Spring 2013

Galois Representations From Non-Torsion Points on Elliptic Curves

Matthew Phillip Hughes
Bard College, mh6379@bard.edu

Galois Representations From Non-Torsion Points on Elliptic Curves

A Senior Project submitted to
The Division of Science, Mathematics, and Computing
of
Bard College

by
Matthew Hughes

Annandale-on-Hudson, New York
May, 2013

Abstract

Working from well-known results regarding ℓ-adic Galois representations attached to elliptic curves arising from successive preimages of the identity, we consider a natural deformation. Given a non-zero point P on a curve, we investigate the Galois action on the splitting fields of preimages of P under multiplication-by-ℓ maps. We give a group-theoretic structure theorem for the corresponding Galois group, and state a conjecture regarding composita of two such splitting fields.

Contents

List of Figures

Dedication

For my folks.

Acknowledgments

Chief amongst those who deserve acknowledgement for this project is my wonderful advisor, John Culliinan. His supportiveness and insight has been unwaveringly helpful during my long struggle to maintain sanity throughout these past nine months.

I am grateful to a all my friends who have restrained themselves from punching me in the face during those inevitable periods of temporary insanity that come with burning the candle at both ends. I am equally grateful to those of my friends who have been willing to provide such face-punching, where appropriate.

I would like to thank Hello Kitty, for existing.

0
Introduction

Let E/K be an elliptic curve defined over a number field K. The abelian group structure of E allows us to define multiplication maps $[m]$ on it, given by adding a point to itself m times. The kernel of this homomorphism is written $E[m]$, and is isomorphic as a group to $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$. We can define a Galois representation

$$\rho_m \colon \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Aut}(E[m]) \simeq \mathrm{Aut}(\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}).$$

by how the Galois action permutes the elements of this kernel, which is by a linear transformation. Taking the sequence of subgroups $E[\ell^n]$ for a prime ℓ, we can map from $E[\ell^{n+1}]$ to $E[\ell^n]$ by way of $[\ell]$. The resulting inverse limit is called the Tate module $T_\ell(E) := \varprojlim E[\ell^n]$, which is an ℓ-adic vector space. We can extend our Galois representation in a natural way along this inverse limit, yielding an ℓ-adic representation of $\mathrm{Gal}(\bar{K}/K)$.

A great deal of mathematics has been done on these ℓ-adic Galois representations. Serre asked in [12] whether there is a bound $n(K)$ for each number field K such that the ℓ-adic Galois representation associated to each curve E/K is surjective for all $\ell \geq n(K)$. (An English-language introduction to this subject can be found in [1].) The standing conjecture is that $n(\mathbf{Q}) = 37$.

In this project we will alter this picture by considering preimages of rational points P of infinite order, rather than the preimages of the identity. This yields a similar inverse limit structure, and a similar ℓ-adic representation. The image of this representation is contained in $T_\ell(E) \rtimes \mathrm{Aut}(T_\ell(E))$. This representation can be used to study the reduction of the point $P \mod \mathfrak{p}$ for some prime $\mathfrak{p}$ of good reduction for E, as is done in [5, 9].

Our heads will not be so firmly set in the clouds, however. We restrict our attention to the first iteration of the $[\ell]$ map and the resulting preimage $E^P[\ell]$ of the point P. We will show that the Galois extension achieved by adjoining to K all the coordinates of preimages of P has Galois group contained in $E[\ell] \rtimes \mathrm{Aut}(E[\ell])$, and describing this group as a linear group over the finite field $\mathbf{F}_\ell$. We then work towards a classification of the behavior of this extension as we allow P to vary among all K-rational points of infinite order on E.

The first two chapters will be devoted to basic prerequisites of elliptic curves and Galois Theory, respectively. In Chapter 1 we will give rational mappings for the multiplication maps $[m]$. Chapter 3 will sketch the Galois extensions coming from taking the preimages of points, beginning with the $E[\ell]$, all the while exploiting the rationality of the multiplication maps $[m]$ to make arguments about the resulting Galois extensions. The last chapter contains a computational guide to the subject, with specific examples computed in PARI/GP.

1
Elliptic Curves

1.1 Fundamentals

This project is intimately related to elliptic curves, so we'll do well to talk about them for a bit.

Definition 1.1.1. An *elliptic curve* over a field K is a smooth, projective algebraic curve of genus 1 with a specified K-rational point $\mathcal{O}$. △

There is a good amount of unpacking to be done with this definition, not all of which we will do here. We will be looking at elliptic curves from a more computational perspective for this project, in terms of the polynomials that define them in the projective plane. So, before we move on, let's give this more conccrete definition. For our purposes, K will denote a perfect field and $\bar{K}$ its algebraic closure.

Definition 1.1.2. As a projective algebraic variety, any elliptic curve E defined over K is given by an equation of the form

$$E\colon\ y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

where $a_1, a_2, a_3, a_4, a_6 \in K$, provided this equation is non-singular. △

Equations of this form are referred to as *Weierstrass* equations.

Remark. We will commonly abbreviate the fact that the curve E is defined over a field K by writing E/K. Although this is in direct competition with the notation we use for field extensions later, the meaning should be clear from the context. By $P \in E$ we mean $P \in E(\bar{K}) = \{P \in \mathbf{P}^2(\bar{K}) \mid f(P) = 0\}$, where $f(x, y, z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3$, and we often represent points P with non-zero z-coordinate in affine coordinates, writing (x, y) for the point $(x, y, 1)$. ◊

When written in affine coordinates this equation is a polynomial of degree 2 on the left side and a cubic in x on the right. The striking absence of the coefficient a_5 will remain somewhat mysterious, as it is the result of the Riemann-Roch theorem (treated in [13, II.5]), which is beyond the scope of this paper. The notation is standard enough that we would be remiss not to point it out to the reader.

Making Definition 1.1.2 clear requires some explanation of what it means for the curve to be non-singular. We can very easily delineate which equations of the form $y^2 + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$ are non-singular, however, in terms of a quantity associated to the curve called the discriminant. When the discriminant Δ is non-zero, the curve is non-singular (smooth). We give a fairly direct way of calculating the discriminant of a curve from the coefficients of its Weierstrass equation:

$$b_2 = a_1^2 + 4a_2 \quad b_4 = 2a_4 + a_1a_3 \quad b_6 = a_3^2 + 4a_6$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

Parenthetically, in practice we will usually describe elliptic curves using much simpler forms of the Weierstrass equation, namely those for which $a_1 = a_2 = a_3 = 0$. Relabeling the coefficients by $a_4 = a$, $a_6 = b$ and writing the equation in affine coordinates (while

understanding that this is shorthand), we get $y^2 = x^3 + ax + b$. This gives a much more intelligible expression (and interpretation, as we will see in Section 2.2) for the discriminant,

$$\Delta = -16(4a^3 + 27b^2). \tag{1.1.1}$$

Returning briefly to Definition 1.1.1, what are we to make of the "genus" of an algebraic curve? The reader is probably more familiar with the genus as a topological notion, which counts the handles on a compact surface. A sphere has genus 0, a torus has genus 1, a double torus has genus 2, and so forth. But in what sense does a curve have genus? Is this use of the term implying some correspondence between elliptic curves and tori?

In essence, yes. The genus of an algebraic curve defined over the complex numbers is the genus of the compact Riemann surface of that curve, which for an elliptic curve is a torus. The correspondence between elliptic curves and tori is by way of the Weierstrass $\wp$-function.

Definition 1.1.3. Let $\Lambda \subset \mathbf{C}$ be a full lattice (i.e. the integral span of two complex numbers ω_1, ω_2, which are $\mathbf{R}$-linearly independent). The Weierstrass $\wp$-function for Λ is defined by

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$$

△

Such $\wp$ are meromorphic, since they are holomorphic everywhere except points of Λ. They are also clearly even elliptic functions, with generators of the lattice ω_1, ω_2 as periods (that is, $\wp(z + \omega_1) = \wp(z + \omega_2) = \wp(z)$ for all $z \in \mathbf{C}$). Interestingly, the Weierstrass $\wp$ corresponding to Λ satisfied the differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda) \tag{1.1.2}$$

for all z not on Λ, where $g_2(\Lambda) = 60\sum_{\omega\in\Lambda-\{0\}}\frac{1}{\omega^4}$ and $g_3(\Lambda) = 140\sum_{\omega\in\Lambda-\{0\}}\frac{1}{\omega^6}$ are convergent *Eisenstein series* for Λ. Looking simply at the exponents of Equation 1.1.2, it bears some resemblance to the Weierstrass equation in Definition 1.1.2. The function $\wp$ can

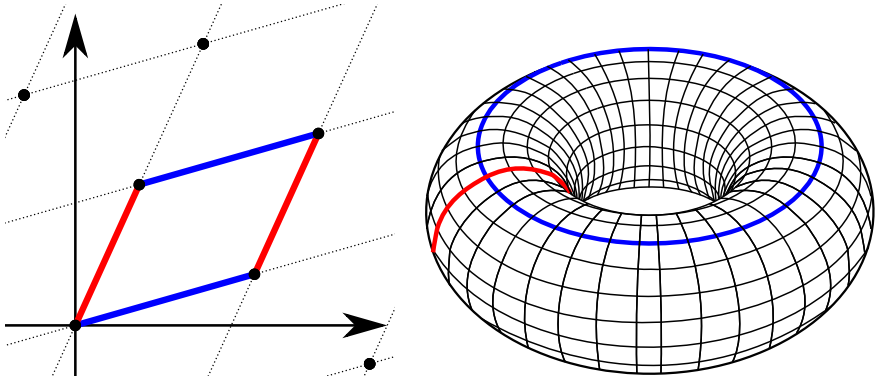

Figure 1.1.1. A lattice Λ in the complex plane with a torus isomorphic to $\mathbf{C}/\Lambda$.

be thought of as a function on the complex numbers modulo a lattice $\mathbf{C}/\Lambda$. The complex numbers modulo a lattice is topologically equivalent to a torus (imagine gluing opposite sides of a rectangular sheet of something stretchy), so we can intuitively see already how this picture is the "genus 1" case. Additionally, the left hand side of the above is of degree 2 on the left hand side, and a cubic on the right, similar to the description of the defining equation for an elliptic curve given earlier.

This is not a coincidence, and in fact the mapping $\phi\colon \mathbf{C}/\Lambda \longrightarrow \mathbf{P}^2(\mathbf{C})$ defined by $z \mapsto [\wp(z), \wp'(z), 1]$ makes the correspondence we've anticipated explicit. For details on this that would be gratuitous here, see [13, §VI.3].

So why would we go to all the trouble of describing elliptic curves using complex analysis when elliptic curves can be defined easily using polynomial expressions? The answer is that certain properties of elliptic curves are much more intuitive when constructed in this way over the complex numbers. Chief among these properties is that elliptic curves are *abelian* varieties, meaning that they have the structure of an abelian group. This is not surprising when we consider them to have come from tori; the complex numbers are an abelian group

under addition, and a quotient by a subgroup lattice is also. So, while I won't be tracing this through the correspondence we just outlined, we have some idea of why we should expect elliptic curves to have an abelian group structure, so that this does not seem to be cosmic coincidence. It also gives a convenient way for me to wave my hands through some details about the torsion subgroups of an elliptic curve, later.

