ELLIPTIC CURVES AND DREAMS OF YOUTH

AMIN IDELHAJ

Abstract. This paper aims to build toward the use of elliptic curves in extending the Kronecker-Weber theorem to imaginary quadratic fields. It begins with some general content on elliptic curves and associated Galois representations. Afterwards, there is discussion about elliptic curves with complex multiplication and their use in generalizing the Kronecker-Weber theorem to imaginary quadratic fields.

Contents

1. Introduction

Many questions that one encounters early on in number theory can be stated with very little machinery. In principle one can expect that their solutions do not require much more. On the contrary, number theory uses a large amount of input from many different branches of math, even to answer questions which can be simply parsed (e.g. Fermat's Last Theorem). There are some cases where the usefulness of various techniques is less of a surprise. For example, it is natural to expect that the study of Diophantine equations would incorporate ideas from algebraic geometry. However, the mechanism by which such connections arise can be unexpected.

Elliptic curves are extremely important in modern number theory. However, much of the original motivation for their study comes from trying to calculate the arc length of an ellipse, as this was related to the computation of integrals which, in the denominator, involved square roots of cubics. This does not, at least initially, seem to give much of a suggestion as to why they are so important in number theory.

Date: July 2018.

Before we begin, a word on background is in order. The reader is assumed to have a working command of algebra; Galois theory in particular is employed heavily in later sections. Section 4 references complex analysis, and Section 5 references representations and p-adic numbers, but the reader need not have much experience in those subjects.

2. Some Geometric Preliminaries

Definition 2.1. Let K be a field. Define the projective plane over K to be

$$\mathbb{P}^2(K) = (K^3 \setminus \{0\})/\sim,$$

where $(x, y, z) \sim (\lambda x, \lambda y, \lambda z)$ for $\lambda \in K^\times$. The equivalence class of (x, y, z) is denoted by $[x : y : z]$.

A homogeneous polynomial $F \in K[x, y, z]$ defines a *projective plane curve*

$$C_F = \{P \in \mathbb{P}^2(\overline{K}) \mid f(P) = 0\}$$

where an element $[x : y : z] \in \mathbb{P}^2(\overline{K})$ is said to be a root of f if a representative (x, y, z) is. This is well-defined because for any $\lambda \in K^\times$, homogeniety implies that

$$F(x, y, z) = 0 \iff F(\lambda x, \lambda y, \lambda z) = \lambda^k F(x, y, z) = 0.$$

The *degree* of the curve C_F is defined to be that of F. The K-rational points of C_F are those which may be written as $[x : y : z]$ for $x, y, z \in K$. A point $P \in C_F$ is said to be a *singular point* if

$$\partial_x F(P) = \partial_y F(P) = \partial_z F(P) = 0,$$

where this is well-defined because the partial derivatives of a homogeneous polynomial are homogeneous. The curve C_F is said to be *nonsingular* or *smooth* if it has no singular points.

For any field K, we may identify $\mathbb{P}^2(K)$ with $K^2 \cup \mathbb{P}^1(K)$ by mapping $[x : y : z]$ to (x, y) if $z = 1$, or to $[x : y]$ if $z = 0$. The $\mathbb{P}^1(K)$ component is called the line at infinity.

The following two theorems are used in studying the group law on an elliptic curve, however their proofs are beyond the scope of this paper.

Theorem 2.2 (Bézout's Theorem)**.** *Let X and Y be projective plane curves of degrees m and n, respectively. Then X and Y intersect in mn points counting multiplicity.*

Theorem 2.3. *Let X and Y be projective plane curves of degree 3. If Z is a cubic curve that contains 8 of the 9 intersection points of X and Y, then it contains the 9th as well.*

With this, we may now begin the study of elliptic curves.

3. Elliptic Curves

Definition 3.1. Let K be a field of characteristic different from 2[1]. An elliptic curve over K is a smooth projective plane curve C_F where F is of the form

$$F(x, y, z) = y^2z - (x^3 + ax^2z + bxz^2 + cz^3),$$

for $a, b, c \in K$.

