Complex Multiplication: Kronecker's Jugendtraum for $\mathbb{Q}(i)$

Alex Halperin

April 29, 2008

Abstract

We discuss Chapter 6 from Silverman & Tate's *Rational Points on Elliptic Curves*, in which the authors outline a means of proving Kronecker's Jugendtraum for $\mathbb{Q}$ and $\mathbb{Q}(i)$. One considers $C[n]$, the kernel of the multiplication-by-n map on an elliptic curve C. After defining the number field $\mathbb{Q}(C[n])$, we examine instances in which its Galois group over a field K is abelian. For the elliptic curve

$$C : y^2 = x^3 + x,$$

we can show that $\mathrm{Gal}(\mathbb{Q}(i)(C[n])/\mathbb{Q}(i))$ is abelian by representing it as a subgroup of $GL_2(\mathbb{Z}_n)$. In fact, $\mathbb{Q}(i)(C[n])$ contains all abelian extensions K of $\mathbb{Q}(i)$ for some positive integer n. Furthermore, one can describe $\mathbb{Q}(i)(C[n])$ and its Galois group using only the Weierstrass $\wp$-function. This is equivalent to saying $\mathbb{Q}(i)(C[n])$ satisfies Kronecker's Jugendtraum for $\mathbb{Q}(i)$.

1 Kronecker's Jugendtraum: A First Look

We want to understand finite extensions of fields $K \supseteq \mathbb{Q}$ and their Galois groups. We focus on *number fields* (finite field extensions) over $\mathbb{Q}$ and $\mathbb{Q}(i)$, since they are easier to analyze and more intuitive than infinite extensions. In particular, we consider a number field $K(a_1, ..., a_m)$ such that $\mathrm{Gal}(K(a_1, ..., a_m)/K)$ is abelian, and refer to such an extension as an *abelian extension*. The Jugendtraum ("Dream of Youth") was Kronecker's desire

to describe any finite abelian extension of a field K and the corresponding Galois group using a single function f and certain values $x_1, ..., x_m$.

For $K = \mathbb{Q}$, the use of complex analysis (and class field theory, which is far beyond the scope of this paper and will be completely ignored) in conjunction with the Kronecker-Weber Theorem allows us to represent any abelian number field $\mathbb{Q}(a_1, ..., a_m)$ as $\mathbb{Q}(f(x_1), ...f(x_m))$, where $f(x) = e^{\frac{2\pi i}{x}}$, for certain $x \in \mathbb{Q}$. Our main focus, however, is to explain the Jugendtraum for $K = \mathbb{Q}(i)$, where any abelian number field $\mathbb{Q}(i)(a_1, ..., a_m)$ is contained in $\mathbb{Q}(i)(C[n]) := \mathbb{Q}(i)(x_1, y_1, ..., x_{n^2}, y_{n^2})$, with $(x_i, y_i) \in C[n]$ for the elliptic curve $C : y^2 = x^3 + x$. $C[n]$ is defined to be $\{(x_j, y_j) \in C |\ n(x_j, y_j) = \mathcal{O}\}$; in other words, the points on the elliptic curve C whose order divides n.[2]

The latter instance involves the use of Galois theory on elliptic curves, and the representation of Galois groups as matrices in $GL_2(\mathbb{Z}_n)$. We single out elliptic curves C that have *complex multiplication* (i.e., curves C that have other endomorphisms $\varphi : C \longrightarrow C$ besides the multiplication-by-n map). We then show that $\mathrm{Gal}(\mathbb{Q}(i)(C[n])/\mathbb{Q}(i))$ is abelian for specific curves C. Finally, we focus on the elliptic curve $C : y^2 = x^3 + x$ in particular, which satisfies the Jugendtraum for $\mathbb{Q}(i)$ as stated above.

1.1 The Kronecker-Weber Theorem

From Galois theory we learn that given Galois extensions $\mathbb{Q}(a_1, ..., a_m)$ over $\mathbb{Q}$, there exist Galois groups (denoted $\mathrm{Gal}(\mathbb{Q}(a_1, ..., a_m)/\mathbb{Q})$), comprising $\mathbb{Q}(a_1, ..., a_m)$-automorphisms that permute the elements a_1 through a_m. The values a_1 through a_m arise from the representation of an irreducible polynomial $f \in \mathbb{Q}[x]$ in the form $f(x) = (x-a_1)...(x-a_m) = 0$. Note that this does not imply that $a_i \in \mathbb{Q}$ for any i. For example, $f(x) = x^2-3 = 0 = (x-\sqrt{3})(x+\sqrt{3})$, but $\pm\sqrt{3} \notin \mathbb{Q}$. Therefore, we say the *splitting field* for f is $\mathbb{Q}(\sqrt{3})$. Even though $\pm\sqrt{3}$ are adjoined to $\mathbb{Q}$, we only need to write $\mathbb{Q}(\sqrt{3})$, since $-\sqrt{3} = -1 \cdot \sqrt{3}$, so $-\sqrt{3} \in \mathbb{Q}(\sqrt{3})$. Since the only possible action a field automorphism can have on $\mathbb{Q}(\sqrt{3})$ is either fixing the entire field or permuting $\sqrt{3}$, we have $\mathrm{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}_2$.

By the Fundamental Theorem of Galois Theory[1, p.245], we know that for any extensions such that $\mathbb{Q} \subseteq E \subseteq F$, E is a Galois over $\mathbb{Q}$ if and only if $\mathrm{Gal}(F/E)$ is a normal subgroup of $\mathrm{Gal}(F/\mathbb{Q})$. Therefore, we want to focus on the situations when $\mathrm{Gal}(F/\mathbb{Q})$ is abelian, since all its subgroups are normal by default. This leads us to the focus of this section. Consider the field $\mathbb{Q}(\zeta)$, where $\zeta = e^{\frac{2\pi i}{n}}$ is a primitive nth-root of unity. $\mathbb{Q}(\zeta)$ is the

splitting field for the polynomial $g(x) = x^n - 1 = 0$.

Theorem 1.1.

$$Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}_n)^*,$$

where $(\mathbb{Z}_n)^*$ *is the unit group of* $\mathbb{Z}_n$.

