Elliptic Curves, Complex Tori, Modular Forms, and ℓ-adic Galois Representations

Benjamin Church

July 13, 2020

Contents

1 Introduction

Elliptic curves are one of the most important objects in modern mathematics. They provide a clear link between geometry, number theory, and algebra. Such objects appear naturally in the study of Diophantine equations and of complex analysis and are vital to the proofs of many famous theorems in number theory such as Fermat's Last theorem. Elliptic curves are so-called one-dimensional projective varieties of genus one meaning they are curves living in projective space defined by a cubic equation.

Definition: Let K be a field then n-dimensional projective space over K is defined by,

$$\mathbb{P}^n(K) = (K^{n+1} \setminus \{0\})/K^\times$$

We write the coordinates as,

$$[X_0 : \cdots : X_n] = [\lambda X_0 : \cdots : \lambda X_n]$$

where $\lambda \in K^\times$.

Definition: An *elliptic curve* E defined over a field K is a smooth projective curve defined by the inhomogeneous equation,

$$y^2 = x^3 + ax + b$$

for $a, b \in K$, that is, for any field L/K, we define,

$$E(L) = \left\{(x, y) \in L^2 \mid y^2 = x^3 + ax + b\right\} \cup \{O\} \subset L^2$$

The distinguished point O is viewed as the "point at infinity." We can express E as a projective curve in $\mathbb{P}^3(L)$ by the homoegenized equation,

$$ZY^2 - X^3 - aZ^2Y - bZ^3 = 0$$

where we identify the points with $Z \neq 0$ such that,

$$[X : Y : Z] = [X/Z : Y/Z : 1]$$

with (x, y) for $x = X/Z$ and $y = Y/Z$. Furthermore we identify the unique point $[X : Y : 0]$ on E with O. Usually, we will either take K to be algebraically closed or define the points E to be $E(\bar{K})$ where $\bar{K}$ denotes the algebraic closure, then $E(L) = E \cap L$ which is exactly the set of fixed points of E under the action of $\mathrm{Gal}\left(\bar{K}/L\right)$.

We will return to the geometric development of elliptic curves. However, we will begin with the complex analyic picture in which an elliptic curve will, somewhat suprisingly, naturally arise.

2 Elliptic Functions

On the real line, analytic periodic functions like sinusoids have wonderful properties are are intimately related to the points quadratic curves i.e. circles. We might naturally ask: "what is the analogue of a periodic function on the complex plane?" The following is one such notion.

Definition: A function $f : \mathbb{C} \to \mathbb{C}$ is *doubly periodic* or *elliptic* if there exits two independent (not real multiples of each other) complex numbers ω_1 and ω_2 such that,

$$f(z + \omega_1) = f(z) \quad \text{and} \quad f(z + \omega_2) = f(z)$$

We define the lattice of periods,

$$\Lambda = \{n\omega_1 + m\omega_2 \mid n, m \in \mathbb{Z}\}$$

so that $f(z + \omega) = f(z)$ for all $\omega \in \Lambda$ so f factors as a function on the quotient $f : \mathbb{C}/\Lambda \to \mathbb{C}$.

Remark 2.1. The space $\mathbb{C}/\Lambda$ is topologically a torus. It is equivalent to the "fundamental parallelogram"

$$\{\alpha\omega_1 + \beta\omega_2 \mid \alpha, \beta \in [0,1]\}$$

with opposite edges identified. This is the standard construction of a torus. However, different lattices Λ will put a different complex structure on $\mathbb{C}/\Lambda$ which we therefore call a complex torus.

We would want to consider elliptic homomorphic functions. However, a classical theorem in complex analysis poses a difficulty.

Theorem 2.1 (Liouville)**.** Every bounded entire[1] function is constant.

Proof. Let $f : \mathbb{C} \to \mathbb{C}$ be entire and bounded everywhere by M. Take $w \in \mathbb{C}$ and let C be a circle arround z with radius R. Then applying the Cauchy integral formula,

$$f'(w) = \frac{1}{2\pi i} \oint_C \frac{f(z)}{(z-w)^2}\,\mathrm{d}z = \frac{1}{2\pi} \int_0^{2\pi} \frac{f(w + Re^{i\theta})}{R^2 e^{2i\theta}} R\,\mathrm{d}\theta$$

Therefore,

$$|f'(w)| = \frac{1}{2\pi}\left|\oint_C \frac{f(z)}{(z-w)^2}\,\mathrm{d}z\right| \leq \frac{1}{2\pi}\int_0^{2\pi} \frac{|f(w+Re^{i\theta})|}{R^2} R\,\mathrm{d}\theta \leq \frac{1}{2\pi}\int_0^{2\pi} \frac{M}{R}\,\mathrm{d}\theta = \frac{M}{R}$$

which goes to zero in the limit $R \to \infty$. Since R is arbitrarily large, $f'(w) = 0$ so f is constant since it has zero derivative everywhere. □

Corollary 2.2. There do not exist nonconstant doubly periodic holomorphic functions.

Proof. Suppose that $f : \mathbb{C} \to \mathbb{C}$ is holomorphic and doubly periodic with periods ω_1 and ω_2. Consider f restricted to the so-called "fundamental domain"

$$D = \{\alpha\omega_1 + \beta\omega_2 \mid \alpha, \beta \in [0,1]\}$$

By using the periodicity, the behavior of f everywhere is determined by its values on D. Since D is compact[2] and f is continuous (since it is holomorphic) it must be bounded[3] on D. Therefore, f is entire and bounded and thus, by Liouville's theorem, constant. □

Our plan has been thwarted as soon as it was devised. Since we cannot find interesting holomorphic examples of elliptic functions we now ask for the next best thing. We want to consider elliptic meromorphic functions. That is, meromorphic functions $f : \mathbb{C}/\Lambda \to \mathbb{C}$. It turns out that now were are in luck. A canonical example of a meromorphic function is z^{-2}. We will try to make such a function periodic. A standard trick is to sum over the entire lattice such that shifts by lattice elements do not effect the sum. We might try,

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

which is doubly periodic because if $\omega \in \Lambda$ then,

$$f(z+\omega) = \sum_{\omega' \in \Lambda} \frac{1}{(z+\omega+\omega')^2} = \sum_{\omega'' \in \Lambda} \frac{1}{(z+\omega'')^2} = f(z)$$

However, this definition has one major flaw. That sum does not converge! To fix this, we use a clever subtraction to remove the divergent part of the sum and arrive at the following definition by Weierstrass.

[1] holomorphic on the entire complex plane

[2] closed and bounded for subsets of Euclidean space

[3] A continuous function on a compact set cannot diverge approaching a point because the set is closed nor diverge off to infinity because the set is bounded.

Theorem 2.3. Let $\Lambda \subset \mathbb{C}$ be a Lattice. The Weierstrass $\wp$-function, defined as,

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda^\times} \left[\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \right]$$

is a well-defined meromorphic function $\wp : \mathbb{C}/\Lambda \to \mathbb{C}$ with double poles on Λ.

Proof. We can write,

$$\begin{aligned} \frac{1}{(z+\omega)^2} &= -\frac{\mathrm{d}}{\mathrm{d}z}\left(\frac{1}{z+\omega}\right) = -\frac{1}{\omega}\frac{\mathrm{d}}{\mathrm{d}z}\left[\sum_{n=0}^{\infty}\left(-\frac{z}{\omega}\right)^n\right] = -\frac{1}{\omega}\sum_{n=0}^{\infty}\left[\frac{(-1)^n n z^{n-1}}{\omega^n}\right] \\ &= \frac{1}{\omega^2}\left[\sum_{n=0}^{\infty}(-1)^n(n+1)\frac{z^n}{\omega^n}\right] \end{aligned}$$

and this series is uniformly convergent for $|z| < |\omega|$. Thus,

$$\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\sum_{n=1}^{\infty}(-1)^n(n+1)\frac{z^n}{\omega^n}$$

and therefore,

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda^\times} \left[\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \right]$$

converges uniformly. Furthermore,

$$\wp'(z) = -\frac{2}{z^3} + \sum_{\omega \in \Lambda^\times}\left(-\frac{2}{(z+\omega)^3}\right) = -2\sum_{\omega \in \Lambda}\frac{1}{(z+\omega)^3}$$

Thus, $\wp'(z)$ is doubly periodic with periods ω_1 and ω_2. Thus, $\wp(z+\omega_1) = \wp(z) + c_1$ so $\wp(-\frac{1}{2}z_1) = \wp(\frac{1}{2}z) + c_1$ but $\wp$ is even so $c_1 = 0$. The same for ω_2. Thus, $\wp(z+\omega_1) = \wp(z)$ and $\wp(z+\omega_2) = \wp(z)$. □

2.1 The Defining Differential Equation for $\wp$

We need to work out he expansion for $\wp(z)$ near 0. We have,

$$\frac{1}{(z-\omega)^2} = \frac{1}{\omega^2}\cdot\frac{1}{(1-\frac{z}{\omega})^2} = \frac{1}{\omega^2}\sum_{n=0}^{\infty}(m+1)\left(\frac{z}{\omega}\right)^m$$

Therefore,

$$\begin{aligned} \wp(z) &= \frac{1}{z^2} + \sum_{\omega \in \Lambda^\times}\sum_{m=1}^{\infty}(m+1)\frac{z^m}{\omega^{m+2}} \\ &= \frac{1}{z^2} + \sum_{m=1}^{\infty}(m+1)z^m\left(\sum_{\omega \in \Lambda^\times}\frac{1}{\omega^{m+2}}\right) \\ &= \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)z^{2k}G_{k+1}(\Lambda) \end{aligned}$$

where we have defined,

$$G_k(\Lambda) = \sum_{\omega \in \Lambda^\times}\frac{1}{\omega^{2k}}$$

The odd terms vanish because if we sum an odd function over the lattice then we get zero. Explicitly,

$$\wp(z) = \frac{1}{z^2} + 3G_2(\Lambda)z^2 + 5G_3(\Lambda)z^4 + O(z^6)$$

Next,

$$\wp'(z) = -\frac{2}{z^3} + \sum_{k=1}^{\infty}(2k+1)(2k)G_{k+1}(\Lambda)z^{2k-1}$$

which we sum as,

$$\wp'(z) = -\frac{2}{z^3} + 6G_2(\Lambda)z + 20G_3(\Lambda)z^3 + O(z^5)$$

Thus, compute,

$$\begin{aligned}\wp'(z)^2 &= \left(-\frac{2}{z^3} + 6G_2(\Lambda)z + 20G_3(\Lambda)z^3 + O(z^5)\right)^2 \\ &= \frac{4}{z^6} - 24G_2(\Lambda)\frac{1}{z^2} - 80G_3(\Lambda) + O(z^2)\end{aligned}$$

Similarly, compute,

$$\begin{aligned}\wp(z)^3 &= \left(\frac{1}{z^2} + 3G_2(\Lambda)z^2 + 5G_3(\Lambda)z^4 + O(z^6)\right)^3 \\ &= \frac{1}{z^6} + 9G_2(\Lambda)\frac{1}{z^2} + 15G_3(\Lambda) + O(z^2)\end{aligned}$$

Therefore,

$$\begin{aligned}\wp'(z)^2 - 4\wp(z)^3 &= -24G_2(\Lambda)\frac{1}{z^2} - 36G_2(\Lambda)\frac{1}{z^2} - 80G_3(\Lambda) - 60G_3(\Lambda) + O(z^2) \\ &= -60G_2(\Lambda)\frac{1}{z^2} - 140G_3(\Lambda) + O(z^2)\end{aligned}$$

Which implies that,

$$\wp'(z)^2 - 4\wp(z)^3 + 60G_2(\Lambda)\wp(z) + 140G_3(\Lambda) = O(z^2)$$

Therefore the function,

$$\wp'(z)^2 - 4\wp(z)^3 + 60G_2(\Lambda)\wp(z) + 140G_3(\Lambda)$$

is holomorphic on $\mathbb{C}$ and is doubly periodic and thus constant. However, it vanishes at $z = 0$ and thus must be the zero function. Therefore, we have the differential equation,

$$\wp'(z)^2 - 4\wp(z)^3 + 60G_2(\Lambda)\wp(z) + 140G_3(\Lambda) = 0$$

We can interpret this differential equation as telling us that the image of the elliptic Weierstrass $\wp$-function lies on a special type of object called an elliptic curve.

Definition: An *elliptic curve* E defined over a field K is a smooth projective curve defined by the inhomogeneous equation,

$$y^2 = x^3 + ax + b$$

for $a, b \in K$, that is, for any field L/K, we define,

$$E(L) = \left\{(x, y) \in L^2 \mid y^2 = x^3 + ax + b\right\} \cup \{O\} \subset L^2$$

The distinguished point O is viewed as the "point at infinity." We can express E as a projective curve in $\mathbb{P}^3(L)$ by the homoegenized equation,

$$ZY^2 - X^3 - aZ^2Y - bZ^3 = 0$$

where we identify the points with $Z \neq 0$ such that,

$$[X : Y : Z] = [X/Z : Y/Z : 1]$$

with (x, y) for $x = X/Z$ and $y = Y/Z$. Furthermore we identify the unique point $[X : Y : 0]$ on E with O. Usually, we will either take K to be algebraically closed or define the points E to be $E(\bar{K})$ where $\bar{K}$ denotes the algebraic closure, then $E(L) = E \cap L$ which is exactly the set of fixed points of E under the action of $\mathrm{Gal}\left(\bar{K}/L\right)$.

Define $g_2 = 60G_2(\Lambda)$ and $g_3 = 140G_3(\Lambda)$. Then we have the fundamental differential equation,

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

Let E be the Elliptic curve over $\mathbb{C}$ defined by the equation,

$$y^2 = x^3 - (g_2/4)x - (g_3/4)$$

then, we see that the Weierstrass $\wp$-function gives a map to this elliptic curve $\Phi_\wp : \mathbb{C}/\Lambda \to E$ given by,

$$z \mapsto [\wp(z), \wp'(z)/2, 1]$$

unless $\wp(z)$ has a pole at z i.e. $z \in \Lambda$ in which case we send z to the "point at infinity" via $z \to [0:1:0]$.