1.2 The Group Structure of an Elliptic Curve

It will be necessary to devote some time to an explicit description of the group structure of an elliptic curve. First, however, we note that when we are defining an elliptic curve E over a field K of characteristic $\neq 2, 3$, we can rationally change the coordinates of the Weierstrass equation to yield a simpler form, namely

$$E\colon\ y^2 = x^3 + ax + b. \tag{1.2.1}$$

The rational coordinate changes are given in [13, III.1]. We note that because this is a polynomial of degree 3, a line in the projective plane $\mathbf{P}^2(\mathbf{C})$ will intersect this curve at precisely 3 points, counting multiplicity and points "at infinity" (this is due to Bézout's Theorem, one thing very convenient about projective geometry). In particular, the point $\mathcal{O} = [0, 1, 0]$ at infinity will provide the identity element of our group.

Definition 1.2.1. Let $P, Q \in E$ be points on an elliptic curve E. Then the line L_1 going through these two points intersects the curve E in one other point; call this point R. The sum $P + Q$ is defined to be the unique third point of intersection of E with the line L_2 passing through R and $\mathcal{O}$. △

Remark. The line L_2 mentioned in the above definition will always be vertical when we plot the curve according to the simplified Weierstrass form (and we will likely not have occasion to do otherwise). Thus the second intersecting process could be described just as easily by a reflection of the point R over the x-axis. ◊

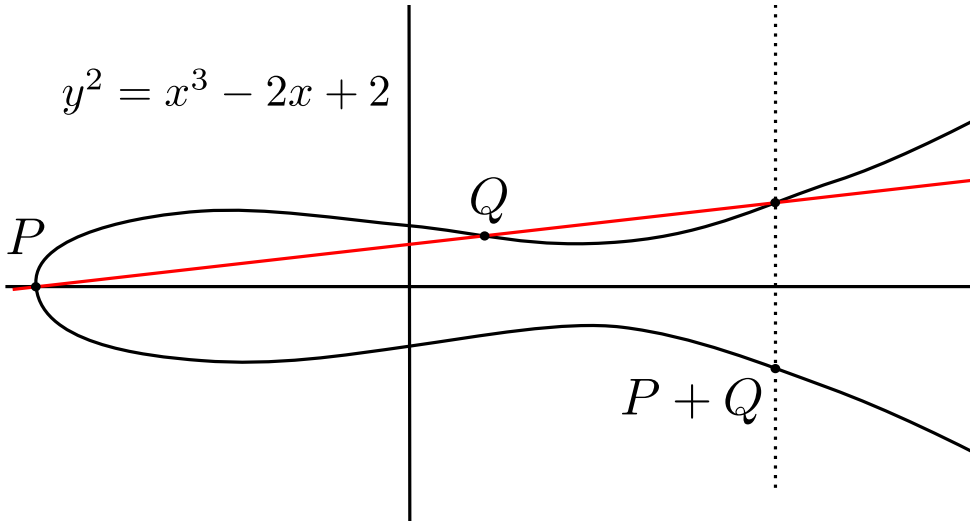

Figure 1.2.1. The addition rule in action.

The commutativity of this operation is clear from the definition. If the Hessian $H(x, y, z)$ for the curve $f(x, y, z) = y^2z - x^3 - axz^2 - bz^3 = 0$ vanishes at $[0, 1, 0] = \mathcal{O}$, then the line at infinity intersects the curve at $\mathcal{O}$ with multiplicity 3. Indeed, the determinant of the matrix of second derivatives is $H(x, y, z) = 24xy^2$, so $H(0, 1, 0) = 0$. Thus the point $\mathcal{O}$ does indeed form the identity element for the abelian group $E(\bar{K})$, since the two lines L_1 and L_2 from Definition 1.2.1 are the same when we try to add $\mathcal{O}$ to any $P \in E(\bar{K})$ (both are vertical). We note that a line through $P = (x_0, y_0)$ and its reflection across the x-axis $(x_0, -y_0)$ will always be vertical, and so will intersect the curve at $\mathcal{O}$. Thus $(x_0, -y_0) + (x_0, y_0) = \mathcal{O}$ according to the group addition. The only remaining property of a group operation is associativity.

Unfortunately, associativity isn't anywhere near as convenient to prove. We can, however, write down explicit rational formulas for the coordinates of the sum of two points. We could use these to check associativity directly, but we have more important things to do with our time. A geometric proof of this fact can be found in [14, §I.2].

Lemma 1.2.2. *For $P = (x_1, y_1), Q = (x_2, y_2)$ on an elliptic curve E: $y^2 = x^3 + ax + b$, if $Q \neq \pm P$ we have*

$$x(P+Q) = \frac{(y_2 - y_1)^2 - (x_2 - x_1)(x_2^2 - x_1^2)}{(x_2 - x_1)^2}, \text{ and}$$

$$y(P+Q) = \frac{(y_2x_2 + 2y_2x_1 - y_1x_1 - 2y_1x_2)(x_2 - x_1)^2 - (y_2 - y_1)^3}{(x_2 - x_1)^3}.$$

We already know what happens in the case when $Q = -P$, then their sum is $\mathcal{O}$. But what happens when $Q = P = (x_1, y_1)$? Remembering that we are considering intersections of lines with multiplicity in the algorithm given in Definition 1.2.1, we note that the first line L_1 must be tangent to the point P. We can find the slope of this line by taking the derivative of the Weierstrass equation, yielding $2y\frac{\mathrm{d}y}{\mathrm{d}x} = 3x^2 + a$, yielding a slope of $m = (3x_1^2 + a)/(2y_1)$. The equation for the line L_1 is thus given by $y - y_1 = m(x - x_1)$, and so the intersection with the curve is given by

$$x^3 + ax + b = y^2 = (m(x - x_1) + y_1)^2 = m^2(x - x_1)^2 + 2my_1(x - x_1) + y_1^2.$$

The resulting cubic polynomial is ... unwieldy. We could factor it directly to find the

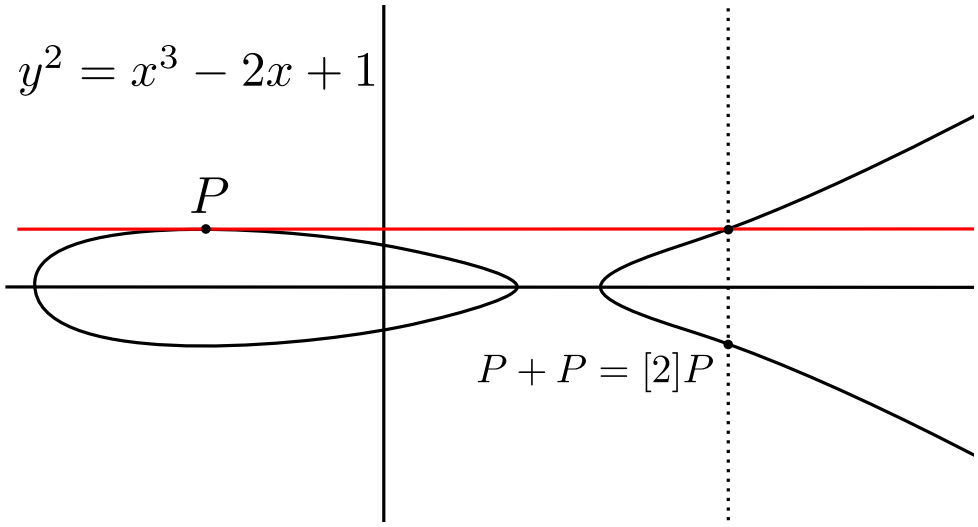

Figure 1.2.2. Adding a point to itself.

x-coordinates of the three points of intersection of L_1 with the curve. However, we already

know two of these points since L_1 was constructed to intersect E at P with multiplicity 2, and we can exploit this information to avoid some messy computation. We note that the coefficient of the x^2 term of a monic cubic polynomial is the negative of the sum of the roots of that cubic. Thus we have $-m^2 = -x(P+P) - 2x_1$, since the x-coordinate of a point on E is the same as that of its negative. Therefore

$$x(P+P) = m^2 - 2x_1 = \frac{(3x_1^2+a)^2}{4y_1} - 2x_1 = \frac{(3x_1^2+a)^2}{4(x_1^3+ax_1+b)} - 2x_1,$$

i.e.

$$x(P+P) = \frac{x_1^4 - 2ax_1^2 - 8bx_1 + a^2}{4(x_1^3+ax_1+b)}. \tag{1.2.2}$$

The y-coordinate can be easily computed by substituting this expression into the equation we found for L_1, remembering that we need to reflect over the x-axis before we arrive at the point $P+P$. The result, for completion:

$$y(P+P) = \frac{(x_1^6 + 5ax_1^4 + 20bx_1^3 - 5a^2x_1^2 - 4abx_1 - 8b^2 - a^2)y_1}{8(x_1^3+ax_1+b)^2} \tag{1.2.3}$$

This case of group addition, in which we are adding a point to itself some number of times, is significantly more relevant to this project. It warrants some special notation: let $[m]\colon E \longrightarrow E$ be defined by $[m]P = \underbrace{P+P+\ldots+P}_{m \text{ summands}}$ for an integer m. In many situations it is natural to consider only $[\ell]$ for primes ℓ, as we will later in the project.

Following Adelmann ([1, §3.3]), we can use the recursively defined *division polynomials* $\psi_m(x,y)$ to write out explicit rational functions for the x- and y-coordinates of $[m]P$ for an arbitrary point $P=(x,y)$. Given an elliptic curve of the form $y^2 = x^3+ax+b$, we define

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

$$\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2$$

$$\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3)$$

$$\psi_{2k} = \psi_k(\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2)/(2y)$$

$$\psi_{2k+1} = \psi_{k+2}\psi_k^3 - \psi_{k-1}\psi_{k+1}^3 \tag{1.2.4}$$

Note that every time a y^2 appears in a division polynomial, we can substitute the defining polynomial $y^2 = x^3 + ax + b$ of the elliptic curve, constraining our view to the polynomial ring $K[x] \oplus yK[x]$. One can easily show by induction that ψ_{2k} is a polynomial divisible by $2y$ for all $k \in \mathbf{N}$, and that $\psi_{2k+1} \in K[x]$ after making this substitution.

As I mentioned earlier, the division polynomials give us formulas for multiplication by m:

$$[m](x,y) = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2}, \frac{\psi_{2m}}{2\psi_m^4}\right) = \left(\frac{x\psi_m^2 - \psi_{m-1}\psi_{m+1}}{\psi_m^2}, \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y\psi_m^3}\right) \tag{1.2.5}$$

An elementary proof of this fact would be lengthy and unenlightening, so we won't pursue one. A very interesting and enlightening derivation of the division polynomials in terms of the Weierstrass $\wp$ function is given in Chapter II of [6].

1.3 The Mordell-Weil Group

For any subfield $k \subseteq \bar{K}$, we denote the set of points on E with coordinates in k by $E(k)$. In this section we explore fundamental structure properties regarding the set of points with rational coordinates on an elliptic curve E/K, where K is a number field. The set $E(K) = \{P \in \mathbf{P}^2(K) \mid f(P) = 0\}$ is called the *Mordell-Weil group* of E/K. To justify its being so named, we note the following:

Lemma 1.3.1. *For any field K, if E/K is an elliptic curve, then $E(K)$ is a subgroup of $E(\bar{K})$.*

Proof. For two distinct K-rational points P, Q on an elliptic curve E/K, the slope of the equation of the line L_1 between them is also K-rational. When $P = Q$, we notice that the slope of the tangent line to E at P must be K-rational, since it is obtained by differentiating the defining equation of the curve which has coefficients in K. Thus the

third point of intersection with the curve must be a K-rational point, so the line L_2 must have coefficients in K, since $\mathcal{O}$ is K-rational. Thus by the same token the third point of intersection $P+Q$ must also be K-rational. Because the slope of the line intersecting the curve at P and $\mathcal{O}$ is K-rational, its third point of intersection $-P$ must be also. □

For $\mathrm{char}(K) \neq 2, 3$ we can verify this explicitly based on the rational functions with coefficients in K for $P+Q$, $-P$, and $[2]P$ given in the last section. This approach of appealing to rational functions will be used (excessively) in later sections, so it is interesting to note it here also.