Remark 3.2. If $z = 0$ in the above equation, then $x = 0$. Thus, the curve C_F can be written as the union of a "point at infinity" $\mathcal{O} = [0 : 1 : 0]$, along with the solutions in $\overline{K}^2$ to $y^2 - f(x)$, where $f(x) = x^3 + ax^2 + bx + c$. We typically write $E : y^2 = f(x)$. For $F \subset \overline{K}$, write $E(F)$ for the set of F-rational points.

Theorem 3.3. *Consider an arbitrary equation of the form*

$$F(x, y, z) = y^2z - (x^3 + ax^2z + bxz^2 + cz^3).$$

Then the associated projective plane curve C_F is singular at points of the form $[x : 0 : 1]$, where x is a multiple root of f. In particular, C_F is smooth if and only if f has no multiple roots (equivalently, if f has non-zero discriminant).

Proof. The partial derivatives are as follows:

$$\partial_x F = -3x^2 - 2axz - bz^2$$

$$\partial_y F = 2yz$$

$$\partial_z F y^2 - ax^2 - 2bxz - 3cz^2$$

The point at infinity is not singular since $\partial_z F$ is non-zero at that point. Otherwise, set $z = 1$. Then $\partial_x F = -f'(x)$ and $\partial_y F = 2y$. If $2y = 0$, then $y^2 = f(x) = 0$. If moreover $-f'(x) = 0$, then x is a multiple root of f. □

Definition 3.4. Fix an elliptic curve E. Given two points P and Q in E, define the line through P and Q as follows:

- If P and Q are distinct points in the $\overline{K}^2$ component of the curve, then the line through them is the extension to $\mathbb{P}^2(\overline{K})$ of the unique line in $\overline{K}^2$ containing both.
- Then line through P and P is the extension to $\mathbb{P}^2(\overline{K})$ of the tangent line of E at P.
- If $P \neq Q = \mathcal{O}$, then the line through them is the extension to $\mathbb{P}^2(\overline{K})$ of the vertical line at P.
- If $P = Q = \mathcal{O}$, then the line through it is the line at infinity.

By Bézout's theorem, the line passing through P and Q will intersect E at a third point; call this point $P*Q$. If $P = (x, y) \neq \mathcal{O}$, then $P*\mathcal{O} = (x, -y)$, reflection of P across the x-axis. The line at infinity intersects E only at $\mathcal{O}$, so $\mathcal{O} * \mathcal{O} = \mathcal{O}$.

Now, define a group operation on E by $P + Q = \mathcal{O} * (P * Q)$. Associativity uses Theorem 2.3, see [1] for details. By the previous discussion, $\mathcal{O}$ is the identity element, and the inverse of $P \neq \mathcal{O}$ is its reflection across the x-axis. Moreover, since $P * Q = Q * P$, the group is abelian.

[1]In general, one can define an elliptic curve as a non-singular projective curve of genus 1 with a specified basepoint. If the field of definition does not have characteristic 2, then we may change variables so the curve is of the above form.

We now present an explicit formula for computing $P + Q$ where $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. Let the line through P and Q be given by $y = \lambda x + \nu$ where $\nu = y_1 - \lambda x_1$. Intersection points of this line and the elliptic curve are solutions to the following:

$$\lambda^2 x^2 + 2\nu\lambda x + \nu^2 = (\lambda x + \nu)^2 = y^2 = x^3 + ax^2 + bx + c$$

Thus, we see that the x-coordinates of the points where the line and curve intersect are given as the solutions to

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2).$$

Since x_1 and x_2 are two of the roots, it follows from Vieta's formulas that $P + Q = (x_3, y_3)$ where

$$x_3 = \lambda^2 - a - x_1 - x_2, y_3 = -\lambda x_3 - \nu.$$

If $P \neq Q$, then $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$. If $P = Q = (x, y)$, then implicit differentiation shows that $\lambda = \frac{f'(x)}{2y}$.

For an elliptic curve E, define $E[n] = \{P \in E \mid nP = \mathcal{O}\}$ to be its group of n-torsion points. These turn out to be of great importance, both in general and toward understanding generalizations of the Kronecker-Weber theorem. For a complex elliptic curve, lattices play a role in understanding torsion points, so we now turn our attention to them.

4. Lattices

While the results of this section inform the discussion to come, the proofs do not, and are thus omitted. The reader is advised to consult [1] for details.