2.2 The Abel Map

The defining differential equation implies that,

$$\int_0^z \frac{\wp'(z)\,\mathrm{d}z}{\sqrt{4\wp(z)^3 - g_2\wp(z) - g_3}} = z$$

Let $u = \wp(z)$ then we have,

$$\int_\infty^{\wp(z)} \frac{\mathrm{d}u}{\sqrt{4u^3 - g_2u - g_3}} = z$$

Thus if we introduce the elliptic integral,

$$E(v) = \int_\infty^v \frac{\mathrm{d}u}{\sqrt{4u^3 - g_2u - g_3}}$$

then we have,

$$E(\wp(z)) = z$$

This elliptic function is known as the Abel map on the elliptic curve. This is inverse to the Wierstrass $\wp$-function. I claim that the Wierstrass $\wp$-function gives a bijection between the complex points of E and the torus $\mathbb{C}/\Lambda$ because the elliptic integral provides an inverse.

3 The Group Law

The truly remarkable thing about the identification via the Weierstrass $\wp$-function of the complex torus $\mathbb{C}/\Lambda$ with the complex points of an elliptic curve is that the complex torus $\mathbb{C}/\Lambda$ naturally has an abelian group structure under the usual addition of complex numbers modulo Λ. This allows us to define an abelian group structure on E as follows. For points $P, Q \in E$, define the analytic group law via,

$$P + Q = \Phi_\wp(\Phi_\wp^{-1}(P) + \Phi_\wp^{-1}(Q))$$

where "+" on the right denotes the usual addition of complex numbers in $\mathbb{C}/\Lambda$. This abelian group law turns E into a very special type of algebraic geometric object called an *abelian variety*.

Now we should investigate the possible geometric interpretations of such a group operation on E.

Lemma 3.1. A line intersects a planar cubic curve at exactly three points (counting multiplicity).

Proof. The linear equation alows us to write y in terms of x. Then the defining equation of the cubic curve reduces to a cubic in x which has exactly three solutions. □

Remark 3.1. We define the points of the curve E always over $\bar{K}$, the algebraic closure, to ensure that there are always enough solutions.

Definition: Let E be an elliptic curve. The *geometric group law* on E with a distinguished point O is defined as follows. For $P, Q \in E$, take the third intersection point $P * Q$, join it to O by a line, and then take the third intersection point to be $P + Q$. In other words, set $P + Q = O * (P * Q)$. In the case that $P = Q$ we define $P * P$ by taking the tangent line at P and the thrid point where it intersects E. The necessity that each point have a well-defined tangent line is one reason we restrict elliptic curves to *nonsingular* cubic curves.

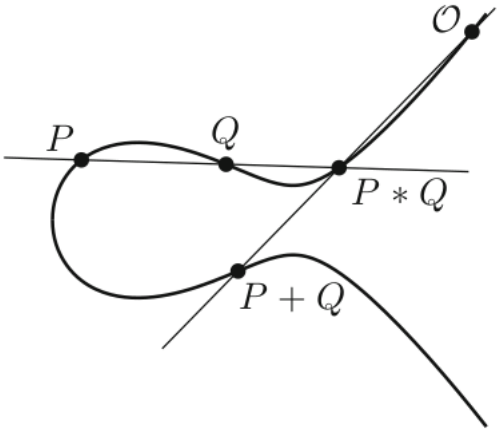

Figure 1: The illustration of addition of *real* points on an elliptic curve.

Lemma 3.2. We have $P * Q = Q * P$ and $P * (P * Q) = Q$.

Proof. Clearly the lines PQ and QP are the same and thus intersect E at the same additional point. Let $S = P * Q$ then P, Q, and S are all three points that the line $PQ = QS = SP$ intersect E at. Thus, $P * S = Q$ since it is the third intersection point. □

Proposition 3.3. The geometric group law on E with respect to O has identity O, is commutative, and admits an inverse, denoted $-P$ for each point P.

Proof. We have $P + O = O * (P * O) = P$. Futhermore, $P * Q = Q * P$ which implies that $P + Q = Q + P$.

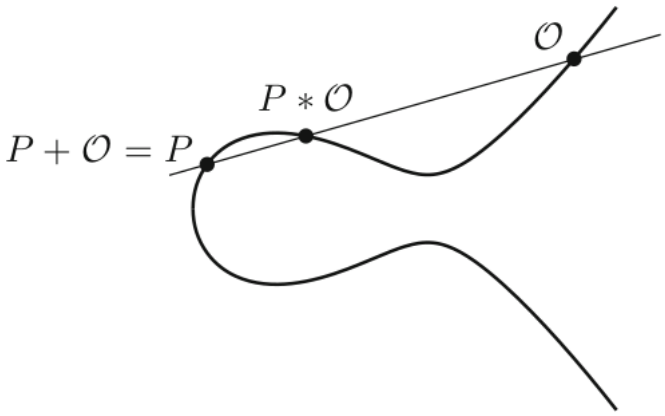

Figure 2: The illustration of the identity on the real points on an elliptic curve.

Next, let $S = O * O$ then define $-P = P * S$. We have, $P + (-P) = O * (P * (P * S))$. However, $P * (P * S) = S$ so $P + (-P) = O * S = O * (O * O) = O$.

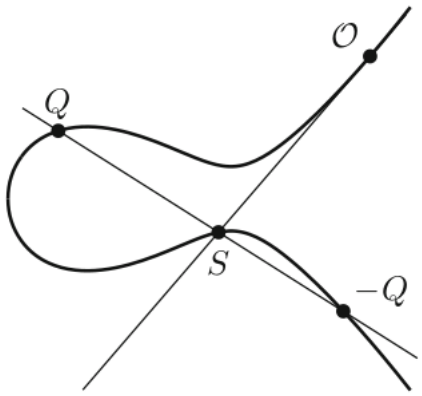

Figure 3: The illustration of inversion of a real point on an elliptic curve.

□

Lemma 3.4. Let C_1 and C_2 be two cubic curves which intersect generically at 9 points. Suppose a cubic curve C intersects C_1 and C_2 at eight of the points then C intersects C_1 and C_2 at all 9 points.

Proof. A generic cubic curve is defined by nine coefficients. The requirement that C intersect C_1 and C_2 at eight points gives eight constraint equations which limit the space of possible curves to a one-dimensional family. Let $F_1(x, y) = 0$ and $F_2(x, y) = 0$ be cubic equations defining C_1 and C_2 then $\lambda_1 F_1(x, y) + \lambda_2 F_2(x, y) = 0$ for arbitrarly λ_1 and λ_2 is at least a one-dimensional family of curves which all pass through the eight defining points. Thus every curve C must be one of these. However, since C_1 and C_2 both pass throught the nineth point F_1 and F_2 vanish there and thus so does $\lambda_1 F_1(x, y)\lambda_2 F_2(x, y)$ which implies that C also passes through the last intersection point. □

Proposition 3.5. The geometric group law is associative. Therefore, $(E, O, +)$ is an abelian group.

Proof. Let $P, Q, R \in E$ be three points on the elliptic curve. Then consider the eight points,

$$O,\ P,\ Q,\ R, P * Q,\ P + Q,\ Q * R,\ Q + R$$

which lie on E and a nineth point N which is the intersection of the lines $(P + Q)R$ and $P(Q + R)$. We want to show that this last point lies on E such that $(P + Q) * R = P * (Q + R)$ which implies that $(P + Q) + R = P + (Q + R)$.

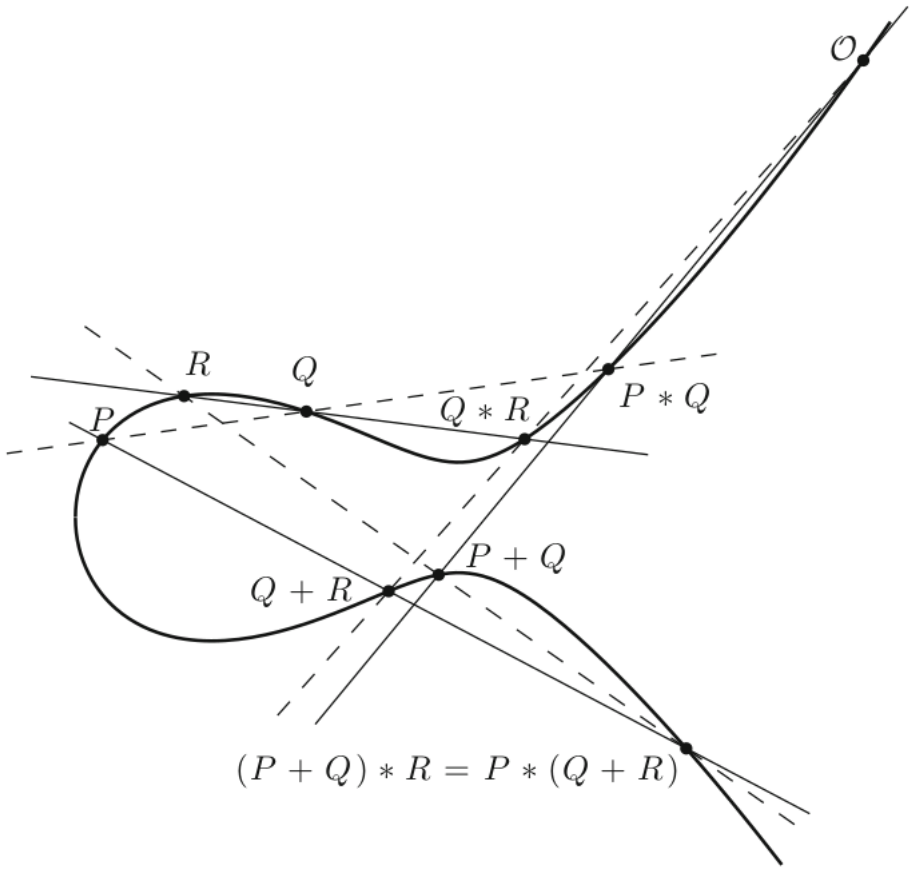

Figure 4: The proof of associatvity of the geometric group law illustrated over the *real* points of an elliptic curve.

The union of three lines is a cubic curve since its defining equation is the product of three linear equations. Call C_1 the union of the solid lines and C_2 the union of the dashed lines. Then, these eight points lie in the intersection of C_1, C_2, and E. Therefore, N, the final nineth intersection point of C_1 and C_2, must also lie on E proving associativity. □

Proposition 3.6. The geometric group law is given by rational functions in the coordinates which makes it a regular map in the algebraic geometry sense. This group law makes the elliptic curve into an abelian variety.

Proof. Suppose we want to add points $P, Q \in E$. Let these points have coordinates $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. We will also write $P * Q = (x_3, y_3)$. Then the line between them has the equation,

$$y = \lambda x + \nu \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$$

We need to intersect this with E which is defined by,

$$y^2 = x^3 + ax + b$$

Therefore we need to solve,

$$(\lambda x + \nu)^2 = x^3 + ax + b$$

which gives,

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\nu)x + b - \nu^2 = 0$$

We know that x_1 and x_2 are solutions to this since they both line on the line at the elliptic curve. Therefore we can factor,

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\nu)x + b - \nu^2 = (x - x_1)(x - x_2)(x - x_3)$$

Therefore, matching x^2 coefficients,

$$\lambda^2 = x_1 + x_2 + x_3$$

which implies that,

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \quad \text{and} \quad y_3 = \lambda x_3 + \nu = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^3 - (2x_1 + x_2)\left(\frac{y_2 - y_1}{x_2 - x_1}\right) + y_1$$

These are clearly rational functions in the coordinates. There are special cases to consider, for example when $P = Q$ and we must take the tanget line or the line PQ is vertical so λ is undefined but all these cases are straigtforward and will give rational functions. □

Proposition 3.7. The geometric group law and the analytic group law coincide.

Proof. Let $\Lambda \subset \mathbb{C}$ be a lattice, E the associated elliptic curve over $\mathbb{C}$ and $\Phi_\wp : \mathbb{C}/\Lambda \to E$ the map induced by the Wierstrass $\wp$-function. For $P \in E$ let $T_P : E \to E$ be the map $Q \mapsto P + Q$. Then define, $\tau_P = \Phi_\wp^{-1} \circ T_P \circ \Phi_\wp : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$. The map τ_P is holomorphic because $\Phi_\wp$ is biholomorphic and T_P is given by rational functions. Let $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ be the projection map and take $g = \tau_P \circ \pi$ which is doubly periodic. Then $g' : \mathbb{C} \to \mathbb{C}$ is a well-defined holomorphic function since, although its image is only defined up to addition by $\omega \in \Lambda$, its derivative is invariant under addition by a constant. Thus, g' is holomorphic and doubly periodic so g' is constant. Thus g is a linear function so $\tau_P = c_P z + d_P$ where c_P and d_P are constants determined by P. Firstly,

$$\tau_P(0) = d_P = \Phi_\wp^{-1} \circ T_P \circ \Phi_\wp(0) = \Phi_\wp^{-1}(T_P(O)) = \Phi_\wp^{-1}(P + O) = \Phi_\wp^{-1}(P)$$

Secondly, since T_A is an automorphism of E and $\Phi_\wp$ is a bijection, τ_P is a map of the fundamental domain D onto itself bijectivly which must preserve area so $|c_P| = 1$. If $c_p \neq 1$ then $c_P z + d_P = z$ has a solution, namely $z = d_P(1 - c_P)^{-1}$ so τ_P has a fixed point. However, if $\tau_P(z) = z$ then

$$T_P \circ \Phi_\wp(z) = \Phi_\wp \circ \tau_P(z) = \Phi_\wp(z)$$

so $\Phi_\wp(z)$ is a fixed point of T_P i.e. $P + \Phi_\wp(z) = \Phi_\wp(z)$ which cannot happen unless $P = O$ since $(E, +)$ is a group. However, in the case $P = O$ we have $T_O = \mathrm{id}_E$ so $\tau(z) = z$. Thus, either way, $c_P = 1$ so $\tau_P(z) = z + \Phi_\wp^{-1}(P)$. Therefore, the geometric group law action T_P is equivalent to a translation $\tau_P(z) = z + \Phi_\wp^{-1}(P)$ on the complex torus. In particular, we defined the analytic group law by,

$$P +_A Q = \Phi_\wp(\Phi_\wp^{-1}(P) + \Phi_\wp^{-1}(Q)) = \Phi_\wp \circ \tau_P \circ \Phi_\wp^{-1}(Q) = T_P(Q) = P +_G Q$$

which equals the geometric group law. □

Remark 3.2. Since we assumed almost nothing about the geometric group law in this proof, we actually proved a far more remarkable fact. We proved that there is a *unique* group law on E whose identity is the distinguished point O and which is regular with respect to $\wp$ in the sense that $\Phi_\wp \circ T_P \circ \Phi_\wp^{-1} : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ is holomorphic. This is true of the geometric group law because it is given by rational functions. This extremely powerful uniqueness shows that there cannot be any other group law on E given by rational functions or even by holomorphic functions in the above sense. Requiring that T_P be a regular map is the defining property of an *algebraic group* or, here in the special case of projective algebraic varieties, of an *abelian variety*. We have shown that the geometry of our elliptic curve determines completely and rigidly the algebraic stucture on it. It is exactly this rigidness which makes the group law on an elliptic curve such a natural and indespensible tool for studying the geometry which uniquely determines it.

