismorphic over k to $\mathbb{P}^1$ if and only if it has a k-rational point.*

Proof: The outline of this proof is as follows. Using the Riemann-Roch theorem, C can be embedded into $\mathbb{P}^2$ as a smooth conic X defined over k. Suppose X does not posses a k-rational point, then clearly X is not parametrizable. Conversely, suppose X possesses a k-rational point P_0. Then use the identification of $\mathbb{P}^1$ with the space of lines in $\mathbb{P}^2$ that go through P_0 to define the following two rational maps;

$$\theta_1 : X \longrightarrow \mathbb{P}^1, \qquad P \mapsto \begin{cases} \text{line through } P \text{ and } P_0 & \text{if } P \neq P_0, \\ \text{tangent line to } X \text{ at } P_0 & \text{if } P = P_0. \end{cases}$$

$$\theta_2 : \mathbb{P}^1 \longrightarrow X, \qquad L \mapsto \text{the point } P \text{ such that } L \cap X = \{P, P_0\}.$$

The composition of these maps is the identity. Furthermore, a rational map from a smooth curve to a projective variety extends to a morphism defined on the whole curve ([HS91], p.69). Therefore, θ_1 and θ_2 are isomorphisms.

■

Example 2.10 *Let k, V, and θ_1 be as given in Example 2.8. Then V is a smooth projective curve of genus 0 and possesses the k-rational point $[-1,0,1]$. From Theorem 2.9, V is isomorphic to $\mathbb{P}^1$. We use this example to illustrate the proof of Theorem 2.9. Let $P_0 = [-1,0,1]$. Since a line in $\mathbb{P}^2$ is given by $sX + tY + rZ = 0$, it is clear that the set of all lines passing through P_0 is given by*

$$sX + tY + sZ = 0. \tag{2.1}$$

Furthermore, we identify the point $[s,t] \in \mathbb{P}^1$ with the line in $\mathbb{P}^2$ given by (2.1). Now consider a point $P = [a,b,c] \neq P_0$ on V. Then the line passing through P_0 and P is given by

$$-\frac{b}{a+c}X + Y - \frac{b}{a+c}Z = 0,$$

which is identified with the point $[-b/(a+c),1]$ on $\mathbb{P}^1$. Therefore,

$$\theta_1(P) = [-b/(a+c),1].$$

Furthermore, the line tangent to V at P_0 is given by

$$X + Z = 0,$$

which is identified with the point $[1,0]$ on $\mathbb{P}^1$ and $\theta_1(P_0) = [1,0]$. Conversely, let $[s,t] \in \mathbb{P}^1$. The point $[s,t]$ is identified with the line

$$L:\ sX + tY + sZ = 0$$

through P_0. Then $L \cap V = \{P_0, P\}$ where $P = [t^2 - s^2, -2st, s^2 + t^2]$. Therefore,

$$\theta_2([s,t]) = [t^2 - s^2, -2st, s^2 + t^2].$$

Hence, θ_2 is a morphism defined over k that maps the point $[s,t]$ (identified with the line $sX + tY + sZ = 0$ on $\mathbb{P}^2$) to the point $P \in \mathbb{P}^2$ such that the line $sX + tY + sZ = 0$ intersects V at $[-1,0,1]$ and P.

2.2.2 Elliptic Curves

An *elliptic curve* defined over k is a pair (E, O_E), where E is a curve of genus 1 defined over k with a rational point $O_E \in E(k)$, called the *basepoint* of E.

Lemma 2.11 ([Sil86], p.63) *Let E be an elliptic curve defined over k. Then E is isomorphic over k to a curve in $\mathbb{P}^2$ given by a Weierstrass equation*

$$ZY^2 + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with coefficients $a_1, ..., a_6 \in k$, and such that O_E gets mapped to $[0, 1, 0]$. Furthermore, any two Weierstrass equations for E are related by a linear change of variables of the form

$$X = u^2X' + rZ'$$

$$Y = u^3Y' + u^2sX' + tZ'$$

$$Z = Z'$$

with $u, r, s, t \in k$, $u \neq 0$.

We call the change of variables given in Lemma 2.11 an *admissible change of variables*, because this is the only change of variables that will preserve the Weierstrass model. Let E be an elliptic curve given by a Weierstrass equation and consider E in affine space by making the substitutions $y = Y/Z$ and $x = X/Z$. Then E is given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.2}$$

with an additional point $[0, 1, 0]$ at infinity. If char $k \neq 2$ we can simplify (2.2) by completing the square and replacing y with $y + (a_1x + a_3)/2$, yielding

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4},$$

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = 2a_4 + a_1a_3, \qquad b_6 = a_3^2 + 4a_6, \qquad 4b_8 = b_2b_6 - b_4^2.$$

Also, define the quantities

$$\begin{aligned} \Delta(E) &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ j(E) &= (b_2^2 - 24b_4)^3/\Delta. \end{aligned}$$

The quantity $\Delta(E)$ given above is called the *discriminant* of the Weierstrass equation and $j(E)$ is called the *j-invariant* of the elliptic curve. It is noted that the change of variables given in Lemma 2.11 leave the j-invariant invariant (hence its name).

If char $k \neq 2, 3$ then we can eliminate the x^2 term by completing the cube and replacing x with $x - b_2/12$ yielding

$$y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864},$$

where

$$c_4 = b_2^2 - 24b_4 \text{ and } c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Lemma 2.12 ([Sil86], p.50) *A curve E given by a Weierstrass equation is non-singular if and only if $\Delta(E) \neq 0$.*

We can simplify the Weierstrass equation of an elliptic curve depending on its j-invariant and on the characteristic of k.

Lemma 2.13 ([Sil86], p.324) *Let E be an elliptic curve in $\mathbb{P}^2$ given by a Weierstrass equation. Then in each of the following cases, there is a substitution of the form*

$$x = u^2x' + r \qquad \text{and} \qquad y = u^3y' + u^2sx' + t, \qquad \text{with } u, r, s, t \in \bar{k}, \text{ and } u \neq 0$$

such that E has a simplified Weierstrass form.

(I) *char* $k \neq 2, 3$

$y^2 = x^3 + a_4x + a_6, \qquad \Delta(E) = -16(4a_4^3 + 27a_6^2), \quad j(E) = 1728\frac{4a_4^3}{4a_4^3+27a_6^2},$

(II) *char* $k = 3$ *and* $j(E) \neq 0$

$y^2 = x^3 + a_2x^2 + a_6, \qquad \Delta(E) = -a_2^3a_6, \qquad j(E) = -a_2^3/a_6,$

(III) *char* $k = 3$ *and* $j(E) = 0$

$y^2 = x^3 + a_4x + a_6, \qquad \Delta(E) = -a_4^3,$

(IV) *char* $k = 2$ *and* $j(E) \neq 0$

$y^2 + xy = x^3 + a_2x^2 + a_6, \quad \Delta(E) = a_6, \qquad j(E) = 1/a_6,$

(V) *char* $k = 2$ *and* $j(E) = 0$

$y^2 + a_3y = x^3 + a_4x + a_6, \quad \Delta(E) = a_3^4.$

Proof: The approach is to consider a general Weierstrass equation

$$y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$$

and use an admissible change of variables as given in Lemma 2.11 to transform the general equation into the desired form. We refer the reader to *([Sil86], p.324)* for more details.

■

An elliptic curve E is isomorphic over $\bar{k}$ to a simplified curve as given in Lemma 2.13. We call this simplified curve the *short Weierstrass form* of E.

A natural progression to our study of elliptic curves is to determine their isomorphism classes. Let E and E' be elliptic curves with base points O_E and $O_{E'}$ respectively. An isomorphism over $\bar{k}$ from E into E' is precisely a change of variables of the form

$$x = u^2x' + r,$$

$$y = u^3y' + u^2sx' + t,$$

where $u \neq 0$, r, s, $t \in \bar{k}$, precisely as in Lemma 2.13.

Lemma 2.14 ([Sil86], p.50) *Let k be a field with algebraic closure $\bar{k}$.*

(a) Two elliptic curves defined over k are isomorphic over $\bar{k}$ if and only if they have the same j-invariant.

(b) Let $u \in \bar{k}$. Then there exists an elliptic curve defined over $k(u)$ with j-invariant equal to u.

Proof:

(a) If two elliptic curves are isomorphic, then the isomorphism is given by an admissible change of variables, which leave the j-invariant fixed. The converse is shown by considering two elliptic curves in Weierstrass form having the same j-invariant, and finding an explicit isomorphism between the two curves of the desired form. We refer the reader to *([Sil86], p.50)* for the details of this proof.

(b) Let $u \in \bar{k}$ and let E be the elliptic curve defined over k with Weiertrass equation

$$E = \begin{cases} y^2 + y = x^3 & \text{if } u = 0, \\ y^2 = x^3 + x & \text{if } u = 1728, \\ y^2 + xy = x^3 - \frac{36}{u_0 - 1728}x - \frac{1}{u_0 - 1728} & \text{if } u \in k \setminus \{0, 1728\}. \end{cases}$$

Then $j(E) = u$.

■

Let E and E' be elliptic curves given in short Weierstrass form. If $E \cong E'$ over $\bar{k}$, then the isomorphism from E to E' is given in the following list.

∘ Case char $k \neq 2, 3$. Let E and E' be given by

$$E : y^2 = x^3 + Ax + B \qquad \text{and} \qquad E' : (y')^2 = (x')^3 + A'x' + B',$$

for some A, A', B, $B' \in k$. An isomorphism from E to E' is of the form $(x, y) = (u^2x', u^3y')$ where $u \in \bar{k}$ is given by

$$u = \begin{cases} (B/B')^{\frac{1}{6}} & \text{if } j(E) = 0, \\ (A/A')^{\frac{1}{4}} & \text{if } j(E) = 1728, \\ (A/A')^{\frac{1}{4}} = (B/B')^{\frac{1}{6}} & \text{if } j(E) \neq 0, 1728. \end{cases}$$

- Case char $k = 2$. If $j(E) \neq 0$, then let E and E' be given by

$$E : y^2 + xy = x^3 + a_2x^2 + a_6 \qquad \text{and} \qquad E' : (y')^2 + x'y' = (x')^3 + a_2'(x')^2 + a_6'.$$

An isomorphism from E to E' is of the form $(x, y) = (x', y' + sx')$ where

$$s^2 + s + a_2 + a_2' = 0.$$

If $j(E) = 0$ then E and E' are of the form

$$y^2 + a_3y = x^3 + a_4x + a_6.$$

An isomorphism from E to E' is of the form $(x, y) = (u^2x' + s^2, u^3y' + u^2x' + t)$, where $u, s, t \in \bar{k}$ satisfy the equations

$$u^3 = a_3'/a_3, \qquad s^4 + a_3s + a_4 - u^4a_4' = 0,$$

$$t^2 + a_3t + s^6 + a_4s^2 + a_6 - u^6a_6' = 0.$$

- Case char $k = 3$. If $j(E) \neq 0$, then E and E' are of the form

$$y^2 = x^3 + a_2x^2 + a_6.$$

An isomorphism from E to E' is of the form $(x, y) = (u^2x', u^3y')$, where $u \in \bar{k}$ satisfies the equation $u^2 = a_2/a_2'$.

If $j(E) = 0$ then E and E' are of the form

$$y^2 = x^3 + a_4x + a_6.$$

An isomorphism from E to E' is of the form $(x, y) = (u^2x' + r, u^3y')$, where $u, r \in \bar{k}$ satisfy the equations

$$u^4 = a_4'/a_4 \qquad \text{and} \qquad r^3 + a_4r + a_6 - u^6a_6' = 0.$$

The set of all points in $\mathbb{P}^n$ on an elliptic curve form an abelian group under the composition law, with identity element O_E. Furthermore, there is an algorithm that calculates the negation and addition of points on E.

Composition Law 2.15 ([Sil86], p.55) *Let E be an elliptic curve defined over a field k with basepoint O_E. Let P and Q be points on E, L be the straight line connecting P and Q (tangent line to E if $P = Q$), and R be the third point of intersection of L with E. Let L' be the straight line connecting R and O_E. Then the third point of intersection of L' with E is defined to be $P + Q$.*

Addition Law 2.16 ([Sil86], p.58) *Let k be a field with algebraic closure $\bar{k}$ and let E be an elliptic curve defined over k with basepoint O_E given by a Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

If $P = (x, y) \in E(\bar{k})$ then $-P = (x, -y - a_1x - a_3)$. Let $P_3 = P_1 + P_2$ with $P_i = (x_i, y_i) \in E(k)$.

If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then

$$P_1 + P_2 = O_E.$$

Otherwise, let

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \qquad v = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \qquad \text{if } x_1 \neq x_2;$$

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \quad v = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \quad \text{if } x_1 = x_2.$$

Then $P_3 = (x_3, y_3)$ is given by

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 &= -(\lambda + a_1)x_3 - v - a_3. \end{aligned}$$

2.3 Drinfeld modules

We begin with the motivation behind the definition of a Drinfeld module. Let k be a field and suppose $f(x) \in k[x]$. The polynomial f is *additive* if $f(x+y) = f(x) + f(y)$

inside the polynomial ring of two variables $k[x, y]$. The following proposition gives the form of additive polynomials depending on the characteristic of k.

Proposition 2.17 ([Ros02], p.197) *Let k be a field and $f(x) \in k[x]$ be an additive polynomial. If char $k = 0$, then $f(x) = ax$ for some $a \in k$. If char $k = p > 0$, then $f(x) = a_0x + a_1x^p + \ldots + a_rx^{p^r}$ for some $a_0, \ldots, a_r \in k$.*

For the remainder of this section we assume k is a field extension of $\mathbb{F}_q$, a finite field with $q = p^n$ elements where p is a prime. Let $\mathcal{A}(k)$ denote the set of additive polynomials in $k[x]$. Then $\mathcal{A}(k)$ is a ring with the standard addition of polynomials and multiplication given by composition. Note that the identity element of $\mathcal{A}(k)$ is x. Let $\tau(x) = x^p$ and let $k\langle\tau\rangle$ be a non-commutative ring with addition and multiplication as in a polynomial ring except when multiplying an element of k by a power of τ, we follow the rule

$$\tau a = a^p\tau. \tag{2.3}$$

Then the identity element of $k\langle\tau\rangle$ is $\tau^0 = 1$. By construction of $k\langle\tau\rangle$, there is a ring isomorphism $\theta : \mathcal{A}(k) \to k\langle\tau\rangle$ defined by

$$\theta(a_0x + a_1x^p + \cdots + a_rx^{p^r}) = a_0\tau^0 + a_1\tau + \cdots + a_r\tau^r.$$

Therefore, the endomorphism ring of the additive group of k over $\mathbb{F}_q$ can be considered either as the non-commutative polynomial ring $k\langle\tau\rangle$ with the relation $\tau a = a^p\tau$, or as the ring of additive polynomials over k with multiplication being given by composition ([Ros02], p.199).

We want the $\mathbb{F}_q$-algebra structure to be preserved by the endomorphism ring $\mathcal{A}(k)$. So we assume k is a field extension of $\mathbb{F}_q$ and only consider additive polynomials which commute with the elements of $\mathbb{F}_q$. That is, if $f = \Sigma a_i\tau^i$ we require that $\alpha^{p^i} = \alpha$ for every $\alpha \in \mathbb{F}_q$ where $a_i \neq 0$. This condition holds if and only if $n|i$ for all i such that $a_i \neq 0$. In other words, $f \in \langle\tau^n\rangle$. Therefore, we will replace the rule given in (2.3) by

$$\tau a = a^q\tau,$$

for every $a \in k$ ([Ros02], p.200).

Definition 2.18 ([Ros02], p.220) *Let $A = \mathbb{F}_q[T]$ and k a field extension of $\mathbb{F}_q$. A Drinfeld A-module over k consists of an $\mathbb{F}_q$-algebra homomorphism δ from A to k, together with an $\mathbb{F}_q$-algebra homomorphism $\rho : A \longrightarrow k\langle\tau\rangle$ such that $D(\rho_a) = \delta(a)$ for all $a \in A$, where ρ_a denotes $\rho(a)$ and $D : k\langle\tau\rangle \longrightarrow k$ is given by*

$$D\left(\Sigma c_i \tau^i\right) = c_0.$$

Moreover, we require that k does not contain the image of ρ. We denote by $\mathrm{Drin}_A(k)$ the set of all Drinfeld A-modules over k, the structural map δ being assumed fixed.

Consider a k-algebra Ω and an $\mathbb{F}_q$-algebra homomorphism δ from A to k. The homomorphism δ makes Ω into an A-module with the relation

$$a \cdot u = \delta(a)u, \qquad \text{for all } a \in A, u \in \Omega,$$

referred to as the standard action of A on Ω. The idea of a Drinfeld module is that it makes Ω into an A-module in a new way, namely,

$$a \ast u = \rho_a(u), \qquad \text{for all } a \in A, u \in \Omega.$$

We denote this new A-module structure on Ω by Ω_ρ. The condition that k does not contain the image of ρ implies that $\rho_a(u) \neq \delta(a)u$ for at least one $a \in A$. This condition guarantees that the action of A on Ω is in fact different from the standard action of A on Ω ([Ros02], 220).

Often δ is taken to be a algebra homomorphism into a field k, however, one can also consider reduction modulo a prime ideal. For example, if $A = \mathbb{F}_2[T]$ then we could take $k = \mathbb{F}_2(T)$ and δ to be the inclusion map from A into k, or take $k = A/(f)$ where $f = T^2 + T + 1$, with (f) being a prime ideal in A, and δ the reduction map modulo f.

Definition 2.19 *The Carlitz module the a Drinfeld A-module given by*

$$C_T = T + \tau.$$

Consider the Carlitz module under the two possibilities for k. We have

$$C_{T^3} = \begin{cases} T^3 + (T^4 + T^3 + T^2)\tau + (T^4 + T^2 + T)\tau^2 + \tau^3 & \text{if } k = \mathbb{F}_2(T), \\ 1 + (T+1)\tau^2 + \tau^3 & \text{if } k = A/(f). \end{cases}$$

Unless otherwise stated, δ is taken to be the map into the field k.

Definition 2.20 ([Ros02], p.200) *The rank of a Drinfeld A-module ρ over k is defined to be the unique positive integer r such that $deg_\tau(\rho_a) = r\, deg_T(a)$ for all $a \in A$, where $deg_x B$ is the highest occurring exponent of x in B.*

We continue with the definition of a morphism between two Drinfeld modules and give criteria so that these modules are in fact isomorphic.

Definition 2.21 ([Ros02], p.226) *Let $\rho, \rho' \in \mathrm{Drin}_A(k)$. A morphism over k from ρ to ρ' is an element f of $k\langle\tau\rangle$ with the property that $f\rho_a = \rho'_a f$ for all $a \in A$. The set of all such morphisms is denoted by $\mathrm{Hom}_k(\rho, \rho')$.*

Proposition 2.22 ([Ros02], p.227) *Let $\rho, \rho' \in \mathrm{Drin}_A(k)$. Then ρ and ρ' are isomorphic over k if and only if there is a nonzero $c \in k$ such that $c\rho_a = \rho'_a c$ for all $a \in A$.*

Proof: Suppose that f is a morphism between ρ and ρ'. By definition, $f \in Hom_k(\rho, \rho')$ is an isomorphism if and only if $gf = \tau^0 = fg$ for some $g \in Hom_k(\rho, \rho')$. In $k\langle\tau\rangle$ this can only happen if $f = c\tau^0$ and $g = c^{-1}\tau^0$ for some nonzero element $c \in k$.

■

Let $A = \mathbb{F}_q[T]$ and k a field extension of $\mathbb{F}_q(T)$. There is only one isomorphism class of rank 1 Drinfeld A-modules over $\bar{k}$. To see this, we will show that a Drinfeld module ρ of rank 1 over k given in the most general form

$$\rho_T = T + u\tau,$$

where $u \in k$, is isomorphic over $\bar{k}$ to the Carlitz module $C_T = T + \tau$. An isomorphism exists if and only if there is a $c \in \bar{k}$ such that $c\rho_T = C_T c$. But $c\rho_T = C_T c$ if and only if $u = c^{q-1}$. Since $c \in \bar{k}$, $\rho_T \cong C_T$.