Because ζ is primitive, we can construct the map

$$\begin{aligned} t: \quad Gal(\mathbb{Q}(\zeta)/\mathbb{Q} \quad &\longrightarrow \quad (\mathbb{Z}_n)^* \\ \sigma \quad &\longmapsto \quad j, \end{aligned}$$

where j and n are relatively prime and $1 \leq j < n$. [2, p.182] Showing that t is an injective homomorphism is not too difficult and will be left to the reader. The hard part showing surjectivity, requires class field theory, so we will take this for granted. Since $(\mathbb{Z}_n)^*$ is abelian, we have shown that $\mathrm{Gal}(\mathbb{Q}(\zeta)/E)$ is a normal subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ for all E. This implies E is Galois over $\mathbb{Q}$. Since $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ and $\mathrm{Gal}(\mathbb{Q}(\zeta)/E)$ are abelian, we know $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\zeta)/E)$ is abelian as well. Furthermore,

$$\frac{\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})}{\mathrm{Gal}(\mathbb{Q}(\zeta)/E)} \cong \mathrm{Gal}(E/\mathbb{Q}),$$

[2, p.183] which implies $\mathrm{Gal}(E/\mathbb{Q})$ is abelian. Using $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, $\mathrm{Gal}(\mathbb{Q}(\zeta)/E)$, and the First Isomorphism Theorem[1], we know $\mathrm{Gal}(E/\mathbb{Q})$ is abelian.

We now arrive at the Kronecker-Weber Theorem, which gives us a somewhat counter-intuitive result: Not only is $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ abelian, but for any finite abelian Galois extension H over $\mathbb{Q}$, $H \subseteq \mathbb{Q}(\zeta)$, for ζ an nth root of unity for some positive integer n. In fact, we can even go one step further: by introducing the function $f(x) = e^{\frac{2\pi i}{x}}$, any number field H over $\mathbb{Q}$ has the property

$$H \subseteq \mathbb{Q}(f(n)),$$

since $\zeta = e^{\frac{2pii}{n}}$ by definition. Furthermore, since any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is a field automorphism, one can show $\sigma(\zeta) = \zeta^j$, where $\gcd(j, n) = 1$. Therefore,

$$H \subseteq \mathbb{Q}\left(f\left(\frac{n}{j_1}\right), ..., f\left(\frac{n}{j_m}\right)\right) \text{ for } j_i \in (\mathbb{Z}_n)^*.$$

In fact, since we know $\sigma(\zeta) = \zeta^{t(\sigma)} = \zeta^j$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}$, We have described both $\mathbb{Q}(\zeta)$ and $\mathrm{Gal}\mathbb{Q}(\zeta)/\mathbb{Q}$using only f and a finite number of x-values. This is the Jugendtraum for $\mathbb{Q}$.

We will now work toward the case when $K = \mathbb{Q}(i)$. The next section discusses Galois groups derived from elliptic curves. We will ultimately express the elements of our Galois group as matrices in $GL_2(\mathbb{Z}_n)$. Finally, we will show that certain curves with complex multiplication lead to finite field extensions whose Galois groups are abelian. These number fields are contained in a number field over $\mathbb{Q}(i)$ that can be described using the Weierstrass $\wp$-function.

2 Galois Groups on Elliptic Curves

An *elliptic curve* is a non-singular cubic $C : y^2 = x^3 + ax^2 + bx + c$. $C(K)$ is the set of all points (x, y) that satisfy the previous equation, and whose x and y-coordinates are elements of K. By defining $(x_1, y_1) + (x_2, y_2)$ in a special way, (see [2, I.4]) it can be shown that $C(\mathbb{C})$ is an abelian group under this operation (that we will refer to as *addition*, or *curve addition* to avoid confusion with normal addition), and that $C(K)$ is a subgroup of $C(\mathbb{C})$ for all $K \subseteq \mathbb{C}$. We refer to the identity in $C(K)$ as $\mathcal{O}$, whose actual coordinate is $(0, 0, 1)$ in the projective plane (thus making it a point at whose x-coordinate equals the x-value for any point (x, y) on C, and whose y-coordinate is at infinity). Since we are now focusing on points $(x, y) \in C(K)$ instead of values $x \in K$, we must redefine the action of an automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ so it can act on $C(K)$.

Hence, if $P = (x, y)$ is a point in $C(K)$, let

$$\sigma(P) = \sigma(x, y) := (\sigma(x), \sigma(y))$$

and $\sigma(\mathcal{O}) := \mathcal{O}$.

Since the addition of points on an elliptic curve uses rational functions on x and y, and since σ is a homomorphism, the reader can easily check that for any $P \in C(K)$, $\sigma(P)$ is also in $C(K)$. For similar reasons, σ also preserves addition, i.e.,

$$\sigma(P + Q) = \sigma(P) + \sigma(Q),$$

for P and Q in $C(K)$. From this, it follows that

$$\sigma(nP) = \sigma(P + ... + P) = \sigma(P) + ... + \sigma(P) = n\sigma(P).$$

Using this, we then show that if P has order n, then $\sigma(P)$ also has order n.
Proof: Since $nP = \mathcal{O}$, we know $\sigma(nP) = \mathcal{O} = n\sigma(P)$, which implies the

order of σ divides n. Let the order of σ be a, such that $a|n$. Then, using composition of functions and the fact that σ is an automorphism, we see $\sigma^{-1}(a\sigma(P)) = \mathcal{O} = a\sigma^{-1}(\sigma(P)) = aP$. But P has order n, so $a = n$, and we are done. $\square$ [2]

We have shown that any element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, is a group homomorphism from $C(K)$ to itself, it preserves the operation, and it even preserves the order of any point it permutes. In other words, $\sigma(P)$ acts very similarly to P in $C(K)$.

2.1 The Multiplication-by-n Map

We now turn our focus to the map λ_n, where

$$\lambda_n : C \longrightarrow C$$
$$P \longmapsto nP$$

is an *endomorphism on* C; that is, a homomorphism from C to itself. In particular, we refer to λ_n as the *multiplication-by-n map*. Note that n will always be an integer. Its kernel is denoted $C[n] = \{P \mid \text{the order of P divides } n\} = \{P \mid nP = \mathcal{O}\}$.

Example 2.1. For $C : y^2 = x^3 + x$, find $C[2]$ and $C[3]$.