From the above lemma it is clear that the Mordell-Weil group of a curve $E/\mathbf{Q}$ is indeed a group. However, what it the structure of this group? One of the more fundamental results about $E(\mathbf{Q})$ is the following, a named special case of the Mordell-Weil Theorem:

Theorem 1.3.2 (Mordell's Theorem)**.** *For an elliptic curve $E/\mathbf{Q}$, the group $E(\mathbf{Q})$ is finitely generated.*

Consequently, by the fundamental theorem for abelian groups,

$$E(\mathbf{Q}) \simeq E(\mathbf{Q})_{\mathrm{tors}} \oplus \mathbf{Z}^r$$

for some positive integer r, and some finite abelian group $E(\mathbf{Q})_{\mathrm{tors}}$. The integer r is referred to as the Mordell-Weil rank of E (although we will commonly refer to it simply as the "rank"). The finite-order part $E(\mathbf{Q})_{\mathrm{tors}}$ is called the *torsion* subgroup of the Mordell-Weil group, and the infinite-order subgroup is called the *free* part of $E(\mathbf{Q})$.

We will proceed by proving a special case of Mordell's theorem, and then discussing how our proof could be generalized. The proof makes use of a height function on a point which, intuitively, measures how "complicated" a point is. We will take a set of points of low height ("simple" points), and show that these points must generate the entire group $E(\mathbf{Q})$. Additionally, we will see that there are only a finite number of points on an

elliptic curve that are simple enough to be in our set, and so $E(\mathbf{Q})$ is finitely generated. This strategy is an adaptation of the method of infinite descent, although we will not be phrasing it as such. First we define the height of a point.

Definition 1.3.3. The *height function* $h\colon E(\mathbf{Q}) \longrightarrow \mathbf{R}$ is defined by

$$h(P) = \log(\max\{|m|, |n|\}) \tag{1.3.1}$$

for any non-zero point $P = (x, y) \in E(\mathbf{Q})$, where $m, n \in \mathbf{Z}$ such that $\frac{m}{n} = x$ is in lowest terms. Additionally, $h(\mathcal{O}) = 0$. △

Points are complicated when they have complicated fractions as their x-coordinate. However, seeing as there are only finitely many rational numbers more simple than a given rational number, we know that for each positive $n \in \mathbf{R}$

$$\{P \in E(\mathbf{Q}) \mid h(P) \leq n\} \tag{1.3.2}$$

is finite, since there are only finitely many x-coordinates allowed for points in this set.

We note several bounds on the height of sums of points which we will use in the proof.

Lemma 1.3.4. *For any rational point $Q \in E(\mathbf{Q})$ there exists a constant $\kappa_0 \in \mathbf{R}$ such that*

$$h(P + Q) \leq 2h(P) + \kappa_0 \qquad \text{for all } P \in E(\mathbf{Q}).$$

This lemma tells us that for any rational point Q, the sum $P + Q$ is not too much more complicated than P for any P. It is in direct contrast to the next bound, which tells us that doubling a point makes it significantly more complicated.

Lemma 1.3.5. *There exists a $\kappa \in \mathbf{R}$ such that for all $P \in E(\mathbf{Q})$,*

$$h(2P) \geq 4h(P) - \kappa.$$

Both of these lemmas can be proven in an elementary way, using the explicit formulas we've given earlier for addition and doubling on an elliptic curve. Some mildly tiresome

proofs in that vein can be found in [14, III.2 and 3]. One final lemma remains to be stated, which is much less elementary to prove.

Lemma 1.3.6 (The Hard Part)**.** *The index of* $2E(\mathbf{Q})$ *in* $E(\mathbf{Q})$ *is finite.*

We refer the reader to a very clear proof given in [14] which splits the process of duplication into two maps, one which takes us into another elliptic curve chosen specifically for this argument and the other bringing us back to the original curve. That proof only suffices for curves which have a rational point of order 2, however, although this can be easily resolved using [13, §VIII.1 Lemma 1.1.1]. We are ready to prove the theorem.

Proof of Theorem 1.3.2. Because $2E(\mathbf{Q})$ is of finite index in $E(\mathbf{Q})$, we can choose a finite set of coset representatives $Q_i \in E(\mathbf{Q})$, such that $\bigcap_i (Q_i + 2E(\mathbf{Q})) = E(\mathbf{Q})$. Take κ_i to be the constant from Lemma 1.3.4 corresponding to $-Q_i$ (noting that $h(-Q_i) = h(Q_i) = h(Q_i + \mathcal{O}) \leq 2h(\mathcal{O}) + \kappa_i = \kappa_i$), and take κ' to be the constant from Lemma 1.3.5. Let $\kappa = \max_i\{\kappa', \kappa_i\}$ and let $S = \{P \in E(\mathbf{Q}) \mid h(P) \leq 2\kappa\}$. Then clearly S is finite. We claim that it generates all of $E(\mathbf{Q})$. Suppose not. Because the height function h has a discrete image, we can choose a point $P' \in E(\mathbf{Q}) - \langle S \rangle$ of minimal height. We note that $P' \in Q_i + 2E(\mathbf{Q})$ for some i, and so $P' = Q_i + 2R$ for some $R \in E(\mathbf{Q})$. Then we have

$$4h(R) \leq h(2R) + \kappa = h(P' - Q_i) + \kappa \leq 2h(P') + 2\kappa < 3h(P')$$

by applying our bound κ according to the two lemmas we've proven and by noting that $h(P') > 2\kappa$ since otherwise P' would be in S. Thus $h(R) < h(P')$, and so $R \in \langle S \rangle$. But $Q_i \in S$, so we have $P' \in \langle S \rangle$, a contradiction. □

This proof strategy can be generalized to arbitrary number fields, by defining a height function with similar properties on such a field. The details of this process rapidly surpass the scope of this project, and so we will simply state the result.

Theorem 1.3.7 (The Mordell-Weil Theorem for Elliptic Curves)**.** *Let E/K be an elliptic curve defined over a number field. Then $E(K)$ is finitely generated.*

The theorem in its full generality holds for arbitrary abelian varieties (higher dimensional analogues of elliptic curves) defined over number fields. We will only have occasion to use this special case of the theorem.

Looking only at the proof we've given for Mordell's Theorem, one might expect the generating set for the Mordell-Weil group to be quite large in the generic case, but in practice the generating sets turn out to be much smaller. This is easier to see when one considers generating sets for the two parts of the Mordell-Weil group separately. While a lot of mathematics has been done exploring both parts, the torsion subgroup is much better understood than the free part. The problem of finding the rational torsion points on an elliptic curve over $\mathbf{Q}$ is solved by the following theorem of Nagell and Lutz.

Theorem 1.3.8 (Nagell & Lutz)**.** *Given a curve $E : y^2 = x^3 + ax + b$ for $a, b \in \mathbf{Z}$, the coordinates x, y of any non-zero rational torsion point satisfy the following:*

1. *$x, y \in \mathbf{Z}$, and*

2. *$y = 0$ or y^2 divides $\Delta/(-16) = 4a^3 + 27b^2$.*

This theorem covers all curves $E/\mathbf{Q}$, since each such curve can be written in the reduced Weierstrass form $y^2 = x^3 + ax + b$ for rational a, b. This can be further rewritten by the rational change of variables $(x, y) \mapsto (r^{-2}x, r^{-3}y)$ to clear denominators, giving rational coefficients a, b.

The theorem allows us to determine all rational torsion points, since there are only finitely many choices for divisors of $\Delta/(-16)$. These finite divisors yield a finite number of possible y-coordinates, which in turn yields a finite set of possible rational torsion points. Thus starting with some $P \in E(\mathbf{Q})$ in this set of candidates, we take successive

multiples $[2]P, [3]P, \ldots$. If P is a torsion point, then we will eventually find some $[m]P = \mathcal{O}$. Otherwise, we will find some $[m]P$ that is outside the set of candidates.

The following theorem of Mazur tells us that the algorithm we just sketched will terminate in a fairly short time. This theorem is, in a word, "baller."

Theorem 1.3.9 (Mazur's Theorem)**.** *For an elliptic curve $E/\mathbf{Q}$, the group $E(\mathbf{Q})_{\text{tors}}$ is of one of the following:*

1. $\mathbf{Z}/n\mathbf{Z}$ *for* $1 \leq n \leq 10$ *or* $n = 12$*, or*

2. $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2n\mathbf{Z}$ *for* $1 \leq n \leq 4$.

Each of these groups occurs infinitely often. It can be further generalized according to a theorem of Merel to arbitrary number fields. We refer the reader to [11] for an introduction to this line of inquiry. Examples of curves with each possible torsion subgroup are given in [13, exer. 8.12].

The rank of an elliptic curve is a much more tricky subject. According to a long-standing folk conjecture, there is no bound on the possible ranks of an elliptic curve. However, it is difficult to find a curve of rank greater than 10, and indeed the largest known ranks are not significantly larger. As far as I can tell, the present record for the number of independent points of infinite order on a curve is held by Noam Elkies, who has found a curve of rank no less than 28 (given in [4]). It is not proven that the rank of this curve isn't larger than this, however.

In summary, generating sets for the Mordell-Weil group of an elliptic curve $E/\mathbf{Q}$ are surprisingly small. The torsion subgroup never requires more than two generators, and the ranks of most curves one will ever write down as an off-the-cuff example will not exceed 3. Unfortunately, the process of finding a generating set for a particular Mordell-Weil group requires some amount of machinery, which we will not have cause to build up here. However, this particular problem is as well-documented as it is well-studied, and

PARI/GP readily gives generators for a large host of indexed curves, as we will explore in Chapter 4.

2
Field Extensions

2.1 Foundations of Galois Theory

For a reader unfamiliar with Galois extensions, I'll provide a very basic (read: unhelpfully terse) exposition on the topic (a much better one can be found in [7] or [3, Ch. 14]). The sketchy picture (or at least the way I've been explaining it at cocktail parties) is simple: given a field K and a some numbers not in K, you throw the numbers into K and let it resolve back into a field (by continuing to throw in multiples, multiplicative inverses et al. until the field is closed under all the things fields are meant to be closed under again). The metaphor of throwing things into a field should not be mistaken for any sort of mathematical formalism, and although I'll reference it several times the reader should remember that it is only an intuitive description of what is going on.

Definition 2.1.1. Let K be a field and let L be a field containing K. We call L an *extension* of the base field K and denote this relation by L/K. We denote the group of field automorphisms of L which fix K pointwise by $\mathrm{Aut}(L/K)$. $\triangle$

We'd like to be able to construct field extensions completely algebraically, which we do by passing to the polynomial ring $K[x]$. Ideals in this ring are generated by a single

polynomial (meaning $K[x]$ is a principal ideal domain), and taking the quotient by such ideals yields a commutative ring. The maximal ideals of $K[x]$ are precisely those generated by a single irreducible polynomial, since the existence of an intermediate superideal of an ideal $M \subseteq M^+ \subseteq K[x]$ provides a divisor for the generating polynomial of M (since, again, $K[x]$ is a PID). The quotient by a maximal ideal is a field, and indeed it contains the base field K.

The "numbers" we intuitively referred to throwing into the field before are the roots of the irreducible polynomial $f(x)$ generating the maximal ideal $\langle f(x)\rangle = M$. When we quotient out by the ideal generated by $f(x)$, we are essentially declaring the polynomial $f(x)$ to be equal to zero for our purposes, since then the coset $x + \langle f(x)\rangle$ behaves like a root of $f(x)$.