Definition 2.23 *Let k be a field extension of $\mathbb{F}_q(T)$. Let $\rho \in \mathrm{Drin}_A(k)$ be a rank 2 Drinfeld A-module given by*

$$\rho_T = T + c_1\tau + c_2\tau^2,$$

where $c_1, c_2 \in k$. Define the j-invariant of ρ_T to be

$$j(\rho_T) = \frac{c_1^{q+1}}{c_2}.$$

Proposition 2.24 ([Dor91], 239) *Let k be a field extension of $\mathbb{F}_q(T)$. Let ρ and μ be rank 2 Drinfeld A-modules given by*

$$\rho_T = T + c_1\tau + c_2\tau^2 \qquad \text{and} \qquad \mu_T = T + d_1\tau + d_2\tau^2$$

with $c_1, c_2, d_1, d_2 \in k$. Then ρ and μ are isomorphic over $\bar{k}$ if and only if

$$\frac{c_1^{q+1}}{c_2} = \frac{d_1^{q+1}}{d_2}.$$

Proof: By Proposition 2.22, ρ and μ are isomorphic over $\bar{k}$ if and only if $b\rho = \mu b$ for some $b \in \bar{k}$. But this occurs if and only if

$$bc_1 = d_1 b^q \qquad \text{and} \qquad bc_2 = d_2 b^{q^2},$$

whence upon solving for b^{q^2-1} in each equation yields

$$\frac{c_1^{q+1}}{d_1^{q+1}} = \frac{c_2}{d_2}.$$

■

As in the elliptic curves case, two Drinfeld modules of rank 2 are isomorphic if and only if they have the same j-invariant. Furthermore, given a $u \in k \setminus \{0\}$ there is a Drinfeld module with j-invariant equal to u.

Proposition 2.25 *Let k be a field extension of $\mathbb{F}_q(T)$ and let $u \in k \setminus \{0\}$. A rank 2 Drinfeld module with j-invariant u is isomorphic to $\rho_T = T + u\tau + u^q\tau^2 \in \mathrm{Drin}_A(k)$ over $\bar{k}$.*

It is noted that the definition for the j-invariant of a rank 2 Drinfeld module can be generalized to a Drinfeld module of rank r [Ham03].

Chapter 3

Torsion submodules and their Galois groups

This chapter contains information on torsion points and division polynomials of elliptic curves and Drinfeld modules. In particular, we will give the structure of field extensions generated by torsion points on elliptic curves and Drinfeld modules.

3.1 Elliptic Curves

Let k be a field with algebraic closure $\bar{k}$. Let E be an elliptic curve over a field k with basepoint O_E. For each $m \in \mathbb{Z}$ and $P \in E(\bar{k})$, let

$$[m] : E \to E$$

be the multiplication by m homomorphism given by

$$[m](P) = \begin{cases} P + P + \cdots + P & (m \text{ terms}) \text{ if } m > 0, \\ -P - P - \cdots - P & (m \text{ terms}) \text{ if } m < 0, \\ O_E & \text{if } m = 0, \end{cases}$$

We say that a point $P \in E(\bar{k})$ is an *m-torsion point* if $[m](P) = O_E$. The the set of m-torsion points on E is precisely the kernel of $[m]$, and hence forms a subgroup of $E(\bar{k})$, denoted by $E[m]$.

Now suppose that k has characteristic p. If $p = 0$ or if gcd(p, m) = 1 then

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

For $m = p^e, e \in \mathbb{Z}_{\geq 1}$, one has

$$E[p^e] \cong \{O_E\} \qquad \text{for all } e = 1, 2, 3, \ldots; \text{ or}$$

$$E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z} \qquad \text{for all } e = 1, 2, 3, \ldots \textit{ ([Sil86], p.89)}$$

Hence, if m is prime to p then $\mathrm{Aut}(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z})$ with respect to a chosen basis for $E[m]$. It is also noted that if $gcd(m, n) = 1$ then using the fundamental theorem of finitely generated abelian groups and p-primary decomposition, $E[mn] \cong E[m] \times E[n]$.

Let E be an elliptic curve over a field k with a Weierstrass model over k and let

$$k_{E,m} = k(\{x, y \mid (x, y) \neq O_E \in E[m](\bar{k})\})$$

be the field extension generated by the x, y-coordinates of the nontrivial m-torsion points in $E(\bar{k})$ and denote its Galois group over k by $G_{E,m}$. It is noted that $k_{E,m}$ and $G_{E,m}$ are invariant under isomorphisms over k (hence, invariant when choosing a Weierstrass model). Then $G_{E,m}$ acts on an m-torsion point $P = (x, y) \in E(\bar{k})$ by the rule

$${}^{\sigma}P = ({}^{\sigma}x, {}^{\sigma}y).$$

Furthermore, $G_{E,m}$ acts linearly on $E[m]$ since ${}^{\sigma}(P + Q) = {}^{\sigma}P + {}^{\sigma}Q$. This follows as the coefficients in the formulae for $P + Q$ are in k as E is defined over k. Therefore, if $P \in E(\bar{k})$ is an m-torsion point then

$$[m]({}^{\sigma}P) = {}^{\sigma}([m](P)) = {}^{\sigma}O_E = O_E,$$

and σ is indeed an automorphism of $E[m]$. Thus, the action of $G_{E,m}$ on $E[m]$ gives rise to a homomorphism

$$\begin{aligned} \varphi_{E,m} : \; G_{E,m} &\to \mathrm{Aut}(E[m]) \\ \sigma &\mapsto (P \mapsto {}^{\sigma}P). \end{aligned}$$

Consider a nontrivial automorphism $\sigma \in G_{E,m}$. Since σ acts nontrivially on at least one coordinate of an m-torsion point in $E(\bar{k})$, it must be the case that $\varphi_{E,m}(\sigma)$ acts

nontrivially on at least one m-torsion point in $E(\bar{k})$. Therefore, the kernel of $\varphi_{E,m}$ is trivial and $\varphi_{E,m}$ is injective. We conclude that $\varphi_{E,m}$ identifies $G_{E,m}$ with a subgroup of $GL_2(\mathbb{Z}/m\mathbb{Z})$ for m prime to char k.

We can now make precise the notion of the Galois group of the field generated by the x-coordinates of torsion points on an elliptic curve.

Definition 3.1 *Let E be an elliptic curve over a field k. Then we define*

$$k'_{E,m} = k(\{x \mid (x,y) \in E[m](\bar{k})\})$$

to be the field extension generated by the x-coordinates of the nontrivial m-torsion points of E and we denote its Galois group over k by $G'_{E,m}$.

We have seen that for m prime to char k, $G_{E,m}$ is isomorphic to a subgroup of $GL_2(\mathbb{Z}/m\mathbb{Z})$. Using this information, we can give the structure of $G'_{E,m}$.

Lemma 3.2 *Let E be an elliptic curve over a field k. Then, $x(P) = x(S)$ if and only if $P = \pm S$ for every $P, S \in E(\bar{k})$.*

Proof: Let E be given by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

and suppose that $P, S \in E(\bar{k})$ and $x(P) = x(S) = a$. Suppose that $P = (a,b)$ and $S = (a,c)$, then

$$b^2 + a_1ab + a_3b = a^3 + a_2a^2 + a_4a + a_6 \qquad \text{and} \tag{3.1}$$

$$c^2 + a_1ac + a_3c = a^3 + a_2a^2 + a_4a + a_6. \tag{3.2}$$

Subtracting (3.2) from (3.1) gives

$$(b-c)(b+c+a_1a+a_3) = 0.$$

Hence, $b = c$ or $b = -c - a_1a - a_3$ and $P = \pm S$ by Lemma 2.16.

■

Lemma 3.3 *Let E be an elliptic curve over a field k with characteristic p. If m is prime to p, then the homomorphism $\phi_{E,m} : G_{E,m} \to GL_2(\mathbb{Z}/m\mathbb{Z})$ factors to a homomorphism*

$$\phi'_{E,m} : G'_{E,m} \to GL_2(\mathbb{Z}/m\mathbb{Z})/\{\pm 1\}.$$

In particular, $\phi_{E,m}$ identifies $G'_{E,m}$ with a subgroup of $GL_2(\mathbb{Z}/m\mathbb{Z})/\{\pm 1\}$.

Proof: Suppose that $g \in G_{E,m}$ and $\phi_{E,m}(g) = \pm 1$, then $g(P) = \pm P$ for all $P \in E[m](\bar{k})$. From Lemma 3.2, $g(P) = \pm P$ if and only if $x(P) = x(g(P))$. Hence g fixes $k'_{E,m}$. Therefore, $\phi_{E,m}(g) = \pm 1$ if and only if g fixes $k'_{E,m}$. The result then follows from the first isomorphism theorem.

■

Suppose that char $k \neq 2, 3$ and consider an elliptic curve E over k. From Lemma 2.13, E has a short Weierstrass form given by

$$E : y^2 = x^3 + Ax + B,$$

where $A, B \in k$. Define *division polynomials* $\psi_m \in k[x, y]$ of E inductively as follows:

$$\psi_1 = 1, \qquad \psi_2 = 2y,$$

$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$

$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \qquad (m \geq 2),$$

$$2y\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \qquad (m \geq 3).$$

Further define polynomials ϕ_m and ω_m by

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$$

$$4y\omega_m = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2.$$

Then ψ_m (for m odd) and $(2y)^{-1}\psi_m$ (for m even) are polynomials in $k[x]$. Furthermore,

$$[m]P = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3}\right)$$

for every point $P \in E(\bar{k})$ ([Sil86], p.105). Therefore, the m-torsion points in $E(\bar{k})$ are precisely the roots of the division polynomial $\psi_m(x)$. We then get that $G'_{E,m}$ is equal to the Galois group of ψ_m over k. Since we are interested in cubic and quartic polynomials, we must check for which values of m does ψ_m have a cubic or quartic factor over k.

If $n, m \in \mathbb{Z}$ and n divides m then it must be the case that ψ_n divides ψ_m since n-torsion points are also m-torsion points. For this reason, we introduce the concept of new torsion points.

Definition 3.4 *Let E be an elliptic curve defined over k and let $m \in \mathbb{Z}$. Then denote the set of points of order exactly m by $E[m]^*$.*

Lemma 3.5 *Let E be an elliptic curve defined over a field k, and let $m \in \mathbb{Z}_{>0}$, with m prime to char k, have prime factorization $p_1^{e_1} \cdots p_r^{e_r}$. Then*

$$|E[m]^*| = \prod_{i=1}^{r} p_i^{2(e_i-1)}(p_i^2 - 1).$$

Proof: Let $f : \mathbb{Z} \to \mathbb{Z}$ be a function defined by

$$f(m) = |E[m]^*|.$$

We prove the result by considering three cases.

(i) Let $m = p^r$, where p is prime. The only proper divisors of p^r are $p^{r-1}, \ldots, p, 1$. Futhermore, $E[p^i] \subset E[p^{r-1}]$ for all $i < r$. Therefore,

$$\begin{aligned} f(m) &= p^{2r} - \left(p^{r-1}\right)^2 \\ &= p^{2(r-1)}(p^2 - 1), \end{aligned}$$

which completes this case.

(ii) Let $m = p_1 \cdots p_r$, where $p_1, \ldots, p_r$ are distinct primes. Then using the inclusion-exclusion principle, we have

$$\begin{aligned} f(m) &= (p_1 \cdots p_r)^2 - \sum_{1 \le i_1 < \cdots < i_{r-1} \le r} (p_{i_1} \cdots p_{i_{r-1}})^2 + \cdots + (-1)^{r-1} \sum_{i=1}^{r} p_i^2 + (-1)^r \\ &= \prod_{i=1}^{r} (p_i^2 - 1), \end{aligned}$$

which completes this case.

(iii) Let $m = p_1^{e_1} \cdots p_r^{e_r}$, where $p_1, \ldots, p_r$ are distinct primes. We note that if $m = p^r s$, where p is a prime such that $p \nmid s$, then

$$\begin{aligned} f(p^r s) &= (p^r s)^2 - (p^{r-1}s)^2 + (p^{r-1})^2 - (p^r)^2 \\ &= p^{2(r-1)}((ps)^2 - s^2 - p^2 + 1) \\ &= p^{2(r-1)} f(ps) \end{aligned} \tag{3.3}$$

Therefore, we have

$$f(m) = p_1^{2(e_1-1)} \cdots p_r^{2(e_r-1)} f(p_1 \cdots p_r).$$

The result then follows from the previous case.

■

Suppose $m > 3$, then by Lemma 3.5 there are at least 12 new points of order m. Therefore, there are at least 6 new x-coordinates that correspond to the new points of order m. This implies that upon dividing ψ_m by ψ_n, for all n dividing m, we are left with a polynomial of degree at least 6. Since we are investigating polynomials of degree at most 4, we restrict the torsion points of interest to be of order 2 and 3.

We would like to limit our study to isomorphism classes of elliptic curves. However, to do so, we must check that the field extension generated by the x-coordinates of the m-torsion points on an elliptic curve is invariant under isomorphisms. In the case where the j-invariant is not 0 or 1728, we can say more.

Corollary 3.6 *Let k be a field with algebraic closure $\bar{k}$ and let E_1, E_2 be two elliptic curves over k given in short Weierstrass form with j-invariants not equal to 0 or 1728. Suppose $\phi : E_1 \to E_2$ is an isomorphism over $\bar{k}$. Then $x(\phi(P)) = \alpha x(P)$ for all $P \in E_1(\bar{k})$, where $\alpha \in k \setminus \{0\}$.*

Proof: If char $k = 2, 3$ then the result follows directly from the proof of Lemma 2.14(a). Suppose char $k \neq 2, 3$. Then using the same notation as in the proof of Lemma 2.14(a), E_1 and E_2 are given by

$$E_1 : y^2 = x^3 + Ax + B \qquad \text{and} \qquad E_2 : (y')^2 = (x')^3 + A'x' + B'$$

for some $A, A', B, B' \in k$. An isomorphism from E to E' that preserves the short Weierstrass form is given by $(x, y) = (u^2x', u^3y')$ where $u \in \bar{k}$ satisfies $u^6 = B/B'$ and $u^4 = A/A'$. Clearly $u^2 \in k$, which completes the proof.

■

By Corollary 3.6, if two elliptic curves E and E' are isomorphic over $\bar{k}$ with j-invariants not equal to 0 or 1728, then $G'_{E,m} \cong G'_{E',m}$, as desired. We refer the reader to the appendix for the cases where the j-invariant is 0 or 1728.

Let E be an elliptic curve over k with j-invariant u. Then the x-coordinates of the non-trivial 2 and 3-torsion points on E are precisely the respective roots of

$$\psi_2(x) = 4x^3 + x^2 - \frac{144}{u - 1728}x - \frac{4}{u - 1728}, \text{ and}$$

$$\psi_3(x) = 3x^4 + x^3 - \frac{216}{u - 1728}x^2 - \frac{12}{u - 1728}x - \frac{u - 432}{(u - 1728)^2}.$$

3.2 Drinfeld modules

Let $A = \mathbb{F}_q[T]$ and let k be an extension of $\mathbb{F}_q$. If $\rho \in Drin_A(k)$, then we say that a point $\lambda \in \bar{k}$ is an *a-torsion point* of ρ if $\rho_a(\lambda) = 0$, where $a \in A$. The set of torsion points of ρ is a A-submodule of $\bar{k}_\rho$ given by

$$\Lambda_\rho = \{\lambda \in \bar{k} \mid \rho_a(\lambda) = 0 \text{ for some nonzero } a \in A\}.$$

By fixing an $a \in A$, we define the submodule $\Lambda_\rho[a]$ of Λ_ρ to be

$$\Lambda_\rho[a] = \{\lambda \in \bar{k} \mid \rho_a(\lambda) = 0\}.$$

The field extension of k generated by the points in $\Lambda_\rho[a]$ is denoted by $k_{\rho,a}$ and its Galois group over k is denoted by $G_{\rho,a}$.

Proposition 3.7 ([Ros02], p.221) *Let $\rho \in \mathrm{Drin}_A(k)$ be a Drinfeld A-module of rank r over k. Then*

$$\Lambda_\rho[a] \cong (A/aA)^r$$

for all $a \notin \ker \delta$.

The action of $G_{\rho,a}$ on $\Lambda_\rho[a]$ gives rise to a homomorphism

$$\begin{aligned} \varphi_{\rho,a}: \ G_{\rho,a} &\to \Lambda_\rho[a] \\ \sigma &\mapsto (\lambda \mapsto^\sigma \lambda). \end{aligned}$$

Consider a nontrivial automorphism $\sigma \in G_{\rho,a}$. Since σ acts nontrivially on at least one a-torsion point in $\Lambda_\rho[a]$, it must be the case that $\varphi_{\rho,a}(\sigma)$ acts nontrivially on at least one a-torsion point in $\Lambda_\rho[a]$. Therefore, the kernel of $\varphi_{\rho,a}$ is trivial and $\varphi_{\rho,a}$ is injective. We conclude that $\varphi_{\rho,a}$ identifies $G_{\rho,a}$ with a subgroup of $GL_r(A/aA)$ for $a \notin ker\ \delta$.

In the elliptic curve case, we considered the field extensions generated by the x-coordinates of torsion points. For Drinfeld modules, the analogue to x-coordinates are the $q-1$ power of torsion points.

Definition 3.8 *Let $\rho \in \mathrm{Drin}_A(k)$ and denote the algebraic closure of k by $\bar{k}$. Define the set $\Lambda_\rho[a]'$ to be*

$$\Lambda_\rho[a]' = \{\lambda^{q-1} \in \bar{k} \mid \rho_a(\lambda) = 0\}.$$

We call the points in $\Lambda_\rho[a]'$ x-coordinates of $\Lambda_\rho[a]$.

We denote the field extensions of k generated by the points in $\Lambda_\rho[a]'$ by $k'_{\rho,a}$. Furthermore, we denote the Galois group of $k'_{\rho,a}$ over k by $G'_{\rho,a}$. What then is the structure of $G'_{\rho,a}$?

Lemma 3.9 *Let ρ be a Drinfeld A-module of rank r over k and let $a \in A$. Then the homomorphism $\phi_{\rho,a} : G_{\rho,a} \to GL_r(A/aA)$ factors to a homomorphism $\phi'_{\rho,a} : G'_{\rho,a} \to GL_r(A/aA)/\mu_{q-1} \cong PGL_r(A/aA)$, where μ_{q-1} is the group of $q-1$ roots of unity in A. In particular, $\phi_{\rho,a}$ identifies $G'_{\rho,a}$ with a subgroup of $PGL_r(A/aA)$.*

Proof: Suppose that $g \in G_{\rho,a}$ and $\phi_{\rho,a}(g) = \beta \in \mu_{q-1}$, then $g(b) = \beta b$ for all $b \in \Lambda_\rho[a]$. However, $g(b) = \beta b$ if and only if $g(b^{q-1}) = b^{q-1}$. Hence g fixes $k'_{\rho,a}$. Therefore, $\phi_{\rho,a}(g) = \beta$ if and only if g fixes $k'_{\rho,a}$. The result then follows from the first isomorphism theorem.

■

Definition 3.10 *Let $a \in A$ and $\rho \in \mathrm{Drin}_A(k)$ be given by*

$$\rho_a = c_n\tau^n + c_{n-1}\tau^{n-1} + \cdots + c_1\tau + a$$

where $c_1, \ldots, c_n \in k$. Define the a-division polynomial of ρ to be

$$\psi_a(x) = x^{q^n-1} + \frac{c_{n-1}}{c_n}x^{q^{n-1}-1} + \cdots + \frac{c_1}{c_n}x^{q-1} + \frac{a}{c_n}.$$

Remark 3.11 *Since ρ is an $\mathbb{F}_q$-algebra homomorphism taking 1 to τ^0, we have $\rho_\alpha = \alpha\tau^0$ for all $\alpha \in \mathbb{F}_q$. Also, $\rho_{\alpha a} = \rho_\alpha\rho_a = \alpha\rho_a$ for all $\alpha \in \mathbb{F}_q$ and $a \in A$ so that $\Lambda_\rho[\alpha a] = \Lambda_\rho[a]$. Therefore, $\Lambda_\rho[a]$ is invariant when a is replaced by non-zero scalar multiples of itself.*

Since $q-1$ divides every exponent of x in ψ_a, we can consider ψ_a as a polynomial in x^{q-1}. We denote ψ_a considered as a polynomial in x^{q-1} by ψ'_a. Using Definition 2.20, ψ_a has degree $q^{r\,deg_T(a)} - 1$ and ψ'_a has degree $q^{r\,deg_T(a)-1} + q^{r\,deg_T(a)-2} + \cdots + q + q^0$.