4 The Mordell-Weil Theorem

One of the most supprising and powerful theorems in the theory of elliptic curves (and abelian varieties in general) is the Mordell-Weil theorem. This theorem tells us that the structure group structure of the points on an elliptic curve over a number field is especially simple. The theorem is very powerful and I will give it in generality. However, we will only dicuss the special case for elliptic curves defined over $\mathbb{Q}$.

Theorem 4.1 (Mordell-Weil)**.** Let A be an abelian variety defined over a number field K then $A(K)$ the K-points of A form a finitely-generated abelian group.

Theorem 4.2 (Mordell)**.** The case with $A = E$, an elliptic curve, and $K = \mathbb{Q}$ gives that the rational points on an elliptic curve form a finitely generated abelian group i.e there exists finitely many elements $P_1, \ldots, P_k \in E(\mathbb{Q})$ such that any $Q \in E(\mathbb{Q})$ can be written in the form,

$$Q = n_1 P_1 + \cdots + n_k P_k$$

4.1 The Elementary Theory of Heights

The proof of Mordell-Weil will use a suprising idea, the height of a number. A height function is a function which measures the "complexity" of the coordinates of a point. For the case of rational points $E(\mathbb{Q})$, a possible choice is,

$$H(\frac{a}{b}) = \max\{|a|, |b|\}$$

When written in lowest terms. Furthermore, the hieght of a rational point we will simply take to be the height of the x-coordinate. We can construct a similar notion of the height of an algebraic number by measuing the size of the coefficients of the minimal polynomial with integer coefficients that is solves. The fundamental property of a height function is that there are a finite number of points with height less than any fixed bound. This fundamental property will allow us to show that various sets of points are finite given that they have a bounded height. It will be convinient to use the 'small height" defined as $h(P) = \log H(P)$. First we will state some lemmata.

Lemma 4.3. For every real number M, the set,

$$\{P \in E(\mathbb{Q}) \mid h(P) \leq M\}$$

is finite.

Lemma 4.4. Let P_0 be a fixed rational point of E. There exists a constant κ_0 depending on P_0 and E such that,

$$h(P + P_0) \leq 2h(P) + \kappa_0$$

for any $P \in E(\mathbb{Q})$.

Lemma 4.5. There exists a constant κ depending only on E such that,

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

for all $P \in E(\mathbb{Q})$. Therefore, doubling a point increases the height significantly.

Lemma 4.6. The quotient group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. That is, there are finitely many cosets of the subgroup $2E(\mathbb{Q})$ which is the image of the map $P \mapsto P + P = 2P$.

Remark 4.1. These lemmata will allow us to prove Mordell-Weil by envoking the following descent theorem. The above relate the height, a fundamentally number theoretic concept, to the geometric group law. We can think of the height as translating geometric information about the curve into number theoretic information.

4.2 The Descent Theorem

Theorem 4.7 (Descent)**.** Let Γ be an abelian group with a function,

$$h : \Gamma \to \mathbb{R}_{>0}$$

satisfying the following properties,

1. For any positive real M the set $\{P \in \Gamma \mid h(p) \leq M\}$ is finite.
2. For each $P_0 \in \Gamma$ there exits a constant κ_0 such that,

$$h(P + P_0) \leq 2h(P) + \kappa_0$$

   for all $P \in \Gamma$.

3. There exists a constant κ such that,

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

   for all $P \in \Gamma$.

and furthermore we assume that $\Gamma/2\Gamma$ is finite then Γ is a finitely generated abelian group.

Proof. We choose representatives of the finite number of cosets of 2Γ. Let these be $Q_1, \cdots, Q_n$ such that for any P there always exists some i_1 such that,

$$P - Q_{i_1} \in 2\Gamma$$

which implies that,

$$P - Q_{i_1} = 2P_1$$

for some $P_1 \in \Gamma$. Now we do the same procedure repeatedly using P_1 to get a list,

$$\begin{aligned} P - Q_{i_1} &= 2P_1 \\ P_1 - Q_{i_2} &= 2P_2 \\ &\vdots \\ P_{m-1} - Q_{i_m} &= 2P_m \end{aligned}$$

By substituting each line into the previous we get,

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m$$

we are going to show that if we make m large enough than we can make $h(P_m)$ less than some constant which does not depend on P. Since there are a finite number of such P_m this will show that any P can be written in terms of a fixed finite set of points.

Applying the second height property with $P_0 = -Q_i$ we get,

$$h(P - Q_i) \leq 2h(P) + \kappa_i$$

for any $P \in \Gamma$. Since there are finitely many Q_i we may take κ' to be the maximum κ_i. Therefore,

$$h(P - Q_i) \leq 2h(P) + \kappa$$

for each Q_i and any $P \in \Gamma$. Furthermore, applying the thrid property,

$$4h(P_j) \leq h(2P_j) + \kappa = h(P_{j-1} - Q_{i_j}) + \kappa \leq 2h(P_{j-1}) + \kappa' + \kappa$$

We can rewrite this as,

$$h(P_j) \leq \frac{1}{2}h(P_{j-1}) + \frac{\kappa' + \kappa}{4} = \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (\kappa' + \kappa))$$

From this relation we see that if $h(P_{j-1}) \geq \kappa' + \kappa$ then,

$$h(P_j) \leq \frac{3}{4}h(P_{j-1})$$

which implies that the sequence of points $P_1, P_2, \ldots, P_m$ has decreasing height, at least as fast as the geometic series $\left(\frac{3}{4}\right)^j$, as long as $h(P_j) \geq \kappa' + \kappa$. Since this sequence has zero limit, there must exists an m such that $h(P_j) \leq \kappa' + \kappa$ otherwise the sequence will continue to decrease to zero. Therefore, we have shown any any point P can be written as,

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m$$

where P_m has height less than $\kappa' + \kappa$. Since there are a finite number of points satisfying this height condition and a finite number of representatives Q_i we can take the finite generating set,

$$\{Q_1, Q_2, \ldots, Q_n\} \cup \{R \in \Gamma \mid h(R) \leq \kappa' + \kappa\}$$

which we have proven can express any point $P \in \Gamma$ in some finite sum. □

Remark 4.2. Assuming the lemata, we have proven Mordell's theorem i.e. the special case of Mordell-Weil for elliptic curves and $K = \mathbb{Q}$. To generalize this result requires proving these lemmata, or some appropreate generalization, for the algebraic heigh function over a number field. We will not give the details here.

4.3 The Proof For $K = \mathbb{Q}$

We will now sketch some of the proofs of the omitted lemmata. (WIP)

5 The Moduli Space of Complex Tori

5.1 Maps Between Complex Tori

Proposition 5.1. Let $\Lambda, \Lambda \subset \mathbb{C}$ be lattices and $m, b \in \mathbb{C}$ be complex numbers. Then the map, $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ given by $[z] \mapsto [mz + b]$ is a well-defined holomorphic map of complex tori iff $m\Lambda \subset \Lambda'$.

Proof. Such a map is clearly holomorphic since it is a linear function. We require that it be well-defined i.e. if $z' = z + \omega$ then $f([z']) = f([z])$ since $[z'] = [z]$. Therefore, $[mz + m\omega + b] = [mz + b]$ which is equivalent to $m\omega \in \Lambda'$ for any $\omega \in \Lambda$. This is exactly the condition that $m\Lambda \subset \Lambda'$ □

Proposition 5.2. Any holomorphic map $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ must be of the form $[z] \mapsto [mz + b]$ for some complex numbers $m, b \in \mathbb{C}$ such that $m\Lambda \subset \Lambda'$. Furthermore, f is a group homomorphism exactly when $b \in \Lambda'$ i.e. $[b] = 0$ in $\mathbb{C}/\Lambda'$.

Proof. We have seen this argument previously in the connection between the geometric and analytic group law. We will be more careful this time.

Consider the projection maps $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ then there is a diagram,

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\tilde{f}} & \mathbb{C} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{C}/\Lambda & \xrightarrow{f} & \mathbb{C}/\Lambda' \end{array}$$

I claim there is a map $\tilde{f} : \mathbb{C} \to \mathbb{C}$ which makes this diagram commute. This is known as lifting to the universal cover in the math lingo but it is easy to see what this map should be. On each parallelogram in $\mathbb{C}$ we want $\tilde{f}$ to just be f up to shifiting by a constant since $\pi \circ \tilde{f} = f \circ \pi$ is defined up to a constant. We glue these together choosing the correct constants to match on the boundaries of the parallelograms.

Now, I claim that $\tilde{f}' : \mathbb{C} \to \mathbb{C}$ is periodic. This is the case because for any $\omega \in \Lambda$ the function, $q_\omega(z) = \tilde{f}(z+\omega) - \tilde{f}(z) \in \Lambda$ since,

$$\pi \circ q_\omega(z) = \pi \circ \tilde{f}(z+\omega) - \pi \circ \tilde{f}(z) = f([z+\omega]) - f([z]) = f([z]) - f([z]) = 0$$

But q_ω is continuous and Λ is discrete so q_ω is constant. Therefore, $q'_\omega = 0$ which implies that $\tilde{f}'(z+\omega) = \tilde{f}'(z)$ so $\tilde{f}'$ is periodic.

Therefore, by Liouville, $\tilde{f}'$ is constant so $\tilde{f} = mz+b$ for some $m, b \in \mathbb{C}$. Therefore, $f([z]) = \pi \circ \tilde{f}(z) = [mz+b]$. Furthermore, we have seen that such a map is well-defined exactly when $m\Lambda \subset \Lambda'$

Finally, for f to be a homomorphism we must have $f([z+w]) = f([z]) + f([w])$ and thus,

$$[m(z+w)+b] = [mz+b] + [mw+b] = [m(z+w)+2b]$$

which is equivalent to $[b] = 0$ in $\mathbb{C}/\Lambda'$. □

Corollary 5.3. The complex tori $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are isomorphic exactly when there exists a complex number $m \in \mathbb{C}^\times$ such that $m\Lambda = \Lambda'$.

Proof. When this is the case then we have shown there is a holomorphic homomorphism $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ given by $[z] \mapsto [mz]$. Furthermore, since we have equality, we can invert to find, $\frac{1}{m}\Lambda' = \Lambda$ so we also get a well-defined inverse map $\mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda$ given by $[z] \mapsto [m^{-1}z]$. These homomorphisms are clearly inverse so $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$.

Furthermore, we have shown that any isomorphisms must be of this type so $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$ implies that $m\Lambda = \Lambda'$ for some $m \in \mathbb{C}^\times$ given by the isomorphism. □

Remark 5.1. We have reduced classifying complex tori up to isomorphism to a problem of algebra: classifying lattices in $\mathbb{C}$ up to scaling by a complex number. We now turn our attention to studying such lattices.

5.2 Lattices

Remark 5.2. Recall that a lattice $\Lambda \subset \mathbb{C}$ is given by sums of two independent periods $\omega_1, \omega_2 \in \mathbb{C}$ explicitly,

$$\Lambda = \{n\omega_1 + m\omega_2 \mid n, m \in \mathbb{Z}\}$$

We first what to know when do periods define the same lattice. First we will fix an orientation.

Definition: Let $\mathfrak{h} \subset \mathbb{C}$ be the upper half plane,

$$\mathfrak{h} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\} = \{x+iy \mid x, y \in \mathbb{R} \text{ and } y > 0\}$$

Remark 5.3. We say a basis (ω_1, ω_2) of a lattice Λ is positively oriented if $\frac{\omega_1}{\omega_2} \in \mathfrak{h}$. Notice that if our basis is not positively oriented then we can simply swap the order to get a positively oriented bais. For simplicity, we will only work with such bases from now on.

Remark 5.4. For any complex torus $\mathbb{C}/\Lambda$ we can always put our lattices in a standard form,

$$\Lambda_\tau = \{n\tau + m \mid n, m \in \mathbb{Z}\}$$

for some $\tau \in \mathfrak{h}$. To see this choose a positively oriented basis (ω_1, ω_2) for Λ and then,

$$\frac{1}{\omega_2}\Lambda = \{\tfrac{\omega_1}{\omega_2} n + m \mid n, m \in \mathbb{Z}\} = \Lambda_\tau$$

where $\tau = \frac{\omega_1}{\omega_2} \in \mathfrak{h}$ by the positive ordering. Furthermore, there is a unique lattice up to scaling in standard form since to preserve the basis element 1 the scaling must be trivial. This argument shows that there is a unique lattice in standard form for each isomorphism class of complex tori since isomorphisms of complex tori are given by scaling their lattices.