Definition 4.1. A lattice in $\mathbb{C}$ is a subset of the form $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, where ω_1 and ω_2 are $\mathbb{R}$-linearly independent.

Definition 4.2. If Λ is a lattice in the plane, we define its associated Weierstrass $\wp$-function as follows:

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

Theorem 4.3. *The function $\wp(z; \Lambda)$ is meromorphic with poles at the points of Λ. Its derivative is*

$$\wp'(z; \Lambda) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z - \omega)^3}.$$

The functions $\wp$ and $\wp'$ are doubly periodic with periods ω_1 and ω_2 (and thus with all points in Λ as periods). Meromorphic functions with two $\mathbb{R}$-linearly independent period are known as elliptic functions. The study of these functions is of great interest in itself, and the Weierstrass $\wp$-functions play a crucial role.

Theorem 4.4. *The functions $\wp$ and $\wp'$ satisfy the following differential equation:*

$$\wp'(z; \Lambda)^2 = 4\wp(z; \Lambda)^3 - g_2(\Lambda)\wp(z; \Lambda) - g_3(\Lambda)$$

where $g_2(\Lambda) = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^4}$ and $g_3(\Lambda) = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^6}$. Additionally, the polynomial $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ has no repeated roots.

Any complex[2] elliptic curve E can be written in the form $y^2 = 4x^3 - ax - b$ after a change of variables, where the equation again has no repeated roots. For any such a and b, there exists some lattice Λ such that $g_2(\Lambda) = a$ and $g_3(\Lambda) = b$. Consider the map

$$z \mapsto (\wp(z;\Lambda), \wp'(z;\Lambda)) \text{ if } z \neq 0; 0 \mapsto \mathcal{O}.$$

This map is an isomorphism of groups and of Riemann surfaces, so we may switch between the two pictures at will. Given a lattice Λ, we see that $\mathbb{C}/\Lambda$ is an elliptic curve with equation $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$. Conversely, given a complex elliptic curve, we may find some lattice such that $\mathbb{C}/\Lambda$ is ismorphic to it. In particular, this shows that elliptic curves are isomorphic to $\mathbb{S}^1 \times \mathbb{S}^1$ as topological gropus. The n-torsion points of the torus are given by $(\frac{j}{n} \mod 1, \frac{k}{n} \mod 1)$, which implies that $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. Note that this isomorphism is not canonical.

Having developed an increased understanding of the torsion points of an elliptic curve, we now proceed to an important point of interaction between Galois theory and elliptic curves, which will come up in our investigation later.

5. Galois Representations

Let E be an elliptic curve with rational coefficients and let K be a Galois extension of $\mathbb{Q}$ with Galois group G. Note that $E(K)$ is a subgroup of E. Then G acts coordinatewise on $E(K)$, which is well-defined since the coordinates are rational. In fact, since the group law is given by rational functions, G acts by endomorphisms, i.e. $\sigma(P+Q) = \sigma(P) + \sigma(Q)$.

Theorem 5.1. *Let E be an elliptic curve with rational coefficients and let $n \geq 0$ be an integer. Define*

$$\mathbb{Q}(E[n]) = \mathbb{Q}(x_1, y_1, \ldots, x_{n^2-1}, y_{n^2-1}),$$

where $(x_i, y_i) \in E[n]$. Then $\mathbb{Q}(E[n])$ is a finite Galois extension of $\mathbb{Q}$

Proof. Let $\sigma : \mathbb{Q}(E[n]) \to \mathbb{C}$ be a field homomorphism. If $P = (x_i, y_i) \in E[n]$, then $(\sigma(x_i), \sigma(y_i)) \in E[n]$ as well, since $\sigma(nP) = n\sigma(P) = \mathcal{O}$. Thus, $\sigma(x_i) = x_j$ for some j, and similarly $\sigma(y_i) = y_j$. Thus, we see $\sigma(\mathbb{Q}(E[n])) \subset \mathbb{Q}(E[n])$, so that this is a Galois extension. Since σ is uniquely determined by its action on the finite set $\{x_1, \ldots, x_{n^2-1}\}$, there are only finitely many possibilities, so that $\mathbb{Q}(E[n])$ is finite. □

By the above discussion, we have an action by endomorphisms of $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ on $E[n]$. From the previous section, we know $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ upon fixing generators P_1 and P_2, so this gives us a representation

$$\rho_n : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \to GL_2(\mathbb{Z}/n\mathbb{Z}).$$

This is injective since if $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ acts trivially on $E[n]$, then it must fix all the x_i and y_i, but then it must be the identity map since those generate $\mathbb{Q}(E[n])$.