Given $\rho \in Drin_A(k)$ and $a \in A$, we are interested in calculating $G_{\rho,a}$ and $G'_{\rho,a}$ using the division polynomials ψ_a and ψ'_a respectively. As we are equipped to deal with cubic and quartic polynomials, we will investigate Drinfeld modules $\rho \in Drin_A(k)$ and elements $a \in A$ that give rise to cubic and quartic division polynomials. That is, we consider all values for q, r, and $deg_T(a)$ such that

$$q^{r\,deg_T(a)} - 1 \leq 4, \text{ or}$$

$$q^{r\,deg_T(a)-1} + q^{r\,deg_T(a)-2} + \cdots + q + q^0 \leq 4.$$

Suppose $q^{r\,deg_T(a)} - 1 \leq 4$. If $q = 2$ then the possible values for r are 1 and 2. If $r = 1$ then the value of $deg_T(a)$ can be 1 or 2, otherwise the value of $deg_T(a)$ must be 1.

If $q = 3, 5$ then $r = deg_T(a) = 1$. If $q > 5$ then the inequality does not hold. Now suppose

$$q^{r\,deg_T(a)-1} + q^{r\,deg_T(a)-2} + \cdots + q + q^0 \leq 4.$$

First note that if $r = deg_T(a) = 1$ then the inequality holds for any value of q. Suppose $rdeg_T(a) > 1$. If $q = 2$ then the possible values of r are 1 and 2. If $r = 1$ then the value of $deg_T(a)$ must be 2. If $r = 2$ then $deg_T(a) = 1$. If $q = 3$ then $r = 1$ and $deg_T(a) = 2$, or $r = 2$ and $deg_T(a) = 1$. If $q > 4$, the inequality does not hold. In addition to studying division polynomials of degree less than 5, we can study the $(T + \alpha)$-division polynomial for a rank 1 Drinfeld module due to its special form, namely, $\phi_{T+\alpha} = x^{q-1} + (T + \alpha)/u$, where $\rho_{T+\alpha} = u\tau + T + \alpha$. The values for q, r, and $deg_T(a)$ given above are shown in Table 3.1.

Table 3.1: Drinfeld modules that give rise to polynomials of degree at most four

Rank of the Drinfeld module	q	$a \in A = \mathbb{F}_q[T]$ $\alpha_1, \alpha_2 \in \mathbb{F}_q$	$f(x)$	$deg\ f$
1	q	$T + \alpha_1$	ψ_a	$q - 1$
1	q	$T + \alpha_1$	ψ'_a	1
1	2	$T^2 + \alpha_1 T + \alpha_2$	$\psi'_a = \psi_a$	3
1	3	$T^2 + \alpha_1 T + \alpha_2$	ψ'_a	4
2	2	$T + \alpha_1$	$\psi'_a = \psi_a$	3
2	3	$T + \alpha_1$	ψ'_a	4

As seen in the proof of Proposition 3.7, a Drinfeld module $\rho \in Drin_A(k)$ acting on $a \in A$ is of the form

$$\rho_a = c_n\tau^n + c_{n-1}\tau^{n-1} + \cdots + c_1\tau + a$$

where $c_1, \ldots, c_n \in k$ and $deg_\tau(\rho_a) = n$. Applying ρ_a to x gives the following polynomial in $k[x]$

$$\begin{aligned}\rho_a(x) &= c_n x^{q^n} + c_{n-1}x^{q^{n-1}} + \cdots + c_1 x^q + ax \\ &= c_n x\left(x^{q^n-1} + \frac{c_{n-1}}{c_n}x^{q^{n-1}-1} + \cdots + \frac{c_1}{c_n}x^{q-1} + \frac{a}{c_n}\right) \\ &= c_n x \psi_a(x)\end{aligned}$$

Therefore, $\Lambda_\rho[a] = \{\lambda \in \bar{k} \mid \psi_a(\lambda) = 0\} \cup \{0\}$ and $G_{\rho,a}$ is equal to the Galois group of $\psi_a(x)$ over k. Similarly, $\Lambda_\rho[a]' = \{\lambda^{q-1} \in \bar{k} \mid \psi_a(\lambda) = 0\} \cup \{0\}$ and $G'_{\rho,a}$ is equal to the Galois group of ψ'_a over k.

We would like to limit our study to isomorphism classes of Drinfeld modules. As seen in Table 3.1, we are only studying $G'_{\rho,a}$. However, to do so, we must check that the field extension generated by the x-coordinates of the a-torsion points on a Drinfeld module is invariant under isomorphisms.

Lemma 3.12 *Let k be a field with an algebraic closure $\bar{k}$ and let ρ, θ be two Drinfeld A-modules over k. Suppose $\rho \cong \theta$ over $\bar{k}$. Then $k'_{\rho,a} = k'_{\theta,a}$.*

Proof: Let $\rho_a = c_n\tau^n + c_{n-1}\tau^{n-1} + \cdots + c_1\tau + a$ and $\theta_a = d_n\tau^n + d_{n-1}\tau^{n-1} + \cdots + d_1\tau + a$. Since $\rho \cong \theta$, there exists a $b \in \bar{k}$ such that $b\rho = \theta b$. Equating the coefficients of τ, we get

$$c_i = d_i b^{q^i - 1} \qquad \text{for } 1 \leq i \leq n.$$

Let $f(x)$ be the a-division polynomial for ρ and $g(x)$ be the a-division polynomial for θ. Then it is easily checked that $g(x) = b^{q^n-1} f(x/b)$. Therefore, if $\lambda^{q-1} \in \Lambda_\rho[a]'$ then $f(\lambda) = 0$ and $g(b\lambda) = 0$. So $b^{q-1}\lambda^{q-1} \in \Lambda_\theta[a]'$. It remains to show that $b^{q-1} \in k$. But this is clear, since $c_1 = d_1 b^{q-1}$ and $c_1, d_1 \in k$. Since the elements of $\Lambda_\rho[a]'$ and $\Lambda_\theta[a]'$ differ by scalar multiples in k, we have $k'_{\rho,a} = k'_{\theta,a}$.

■

We now compute the division polynomials of rank 1 and 2 Drinfeld modules using the values listed in Table 3.1. First, let ρ be a rank 1 Drinfeld A-module over k. From Lemma 3.12, $G'_{\rho,a}$ is invariant under isomorphism classes. Since there is only

one isomorphism class of rank 1 Drinfeld A-modules, it suffices to only consider the Carlitz module given by $\rho_T = T + \tau$. If $deg_T(a) = 1$ then $a = T + \alpha$, and ρ_a and ψ'_a are given by

$$\rho_a = a + \tau \qquad \text{and} \qquad \psi'_a(x) = x + (T + \alpha_1).$$

If a has degree 2 in T, then $a = T^2 + \alpha_1 T + \alpha_2$ and

$$\rho_a = a + (\alpha_1 + T + T^q)\tau + \tau^2,$$

$$\psi'_a = x^{q^2-1} + (T^q + T + \alpha_1)x^{q-1} + a.$$

Next, let ρ be a rank 2 Drinfeld module with j-invariant u. Then ρ gives rise to a cubic or quartic division polynomial precisely when ρ acts on $T + \alpha_1$, where $\alpha_1 \in \mathbb{F}_q$, and q is 2 or 3, yielding

$$\psi'_{T+\alpha_1} = x^{q^2-1} + \frac{1}{u^{q-1}}x^{q-1} + \frac{T + \alpha_1)}{u^q}.$$

3.3 Galois groups

This section is concerned with finding criteria to determine the Galois group of a polynomial. Let f be a polynomial of degree n over a field k with distinct roots and with Galois group G over k. As seen in the previous section, G is isomorphic to a subgroup of S_n and if f is irreducible then G is transitive.

The discriminant of f is used to determine if G is isomorphic to a subgroup of A_n (the group of even permutations). The general definition of a discriminant is used for fields of characteristic not equal to two, whereas in fields of characteristic 2 the Berlekamp discriminant is used.

Definition 3.13 ([Gar86], p.111) *Let f be a polynomial of degree n over a field k. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in a splitting field extension of k. Then the discriminant of f, denoted Δ, is defined as δ^2 where*

$$\delta = \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i).$$

The discriminant of a quadratic polynomial $f(x) = ax^2 + bx + c$ over a field k with char $k \neq 2$ is $b^2 - 4ac$. To ease the computation of cubic and quartic polynomials, we first make a linear transformation to eliminate the trace term of the polynomial. The general form of a monic cubic polynomial over a field k is $x^3 + a_2x^2 + a_1x + a_0$, where $a_0, a_1, a_2 \in k$. If char $k \neq 3$ then replacing x with $x - a_2/3$ yields $x^3 + px + q$ where

$$p = a_1 - \frac{1}{3}a_2^2 \qquad \text{and} \qquad q = a_0 + \frac{2}{27}a_2^3 - \frac{1}{3}a_2a_1.$$

Similarly, the general form of a monic quartic polynomial over a field k is $x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, where $a_0, a_1, a_2, a_3 \in k$. If char $k \neq 2$ then replacing x with $x - a_2/4$ yields $x^4 + px^2 + qx + r$ where

$$p = a_2 - \tfrac{3}{8}a_3^2,$$

$$q = -\tfrac{1}{2}a_2a_3 + \tfrac{1}{8}a_3^3 + a_1,$$

$$r = -\tfrac{1}{4}a_1a_3 + a_0 + \tfrac{1}{16}a_2a_3^2 - \tfrac{3}{256}a_3^4.$$

Lemma 3.14 ([Gar86], p.113) *Let k be a field with char $k \neq 2$ and let $f(x) = x^3 + px + q$ be a polynomial in $k[x]$. Then the discriminant of f is*

$$\Delta = -4p^3 - 27q^2.$$

Lemma 3.15 ([Gar86], p.113) *Let k be a field with char $k \neq 2$ and let $f(x) = x^4 + px^2 + qx + r$ be a polynomial in $k[x]$. Then the discriminant of f is*

$$\Delta = -4p^3q^2 - 27q^4 + 16p^4r - 128p^2r^2 + 144prq^2 + 256r^3.$$

Lemma 3.16 ([Gar86], p.111) *Let k be a field of characteristic not 2 with algebraic closure $\bar{k}$. Suppose that $f \in k[x]$ is separable with n distinct roots in $\bar{k}$. Then the Galois group of f over k is isomorphic to a subgroup of A_n if and only if $\delta \in k$.*

Proof: Recall that

$$\delta = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i).$$

If t is a transposition of S_n, then t reverses the order of exactly one of the terms in the above product and $t(\delta) = -\delta$. Therefore, if $\sigma \in S_n$ then

$$\sigma(\delta) = \prod_{1 \le i < j \le n} (\sigma(\alpha_j) - \sigma(\alpha_i)) = \varepsilon_\sigma \delta,$$

where $\varepsilon_\sigma = 1$ if σ is an even permutation and $\varepsilon_\sigma = -1$ if σ is an odd permutation. Let G be the Galois group of f over k and Φ an injective map from G into S_n. If $\Phi(G) \subseteq A_n$, then $g(\delta) = \delta$ for all $g \in \Phi(G)$ so that δ is in the fixed field of G and $\delta \in k$. Suppose that $\delta \in k$, then $g(\delta) = \delta$ for all $g \in \Phi(G)$ so that $\Phi(g)$ must be an even permutation and $\Phi(G) \subseteq A_n$.

■

In a field of characteristic 2, the Berlekamp discriminant is used to test if the Galois group of a polynomial is isomorphic to a subgroup of the group of even permutations.

Definition 3.17 ([Ber76], p.315) *Let f be a monic polynomial of degree n over a field k with n distinct roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ in a splitting field extension of k. Define the Berlekamp discriminant to be*

$$\beta = \sum_{i<j} \frac{\alpha_i}{\alpha_i + \alpha_j}.$$

In a field of characteristic 2, the Berlekamp discriminant of a polynomial f is increased by one whenever any adjacent pair of roots of f is transposed. To see this, upon labeling the roots of f, consider two consecutive root indices a and b and write β as a sum of five summands:

$$\begin{aligned}\beta \;=\; & \frac{\alpha_a}{\alpha_a + \alpha_b} + \sum_{i<j<a} \frac{\alpha_i}{\alpha_i + \alpha_j} + \sum_{i<a} \left(\frac{\alpha_i}{\alpha_i + \alpha_a} + \frac{\alpha_i}{\alpha_i + \alpha_b} \right) \\ & + \sum_{b<j} \left(\frac{\alpha_a}{\alpha_a + \alpha_j} + \frac{\alpha_b}{\alpha_b + \alpha_j} \right) + \sum_{b<i<j} \frac{\alpha_i}{\alpha_i + \alpha_j}.\end{aligned}$$

Let σ be the transposition of the roots α_a and α_b. Then it is clear that $\beta^\sigma + \beta = 1$, hence $\beta^\sigma = \beta + 1$. We conclude that β is invariant under the alternating group acting on the set of roots of f when k is a field of characteristic 2, but it is not invariant under the symmetric group.

Lemma 3.18 ([Ber76], p.315) *Let $f(x)$ be a monic polynomial of degree n over a field k of characteristic 2 with n distinct roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ in a splitting field extension of k. Let G be the Galois group of f over k, and Φ be a monomorphism from G into S_n. Define*

$$b(x) = x^2 + x + C, \qquad \text{where} \qquad C = \sum_{i<j} \frac{\alpha_i \alpha_j}{\alpha_i^2 + \alpha_j^2}.$$

Then $b(x) \in k[x]$. Furthermore $\Phi(G) \subseteq A_n$ if and only if $b(x)$ has a root in k.

Proof: Since C is a symmetric function, $C \in k$ and $b(x) \in k[x]$. Then $b(\beta) = 0$ where β is the Berlekamp discriminant of f. Therefore, $b(x)$ has a root in k if and only if $\beta \in k$. From the above discussion, $\beta \in k$ if and only if $\Phi(G) \subseteq A_n$.

■

Lemma 3.19 *Let k be a field of characteristic 2 and $f \in k[x]$. Using Magma [BCP97], we compute C when f is a quadratic, cubic, and quartic polynomial.*

$$\begin{aligned} f(x) &= x^2 + ax + b, \\ C &= b/a^2, \end{aligned}$$

$$\begin{aligned} f(x) &= x^3 + ax^2 + bx + c, \\ C &= \frac{a^3c + abc + b^3 + c^2}{a^2b^2 + c^2}, \end{aligned}$$

$$\begin{aligned} f(x) &= x^4 + ax^3 + bx^2 + cx + d, \\ C &= \frac{a^4d^2 + a^3bcd + a^3c^3 + a^2b^3d + abc^3 + b^3c^2 + c^4}{a^4d^2 + a^2b^2c^2 + c^4}. \end{aligned}$$

A result given in [Sch91] shows that a cubic polynomial over the rational numbers has 3 linear factors over $\mathbb{Q}$ if and only if it has a rational root and its discriminant is a square. This result can be generalized to all fields of all characteristics using Galois theory.

Theorem 3.20 *Let f be a polynomial of degree n over a field k with n distinct roots in $\bar{k}$. Then f splits over k if and only if its discriminant is a square in k and f has*

$n-2$ roots in k. If char $k = 2$, use the Berlekamp discriminant, otherwise use the standard discriminant.

Proof: Let G be the Galois group of f over k. Then f splits over k if and only if $G = \{e\}$, or equivalently, G is isomorphic to a subgroup of $A_n \cap C_2$. By Proposition 3.16, G is isomorphic to a subgroup of A_n if and only if the discriminant of f is a square. Furthermore, G is isomorphic to a subgroup of C_2 if and only if f has $n-2$ roots in k.

■

To further determine the Galois group of a polynomial, we express the polynomial as a product of irreducible factors. The first step in this process is to test if the polynomial in question has a linear factor. In the cubic case, one method of determining if the polynomial has a linear factor is to use the formulas for its roots.

Theorem 3.21 ([Gar86], p.115) *Let k be a field with char $k \neq 2, 3$. Suppose $f(x) = x^3 + px + q \in k[x]$ has discriminant Δ, and that α_1, α_2, and α_3 are the roots of f in some splitting field extension $K|k$. Then*

$$\alpha_1 = \tfrac{1}{3}(\omega^2\beta + \omega\gamma),$$

$$\alpha_2 = \tfrac{1}{3}(\omega\beta + \omega^2\gamma),$$

$$\alpha_3 = \tfrac{1}{3}(\beta + \gamma),$$

where

$$\beta^3 = \frac{-27}{2}q + \frac{3}{2}\sqrt{-3\Delta}, \gamma^3 = \frac{-27}{2}q - \frac{3}{2}\sqrt{-3\Delta},$$

and ω is a third root of unity.

Essentially, one tries to solve f by radicals using radical extensions. Consider the extension $k(\delta)$, where $\delta^2 = \Delta$. Since $[K|k(\delta)] = 3$, we have that $\Gamma(K|k(\delta)) \cong A_3$. This implies that our next extension should be generated by a cube root of an element from k or $k(\delta)$. The proof proceeds by choosing an appropriate $\beta \in K(\omega)$, where ω is

a third root of unity, such that $k(\beta^3)|k$ is a quadratic extension and the three roots of f can be expressed in terms of β.

Given a cubic polynomial f over k, we can use its discriminant and the formulas for its roots to determine its Galois group over k. If the cubic polynomial does not have a linear factor then the Galois group is isomorphic to A_3 if and only if its discriminant is a square, otherwise it is isomorphic to S_3. If the cubic polynomial does have a linear factor, then we use the result given in Proposition 3.20 to determine if the Galois group is trivial or isomorphic to a conjugate of $\langle(1\,2)\rangle$.

We continue with determining the Galois groups of quartic polynomials. By Lemma 2.5 and Theorem 2.4, the Galois group of an irreducible separable polynomial of degree n over a field k is isomorphic to a transitive subgroup of S_n. The transitive subgroups of S_n are known for $n \leq 31$ [Coh93]. For the investigation of quartic polynomials, we begin by listing the transitive subgroups of S_4.

Lemma 3.22 ([Esc97], p.264) *The transitive subgroups of S_4 are comprised of S_4, A_4, three conjugate subgroups isomorphic to D_4, one subgroup isomorphic to V_4 (the Klein Viergruppe of order 4), and three conjugate subgroups isomorphic to C_4.*

Let S be a set of four distinct elements and S_4 the permutation group acting on S. Suppose that H is a transitive subgroup of S_4. The order of H is a multiple of 4. Hence, the possible orders of H are 4, 8, 12, and 24. If the order of H is 24 then $H = S_4$ and if the order of H is 12 then $H = A_4$. If the order of H is 8 then H is one of the three Sylow 2-subgroups of S_4 isomorphic to D_4. These three groups are

$$H_1 = \{e, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\},$$

$$H_2 = \{e, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)\},$$

$$H_3 = \{e, (14), (23), (12)(34), (13)(24), (14)(23), (1243), (1342)\}.$$

If the order of H is 4 then H must be a subgroup of H_1, H_2, or H_3. The subgroups of H_1, H_2, and H_3 of order 4 are isomorphic to the Klein Viergruppe

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\},$$

and the three mutually conjugate subgroups of S_4 isomorphic to C_4 are

$$J_1 = \{e, (1324), (12)(34), (1423)\},$$

$$J_2 = \{e, (1234), (13)(24), (1432)\},$$

$$J_3 = \{e, (1243), (14)(23), (1342)\}.$$

Remark 3.23 *If f is a quartic polynomial over a field k, then either f is irreducible and the Galois group of f over k is isomorphic to a transitive subgroup of S_4, or f is reducible and the Galois group of f either trivial, or isomorphic to a subgroup of S_3 or a conjugate of $\langle(1\,2)\rangle \times \langle(3\,4)\rangle$.*

The following two lemmas are used to test if $\Phi(G) \subseteq H_1 \cong D_4$ and if $\Phi(G) \subseteq J_1 \cong C_4$ respectively. The Galois group of an irreducible quartic can then be determined from the results of these tests.