First, find $C[2]$. Using the Nagell-Lutz Theorem [2, p. 56], we know $P = (x, y)$ has order 2 if and only if $y = 0$. Therefore, $(0, 0)$, $(1, 0)$, and $(-1, 0)$ all have order 2. Also note that $\mathcal{O} \in C[n]$ for all n, since $\mathcal{O}$ has order 1. Therefore, $C[2] = \{\mathcal{O}, (0, 0), (1, 0), (-1, 0)\}$. With a little bit of work, we see that $(1, 0) + (-1, 0) = (0, 0)$, $(0, 0) + (1, 0) = (-1, 0)$, and $(0, 0) + (-1, 0) = (1, 0)$ (and that addition in this case is commutative). This, combined with the fact that all elements have order 2, shows that

$$C[2] \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

To find $C[3]$, we find all points P such that $3P = \mathcal{O}$. To do this, note that for any such point, $2P = -P$, and therefore the x-coordinates of P and $2P$ (denoted P_x and $2P_x$) are the same. Thus, we have

$$2P_x = \frac{x^4 - 2x^2 + 1}{4x^3 + 4x} = x = P_x \tag{1}$$
$$\Rightarrow\ 3x^4 + 6x^2 - 1 = 0. \tag{2}$$

Even though this equation is reasonably clean as far as elliptic curves go, solving for x still requires more work than is gratifying, and our answers are anything but pretty. It turns out that

$$x = \pm\alpha, \pm(i\sqrt{3}\alpha)^{-1}$$

for $\alpha = \sqrt{\frac{2\sqrt{3}-3}{3}}$, and

$$C[3] = \left\{(\alpha, \pm\beta), (-\alpha, \pm i\beta), \left(\frac{i}{3\alpha}, \pm\frac{2\sqrt{-i}}{\sqrt[4]{27}\beta}\right), \left(\frac{-i}{3\alpha}, \pm\frac{2\sqrt{i}}{\sqrt[4]{27}\beta}\right)\right\}$$

for $\beta = \sqrt[4]{\frac{2\alpha}{\sqrt{3}}}$. [2] With more work, one can show that $C[3] \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$. We will now work toward proving that this pattern works for all positive integers n.

Note: We will be using the elliptic curve $C : y^2 = x^3 + x$ throughout the paper, for reasons that stated earlier.

As we can see, the addition of points on an elliptic curve often causes $C[n]$ to appear more messy than helpful. We want to visualize $C[n]$ in order to better understand why it behaves like $\mathbb{Z}_n \oplus \mathbb{Z}_n$. In order to do this, we need to express $C[n]$ using complex numbers.

Expressing any elliptic curve

$$C : f(x) = y^2 = x^3 + ax^2 + bx + c$$

as

$$y^2 = 4x^3 + dx + e,$$

[1, p. 271], [5, p. 249] we can find generators $\omega_1, \omega_2 \in \mathbb{C}$ for the *lattice* $L = \{n_1\omega_1 + n_2\omega_2 \mid n_1, n_2 \in \mathbb{Z}\}$. L is a group under addition. The graph of L in the complex plane looks like a parallelogram with sides of length ω_1 and ω_2. Since n_1 and n_2 are integers, L consists of discrete points (hence, the word "lattice"). We will now use a meromorphic function whose poles are exactly the points in L.

Using the *Weierstrass $\wp$-function*

$$\wp : \quad \mathbb{C} \quad \longrightarrow \quad \mathbb{C}$$

$$\wp(z) = \frac{1}{z^2} + \sum_{0 \neq \omega \in L} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

[2] we get a fascinating connection to our curve C. If we differentiate $\wp$ with respect to z, it turns out that

$$(\wp')^2 = 4\wp^3 + d\wp + e.$$

This means that not only can $(\wp(z), \wp'(z))$ be expressed as a point on C, but we can create a map

$$\begin{array}{rccc} P: & \mathbb{C} & \longrightarrow & C(\mathbb{C}) \\ & z & \longmapsto & (\wp(z), \wp'(z)) \end{array}$$

[2] where any element $z \in L$ maps to the identity element $\mathcal{O} \in C(\mathbb{C})$. This is not a coincidence, since L consists of all nonzero points $z \in \mathbb{C}$ such that $\wp(z)$ has a pole, and $\mathcal{O}$ is the point at infinity on any curve C. So we are relating the poles in $\mathbb{C}$ to the pole in $C(\mathbb{C})$. This map is in fact a homomorphism, i.e. $P(z_1 + z_2) = P(z_1) + P(z_2)$, which is remarkable, since addition on the complex numbers is *not* the same as addition on C. This is because $\wp(z_1+z_2)$ can be expressed in terms of rational functions of $\wp(z_1)$ and $\wp(z_2)$. In fact, $\wp(z_1+z_2) = \frac{1}{4}\left(\frac{\wp'(z_1)-\wp'(z_2)}{\wp(z_1)-\wp(z_2)}\right)^2 - \wp(z_1) - \wp(z_2)$, and $\wp(2z) = \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2 - 2\wp(z)$, [4, p. 440-442] which is *exactly the same as curve addition!* This is not a coincidence, as Weierstrass first developed the $\wp$-function before the study of "elliptic curves." Weierstrass studied functional analysis and referred to $\wp$ as an *elliptic function* [5], a term still used today. Although it is onto, P is not one-to-one. Remember the earlier comment regarding poles of $\wp$: since there are multiple points in L, we have $P(a) = P(b) = \mathcal{O}$, for $a, b \in L$ and $a \neq b$. However, if we mod out $\mathbb{C}$ by L, we solve this problem. $\mathbb{C}/L$ is still a group under addition.

Lemma 2.2.

$$\begin{array}{rccc} P: & \mathbb{C}/L & \longrightarrow & C(\mathbb{C}) \\ & z & \longmapsto & (\wp(z), \wp'(z)) \end{array}$$

is one-to-one. Therefore $\mathbb{C}/L \cong C(\mathbb{C})$.

Proof: Since we mod out by L, $Ker(P) = \{0\}$ (out of all complex numbers in $\mathbb{C}/L$, 0 is the only pole for $\wp$). Since P is a homomorphism, $P\restriction_{\mathbb{C}/L}$ is one as well. $P\restriction_{\mathbb{C}/L}(0) = \mathcal{O}$ implies $P\restriction_{\mathbb{C}/L}$ is one-to-one. This is same as using the First Isomorphism Theorem. $\square$

Corollary 2.3. *Let* $\mathbb{C}[n] = \{z \in \mathbb{C} \mid$ *the order of* z *divides* $n\}$. *Then* $\mathbb{C}[n] \cong C[n]$.