Example 2.1.2. One of the most standard examples of a field extension is "throwing" the square root of 2 into the field of rational numbers. Consider the polynomial $f(x) = x^2 - 2$. The coefficients are clearly rational, but the roots aren't; they're $\pm\sqrt{2}$. We note that $f(x)$ is irreducible, since it cannot be written as a product of smaller-degree factors with rational coefficients. If we take the polynomial ring $\mathbf{Q}[x]$ and quotient out by the ideal $\langle f(x)\rangle$, we get a ring of polynomials in x, with the addition and multiplication carried out mod $x^2 - 2$. This makes x in the polynomial ring the square root of 2 we've thrown in. Thus we could identify $\mathbf{Q}[x]/\langle f(x)\rangle$ with $\mathbf{Q}(\sqrt{2})$, where the use of parentheses rather than square brackets indicates that we are adjoining both the square root of 2 and its multiplicative inverse so that the result is a field, and not just a ring. $\Diamond$

Every element in the field $\mathbf{Q}(\sqrt{2})$ is of the form $a + b\sqrt{2}$ for $a, b \in \mathbf{Q}$. This gives $\mathbf{Q}(\sqrt{2})$ the structure of a 2-dimensional $\mathbf{Q}$-vector space. This observation can be easily generalized.

Proposition 2.1.3. *Any field extension L/K generated in this way with $L \simeq K[x]/\langle f(x)\rangle$ is a d-dimensional K-vector space, where $d = \deg(f(x))$.*

It is not difficult to show that any extension L/K has a vector space structure over the base field K.

Definition 2.1.4. We call the dimension of the field L/K as a K-vector space the *index* of the extension L/K, and we write it as $[L\colon K]$. When the index is finite we say the extension L/K is finite. △

By proposition 2.1.3, all the extensions that we've constructed are finite, with their vector space structure easily describable in terms of polynomials. One basis for this vector space (apologetically continuing to use the coset notation of $K[x]/\langle f(x)\rangle$) is $\{x^i + \langle f(x)\rangle\}_{0\leq i<[L\colon K]}$. We note that $x^{[L\colon K]} \equiv x^{[L\colon K]} - f(x) \mod f(x)$, which can be written entirely in terms of our basis since an irreducible $f(x)$ is monic.

In number theory, we are interested in exploring the properties of the field $\mathbf{Q}$. The following class of fields is correspondingly of particular interest.

Definition 2.1.5. A field K is called a *number field* if it is a finite extension of $\mathbf{Q}$. △

Another important class of extensions is Galois extensions, which provide a foundation for the study of field extensions in general.

Definition 2.1.6. We say that an extension L/K is *Galois* if $|\mathrm{Aut}(L/K)| = [L\colon K]$. If so, we call $\mathrm{Aut}(L/K)$ the *Galois group* of L/K, and use the alternate notation $\mathrm{Gal}(L/K)$ for it. △

We consider now the automorphism group of the extension given in Example 2.1.2. Which field automorphisms of $\mathbf{Q}(\sqrt{2})$ fix the base field $\mathbf{Q}$ of rational numbers?

Well, for any extension L/K any field automorphism $\sigma\colon L \longrightarrow L$ acting trivially on K must satisfy

$$\sigma(a\alpha) = \sigma(a)\sigma(\alpha) = a\sigma(\alpha), \text{ and } \quad \sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta)$$

for any $a \in K$ and any $\alpha, \beta \in L$, since any such σ must be a field homomorphism. Clearly σ is determined entirely by how it acts on $L - K$, and further by how it acts on just those roots of the defining polynomial for L, since L consists only of K-linear combinations of these roots. Thus we know that the degree of an extension, or rather the degree of the defining polynomial of an extension, places an upper bound on the automorphism group. Said again, $\mathrm{Gal}(L/K) \leq S_d$, the symmetric group, where d is the degree. For our example $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$, this tells us that the automorphism group must be either S_2 or trivial, since there are only 2 roots of $x^2 - 2$. As it turns out, the automorphism group is S_2, since we can define the order-2 automorphism sending $\sqrt{2} \mapsto -\sqrt{2}$, which by the homomorphism property must also entail sending $-\sqrt{2} \mapsto \sqrt{2}$.

By Definition 2.1.6, we can see clearly that $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ is a Galois extension. While this particular definition is technically correct, Galois extensions can be characterized in a more intuitively useful way.

Theorem 2.1.7. *The extension L/K is Galois if and only if L is the splitting field of some polynomial without repeated roots over K, i.e. L is the smallest field over which such a polynomial splits into linear factors.*

The benefit of thinking about Galois extensions in this way is that it is much more computationally direct, since polynomials are relatively easy to work with. It also shows us a natural way in which every finite extension constructed by our method of taking quotients of polynomial rings can be embedded into a Galois extension: if $L \simeq K[x]/\langle f(x) \rangle$, then the splitting field of $f(x)$ (which we can assume without loss of generality has no repeated roots) contains L and is Galois.

Returning to our example, we needn't stop with the square root of 2. We can continue to throw things into the field $\mathbf{Q}(\sqrt{2})$, perhaps carrying out another extension by a quadratic polynomial, say $g(x) = x^2 - 3$. We note that this polynomial is still irreducible over the

extended field $\mathbf{Q}(\sqrt{2})$, so it does yield an honest-to-goodness field extension $\mathbf{Q}(\sqrt{2},\sqrt{3})$. We'll also discuss its relationship to the extension $\mathbf{Q}(\sqrt{3})/\mathbf{Q}$. The extension in question is

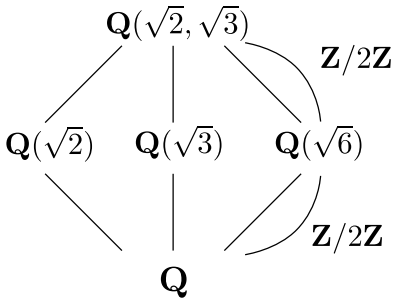

Figure 2.1.1. A field diagram showing the subfields of the biquadratic extension $\mathbf{Q}(\sqrt{2},\sqrt{3})$.

termed *biquadratic*, because it is the composition of two independent quadratic extensions. In general, any two non-square rationals d_1, d_2 whose product isn't a square will yield a biquadratic extension in the same way. The extension $\mathbf{Q}(\sqrt{d_1},\sqrt{d_2})$ has the Klein 4-group V_4 as its Galois group, with each of the three subgroups $S_2 \leq V_4$ acting trivially on one quadratic subextension: $\mathbf{Q}(\sqrt{d_1})/\mathbf{Q}, \mathbf{Q}(\sqrt{d_2})/\mathbf{Q}$, or $\mathbf{Q}(\sqrt{d_1 d_2})/\mathbf{Q}$. The correspondence between the subfields of the extension to subgroups of the Galois group is made precise by the Fundamental Theorem of Galois Theory.

Theorem 2.1.8 (Fundamental Theorem of Galois Theory)**.** *Let L/K be a Galois extension, and set $G = \mathrm{Gal}(L/K)$. Then there exists a bijective correspondence of subfields E/K of L/K and subgroups of $H \leq G$, which assigns to each H the field it fixes point-wise. Furthermore, $\mathrm{Gal}(L/E) = H$, and if $H \triangleleft G$ then $\mathrm{Gal}(E/K) = G/H$.*

We refer the reader to [3, §14.2] for a proof (and a less condensed statement) of this theorem. Before illustrating the theorem, however, we first provide an example of a non-Galois extension.

Again, we can continue. We can use additional polynomials to extend our field indefinitely. If I "take the limit" of these increasingly extended fields, I am left with an infinite extension of the base field. A particularly natural example of an infinite extension is the

$$\begin{array}{ccccc} L & & \mathrm{Gal}(L/L) & \simeq & 1 \\ | & & | & & | \\ E & \leftrightarrow & \mathrm{Gal}(L/E) & \simeq & H \\ | & & | & & | \\ K & & \mathrm{Gal}(L/K) & \simeq & G \end{array}$$

Figure 2.1.2. The correspondence in the Fundamental Theorem of Galois theory.

algebraic closure of a field K, written $\bar{K}$, which is the set of all numbers that are algebraic over K, i.e. numbers for which there exists a single-variable polynomial over K with that number as a root. The algebraic closure will be referenced often throughout the project, as it is a convenient way to package statements about automorphisms in any Galois group.

2.2 Examples

In this section we will address several additional examples of field extensions to help the reader build up some intuition about Galois theory. In particular, an example of a non-Galois extension is has been conspicuously missing from our exposition so far.

Example 2.2.1. The extension achieved by adjoining the real fourth root of 2 to $\mathbf{Q}$, written $\mathbf{Q}(\sqrt[4]{2})$, is not a Galois extension. To see this, notice that any $\sigma \in \mathrm{Aut}(\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q})$ must send $\sqrt[4]{2}$ to another root of the polynomial $x^4 - 2$. Considering this polynomial over $\mathbf{C}$, we can get an idea of what these roots look like. There are two real 4th roots of 2, and two imaginary roots. The extension $\mathbf{Q}[x]/\langle x^4 - 2\rangle$ contains only two of these, however, since if we embed the extension into $\mathbf{C}$ by sending $x + \langle x^4 - 2\rangle$ to a root r then $\mathbf{Q}$-linear combinations of r, $r^2 (= \pm\sqrt{2})$, and r^3 can only give us $-r$, and not $\pm ir$. Because any automorphism of $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q})$ is fully determined by how it permutes the roots of $x^4 - 2$, we note that there is only one non-trivial automorphism, the one switching r and $-r$, since

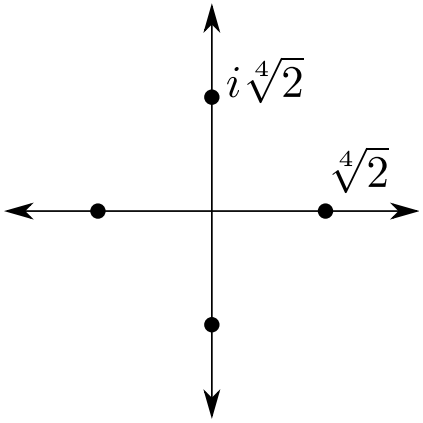

Figure 2.2.1. The fourth roots of 2 in the complex plane.

$\pm ir$ aren't in the field. Thus $\mathrm{Aut}(\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}) \simeq S_2$, so we see that $|\mathrm{Aut}(\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q})| < [\mathbf{Q}(\sqrt[4]{2}) : \mathbf{Q}]$. Thus the extension is not Galois. $\Diamond$

Making this argument, we could also note that the field is not the splitting field for its defining polynomial, since it did not contain all of its roots. If we take the splitting field of $x^4 - 2$, we must also include a primitive 4th root of unity, so that we can have all four roots simultaneously. This allows us to describe automorphisms of the extension which permute the roots of $x^4 - 2$ transitively. This reflects a general property of Galois extensions viewed as splitting fields, namely that the Galois group of the splitting field of an irreducible polynomial (like $x^4 - 2$) acts transitively on the roots of that polynomial. Further, the Galois group of the splitting field of any polynomial is a product of groups that act transitively on the irreducible factors of that polynomial. This is a useful perspective to take for small extensions, when there are not too many transitive subgroups of the symmetric groups on the roots of polynomials of small degree.

In the previous section we gave an example of a quadratic extension of $\mathbf{Q}$, and passingly mentioned that $\mathbf{Q}(\sqrt{d})$ behaves similarly for any non-square rational d. Intuitively, this should be the only kind of non-trivial Galois extension we can get out of a quadratic

extension. We show this by considering the different possibilities for the discriminant of quadratic polynomials.