Lemma 3.24 ([Esc97], p.267) *Let k be a field with algebraic closure $\bar{k}$. Suppose $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in k[x]$ has distinct roots in $\bar{k}$ and set*

$$R(x) = (x - (\alpha_1\alpha_2 + \alpha_3\alpha_4))(x - (\alpha_1\alpha_3 + \alpha_2\alpha_4))(x - (\alpha_1\alpha_4 + \alpha_2\alpha_3)).$$

Let G be the Galois group of f over k and Φ be a monomorphism from G into S_4. Then

$$\Phi(G) \subseteq H_1 \text{ if and only if } \alpha_1\alpha_2 + \alpha_3\alpha_4 \in k,$$
$$\Phi(G) \subseteq H_2 \text{ if and only if } \alpha_1\alpha_3 + \alpha_2\alpha_4 \in k,$$
$$\Phi(G) \subseteq H_3 \text{ if and only if } \alpha_1\alpha_4 + \alpha_2\alpha_3 \in k.$$

Proof: First we note that $R(x)$ has distinct roots in $\bar{k}$. This can be seen by supposing the contrary, that is $\alpha_1\alpha_2 + \alpha_3\alpha_4 = \alpha_1\alpha_3 + \alpha_2\alpha_4$. Factoring then yields $(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3) = 0$ and we get the contradiction that either $\alpha_1 = \alpha_4$ or $\alpha_2 = \alpha_3$.

Without loss of generality, we will prove the result for the first case, that is $\Phi(G) \subseteq H_1$ if and only if $\alpha_1\alpha_2 + \alpha_3\alpha_4 \in k$. It is noted that for every $g \in \Phi(G)$, $g(\alpha_1\alpha_2 + \alpha_3\alpha_4)$

is either $\alpha_1\alpha_2 + \alpha_3\alpha_4$, $\alpha_1\alpha_3 + \alpha_2\alpha_4$, or $\alpha_1\alpha_4 + \alpha_2\alpha_3$. Furthermore, the fixed group of $\alpha_1\alpha_2 + \alpha_3\alpha_4$ as a polynomial is precisely H_1. Suppose that $\Phi(G) \subseteq H_1$, then $g(\alpha_1\alpha_2 + \alpha_3\alpha_4) = \alpha_1\alpha_2 + \alpha_3\alpha_4$ for every $g \in \Phi(G)$ and $\alpha_1\alpha_2 + \alpha_3\alpha_4 \in k$ as desired. Conversely, suppose that $\Phi(G) \not\subseteq H_1$. Then there exists some $g \in \Phi(G)$ such that $g \notin H_1$. Since $g \notin H_1$, $g(\alpha_1\alpha_2 + \alpha_3\alpha_4) \neq \alpha_1\alpha_2 + \alpha_3\alpha_4$ and $g(\alpha_1\alpha_2 + \alpha_3\alpha_4)$ is one of the other two roots of R. Since the roots of R are distinct, g does not fix $\alpha_1\alpha_2 + \alpha_3\alpha_4$. Consequently, $\alpha_1\alpha_2 + \alpha_3\alpha_4 \notin k$.

■

Remark 3.25 *The polynomial $R(x)$ as given in Lemma 3.24 is in $k[x]$, since expanding and simplifying R gives*

$$R(x) = x^3 - a_2x^2 + (a_3a_1 - 4a_0)x + 4a_0a_2 - a_1^2 - a_0a_3^2.$$

Lemma 3.26 ([Esc97], p.268) *Let $k, \bar{k}$, f and G be as in Lemma 3.24. Suppose that $\Phi(G) \subseteq H_1 \cong D_4$ and set*

$$C(x) = (x - (\alpha_1\alpha_3^2 + \alpha_3\alpha_2^2 + \alpha_2\alpha_4^2 + \alpha_4\alpha_1^2))(x - (\alpha_2\alpha_3^2 + \alpha_3\alpha_1^2 + \alpha_1\alpha_4^2 + \alpha_4\alpha_2^2)).$$

Suppose $C(x)$ has distinct roots. Then $\Phi(G) \subseteq J_1 \cong C_4$ if and only if $\alpha_1\alpha_3^2 + \alpha_3\alpha_2^2 + \alpha_2\alpha_4^2 + \alpha_4\alpha_1^2 \in k$.

Proof: Let $a = \alpha_1\alpha_3^2 + \alpha_3\alpha_2^2 + \alpha_2\alpha_4^2 + \alpha_4\alpha_1^2$ and $b = \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2 + \alpha_1\alpha_4^2 + \alpha_4\alpha_2^2$. It is noted that for every $g \in \Phi(G) \subset H_1$, $g(a)$ is either a or b. Furthermore, the fixed group of a as a polynomial is precisely J_1. Suppose $\Phi(G) \subseteq J_1$, then $g(a) = a$ for every $g \in \Phi(G)$. Therefore, $a \in k$ as desired. Conversely, suppose that $\Phi(G) \not\subseteq J_1$. Then there exists some $g \in \Phi(G)$ such that $g \notin J_1$. Since $g(a)$ is a conjugate of a and $g \notin J_1$, $g(a) = b$. Since the roots of C are distinct, $g(a) \neq a$ and therefore $a \notin k$.

■

Remark 3.27 *Let t denote the root of $R(x)$ in k from Lemma 3.24 and $C(x)$ be as given in Lemma 3.26. Then $C(x) \in k[x]$ and is given by*

$$C(x) = x^2 + (-ta_3 + a_2a_3 - 2a_1)x - 2t^2a_2 + 2ta_1a_3 - 4ta_0 - a_0a_3^2 + a_1a_3^3 + a_2^3 \\ -5a_1a_2a_3 + t^2a_3^2 + 4a_1^2 + 4a_0a_2 - ta_2a_3^2 + ta_2^2.$$

3.4 The structure of $\mathrm{PGL}_2(\mathbb{Z}/\mathrm{m}\mathbb{Z})$

Proposition 3.28 *$PGL_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$.*

Proof: Let $G = GL_2(\mathbb{Z}/2\mathbb{Z})/\{\pm 1\} = GL_2(\mathbb{Z}/2\mathbb{Z})$. The order of G is 6. Suppose G contains an element of order 6. Then G is cyclic, hence abelian which gives a contradiction. Furthermore, G has one cyclic subgroup of order 3 and three cyclic subgroups of order 2. Let $H =< \sigma >$ be the cyclic subgroup of G of order 3 and $\tau \in G$ be an element of order 2. Then $G = H \amalg \tau H$, where H contains all elements of order dividing 3 and τH is the set of all elements in G of order 2. Then $(\tau\sigma^i)(\tau\sigma^i) = e$ and we have $\tau\sigma^i\tau = \sigma^{-i}$. In particular, $\tau^{-1}\sigma\tau = \sigma^{-1}$. Hence, $G \cong D_3 \cong S_3$ which completes the proof.

■

Proposition 3.29 *$PGL_2(\mathbb{Z}/3\mathbb{Z}) \cong S_4$.*

Proof: Let $G = PGL_2(\mathbb{Z}/3\mathbb{Z})$. Consider the map θ given by the action of G on $F = \mathbb{P}^1(\mathbb{Z}/3\mathbb{Z}) = \{[1,0],[1,-1],[1,1],[0,1]\}$. Then $\theta : G \to \Sigma_F \cong S_4$ is injective, since if $g \in G$ fixes every element of F then g must be the identity. In addition, θ is an isomorphism since $|G| = |S_4| = 24$. Therefore, $G \cong S_4$ as desired.

■

Theorem 3.30 ([Lan76], p.185) *Let F be a field of characteristic l. Let G be a finite subgroup of $GL_2(F)$, of order prime to l. Let H be the image of G in $PGL_2(F)$. Then we have the following cases.*

(i) H is cyclic.

(ii) H is dihedral.

(iii) H is isomorphic to A_4, S_4, or A_5.

Theorem 3.31 ([Lan76], p.183) *Let F be a field of characteristic l. Let G be a finite subgroup of $GL_2(F)$, of order divisible by l. Then either G is contained in a Borel subgroup (the group of upper triangular matrices), or G contains $SL_2(F)$.*

Using Theorem's 3.30 and 3.31, we can give the correspondence between subgroups of S_4 and $PGL_2(\mathbb{Z}/3\mathbb{Z})$. Let H be a subgroup of $PGL_2(\mathbb{Z}/3\mathbb{Z})$. If $|H|$ is prime to 3 then H is either cyclic or dihedral. If H is cyclic, then H is isomorphic to C_2 or C_4, which in turn is isomorphic to a conjugate of $\langle(1\,2)\rangle$ or $\langle(1\,3\,2\,4)\rangle$. If H is dihedral, then H is isomorphic to D_4 or D_2, which in turn is isomorphic to a conjugate of H_1 or V_4 as given in Lemma 3.22, or $\langle(1\,2)\rangle \times \langle(3\,4)\rangle$.

Let B a Borel subgroup of $GL_2(\mathbb{Z}/3\mathbb{Z})$ and consider B as a subgroup $GL_2(\mathbb{Z}/3\mathbb{Z})/\{\pm 1\}$, denoted by $\bar{B}$. Then $|\bar{B}| = 6$ and $\bar{B}$ is isomorphic to S_3. Let $S = SL_2(\mathbb{Z}/3\mathbb{Z})/\{\pm 1\}$. Then $|S| = 12$ and S is isomorphic to A_4. Therefore, if H is a subgroup of G of order divisible by 3, then H is isomorphic to either a subgroup of S_3, or a group containing A_4.

Chapter 4

Elliptic curves

In this chapter, we calculate the Galois groups of fields generated by the x-coordinates of torsion points on an elliptic curve. We refer the reader to Section 3.1 for background information on torsion points on elliptic curves relevant to this section. Let k be a field of characteristic p and let E be an elliptic curve over k with j-invariant u_o. From Lemma 3.3, for m prime to p, $G'_{E,m}$ is isomorphic to a subgroup of $GL_2(\mathbb{Z}/m\mathbb{Z})/\{\pm 1\}$. We wish to find necessary and sufficient algebraic conditions on u_o that determine the containment of $G'_{E,m}$ in subgroups of $GL_2(\mathbb{Z}/m\mathbb{Z})/\{\pm 1\}$.

In what follows, we categorize $G'_{E,m}$ for $m = 2, 3$ based on algebraic conditions on u_o. In several cases, we parametrize curves of genus 0 with a k-rational point in order to get algebraic conditions on u_o. These parametrizations are guaranteed to exist by Theorem 2.9.

4.1 Galois group of 2-torsion submodule

Let E be an elliptic curve over a field k. Suppose char k is 0 or prime to 2. From Proposition 3.3, $G'_{E,2}$ is isomorphic to a subgroup of $G = GL_2(\mathbb{Z}/2\mathbb{Z})/\{\pm 1\}$ and from Proposition 3.28, $G \cong S_3$. Hence, $G'_{E,2}$ is isomorphic to a subgroup of S_3. In what follows, we determine the structure of $G'_{E,2}$ by considering two cases; char $k = 2$, and char $k \neq 2$. In the case that char $k = 2$, we will see that if k is perfect then

$G'_{E,2} = G_{E,2}$.

Remark 4.1 *Suppose E is an elliptic curve over a field k of characteristic 2 with j-invariant equal to $u_o \in k \setminus \{0\}$. Then up to isomorphism over $\bar{k}$, E is of the form*

$$y^2 + xy = x^3 - \frac{1}{u_o}$$

with 2-torsion division polynomial

$$\psi_2(x) = x^2.$$

The Galois group of ψ_2 over k is trivial and the y-coordinate corresponding to $x = 0$ is $1/\sqrt{-u_o}$, hence $G'_{E,2}$ is trivial and $G_{E,2}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ if $\sqrt{-u_o} \notin k$, otherwise it is trivial. Furthermore, if k is a perfect field, then $G'_{E,2} = G_{E,2}$ and E is ordinary.

Theorem 4.2 *Let k be a field with char $k \neq 2$ and let E be an elliptic curve over k with j-invariant $u_o \in k \setminus \{0, 1728\}$. Then*

(i) $G'_{E,2}$ is trivial if and only if [1]

$$u_o = \frac{2^8(t_o^2 - t_o + 1)^3}{t_o^2(t_o - 1)^2}$$

for some $t_o \in k$;

(ii) $G'_{E,2}$ is isomorphic to a subgroup of C_2 if and only if [2]

$$u_o = \frac{(t_o + 256)^3}{t_o^2}$$

for some $t_o \in k$;

(iii) $G'_{E,2}$ is isomorphic to a subgroup of A_3 if and only if

$$u_o = t_o^2 + 1728$$

for some $t_o \in k$;

[1] *This is the Legendre family of elliptic curves with j-invariant u_o* ([Sil86], p.54).

[2] *The expression $u_o = (t_o+256)^3/t_o^2$ relates to the complex analytic parametrization of the modular curve $X_0(2)$ [Bir72].*

(iv) otherwise, $G'_{E,2} \cong S_3$.

Proof of Theorem 4.2

From Lemma 2.14, E is isomorphic over $\bar{k}$ to an elliptic curve E' with Weierstrass equation

$$y^2 + xy = x^3 - \frac{36}{u_o - 1728}x - \frac{1}{u_o - 1728}.$$

Then from Corollary 3.6, $G'_{E,m} \cong G'_{E',m}$. Therefore, it suffices to only consider the family of elliptic curves given by E'. Let $f(x) \in k[x]$ be the division polynomial of the 2-torsion points in $E'(\bar{k})$. Then f is given by

$$f(x) = \psi_2 = 4x^3 + x^2 - \frac{144}{u_o - 1728}x - \frac{4}{u_o - 1728}, \tag{4.1}$$

and the x-coordinates of the 2-torsion points in $E'(\bar{k})$ are precisely the roots of f. Furthermore, $G'_{E,2}$ is equal to the Galois group of f over k, denoted by G. The discriminant of f is

$$\frac{16u_o^2}{(u_o - 1728)^3},$$

which is never equal to 0 since $u_o \neq 0$. Therefore, the roots of f are distinct. Let Φ be a choice of monomorphism $G \hookrightarrow S_3$ after labeling the roots of f. Then it suffices to categorize $\Phi(G)$ based on algebraic conditions on u_o. We begin by giving constraints on u_o that determine the factorization of f over k.

Proposition 4.3 *Let k be a field with char $k \neq 2$ and $u_o \in k \setminus \{0, 1728\}$, and let f be as given in (4.1). Then f has a linear factor over k if and only if*

$$u_o = \frac{(t_o + 256)^3}{t_o^2}$$

for some $t_o \in k$.

Proof: If $u_o = (t_o + 256)^3/t_o^2$ for some $t_o \in k$ then f factors as

$$\left(4x + \frac{t_o}{t_o - 512}\right)\left(x^2 - \frac{128}{t_o - 512}x - \frac{4t_o}{(t_o + 64)(t_o - 512)}\right).$$

Conversely, suppose f has a linear factor over k. Then

$$4\alpha^3 + \alpha^2 - \frac{144}{u_o - 1728}\alpha - \frac{4}{u_o - 1728} = 0$$

for some $\alpha \in k$. Solving for u_o in terms of α gives

$$u_o = \frac{4(12\alpha + 1)^3}{\alpha^2(4\alpha + 1)}.$$

Then there is a Möbius transformation, namely $t_o = 2048\alpha/(4\alpha + 1)$, such that

$$u_o = \frac{(t_o + 256)^3}{t_o^2}.$$

■

Proposition 4.4 *Let k be a field with char $k \neq 2$ and $u_o \in k \setminus \{0, 1728\}$, and let f be as given in (4.1). Then f has three linear factors over k if and only if*

$$u_o = \frac{2^8(t_o^2 - t_o + 1)^3}{t_o^2(t_o - 1)^2}$$

for some $t_o \in k$.

Proof: If

$$u_o = \frac{2^8(t_o^2 - t_o + 1)^3}{t_o^2(t_o - 1)^2}$$

for some $t_o \in k$, then f factors as

$$\left(4x - \frac{t_o}{(2t_o - 1)(t_o - 2)}\right)\left(x + \frac{t_o(t_o - 1)}{4(t_o + 1)(t_o - 2)}\right)\left(x + \frac{t_o - 1}{4(t_o + 1)(2t_o - 1)}\right).$$

Conversely, suppose f has three linear factors over k. By Proposition 4.3, there exists some $s_o \in k$ such that

$$u_o = \frac{(s_o + 256)^3}{s_o^2} \tag{4.2}$$

and the quadratic term of f in terms of s_o is

$$g(x) = x^2 - \frac{128}{s_o - 512}x - \frac{4s_o}{(s_o + 64)(s_o - 512)}.$$

Then the discriminant of g over k, namely

$$\frac{16(s_o + 256)^2}{(s_o - 512)^2(s_o + 64)},$$

is a square in k. Therefore, there exists some $n_o \in k$ such that

$$n_o^2 = s_o + 64, \text{ and}$$
$$u_o = \frac{(n_o^2 + 192)^3}{n_o^6}.$$

Furthermore, there is a Möbius transformation, namely $t_o = (n_o - 8)/(n_o + 8)$, such that

$$u_o = \frac{2^8(t_o^2 - t_o + 1)^3}{t_o^2(t_o - 1)^2}.$$

■

Let us now return to the proof of Theorem 4.2. Clearly, $\Phi(G) = \{e\}$ if and only if f has three linear factors over k. Part (i) then follows from Proposition 4.4. $\Phi(G)$ is contained in a conjugate of $\langle(1\,2)\rangle$ if and only if f has a linear factor over k. Part (ii) then follows from Proposition 4.3. The discriminant of f, namely

$$\frac{16u_o^2}{(u_o - 1728)^3},$$

is a square in k if and only if $u_o = t_o^2 + 1728$ for some $t_o \in k$. Part (iii) then follows directly from Lemma 3.16. Part (iv) is clear since the only proper nontrivial subgroups of S_3 are A_3 and conjugates of $\langle(1\,2)\rangle$.

4.2 Galois group of 3-torsion submodule

Let E be an elliptic curve over a field k. Suppose char k is 0 or prime to 3. From Proposition 3.3, $G'_{E,3}$ is isomorphic to a subgroup of $G = GL_2(\mathbb{Z}/3\mathbb{Z})/\{\pm 1\} = PGL_2(\mathbb{Z}/3\mathbb{Z})$ and from Proposition 3.29, $G \cong S_4$. Hence, $G'_{E,3}$ is isomorphic to a subgroup of S_4. As we have seen in Section 3.4, the subgroups of $PGL_2(\mathbb{Z}/3\mathbb{Z})$ are isomorphic to C_2, C_4, D_2, D_4, S_3, A_4, S_4, or a Borel subgroup. In what follows, we determine $G'_{E,3}$ by considering two cases; char $k = 3$, and char $k \neq 3$.

Remark 4.5 *Suppose E is an elliptic curve over a field k of characteristic 3 with j-invariant equal to $u_o \in k \setminus \{0\}$. Then up to isomorphism over $\bar{k}$, E is of the form*

$$y^2 + xy = x^3 - \frac{1}{u_o}$$

with 3-torsion division polynomial

$$\psi_3 = x^3 - \frac{1}{u_o}.$$

The Galois group of ψ_3 over k is trivial. Suppose k is a perfect field, then the 3-torsion points on E are $(1/u_o, 0)$, $(1/u_o, 2/u_o)$, and O_E. Therefore, $E[3] \cong \mathbb{Z}/3\mathbb{Z}$ and E is ordinary.