We have now developed all the representation-theoretic material we need in order to study imaginary quadratic fields. However, the study of Galois representations is important in its own right, and the representations we have developed may be

[2]More generally, over any field of characteristic not equal to 2 or 3

used in order to give an example of a p-adic representation of the absolute Galois group of $\mathbb{Q}$, so we divert attention briefly from the main goal in order to mention this. The remainder of this section may be skipped without loss of continuity.

Definition 5.2. Let p be a prime. The p-adic Tate module $T_p(E)$ of an elliptic curve E is the inverse limit of $E[p^n]$ with respect to the multiplication-by-p maps.

We see that $E[p^n] \cong (\mathbb{Z}/p^n\mathbb{Z})^2$, and then the multiplication by p map $E[p^n] \to E[p^{n-1}]$ becomes the natural projection $(\mathbb{Z}/p^n\mathbb{Z})^2 \to (\mathbb{Z}/p^{n-1}\mathbb{Z})^2$. Thus, we see that $T_p(E) \cong \mathbb{Z}_p^2$.

Recall that there is a restriction map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q})$, so the absolute Galois group of $\mathbb{Q}$ acts by endomorphisms on $E[p^n]$ for each n. Multiplicaton by p commutes with the Galois action, giving the following representation:

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_p(E)) \cong GL_2(\mathbb{Z}_p) \hookrightarrow GL_2(\mathbb{Q}_p).$$

6. Isogenies and Complex Multiplication

Now we focus on a particular class of elliptic curves which will be of principle importance later.

Definition 6.1. Let E_1 and E_2 be elliptic curves over some field K. A map $\phi : E_1 \to E_2$ is called an isogeny if $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$ and $\phi(x, y) = (f(x, y), g(x, y))$ where f and g are rational functions with coefficients in K. An isogeny from an elliptic curve to itself is called an endomorphism.

An isogeny is a group homomorphism (see [1,III.4.8]). The endomorphisms $\mathrm{End}(E)$ of an elliptic curve form a ring under pointwise addition and composition.

Example 6.2. The explicit form of the group law is given in terms of rational functions. Thus, the multiplication by n map $[n] : E \to E$ defined by is an endomorphism of E for any n. This gives a ring embedding $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$.

We now restrict attention to complex elliptic curves. Oftentimes, the above embedding is an isomorphism. Otherwise, the endomorphism ring is strictly larger than $\mathbb{Z}$, in which case we say the elliptic curve has *complex multiplication*.

Example 6.3. Suppose $E : y^2 = x^3 + ax$ and define the multiplication-by-i map $[i] : E \to E$ by $[i](x, y) = (-x, iy)$. Note that $[i] \circ [i](P) = -P$ for all P, while the square of a multiplication-by-n map is either the identity for $n = \pm 1$, or of infinite order otherwise. This gives an embedding $\mathbb{Z}[i] \hookrightarrow \mathrm{End}(E)$, and shows that E has complex multiplication.

Example 6.4. Suppose $E : y^2 = x^3 + a$ let ζ be a primitive third root of unity. Define the multiplication-by-ζ map $[\zeta] : E \to E$ by $[\zeta](x, y) = (\zeta x, y)$. This map is an isogeny and $\phi^3(P) = P$, so by a similar argument to the previous example, E has complex multiplication.