Proof: Restrict the domain of P to $\mathbb{C}[n]$, and the image is $C[n]$.

In general, $\wp$ is *doubly-periodic*, which means $\wp(z+\omega_1) = \wp(z)$ and $\wp(z+\omega_2) = \wp(z)$ for all $z \in \mathbb{C}$. Thus, any complex numbers of order n in $\mathbb{C}/L$ have the form $\frac{a_1}{n}\omega_1 + \frac{a_2}{n}\omega_2$, where $a_1\omega_1 + a_2\omega_2 \in L$.

Theorem 2.4.

$$\theta : \mathbb{C}[n] \longrightarrow \mathbb{Z}_n \oplus \mathbb{Z}_n$$
$$\frac{a_1}{n}\omega_1 + \frac{a_2}{n}\omega_2 \longmapsto (a_1, a_2)$$

is an isomorphism. Therefore $\mathbb{C}[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$.

[2] The proof is not difficult and will be left to the reader.

Corollary 2.5. $C[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$

Proof: This is immediate by Corollary 2.3.

We will now relate all of this to our previous discussion about Galois theory.

Theorem 2.6. $\mathbb{Q}(C[n]) = \mathbb{Q}(\{x_i, y_i \mid (x_i, y_i) \in C[n]\})$ *is a Galois extension over* $\mathbb{Q}$.

Proof: One way to show a number field K is a Galois extension of $\mathbb{Q}$ is to show that for all field homomorphisms $\sigma : K \longrightarrow \mathbb{C}$, $\sigma(K) = K$. Since σ is a field homomorphism, $Ker(\sigma) = \{0\}$, so it is one-to-one. Therefore, if we can show $\sigma(K) \subseteq K$, we know σ is a bijection. Now, for $K = \mathbb{Q}(C[n])$, take any $x_i, y_i \in K$. Since $(x_i, y_i) \in C[n]$, we know $n(x_i, y_i) = \mathcal{O} = \sigma(n\mathcal{O}) = n\sigma(\mathcal{O})$. This implies that $(\sigma(x_i), \sigma(y_i)) \in C[n]$, and $\sigma(x_i), \sigma(y_i) \in K$. Therefore, $\sigma(K) \subseteq K$.□ [2]

(As a side note, this also implies that each pair of values $\{x_i, y_i\}$ is algebraic over $\mathbb{Q}$, since K is a finite extension, with $|Aut(K)| \leq n^2!$ If any x_i or y_i value were transcendental, it would not permute with any other element.)[2]

Remark 2.7. Galois extensions over a field give Galois groups over said field. Therefore, we know that $\mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q})$ exists for any curve C and for all n.

Re-examining Example 2.1, we find $\mathrm{Gal}(\mathbb{Q}(C[2])/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}/\mathbb{Q}) = \{\mathrm{id}\}$. Reducing the number field $\mathbb{Q}(C[3])$ to $\mathbb{Q}(\beta, i)$ requires more work. Surprisingly, $\mathrm{Gal}(\mathbb{Q}(\beta, i)/\mathbb{Q})$ turns out to be a non-abelian group. Even though $C[n]$ is abelian for all n, $\mathrm{Gal}(\mathbb{Q}(C[3])/\mathbb{Q})$ is not necessarily abelian. This is a drawback, since we are trying to only focus on number fields that have abelian Galois groups. In order to further narrow things down, we must first introduce complex multiplication and then represent any Galois group as a set of matrices.

2.2 The Existence of Other Homomorphisms

We have shown that Galois groups can act on elliptic curves . Also, while we know that the multiplication-by-n map is a homomorphism, we have not considered other maps that may also preserve addition in $C(\mathbb{C})$. Although the multiplication-by-n map exists on C for all curves C, it not easy to find other group homomorphisms. This is mainly because given the complicated definition of curve addition, it can be difficult to show closure under the operation.

In order to look for homomorphisms that can be easily checked for closure, we will focus on *isogenies*, group homomorphisms that perform rational operations on all points (x, y). Before we look at any examples, it should be noted that any map from C to itself that sends $\mathcal{O}$ to $\mathcal{O}$ is an endomorphism [3, III.4.8].

Example 2.8. The map

$$\begin{aligned} \varphi : C(\mathbb{C}) &\longrightarrow C(\mathbb{C}) \\ (x, y) &\longrightarrow \quad (x, -y) \end{aligned}$$

is an isogeny. This works for any elliptic curve C, which makes sense because C is even with respect to y.

Example 2.9. For the curves

$$C : y^2 = x^3 + ax^2 + bx \quad \text{and} \quad C' : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$$

$$\Phi : C(\mathbb{C}) \longrightarrow C'(\mathbb{C}) \qquad (x, y) \longrightarrow \quad \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2} \right)$$

is an isogeny. [2]

Recall that a curve C has *complex multiplication* if there exists an isogeny $\varphi : C \longrightarrow C$ that is not the multiplication-by-n map. We also refer to φ as a *complex multiplication* map on C. Before explaining the importance of this, we will give a few examples.

Example 2.10. Why isn't any curve C have the complex multiplication φ? After all, $\varphi(\mathcal{O}) = \mathcal{O}$, and for any $(x, y) \in C$, $(x, -y) \in C$) as well, so φ must be an endomorphism on C. The reason is that $\varphi(P) = -P$, making it the multiplication-by-(-1) map. In other words, $(x, -y) = -(x, y)$ for all $(x, y) \in C$. The reader can use curve addition to verify that $(x, y)+(x, -y) = \mathcal{O}$, or peruse an illustration of curve addition, to see why this is true.

Example 2.11. The curve $C : y^2 = x^3 + bx$ has the complex multiplication

$$\begin{aligned} \varphi : \quad C \quad &\longrightarrow \quad C \\ (x, y) \quad &\longmapsto \quad (-x, iy). \end{aligned}$$

$\varphi(\mathcal{O}) = \mathcal{O}$, meaning φ is a homomorphism. In addition, for any point (x, y) on C,

$$\varphi(-y^2 = x^3 + x) \Rightarrow (iy)^2 = -x^3 - x = (-x)^3 + (-x),$$

or simply, $y^2 = x^3 + x$. φ is an endomorphism. This means that $\mathrm{im}(\varphi) = C$. To show $\varphi(x, y) \neq n(x, y)$ for any n, we compare their kernels. $\mathrm{Ker}(\varphi) = \mathcal{O}$, but the $\mathrm{Ker}(\lambda_n) = C[n] = \mathcal{O}$ if and only if $n = \pm 1$. $\varphi \neq \lambda_{\pm 1}$, so φ is a complex multiplication map on C.