Definition: The modular group $\mathrm{SL}_2(\mathbb{Z})$ is defined the group of matrices with integer coefficients and determinant one,

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \middle| \quad a, b, c, d \in \mathbb{Z} \text{ and } ad - bc = 1 \right\}$$

Proposition 5.4. Positively oriented bases (ω_1, ω_2) and (ω_1', ω_2') generate the same lattice Λ iff,

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

for some matrix,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

Proof. Let (ω_1', ω_2') and (ω_1, ω_2) generate Λ' and Λ. Suppose that $\Lambda' \subset \Lambda$ then $\omega_1', \omega_2' \in \Lambda$ so we must have,

$$\begin{aligned} \omega_1' &= a\omega_1 + b\omega_2 \\ \omega_2' &= c\omega_1 + d\omega_2 \end{aligned}$$

However, if $\Lambda' = \Lambda$ then $\Lambda \subset \Lambda'$ so there exist integers satisfying the inverse relation. Thus,

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

has an integer inverse i.e. $\gamma \in \mathrm{GL}_2(\mathbb{Z})$. It suffices to show that $\det \gamma = 1$. Since $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ we know that $\det \gamma = \pm 1$ since the determinant must have a multiplicative inverse in $\mathbb{Z}$. The condition that both bases are positivly oriented means that $\det \gamma > 0$ proving the proposition. □

Remark 5.5. Consider how this proposition works on lattices Λ_τ in standard form. It says that we can act on the basis $(\tau, 1)$ by some matrix,

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

to get,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a\tau + b \\ c\tau + d \end{pmatrix}$$

so $\Lambda_\tau = \{(a\tau + b)n + (c\tau + d) \mid n, m \in \mathbb{Z}\}$. We can put this lattice in standard form by the usual trick to get,

$$\Lambda_{\tau'} = \frac{1}{c\tau + d}\Lambda_\tau$$

where,

$$\tau' = \frac{a\tau + b}{c\tau + d}$$

Therefore, doing this strange matrix transformation to τ does not change the corresponding complex torus. Accordingly, we define an action of $\mathrm{SL}_2(\mathbb{Z})$ on points $\tau \in \mathfrak{h}$ via,

$$\gamma \cdot \tau = \frac{a\tau + b}{c\tau + d}$$

We can check that $\tau' \in \mathfrak{h}$ and that $(\gamma_1\gamma_2) \cdot \tau = \gamma_1 \cdot (\gamma_2 \cdot \tau)$. Also, since every lattice has a unique standard form and lattices are equivalent exactly when they linked by some $\mathrm{SL}_2(\mathbb{Z})$ action and complex tori are isomorphic exacly when their corresponding lattices are equal up to scaling we have shown that there is a unique isomorphism class for each $\tau \in \mathfrak{h}$ up to the action of $\mathrm{SL}_2(\mathbb{Z})$.

Theorem 5.5. Consider the space $\mathfrak{M} = \mathfrak{h}/\mathrm{SL}_2(\mathbb{Z})$ which are orbits of $\tau \in \mathfrak{h}$ under the action of $\mathrm{SL}_2(\mathbb{Z})$. There is a unique isomorphism class of complex tori for each $\tau \in \mathfrak{M}$ represented by $\mathbb{C}/\Lambda_\tau$. We therefore call $\mathfrak{M}$ the *moduli space* of complex tori.

Remark 5.6. The modular group is extremely important in what follows so it is vital to understand its properties.

Proposition 5.6. $\mathrm{SL}_2(\mathbb{Z})$ is generated by the two matrices,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

These correspond to the transformations of lattices $\tau \mapsto \tau + 1$ and $\tau \mapsto -\frac{1}{\tau}$.

(DRAW THESE CORRESPONDING LATTICE TRANSLATIONS)

6 Modular Forms

6.1 Discriminants

Remark 6.1. For a quadratic equation,

$$ax^2 + bx + c$$

we all know that the roots are given by,

$$\alpha_\pm = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Notice that the quantity,

$$\Delta = b^2 - 4ac$$

determines the number and reality of the roots. We call this quantity the discriminant. We would like to look for an analogous quantity for higher-order polynomials. Notice that,

$$\Delta = (\alpha_+ - \alpha_-)^2$$

Definition: Given a polynomial $f(z) \in \mathbb{C}[z]$ of degree n, we know that f has exactly n roots $\alpha \in \mathbb{C}$ (counted with multiplicity). We define the *discriminat* of f to be,

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

Notice that $f(z)$ has a double root iff $\Delta(f) = 0$.

Proposition 6.1. The discriminat $\Delta(f)$ can be written as a polynomial in the coefficients of $f(z)$.

Remark 6.2. We have already seen how for a quadratic $f(z) = az^2 + bz + c$ then $\Delta(f) = b^2 - 4ac$ is a polynomial in the coefficients of f. Now we see how we can do this for a cubic which will be the main case we care about.

Proposition 6.2. For a cubic of the form $x^3 + px + q$ we have,

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

Proof. Recall that a monic polynomial is determined exactly as,

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i)$$

For the cubic case we have,

$$\begin{aligned} x^3 + px + q &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \\ &= x^3 - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3)x - \alpha_1\alpha_2\alpha_3 \end{aligned}$$

Therefore we must have,

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= 0 \\ \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3 &= p \\ -\alpha_1\alpha_2\alpha_3 &= q \end{aligned}$$

Now consider,

$$\Delta = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_1 - \alpha_2)^2$$

One can show, by expanding out both sides (I don't recommend it) that,

$$\begin{aligned} \Delta = &-27(\alpha_1\alpha_2\alpha_3)^2 - 4\alpha_1\alpha_2\alpha_3(\alpha_1 + \alpha_2 + \alpha_3)^3 + 18\alpha_1\alpha_2\alpha_3(\alpha_1 + \alpha_2 + \alpha_3)(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) \\ &+ (\alpha_1 + \alpha_2 + \alpha_2)^2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)^2 - 4(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)^3 \end{aligned}$$

Each factor is a term we know in terms of coefficients so plugging in,

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

□

Remark 6.3. You may wonder how in the hell I knew to write down that expansion of Δ in terms of the known polynomials. Well it turns out there is general theory which gives an algorithm to do this in general. What do I mean by this? We say a polynomial is symmetric if it remains unchanged under permuting its variables so Δ is symmetric in the roots α_i and the coefficient polynomials,

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 \\ \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3 \\ \alpha_1\alpha_2\alpha_3 \end{aligned}$$

are also symmetric. In fact, these are very special they are called the elementary symmetric polynomials on three variables (think about how you would generalize these to any number of variables). A marvelous theorem says that *any* symmetric polynomial can be decomposed into sums and products of these elementary symmetric polynomials. Furthermore, Vieta's formula tells us that the coefficients of a polynomial are always elementary symmetric polynomials of the roots. Can you see how this proves that the discriminant $\Delta(f)$ must always be some polynomial in the coefficients of f rather than the roots themselves? Furthermore, the Newton identities actually give an algorithm for computing these expansions in terms of elementary symmetric polynomials. I highly recommend you look into this story further, symmetric polynomials, Newton sum and Newton identities, and Vieta's formula are all good places to start.

Remark 6.4. For an elliptic curve defined by a Weirstrass equation,

$$y^2 = x^3 + ax + b$$

it is important to know when $f(x) = x^3 + ax + b$ has a double root. Why? Consider,

$$y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

and suppose that $\alpha_1 = \alpha_2$. Then there are two solutions,

$$y = \pm(x - \alpha_1)\sqrt{x - \alpha_3}$$

However note that if $x > \alpha_3$ then close to $(\alpha_1, 0)$ the solutions look like two crossed lines intersecting at $(\alpha_1, 0)$. This is called a node on a curve and it means the curve is *singular* and thus is not *smooth*. There are lots of nice algebraic geometric properties that the curve loses when it is not smooth so we want to avoid this case.

In this case being smooth is equivalent to requiring that $f(x)$ and $f'(x) = 3x^2 + a$ have no common zeros and recall that this is exactly the condition for a polynomial to have no repeated roots (if f has a double root then $f(x) = (x - r)^2 q(x)$ so $f(r) = 0$ and $f'(x) = 2(x - r)q(x) + (x - r)^2 q(x)$ also has $q'(r) = 0$). Furthermore, recall that we constructed the discriminant $\Delta(f)$ in such a way that it is zero exactly when f has repeated roots. Therefore, our elliptic curve is smooth exactly when,

$$\Delta(f) = -4a^3 - 27b^2 \neq 0$$

Definition: Consider the lattice Λ_τ. Recall the defining equation of the elliptic Weierstrass $\wp$-function defined on Λ_τ is,

$$y^2 = f(x) = x^3 - (g_2(\tau)/4)x - (g_3(\tau)/4)$$

such that $(\wp(z), \wp'(z)/2)$ satisfy $y^2 = f(z)$,

$$(\wp'(z)/2)^2 = \wp(z)^3 - (g_2(\tau)/4)\wp(z) - (g_3(\tau)/4)$$

Thus we define the Modular discriminant to be (up to a constant to remove tedious fractions) the discriminant of this cubic,

$$\Delta(\tau) = -4^2\Delta(f) = g_2(\tau)^3 - 27g_3(\tau)^2$$

Remark 6.5. For $\tau \in \mathfrak{h}$ we know that $\mathbb{C}/\Lambda_\tau$ is a smooth torus (unless $\tau \in \mathbb{R}$ in which case the lattice is degenerate which is why we restric to $\mathrm{Im}(\tau) > 0$ strictly). Therefore due to the isomorphism $\mathbb{C}/\Lambda \to E$ the elliptic curve E must also be smooth so $\Delta(\tau) \neq 0$. Thus we have shown that $\Delta(\tau)$ is nonvanishing on $\mathfrak{h}$ but must vanish when $\tau \in \mathbb{R}$. However, we have shown how multiple values of τ can define the same complex torus and thus elliptic curve, those related by modular transformations. We would like a numerical invariant of the curve which does not depend on the choice of τ. The discriminant Δ is a natural hope but this turns out not to work. To see why we need to consider the transformation of the Eisenstein series which will lead us to modular forms.

6.2 Eisenstein Series

Remark 6.6. Much earlier, we saw the Eisenstein series $G_k(\Lambda)$ arrise in the defining equation of the Weirstrass $\wp$-function. We defined these series for a given lattice but we now know that we can do a modular transformation to our lattice which leaving the complex torus in question invariant. Therefore, we should investigate how our defining equation and thus the Eisenstein series change under a modular transformation.

Definition: For a lattice $\Lambda \subset \mathbb{C}$ we define the Eisenstein series,

$$G_k(\Lambda) = \sum_{\omega \in \Lambda^\times} \frac{1}{\omega^{2k}}$$

Explicitly, for the lattice $\Lambda = \{n\omega_1 + m\omega_2 \mid n, m \in \mathbb{Z}\}$ with periods ω_1, ω_2 we have,

$$G_k(\Lambda) = \sum_{n,m \neq 0} \frac{1}{(n\omega_1 + m\omega_2)^{2k}}$$

In particular, for the lattice Λ_τ in normal form we have,

$$G_k(\tau) = \sum_{n,m \neq 0} \frac{1}{(n\tau + m)^{2k}}$$

where we now view $G_k : \mathfrak{h} \to \mathbb{C}$ as a function on the upper half plane $\mathfrak{h}$.

Remark 6.7. We now investigate how $G_k(\tau)$ changes under modular transformations. Consider,

$$\begin{aligned} G_k(\gamma \cdot \tau) &= \sum_{n,m \neq 0} \frac{1}{(n\gamma \cdot \tau + m)^{2k}} \\ &= \sum_{n,m \neq 0} \frac{1}{(n\left(\frac{a\tau+b}{c\tau+d}\right) + m)^{2k}} \\ &= (c\tau + d)^{2k} \sum_{n,m \neq 0} \frac{1}{(n(a\tau + b) + m(c\tau + d))^{2k}} \\ &= (c\tau + d)^{2k} \sum_{n,m \neq 0} \frac{1}{((an + cm)\tau + (bn + dm))^{2k}} \end{aligned}$$

Notice that this is the same sum but with basis changed to,

$$\begin{pmatrix} n' \\ m' \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} n \\ m \end{pmatrix} = \gamma^\top \begin{pmatrix} n \\ m \end{pmatrix}$$

Recall that since $\gamma^\top \in \mathrm{SL}_2(\mathbb{Z})$ it acts on bases of integral lattices to give equivalent bases. Therefore, $n', m' \in \mathbb{Z}$ range over the same values as n and m meaning that,

$$G_k(\gamma \cdot \tau) = (c\tau + d)^{2k} \sum_{n',m' \neq 0} \frac{1}{(n'\tau + m')^{2k}} = (c\tau + d)^{2k} G_k(\tau)$$

Therefore, G_k is almost invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$ except for this strange factor of $(c\tau + d)^{-2k}$ in the front. We call this transformation property being weakly modular of weight $2k$ and such a function (with certain regularity conditions) a modular form of weight $2k$.