The nomenclature is explained by viewing elliptic curves as quotients of the complex plane by lattices. Abusing notation, we write $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$. This is a holomorphic function. Let B be a neigborhood of the origin containing no other lattice points, and consider $f = \phi|_B$. Since ϕ is an isogeny, it must be a homomorphism, so $f(z_1 + z_2) - f(z_1) - f(z_2) \in \Lambda$ for any $z_1, z_2 \in B$. Fixing z_1

and letting z_2 vary gives a holomorphic function $B \to \Lambda$. By the open mapping theorem, this must be constant, and since translation by an element of Λ will not influence the map on $\mathbb{C}/\Lambda$, this constant may be taken to be 0. Now, let g be some holomorphic function in a neighborhood of 0 such that $g(z+w) = g(z) + g(w)$. Then:

$$g'(z) = \lim_{h\to 0} \frac{g(z+h) - g(z)}{h} = \lim_{h\to 0} \frac{g(h)}{h} = g'(0)$$

Since ϕ is determined by this behavior near the origin, we see that it must be of the form $z \mapsto cz \mod \Lambda$ for some $c \in \mathbb{C}$. Now, fix generators ω_1 and ω_2 for the lattice. Then $c\omega_1 = a\omega_1 + b\omega_2$ for some $a, b \in \mathbb{Z}$ since $c\Lambda \subset \Lambda$. Then $(c-a)\omega_1 + b\omega_2 = 0$. If c were real, then real linear independence of the ω_i would imply that $c = a$, and thus that ϕ is a multiplication by a map. Thus, if an elliptic curve has any additional isogenies, then they are of the form $z \mapsto cz \mod \Lambda$ where c is not real.

Elliptic curves with complex multiplication are central to the study of imaginary quadratic extensions of $\mathbb{Q}$. Now that we've developed their general theory, we discuss some Galois-theoretic interactions.

7. Complex Multiplication and $\mathbb{Q}(i)$

We now focus our attention on the elliptic curve:

$$y^2 = x^3 - x$$

From Example 6.3, we see that this curve has complex multiplication given by $[i](x, y) = (-x, iy)$, and in fact its endomorphism ring is $\mathbb{Z}[i]$. Let $K_n = \mathbb{Q}(i)(E[n])$, which is Galois over $\mathbb{Q}$, and let $G_n = \mathrm{Gal}(K_n/\mathbb{Q}(i))$. Given $\sigma \in G_n$, we have

$$\sigma([i](x, y)) = \sigma(-x, iy) = (-\sigma(x), i\sigma(y)) = [i](\sigma(x, y)).$$

In fact, an element $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$ fixes $\mathbb{Q}(i)$ if and only if it commutes with $[i]$. Since ϕ is also a homomorphism $E[n] \to E[n]$, upon choosing a basis for $E[n]$ over $\mathbb{Z}/n\mathbb{Z}$ we see that ϕ is represented by a matrix A which commutes with all the $\rho_n(\sigma)$ for $\sigma \in G_n$, where $\rho_n : \mathrm{Gal}(K_n/\mathbb{Q}) \to GL_2(\mathbb{Z}/n\mathbb{Z})$ is the representation outlined in Section 6. Furthermore, we see that $A^2 = -I$, which has determinant 1, so A is invertible.

Theorem 7.1. *The matrix A is not a scalar multiple of the identity mod ℓ for any prime $\ell \mid n$.*

Proof. Assume that $A \equiv mI \mod \ell$. Then for any point $P = (x, y) \in E[\ell]$, we have that $[i](P) = mP$. Cmplex conjugation is a homomorphism of $E[\ell]$, so that

$$m\overline{P} = \overline{mP} = \overline{[i](P)} = \overline{(-x, iy)} = (-\overline{x}, -i\overline{y}) = -[i](\overline{P}) = -m\overline{P}.$$

Thus, $2mP = \mathcal{O}$ for $P \in E[\ell]$, which implies that $\ell = 2$ or $\ell \mid m$. Choosing $(0, 0)$ and $(i, 0)$ as a basis of $E[2]$ gives the matrix of ϕ as $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. This is not similar to any scalar multiple of the identity, so $\ell \neq 2$. If $\ell \mid m$, then $[i] \mid_{E[\ell]} = \mathcal{O}$, which is impossible since $[i]^2(P) = -P$, so $\ell \nmid m$. □

Theorem 7.2. *If $A \in GL_2(\mathbb{Z}/n\mathbb{Z})$ is not a scalar matrix mod ℓ for any prime $\ell \mid n$, then $\{B \in GL_2(\mathbb{Z}/n\mathbb{Z}) \mid AB = BA\}$ is an abelian subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$.*

Theorems 7.1 and 7.2 show that the image of $\mathrm{Gal}(K_n/\mathbb{Q}(i))$ in $GL_2(\mathbb{Z}/n\mathbb{Z})$ under the representation in Section 6 is abelian. Since that representation is injective, the same is true for the Galois group. It suffices to prove Theorem 7.2 where $n = \ell^e$ is a prime power, as the general case follows by the Chinese Reimander Theorem.