We want to understand curves that have complex multiplication and see how they differ from curves that do not. We proved earlier that there is an isomorphism ψ between $C(\mathbb{C})$, the complex points on an elliptic curve, and $\mathbb{C}/L$, the complex numbers modulo the lattice L. Using an isogeny $\varphi : C(\mathbb{C}) \to C(\mathbb{C})$ and the previous isomorphism ψ, we create a map

$$\begin{aligned} f : \quad \mathbb{C}/L \quad &\longrightarrow \quad \mathbb{C}/L \\ f(z) = \psi^{-1} \circ \varphi \circ \psi(z) & \end{aligned}$$

that is a meromorphic homomorphism. ψ has a single pole at $z = 0$ (since $\psi(0) = \mathcal{O}$), so we need to see whether or not f is holomorphic at 0. Since f is holomorphic at all $z \neq 0 \in \mathbb{C}$, we can express $f(z)$ as an infinite series,

i.e., $f(z) = a_0x^0 + a_1x^1 + a_2x^2 + ...$ We also know f is a homomorphism at all points z_1 and z_2 not equal to 0. So

$$f(z_1 + z_2) = f(z_1) + f(z_2)$$

for all z_1, z_2 near 0. Since we are in the group $\mathbb{C}/L$, we can also say

$$\begin{aligned} f((z_1 + z_2) + 0) &= f(z_1 + z_2) + f(0) \\ &= f(z_1) + f(z_2) + f(0), \end{aligned}$$

but since f is a homomorphism, we know $f(0) = 0$. This implies that

$$f(z_1 + z_2) = f(z_1) + f(z_2)$$

for all z_1, $z_2 \in \mathbb{C}/L$. [2]

Theorem 2.12. *If f is a holomorphic function (including at $z = 0$), then $f(z) = cz$ for some $c \in \mathbb{C}$.*

Proof: Use the definition of the derivative and the fact that $f(0) = 0$.□ [2]

Remark 2.13. This does not just apply to f, but to any elliptic function [4, p. 431] ($\wp$ is one such function).

If c were a fraction or an irrational number, cz would not be an element of $\mathbb{C}/L$. Therefore either $c \in \mathbb{Z}$ (in which case, φ is the multiplication-by-n homomorphism), or $c \in \mathbb{C} \setminus \mathbb{R}$ (with φ being a complex multiplication map).

Before continuing down this path, we will discuss matrix representations of $\mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q})$ and conclude the next section with Serre's Theorem, which ties representation theory together with complex multiplication.

3 Galois Representations

Having defined $\mathbb{Q}(C[n])$ to be equal to $\mathbb{Q}(x_1, y_1, ...x_{n^2}, y_{n^2})$, where $(x_i, y_i) \in C[n]$ for all i, we now wish to understand its Galois group, $\mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q})$. Usually, we can do this by examining x_i and y_i for all i. However, simply looking at the values of points on an elliptic curve can be confusing (see Example 2.1). If we could somehow convert the elements of the Galois group into something more familiar, we could easily see whether or not $\mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q})$

is abelian, and to which group it is isomorphic. As a result, this section will explain how to represent $\mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q})$ as a subgroup of $GL_2(\mathbb{Z}_n)$. We first will reduce the elements of $\mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q})$ to $C[n]$-automorphisms. We then will create an isomorphism from $\mathrm{Aut}(C[n])$ to $GL_2(\mathbb{Z})$.

Theorem 3.1. ***(Galois Representation Theorem)***

$$\rho_n : Gal(\mathbb{Q}(C[n])/\mathbb{Q}) \longrightarrow GL_2(\mathbb{Z}_n)$$

$$\sigma \qquad \longrightarrow \qquad \begin{bmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{bmatrix}$$

is a one-to-one homomorphism.

Proof: Instead of trying to directly relate $\mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q})$ to $GL_2(\mathbb{Z}_n)$, we will first discuss $\mathrm{Aut}(C[n])$, the set of *group* (not field) automorphisms of $C[n]$. In the following lemmas, we will show that $\mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q})$ maps into $\mathrm{Aut}(C[n])$, and then that $\mathrm{Aut}(C[n])$ is isomorphic to $GL_2(\mathbb{Z}_n)$.□

Lemma 3.2. *Any field automorphism $\sigma \in Gal(\mathbb{Q}(C[n])/\mathbb{Q})$ induces a group automorphism $g_\sigma \in Aut(C[n])$, where $g_\sigma(P) = \sigma(P)$. Moreover,*

$$Gal(\mathbb{Q}(C[n])/\mathbb{Q}) \longrightarrow Aut(C[n])$$

$$\sigma \qquad \longmapsto \qquad g_\sigma$$

is one-to-one.

Proof: We previously showed that if $P \in C(\mathbb{C})$ has order n, then $\sigma(P)$ also has order n for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q})$. Therefore, σ acts on elements in $C[n]$ and sends them to other elements in $C[n]$. Because of this, σ induces a group automorphism g_σ from $C[n]$ to itself such that

$$g_\sigma : P \longmapsto \sigma(P).$$

In fact, since σ is completely determined by where it sends the elements of $C[n]$, each σ maps to a unique $g \in \mathrm{Aut}(C[n])$. Therefore, the map

$$\varphi : \mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q}) \longrightarrow \mathrm{Aut}(C[n])$$

$$\sigma \qquad \longmapsto \qquad g_\sigma$$

is one-to-one. Another, more formal proof involves showing that $Ker(\varphi) = \{\mathrm{id}\}$, where $\mathrm{id} \in \mathrm{Gal}(\mathbb{Q}(C[n]/\mathbb{Q}))$ is the identity map. With composition of functions as the operation, one can show φ is a homomorphism.□

Remark 3.3. Even though $\mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q}) = \mathrm{Aut}(\mathbb{Q}(C[n])$, we still needed to prove that φ is a one-to-one map, because we are going from a field homomorphism to a group homomorphism. In other words, we are mapping $\mathrm{Aut}(C[n])$, not $\mathrm{Aut}(\mathbb{Q}(C[n])$. The reason this map is not onto is because there are $n!$ group automorphisms in $\mathrm{Aut}(C[n])$, while there are $\leq n!$ automorphisms comprising $\mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q})$.