Definition: A meromorphic function $f : \mathfrak{h} \to \mathbb{C}$ is weakly modular of weight k if for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ we have,

$$f(\gamma \cdot \tau) = (c\tau + d)^k f(\tau)$$

for all $\tau \in \mathfrak{h}$. Note that because $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

which have corresponding actions $\tau \mapsto \tau + 1$ and $\tau \mapsto -\frac{1}{\tau}$ it suffices to check that,

$$f(\tau + 1) = f(\tau) \quad \text{and} \quad f\left(-\tfrac{1}{\tau}\right) = \tau^k f(\tau)$$

Definition: A function $f : \mathfrak{h} \to \mathbb{C}$ is a *modular form* of weight k if,

1. f is holomorphic on $\mathfrak{h}$
2. f is weakly modular of weight k i.e. $f(\gamma \cdot \tau) = (c\tau + d)^k f(\tau)$
3. f is holomorphic at ∞

Remark 6.8. The last property requires some additional explination which we now give. Notice that as $\tau \to i\infty$ the *nome* $q = e^{2\pi i\tau} \to 0$ since for $\tau = x + it$ we have,

$$q = e^{2\pi ix} \cdot e^{-2\pi t} \xrightarrow{t\to\infty} 0$$

Therefore, to ask that f be "holomorphic at ∞" we could that f is holomorphic as a function of q. But how is f a function of q? Consider the function,

$$g(q) = f\left(\frac{\log q}{2\pi i}\right)$$

then $g(q) = f(\tau)$ for $q = e^{2\pi i\tau}$. However, the logarithm is not well-defined for complex numbers since $e^{z+2\pi in} = e^z$ for $n \in \mathbb{Z}$. Therefore, $\log q$ is multi-valued, its value is only determined up to an element of $2\pi i\mathbb{Z}$. In fact, we can define $\log : \mathbb{C}^\times \to \mathbb{C}/(2\pi i\mathbb{Z})$. However, modularity here steps in to save the day. Recall that $\tau \mapsto \tau + 1$ is the modular transformation for,

$$\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

then weak moularity fo f implies that,

$$f(\tau + 1) = f(\gamma \cdot \tau) = (c\tau + d)^k f(\tau) = f(\tau)$$

Thus, f is periodic by integer steps along the real axis. This solves the multivaluedness issue since,

$$f\left(\frac{\log q}{2\pi i}\right)$$

is well-defined since it is invariant under $\log q \mapsto \log q + 2\pi in$.

Thus, since $f : \mathfrak{h} \to \mathbb{C}$ is holomorphic on all of $\mathfrak{h}$ this implies that g is holomorphic on the puntured disc $D^\times = \{z \in \mathbb{C}^\times \mid |z| < 1\}$ which is the image of $q = e^{2\pi i\tau}$ for all $\tau \in \mathfrak{h}$. Therefore, g must have a Laurent series at $q = 0$,

$$g(q) = \sum_{n\in\mathbb{Z}} a_n(f)\, q^n$$

Since $g(q) = f(\tau)$ for $q = e^{2\pi i\tau}$ we will schematicall write,

$$f(\tau) = \sum_{n\in\mathbb{Z}} a_n(f)\, q^n \qquad q = e^{2\pi i\tau}$$

which we call the Fourier expansion of f.

Finally, we say that f is holomorphic at ∞ if g is holomorphic on the entire disc D, in particular, if g is holomorphic at $q = 0$. This is equivalent to having no negative terms (poles) in the Laurent series so,

$$g(q) = \sum_{n=0}^{\infty} a_n(f)\, q^n$$

(Q-EXPANSION, HOL AT INFINITY, CUSP FORM)
(SPACES OF MODULAR AND CUSPFORMS AND RINGS)

Definition: A function $f : \mathfrak{h} \to \mathbb{C}$ is holomorphic at ∞ if f has a Fourier expansion

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f)\, q^n \qquad q = e^{2\pi i \tau}$$

Remark 6.9. To show a weakly modular holomorphic function f is holomorphic at ∞ one only needs to show that $f(\tau)$ is bounded as $\mathrm{Im}(\tau) \to \infty$.

Definition: A modular form $f : \mathfrak{h} \to \mathbb{C}$ is a *cusp* form if f vanishes at ∞ meaning that $a_0(f) = 0$ in its Fourier series. That is,

$$f(\tau) = \sum_{n=1}^{\infty} a_n(f)\, q^n = a_1(f)q + a_2(f)q^2 + \cdots \qquad q = e^{2\pi i \tau}$$

so g vaishes at $q = 0$. This is equivalent to the requirement that $\lim_{t\to\infty} f(it) = 0$.

Definition: We denote the vectorspace of weight k modular forms by $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ and the subspace of cups forms by $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$. Furthermore, under multiplication, these spaces form the graded rings of modular forms and cusp forms denoted, respectively, by,

$$\mathcal{M}(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_{k\geq 0} \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z})) \quad \text{and} \quad \mathcal{S}(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_{k\geq 0} \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$$

Remark 6.10. In the theory of modular forms one often considers functions which are only required to by weakly modular with respect to special subgroups $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ known as congruence subgroups. In that case we would have larger spaces of modular forms $\mathcal{M}_k(\Gamma)$ and $\mathcal{S}_k(\Gamma)$. We will not consider such objects here but they are essential in formulating the modularity theorem and the theory of modular curves.

Remark 6.11. Since a weakly modular function of weight 0 satisfies $f(\gamma \cdot \tau) = f(\tau)$ it is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$. Thus, we may consider weight 0 modular forms as functions $f : \mathfrak{M} \to \mathbb{C}$ on the moduli space of complex tori.

6.3 Computing Fourier Series of the Eisenstein Forms

Our goal is to expand the functions,

$$G_k(\tau) = \sum_{a,b\neq 0} \frac{1}{(a\tau + b)^{2k}}$$

in terms of the nome $q = e^{2\pi i \tau}$. Note that we can split up the terms where $n = 0$ to give,

$$G_k(\tau) = \sum_{b\neq 0} \frac{1}{m^{2k}} + \sum_{a\neq 0} \sum_{b\in\mathbb{Z}} \frac{1}{(a\tau + b)^{2k}}$$

Therefore, it suffices to understand the series,

$$s_{2k}(\tau) = \sum_{b\in\mathbb{Z}} \frac{1}{(\tau + b)^{2k}}$$

since we have,

$$G_k(\tau) = 2\zeta(2k) + 2\sum_{a=0}^{\infty} s_{2k}(a\tau)$$

where,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

is the Riemann zeta function. It turns out that,

$$s_{2k}(\tau) = \frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{m=1}^{\infty} m^{2k-1} q^m$$

Assuming this and noting that $q_a = e^{2\pi i a\tau} = (e^{2\pi i\tau})^a = q^a$ we then find that,

$$G_k(\tau) = 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{a=1}^{\infty} \sum_{m=1}^{\infty} m^{2k-1} q^{am}$$

We can rearange these sums by summing over $n = am$ and all possible divisors $m \mid n$,

$$G_k(\tau) = 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \left(\sum_{m|n} b^{2k-1} \right) q^n$$

These coefficients are called the divisor sum functions for obvious reasons,

$$\sigma_r(n) = \sum_{m|n} m^r$$

where $\sigma_0(n)$ is the number of divisors of n and $\sigma_1(n)$ is the sum of the divisors of n. Therefore, we have shown that,

$$G_k(\tau) = 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n)\, q^n$$

In particular, we need the cases $k = 2$ and $k = 3$ so we need the values of the Riemann zeta function,

$$\zeta(4) = \frac{\pi^4}{90} \qquad \zeta(6) = \frac{\pi^6}{945}$$

these are marvelous facts which we do not have time to prove. I highly encourage you to look up proofs of these facts. Therefore we have,

$$G_2(\tau) = \frac{\pi^4}{45} + \frac{(2\pi)^4}{3} \sum_{n=1}^{\infty} \sigma_3(n)\, q^n = \frac{\pi^4}{45} \left(1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)\, q^n \right) = \frac{\pi^4}{45} \left(1 + 240q + 2160q^2 + \cdots \right)$$

$$G_3(\tau) = \frac{2\pi^6}{945} - \frac{(2\pi)^6}{60} \sum_{n=1}^{\infty} \sigma_5(n)\, q^n = \frac{2\pi^6}{945} \left(1 - 504 \sum_{n=1}^{\infty} \sigma_5(n)\, q^n \right) = \frac{2\pi^6}{945} \left(1 - 504q - 16632q^2 + \cdots \right)$$

Since these series are well-defined at $q = 0$ the Eisenstein series do indeed define modular forms of weight $2k$.

6.4 The j-invariant of an Elliptic Curve

We now return to our quest of finding an numerical invariant of complex tori. The modular discriminant $\Delta(\tau)$ turns out not to work because it is not invariant under the modular group. Instead we have the following.

Proposition 6.3. The modular discriminant Δ is a weight 12 cusp form i.e. $\Delta \in \mathcal{S}_{12}(\mathrm{SL}_2(\mathbb{Z}))$.

Proof. $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$ and since g_2 has weight 4 and g_3 has weight 6 both terms have weight 12. Now we need to consider the q-expansion of Δ. Recall that $g_2(\tau) = 60G_2(\tau)$ and $g_3(\tau) = 140G_3(\tau)$. Now we use the q-expansions of these functions we computed earlier to find,

$$g_2(\tau)^3 = \frac{4^3\pi^{12}}{3^3} \left(1 + 720q + \cdots \right)$$

$$27g_3(\tau)^2 = \frac{4^3\pi^{12}}{3^3} \left(1 - 1008q + \cdots \right)$$

Therefore,

$$\Delta(\tau) = (2\pi)^{12} q + O(q^2)$$

Therefore, $\Delta(\tau)$ is holomorphic at infinity and moreover since the constant zero in its q-expansion is zero Δ is a cusp form. □

Remark 6.12. Therefore under the modular transformation $\Delta(\gamma \cdot \tau) = (c\tau + d)^{12}\Delta(\tau)$ so it is not a good invariant. However, we have annother weight 12 form so we can take the quotient.

Definition: The j-invariant $j : \mathfrak{h} \to \mathbb{C}$ is a weakly-modular function of weight 0 (invariant under the modular group) defined as,

$$j(\tau) = (12)^3 \, \frac{g_2(\tau)^3}{\Delta(\tau)}$$

Remark 6.13. This is modular invariant because,

$$j(\gamma \cdot \tau) = (12)^3 \, \frac{g_2(\gamma \cdot \tau)^3}{\Delta(\gamma \cdot \tau)} = (12)^3 \, \frac{(c\tau + d)^{12} \, g_2(\tau)^3}{(c\tau + d)^{12}\Delta(\tau)} = (12)^3 \, \frac{g_2(\tau)^3}{\Delta(\tau)} = j(\tau)$$

The constant $(12)^3$ is choosen such that the leading coefficent of the Fourier expansion is 1 as we will now demonstrate.

Proposition 6.4. The j-invariant has a Fourier expansion,

$$j(\tau) = \frac{1}{q} + 744 + 196884q + \cdots$$

Proof. First note that the $(12)^3$ simplifies the q-expansion of $g_2(\tau)^3$ to giveme

$$g_2(\tau)^3 = 4^6\pi^{12}(1 + 720q + \cdots) = (2\pi)^{12}(1 + 720q + \cdots)$$

Therefore, the q-expansion for the j-invariant becomes,

$$j(\tau) = \frac{(2\pi)^{12}(1 + 720q + \cdots)}{(2\pi)^{12}q + \cdots} = \frac{1 + 720q + \cdots}{q + \cdots} = \frac{1}{q} + O(1)$$

Therefore j has a simple pole at ∞ with residue 1. □

Remark 6.14. The j-invariant is not a modular form since it is not holomorphic but rather meromorphic at ∞ since it has a simple pole q^{-1} in its q-expansion. We call j a modular function of weight zero or sometimes automorphic form of weight zero.

Theorem 6.5. The j-invariant $j : \mathfrak{M} \to \mathbb{C}$ is surjective.

Proof. From the Fourier expansion, we have computed,

$$\lim_{t \to \infty} j(it) = \infty$$

This, along with the modular invariance, applies that j is a proper map (preimage of compact is compact) so its image is closed. Furthermore, j is holomorphic (and nonconstant) so its image is open. Therefore, it is surjective. To see this consider the compactification,

$$\hat{j} : \hat{\mathfrak{M}} \to \hat{\mathbb{C}}$$

us The j-invariant extends to a a holomorphic function exact because of this limit condition so it is continuous at ∞. Then, we get a nonconstant holomorphic map of compact Riemann surfaces which again is open (by open mapping) and closed (by compactness of the image) and thus is surjective. Furthermore, since $\hat{j}(i\infty) = \infty$ we see that $j : \mathfrak{M} \to \mathbb{C}$ must be surjective since $\hat{j}$ hits all of $\mathbb{C}$ and $i\infty$ is not mapped to $\mathbb{C}$. □

Definition: By analogy to the complex analytic j-invariant, given an elliptic curve E defined by the Wierstrass equation,

$$y^2 = x^3 - (g_2/4)x - (g_3/4)$$

we define the j-invariant of the curve to be,

$$j(E) = (12)^3 \cdot \frac{g_2^3}{4g_2^2 - 27g_3^3}$$

Theorem 6.6. Two elliptic curves E and E' are isomorphic over $\mathbb{C}$ if and only if $j(E) = j(E')$.

Proof. Let E and E' be defined by Weierstrass equations,

$$y^2 = x^3 - ax - b \qquad y^2 = x^3 - a'x - b'$$

respectively. Then,

$$j(E) = (12)^3 \cdot \frac{4a^3}{4a^3 - 27b^2}$$

Suppose that $j(E) \neq 0, (12)^3$ then,

$$\frac{j(E)}{j(E) - (12)^3} = \frac{4a^3}{27b^2}$$

Therefore, $j(E) = j(E')$ implies that,

$$\frac{a^3}{b^2} = \frac{a'^3}{b'^2}$$

Since we are working over the complex numbers we can choose a square root to get the following $\mu \in \mathbb{C}$ s.t.

$$\mu^2 = \frac{ab'}{a'b}$$

Then note that,

$$\mu^4 a = \frac{a^3 b'^2}{a'^2 b^2} = a'$$

and likewise,

$$\mu^6 b = \frac{a^3 b'^3}{a'^3 b^2} = b'$$

Therefore, we define a map $(x, y) \mapsto (\mu^2 x, \mu^3 y)$. Consider,

$$(\mu^3 y)^2 - (\mu^2 x)^3 - a'(\mu^2 x) - b' = (\mu^3 y)^2 - (\mu^2 x)^3 - \mu^4 a(\mu^2 x) - \mu^6 b = \mu^6(y^2 - x^3 - ax - b)$$

Thus, $(x, y) \in E \implies (\mu^2 x, \mu^3 y) \in E'$. This is clearly invertible so it suffices to check that it is a group homomorphism. Since E is an algebraic group, the biregular bijection $E \to E'$ induces a group structure on E'. Recall that, up to choosing an origin, there is a unique algebraic group structure on E' so it suffices to show that the map $E \to E'$ preserves the origin (for affine Weierstrass patches this is canonically chosen to be the point at infinity). In terms of projective coordinates, this map sends $[X : Y : Z] \mapsto [\mu^2 X : \mu^3 Y : Z]$ so the point at infinity $[0 : 1 : 0] \mapsto [0 : \mu^3 : 1] = [0 : 1 : 0]$ proving the theorem. In the case $j(E) = j(E') = 0$ then $a = a' = 0$ so choose $\mu^6 b = b'$ and repeat the argument. For $j(E) = j(E') = (12)^3$ then $b = b' = 0$ so choose $\mu^4 a = a'$ and repeat the argument. □

Theorem 6.7. Two complex tori $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are isomorphic iff $j(\Lambda) = j(\Lambda')$. In particular $j : \mathfrak{M} \to \mathbb{C}$ is injective.