Proof. If $AB = BA$ and $AC = CA$, then $A(BC) = (BC)A$, so this set is closed under multiplication. Since the ambient group $GL_2(\mathbb{Z}/n\mathbb{Z})$ is finite, this suffices to show that the set in question is a subgroup.

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be the matrix of $[i]$.

- If $b \not\equiv 0 \mod \ell$, let $T = \begin{pmatrix} 0 & b \\ 1 & d \end{pmatrix}$. Then $\det(T) = b$, so that T is invertible, and $T^{-1}AT = \begin{pmatrix} 0 & bc - ad \\ 1 & a + d \end{pmatrix}$.
- Otherwise, and if $c \not\equiv 0 \mod l$, let $T = \begin{pmatrix} 1 & a \\ 0 & c \end{pmatrix}$. Then $\det(T) = c$, so that T is invertible, and $T^{-1}AT = \begin{pmatrix} 0 & cb - ad \\ 1 & a + d \end{pmatrix}$.
- Otherwise, we will have that $a \not\equiv d \mod l$, so let $T = \begin{pmatrix} 1 & a + b \\ 1 & c + d \end{pmatrix}$. Then $\det(T) = c + d - a - b$, which is equivalent mod ℓ to the $d - a$, so T is invertible. Then $T^{-1}AT = \begin{pmatrix} 0 & bc - ad \\ 1 & a + d \end{pmatrix}$.

Thus, without loss of generality, A may be assumed to be in rational canonical form $\begin{pmatrix} 0 & b \\ 1 & d \end{pmatrix}$. For $B = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$, write

$$AB = \begin{pmatrix} bz & bw \\ x + dz & y + dw \end{pmatrix} = \begin{pmatrix} y & bx + dy \\ w & bz + dw \end{pmatrix} = BA.$$

This holds if and only if $y = bz$ and $w = x + dz$. Let $B = \begin{pmatrix} x & bz \\ z & x + dz \end{pmatrix}$ and $C = \begin{pmatrix} x' & bz' \\ z' & x' + dz' \end{pmatrix}$ be two matrices satisfying this property. Then

$$BC = \begin{pmatrix} xx' + bzz' & xbz' + x'bz + bdzz' \\ x'z + z'x + dzz' & bzz' + xx' + xdz' + dzx' + d^2zz' \end{pmatrix} = CB$$

□

Example 7.3. We now compute $\mathrm{Gal}(K_3/\mathbb{Q}(i))$. A point $P = (x_0, y_0)$ is in $E[3]$ if and only if $2P = -P$. By the explicit form of the group law as described in Section 2, the first coordinate of $2P$ is

$$\frac{9x_0^4 - 6x_0^2 + 1}{4x_0^3 - 4x_0} - 2x_0 = \frac{x_0^4 + 2x_0^2 + 1}{4x_0^3 - 4x_0}.$$

This must be equal to x_0 since P and $-P$ have the same first coordinate. The solutions to this are $x_0 = \pm\sqrt{1 \pm \frac{2}{\sqrt{3}}}$. Solving for all the possibilities for y_0 and simplifying, we see that $K_3 = \mathbb{Q}(i, \sqrt[4]{12 + 8\sqrt{3}})$. The minimal polynomial of $\sqrt[4]{12 + 8\sqrt{3}}$ over $\mathbb{Q}(i)$ is $x^8 - 24x^4 - 48$, which is irreducible by Eisenstein's criterion for $p = 3$.