Lemma 3.4.

$$\begin{aligned} \upsilon_n : Aut(C[n]) &\longrightarrow GL_2(\mathbb{Z}_n). \\ g \qquad &\longrightarrow \qquad \begin{bmatrix} \alpha_g & \beta_g \\ \gamma_g & \delta_g \end{bmatrix} \end{aligned}$$

is an isomorphism.

Proof: Remember that $C[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$ and therefore has two generators P_1 and P_2. In other words, any element in $C[n]$ can be uniquely written as $aP_1 + bP_2$, where $a, b \in \mathbb{Z}_n$. So, for any group homomorphism

$$g : C[n] \longrightarrow C[n]$$

we have

$$g(P) = g(aP_1 + bP_2) = ag(P_1) + bg(P_2),$$

meaning g is completely determined by $\sigma(P_1)$ and $\sigma(P_2)$.

Of course, since $g(P_1)$ and $g(P_2)$ are both elements of $C[n]$, they too can be uniquely expressed in terms of P_1 and P_2.

$$g(P_1) = \alpha_g g(P_1) + \gamma_g g(P_2),$$

$$g(P_2) = \beta_g g(P_1) + \delta_g g(P_2).$$

Expressing this in terms of matrices, we get

$$(g(P_1), g(P_2)) = (P_1, P_2) \begin{bmatrix} \alpha_g & \beta_g \\ \gamma_g & \delta_g \end{bmatrix}.$$

Therefore, we can create a map

$$\begin{aligned} \upsilon_n : \mathrm{Aut}(C[n]) &\longrightarrow M_{2x2}(\mathbb{Z}_n) \\ g \qquad &\longmapsto \qquad \begin{bmatrix} \alpha_g & \beta_g \\ \gamma_g & \delta_g \end{bmatrix} \end{aligned}$$

between homomorphisms and matrices. However, we can reduce $M_{2x2}(\mathbb{Z}_n)$ to $GL_2(\mathbb{Z}_n)$, because υ_n is a homomorphism under composition of functions. The reader can check that

$$\begin{bmatrix} \alpha_{g\circ h} & \beta_{g\circ h} \\ \gamma_{g\circ h} & \delta_{g\circ h} \end{bmatrix} = \begin{bmatrix} \alpha_g & \beta_g \\ \gamma_g & \delta_g \end{bmatrix} \begin{bmatrix} \alpha_h & \beta_h \\ \gamma_h & \delta_h \end{bmatrix}$$

for any group homomorphisms g and h.

Furthermore, for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q})$, there exists σ^{-1} such that $\sigma\sigma^{-1} = \mathrm{id}$. If $h : P \longmapsto \sigma(P)$, then $h^{-1} : P \longmapsto \sigma^{-1}(P)$. $\sigma\sigma^{-1}$ relates to $h \circ h^{-1}$, and by the previous lemma, $h \circ h^{-1}$ corresponds to

$$\begin{bmatrix} \alpha_g & \beta_g \\ \gamma_g & \delta_g \end{bmatrix} \begin{bmatrix} \alpha_g^{-1} & \beta_g^{-1} \\ \gamma_g^{-1} & \delta_g^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

This means all of our matrices related to group homomorphisms are invertible as well, and therefore belong to $GL_2(Z_n)$. Only the identity homomorphism will give you the identity matrix, so υ_n is one-to-one. In the reverse direction, for any matrix

$$\begin{bmatrix} \alpha_h & \beta_h \\ \gamma_h & \delta_h \end{bmatrix} \in GL_2(\mathbb{Z}_n)$$

there exists a map $h \in \mathrm{Aut}(C[n])$ such that

$$h(P_1) = \alpha_h h(P_1) + \gamma_h h(P_2),$$

$$h(P_2) = \beta_h h(P_1) + \delta_h h(P_2),$$

meaning υ_n is onto.□ [2]

Remark 3.5. Combining Lemmas 3.2 and 3.4 proves Theorem 3.1. Note that we could have proved that $Hom(C[n], C[n]) \cong M_{2x2}(\mathbb{Z}_n)$, but we only wanted to focus on $GL_2(\mathbb{Z}_n)$. This is often the case, since groups only have invertible elements, as does $GL_2(\mathbb{Z}_n)$ under matrix multiplication.

The study of using matrices to describe groups is *representation theory*. The general idea is that matrices are often easier to analyze than the group elements they represent. This is one such case. Now, instead of trying to manage complex group elements , we can look at a set of matrices and have an intuitive idea of the group structure.

Example 3.6. Consider the elliptic curve

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

and the set $C[2]$ of points on C with order 2. In other words, we need to find points (x, y) such that $y = 0$. We find that

$$C[2] = \{\mathcal{O}, (\sqrt[3]{2}, 0), (\zeta\sqrt[3]{2}, 0), (\zeta^2\sqrt[3]{2}, 0)\} = \{\mathcal{O}, P_1, P_2, P_1 + P_2\}$$

where $\zeta = -\frac{1}{2} + \frac{\sqrt{3}i}{2} = \sqrt[3]{1}$. Since $C[2]$ has both $\sqrt[3]{2}$ by itself and as a product with $\sqrt{3}i$, $\mathbb{Q}(C[2]) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$. This means that $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)/\mathbb{Q})$ has order 6, and it permutes the three points in $C[2]$. Therefore $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)/\mathbb{Q})$ is generated by two automorphisms, σ and τ, with the properties:

$$\sigma(\sqrt{3}i) = \sqrt{3}i, \qquad \tau(\sqrt{3}i) = -\sqrt{3}i$$

$$\sigma(\sqrt[3]{2}) = \zeta\sqrt[3]{2}, \qquad \tau(\sqrt[3]{2}) = \sqrt[3]{2}.$$

Rather than figuring out the group structure using σ and τ, we can instead convert these maps into matrices. Since $\sigma(P_1) = P_2$ and $\sigma(P_2) = P_1 + P_2$, by our previous theorem we can represent σ as $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. By the same logic, we can write τ as $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Now, since υ_n is a homomorphism, we can represent any element of $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)/\mathbb{Q})$ as a matrix. For example, $\tau\sigma = \sigma^2\tau$, so $\upsilon_n(\tau\sigma) = \upsilon(\sigma^2\tau) \to \upsilon(\tau)\upsilon(\sigma) = \upsilon(\sigma)^2\upsilon(\tau) \to \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. With a little more work, we see this group is isomorphic to S_3, which is non-abelian.