Proof. If $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$ then $j(\Lambda) = j(\Lambda')$ since scalling the lattice does not change j and j is invariant under the modular group whose orbits are isomorphism classes of lattices in standard form. Now suppose that $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$. The Weierstrass $\wp$-function associates these tori to elliptic curves $\mathbb{C}/\Lambda \cong E$ and $\mathbb{C}/\Lambda' \cong E'$. By definition $j(E) = j(\Lambda)$ and thus $j(E) = j(E')$ so $E \cong E'$ and thus $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$. □

Theorem 6.8 (Algebrization)**.** Every elliptic curve over $\mathbb{C}$ comes from Weierstrass elliptic functions. Furthermore, from Weierstrass function theory we know that every complex torus is algebrizable.

Proof. Given an elliptic curve E consider $j(E) \in \mathbb{C}$. Since the j-invariant $j : \mathfrak{M} \to \mathbb{C}$ is surjective, there exists $\tau \in \mathfrak{M}$ such that $j(\tau) = j(E)$. Then, the Weierstrass $\wp$-function gives an isomorphism to an elliptic curve, $\mathbb{C}/\Lambda_\tau \xrightarrow{\Phi_\wp} E_\wp$ where $j(E_\wp) = j(\Lambda_\tau) = j(\tau) = j(E)$. Therefore, by the previous theorem $E \cong E_\wp$ so we get $\mathbb{C}/\Lambda_\tau \cong E$. □

7 The Modularity Theorem

We saw that the j-invariant could be extended to a function of compact Riemann surfaces $\hat{j} : \hat{\mathfrak{M}} \to \hat{\mathbb{C}}$. In fact, we have shown that $\hat{j}$ is an isomorphism so the moduli space of complex tori is isomorphic to the Riemann sphere.

Recall when I introduced the notion of a modular form I remarked that we often do not require modular invariance under the full group $\mathrm{SL}_2(\mathbb{Z})$ but rather a "congruence subgroup" $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$. There is a particularly interesting family of such congruence subgroups,

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; ad - bc = 1 \quad c \equiv 0 \pmod{N} \right\}$$

Then we can define a larger moduli space $\mathfrak{M}_0(N) = \mathfrak{h}/G_0(N)$. In the same way that $\mathfrak{M}$ parametrized all complex tori, it turns out $\mathfrak{M}_0(N)$ parametrizes complex tori E with a distinguished order N cyclic subgroup C where two such pairs are isomorphic if there is an isomorphism $E \to E'$ restricting to an isomorphism $C \to C'$ of the distinguished subgroups. We then define the modular curve $X_0(N) = \hat{\mathfrak{M}}_0(N)$ as the compactification of this extended moduli space. This alows us to state an analytic form of the modularity theorem relating these modular curves to elliptic curves with rational j-invariants.

Theorem 7.1 (Modularity)**.** Let E be a complex elliptic curve with $j(E) \in \mathbb{Q}$. Then for some positive integer N there eixsts a surjective holomorphic map,

$$X_0(E) \longrightarrow E$$

Remark 7.1. The modularity theorem was the missing piece of the puzzle whose verification alowed Andew Wiles' to prove Fermat's Last Theorem (FLT). Very roughly, the proof proceeds by, for any counter-example to Fermat Last Theorem, constructing a corresponding elliptic curve which cannot come from modular functions in the sense of the modularity theorem. Then Wiles and collaborators were able to prove the modularity theorem as thus establish a proof of FLT.

The modulariety theorem says that all rational elliptic curves arise from modular forms. This was suggested by Taniyama in 1950's, and proved by Wiles and Taylor. Finish the prove of Fermat's last theorem.

Let E is an elliptic curve defined by

$$y^2 = 4x^3 - g_2 x - g_3$$

given that $g_2, g_3 \in \mathbb{Z}$ and $g_2^3 - 27g_3^2 \neq 0$.

Then for each prime number p, we define a number $a_p(E)$ associated to this ellptic curve E by

$$a_p(E) = p - \#\{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 : E(x, y) = 0\}.$$

Let modular form be defined as above, with the Fourier expansion

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f) e^{2\pi i n \tau}, a_n(f) \in \mathbb{C} \;\; \forall n.$$

The modular form of given weight and level form a vector space. There are linear operators called Hecke operator T_p, for each prime p. An eigenform is a modular form that is a simultaneous eigenvector for all the Hecke operators. The modularity theorem associate to the equation E an eigenform $f = f_E$ in a vector space of weight 2 modular forms at level N. The eigenvalues of f are its Fourier coefficients.

$$T_p(f) = a_p(f)f.$$

The theorem states that the Fourier coefficient gives the solution counts,

$$a_p(f) = a_p(E)$$

for all primes p.

We can also phrase this result in term of L-series. We can define L-function in general as

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

if a_n here is $s_n(f)$ for a weight 2 Hecke eigenform of level N, then the L-series has the corresponding factorization

$$L(s, f) = \prod_p (1 - a_p(f)p^{-s}1_N(p)p^{1-2s})^{-1},$$

the product is taken over all the primes p, and $1_N(p)$ is 1 if $p \nmid N$, and 0 otherwise.

We can define the Hasse-Weil L-function of an elliptic curve E in term of $a_p(E)$.

Remark 7.2. Warning! Advanced material including Galois theory assumed beyond this point. Should not be attempted by the faint of heart! However, the main meat of this course has already been covered the next sections will give a more number theoretical application of elliptic curves to giving explcit constructions of interesting extensions of quadratic number fields.

8 Complex Multiplication

Remark 8.1. We will study the endomorphisms of a complex torus $\mathbb{C}/\Lambda$ which is a group homomorphism $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$. Recall that any such map takes the form $z \mapsto \alpha z$ for some $\alpha \in \mathbb{C}$ such that $\alpha\Lambda \subset \Lambda$.

Definition: Clearly for any integer $n \in \mathbb{Z}$ the map $z \mapsto nz$ is an endomorphism since $n\Lambda \subset \Lambda$. We say a complex torus $\mathbb{C}/\Lambda$ has *complex multiplication* or CM if there exists an endomorphism $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ defined by some noninteger complex number $\alpha \in \mathbb{C}$.

Example 8.1. For $\tau = i$, the complex torus $\mathbb{C}/\Lambda_\tau$ where $\Lambda_\tau = \{n + im \mid n, m \in \mathbb{Z}\}$ has complex multiplication. This is because $i\Lambda = \Lambda$ since $i(n + im) = -m + im \in \Lambda$.

Proposition 8.2. Let Λ_τ have complex multiplication by α. Then τ and α are imaginary quadratics and α is an imaginary quadratic algbraic integer.

Proof. We know that $\alpha\Lambda \subset \Lambda$ or equivalently $\alpha \cdot \tau = \tau n_1 + m_1$ and $\alpha \cdot 1 = \tau n_2 + m_2$ for integers $n_1, n_2, m_1, m_2 \in \mathbb{Z}$. Therefore,

$$(\tau n_2 + m_2) \cdot \tau = \tau n_1 + m_1$$

which implies that,

$$n_2\tau^2 + (m_2 - n_1)\tau - m_1 = 0$$

Also, $\tau \in \mathfrak{h}$ so τ is imaginary quadratic. Furthermore,

$$\tau = \frac{\alpha - m_2}{n_2} \qquad \tau(\alpha - n_1) = m_1$$

and thus,

$$(\alpha - n_1) \cdot (\alpha - m_2) = m_1 n_2$$

or expanding,

$$\alpha^2 - (n_1 + m_2)\alpha + m_1 m_2 - m_1 n_2$$

and thus α is a quadratic algebraic integer. Furthermore, suppose $\alpha \in \mathbb{R}$ then since $\tau \notin \mathbb{R}$ we must have $\alpha \cdot 1 = m_2$ so $\alpha \in \mathbb{Z}$ which we assume is not the case for Λ_τ to have complex multiplication. Thus α is an imaginary quadratic integer. □

Definition: Let Λ be a lattice then we define a field extension $K_\Lambda = \mathbb{Q}(\{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\})$.

Remark 8.2. When Λ is not CM then clearly $K_\Lambda = \mathbb{Q}$ since all such $\alpha \in \mathbb{C}$ are integers.

Proposition 8.3. Let Λ have complex multiplication by α then $K_\Lambda = \mathbb{Q}(\alpha)$.

Proof. Clearly $\mathbb{Q}(\alpha) \subset K_\Lambda$ so it suffices to show the other inclusion namely that any endomorphism of $\mathbb{C}/\Lambda$ is generated by 1 and α over $\mathbb{Q}$.

We know that $\alpha = \tau n + m$ for some $n, m \in \mathbb{Z}$ so either $n = 0$ in which case $\alpha \in \mathbb{Q}$ or,

$$\tau = \frac{\alpha - m}{n}$$

in which case $\tau \in \mathbb{Q}(\alpha)$. Then for any other $\alpha'\Lambda \subset \Lambda$ we have $\alpha' = \tau n' + m'$ for $n', m' \in \mathbb{Z}$. Since $\tau \in \mathbb{Q}(\alpha)$ then $\alpha' \in \mathbb{Q}(\alpha)$ proving the proposition. □

Remark 8.3. In particular, either $K_\Lambda = \mathbb{Q}$ or $K_\Lambda = \mathbb{Q}(\alpha)$ is an imaginary quadratic field which we call a CM-field as per the following definition.

Definition: We say a number field K is a CM-field if it is a quadratic extension K/F where F is totally real i.e. every embedding $F \hookrightarrow \mathbb{C}$ factors through $\mathbb{R} \hookrightarrow \mathbb{C}$ (meaning its image is real) but K is totally imaginary i.e. no embedding $F \hookrightarrow \mathbb{C}$ factors through $\mathbb{R} \hookrightarrow \mathbb{C}$ (meaning its image is complex).

Remark 8.4. Thus Λ has CM iff K_Λ is a CM-field since $K/\mathbb{Q}$ of degree < 4, is CM exactly when K is imaginary quadratic.

Proposition 8.4. Given $\mathbb{C}/\Lambda$ set $K = K_\Lambda$. If $\mathbb{C}$ has complex multiplication by some minimal α then the endomorphism ring of $\mathbb{C}/\Lambda$ is $\mathrm{End}(\mathbb{C}/\Lambda) \cong \mathbb{Z}[\alpha] \subset \mathcal{O}_K$.

Proof. The field K is generated by $\alpha \in \mathbb{C}$ such that $\alpha\Lambda \subset \Lambda$ which are all algebraic integers. Therefore, there is a map $\mathrm{End}(\mathbb{C}/\Lambda) \to \mathcal{O}_K$ by $\phi_\alpha \mapsto \alpha$. This is clearly an injective ring map whose image is $\mathbb{Z}[\alpha]$ by the previous result. □

Remark 8.5. When Λ does not have complex multiplication then $K_\Lambda = \mathbb{Q}$ which has integers $\mathbb{Z} \cong \mathrm{End}(\Lambda)$. When Λ has complex multiplication by a primitive α then $K_\Lambda = \mathbb{Q}(\alpha)$ and,

$$\mathrm{End}(\mathbb{C}/\Lambda) = \mathbb{Z}[\alpha] \subset \mathbb{Q}(\alpha)$$

Theorem 8.5. If Λ has CM then $j(\Lambda)$ is an algebraic integer and $[\mathbb{Q}(j(\Lambda)) : \mathbb{Q}] = h_K$ where h_K is the class number of K_Λ. Furthermore $\mathbb{Q}(j(\Lambda))$ is the Hilbert Class field of the imaginary quadratic extension $\mathbb{Q}(\tau)/\mathbb{Q}$.

Proof. WIP □

Theorem 8.6. If τ is an imaginary quadratic integer number then Λ_τ has complex multiplication.

Proof. Consider $\tau\Lambda_\tau = \{\tau^2 n + \tau m \mid n, m \in \mathbb{Z}\}$. However, it τ is a quadratic integer then it satisfies some monic,

$$\tau^2 = a\tau + b$$

and thus,

$$\tau\Lambda_\tau = \{(an+m)\tau + bn \mid n, m \in \mathbb{Z}\} \subset_\tau$$

Therefore Λ_τ has complex multiplication by τ. □

Definition: We call d a Heegner number if it is squarefree and $\mathbb{Q}(\sqrt{-d})$ has clas number 1 or equivalently its ring of integers is a PID.

Theorem 8.7 (Stark-Heegner)**.** The only Heegner numbers are,

$$d = 1, 2, 3, 7, 11, 19, 43, 67, 163$$

Remark 8.6. Here, I cannot restrain myself from telling a wonderous story. Ramanujian is famed to have noticed that the transcendental number,

$$e^{\pi\sqrt{163}} = 640320^3 + 744 - 0.00000000000075\ldots$$

is almost exactly an integer. It turns out this is not a coincidence.