Theorem 4.6 *Let k be a field with char $k \neq 3$ and let E be an elliptic curve over k with j-invariant $u_o \in k \setminus \{0, 1728\}$. Then*

(i) $G'_{E,3}$ is trivial if and only if $G'_{E,3}$ is isomorphic to a subgroup of C_2 and x^2+x+1 has a root in k;

(ii) $G'_{E,3}$ is isomorphic to a subgroup of C_2 if and only if

$$u_o = \frac{27(t_o^2 - 2t_o + 4)^3 t_o^3 (t_o + 2)^3}{(t_o - 1)^3 (t_o^2 + t_o + 1)^3} \qquad [C_2]$$

for some $t_o \in k$;

(iii) $G'_{E,3}$ is isomorphic to a subgroup of A_3 if and only if $x^2 + x + 1$ has a root in k and

$$u_o = \frac{27t_o(t_o + 8)^3}{(t_o - 1)^3} \qquad [\subset B]$$

for some $t_o \in k$;

(iv) $G'_{E,3}$ is isomorphic to a subgroup of S_3 if and only if

$$u_o = \frac{27t_o(t_o + 8)^3}{(t_o - 1)^3} \qquad [B]$$

for some $t_o \in k$;

(v) $G'_{E,3}$ is isomorphic to a subgroup of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if and only if

$$u_o = -\frac{(t_o + 9)^3 (t_o - 3)^3}{t_o^3} \qquad [D_2]$$

for some $t_o \in k$;

(vi) $G'_{E,3}$ *is isomorphic to a subgroup of* C_4 *if and only if char* $k = 2$ *and*

$$u_o = \frac{1}{(t_o^2 + t_o + 1)^3} \qquad [C_4]$$

for some $t_o \in k$, *or char* $k \neq 2$ *and* $u_o = t_o^3$ *for some* $t_o \in k$ *and there exists some* $v_o \in k$ *such that* $-3(v_o^2 + 12v_o + 144)$ *is a square in* k;

(vii) $G'_{E,3}$ *is isomorphic to a subgroup of* V_4 *if and only if* $u_o = t_o^3$ *for some* $t_o \in k$ *and* $x^2 + x + 1$ *has a root in* k;

$$[D_2]$$

(viii) $G'_{E,3}$ *is isomorphic to a subgroup of* D_4 *if and only if* $u_o = t_o^3$ *for some* $t_0 \in k$;

(ix) $G'_{E,3}$ *is isomorphic to a subgroup of* A_4 *if and only if* $x^2 + x + 1$ *has a root in* k;

(x) otherwise, $G \cong S_4$.

Proof of Theorem 4.6

From Lemma 2.14, E is isomorphic over $\bar{k}$ to an elliptic curve E' with Weierstrass equation

$$y^2 + xy = x^3 - \frac{36}{u_o - 1728}x - \frac{1}{u_o - 1728}.$$

Then from Corollary 3.6, $G'_{E,m} \cong G'_{E',m}$. Therefore, it suffices to only consider the family of elliptic curves given by E'. Let $f(x) \in k[x]$ be the division polynomial of the 3-torsion points in $E'(\bar{k})$. Then f is given by

$$f(x) = \psi_3 = 3x^4 + x^3 - \frac{216}{u_o - 1728}x - \frac{12}{u_o - 1728} - \frac{u_o - 432}{(u_o - 1728)^2}, \qquad (4.3)$$

and the x-coordinates of the 3-torsion points in $E'(\bar{k})$ are precisely the roots of f. Furthermore, $G'_{E,3}$ is equal to the Galois group of f over k, denoted by G. If char $k \neq 2$ then the discriminant of f is

$$-\frac{27u_o^4}{(u_o - 1728)^6},$$

which is not equal to zero since $u_o \neq 0$. If char $k = 2$ then the discriminant of f is a root of $x^2 + x + 1$, which clearly cannot be zero. Therefore, the roots of f are distinct.

Let Φ be a choice of monomorphism $G \hookrightarrow S_3$ after labeling the roots of f. Then it suffices to categorize $\Phi(G)$ based on algebraic conditions on u_o. We begin by giving constraints on u_o that determine the factorization of f over k.

Proposition 4.7 *Let k be a field with char $k \neq 3$ and $u_o \in k \setminus \{0, 1728\}$, and let f be as given in (4.3). Then f has a linear factor over k if and only if*

$$u_o = \frac{27t_o(t_o+8)^3}{(t_o-1)^3}$$

for some $t_o \in k$.

Proof: If

$$u_o = \frac{27t_o(t_o+8)^3}{(t_o-1)^3}$$

for some $t_o \in k$, then f factors as

$$\left(3x + \tfrac{(t_o-1)(t_o+2)}{t_o^2-20t_o-8}\right)$$

$$\left(x^3 - \tfrac{7t_o+2}{t_o^2-20t_o-8}x^2 - \tfrac{(t_o-1)(t_o^2-32t_o+4)}{3(t_o^2-20t_o-8)^2}x - \tfrac{(t_o^3+6t_o^2+228t_o+8)(t_o-1)^2}{27(t_o^2-20t_o-8)^3}\right).$$

Conversely, suppose $f(\alpha) = 0$ for some $\alpha \in k$. Then making the substitution $x = \alpha$ in f, clearing denominators, and regarding the result as a polynomial in u_o, yields

$$g(u_o) = \alpha^3(3\alpha+1)u_o^2 - (12\alpha+1)(864\alpha^3+216\alpha^2+1)u_o + 432(12\alpha+1)^4 = 0. \quad (4.4)$$

If the characteristic of k is 2 then

$$u_o = \frac{1}{\alpha^4+\alpha^3},$$

and there is a Möbius transformation, namely $t_o = 1/(\alpha+1)$, such that

$$u_o = \frac{t_o^4}{(t_o+1)^3}$$

as desired. Suppose that the characteristic of k is not 2. Then the discriminant of g regarded as a polynomial in u_o is $(12\alpha+1)^2(432\alpha^2+1)$. Since $u_o \in k$, there exists

some $v_o \in k$ such that $432\alpha^2 + 1 = v_o^2$. By parametrizing the conic $432x^2 + 1 - y^2 = 0$ with the line $y = sx + 1$, we have

$$x = \frac{-2s}{s^2 - 432}.$$

Therefore

$$\alpha = \frac{-2s_o}{s_o^2 - 432} \tag{4.5}$$

for some $s_o \in k$. Using equations (4.4) and (4.5) to solve for u_o in terms of s_o gives

$$u_o = \frac{-(s_o - 36)(s_o + 12)^3}{8(s_o + 18)}, \quad \text{or} \tag{4.6}$$

$$\frac{432(s_o - 36)^3(s_o + 12)}{s_o^3(s_o - 24)}. \tag{4.7}$$

Then there are Möbius transformations, namely

$$t_o = \begin{cases} \frac{s_o - 36}{s_o + 18} & \text{if (4.6) occurs,} \\ \\ \frac{-2(s_o + 12)}{s_o - 24} & \text{if (4.7) occurs.} \end{cases}$$

such that

$$u_o = \frac{27t_o(t_o + 8)^3}{(t_o - 1)^3} \quad \text{and}$$

$$\alpha = \frac{-(t_o - 1)(t_o + 2)}{3(t_o^2 - 20t_o - 8)}$$

as desired.

■

Proposition 4.8 *Let k be a field with char $k \neq 3$ and $u_o \in k \setminus \{0, 1728\}$, and let f be as given in (4.3). Then f has a quadratic factor over k if and only if*

$$u_o = -\frac{(t_o + 9)^3(t_o - 3)^3}{t_o^3}$$

for some $t_o \in k$.

Proof: If

$$u_o = -\frac{(t_o+9)^3(t_o-3)^3}{t_o^3}$$

for some $t_o \in k$, then f factors as

$$\left(3x^2 + \tfrac{t_o(t_o+3)}{t_o^2+27}x + \tfrac{t_o^2(t_o^3+9t_o^2+27t_o-81)}{(t_o^2+18t_o-27)(t_o^2+27)^2}\right)$$

$$\left(x^2 - \tfrac{(t_o-9)}{t_o^2+27}x + \tfrac{t_o(t_o^3+9t_o^2-81t_o+243)}{(t_o^2+18t_o-27)(t_o^2+27)^2}\right).$$

Conversely, suppose f has a quadratic factor over k. Then there exist $a, b, c, d \in k$ such that

$$\begin{aligned} f(x) &= (3x^2+ax+b)(x^2+cx+d) \\ &= 3x^4+(a+3c)x^3+(b+ac+3d)x^2+(bc+ad)x+bd. \end{aligned}$$

Equating the coefficients of the above polynomial with the coefficients of f gives

$$\begin{aligned} a+3c &= 1, \\ b+ac+3d &= \frac{-216}{u_o-1728}, \\ bc+ad &= \frac{-12}{u_o-1728}, \\ bd &= \frac{432-u_o}{(u_o-1728)^2}. \end{aligned}$$

Let $a = 1-3c$, $b = b'/(u-1728)$ and $d = d'/(u-1728)$. Then

$$b' - c(3c-1)(u_o-1728) + 3d' = -216, \tag{4.8}$$

$$b'c - 3d'c + d' = -12, \tag{4.9}$$

$$b'd' = 432 - u_o. \tag{4.10}$$

If $c = 0$ then $a = 1$, $d' = -12$, $b' = -180$, and $-12b' = 432 - u_o$ yielding $u_o = -1728$. In this case, there exists some t_o, namely $t_o = -3$, such that

$$u_o = -\frac{(t_o+9)^3(t_o-3)^3}{t_o^3}.$$

Suppose $c \neq 0$. Using equations (4.8) and (4.9) in succession to solve for b' and d' in terms of c and substituting these values in equation (4.10) gives

$$(6-\frac{1}{c})^2(c^3(3c-1)^3u_o^2 - (72c^2-24c-1)(6c-1)^4u_o + 1728(6c-1)^6) = 0.$$

There are two cases to consider; char $k = 2$ and char $k \neq 2$.

Suppose char $k = 2$. If $6 - 1/c = 0$ then we get the contradiction $1 = 0$. Therefore,

$$c^3(c-1)^3u_o^2 + u_o = 0.$$

Since $u_o \neq 0$, we have $c \neq 0, 1$ and

$$u_o = \frac{1}{c^3(c+1)^3}.$$

Then there is a Möbius transformation, namely $t_o = c/(c+1)$, such that

$$u_o = \frac{(t_o+1)^6}{t_o^3}.$$

Now suppose char $k \neq 2$. If $6 - 1/c = 0$ then we get the contradiction $u_o = 0$. Therefore,

$$h(x) = c^3(3c-1)^3x^2 - (72c^2 - 24c - 1)(6c-1)^4x + 1728(6c-1)^6$$

must have a root in k, namely u_o. The discriminant of h is

$$(1 + 36c - 108c^2)(6c-1)^6,$$

which has a square root in k since $u_o \in k$ is a zero of h. Hence, $1 + 36c - 108c^2 = v_o^2$ for some $v_o \in k$. By parametrizing the curve $1 + 36x - 108x^2 - y^2 = 0$ with the line $y = sx + 1$ we have

$$x = \frac{36 - 2s}{s^2 + 108}.$$

Therefore,

$$c = \frac{36 - 2s_o}{s_o^2 + 108}$$

for some $s_o \in k$. Furthermore, u_o in terms of s_o is given by

$$u_o = -\frac{(s_o+18)^3(s_o-6)^3}{8s_o^3}, \quad \text{or} \tag{4.11}$$

$$-\frac{1728(s_o+18)^3(s_o-6)^3}{(s_o+6)^3(s_o-18)^3}. \tag{4.12}$$

Then there are Möbius transformations, namely

$$t_o = \begin{cases} \frac{s_o}{2} & \text{if (4.11) occurs,} \\ \\ \frac{-3(s_o-18)}{s_o+6} & \text{if (4.12) occurs.} \end{cases}$$

such that

$$u_o = -\frac{(t_o+9)^3(t_o-3)^3}{t_o^3}$$

as desired.

■

Proposition 4.9 *Let k be a field with char $k \neq 3$ and $u_o \in k \setminus \{0, 1728\}$, and let f be as given in (4.3). Then f has two linear factors over k if and only if*

$$u_o = \frac{27(t_o^2-2t_o+4)^3t_o^3(t_o+2)^3}{(t_o-1)^3(t_o^2+t_o+1)^3}$$

for some $t_o \in k$.

Proof: If

$$u_o = \frac{27(t_o^2-2t_o+4)^3t_o^3(t_o+2)^3}{(t_o-1)^3(t_o^2+t_o+1)^3}$$

for some $t_o \in k$, then f factors as

$$\left(x - \frac{(t_o^3+6t_o+2)(t_o^2+t_o+1)}{3(t_o^2-2t_o-2)(t_o^4+2t_o^3+6t_o^2-4t_o+4)}\right)\left(x + \frac{(t_o-1)(t_o^3+2)(t_o^2+t_o+1)}{3(t_o^2-2t_o-2)(t_o^4+2t_o^3+6t_o^2-4t_o+4)}\right)$$

$$\left(3x^2 + \frac{(t_o^2+4t_o-2)(t_o-1)}{(t_o^2-2t_o-2)(t_o^4+2t_o^3+6t_o^2-4t_o+4)}x + \frac{(t_o^2+t_o+1)(t_o^6-6t_o^4+4t_o^3+36t_o^2-12t_o+4)(t_o-1)^2}{3(t_o^2-2t_o-2)^2(t_o^4+2t_o^3+6t_o^2-4t_o+4)^2}\right)$$

Conversely, suppose f has two linear factors over k. Then f has a linear and a quadratic factor and by Propositions 4.7 and 4.8,

$$u_o = \frac{27n_o(n_o+8)^3}{(n_o-1)^3} \quad \text{and} \quad u_o = -\frac{(m_o+9)^3(m_o-3)^3}{m_o^3}$$

for some $m_o, n_o \in k$. Equating the above values for u_o gives

$$n_o = \left(\frac{(n_o-1)(m_o+9)(m_o-3)}{-3(n_o+8)m_o}\right)^3.$$

Hence, there exists some $t_o \in k$ such that $n_o = t_o^3$ and u_o in terms of t_o is

$$u_o = \frac{27(t_o^2-2t_o+4)^3t_o^3(t_o+2)^3}{(t_o-1)^3(t_o^2+t_o+1)^3}$$

as desired.

■

Let us now return to the proof of Theorem 4.6.

(ix) If char $k \neq 2$, then the discriminant of f is

$$-\frac{27u_o^4}{(u_o - 1728)^6},$$

which is a square in k if and only if -3 is a square in k. If char $k = 2$ then the Berlekamp discriminant of f is in k if and only if $x^2 + x + 1$ has a root in k. The result then follows from Lemmas 3.16 and 3.18.

(viii) The D_4 resolvent of f is

$$R(x) = x^3 + \frac{72}{u_o - 1728}x^2 + \frac{1728}{(u_o - 1728)^2}x + \frac{u_o^2 + 373248}{27(u_o - 1728)^3}.$$

If char $k = 2$, then $R(x)$ has a root in k if and only if u_o is a cube in k. Suppose char $k \neq 2$ and let c_1, c_2, and c_3 denote the roots of $g(x) = x^3 - u_o^2 \in k[x]$ in a splitting field extension of k. Then

$$R(x) = \left(x + \frac{c_1 + 72}{3(u_o - 1728)}\right)\left(x + \frac{c_2 + 72}{3(u_o - 1728)}\right)\left(x + \frac{c_3 + 72}{3(u_o - 1728)}\right)$$

by Theorem 3.21, and R has a root in k if and only if $c_i \in k$ for some $i \in \{1, 2, 3\}$. We will show that $c_i \in k$ for some $i \in \{1, 2, 3\}$ if and only if u_o is a cube in k. Suppose u_o is a cube in k and let $u_o = a^3$, for some $a \in k$. Then $g(a^2) = 0$ and $R(x)$ has a root in k. Conversely, suppose $c_i \in k$ for some $i \in \{1, 2, 3\}$. Then $c_i^3 = u_o^2$ yielding $u_o = u_o^3/c_i^3$, and u_o is a cube in k. The result then follows from Lemma 3.24.

(vii) The result follows from parts (ix) and $(viii)$ since V_4 is a subgroup of A_4 and D_4.

(vi) Suppose $\Phi(G)$ is isomorphic to a subgroup of D_4. Then there exists some $v_o \in k$ such that $u_o = v_o^3$ and R has a linear factor over k, namely

$$x + \frac{v_o^2 + 72}{3(v_o - 12)(v_o^2 + 12v_o + 144)}.$$

Then the C_4 resolvant of f is

$$\begin{aligned} C(x) &= x^2 + \frac{v_o^2 - 72}{9(v_o - 12)(v_o^2 + 12v_o + 144)}x \\ &\quad + \frac{v_o^6 + 3v_o^5 - 432v_o^3 - 3888v_o^2 + 15552v_o + 186624}{81(v_o - 12)^2(v_o^2 + 12v_o + 144)^3}. \end{aligned}$$

Suppose char $k = 2$. Then

$$C(x) = x^2 + \frac{1}{v_o}x + \frac{v_o + 1}{v_o^3}.$$

Making the substitution $x = x/v_o$ gives

$$C_1(x) = C(x/v_o) = x^2 + x + \frac{v_o + 1}{v_o}.$$

Suppose $C_1(x)$ has a linear factor over k, namely $x - t_o$. Then $t_o^2 + t_o + (v_o+1)/v_o = 0$ and v_o in terms of u_o is

$$v_o = \frac{1}{t_o^2 + t_o + 1}$$

as desired. Conversely, suppose $v_o = 1/(t_o^2 + t_o + 1)$ for some $t_o \in k$. Then

$$C_1(x) = (x + t_o)(x + t_o + 1).$$

Therefore, $C_1(x)$ (consequently $C(x)$) has a linear factor over k if and only if

$$v_o = \frac{1}{t_o^2 + t_o + 1}$$

for some $t_o \in k$, which completes the case when char $k = 2$.

Suppose char $k \neq 2$. Then the discriminant of $C(x)$ is

$$-\frac{v_o^6}{27(v_o - 12)^2(v_o^2 + 12v_o + 144)^3},$$

which has a square root in k if and only $-3(v_o^2 + 12v_o + 144)$ is a square in k. Hence, by Lemma 3.26, $\Phi(G) \subseteq J \cong C_4$ if and only if char $k = 2$ and

$$u_o = \frac{1}{(t_o^2 + t_o + 1)^3}$$

for some $t_o \in k$, or char $k \neq 2$ and there exists some $v_o \in k$ such that $u_o = v_o^3$ and $-3(v_o^2 + 12v_o + 144)$ has a square root in k.

(v) The subgroup $\Phi(G)$ is contained in a conjugate of $\langle(1\,2)\rangle \times \langle(3\,4)\rangle$ if and only if f has two quadratic factors over k. Part (vi) follows directly from Proposition 4.8.

(iv) The subgroup $\Phi(G)$ is contained in a conjugate of $Stab_{S_4}(4)$ if and only if f has a linear factor over k and part (iv) follows directly from Proposition 4.7.

(iii) Suppose $\Phi(G)$ is contained in a conjugate of $Stab_{S_4}(4)$. Then f has a cubic factor over k. From Proposition 4.7,

$$u_o = \frac{27t_o(t_o+8)^3}{(t_o-1)^3}$$

for some $t_o \in k$, and the cubic factor of f in terms of t_o is

$$\begin{aligned} Q(x) &= x^3 - \frac{7t_o+2}{t_o^2-20t_o-8}x^2 - \frac{t_o^3-33t_o^2+36t_o-4}{3(t_o^4-40t_o^3+384t_o^2+320t_o+64)}x \\ &\quad - \frac{t_o^5+4t_o^4+217t_o^3-442t_o^2+212t_o+8}{27(t_o^6-60t_o^5+1176t_o^4-7040t_o^3-9408t_o^2-3840t_o-512)}. \end{aligned}$$

Furthermore, if char $k \neq 2$, then the discriminant of $Q(x)$ is

$$-\frac{1}{3}\left(\frac{t_o(t_o-1)(t_o+8)^3}{3(t_o^2-20t_o-8)^3}\right)^2,$$

which has a square root in k if and only if -3 is a square in k. Similarly, if char $k = 2$, then the Berlekamp discriminant is a root of x^2+x+1. Hence, by Lemmas 3.16 and 3.18, $\Phi(G)$ is contained in a conjugate of $\langle(1\,2\,3)\rangle$ if and only if x^2+x+1 has a root in k.