By turning our group elements into matrices, we can quickly tell whether or not our group is abelian, and we can obtain the structure of the group easily once we find its generators. Of course, we are looking for elliptic curves whose Galois groups are abelian for all $n \geq 2$, so we can forget about the previous curve. Notice that in this case, $\mathrm{Gal}(\mathbb{Q}(C[2])/\mathbb{Q}) \cong GL_2(\mathbb{Z}_2)$. In general, whenever $\mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q}) \cong GL_2(\mathbb{Z}_n)$, we know the curve does not give an abelian Galois group. $GL_2(\mathbb{Z}_n)$ is never abelian for $n \geq 2$ because the matrices $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ are both in $GL_2(\mathbb{Z}_n)$ and do not commute with each other. Therefore, we do not consider any curves that are isomorphic to $GL_2(\mathbb{Z}_n)$ for *any* $n \geq 2$.

Theorem 3.7. ***(Serre's Theorem)*** *For any elliptic curve C that does not have complex multiplication, for a certain sufficiently large $p \in \mathbb{Z}$ (that is determined by C), if $gcd(p, n) = 1$, then $Gal(\mathbb{Q}(C[n])/\mathbb{Q}) \cong GL_2(\mathbb{Z}_n)$.*

In other words, we disregard curves without complex multiplication.

4 Kronecker's Jugendtraum for $\mathbb{Q}(i)$

$C : y^2 = x^3 + x$ has complex multiplication φ, where

$$\varphi : C \longrightarrow C$$

$$(x, y) \longmapsto (-x, iy)$$

has a peculiar property. Notice that for any field automorphism $\sigma \in \text{Gal}(\mathbb{Q}(i)(C[n])/\mathbb{Q})$,

$$\sigma(\varphi(x, y)) = \sigma(-x, iy) = (-\sigma(x), \sigma(i)\sigma(y))$$

and

$$\varphi(\sigma(x, y)) = \varphi(\sigma(x), \sigma(y)) = (-\sigma(x), i\sigma(y)).$$

This means that $\sigma(\varphi(P)) = \varphi(\sigma(P))$ if and only if $\sigma(i) = i$ for all $\sigma \in \text{Gal}(\mathbb{Q}(i)(C[n])/\mathbb{Q})$. In other words,

$$\sigma(\varphi(x, y)) = \varphi(\sigma(x, y))$$

for all $\sigma \in \text{Gal}(\mathbb{Q}(i)(C[n])/\mathbb{Q}(i))$. The extension $\mathbb{Q}(i)(C[n])$ is Galois over $\mathbb{Q}(i)$ for the same reason $\mathbb{Q}(C[n])$ is Galois over $\mathbb{Q}$.

We can represent both σ and φ as matrices. $\rho_n(\sigma) = \begin{bmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{bmatrix}$,and let S be the subgroup of $GL_2(\mathbb{Z}_n)$ corresponding to $\text{Gal}(\mathbb{Q}(i)(C[n])/\mathbb{Q}(i))$. Since φ is a field automorphism, it induces a group automorphism ψ on $C[n]$ (see the proof of Theorem 3.2). Therefore, $\upsilon(\psi) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ for $a, b, c, d \in \mathbb{Z}$. Since σ and ψ commute, their corresponding matrices commute as well. This should not immediately imply that S is abelian. If the matrix A corresponding to φ is a *scalar matrix* (a scalar multiple of the identity matrix), then S may not be abelian. This is because every matrix in $GL_2(\mathbb{Z}_n)$ commutes with the identity and its scalar multiples. After proving that A is not in fact such a matrix, we will state why this (nontrivial) commutativity implies that $\text{Gal}(\mathbb{Q}(i)(C[n])/\mathbb{Q}(i))$ is in fact abelian.

Lemma 4.1. *$B \in GL_2(\mathbb{Z}_n)$ is not a scalar multiple of the identity matrix modulo d, for all $d|n$.*

Proof: The corresponding endomorphism φ has the property that $\varphi(\varphi(x,y)) = (-(-x), i(iy)) = (x,-y)$, and thus

$$\varphi(\varphi(P)) = -P.$$

This implies $\upsilon(\varphi(\varphi)) \mapsto -\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$, whose determinant is -1 and therefore is invertible in $GL_2(\mathbb{Z}_n)$.

Now, if we assume B is a scalar matrix (mod d), then we know that φ is really just the multiplication-by-c map for all $P \in C[d]$. Now, consider $\sigma \in$Gal$(\mathbb{Q}(i)(C[d])/\mathbb{Q})$, where $\sigma(i) = -i$ (complex conjugation). We know that this element will always exist in the Galois group, because any element will either fix each element not in $\mathbb{Q}$ or send it to its complex conjugate. Then

$$\sigma(\varphi(x,y)) = (-\sigma(x), -i\sigma(y)) = -\varphi(\sigma(x,y)).$$

So $2\sigma(\varphi(P)) = 2\varphi(\sigma(P)) = 2c(\sigma(P))$. In particular,

$$2cP = \mathcal{O}$$

for all $P \in C[d]$, since σ is an automorphism. Therefore $C[d] = C[2]$, or $d|c$. But if $d|c$,

$$\varphi(P) = dP = \mathcal{O}$$

for all $P \in C[d]$, and this is clearly not the case. The reader can check using the generators $P_1 = (0,0)$ and $P_2 = (i,0)$ that the matrix corresponding to $C[2]$ is $\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix} \neq \begin{bmatrix}d & 0\\ 0 & d\end{bmatrix}$, which means B is not a scalar matrix.□

While we have shown that φ is a non-scalar matrix that commutes with Gal$(\mathbb{Q}(i)(C[n])/\mathbb{Q}(i))$, this is still not enough to show that the group is abelian. After all, there is no reason to think that φ is actually an element of the Galois group, and in fact, it often will not be. However, one can use linear algebra to prove the following lemma. [2]

Lemma 4.2. *All matrices $A \in GL_2(\mathbb{Z}_n)$ that commute with $B = \begin{bmatrix}a & b\\ c & d\end{bmatrix}$ commute with each other, assuming $B \not\equiv cI_2$ (mod d) for some $d|n$. Furthermore, the set of all such matrices A forms an abelian subgroup H of $GL_2(\mathbb{Z}_n)$.*

The proof [2, p. 210] of this lemma uses only linear algebra, and not complex multiplication at all. Since it is not particularly relevant, we will omit it.