Recall that $d = 163$ is a Heegner number and,

$$\alpha = \frac{1+\sqrt{-163}}{2}$$

is an algebraic integer. Then, we have shown that the elliptic curve $E = \mathbb{C}/\Lambda_\alpha$ has CM and thus $j(E) = j(\alpha)$ is an algebraic integer of degree h_K. However, since α is a Heegner number, $h_K = 1$ and thus $j(E)$ is an ordinary rational integer. However, from the q-expansion,

$$j(\alpha) = \frac{1}{q} + 744 + O(q)$$

However, $q = e^{2\pi i\alpha} = e^{\pi i + \pi i\sqrt{-163}} = -e^{\pi\sqrt{163}}$. However,

$$\frac{1}{q} + O(q) = j(\alpha) - 744 \in \mathbb{Z}$$

and thus,

$$e^{\pi\sqrt{163}} + O(e^{-\pi\sqrt{163}}) \in \mathbb{Z}$$

Therefore, since $e^{-\pi\sqrt{163}}$ is very small, $e^{\pi\sqrt{163}}$ is very close to an integer.

9 Machinery

9.1 Projective Limits

Definition: A projective system is a family of objects indexed by a poset $(I, \leq)$ with morphisms $f_{ij} : A_j \to A_i$ when $i \leq j$ such that,

1. $f_{ii} = \mathrm{id}_{A_i}$
2. $f_{ik} = f_{ij} \circ f_{jk}$ for all $i \leq j \leq k$
3. $(I, \leq)$ is directed meaning that for every $i, j \in I$ there exists $k \in I$ such that $i \leq k$ and $j \leq k$. This means that for all A_i and A_j there is an object A_k such that there are maps $f_{ik} : A_k \to A_i$ and $f_{jk} : A_k \to A_j$.

we define the projective limit $\varprojlim A_n$ to be the categorical limit of this system. Concretely, for groups or modules, we can give the explicit construction of such an object,

$$\varprojlim A_i = \left\{ (a_i)_I \in \prod_{i \in I} A_i \;\middle|\; \forall i \leq j : f_{ij}(a_j) = a_i \right\}$$

Therefore, the projective limit is the set of sequences which reduce compatibly under the maps f.

A very important special case is that of a leftward mapping sequence where $I = \mathbb{N}$ with the usual order.

Definition: Given a diagram,

$$A_0 \xleftarrow{f_0} A_1 \xleftarrow{f_1} A_2 \xleftarrow{f_2} A_3 \xleftarrow{f_3} \cdots$$

we define the projective limit $\varprojlim A_n$ to be the categorical limit of the diagram. Concretely, for groups or modules, we can give the explicit construction of such an object,

$$\varprojlim A_n = \left\{ (a_n) \in \prod_{n} A_n \;\middle|\; \forall n \in \mathbb{N} : f_n(a_n) = a_{n-1} \right\}$$

Therefore, the projective limit is the set of sequences which reduce compatibly under the maps f.

Remark 9.1. One should view the projective limit as the object which "naturally projects" compatibly with the maps onto each of the given objects. There are clear projection maps $\pi_i : \varprojlim A_n \to A_i$ given by $\pi_i((a_n)) = a_i$. Reversing all the maps, we can define the dual notion called the direct limit which is the objective into which each of the given objects include compatibly via maps $\iota_i : A_i \to \varinjlim A_n$. When the given morphisms are inclusions the direct limit is simply the union.

Example 9.1. Let R be a ring. The ring of formal power series on R is

$$R[[X]] \cong \varprojlim R[X]/X^n R[X]$$

with maps $R[X]/X^{n+1}R[X] \to R[X]/X^n R[X]$ given by reduction modulo X^n. The sequences making up the projective limit give the partial sums of a formal power series.

9.2 Infinite Galois Theory

Proposition 9.2. Let F/K be Galois. Then there exists an isomorphism,

$$\mathrm{Gal}\,(F/K) \cong \varprojlim_{L/K} \mathrm{Gal}\,(L/K)$$

where L runs over all finite Galois extensions $K \subset L \subset F$. The projective system is given by the restriction maps $\mathrm{Gal}\,(L/K) \to \mathrm{Gal}\,(L'/K)$ when $L' \subset L$.

Proof. Given $\sigma \in \mathrm{Gal}\,(F/K)$ we consider the restriction $\sigma|_L$ to each finite Galois extension L/K which are clearly compatible with restrictions between finite extensions. This gives a map to the projective limit. Since each $\alpha \in F$ is algebraic over K we know that α lies in a finite Galois extension of K so if σ is trivial on all finite Galois extensions then $\sigma(\alpha) = \alpha$ so $\sigma = \mathrm{id}_F$. Thus the map is injective. Furthermore, an element of the projective limit induces an automorphism of F/K by mapping each $\alpha \in F$ to its image under the automorphism acting on any finite Galois extension containing α. Thus the mapping is surjective. □

Remark 9.2. The above identification gives a natural profinite topology on $\mathrm{Gal}\,(F/K)$ by making the projection maps $\mathrm{Gal}\,(F/K) \to \mathrm{Gal}\,(L/K)$ continuous for each finite Galois extension L/K. In particular, the kernels of these maps $\mathrm{Gal}\,(F/L)$ are open subgroups and form a neighborhood basis of id.

Example 9.3. The absolute Galois group of $\mathbb{F}_p$ is equal to the profinite completion of $\mathbb{Z}$,

$$\mathrm{Gal}\left(\overline{\mathbb{F}_p}/\mathbb{F}_p\right) \cong \hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$$

Theorem 9.4 (Galois Correspondence)**.** Let F/K be a Galois extension with $G = \mathrm{Gal}\,(F/K)$. There is an inclusion reversing correspondence between *closed* subgroups $H \subset G$ and subfields $K \subset L \subset F$ given by $H \mapsto F^H$ and $L \mapsto \mathrm{Gal}\,(F/L)$. Furthermore, finite extensions $K \subset L \subset F$ correspond to open subgroups $\mathrm{Gal}\,(F/L) \subset G$ whose cosets correspond to embeddings of L into F fixing K. Galois extensions $K \subset L \subset F$ correspond to closed normal subgroups.

9.3 ℓ-adic Numbers

Definition: The ℓ-adic integers are the projective limit,

$$\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^n\mathbb{Z}$$

under the maps $\mathbb{Z}/\ell^{n+1}\mathbb{Z} \to \mathbb{Z}/\ell^n\mathbb{Z}$ given by reduction mod ℓ.

Remark 9.3. There is an inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_\ell$ given by reducing $a \in \mathbb{Z}$ modulo each ℓ^n. The sequences representing $\mathbb{Z} \subset \mathbb{Z}_\ell$ are exactly those which are eventually constant after the largest power dividing the integer in question. Using the intuition gained from the ring of formal power series, we can write any ℓ-adic integer as a formal "base-ℓ" power series,

$$z = a_0 + a_1\ell + a_2\ell^2 + a_3\ell^3 + \cdots$$

which is the natural extension of how integers may be represented in base ℓ. Although this expression is simply convenient and suggestive shorthand for the projective limit sequence of partial sums,

$$z = (a_0,\, a_0 + a_1\ell,\, a_0 + a_1\ell + a_2\ell^2,\, a_0 + a_1\ell + a_2\ell^2 + a_3\ell^3,\, \cdots)$$

we can actually give meaning to this infinite sum by changing the standard definition of convergence. Define the ℓ-adic valuation $v_\ell : \mathbb{Z}_\ell \to \mathbb{N} \cup \{\infty\}$ by $v_\ell((a_i))$ equals the index of the first nonzero term a_i and $v_\ell(0) = \infty$. All terms in the sequence past $v_\ell((a_i))$ are nonzero because if $a_i = 0$ then $a_{i-1} = f_i(a_i) = 0$. We can then define an absolute value, $|z|_\ell = \ell^{-v_\ell(z)}$ which gives a non-archimedean metric on Z_ℓ. Under this metric, the sequence of elements in $\mathbb{Z} \subset \mathbb{Z}_\ell$ given by these the partial sums actually does converge to the ℓ-adic number,

$$z = a_0 + a_1\ell + a_2\ell^2 + a_3\ell^3 + \cdots$$

because the element,

$$z - z_{N-1} = z - \sum_{i=0}^{N-1} a_i\ell^n = a_N\ell^N + a_{N+1}\ell^{N+1} + a_{N+2}\ell^{N+2} + \cdots$$

has valuation $v_\ell(z_n) \geq N$ because $z_N = (0, \cdots, a_N\ell^N, a_{N+1}\ell^{N+1}, \cdots)$ where the first $N-1$ terms are 0. Therefore,

$$|z - z_n|_\ell \leq \frac{1}{\ell^N} \to 0$$

so the sequence converges $z_n \to z$.

Definition: The ℓ-adic field is the field of fractions of $\mathbb{Z}_\ell$,

$$\mathbb{Q}_\ell = \mathrm{Frac}(\mathbb{Z}_\ell)$$

on which we extend the ℓ-adic valuation to $v_\ell : \mathbb{Q}_\ell \to \mathbb{Z}$ by $v_\ell(a/b) = v_\ell(a) - v_\ell(b)$.

Proposition 9.5. $\mathbb{Z}_\ell^\times = \{z \in \mathbb{Z}_\ell \mid |z|_\ell = 1\}$

Proof. Let $z = (a_i) \in \mathbb{Z}_\ell$. If $v_\ell(z) > 0$ then $a_0 = 0$ so for any $(b_i) \in \mathbb{Z}_\ell$ we have $a_0 b_0 = 0$ so $z \notin \mathbb{Z}_\ell$. However, if $v_\ell(z) = 0$ then choose $b_n = a_n^{-1} \in \mathbb{Z}/\ell^n\mathbb{Z}$ which exists because a_n is coprime to ℓ since it projects down to $a_0 \neq 0$ in $\mathbb{Z}/\ell\mathbb{Z}$. Then we have,

$$(a_i) \cdot (b_i) = (a_i b_i) = (1)$$

so $z \in \mathbb{Z}_\ell^\times$. □

Proposition 9.6. Every element $z \in \mathbb{Q}_\ell$ can be written uniquely as $z = \ell^n u$ where $u \in \mathbb{Z}_\ell^\times$ and $n = v_\ell(z)$.

Proof. First we will prove this for $z = (a_i) \in \mathbb{Z}_\ell$. Take $n = v_\ell(z)$ so we know that $f_{n-1,k}(a_k) = 0$ so $\ell^n \mid a_k$ but ℓ^{n+1} does not. Thus we can write $a_k = \ell^n u_k$ with $u_k \in (\mathbb{Z}/\ell^k\mathbb{Z})^\times$. Take $u = (u_k)$ with $u_k = f_{kn}(u_n) \neq 0$ since $\ell \nmid u_n$ for $k < n$ so clearly $z = \ell^n u$ and $v_\ell(u) = 0$. Furthermore, if $z \in \mathbb{Q}_\ell$ then $z = \frac{a}{b}$ for $a, b \in \mathbb{Z}_\ell$ so we can write $a = \ell^n u$ and $b = \ell^m v$ with $u, v \in \mathbb{Z}^\times$. Thus,

$$z = \frac{\ell^n u}{\ell^m v} = \ell^{n-m} u v^{-1}$$

with $v_\ell(z) = v_\ell(a) - v_\ell(b) = n - m$ an $uv^{-1} \in \mathbb{Z}_\ell^\times$. □

Proposition 9.7.

$$\mathbb{Q}_\ell = \mathbb{Z}_\ell\left[\frac{1}{\ell}\right] = \bigcup_n \frac{1}{\ell^n}\mathbb{Z}_\ell$$

Therefore we may represent an element of $\mathbb{Q}_\ell$ as a power series,

$$a_{-N}\ell^{-N} + a_{-N+1}\ell^{-N+1} + \cdots + a_0 + a_1\ell + a_2\ell^2 + \cdots$$

with only finitely many negative exponent terms.

Proof. By the previous proposition we can write any element $z \in \mathbb{Q}_\ell$ as $\ell^n u$ for $u \in \mathbb{Z}_\ell^\times$ and $n \in \mathbb{Z}$. Therefore, we simply need to invert ℓ to get negative powers of ℓ to represent all of $\mathbb{Q}_\ell$ from $\mathbb{Z}_\ell$. □

Proposition 9.8. $\mathbb{Z}_\ell$ is a local PID (and thus a discrete valuation ring) with unique maximal ideal $\ell\mathbb{Z}_\ell$ and residue field $\mathbb{F}_\ell$.

Proof. Let $I \subset \mathbb{Z}_\ell$ be an ideal. Consider $n = v_\ell(I) = \min\{v_\ell(z) \in \mathbb{N} \mid z \in I\}$ where the minimum value exists by well ordering. Thus, there exists $z_0 \in I$ with $v_\ell(z) = n$. I claim that $I = (\ell)^n$. We can write $z_0 = \ell^n u$ for some $u \in \mathbb{Z}_\ell^\times$. Therefore, $I \subset (z) = (\ell^n u) = (\ell)^n$. Furthermore for any $z \in I$ we have $v_\ell(z) = m \geq n$ so $\ell^n \mid z$ since $z = \ell^m v$ for $v \in \mathbb{Z}_\ell^\times$ so $z = \ell^{m-n} v \ell^n$ with $\ell^{m-n} v \in \mathbb{Z}_\ell$ and thus $z \in (\ell)^n$. Therefore, $I = (\ell)^n$.

Thus, all proper ideals are contained in (ℓ) so $\mathfrak{m} = (\ell)$ is the unique maximal ideal. Consider the map,

$$\phi : \mathbb{Z} \to \mathbb{Z}_\ell/\ell\mathbb{Z}$$

given by inclusion and then projection. Given $z = (a_i) \in \mathbb{Z}_\ell$ take $a \in \mathbb{Z}$ such that $a \equiv a_i \bmod \ell$. Then $v_\ell(z - a) \geq 1$ so $\ell \mid z - a$. Therefore, $[a] = [z]$ in $\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell$ so ϕ is surjective. Furthermore, $\ker\phi = \ell\mathbb{Z}$ since $[a] = 0$ exactly when $a = (0, a, \cdots)$ i.e. $a \equiv 0 \bmod \ell$. Therefore,

$$\mathbb{Z}/\ell\mathbb{Z} \cong \mathbb{Z}_\ell/\ell\mathbb{Z}$$

so the residue field is given by $\mathbb{Z}_\ell/\mathfrak{m} \cong \mathbb{F}_\ell$. □

Proposition 9.9. $\mathbb{Q}_\ell/\mathbb{Z}_\ell \cong \mathbb{Q}/\mathbb{Z}$ and $\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell \cong \mathbb{Z}/\ell^n\mathbb{Z}$

Proof. Quotienting by $\ell^n\mathbb{Z}_\ell$ is equivalent to ignoring all elements of the sequence with index greater than or equal to n. Therefore, we can choose a rational number (or integer) which reduces modulo $\ell^n\mathbb{Z}$ to the required value which is consistently reduced by the reduction maps. □

Definition: A complete non-archimedean field K is a topological field which is complete with respect to an absolute value satisfying the non-archimedean property or ultrametric inequality,

$$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$$

For example $\mathbb{Q}_\ell$ with the ℓ-adic absolute value $|\cdot| : \mathbb{Q}_\ell \to \mathbb{Z}$.