(ii) The subgroup $\Phi(G)$ is contained in a conjugate of $\langle(1\,2)\rangle$ if and only if f has two linear factors over k. Part (ii) then follows directly from Proposition 4.9.

(i) From Theorem 3.20, $\Phi(G) = \{e\}$ if and only if $\Phi(G)$ is contained in a conjugate of $\langle(1\,2)\rangle$ and A_4. The result then follows from Parts (ii) and (ix).

(x) The nontrivial subgroups of S_4 are the transitive subgroups listed in Lemma 3.22 and conjugates of $Stab_{S_4}(4)$, $\langle(1\,2\,3)\rangle$, $\langle(1\,2)\rangle$, and $\langle(1\,2)\rangle \times \langle(3\,4)\rangle$. Since $\Phi(G)$ is a subgroup of S_4, if cases $(i) - (ix)$ do not occur then $\Phi(G) = S_4$.

4.3 Example

Consider the elliptic curve given by $E : x^3 + y^3 + z^3 = 3\lambda xyz$ over a field k where $\lambda \in k$. Let H be the Hessian of E then

$$H = \begin{bmatrix} 6x & -3\lambda z & -3\lambda y \\ -3\lambda z & 6y & -3\lambda x \\ -3\lambda y & -3\lambda x & 6z \end{bmatrix}$$

with determinant $|H| = 216xyz - 54\lambda^2x^3 - 54\lambda^2z^3 - 54\lambda^3xyz - 54\lambda^2y^3$. Taking the intersection of E and $|H|$ gives the following rational points

$$[0, -1, 1], [-1, 0, 1], [-1, 1, 0],$$

which are the flex points of E. The following transformations are made to put E in canonical normal form. Note that in each step the transformation is given followed by the resulting equation representing the elliptic curve E.

1. Move the flex point $[-1, 1, 0]$ to $[0, 1, 0]$.

$$x = x' + y',\ y = x' - y',\ z = z'$$

$$E : 2x^3 + 6xy^2 + z^3 - 3\lambda x^2z + 3\lambda y^2z = 0$$

2. Interchange x and z.

$$x = \frac{z'}{6},\ y = y',\ z = -x'$$

$$E : (z - 3\lambda x)y^2 = x^3 - \frac{1}{12}\lambda xz^2 - \frac{1}{108}z^3$$

3. Consider z as the coefficient term of y^2.

$$x = x',\ y = y',\ z = z' - 3\lambda x$$

$$E : y^2z = (1 - \lambda^3)x^3 - \frac{3\lambda^2}{4}x^2z - \frac{\lambda}{6}xz^2 - \frac{1}{108}z^3$$

4. Make a transformation so that E is monic in x.

$$x = \frac{x'}{(1 - \lambda^3)^{1/3}},\ y = y',\ z = z'$$

$$E : y^2z = x^3 - \frac{3\lambda^2}{4(1 - \lambda^3)^{2/3}}x^2z - \frac{\lambda}{6(1 - \lambda^3)^{1/3}}xz^2 - \frac{1}{108}z^3$$

5. Set $z = 1$.

$$E : y^2 = x^3 - \frac{3\lambda^2}{4(1-\lambda^3)^{2/3}}x^2 - \frac{\lambda}{6(1-\lambda^3)^{1/3}}x - \frac{1}{108}$$

Now that E is in the canonical normal form, the j-invariant can be computed. Let ϕ be the j-invariant of E. Then

$$\phi = \frac{27\lambda^3(\lambda+2)^3(\lambda^2-2\lambda+4)^3}{(\lambda-1)^3(\lambda^2+\lambda+1)^3}.$$

Since $\lambda \in k$, by Theorem 4.6, if x^2+x+1 has a root in k then $G'_{E,3}$ trivial. otherwise $G'_{E,3} \cong C_2$.

Chapter 5

Drinfeld Modules

In this chapter, we calculate the Galois groups of fields generated by torsion points on a Drinfeld module. We refer the reader to Section 3.2 for background information on torsion points on Drinfeld modules relevant to this section. Let $A = \mathbb{F}_q[T]$ and let ρ be a rank 2 Drinfeld A-module over k with j-invariant u_o. For $a \in A$, we wish to determine necessary and sufficient algebraic conditions on u_o that determine the containment of $G'_{\rho,a}$ in subgroups of $GL_r(A/a)/\mu_{q-1}$.

In what follows, we categorize $G'_{\rho,a}$ for the cases when ρ has rank 1 and a is a linear or quadratic polynomial in A and when ρ has rank 2 and a is a linear polynomial in A. We also categorize $G_{\rho,a}$ when ρ is a rank 1 Drinfeld module and a is linear in T. The values for r, q and a are summarized in Table 5.1. In several instances, we parametrize curves of genus zero with a rational point in k to get algebraic conditions on u_o. These parametrizations are guaranteed to exist by Theorem 2.9.

5.1 Rank 1 Drinfeld modules

5.1.1 Galois group of $(T + \alpha)$-torsion submodule

It has been shown that for $k = \mathbb{F}_q(T)$ there are only finitely many rank one Drinfeld modules (up to isomorphism over k) that have nonzero torsion in k. In particular,

Table 5.1: Drinfeld modules that give rise to polynomials of degree at most four

Rank of the Drinfeld module	q	$a \in A = \mathbb{F}_q[T]$ $\alpha_1, \alpha_2 \in \mathbb{F}_q$	$f(x)$	$deg\ f$
1	q	$T + \alpha_1$	ψ_a	$q-1$
1	q	$T + \alpha_1$	ψ'_a	1
1	2	$T^2 + \alpha_1 T + \alpha_2$	$\psi'_a = \psi_a$	3
1	3	$T^2 + \alpha_1 T + \alpha_2$	ψ'_a	4
2	2	$T + \alpha_1$	$\psi'_a = \psi_a$	3
2	3	$T + \alpha_1$	ψ'_a	4

if $q = 2$ then ρ is isomorphic to the Carlitz module over k and $\{\lambda \in k | \rho_a(\lambda) = 0$ for some nonzero $a \in A\} \cong \mathbb{F}_q[T]/(T^2 + T)$ as an $\mathbb{F}_q[T]$-module. Suppose $q > 2$. If ρ is isomorphic over k to $\psi_T = T - (T + c)\tau$ for some $c \in \mathbb{F}_q$ then the torsion submodule

$$\{\lambda \in k | \rho_a(\lambda) = 0 \text{ for some nonzero } a \in A\}$$

equals $\mathbb{F}_q$ and is isomorphic to $\mathbb{F}_q[T]/(T+c)$ as an $\mathbb{F}_q[T]$-module. If ρ is not isomorphic to such a Drinfeld module, then the torsion submodule

$$\{\lambda \in k | \rho_a(\lambda) = 0 \text{ for some nonzero } a \in A\}$$

equals $\{0\}$ ([Poo97], p.582). For the purpose of this thesis, we take k to be an extension of $\mathbb{F}_q(T)$ and we study torsion submodules of $\bar{k}_\rho$ rather than in k_ρ.

Theorem 5.1 *Let ρ be a Drinfeld A-module of rank 1 over a field extension k of $\mathbb{F}_q(T)$ given by $\rho_T = T + u_o\tau$, where $u_o \in k \setminus \{0\}$. If $a = T + \alpha \in A$ and $v_o = 1/u_o$ then $G_{\rho,a}$ is contained in a cyclic group of order d dividing $q-1$ if and only if*

$$v_o = -\frac{z_o^{(q-1)/d}}{T + \alpha}$$

for some $z_o \in k$.

Corollary 5.2 *If* $u_o = 1$ *and* $k = \mathbb{F}_q(T)$ *then* $G_{\rho,a}$ *is isomorphic to* $(\mathbb{F}_q)^*$.[1]

Remark 5.3 *First we note that a Drinfeld* A*-module* $\rho_T = T + u_o\tau$ *is isomorphic to* $\psi_T = T - (T + c)\tau$ *over* k *if and only if*

$$v_o = -\frac{z_o^{q-1}}{(T + c)},$$

where $c \in \mathbb{F}_q$ *and* $z_o \in k$. *From Theorem 5.1,* $G_{\rho,a}$ *is trivial, where* $a = T$. *This implies that the set of torsion points of* ρ_a *is contained in* k. *From Poonen's result, we also have that* $\Lambda_\rho[a] \subseteq \mathbb{F}_q$.

Proof of Theorem 5.1

Let $u_o \in k$ and let ρ be a Drinfeld A-module of rank 1 over a field extension k of $\mathbb{F}_q(T)$ given by

$$\rho_T = u_o\tau + T.$$

Let $a = T + \alpha \in A$, $v_o = 1/u_o$, and let $f(x) \in k[x]$ be the a-division polynomial of ρ. Then f is given by

$$f(x) = x^{q-1} + (T + \alpha_1)v_o$$

and $G_{\rho,a}$ is equal to the Galois group of f over k.

The ideas presented in this proof are taken from *([Lan02], p.289).* Let $\beta \in \bar{k}$ be a root of f. Since k contains all of the $q - 1$ roots of unity, f splits over $k(\beta)$. Furthermore, all the roots of f are distinct. Let G be the Galois group of $k(\beta)$ over k.

If $\sigma \in G$ then $\sigma(\beta) = \omega_\sigma\beta$, where ω_σ is a $q - 1$ root of unity. The map $\sigma \mapsto \omega_\sigma$ is clearly a homomorphism of G into the group of $q - 1$ roots of unity. Since a subgroup of a cyclic group is cyclic, G is cyclic.

Suppose that

$$v_o = -\frac{z_o^{(q-1)/d}}{T + \alpha_1}$$

[1] *This result corresponds with Proposition 12.7 in [Ros02] with* $P = T + \alpha_1$ *and* $e = 1$.

for some $d|(q-1)$ and $z_o \in k$. Then

$$(-(T+\alpha_1)v_o)^d = z_o^{q-1}.$$

But we also have that

$$-(T+\alpha_1)v_o = \beta^{q-1},$$

so that

$$(\beta^d)^{q-1} = z_o^{q-1},$$

and $\beta^d \in k$. Let σ be a generator of G. Since β^d is fixed under G,

$$\sigma(\beta^d) = (\sigma\beta)^d = (\omega_\sigma\beta)^d = \beta^d$$

and ω_σ is a primitive d root of unity. Therefore, G is contained in a cyclic group of order d dividing $q-1$.

Conversely, suppose that G is contained in a cyclic group of order d dividing $q-1$. If σ is a generator for G, then ω_σ is a primitive d root of unity and we get

$$\sigma(\beta^d) = (\sigma\beta)^d = (\omega_\sigma\beta)^d = \beta^d.$$

Hence, β^d is fixed under G and $\beta^d \in k$. Furthermore, we have

$$v_o = -\frac{(\beta^d)^{(q-1)/d}}{T+\alpha_1},$$

and the theorem is proved.

Proof of Corollary 5.2

If $u = 1$, then $v_o = 1$ and there exists a $z_o \in k$, namely $-(T+\alpha_1)$, such that

$$v_o = -\frac{z_o}{T+\alpha_1}.$$

By Theorem 5.1, G is contained in a cyclic group of order $q-1$. Suppose there exists a $d < q-1$ such that d divides $q-1$ and

$$v_o = -\frac{z_o^{(q-1)/d}}{T+\alpha_1}$$

for some $z_o \in k$. Then the degree in T of the denominator is strictly smaller than the degree in T of the numerator, yielding a contradiction. Therefore G is a cyclic group of order $q-1$, hence $G \cong (\mathbb{F}_q)^*$.

5.1.2 Galois group of $(T^2 + \alpha_1 T + \alpha_2)$-torsion submodule

Theorem 5.4 *Let ρ be a rank 1 Drinfeld A-module over a field extension k of $\mathbb{F}_2(T)$.*

(a) If $a = T^2 + T$ then $G_{\rho,a}$ is trivial;

(b) If $a = T^2 + \alpha$, then $G_{\rho,a}$ is trivial if and only if

$$x^2 + x + \frac{1}{T + \alpha}$$

has a root in k, otherwise $G_{\rho,a} \cong \langle (1\ 2) \rangle$;

(c) If $a = T^2 + T + 1$, then $G_{\rho,a}$ is trivial if and only if

$$x^3 + (T^2 + T + 1)x + (T^2 + T + 1)$$

has a root in k, otherwise $G_{\rho,a} \cong A_3$.

Theorem 5.5 *Let ρ be a Drinfeld A-module of rank 1 over a field extension k of $\mathbb{F}_3(T)$ and let $a = T^2 + \alpha_1 T + \alpha_2 \in A$.*

(i) If $(\alpha_1, \alpha_2) \in \{(1,0), (-1,0), (0,-1)\}$, then $G'_{\rho,a}$ is trivial if and only if $(T - (\alpha_1 + 1))(T - \alpha_1 + 1)$ is a square in k, otherwise $G'_{\rho,a} \cong C_2$.

(ii) If $(\alpha_1, \alpha_2) \in \{(0,0), (1,1), (-1,1)\}$, then $G'_{\rho,a}$ is trivial if and only if

$$x^3 - (T + \alpha_1)x^2 + (T + \alpha_1)^2 x + (T + \alpha_1)$$

has a root in k, otherwise $G'_{\rho,a} \cong A_3$.

(iii) If $(\alpha_1, \alpha_2) \in \{(0,1), (-1,-1), (1,-1)\}$, then $G'_{\rho,a}$ is trivial if and only if

$$x^4 + (T^3 + T + \alpha_1)x + (T^2 + \alpha_1 T + \alpha_2)$$

has a root in k, otherwise $G'_{\rho,a} \cong C_4$.

Proof of Theorem 5.4

Let ρ be a Drinfeld A-module of rank 1 over a field extension k of $\mathbb{F}_2(T)$. From Lemma 3.12, $G'_{\rho,a}$ is invariant under isomorphisms over $\bar{k}$. Therefore, it suffices to only consider the rank 1 Drinfeld A-module given by

$$\rho_T = \tau + T.$$

Let $a = T^2 + \alpha_1 T + \alpha_2 \in A$ and let $f(x) \in k[x]$ be the a-division polynomial of ρ. Then f is given by

$$f(x) = x^3 + (T^2 + T + \alpha_2)x + (T^2 + \alpha_1 T + \alpha_2),$$

where f has distinct roots in $\bar{k}$. To see this, suppose f has a double root for a contradiction. If f has a double root then $f(x) = (x+a)^2(x+b)$, for some $a, b \in \bar{k}$. This implies that $f(x) = x^3 + bx^2 + a^2x + a^2b$, yielding $b = 0$. But clearly, 0 is not a root of $f(x)$, giving a contradiction. Let G be the Galois group of f over k, and Φ be a choice of monomorphism $G \hookrightarrow S_3$ after labeling the roots of f. Then $G'_{\rho,a} \cong G_{\rho,a} \cong \Phi(G)$.

(a) If $\alpha_1 = 1$ and $\alpha_2 = 0$ then f factors as $(x+1)(x+T)(x+(T+1))$ and $\Phi(G) = \{e\}$.

(b) If $\alpha_1 = 0$ then f factors as $(x + (T + \alpha_2))(x^2 + (T + \alpha_2)x + (T + \alpha_2))$. The Berlekamp discriminant of the quadratic factor of f is a root of

$$x^2 + x + \frac{1}{T + \alpha_2}. \tag{5.1}$$

By Lemma 3.18, f has three linear factors (equivalently, $\Phi(G) = \{e\}$) if and only if (5.1) has a root in k. Otherwise, $\Phi(G)$ is a conjugate of $\langle(1\,2)\rangle$.

(c) If $\alpha_1 = \alpha_2 = 1$, then the Berlekamp discriminant of f is in k if and only if

$$b(x) = x^2 + x + T^2 + T$$

has a root in k. Since $b(T) = 0$, $\Phi(G) \subseteq A_3$. If $a \in k$ is a root of f then

$$f(x) = (x + a)(x + a(a + T))(x + a(a + (T + 1))).$$

Therefore, $\Phi(G) = \{e\}$ if and only if f has a root in k, otherwise $\Phi(G) = A_3$.

Proof of Theorem 5.5

Let ρ be a Drinfeld A-module of rank 1 over a field extension k of $\mathbb{F}_3(T)$. From Lemma 3.12, $G'_{\rho,a}$ is invariant under isomorphisms over $\bar{k}$. Therefore, it suffices to only consider the rank 1 Drinfeld A-module given by

$$\rho_T = \tau + T.$$

Let $a = T^2 + \alpha_1 T + \alpha_2 \in A$ and let $f(x) \in k[x]$ be the a-division polynomial of the x-coordinates of ρ. Then f is given by

$$f(x) = x^4 + (T^3 + T + \alpha_1)x + (T^2 + \alpha_1 T + \alpha_2).$$

The discriminant of f is $(T^2 + \alpha_1 T + \alpha_2)^3 \neq 0$, therefore f has distinct roots in $\bar{k}$. Let G be the Galois group of f over k, and Φ be a choice of monomorphism $G \hookrightarrow S_4$ after labeling the roots of f. Then $G'_{\rho,a} \cong \Phi(G)$.

(i) Suppose $(\alpha_1, \alpha_2) \in \{(1,0), (-1,0), (0,-1)\}$. Then f factors as

$$f(x) = (x + (T + \alpha_2))(x + (T + \alpha_1 + \alpha_2))(x^2 + (T + 2\alpha_1)x + 1),$$

and $\Phi(G)$ is contained in a conjugate of $\langle (12) \rangle$. The discriminant of the quadratic factor is

$$(T - (\alpha_1 + 1))(T - \alpha_1 + 1),$$

which is a square in k if and only if $(T - (\alpha_1 + 1))(T - \alpha_1 + 1)$ is a square in k. The result then follows.

(ii) Suppose $(\alpha_1, \alpha_2) \in \{(0,0), (1,1), (2,1)\}$. Then f factors as

$$(x + (T + \alpha_1))(x^3 - (T + \alpha_1)x^2 + (T + \alpha_1)^2 x + T + \alpha_1),$$

and $\Phi(G)$ is contained in a conjugate of $Stab_{S_4}(4)$. Furthermore, $\Phi(G)$ is contained in a conjugate of $\langle (1\ 2\ 3) \rangle$ since the discriminant of the cubic factor, namely

$$(T + \alpha_1)^4,$$

is a square in k. Furthermore, f has two linear factors over k when

$$x^3 - (T + \alpha_1)x^2 + (T + \alpha_1)^2 x + (T + \alpha_1)$$

has a root in k. The result then follows from Theorem 3.20.

(iii) Suppose $(\alpha_1, \alpha_2) \in \{(0,1),(2,2),(1,2)\}$. The D_4 resolvant of $f(x)$ given by

$$R(x) = x^3 - (T^2 + \alpha_1 T + \alpha_2)x - (T^3 + T + \alpha_1)^2,$$

which factors over k as

$$(x - (T^2 + \alpha_1 T + \alpha_2))(x^2 + (T^2 + \alpha_1 T + \alpha_2)x + (T - \alpha_1)(T^2 + \alpha_1 T + \alpha_2)).$$

Hence, $\Phi(G) \subseteq H \cong D_4$. The C_4 resolvant of $f(x)$ is given by

$$C(x) = x^2 + (T^3 + T + \alpha_1)x + (T + \alpha_1\alpha_2 - 1)(T + \alpha_1\alpha_2 + 1)(T^2 + \alpha_1 T + \alpha_2)^2$$

and has a linear factor over k since its discriminant,

$$(T^2 + \alpha_1 T + \alpha_2)^2,$$

is a square in k. Therefore, $\Phi(G) \subseteq J \cong C_4$. Using Magma [BCP97], if f has one linear factor over k, then f has four linear factors. Therefore, if $\Phi(G) = \{e\}$ if and only if f has a linear factor over k, otherwise $\Phi(G) \cong C_4$.