Definition 2.2.2. Let $f(x)$ be a polynomial with coefficients in some field K, and factor it over $\bar{K}$ as $f(x) = \prod_i (x - \alpha_i)$. The *discriminant* of $f(x)$ is

$$D = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

This is well-defined, since permuting indices negates some number of factors $(\alpha_i - \alpha_j)$, which is squared out in the final result. △

Example 2.2.3. Let $f(x) = x^2 + ax + b$ be an arbitrary quadratic polynomial with rational coefficients. We will compute the Galois group of the splitting field of $f(x)$. The extension is that given by adjoining the square root of the discriminant $a^2 - 4b$ of $f(x)$ (explanation for this requires no more than recalling the quadratic formula from middle school algebra). Thus the Galois group of the splitting field is S_2 if and only if the discriminant is not a rational square; otherwise we get a trivial extension. ♢

Things get a bit more interesting when we apply the same strategy to cubic rational polynomials. The case of a reducible cubic is easy, since it must factor into three linear factors (which does not define an extension at all) or into one linear and one quadratic irreducible factor (the group of which we have already considered). For irreducibles, we again need to reference the discriminant.

Example 2.2.4. Let $g(x) = x^3 + ax^2 + bx + c$ be an arbitrary irreducible cubic polynomial over $\mathbf{Q}$. The Galois group must be a transitive subgroup of S_3, of which there are two: S_3 itself and $A_3 \simeq \mathbf{Z}/3\mathbf{Z}$. Which one occurs for a particular cubic is determined by the discriminant of the cubic, which we note for the reader's convenience is computed much more easily after a simple change of coordinates. Letting $y = x + a/3$ yields an altered polynomial of the form $g(y) = y^3 + a'y + b'$ for rational a' and b'. Geometrically, this

amounts to shifting the polynomial over by a rational number, which doesn't change anything for the purposes of automorphisms of the splitting field. It also allows us to write the discriminant as

$$D = -4a'^3 - 27b'^2,$$

which bears a striking resemblance to Equation 1.1.1 (see [3, §14.6] for more details on this expression of the discriminant). We know from the definition that the discriminant is in the splitting field of $g(y)$, and further that its square root is as well since it can be written as $(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$, a combination of the roots of $g(y)$. A permutation of the roots of $g(y)$ will negate this expression if and only if that permutation is odd. It follows that the Galois group of the splitting field contains an odd permutation (and is therefore all of S_3) if and only if the discriminant is not the square of a rational number. $\Diamond$

We could proceed to quartic polynomials, but we will instead refer the reader (again) to [3, §14.6], and trust that we have given sufficiently many examples for a basic introduction.

3
Field Extensions from Elliptic Curves

3.1 Torsion Point Extensions

In this chapter we explore Galois extensions achieved by adjoining to a number field K the preimages of a point P under multiplication maps $[m]$. The case when $P = \mathcal{O}$ is well-studied ([1]), and these extensions are the subject of this section. In later sections we will address the main topic of this project, which is the case when P is a rational point of infinite order.

The map $[m]\colon E \longrightarrow E$ is a particularly simple example of an isogeny on an elliptic curve.

Definition 3.1.1. A map $\phi\colon E_1 \longrightarrow E_2$ between elliptic curves is called an *isogeny* if it is a morphism fixing the identity. △

Morphism is also a term requiring definition, for which we refer the reader to [13, §I.3]. In short, a morphism is a mapping on projective varieties described by rational maps on the coordinates of points (although there are some subtleties I am not getting into). These maps may only be "rational" over relatively inconvenient fields, however. We will usually restrict our view of morphisms and isogenies to those which are defined over

the field of definition K for our elliptic curve. The main reason we do this is because such isogenies behave well with respect to Galois actions of $\mathrm{Gal}(\bar{K}/K)$. Note that we have already given K-rational mappings describing the multiplication maps $[m]$ in writing down Equation 1.2.5 using division polynomials.

There are a few important details about isogenies which bear mentioning before we move on to other things (although they do not have much bearing on the tasks at hand).

Proposition 3.1.2. *Let $\phi\colon E_1 \longrightarrow E_2$ be an isogeny. Then ϕ is a group homomorphism. That is, for all $P, Q \in E(\bar{K})$,*

$$\phi(P +_{E_1} Q) = \phi(P) +_{E_2} \phi(Q),$$

where the addition on the left-hand side is the addition of the curve E_1 and on the right that of the curve E_2. Additionally, $\phi$is either trivial or has finite kernel.

These facts can be found in [13, §III.4]. This discussion is rather unenlightening for $[m]$, which we knew to be a group homomorphism before we wrote out rational maps for it, since elliptic curves are abelian groups. We can also easily read off the fact that the kernel of $[m]$ is finite from the rational mappings we've given for it; the degree of polynomial in the numerator of Equation 1.2.5. The argument for general isogenies is similar.

Now that we have spent some time discussing general isogenies, we use $[m]$ to exemplify the nice behavior of the Galois action with respect to K-rational isogenies.

Lemma 3.1.3. *The action of the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ on the coordinates of a point commutes with addition of points on an elliptic curve. That is, for points $P, Q \in E$ and an automorpism $\sigma \in \mathrm{Gal}(\bar{K}/K)$,*

$$\sigma(P+Q) = \sigma(P) + \sigma(Q), \text{ and so } \sigma([m]P) = \sigma(\underbrace{P + P + \ldots + P}_{m \text{ summands}}) = [m]\sigma(P).$$

To see this, note that any element of the absolute Galois group $\sigma \in \mathrm{Gal}(\bar{K}/K)$ fixes all the coefficients of these polynomials, and σ distributes over field operations since it is a

field homomorphism, we see that $\sigma(f(x,y)) = f(\sigma(x),\sigma(y))$ for any rational map f. As we have seen, addition on the elliptic curve is also rational on the coordinates of the points involved, so it is clear that the Galois action commutes. It is also clear that the same will hold for any K-rational isogeny, since they are described by such rational maps.

Define the set of m-torsion points by $E[m] = \ker([m]) = \{P \in E \mid [m]P = \mathcal{O}\}$. We notice that because $\mathcal{O}$ is K-rational (its projective coordinates are K-rational), that the Galois action fixes the set of m-torsion points.

Corollary 3.1.4. *For an elliptic curve E defined over K with a point $P \in E(K)$ and an automorphism $\sigma \in \mathrm{Gal}(\bar{K}/K)$, we have the equality of sets $\sigma([m]^{-1}P) = [m]^{-1}P$ for any $m \in \mathbf{N}$. In particular, $\sigma(E[m]) = E[m]$.*

Proof. Let Q be an m-th root of P on E for some m. Then $[m]Q = P = \sigma(P) = \sigma([m]Q) = [m]\sigma(Q)$, where $P = \sigma(P)$ is due to the K-rationality of P. Thus $\sigma(Q)$ must also be an mth root of P. The opposite inclusion is clear by the injectivity of σ. □

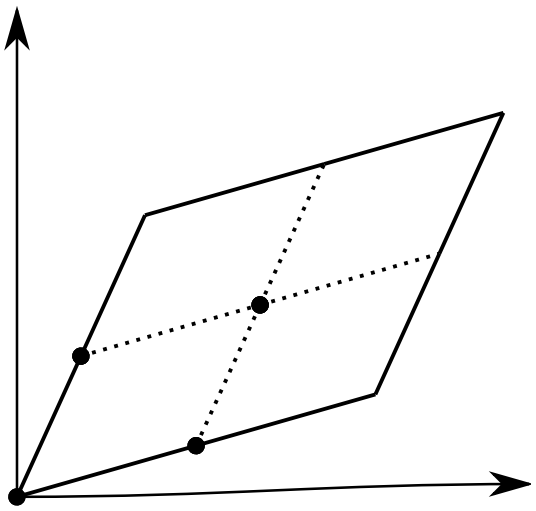

Figure 3.1.1. The points of order 2 on $\mathbf{C}$ modulo a lattice Λ. The group $E[2]$ clearly has the structure $(\mathbf{Z}/2\mathbf{Z})^2$.

It turns out that, as a group, $E[m] \simeq \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$, assuming m is relatively prime to the characteristic of the field of definition for E (see [13, III.6.4]). Recalling the construction given in Section 1.1 of an elliptic curve over $\mathbf{C}$, this makes a lot of sense (see Figure 3.1.1). Additionally, recalling that addition on E is also merely a rational mapping, each $\sigma \in \mathrm{Gal}(\bar{K}/K)$ induces a group homomorphism of E, as we saw in Corollary 3.1.4. Thus we naturally define the *Galois representation*

$$\rho_m \colon \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Aut}(E[m]) \simeq \mathrm{Aut}(\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}) \tag{3.1.1}$$

by taking σ to the automorphism it induces. This is then a 2-dimensional representation over a $\mathbf{Z}/m\mathbf{Z}$-module, and, when m is prime, over a finite field. (To refer to ρ_m as a representation in the case of composite m is abuse of terminology, since generally the term representation is reserved for transformations of a vector space, which $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ is not. I hope the reader will not hold this against me.) The kernel of this representation has as its fixed field the mth *torsion point field* $K(E[m])$ (which is just the coordinates of the points in $E[m]$ adjoined to K), which shows us that $K(E[m])/K$ is a Galois extension. Because each $\sigma \in \mathrm{Gal}(K(E[m])/K)$ is completely determined by its restriction to $E[m]$, we know that the restricted representation

$$\overline{\rho}_m \colon \mathrm{Gal}(K(E[m])/K) \longrightarrow \mathrm{Aut}(E[m]) \tag{3.1.2}$$

is faithful. Thus $\mathrm{Gal}(K(E[\ell])/K) \leq \mathrm{GL}_2(\mathbf{F}_\ell)$ for any prime ℓ, where $\mathbf{F}_\ell$ denotes the finite field of order ℓ.

In the general case, the representation $\overline{\rho}_\ell$ for prime ℓ surjects onto $\mathrm{GL}_2(\mathbf{F}_\ell)$ (see [1, Prop. 3.5.1-3]). In this case, the subfields of $K(E[\ell])$ can be read off by listing the subgroups of $\mathrm{GL}_2(\mathbf{F}_\ell)$, according to the Fundamental Theorem of Galois Theory (2.1.8).

One of the main goals of this project is to obtain a result similar to this one, but generalizing $E[m]$ to preimages of points $P \in E$ not the identity on E. We will denote this preimage $E^P[m] = \{Q \in E \mid [m]Q = P\}$. This question is taken up in section 3.3.

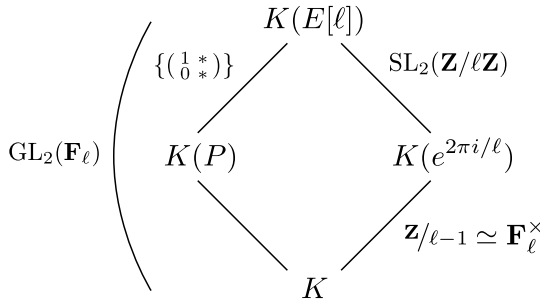

Figure 3.1.2. Examples of subfields of the torsion-point field, assuming ρ_ℓ is surjective. Here P is a single ℓ-torsion point. For more details (and more subfields), see [1, §5.2].

3.2 An Adapted Lemma

We adapt a helpful lemma found in [10], which simplifies the process of calculating the extensions $K(E^P[m])/K$. The lemma is stated for general isogenies, and so holds in particular for each $[m]$. Let K be a field with $\mathrm{char}(K) \neq 2$ and let E be an elliptic curve defined over K. Then there is a Weierstrass equation of the form $y^2 = f(x)$ where f is a cubic polynomial [13, §III.1]. In particular, as in Section 1.2, it is clear that $-(x, y) = (x, -y)$ for any point (x, y) on the elliptic curve.