The roots of this polynomial are $i^k \sqrt[4]{12 \pm 8\sqrt{3}}$ for $0 \leq k \leq 3$. Let σ_k be the automorphism sending $\sqrt[4]{12 + 8\sqrt{3}}$ to $i^k \sqrt[4]{12 - 8\sqrt{3}}$. Each σ_k maps $\sqrt{3}$ to $-\sqrt{3}$. Thus, $\sigma_k(\sqrt[4]{-3})^2 = \sigma_k(i\sqrt{3}) = -i\sqrt{3}$, so that $\sigma_k(\sqrt[4]{-3}) = \pm i\sqrt[4]{-3}$, which implies that the σ_k must have order at least 4. If all of them had order equal to 4, then the group would have 6 elements of order 4. This is not satisfied by any abelian group of order 8, so at least one of the σ_k has order 8, implying that the Galois group is $\mathbb{Z}/8\mathbb{Z}$.

8. Kronecker's Jugendtraum

One of the core goals of algebraic number theory is to try to understand the arithmetic theory of number fields. Galois extensions of $\mathbb{Q}$ are an important and tractable special case. For one, subgroups of the Galois group classify intermediate field extensions (and we can always embed some number field into its Galois closure). Additionally, the Galois group acts in very useful ways, e.g. on the prime ideals in the ring of integers lying over a given prime in $\mathbb{Z}$. Among these extensions, a natural first step would be to try and understand those with abelian Galois group. The *Kronecker-Weber theorem* completely settles this case via cyclotomic fields:

Theorem 8.1. *For any abelian extension F of $\mathbb{Q}$, there exists some n such that $F \subset \mathbb{Q}(\zeta_n)$.*

This is one of the most important theorems in Galois theory, laying the foundations for such subjects as class field theory. Kronecker's Jugendtraum, or dream of youth, was to obtain variants of this theorem for all number fields. The following example shows that, cyclotomic fields do not take us much farther than $\mathbb{Q}$.

Example 8.2. Suppose $K = \mathbb{Q}(i, \sqrt[4]{-3})$. This is an abelian extension of $\mathbb{Q}(i)$, since it has order 4. However, it is not an abelian extension of $\mathbb{Q}$, and thus is not contained in any cyclotomic extension of it. Since a cyclotomic extension of $\mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$ is also one of $\mathbb{Q}$, the naive extension of the Kronecker-Weber theorem to $\mathbb{Q}(i)$ fails.

Recall from Example 7.3 that $\mathbb{Q}(i)(E[3]) = \mathbb{Q}(i, \sqrt[4]{12 + 8\sqrt{3}})$ where E is given by $y^2 = x^3 - x$. The computation

$$\sqrt[4]{12 + 8\sqrt{3}}\sqrt[4]{12 - 8\sqrt{3}} = \sqrt[4]{-48} = 2\sqrt[4]{-3}$$

shows that $\mathbb{Q}(i, \sqrt[4]{-3}) \subset \mathbb{Q}(i)(E[3])$. Thus, the 3-torsion points of this elliptic curve are able to detect an extension that cyclotomic fields could not. In fact, the torsion points of this curve allow for the extension of the Kronecker-Weber theorem to $\mathbb{Q}(i)$.

Theorem 8.3. *Let $E : y^2 = x^3 - x$. Then for any abelian extension F of $\mathbb{Q}(i)$, there exists some n such that $F \subset \mathbb{Q}(i)(E[n])$.*

Since $\mathrm{Gal}(\mathbb{Q}(i)(E[n])/\mathbb{Q}(i))$ is abelian, as proven in the previous section, this theorem really is an extension of the Kronecker-Weber theorem to $\mathbb{Q}(i)$. Moreover, elliptic curves provide us with a large class of fields to which we can extend the Kronecker-Weber theorem.

Theorem 8.4. *Let K be an imaginary quadratic field. Then there exists some elliptic curve E whose endomorphism ring is $\mathcal{O}_K$, and every abelian extension of K is contained in $K(E[n])$ for some n.*

Acknowledgements

I would like to thank my mentors, Karl Schaefer and Billy Lee, for their inspiration in guiding me to my chosen topic, support during the research process, and assistance in revising my paper. I would also like to thank my professor, Matthew Emerton, for guidance and inspiration. Finally, I would like to thank Peter May for organizing the program and making it a wonderful experience.

References

[1] Joseph H. Silverman. The Arithmetic of Elliptic Curves, Second Edition Springer. 2009.
[2] Joseph H. Silverman, John T. Tate. Rational Points on Elliptic Curves, Second Edition Spinrger, 2015