5.2 Rank 2 Drinfeld modules

5.2.1 Galois group of $(T + \alpha)$-torsion submodule

Theorem 5.6 *Let ρ be a Drinfeld A-module of rank 2 over a field extension k of $\mathbb{F}_2(T)$ with j-invariant $u_o \in k \setminus \{0\}$. If $a = T + \alpha \in A$ and $v_o = 1/u_o$, then*

(i) $G_{\rho,a}$ is trivial if and only if

$$v_o = \frac{z_o^2(z_o + 1)^2}{(T + \alpha)^2(z_o^2 + z_o + 1)^3}$$

for some $z_o \in k$;

(ii) $G_{\rho,a}$ is isomorphic to a subgroup of C_2 if and only if

$$v_o = z_o^2(z_o(T + \alpha) + 1)$$

for some $z_o \in k$;

(iii) $G_{\rho,a}$ *is isomorphic to a subgroup of* A_3 *if and only if*

$$v_o = \frac{z_o^2}{(T+\alpha)^2(z_o^2+z_o+1)}$$

for some $z_o \in k$;

(iv) otherwise, $G_{\rho,a} \cong S_3$.

Theorem 5.7 *Let* ρ *be a Drinfeld* A*-module of rank 2 over a field extension* k *of* $\mathbb{F}_3(T)$ *with* j*-invariant* $u_o \in k \setminus \{0\}$. *If* $a = T + \alpha \in A$ *and* $v_o = 1/u_o$, *then*

(i) $G'_{\rho,a}$ *is trivial if and only if* $2x^6 + (T+\alpha)v_o^3x^2 + v_o^4$ *has a root in* k *and*

$$v_o = (T+\alpha)z_o^2$$

for some $z_o \in k$;

(ii) $G'_{\rho,a}$ *is isomorphic to a subgroup of* C_2 *if and only if* $v_o = 2z_o^3(z_o(T+\alpha)+1)$ *for some* $z_o \in k$ *and*

$$2x^6 + (T+\alpha)v_o^3x^2 + v_o^4$$

has a root in k;

(iii) $G'_{\rho,a}$ *is isomorphic to a subgroup of* A_3 *if and only if*

$$v_o = \frac{z_o^2(T+\alpha)}{(2z_o^2(T+\alpha)^2+2)^4}$$

for some $z_o \in k$;

(iv) $G'_{\rho,a}$ *is isomorphic to a subgroup of* S_3 *if and only if* $v_o = 2z_o^3(z_o(T+\alpha)+1)$ *for some* $z_o \in k$,

(v) $G'_{\rho,a}$ *is isomorphic to a subgroup of* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *if and only if*

$$v_o = \frac{(1-z_o^2)^3}{z_o^4(T+\alpha)^3}$$

for some $z_o \in k$;

(vi) $G'_{\rho,a}$ *is isomorphic to a subgroup of* V_4 *if and only if*

$$v_o = \frac{(T+\alpha)^3}{z_o^2(z_o^2+(T+\alpha)^2)^2}$$

for some $z_o \in k$;

(vii) $G'_{\rho,a}$ *is isomorphic to a subgroup of* C_4 *if and only if*

$$v_o = \frac{1}{z_o^4(z_o^2+1)(T+\alpha)^3}$$

for some $z_o \in k$;

(viii) $G'_{\rho,a}$ *is isomorphic to a subgroup of* D_4 *if and only if*

$$v_o = \frac{1}{z_o^2(T+\alpha+z_o)}$$

for some $z_o \in k$;

(ix) $G'_{\rho,a}$ *is isomorphic to a subgroup of* A_4 *if and only if* $v_o = (T+\alpha)z_o^2$ *for some* $z_o \in k$;

(x) otherwise, $G'_{\rho,a} \cong S_4$.

Proof of Theorem 5.6

Let ρ be a Drinfeld A-module of rank 2 over a field extension k of $\mathbb{F}_2(T)$ with j-invariant $u_o \in k$ given by

$$\rho_T = u_o^q \tau^2 + u_o \tau + T.$$

Let $a = T + \alpha \in A$, $v_o = 1/u_o$, and let $f(x) \in k[x]$ be the a-division polynomial of ρ. Then f is given by

$$f(x) = x^3 + v_o x + (T+\alpha_1)v_o^2,$$

where f has distinct roots in $\bar{k}$. To see this, suppose f has a double root for a contradiction. If f has a double root then $f(x) = (x+a)^2(x+b)$, for some $a, b \in \bar{k}$. This implies that $f(x) = x^3 + bx^2 + a^2x + a^2b$, yielding $b = 0$. But clearly, 0 is not a root of $f(x)$, giving a contradiction. Let G be the Galois group of f over k, and Φ be a choice of monomorphism $G \hookrightarrow S_3$ after labeling the roots of f. Then $G_{\rho\, a} \cong \Phi(G)$.

(ii) By parametrizing the cubic $D(x,y) = x^3 + yx + y^2(T+\alpha_1)$ with the line $y = zx$ we have

$$x = z(z(T+\alpha_1)+1), \qquad \text{and} \qquad y = z^2(z(T+\alpha_1)+1).$$

Then f has a linear factor over k if and only if there exists a $z_o \in k$ such that $D(x_o, v_o) = 0$. Therefore, f has a linear factor over k and $\Phi(G)$ is contained in a conjugate of $\langle(1\ 2)\rangle$ if and only if

$$v_o = z_o^2(z_o(T+\alpha_1)+1)$$

for some $z_o \in k$. Furthermore, writing v_o in terms of z_o in $f(x)$ and factoring gives

$$f(x) = (x+z_o(z_o(T+\alpha_1)+1))(x^2+z_o(z_o(T+\alpha_1)+1)x+z_o^3(T+\alpha_1)(z_o(T+\alpha_1)+1)).$$

(i) Using the results from the previous case, $\Phi(G) = \{e\}$ if and only if $v_o = m_o^2(m_o(T+\alpha_1)+1)$ for some $m_o \in k$ and the quadratic

$$x^2 + m_o(m_o(T+\alpha_1)+1)x + m_o^3(T+\alpha_1)(m_o(T+\alpha_1)+1) \tag{5.2}$$

has a linear factor over k. Using the Berlekamp discriminant, (5.2) has a linear factor over k if and only if

$$b(x) = x^2 + x + \frac{m_o(T+\alpha_1)}{m_o(T+\alpha_1)+1}, \tag{5.3}$$

has a root in k. Let $m_1 = m_o(T+\alpha_1)+1 \in k$ be nonzero. Then $b(x)$ has a root in k if and only if

$$b_1(x) = x^2 + x + \frac{m_1+1}{m_1}$$

has a root in k. Suppose $b_1(z_o) = 0$ for some $z_o \in k$. Then writing m_1 in terms of z_o gives

$$m_1 = \frac{1}{z_o^2 + z_o + 1}.$$

Conversely, suppose $m_1 = 1/(z_o^2 + z_o + 1)$ for some $z_o \in k$. Then $b_1(x) = (x+z_o)(x+z_o+1)$. Therefore, $b_1(x)$ (hence $b(x)$) has a root in k if and only if $m_1 = 1/(z_o^2 + z_o + 1)$ for some $z_o \in k$.

The result then follows upon writing m_o in terms of z_o, namely

$$m_o = \frac{z_o(z_o+1)}{(T+\alpha_1)(z_o^2+z_o+1)},$$

and writing v_o in terms of z_o, yielding

$$v_o = \frac{z_o^2(z_o+1)^2}{(T+\alpha_1)^2(z_o^2+z_o+1)^3}.$$

(iii) From Lemma 3.18, $\Phi(G) \subseteq A_3$ if and only if

$$b(x) = x^2 + x + \frac{1+(T+\alpha_1)^2 v_o}{(T+\alpha_1)^2 v_o} \tag{5.4}$$

has a root in k. However, substituting $m_1 = (T+\alpha_1)^2 v_o$ in $b(x)$ yields

$$b_1(x) = x^2 + x + \frac{m_1+1}{m_1}.$$

Using the same method as given in case (i) above, $b(x)$ has a root in k if and only if

$$v_o = \frac{z_o^2}{(T+\alpha_1)^2(z_o^2+z_o+1)}$$

for some $z_o \in k$.

(iv) The nontrivial subgroups of S_3 are A_3 and conjugates of $\langle(1\,2)\rangle$. Since $\Phi(G)$ is a subgroup of S_3, if cases (i) to (iii) do not occur, $\Phi(G) = S_3$.

Proof of Theorem 5.7

Let ρ be a Drinfeld A-module of rank 2 over a field extension k of $\mathbb{F}_3(T)$ with j-invariant $u_o \in k$ given by

$$\rho_T = u_o^q \tau^2 + u_o \tau + T.$$

Let $a = T + \alpha \in A$, $v_o = 1/u_o$, and let $f(x) \in k[x]$ be the a-division polynomial of the x-coordinates of ρ. Then f is given by

$$f(x) = x^4 + v_o^2 x + (T+\alpha_1)v_o^3.$$

The discriminant of f is $v_o^9(T+\alpha_1)^3 \neq 0$, therefore f has distinct roots in $\bar{k}$. Let G be the Galois group of f over k, and Φ be a choice of monomorphism $G \hookrightarrow S_4$ after labeling the roots of f. Then $G'_{\rho,a} \cong \Phi(G)$.

Proposition 5.8 *Let k be a field extension of $\mathbb{F}_3(T)$ and $v_o \in k$. Let $a \in A$ and f be as given in Theorem 5.7. Then f has a linear factor over k if and only if*

$$v_o = 2z_o^3(Tz_o + \alpha_1 z_o + 1)$$

for some $z_o \in k$.

Proof: If

$$v_o = 2z_o^3(Tz_o + \alpha_1 z_o + 1)$$

for some $z_o \in k$, then f factors as

$$(x + z_o^2(z_o(T + \alpha_1) + 1))$$

$$(x^3 + 2z_o^2(z_o(T + \alpha_1) + 1)x^2 + z_o^4(z_o(T + \alpha_1) + 1)^2 x + 2z_o^7(T + \alpha_1)(z_o(T + \alpha_1) + 1)^2).$$

Conversely, suppose $f(x_o) = 0$ for some $x_o \in k$. By parametrizing the quartic $x^4 + v^2x + (T + \alpha_1)v^3$ with the line $v = zx$, we have

$$x = 2z^2((T + \alpha_1)z + 1), \qquad \text{and} \qquad v = 2z^3((T + \alpha_1)z + 1).$$

Since $f(x_o) = 0$,

$$\begin{aligned} x_o &= 2z_o^2((T + \alpha_1)z_o + 1) \qquad \text{and} \\ v_o &= 2z_o^3((T + \alpha_1)z_o + 1) \end{aligned}$$

for some $z_o \in k$, which completes the proof.

■

Proposition 5.9 *Let k be a field extension of $\mathbb{F}_3(T)$ and $v_o \in k$. Let $a \in A$ and f be as given in Theorem 5.7. Then f has a quadratic factor over k if and only if*

$$v_o = \frac{(1 - z_o^2)^3}{z_o^4(T + \alpha_1)^3}$$

for some $z_o \in k$.

Proof: The polynomial $f(x)$ has a quadratic factor over k if and only if

$$f(x) = (x^2 + mx + b)(x^2 + cx + d)$$

for some $m, b, c, d \in k$. Solving for the coefficients of f gives $c = -m$ and

$$\begin{aligned} b + 2m^2 + d &= 0, & (5.5)\\ m(2b + d) &= v_o^2, & (5.6)\\ bd &= (T + \alpha_1)v_o^3. & (5.7) \end{aligned}$$

Obviously, $m \neq 0$. Then using equations (5.5) and (5.6) in succession to solve for b and d, and writing equation (5.7) in terms of m yields

$$2m^6 + (T + \alpha_1)v_o^3 m^2 + v_o^4 = 0. \quad (5.8)$$

Dividing both sides by m^6 and making the substitutions $w = v_o/m$ and $y = v_o^2/m^3$ gives

$$2 + (T + \alpha_1)wy + y^2 = 0.$$

By parametrizing the above curve with the line $y = z_o$, we have

$$w = \frac{1 - z_o^2}{(T + \alpha_1)z_o}.$$

Then substituting $m^3 = v_o^2/z_o$ into $w^3 = v_o^3/m^3$ gives $v_o = w/z_o$. Therefore, equation (5.8) has a root in k if and only if

$$v_o = \frac{(1 - z_o^2)^3}{z_o^4(T + \alpha_1)^3}$$

for some $z_o \in k$ and the result then follows.

■

Let us now return to the proof of Theorem 5.7.

(ix) The discrimimant of f is

$$v_o^9(T + a_1)^3,$$

which is a square in k if and only if $v_o = (T + a_1)z_o^2$ for some $z_o \in k$. The result then follows from Lemma 3.16.

(viii) The D_4 resolvant of f is $R(x) = x^3 + 2(T+\alpha_1)v_o^3 x + 2v_o^4$. If

$$v_o = \frac{1}{z_o^2(T+\alpha_1+z_o)}$$

for some $z_o \in k$, then R factors as

$$\left(x + \frac{2}{z_o^3(T+\alpha_1+z_o)}\right)\left(x^2 + \frac{1}{z_o^3(T+\alpha_1+z_o)}x + \frac{1}{z_o^5(T+\alpha_1+z_o)^3}\right).$$

Conversely, suppose $R(x_o) = 0$ for some $x_o \in k$. By parametrizing the curve $x^3 + 2(T+\alpha_1)v^3x + 2v^4$ with the line $v = zx$, we have

$$x = \frac{1}{z^3(T+\alpha_1+z)}, \qquad \text{and} \qquad v = \frac{1}{z^2(T+\alpha_1+z)}.$$

Since $R(x_o) = 0$,

$$x_o = \frac{1}{z_o^3(T+\alpha_1+z_o)} \qquad \text{and} \qquad v_o = \frac{1}{z_o^2(T+\alpha_1+z_o)}$$

for some $z_o \in k$. Part $(viii)$ then follows form Lemma 3.24.

(vii) Suppose $\Phi(G) \subseteq V \cong V_4$, then $\Phi(G) \subseteq A_4$ and $\Phi(G) \subseteq H \cong D_4$. By parts $(viii)$ and (ix)

$$v_o = \frac{1}{m_o^2(T+\alpha_1+m_o)} \qquad \text{and} \qquad v_o = (T+\alpha_1)n_o^2$$

for some $m_o, n_o \in k$, yielding

$$m_o^2 n_o^2 (T+\alpha_1+m_o)(T+\alpha_1) + 2 = 0. \tag{5.9}$$

Clearly, it must be the case that $(T+\alpha_1+m_o)(T+\alpha_1) = z_o^2$ for some $z_o \in k$. Solving for m_o in terms of z_o gives

$$m_0 = \frac{z_o^2 + 2(T+\alpha_1)}{T+\alpha_1}. \tag{5.10}$$

Substituting (5.10) in (5.9) and solving for n_o in terms of z_o gives

$$n_o = \frac{2(T+\alpha_1)}{z_o(z_o^2 + 2(T+\alpha_1)^2)},$$

and we have

$$v_o = \frac{(T+\alpha_1)^3}{z_o^2(z_o^2+2(T+\alpha_1)^2)^2}$$

as desired. Conversely, if

$$v_o = \frac{(T+\alpha_1)^3}{z_o^2(z_o^2+2(T+\alpha_1)^2)^2}$$

for some $z_o \in k$, then with

$$m_o = \frac{z_o^2+2(T+\alpha_1)^2}{T+\alpha_1} \qquad \text{and} \qquad n_o = \frac{2(T+\alpha_1)}{z_o(z_o^2+2(T+a)^2)},$$

$\Phi(G) \subseteq A_4$ and $\Phi(G) \subseteq H \cong D_4$. Hence, $\Phi(G) \subseteq V \cong V_4$.

(vi) Suppose that $\Phi(G) \subseteq H \cong D_4$. Then

$$v_o = \frac{1}{m_o^2(T+\alpha_1+m_o)}$$

for some $m_o \in k$. The C_4 resolvant of f is

$$C(x) = x^2 + \frac{1}{m_o^4(T+a+m_o)^2}x + 2\frac{T+a}{m_o^9(T+a+m_o)^4} + \frac{1}{m_o^8(T+a+m_o)^4}$$

with discriminant

$$\frac{T+\alpha_1}{m_o^9(T+\alpha_1+m_o)^4},$$

which is a square in k if and only if $m_o = (T+\alpha_1)z_o^2$ for some $z_o \in k$. Furthermore, v_o written in terms of z_o is

$$v_o = \frac{1}{z_o^4(z_o^2+1)(T+\alpha_1)^3}.$$

The result then follows from Lemma 3.26.

(v) The subgroup $\Phi(G)$ is contained in a conjugate of $\langle(1\,2)\rangle \times \langle(3\,4)\rangle$ if and only if f has a quadratic factor. Part (v) then follows directly from Proposition 5.9.

(iv) The subgroup $\Phi(G)$ is contained in a conjugate of $Stab_{S_4}(4)$ if and only if f has a linear factor. Part (iv) then follows directly from Proposition 5.8.

(iii) Suppose that $\Phi(G)$ is contained in a conjugate of $Stab_{S_4}(4)$. Then

$$v_o = 2m_o^3(Tm_o + \alpha_1 m_o + 1)$$

for some $m_o \in k$, and f has a cubic factor with discriminant

$$2m_o^{13}(T + \alpha_1)(m_o(T + \alpha_1) + 1)^5,$$

which is a square in k if and only if $2m_o(T + \alpha_1)(m_o(T + \alpha_1) + 1)$ is a square in k. By parametrizing the curve $2m(T + \alpha_1)(m(T + \alpha_1) + 1) + 2n^2$ with the line $m = zn$, we get

$$m = \frac{z^2(T + \alpha_1)}{2z^2(T + \alpha_1)^2 + 2}$$

and $2m_o(T + \alpha_1)(m_o(T + \alpha_1) + 1)$ is a square in k if and only if

$$v_o = \frac{z_o^2(T + \alpha_1)}{(2z_o^2(T + \alpha_1)^2 + 2)^4}$$

for some $z_o \in k$. The result then follows from Lemma 3.16.

(ii) The result follows from parts (iv) and (v), since $\Phi(G)$ is contained in a conjugate of $\langle(1\ 2)\rangle$ if and only if $\Phi(G)$ is contained in a conjugate of $Stab_{S_4}(4)$ and $\langle(1\ 2)\rangle \times \langle(3\ 4)\rangle$.

(i) The result follows from parts (ii) and (ix), since the only subgroup of C_2 and A_4 is the identity.

(x) The nontrivial subgroups of S_4 are the transitive subgroups listed in Lemma 3.22 and conjugates of $Stab_{S_4}(4)$, conjugates of $\langle(1\ 2\ 3)\rangle$, conjugates of $\langle(1\ 2)\rangle$, and conjugates of $\langle(1\ 2)\rangle \times \langle(3\ 4)\rangle$. Since $\Phi(G)$ is a subgroup of S_4, if cases $(i) - (ix)$ do not occur, then $\Phi(G) = S_4$.

Appendix A

Elliptic curves with j-invariant equal to 0 or 1728

In this appendix, we investigate the Galois groups of fields generated by the x-coordinates of torsion points of order 2 and 3 on an elliptic curve with j-invariant $u_o = 0, 1728$. We refer the reader to Sections 2.2 and 3.1 for background information on elliptic curves relevant to this section. Recall from Lemma 2.14(a), two elliptic curves defined over k are isomorphic over $\bar{k}$ if and only if they have the same j-invariant. If E and E' are isomorphic elliptic curves with j-invariant 0 or 1728, then $k_{E,m}$ is not necessarily isomorphic to $k'_{E,m}$. Therefore, we will study the elliptic curves with j-invariant 0 or 1728 in their most general form.