Lemma 3.2.1 (Reynolds)**.** *Let $P \in E(K)$ be a non-torsion K-rational point on E. Let E'/K be an elliptic curve and suppose there exists a K-rational isogeny $\phi\colon E' \longrightarrow E$ with $\phi(R) = P$. Then $K(x(R), y(R)) = K(x(R))$.*

Based on the fact that there can only ever be finitely many rational torsion points on a given elliptic curve (according to the Mordell-Weil theorem), this simplifies the extensions we hope to investigate for large swaths of the cases at hand. However, in the course of proving the lemma we will see that our conditions on P can be relaxed to still yield the same result.

Proof of 3.2.1. Let $L = K(x(R))$ and $L' = K(x(R), y(R))$. We note that because the coordinates of R satisfy the Weierstrass equation for E' of the form $y^2 = f(x)$ for some

cubic f, L' can be at most a quadratic extension of L. Suppose it is. Take a non-trivial $\sigma \in \mathrm{Gal}(L'/L)$. Because σ fixes the x-coordinates of R, we note that $\sigma(R) = \pm R$ (since the only two points on an elliptic curve written in the above Weierstrass of the same x-coordinate are a point and its negative). But for σ to be non-trivial, it must take $\sigma(R) = -R$. Because K-rational isogenies commute with Galois automorphisms and isogenies are group homomorphisms, this yields

$$P = \sigma(P) = \sigma(\phi(R)) = \phi(\sigma(R)) = \phi(-R) = -\phi(R) = -P,$$

i.e. $[2]P = \mathcal{O}$. This contradicts the fact that P is non-torsion. □

As the reader might've noticed, the contradiction reached only required that $[2]P \neq \mathcal{O}$. This is a much nicer condition, given that we can now extend the result to all points on curves without 2-torsion, of which there are many. Additionally, it is very easy to find all torsion points on a given curve, using both the Nagell-Lutz theorem and Mazur's theorem, so we can very easily avoid these cases.

In the ℓ-torsion case, when $P = \mathcal{O}$ is its own inverse, we have $[K(E[\ell])\colon K(x(E[\ell]))] \leq 2$, and indeed the Galois group of this extension is $\{\pm 1\}$ when the Galois representation $\overline{\rho}_\ell$ is surjective. See [1, §5.2].

In the case where we are taking the preimage of a point of order greater than 2, this Lemma allows us to ignore the distinction between adjoining both coordinates of a point and only adjoining the x-coordinate of that point to a field K. In the sequel we may also ignore this distinction notationally as well, writing $K(P)$ for $K(x(P))$ and so forth.

3.3 The Structure of $E^P[\ell]$

Take a rational point P of infinite order on a curve E. The preimage of this point under a multiplication map $[m]$ we have already introduced, denoted by $E^P[m]$. We have already noted that the absolute Galois group permutes this set, by Lemma 3.1.4. Thus we can

define another Galois representation

$$\rho_{m,P}\colon \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Aut}(E^P[m]) \tag{3.3.1}$$

in a manner analogous to the m-torsion representations. Writing $\mathrm{Aut}(E^P[m])$ is extremely abusive of me, since we have not explicitly described the algebraic structure of $E^P[m]$. For the time being, we can think of $\mathrm{Aut}(E^P[m])$ as merely permutations of the set. To obtain a linear-algebraic description of $\mathrm{Aut}(E^P[m])$ like the one we had in the m-torsion case, we'll need to describe $E^P[m]$ algebraically.

Lemma 3.3.1. *For a point $P \in E/K$ of infinite order and a fixed preimage $Q \in E$ satisfying $[m]Q = P$ for some $m \in \mathbf{N}$, we have*

$$E^P[m] = Q + E[m]$$

Proof. This follows directly from the fact that $[m]$ is a group homomorphism. Note $[m](Q+M) = [m]Q+[m]M = P+\mathcal{O} = P$ for any $M \in E[m]$, so we have $Q+E[m] \subseteq E^P[m]$ straightaway. Furthermore, the difference between any two preimages Q, Q' must be in $E[m]$, since $[m](Q - Q') = [m]Q - [m]Q' = P - P = \mathcal{O}$. Thus $E^P[m] \subseteq Q + E[m]$. □

Moving forward to Galois theory, we find it helpful to take note:

Lemma 3.3.2. *If an extension K' of a field K contains the coordinates of points P, Q on an elliptic curve E/K, then the extension achieved by adjoining the sum of P and Q is contained in K'. In symbols, $K(P \pm Q) \subseteq K'$. Correspondingly, $K([m]P) \subseteq K'$.*

This is a result of the fact that addition on an elliptic curve is a rational mapping on the coordinates of the points being added together, similarly to Lemma 3.1.3. Rational mappings are specified only by operations that fields are necessarily closed under (e.g. addition, division), so anything that can be reached by applying a rational mapping to coordinates of points contained in a field must also be contained in that field.

Corollary 3.3.3. *The field $K(E^P[m])$ contains all differences of points in $E^P[m]$, so we have*

$$K(E^P[m]) \supseteq K(E[m]).$$

Another obvious corollary is that if any preimage Q of P is K-rational, then the image $\rho_{m,P}(\mathrm{Gal}(\bar{K}/K)) \simeq \mathrm{Gal}(K(E^P[m])/K) = \mathrm{Gal}(K(E[m])/K) \simeq \rho_m(\mathrm{Gal}(\bar{K}/K))$ is the same as the image from the m-torsion case (we will see a specific example of this special case later). This observation is a big step towards a complete characterization of the images $\mathrm{im}(\rho_{m,P})$ as P is allowed to vary along a free part of the Mordell-Weil group.

If a rational point P has infinite order, then its multiples $[m]P$ also clearly have infinite order. The multiples must also be rational points, since multiplication on the elliptic curve is a rational mapping (as described by division polynomials).

Lemma 3.3.4. *For a prime ℓ and an integer m, we have*

$$K(E^P[\ell]) \supseteq K(E^{[m]P}[\ell]).$$

Proof. Note that for a preimage $Q \in E^P[m]$, we know that $[m]Q \in E^{[m]P}[\ell]$ since $[\ell][m]Q = [m]([\ell]Q) = [m]P$. But then $K([m]Q) \in K(E^P[\ell])$ by Lemma 3.3.2. Since we already have $K(E[\ell]) \subseteq K(E^{[m]P}[\ell])$ by Corollary 3.3.3, we have all coordinates of points in $E^{[m]P}[\ell]$. □

None of our results thus far strictly requires that P be of infinite order. It is a much more illustrative case for us to consider, however. If $[m]P = \mathcal{O}$ for some m, it is easy to see that $K(E^{[m]P}[\ell]) = K(E[\ell])$, and further $K(E^{[n]P}[\ell]) = K(E^{[n+m]P}[\ell])$ for any n. This periodic behavior can be very easily explained just using finite group theory. However, we will show a similar periodic behavior occurs with points P of infinite order. Starting with a torsion point can only serve to make the sequence of fields $K(E^{[m]P}[\ell])$ simpler, so it will suffice to consider only points P of infinite order.

Given a minimal generating set S for the Mordell-Weil group of a curve, Lemma 3.3.4 makes the generators $P \in S$ of infinite order particularly natural choices of points with which to start, since they yield the "largest" fields. This makes sense, since taking such generators is also a surefire way to ensure that no ℓth root of P is rational. We will consider P to be such a generator for the remainder of this chapter.

Theorem 3.3.5. *Given a generator P of infinite order on an elliptic curve E/K and a prime ℓ, we have $K(E^P[\ell]) = K(E^{[m]P}[\ell])$ whenever $m \not\equiv 0 \mod \ell$. When $\ell \mid m$ we have $K(E^{[m]P}[\ell]) = K(E[\ell])$.*

Proof. If $\ell \nmid m$, then there is some integer m' such that $m \times m' \equiv 1 \mod \ell$, by basic group theory. Let Q be some ℓth root of P, so that $[\ell]Q = P$. Then we have the coordinates of $[m]Q$ in $K(E^{[m]P}[\ell])$, so by Lemma 3.3.2 the coordinates of $[m \times m']Q$ are also in there. But $[m \times m']Q = Q + [m \times m' - 1]Q = Q + [s]P$ for some integer s. But because the rational point $[s]P$ is in $K(E^{[m]P}[\ell])$, we have the coordinates of Q in there also, by another application of Lemma 3.3.2. Thus we have the inclusion $K(E^P[\ell]) \subseteq K(E^{[m]P}[\ell])$.

The case where $m \equiv 0 \mod \ell$ was discussed earlier; if $\ell \mid m$ then $E^{[m]P}[\ell] = [\frac{m}{\ell}]P + E[\ell]$. Because $[\frac{m}{\ell}]P$ is a rational point, the extension $K(E^{[m]P}[\ell])$ of K is achieved by adjoining just $E[\ell]$. □

This reduces the problem of non-torsion points significantly. A description of the extensions resulting from a set of independent generators for the free part of the Mordell-Weil group tells us about a large number of extensions. We now set about characterizing this structure. As noted at the beginning of this section, the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ fixes $E^P[m]$ as a set for any rational point P and any integer m. Because all elements of $E^P[m]$ are of the form $Q + M$ where $M \in E[m]$ and Q is some fixed mth root of P, the action of an automorphism $\sigma \in \mathrm{Gal}(K(E^P[m])/K)$ on $E^P[m]$ is determined entirely by

its restriction to $\mathrm{Gal}(K(E[m])/K)$ and by $\sigma(Q)$. These observations allow us to describe the Galois group explicitly.

Theorem 3.3.6. *Given a generator P (as in Theorem 3.3.5) and a prime ℓ, we can embed $\mathrm{Gal}(K(E^P[\ell])/K)$ into $E[\ell] \rtimes \mathrm{Aut}(E[\ell])$, where the semidirect product is defined by the natural action of the latter factor $\mathrm{Aut}(E[\ell])$ on the former $E[\ell]$.*

Proof. Fix a point Q satisfying $[\ell]Q = P$. The action of an automorphism $\sigma \in \mathrm{Gal}(K(E^P[\ell])/K)$ on Q must be to map it to some $Q + M$ for $M \in E[\ell]$ by Lemma 3.1.4. The restriction homomorphism $\sigma \mapsto \sigma\,|_{K(E[\ell])}$ (which carries the same information as $\rho_\ell(\sigma)$) determines everything except for the action on Q, which must be to $Q + M$ for some $M \in E[\ell]$. We define the embedding $\phi\colon \mathrm{Gal}(K(E^P[\ell])) \longrightarrow E[\ell] \rtimes \mathrm{Aut}(E[\ell])$ by $\phi(\sigma) = (\sigma(Q) - Q, \rho_\ell(\sigma))$. □

Only now are we ready to make clear why we called $\rho_{m,P}\colon \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Aut}(E^P[m])$ a Galois *representation*, putting the permutations of the set $E^P[m]$ in a linear algebraic setting. For a prime ℓ, elements of the group $E[\ell] \rtimes \mathrm{Aut}(E^P[\ell])$ can be described as linear transformations of a vector space of dimension 4 over $\mathbf{F}_\ell$. We will describe these transformations as matrices in the interest of showing how the multiplication in the semidirect product works explicitly.