Based on the previous two lemmas, we now know that $\mathrm{Gal}(\mathbb{Q}(i)(C[n])/\mathbb{Q}(i))$ maps into the abelian subgroup $H < GL_2(\mathbb{Z}_n)$. Therefore, for $C : y^2 = x^3+x$, $\mathbb{Q}(i)(C[n])$ is an abelian extension over $\mathbb{Q}(i)$. Using the exact same reasoning as above, we can show that $\mathbb{Q}(\sqrt{3}i)(C[n])$ is an abelian extension over $\mathbb{Q}(\sqrt{3}i)$ for $C : y^2 = x^3 + 1$. However, the Jugendtraum has only been solved for $\mathbb{Q}(i)$.

Theorem 4.3. *Consider the elliptic curve $C : y^2 = x^3+x$. Gal($\mathbb{Q}(i)(C[n])/\mathbb{Q}(i)$) is abelian. In addition, if K is any abelian extension of $\mathbb{Q}(i)$, then*

$$K \subseteq \mathbb{Q}(i)(C[n])$$

for some positive integer n.

While the proof is beyond the scope of this paper, the implications of this theorem are powerful. The same way $\mathbb{Q}(\zeta)$ contained any abelian extension of $\mathbb{Q}$ for some root of unity, $\mathbb{Q}(i)(C[n])$ contains any abelian extension of $\mathbb{Q}(i)$ for some n. The reader may recall that $\mathbb{Q}(\zeta) = \mathbb{Q}(f(x_1, ..., x_m))$ for $f(x) = e^{\frac{2\pi i}{x}}$ and certain integers x_i. In this case, we can express and point in $C[n]$ as $(\wp(\frac{a_1\omega_1}{n} + \frac{a_2\omega_2}{n}), \wp'(\frac{a_1\omega_1}{n} + \frac{a_2\omega_2}{n}))$. Therefore, as with $\mathbb{Q}$, for abelian extensions of $\mathbb{Q}(i)$, we can create the "bound" for all abelian extensions using only a single function.

In addition, we can use $\wp$ to describe any automorphism $\sigma \in \mathrm{Gal}\mathbb{Q}(i)(C[n])$. Recall that σ only permutes x and y values of points in $C[n]$. This means

$$\begin{aligned}
\sigma(P) &= \sigma(x, y) && (3)\\
&= \sigma(\wp(\frac{a_1\omega_1}{n} + \frac{a_2\omega_2}{n}), \wp'(\frac{a_1\omega_1}{n} + \frac{a_2\omega_2}{n})) && (4)\\
&= \sigma(a_1P_1 + a_2P_2, b_1P_1 + b_2P_2) && (5)\\
&= (a_1\sigma(P_1) + a_2\sigma(P_2), b_1\sigma(P_1) + b_2\sigma(P_2)). && (6)\\
& && (7)
\end{aligned}$$

But remember from Section 3 that $\sigma(P_1) = \alpha P_1 + \gamma P_2$ and $\sigma(P_2) = \beta P_1 + \delta P_2$

with α, β, γ, and $\delta \in \mathbb{Z}_n$. Substituting, we get

$$\sigma(P) = (a_1\sigma(P_1) + a_2\sigma(P_2), b_1\sigma(P_1) + b_2\sigma(P_2)) \tag{8}$$
$$= (a_1(\alpha P_1 + \gamma P_2) + a_2(\beta P_1 + \delta P_2), b_1(\alpha P_1 + \gamma P_2) + b_2(\beta P_1 + \delta P_2)). \tag{9}$$
$$\tag{10}$$

Remember that P_1 and P_2 correspond with $\wp(\frac{\omega_1}{n})$ and $\wp(\frac{\omega_2}{n}) \in \mathbb{C}$, respectively (see Theorem 2.4 and Corollary 2.5). So

$$\sigma(P) = (a_1(\alpha\frac{\omega_1}{n} + \gamma\frac{\omega_2}{n}) + a_2(\beta\frac{\omega_1}{n} + \delta\frac{\omega_2}{n}), \tag{11}$$
$$b_1(\alpha\frac{\omega_1}{n} + \gamma\frac{\omega_2}{n}) + b_2(\beta\frac{\omega_1}{n} + \delta\frac{\omega_2}{n})). \tag{12}$$

Therefore, this is the Jugendtraum for $\mathbb{Q}(i)$.

5 Conclusion: the Jugendtraum for Other Fields

Mathematicians have proved Kronecker's Jugendtraum for all fields $\mathbb{Q}(\sqrt{-D})$ for all positive integers D such that $\sqrt{D}$ is not an integer. [6] The single function that describes the "bounding" number field and Galois group is called the *j-function*, used by Kronecker, Gauss, Weber, and Hermite in the mid-1800's. [6] It is too complicated to even write down in this paper, unfortunately. Still, Kronecker's Jugendtraum is unsolved except for these general cases. It is interesting that the j-function works only for imaginary extensions of $\mathbb{Q}$, since one usually considers imaginary numbers to be more difficult to understand than real numbers.

If I had more time to research this topic, I would have liked to at least begin to understand the j-function, its different representations, [6] and how it applies to elliptic curves. I also am interested in how this works with modular forms in determining Ramanujan's constant $e^{pi\sqrt{163}} = 12^3(231^2 - 1)^3 + 743.9999999999925007....$ [7] It fascinates me that using three irrational numbers, two of which are transcendental, gives us a number so close to an integer, and that one could derive such a concept from elliptic curves. I also would have liked to see if there were a way of determining the complex multiplication of any given elliptic curve, or if such a goal is even possible.

References

[1] Hungerford, Thomas W. *Algebra*, Springer Science+Business Media, LLC, New York, 1974.

[2] Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves*, Springer Science+Business Media, LLC, New York, 1974

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

[4] E.T. Whittaker and G.N. Watson *A Course of Modern Analysis*, Cambridge University Press, London, 1958

[5] Weierstrass, Karl. *Mathematische Werke II*, Georg Olms Verlagsbuchhandlung, Hildsheim, 1895 (reprinted by Johnson Reprint Corporation, New York, year unknown)

[6] Tito Piezas III. *www.mathworld.wolfram.com/j-Function.html*

[7] Tito Piezas III. *www.mathworld.wolfram.com/RamanujanConstant.html*