Consider an elliptic curve E defined over a field k with j-invariant equal to 0. Then E has complex multiplication, that is, the ring $\mathrm{End}(E)$ of endomorphisms of E is bigger than $\mathbb{Z}$. Suppose $p \neq 2, 3$. Then $R = \mathrm{End}(E)$ is $\mathbb{Z}[\omega]$, where ω is a third root of unity. In this case, the group of units of R is $\{\pm 1, \pm\omega, \pm\omega^2\}$ which is isomorphic to $\mathbb{Z}/6\mathbb{Z}$. Therefore, $G_{E,m}$ is isomorphic to a subgroup of $\mathbb{Z}/6\mathbb{Z}$. We refer the reader to ([Har77], p.331) for more details. If char k is 2 or 3 then E is supersingular. Furthermore, if char $k = 2$ then the only 2-torsion point in $E(\bar{k})$ is O_E. Similarly, if char $k = 3$, then the only 3-torsion point in $E(\bar{k})$ is O_E. We now determine $G'_{E,m}$, where char $k \neq 2, 3$ and $m = 2, 3$.

Theorem A.1 *Let k be a field with char $k \neq 2, 3$ and let E be an elliptic curve over k with j-invariant 0 given by*

$$E: \ y^2 = x^3 + B,$$

where $B \in k \setminus \{0\}$. Then

(i) $G'_{E,2}$ is trivial if and only if -3 is a square in k and $-B$ is a cube in k;

(ii) $G'_{E,2}$ is isomorphic to a subgroup of C_2 if and only if $-B$ is a cube in k;

(iii) $G'_{E,2}$ is isomorphic to a subgroup of A_3 if and only if -3 is a square in k;

(iv) otherwise, $G \cong S_3$.

Proof: Let $f(x) \in k[x]$ be the division polynomial of the 2-torsion points in $E(\bar{k})$. Then f is given by

$$f(x) = 4(x^3 + B),$$

and the x-coordinates of the 2-torsion points in $E(\bar{k})$ are precisely the roots of f. Furthermore, $G'_{E,2}$ is equal to the Galois group of f over k. The discriminant of f is

$$-3(48B)^2,$$

which is not equal to zero. Therefore the roots of f are distinct. Let Φ be a choice of monomorphism $G \hookrightarrow S_3$ after labeling the roots of f. Then it suffices to categorize $\Phi(G)$ based on algebraic conditions on u_o.

The discriminant of $f(x)$ has a square in k if and only if $\sqrt{-3} \in k$. Part (iii) then follows from Lemma 3.16. Part (ii) follows since $f(x)$ has a linear factor over k if and only if $-B$ is a cube in k. Part (i) follows directly from Theorem 3.20. Part (iv) is clear since the only nontrivial proper subgroups of S_3 are A_3 and conjugates of $\langle(1\,2)\rangle$.

■

Theorem A.2 *Let k be a field with char $k \neq 2, 3$ and let E be an elliptic curve over k with j-invariant 0 given by*

$$E: \ y^2 = x^3 + B,$$

where $B \in k \setminus \{0\}$.

(i) $G'_{E,3}$ *is trivial if and only if* -3 *is a square in* k *and* $-4B$ *is a cube in* k*;*

(ii) $G'_{E,3}$ *is isomorphic to a subgroup of* C_2 *if and only if* $-4B$ *is a cube in* k*;*

(iii) $G'_{E,3}$ *is isomorphic to a subgroup of* A_3 *if and only if* -3 *is a square in* k*;*

(iv) otherwise, $G'_{E,3} \cong S_3$.

Proof: Let $f(x) \in k[x]$ be the division polynomial of the 3-torsion points in $E(\bar{k})$. Then f is given by

$$f(x) = 3x(x^3 + 4B),$$

and the x-coordinates of the 3-torsion points in $E(\bar{k})$ are precisely the roots of f. Furthermore, $G'_{E,3}$ is equal to the Galois group of f over k, denoted by G. The discriminant of f is

$$-3(1296B^2)^2,$$

which is not equal to zero. Therefore the roots of f are distinct. Let Φ be a choice of monomorphism $G \hookrightarrow S_4$ after labeling the roots of f. Then it suffices to categorize $\Phi(G)$ based on algebraic conditions on u_o.

Clearly, $\Phi(G)$ is isomorphic to a subgroup of S_3. The discriminant of $x^3 + 4B$ is $-3(12B)^2$, which has a square in k if and only if $\sqrt{-3} \in k$. Part (iii) then follows from Lemma 3.16. Part (ii) follows since $x^3 + 4B$ has a linear factor over k if and only if $-4B$ is a cube in k. Part (i) follows directly from Theorem 3.20. Part (iv) is clear since the only nontrivial proper subgroups of S_3 are A_3 and conjugates of $\langle(1\,2)\rangle$.

■

If E is an elliptic curve defined over a field k with $j(E) = 1728$ then E has complex multiplication, that is, the ring $\mathrm{End}(E)$ of endomorphisms of E is bigger than $\mathbb{Z}$. Suppose $j(E) = 1728$ and $p \neq 2, 3$. Then $R = \mathrm{End}(E)$ is the ring of Gaussian integers $\mathbb{Z}[i]$ and the group of units of R, or equivalently $\mathrm{Aut}(E)$, is $\{\pm 1, \pm i\} \cong \mathbb{Z}/4\mathbb{Z}$. Therefore, $G_{E,m}$ is isomorphic to a subgroup of $\mathbb{Z}/4\mathbb{Z}$. We refer the reader to ([Har77], p.331) for more details. We now determine $G'_{E,m}$, where char $k \neq 2, 3$ and $m = 2, 3$.

Theorem A.3 *Let k be a field with char $k \neq 2, 3$, and let E be an elliptic curve over k with j-invariant 1728 given by*

$$E: y^2 = x^3 + Ax,$$

where $A \in k \setminus \{0\}$. Then $G'_{E,2}$ is trivial if and only if $-A$ is a square in k. Otherwise, $G'_{E,2}$ is isomorphic to C_2.

Proof: Let $f(x) \in k[x]$ be the division polynomial of the 2-torsion points in $E(\bar{k})$. Then f is given by

$$f(x) = 4x(x^2 + A),$$

and the x-coordinates of the 2-torsion points in $E(\bar{k})$ are precisely the roots of f. Furthermore, $G'_{E,2}$ is equal to the Galois group of f over k, denoted by G. The discriminant of f is

$$-1024A^3,$$

which is not equal to zero. Therefore the roots of f are distinct. Let Φ be a choice of monomorphism $G \hookrightarrow S_3$ after labeling the roots of f. Then it suffices to categorize $\Phi(G)$ based on algebraic conditions on u_o.

Clearly, $\Phi(G)$ is isomorphic to a subgroup of $\langle(1\,2)\rangle$. Also, it is clear that $\Phi(G) = \{e\}$ if and only if $-A$ is a square in k.

■

Theorem A.4 *Let k be a field with char $k \neq 2, 3$ and let E be an elliptic curve over k with j-invariant 1728 given by*

$$E: y^2 = x^3 + Ax,$$

where $A \in k \setminus \{0\}$. Then

(i) $G'_{E,3}$ is trivial if and only if $A = (3+2\sqrt{3})a^2$ for some $a \in k$ and -3 is a square in k;

(ii) $G'_{E,3}$ is isomorphic to C_2 if and only if $A = (3+2\sqrt{3})a^2$ or $A = (3-2\sqrt{3})a^2$, for some $a \in k$;

(iii) $G'_{E,3}$ *is isomorphic to a subgroup of* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *if and only if either* 3 *is a square in* k *or* -3 *is a square in* k *and*

$$A = -\frac{1}{8}a^2(3+u), \qquad or \qquad A = -\frac{1}{8}a^2(3-u),$$

where $u^2 = -3$ *and* $a \in k$*;*

(iv) otherwise, $G'_{E,3}$ *is isomorphic to a subgroup of* D_4*.*

Proof: Let $\psi_3(x) \in k[x]$ be the division polynomial of the 3-torsion points in $E(\bar{k})$ and set $f(x) \in k[x]$ to be

$$f(x) = \frac{1}{3}\psi_3 = x^4 + 2Ax^2 - \frac{1}{3}A^2.$$

Then the x-coordinates of the 3-torsion points in $E(\bar{k})$ are precisely the roots of f. Furthermore, $G'_{E,3}$ is equal to the Galois group of f over k, denoted by G. The discriminant of f is

$$-3\left(\frac{64A^3}{9}\right)^2,$$

which is not equal to zero. Therefore the roots of f are distinct. Let Φ be a choice of monomorphism $G \hookrightarrow S_4$ after labeling the roots of f. Then it suffices to categorize $\Phi(G)$ based on algebraic conditions on u_o.

(iii) Suppose 3 is a square in k and $u^2 = 3$ for some $u \in k$. Then f factors as

$$3(x^2 + \frac{1}{3}(3-2u)A)(x^2 + \frac{1}{3}(3+2u)A).$$

Suppose -3 is a square in k and $u^2 = -3$ for some $u \in k$. If $A = -\frac{1}{8}a^2(3+u)$ for some $a \in k$, then f factors as

$$(x^2 - ax + \frac{1}{8}(1-u)a^2)(x^2 + ax + \frac{1}{8}(1-u)a^2).$$

If $A = -\frac{1}{8}a^2(3-u)$ for some $a \in k$, then f factors as

$$(x^2 - ax + \frac{1}{8}(1+u)a^2)(x^2 + ax + \frac{1}{8}(1+u)a^2).$$

Conversely, suppose f has two quadratic factors. Then there exist $a, b, c, d \in k$ such that

$$\begin{aligned} f(x) &= (x^2 + ax + b)(x^2 + cx + d) \\ &= (x^4 + (a+c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd). \end{aligned}$$

Equating the coefficients of the above polynomial with the coefficients of f gives

$$\begin{aligned} a + c &= 0, \\ b + d + ac &= 2A, \\ ad + bc &= 0, \\ bd &= -\frac{1}{3}A^2. \end{aligned}$$

Let $a = -c$ and consider two cases; $c = 0$ and $c \neq 0$. If $c = 0$ then $b+d = 2A$ and $bd = -A^2/3$. Substituting $b = 2A-d$ into $bd = -A^2/3$ gives $d^2-2Ad--A^2/3 = 0$. Therefore, d is a root of

$$g(x) = x^2 - 2Ax - A^2/3,$$

whose disriminant is a $\sqrt{3}$. Since $d \in k$ the discriminant of g is in k, hence 3 is a square in k.

If $c \neq 0$ then $b = d$ and

$$2d - c^2 = 2A, \qquad d^2 = -A^2/3.$$

Substituting $d = A + c^2/2$ into $d^2 = -A^2/3$ gives

$$\frac{4}{3}A^2 + Ac^2 + \frac{1}{4}c^4 = 0.$$

Hence, A is a root of $g(x) = \frac{4}{3}x^2 + c^2x + \frac{1}{4}c^4 \in k[x]$ and the discriminant of g, namely $-c^4/3$, has a square in k. Therefore, $u^2 = -3$ for some $u \in k$. Furthermore,

$$A = -\frac{1}{8}c^2(3 \pm u),$$

as desired.

(ii) Suppose that $u^2 = 3$ for some $u \in k$. If $A = (3 + 2u)a^2$ for some $a \in k$, then f factors as

$$(x - a)(x + a)(x^2 + (7 + 4u)a^2).$$

If $A = (3 - 2u)a^2$ for some $a \in k$, then f factors as

$$(x - a)(x + a)(x^2 + (7 - 4u)a^2).$$

Conversely, suppose f has a linear factor over k. Then $f(a) = 0$ for some $a \in k$ and

$$a^4 + 2Aa^2 - \frac{1}{3}A^2 = 0.$$

Hence, A is a root of $g(x) = -x^2/3 + 2a^2x + a^4$ and the discriminant of g, namely $3(4a^2)^2$, has a square in k. Therefore, $u^2 = 3$ for some $u \in k$. Furthermore,

$$A = (3 \pm 2u)a^2.$$

It is noted that if f has a linear factor, $x - a$, over k then f factors over k as

$$(x - a)(x + a)(x^2 + a^2 + 2A).$$

(i) The discriminant of f is

$$\frac{(64A^3)^2}{-27},$$

which has a square in k if and only if -3 is a square in k. The result then follows directly using the results from part *(ii)* and Theorem 3.20.

(iv) The D_4 resolvent of $f(x)$ is

$$R(x) = \frac{1}{3}(x - 2A)(3x^2 + 4A^2),$$

whence $\Phi(G) \subseteq H \cong D_4$ by Lemma 3.24. Furthermore, the C_4 resolvent of $f(x)$ is $C(x) = x^2$, which does not have distinct roots in k. Therefore, we cannot use Lemma 3.26.

■

Theorem A.5 *Let k be a field with char $k = 2$ and let E be an elliptic curve over k with j-invariant 0 given by*

$$E: \ y^2 + Ay = x^3 + Bx + C,$$

where $A, B, C \in k$ and $A \neq 0$. Then

(i) $G'_{E,3}$ is trivial if and only if $x^4 + A^2x + B^2$ and $x^2 + x + 1$ each have a root in k and A is a cube in k;

(ii) $G'_{E,3}$ is isomorphic to a subgroup of C_2 if and only if $x^4 + A^2x + B^2$ has a root in k and A is a cube in k;

(iii) $G'_{E,3}$ is isomorphic to a subgroup of A_3 if and only if $G'_{E,3}$ is isomorphic to a subgroup of S_3 and $x^2 + x + 1$ has a root in k;

(iv) $G'_{E,3}$ is isomorphic to a subgroup of S_3 if and only if $x^4 + A^2x + B^2$ has a root in k;

(v) $G'_{E,3}$ is isomorphic to a subgroup of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if and only if $A^2 = c^3$ and $B^2 = (c^2 + d)d$, for some $c, d \in k$;

(vi) $G'_{E,3}$ is isomorphic to a subgroup of D_4 if and only if A is a cube in k;

(vii) $G'_{E,3}$ is isomorphic to a subgroup of A_4 if and only if $x^2 + x + 1$ has a root in k;

(viii) $G'_{E,3} \cong S_4$.

Proof: Let $f(x) \in k[x]$ be the division polynomial of the 3-torsion points in $E(\bar{k})$. Then f is given by

$$f(x) = \psi_3 = x^4 + A^2x + B^2,$$

and the x-coordinates of the 3-torsion points in $E(\bar{k})$ are precisely the roots of f. Furthermore, $G'_{E,3}$ is equal to the Galois group of f over k, denoted by G. The Berlekamp discriminant of f is a root of $x^2 + x + 1$, which is clearly not equal to zero. Therefore the roots of f are distinct. Let Φ be a choice of monomorphism $G \hookrightarrow S_4$ after labeling the roots of f. Then it suffices to categorize $\Phi(G)$ based on algebraic conditions on u_o.

(vii) The Berlekamp discriminant of f is a root of x^2+x+1. The result then follows from Theorem 3.16.

(vi) The D_4 resolvent of f is

$$R(x) = x^3 + A^4,$$

which has a root in k if and only if A is a cube in k. Suppose $a \in k$ is a root of R. Then the C_4 resolvent of f is $C(x) = x^2$, which does not have distinct roots in k. Therefore, we cannot use Lemmas 3.26.

(v) Suppose $A^2 = c^3$ and $B^2 = (c^2+d)d$ for some $c, d \in k$. Then f factors as

$$(x^2+cx+d)(x^2+cx+c^2+d).$$

Conversely, suppose f has two quadratic factors. Then there exist $a, b, c, d \in k$ such that

$$\begin{aligned} f(x) &= (x^2+ax+b)(x^2+cx+d) \\ &= x^4+(a+c)x^3+(b+d+ac)x^2+(ad+bc)x+bd. \end{aligned}$$

Equating the coefficients of the above polynomial with the coefficients of f gives

$$\begin{aligned} a+c &= 0, \\ b+d+ac &= 0, \\ ad+bc &= A^2, \qquad \text{(A.1)} \\ bd &= B^2. \qquad \text{(A.2)} \end{aligned}$$

Substituting $a = -c$ and $b = c^2 - d$ into equations (A.1) and (A.2) gives

$$A^2 = c^3 \qquad \text{and} \qquad B^2 = d(d+c^2)$$

as desired.

(iv) This is clear.

(iii) The result follows directly from Parts (iv) and (vii).

(ii) The result follows directly from Parts (iv) and (vi).

(i) From Theorem 3.20, $\Phi(G) = \{e\}$ if and only if $\Phi(G)$ is contained in a conjugate of $\langle(1\,2)\rangle$ and A_4. The result then follows from Parts (ii) and (vii).

■

Theorem A.6 *Let k be a field with char $k = 3$, and let E be an elliptic curve over k with j-invariant 0 given by*

$$E:\ y^2 = x^3 + Ax + B,$$

where $A, B \in k$ and $A \neq 0$. Then

(i) $G'_{E,2}$ is trivial if and only if A is a square in k and $x^3 + Ax + B$ has a root in k;

(ii) $G'_{E,2}$ is isomorphic to a subgroup of C_2 if and only if $x^3 + Ax + B$ has a root in k;

(iii) $G'_{E,2}$ is isomorphic to a subgroup of A_3 if and only if A is a square in k;

(iv) otherwise, $G'_{E,2} \cong S_3$.

Proof: Let $f(x) \in k[x]$ be the division polynomial of the 2-torsion points in $E(\bar{k})$. Then f is given by

$$f(x) = \psi_2 = x^3 + Ax + B,$$

and the x-coordinates of the 2-torsion points in $E(\bar{k})$ are precisely the roots of f. Furthermore, $G'_{E,2}$ is equal to the Galois group of f over k, denoted by G. The discriminant of f is $2A^3$, which is not equal to zero. Therefore the roots of f are distinct. Let Φ be a choice of monomorphism $G \hookrightarrow S_3$ after labeling the roots of f. Then it suffices to categorize $\Phi(G)$ based on algebraic conditions on u_o.

The discriminant of f is $2A^3$, which has a square in k if and only if A is a square in k. Part (iii) then follows directly from Lemma 3.16. Part (ii) is clear. Part (i) follows directly from Theorem 3.20. Part (iv) is clear since the only nontrivial proper subgroups of S_3 are A_3 and conjugates of $\langle(1\,2)\rangle$.

■

Bibliography

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over **Q**: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The magma algebra system i: the user language. *J. Symbolic Computation*, 24(3-4):235–265, 1997.

[Ber76] E.R. Berlekamp. *An Analog to the Discriminant over Fields of Characteristic Two*, volume 38. McGraw-Hill Inc., 1976.

[Bir72] B. Birch. *Lecture Notes in Mathematics, v.320.* Springer-Verlag, Germany, 1972.

[Coh93] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag New York Inc., Berlin, 1993.

[Dor91] D. R. Dorman. On singular moduli for rank 2 drinfeld modules. *Compositio Mathematica*, 80:239–240, 1991.

[Esc97] J-P. Escofier. *Galois Theory.* Springer-Verlag New York Inc., Paris, 1997.

[Gar86] D.J.H. Garling. *Galois Theory.* Cambridge University Press, Cambridge, 1986.

[GGC81] K. O. Geddes, Gaston H. Gonnet, and Bruce W. Char. Maple user's manual. Technical Report CS-82-40, Computer Science Department, University of Waterloo, Canada, 1981.

[Ham03] Y. Hamahata. The values of j-invariants for drinfeld modules. *Manuscripta Math*, 112:93–108, 2003.

[Har77] R. Hartshorne. *Algebraic Geometry.* Springer-Verlag New York Inc., USA, 1977.

[HS91] M. Hindry and J.H. Silverman. *Diophantine Geometry: An Introduction.* Springer-Verlag New York Inc., USA, 1991.

[Lan76] S. Lang. *Introduction to Modular Forms.* Springer-Verlag New York Inc., Berlin, 1976.

[Lan02] S. Lang. *Algebra Revised Third Edition.* Springer-Verlag New York Inc., USA, 2002.

[Poo97] B. Poonen. Torsion in rank 1 drinfeld modules and the uniform boundedness conjecture. *Mathematische Annalen*, 308:571–586, 1997.

[Ros02] M. Rosen. *Number Theory in Function Fields.* Springer-Verlag New York Inc., USA, 2002.

[Sch91] W.C. Schulz. Cubics with a rational root. *Mathematics Magazine*, 64(3):172–175, June 1991.

[Sil86] J. H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag New York Inc., USA, 1986.

[Wil95] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.