Let $\sigma \in \mathrm{Gal}(\bar{K}/K)$, and choose two points $M_1, M_2 \in E[\ell]$ that generate the entire group. The two chosen points will provide us with a basis for $E[\ell]$ as a vector space, with respect to which we write $\rho_\ell(\sigma)$ as a 2×2 matrix Γ_σ. Fix a preimage Q of P (so that $[\ell]Q = P$), and decompose $\sigma(Q) - Q = [n_1]M_1 + [n_2]M_2$ with respect to our basis. Then the block matrix corresponding to $\rho_{\ell,P}(\sigma)$ is

$$\begin{pmatrix} \Gamma_\sigma & M_\sigma \\ 0 & I \end{pmatrix}, \tag{3.3.2}$$

where M_σ is the diagonal matrix $\left(\begin{smallmatrix} n_1 & 0 \\ 0 & n_2 \end{smallmatrix}\right)$, and both the zero and identity matrices are 2×2. These matrices mutiply exactly as elements of the semidirect product do. For two automorphisms $\sigma, \tau \in \mathrm{Gal}(\bar{K}/K)$, we have

$$\begin{pmatrix} \Gamma_\sigma & M_\sigma \\ 0 & I \end{pmatrix} \begin{pmatrix} \Gamma_\tau & M_\tau \\ 0 & I \end{pmatrix} = \begin{pmatrix} \Gamma_\sigma\Gamma_\tau & \Gamma_\sigma M_\tau + M_\sigma \\ 0 & I \end{pmatrix}. \tag{3.3.3}$$

These matrices act on elements of $E^P[\ell]$ as 4-dimensional vectors. Write each $Q + [n_1]M_1 + [n_2]M_2 \in E^P[\ell]$ as $(\,n_1\ n_2\ 1\ 1\,)^\top$. Note that only the first two entries in these vectors carry any information. This is because we have embedded affine transformations of the 2-dimensional $E[\ell]$ into the linear transformations of a larger space, a standard construction in linear algebra.

3.4 Independent Points of Infinite Order

In the previous section we classified the behavior of the extensions given multiples of generators of infinite order P of the Mordell-Weil group for a curve E/K defined over a number field. But this leaves a significant question unsolved. What if the rank of the elliptic curve is greater than 1, such that there are at least 2 independent points of infinite order?

Given two independent rational points of infinite order P, Q on E/K, what can be said about the extension of K given by adjoining the preimages of both P and Q under a particular $[\ell]$? Denote the extension given by a set S of independent points of $E(K)$ by $K(E^S[\ell])$, and, just for convenience, write $K(E^{P,Q}[\ell])$ when $S = \{P, Q\}$. Then $K(E^{P,Q}[\ell])$ obviously contains both $K(E^P[\ell])$ and $K(E^Q[\ell])$ as subfields.

We know that $K(E^{P,Q}[\ell])/K$ is a Galois extension, since it is the compositum of two Galois extensions. Let's make this argument precise.

Definition 3.4.1. Let K_1 and K_2 be subfields of a field K. We call the smallest subfield of K containing both K_1 and K_2 the *compositum* of these two, and denote it by K_1K_2.

Further, the compositum of a set of subfields of K is the smallest subfield K containing every field in the set. $\triangle$

Clearly $K(E^{P,Q}[\ell]) = K(E^P[\ell])K(E^Q[\ell])$ is an example. It is not difficult to show that the compositum of two splitting fields for separable polynomials $f(x), g(x)$ will be the splitting field for the squarefree version of the product $f(x)g(x)$. By Theorem 2.1.7, this shows us that the compositum of Galois extensions is Galois. But we can say more:

Proposition 3.4.2. *For Galois extensions K_1, K_2 over the same field K, the galois group of the compositum K_1K_2/K is*

$$H = \{(\sigma, \tau) \mid \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\}.$$

Consequently, if $K_1 \cap K_2 = K$, then $\mathrm{Gal}(K_1K_2/K) \simeq \mathrm{Gal}(K_1/K) \times \mathrm{Gal}(K_2/K)$.

We have already seen this principle in action in Chapter 2, when we discussed adjoining the square roots of 2 and 3 to the rational numbers. The biquadratic extension $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is the compositum of the two quadratic extensions $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{3})$. The resulting Galois group is the direct product of the Galois groups of the composed extensions.

Intuitively, independent points of infinite order P and Q should yield independent extensions in exactly the same manner, i.e. $\mathrm{Gal}(K(E^{P,Q}[\ell])/K(E[\ell])) \simeq \mathrm{Gal}(K(E^P[\ell])/K(E[\ell])) \times \mathrm{Gal}(K(E^Q[\ell])/K(E[\ell]))$.

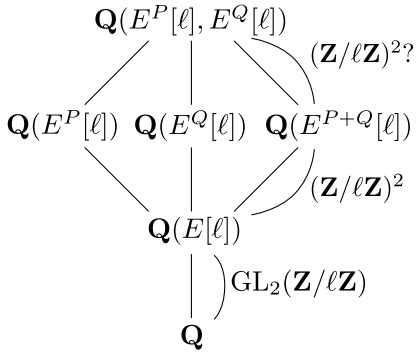

Figure 3.4.1. A diagram of inclusions of fields, similar to a biquadratic extension.

Conjecture 3.4.3. *Let E/K be an elliptic curve of rank greater than* 1. *Suppose P and Q are two points of infinite order in a set S of generators for the Mordell-Weil group $E(K)$. Then for any prime ℓ, we have $K(E^P[\ell]) \cap K(E^Q[\ell]) = K(E[\ell])$.*

By Proposition 3.4.2, this would suffice to show the isomorphism we just proposed. As extensions over the ℓ-torsion point field, $K(E^P[\ell])$ and $K(E^Q[\ell])$ are generated by adjoining the x-coordinate of any choice of preimage $P' \mapsto P$ and $Q' \mapsto Q$, respectively. (We only need the x-coordinate because of Lemma 3.2.1.)

In the case of the biquadratic extension we can see easily that the intersection of the two fields is as small as possible by arguing by contradiction. Suppose there is a non-trivial $\mathbf{Q}$-linear dependency between $\sqrt{2}$ and $\sqrt{3}$. In this dependency, isolate $\sqrt{2}$. Since $\sqrt{2}$ is not a rational multiple of $\sqrt{3}$, squaring will show that $\sqrt{3}$ is rational, a contradiction.

It is not difficult to see that this is not the right way to think about the extensions $K(E^P[\ell])$ and $K(E^Q[\ell])$. It is much more difficult to describe how the multiplication map $[\ell]$ behaves with respect to field addition than to describe how squaring did.

4
Computing with PARI

4.1 Basic Functions for Elliptic Curves

In this chapter we hope to give some sense of the computational methods used to develop this project, as well as to give some examples. The main computational tool used in the project is the computer algebra system PARI/GP (henceforth just PARI), a system useful for doing number theoretic calculations. There is a large library of information about elliptic curves that can be accessed through PARI, in particular about the ranks of these curves.

Our approach throughout this chapter is decidedly more elementary than that of previous ones.

Recall from Section 1.1 that an elliptic curve E defined over a field K is specified by a non-singular Weierstrass equation of the form

$$E\colon\ y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

with $a_1, \ldots, a_6 \in K$. PARI uses this as the standard way of specifying an elliptic curve. Thus the code for initializing an elliptic curve object in PARI and assigning that object to the variable `e` is:

```
>e = ellinit([a1, a2, a3, a4, a6]);
```

with $a_1, \ldots, a_6$ being elements of some field. (The semicolon at the end of this line of input tells PARI not to print the result of this assignment.) PARI allows us to easily specify a curve using coefficients from finite fields, ℓ-adic fields or the real numbers, but we will only ever be using rational inputs since we are interested in curves defined over number fields. Curves defined over some other fields are fully supported in PARI, but working with such coefficients is inconvenient. For the remainder of this chapter we will assume our curves to be defined over the rationals.

In the code above, we store the ell object that the function `ellinit` returns in the variable `e` for later use. Ell objects contain a great deal of useful information about an elliptic curve which can be accessed by member functions. By way of example, we could ask for the discriminant of the curve `e` by typing `e.disc`.

Getting to things more related to the subject at hand, PARI also allows us to play with non-zero points P on the elliptic curve, which are represented by their affine x- and y-coordinates as `[x,y]`, whereas the identity $\mathcal{O}$ is represented by `[0]`. We can check whether a point is on the curve using the function `ellisoncurve(e,[x,y])`. We can find a few particularly interesting points on the curve `e` by typing

```
>elltors(e)
```

which gives information about the subgroup of rational torsion on `e` in a three-entry vector. The interpretation of the entries of this vector is more easily explained by example.

Example 4.1.1. We compute the torsion subgroup of the Mordell-Weil group $E(\mathbf{Q})$ of the curve $y^2 = x^3 - x$.

```
>e = ellinit([0,0,0,-1,0]);
>elltors(e)
%2 = [4, [2, 2], [[1, 0], [0, 0]]]
```

We note that because the Weierstrass equation for the curve factors completely over the rationals as $y^2 = x(x-1)(x+1)$, the curve has three rational points of order 2 lying on the x-axis, where the tangent line to the curve is vertical (one for each root). These points form a subgroup isomorphic to $(\mathbf{Z}/2\mathbf{Z})^2$, since adding any two points yields the third (the x-axis is L_1, and each point is its own reflection over the x-axis). We know from Mazur's Theorem (1.3.9) that there are only a few possibilities for the torsion subgroup containing a copy of $(\mathbf{Z}/2\mathbf{Z})^2$. PARI's vector output tells us that the subgroup we have found is the entire torsion subgroup, telling us in the first entry that the group is of order 4, in the third a generating set of points, and in the second the structure of the group as a product of cyclic groups (giving the order of each cyclic factor in each entry of a vector). ◊

We will return to this example later to verify that the torsion is in fact no larger than PARI reports, in case you distrust the programmer who wrote the `elltors` function. We assure the reader that such skepticism is misplaced.

The output of every computation printed to the screen in PARI is automatically stored in an indexed variable `%n` for some natural number n. You can refer to last output by typing `%`, without an index. The ability to reference the results of previous computations is extremely useful when we are using PARI as an over-powered calculator, which is essentially always for our purposes.

PARI can also tell us about the free part of the Mordell-Weil group of the curve. With a curve `e` initialized, we can type

```
>ellgenerators(e)
```

to receive a vector of generators for the free part of the Mordell-Weil group of `e`. This is useful information for us to have for this project, since these generators are the natural choice of point to study for $E^P[\ell]$. In the next example we make use of the standard indexing of curves by their conductor, which (loosely) is an algebraic invariant encoding

which primes a curve behaves poorly over. Curves are indexed by conductor in the famously exhaustive tables of J. E. Cremona [2], from whence we get most of our interesting examples of curves.

Example 4.1.2. The elliptic curve of smallest conductor having rank 2 is $y^2 + y = x^3 + x^2 - 2x$. We can find its two generators by typing

```
>e=ellinit([0,1,1,-2,0]);
>ellgenerators(e)
%2 = [[-1, 1], [0, 0]]
```

to find that the two points $(-1, 1)$ and $(0, 0)$ are independent points of infinite order. We can add these two points and verify that the result is also of infinite order by

```
>elladd(e,[-1,1],[0,0])
%3 = [1,0]
>ellorder(e, %3)
%4 = 0
```

As per usual, the first argument for each `ell` function is the curve we're working with. ◊

In the previous example we saw how one can easily compute the sum of two points on an elliptic curve. But what about adding a point to itself some number of times? Thankfully, we do not need to call `elladd` multiple times to find the multiple of a point. Instead we can use `ellpow(e, [x, y], n)` to compute $[n](x, y)$. This function is a great way to demonstrate the preposterous power and usefulness of PARI for these sorts of computations. For example, the reader is encouraged to try executing the following for `e` defined as above.

```
> ellpow(e, [-1, 1], 1000)
```

4.2 Computing Preimages

Now that we know how to use PARI to do basic calculations with points on an elliptic curve, we move on to computing the coordinates of points in the preimage $E^P[\ell]$. The general procedure is that we produce a single-variable rational function for the x-coordinate of the point $[\ell](x, y)$, and set this rational function equal to the x-coordinate of the point P. This yields a polynomial, the roots of which correspond to points in $E^P[\ell]$. We will illustrate this procedure by finding a particular preimage under [2].

For `e=ellinit([0,1,1,-2,0])`, we can make PARI tell us what [2] does to an arbitrary point. What we get is

```
>ellpow(e, [x, y], 2)
%2 = [9/(4*y^2 + 4*y + 1)*x^4 + 12/(4*y^2 + 4*y + 1)*x^3 - 8/(4*y^2 + 4*y + 1)*x^2
 + ((-8*y^2 - 8*y - 10)/(4*y^2 + 4*y + 1))*x + ((-4*y^2 - 4*y + 3)/(4*y^2 + 4*y + 1)),
  -27/(8*y^3 + 12*y^2 + 6*y + 1)*x^6 - 54/(8*y^3 + 12*y^2 + 6*y + 1)*x^5
  + 18/(8*y^3 + 12*y^2 + 6*y + 1)*x^4 + ((36*y^2 + 36*y + 73)/(8*y^3
  + 12*y^2 + 6*y + 1))*x^3 + ((36*y^2 + 36*y - 3)/(8*y^3 + 12*y^2 + 6*y + 1))*x^2
  + ((-16*y^2 - 16*y - 28)/(8*y^3 + 12*y^2 + 6*y + 1))*x
  + ((-8*y^4 - 20*y^3 - 26*y^2 - 15*y +5)/(8*y^3 + 12*y^2 + 6*y + 1))]
```

. . . something horrible. We can simplify this, however, by choosing to work with a different form of this curve. As we did in Section 1.3, we will want to use equations of the form $y^2 = x^3 + ax + b$, since otherwise we will not be able to use the division polynomial expression in Equation 1.2.5. Following Silverman ([13, p. 48]), we can write any curve defined over the rationals in the form

$$y^2 = x^3 - 27c_4x - 54c_6,$$

where c_4 and c_6 are given by fairly simple expressions in the coefficients b_2 through b_6 that we gave in Section 1.1 (in our discussion of the discriminant). Rather than write down another expression that we would never use in practical circumstances, we note that PARI computes them for us automatically. Access is given by the member functions `e.c4` and `e.c6`. Taking `e` defined as before,

```
>E = ellinit([0,0,0,-27*e.c4,-54*e.c6])
%2 = [0, 0, 0, -3024, 46224, ... et al.]
```

(Variable names in PARI are case-sensitive.) When we do not suppress the output of `ellinit`, we get a very long vector full of information about the curve. In particular, the first five entries are the coefficients $a_1, \ldots, a_6$ that we just provided. We verify that this is indeed the same curve by checking the "minimal model" for `E` and seeing that it matches, and compute the coordinates of the points of infinite order on this short model.

```
>ellminimalmodel(E)
%3 = [0, 1, 1, -2, 0, ... et al.]
>ellgenerators(E)
%4 = [[-24, 324], [12, 108]]
```

The reader may not be surprised to find that the curve we plucked from low-lying branches of the internet was given in some sort of "minimal form." Getting too bogged down in the details of defining this minimal form for a curve over $\mathbf{Q}$ would be very counter-productive, so we'll proceed to other things. The duplication mapping PARI spits out for us now is much easier to look at.

```
>ellpow(E, [x, y], 2)
%5 = [9/(4*y^2)*x^4 - 4536/y^2*x^2 - 2*x + 2286144/y^2,
 -27/(8*y^3)*x^6 + 10206/y^3*x^4 + 9/(2*y)*x^3 - 10287648/y^3*x^2
 - 4536/y*x + ((-y^4 + 3456649728)/y^3)]
```

This is much easier to look at. Additionally, a particular simplification we can make is much more visually apparent with this rational expression. Everywhere y is found in the first rational expression (the first entry of the vector), it has an exponent of 2. But because the point (x, y) was presumed to be on the curve, we can substitute $y^2 = x^3 - 3024x + 46224$. While this does introduce several messy coefficients, it completely eliminates y from our formula for the first coordinate of $[2](x, y)$. Doing so finally gives us an expression matching the duplication formula given in Section 1.2.

```
>f(x) = (x^4 + 6048*x^2 - 369792*x + 9144576)/(4*x^3 - 12096*x + 184896);
```

The benefit of replacing all the ys in this expression is that it allows us write out a single-variable polynomial in x, the roots of which will be the x-coordinates of the preimages of (x_0, y_0). We get this polynomial by setting our rational expression in x equal to x_0. Once we find the x-coordinate of the points in the preimage, we can plug these values back into the Weierstrass equation for E. Since we can easily double the resulting points (x, y), we can verify which of these gives the correct point (x_0, y_0).

As it turns out, however, this is usually overkill. We are concerned in this project with the Galois extensions admitted by these preimages, rather than their actual coordinates. Recall that Lemma 3.2.1 tells us that for the purposes of Galois theory we need only calculate the x-coordinate of the preimage points when we are taking the preimage of any point of order greater than 2.

In fact, our previously stated goal of calculating the coordinates of points in the preimage $E^P[\ell]$ is slightly excessive, since the Galois extension we are interested can be computed as the splitting field of the roots of the polynomial we've found. To actually compute the roots is unnecessary.

We now compute the Galois group of the splitting field of the polynomial achieved by setting `f(x)` equal to -24, the x-coordinate of one generator of infinite order.

```
> polgalois(numerator(f(x))+24*denominator(f(x)))
%7 = [24, -1, 1, "S4"]
```

The function `polgalois` specifies transitive subgroups of S_d (with d the degree of the polynomial) using a four-vector. The last entry is the "name" of the group, which in this case tells us that the group is S_4, the permutation group on four letters. This is the largest the group can be for the splitting field of a quartic polynomial. The other entries in the vector tell us other details about the group, namely its order, signature, and index as a subgroup of the symmetric group on d letters, where d is the degree of the polynomial of which we're taking the splitting field.

The group S_4 contains a normal subgroup isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, with a quotient group of $S_3 \simeq \mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z})$. This therefore perfectly illustrates Theorem 3.3.6, since then the group $\mathrm{Gal}(\mathbf{Q}(E^P[2])/\mathbf{Q}) \simeq (\mathbf{Z}/2\mathbf{Z})^2 \rtimes \mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z})$. Because the torsion subgroup $E[2] \simeq (\mathbf{Z}/2\mathbf{Z})^2$, it is of precisely the form we predicted.

Now, this strategy works perfectly well for points which we can write in affine coordinates as (x_0, y_0), but it does not work well for the point at infinity $\mathcal{O}$. For this point we will need to take a different approach. Thankfully, we can make use of the fact that the curve is given by a short Weierstrass equation (one like $y^2 = x^3 + ax + b$) to make a geometric argument.

Points of order 2 can only occur on a curve in short Weierstrass form on the x-axis. We noted in Section 1.2 that the negative of a point on a curve given by a short Weierstrass equation is just the reflection of that point over the x-axis. Point that is its own negative (i.e. any point of order 2) must be fixed by this reflection. Thus the points on the elliptic curve of order 2 must have a y-coordinate of 0. Putting this into the Weierstrass equation yields $0 = x^3+ax+b$, so the x-coordinates are given by the roots of the defining polynomial for the curve!

We've explored in somewhat excruciating detail when we acquire which Galois extension from the roots of a particular cubic polynomial in Section 2.2, so we know already what each of these extensions looks like.

We also note that the polynomial $x^3 + ax + b$ is $\frac{1}{4}$ of the denominator of the rational function in Equation 1.2.2 for duplication on the elliptic curve. This makes sense, since duplication maps a finite point of order 2 to a point *at infinity*, which can only happen at the poles of the rational mapping. This is a more useful way of determining the 2-torsion points, since it generalizes to integers greater than 2. Recalling Equation 1.2.5 and noting that it does not further cancel (see [1, §3.3]), we see that the m-torsion point extension is given by adjoining the roots of the mth division polynomial.

Taking `polgalois(numerator(f(x))-12*denominator(f(x)))` in the interest of studying the preimages of the other point of infinite order which has x-coordinate 12, we get the same Galois group as before. Thus we have two polynomials with the same Galois group. Can we verify that their compositum has the appropriate order very easily using MAGMA (another computer algebra system). Unfortunately there doesn't seem to be a simple way of doing this with PARI, despite the multiplicity of functions implemented for working over number fields.

```
QQ:=RationalField();
R<x>:=PolynomialRing(QQ);
P:=SplittingField(x^4 - 48*x^3 + 6048*x^2 - 224640*x + 6925824);
Q:=SplittingField(x^4 + 96*x^3 + 6048*x^2 - 660096*x + 13582080);
Compositum(P,Q);
```

The first two lines are just telling MAGMA to treat `x` as a variable in a polynomial ring; only in the last three lines do we compute anything. MAGMA demands semicolons at the end of every line; they have no semantic significance. The `SplittingField` and

`Compositum` functions are fairly self-explanatory. Output is given only for the last line (since it is the only line that is not a definition).

```
Number Field with defining polynomial x^96 - 3456*x^95 + 7776000*x^94 -
  13015157760*x^93 + 17994572734464*x^92 - 21344175079391232*x^91 +
                              ...
  7265906745155084353536 over the Rational Field
```

This polynomial is very long, too long to print here. However, the degree of the polynomial is really all we're concerned about. MAGMA gives defining polynomials of degree equal to the degree of the extension over $\mathbf{Q}$, so we can conclude the degree of the extension is $96 = 6 \times 4^2 = |\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z})| \times |(\mathbf{Z}/2\mathbf{Z})^2|^2$. At least the order of the extension (which we know a priori to be Galois, since it it the compositum of two Galois extensions) matches Conjecture 3.4.3.

Bibliography

[1] Clemens Adelmann, *The Decomposition of Primes in Torsion Point Fields*, Springer, New York, 2001.

[2] J. E. Cremona, *Tables of Elliptic Curve Data* (October 22, 2012). http://homepages.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html.

[3] David S. Dummit and Richard M. Foote, *Abstract Algebra*, 3rd ed., Jon Wiley and Sons, Hoboken, NJ, 2004.

[4] Noam D. Elkies, *Three Lectures on Elliptic Surfaces and Curves of High Rank*, eprint arXiv:0709.2908 (2007).

[5] Rafe Jones and Jeremy Rouse, *Galois Theory of Iterated Endomorphisms*, Proc. Lond. Math. Soc. **100(3)** (2010), pp. 763-794. (The preprint on Rafe Jones' website is somewhat easier to follow.)

[6] Serge Lang, *Elliptic Curves and Diophantine Analysis*, Springer-Verlag, Berlin Heidelberg, 1978.

[7] Patrick Morandi, *Field and Galois Theory*, Springer, New York, 1996.

[8] *PARI/GP, version 2.3.4*, http://pari.math.u-bordeaux.fr/ (2008).

[9] Richard Pink, *On the Order of the Reduction of a Point on an Abelian Variety*, Mathematische Annalen **330** (2004), pp. 275-291.

[10] Jonathan Reynolds, *On the Pre-Image of a Point Under an Isogeny*, eprint arXiv:0810.0092 (2008).

[11] Marusia Rebolledo, *Merel's theorem on the boundedness of the torsion of elliptic curves*, Clay Mathematics Proceedings (2009).

[12] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones Mathematicae **15** (1972), pp. 259 - 331.

[13] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.

[14] Joseph H. Silverman and John Tate, *Rational Points on Elliptic Curves*, Springer, New York, 1992.