Proposition 9.10. Let K be a complete non-archimedean field and L/K a separable extension. The absolute value on K extends uniquely to a non-archimedean absolute value on L. Furthermore, if L/K is finite then L is complete with respect to the extended absolute value.

Lemma 9.11 (Krasner)**.** Let K be a complete non-archimedean field and $\alpha, \beta \in \bar{K}$. If α is strictly closer to β than to any conjugate of α then $K(\alpha) \subset K(\beta)$.

Proof. Consider an automorphism $\sigma \in \mathrm{Gal}\left(\bar{K}/K\right)$. By assumption, $|\alpha - \beta| < |\alpha - \sigma(\alpha)|$ whenever $\sigma(\alpha) \neq \alpha$. Suppose that $\sigma(\beta) = \beta$ and consider the value,

$$|\alpha - \sigma(\alpha)| = |\alpha - \beta + \beta - \sigma(\alpha)| \leq \max\left\{|\alpha - \beta|, |\beta - \sigma(\alpha)|\right\}$$

We know that $|\beta - \sigma(\alpha)| = |\sigma(\beta - \alpha)| = |\alpha - \beta|$ by uniqueness of the absolute value. Therefore, unless $\sigma(\alpha) = \alpha$,

$$|\alpha - \sigma(\alpha)| \leq |\alpha - \beta| < |\alpha - \sigma(\alpha)|$$

which is a contradiction so $\sigma(\alpha) = \alpha$. Therefore, $\mathrm{Gal}\left(\bar{K}/K(\beta)\right) \subset \mathrm{Gal}\left(\bar{K}/K(\alpha)\right)$ and thus $K(\alpha) \subset K(\beta)$. □

Theorem 9.12. Let $K/\mathbb{Q}_\ell$ be finite. There exists $\alpha \in \overline{\mathbb{Q}}$ such that $K = \mathbb{Q}_\ell(\alpha)$.

Proof. By the primitive element theorem, $K = \mathbb{Q}_\ell(\alpha')$ for some α' algebraic over $\mathbb{Q}_\ell$ with minimal polynomial $f \in \mathbb{Q}_\ell[X]$. Take $g \in \mathbb{Q}[X]$ which is monic of the same degree. Write,

$$g(X) = \prod_{i=0}^{n}(X - \alpha_i)$$

for roots $\alpha_i \in \overline{\mathbb{Q}}$. Consider,

$$|(f - g)(\alpha')|_\ell = |g(\alpha')|_\ell = \prod_{i=0}^{n} |\alpha' - \alpha_i|_\ell$$

by choosing g such that $f - g$ is sufficiently small we can ensure that for any $\epsilon > 0$ there is some root α of g such that $|\alpha' - \alpha| < \epsilon$. In particular, for sufficiently small ϵ the root α will be strictly closer to α' than any conjugate of α'. Therefore, by Krasner's Lemma,

$$\mathbb{Q}_\ell(\alpha') \subset \mathbb{Q}_\ell(\alpha)$$

However because f is irreducible,

$$[\mathbb{Q}_\ell(\alpha) : \mathbb{Q}_\ell] \leq \deg g = \deg f = [\mathbb{Q}_\ell(\alpha') : \mathbb{Q}_\ell] \leq [\mathbb{Q}_\ell(\alpha) : \mathbb{Q}_\ell]$$

forcing an equality. Therefore $\mathbb{Q}_\ell(\alpha) = \mathbb{Q}_\ell(\alpha') = K$ and furthermore g is irreducible in $\mathbb{Q}_\ell[X]$ thus in $\mathbb{Q}[X]$ so,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg g = [\mathbb{Q}_\ell(\alpha) : \mathbb{Q}_\ell]$$

□

10 ℓ-adic Galois Representations and the Jugendtraum

Considering the importance of Galois groups in number theory and geometry, it is natural to study their representation theory. However, Galois groups have additional structure which makes the theory of their representations remarkably rich. They are profinite topological groups and using topological arguments is extremely fruitful in studying their general representation theory. We will see that the topology is too restrictive to admit interesting Galois representations over $\mathbb{C}$. However, the profinite topology interacts much more favorably with ℓ-adic numbers due to their profinite-like topology. Therefore, we will seek out vector spaces over $\mathbb{Q}_\ell$ on which the Galois group naturally acts. Furthermore, Galois groups act on algebraic fields and preserve certain polynomial equations meaning that Galois groups act naturally on algebraic varieties built from fields and polynomials. This action allows many Galois representations to be viewed as automorphisms of certain geometric objects giving a powerful link between the number theory of field extensions and the geometry of algebraic objects.

Definition: Let G be a profinite group and F a topological field. An n-dimensional representation of G is a continuous homomorphism,

$$\rho : G \to \mathrm{GL}_n(F)$$

If $G = G_K = \mathrm{Gal}\left(\bar{K}/K\right)$, the absolute Galois group of K, then we call such a representation a Galois representation and if F is algebraic over $\mathbb{Q}_\ell$ then we call it an ℓ-adic Galois representation.

10.1 Torsion Points and Galois Automorphisms

Lemma 10.1. If $\sigma : \overline{K} \to \overline{K}$ is a field automorphism fixing K then σ preserves the form and thus solutions to polynomial and thus rational equations with coefficients in K.

Proof. Consider the polynomial $p \in K[X]$ given by,

$$p(X) = a_n X^n + \cdots + a_1 X + a_0$$

Suppose that $p(\alpha) = 0$ then since $a_i \in K$ and σ is a field automorphism fixing K we have,

$$\sigma(p(\alpha)) = a_n \sigma(\alpha)^n + \cdots + a_1 \sigma(\alpha) + a_0 = p(\sigma(\alpha)) = 0$$

so σ commutes with polynomial functions and preserves being a root. The same argument holds for rational functions since σ, as an automorphism of fields, cannot take a nonzero quantity to zero. □

Corollary 10.2. Let E be an elliptic curve defined over K and $\sigma : \overline{K} \to \overline{K}$ be an automorphism fixing K. Then, σ acting coordinate-wise perserves E. That is, if $P \in E$ then $\sigma(P) \in E$ where we define $\sigma(O) = O$. Furthermore, σ commutes with addition on E, i.e. for $P, Q \in E$,

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

Therefore, σ induces an automorphism $E \to E$.

Proof. Since σ is a field automorphism and σ fixes K we know that σ preserves the form of the defining equation of the elliptic curve E which have coefficients in K. Thus, if $P \in E$ then $\sigma(P) \in E$. Furthermore, since addition is given by rational functions with coefficients in K then applying σ preserves the form of such equations meaning that,

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

□

Definition: Let E be an elliptic curve defined over K. For $n \in \mathbb{Z}$, define the n-torsion of E, denoted by $E[n]$, to be the kernel of the map $x \mapsto nx$.

Remark 10.1. Any automorphism $\sigma : \overline{K} \to \overline{K}$ fixing K preserves n-torsion of E since $n\sigma(P) = \sigma(nP) = \sigma(O) = O$. Therefore, σ induces an automorphism $E[n] \to E[n]$ for any n.

Definition: A *number field* is a finite field extension of $\mathbb{Q}$. For example,

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\} \text{ or } \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

are quadratic number fields with $\mathbb{Q}(i)$ a *complex number field* and $\mathbb{Q}(\sqrt{2})$ a *real number field*. We may construct larger number fields such as $\mathbb{Q}(\sqrt[3]{2})$ which is not Galois. Its Galois closure $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is a degree six number field which is normal over $\mathbb{Q}$.

Proposition 10.3. Let E be an elliptic curve defined over a number field K (in particular $\mathbb{Q}$) then,

$$E[n] \cong (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$$

Proof. Consider the elliptic curve E defined over all complex numbers. Take a lattice $\Lambda \subset \mathbb{C}$ such that the invariants[4] g_2 and g_3 give the coefficients on the defining equation of E. Then, we know that there is an isomorphism of algebraic groups $\Phi_\wp : \mathbb{C}/\Lambda \to E$. Let Λ be generated by the complex numbers ω_1, ω_2 called the fundamental periods of the lattice. Then the n-torsion points in $\mathbb{C}/\Lambda$ are exactly the points,

$$z = \frac{a}{n}\omega_1 + \frac{b}{n}\omega_2 \text{ for } a, b \in \mathbb{Z}/n\mathbb{Z}$$

such that $nz = a\omega_1 + b\omega_2 \in \Lambda$ is trivial in $\mathbb{C}/\Lambda$. Therefore, via the isomorphism $\Phi_\wp$, we have,

$$E[n] \cong (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$$

as abstract groups. However, these are the *complex* n-torsion points. We are interested in the points of E over $\overline{K} = \overline{\mathbb{Q}}$. However, any complex n-torsion point of E satisfies, in each coordinate, a polynomial equation with coefficients in K because addition and therefore $x \mapsto nx$ is a rational function of x. Therefore any complex n-torsion point is automatically in $E(\overline{K})$. □

10.2 The Tate Module

Proposition 10.4. Let E be an elliptic curve defined over K then there is a natural action of the absolute Galois group,

$$\mathrm{Gal}\left(\bar{K}/K\right) \to \mathrm{Aut}(E)$$

which, because automorphism preserve n-torsion, reduces to an action,

$$\mathrm{Gal}\left(\bar{K}/K\right) \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2\left(\mathbb{Z}/n\mathbb{Z}\right)$$

Proof. Let $\sigma \in \mathrm{Gal}\left(\bar{K}/K\right)$ act component-wise on E (and fix O). Because σ is a field automorphism fixing K, the action of σ preserves the defining equations of E so it gives a map $E \to E$. Furthermore, since addition in E is given by rational functions with coefficients in K, the action of σ also preserves addition, that is,

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

and thus σ, being inevitable point-wise, is an automorphism of E. Finally, let P_1, P_2 be a $\mathbb{Z}/n\mathbb{Z}$-basis of $E[n]$ as a free $\mathbb{Z}/n\mathbb{Z}$-module. Then there exist unique elements $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$ such that,

$$\sigma(P_1) = aP_1 + cP_2 \text{ and } \sigma(P_2) = bP_1 + dP_2$$

Then the action of σ on any element $n_1P_1 + n_2P_2$ is given by,

$$\sigma(n_1P_1 + n_2P_2) = n_1\sigma(P_1) + n_2\sigma(P_2) = (an_1 + bn_2)P_1 + (cn_1 + dn_2)P_2 = n_1'P_1 + n_2'P_2$$

Which we may write suggestively as,

$$\begin{pmatrix} n_1' \\ n_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$$

explicitly showing the representation of $\mathrm{Gal}\left(\bar{K}/K\right)$ as matrices in $\mathrm{GL}_2\left(\mathbb{Z}/n\mathbb{Z}\right)$. □

[4] up to factors of 2

Definition: The Tate module of an elliptic curve E is the group,

$$T_\ell(E) = \varprojlim E[\ell^n]$$

under the multiplication by ℓ maps,

$$E[\ell] \longleftarrow E[\ell^2] \longleftarrow E[\ell^3] \longleftarrow \cdots$$

The Tate module $T_\ell(E)$ can be given the structure of a $\mathbb{Z}_\ell$ module via the action, $(a_n) \in \mathbb{Z}_\ell$ acts on $(P_n) \in T_\ell(E)$ via $(a_n) \cdot (P_n) = (a_n \cdot P_n)$. This action is well defined because P_n has ℓ^n torsion so a_n need only be defined up to multiples of ℓ^n.

Theorem 10.5. Let E be an elliptic curve over $K/\mathbb{Q}$. There exists an ℓ-adic Galois representation $V_\ell E = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ with action,

$$\rho_{E,\ell} : \mathrm{Gal}\left(\bar{K}/K\right) \to \mathrm{Aut}(V_\ell E) \cong \mathrm{GL}_2\left(\mathbb{Q}_\ell\right)$$

called the Galois representation attached to E at ℓ.

Proof. For each $n \in \mathbb{Z}^+$ we have an action of $\sigma \in \mathrm{Gal}\left(\bar{K}/K\right)$ on $P \in E[\ell^n]$ component-wise. However, $\ell \cdot \sigma(P) = \sigma(\ell \cdot P)$ because σ is a group homomorphism of E so σ is compatible with the restriction maps. Therefore, σ lifts to $\tilde{\sigma}$ a unique automorphism of the Tate module $T_\ell(E)$. By choosing bases compatible with the multiplication by ℓ maps gives an isomorphism,

$$T_\ell(E) \cong \varprojlim \left(\mathbb{Z}/\ell^n\mathbb{Z}\right) \oplus \left(\mathbb{Z}/\ell^n\mathbb{Z}\right) \cong \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$$

The action on the Tate module induces a map,

$$\rho_T : \mathrm{Gal}\left(\bar{K}/K\right) \to \mathrm{Aut}(T_\ell(E)) \cong \mathrm{Aut}(\mathbb{Z}_\ell \oplus \mathbb{Z}_\ell) = \mathrm{GL}_2\left(\mathbb{Z}_\ell\right) \subset \mathrm{GL}_2\left(\mathbb{Q}_\ell\right)$$

The desired map is given by taking the tensor product with the trivial ℓ-adic representation $(\mathbb{Q}_\ell, \rho_0)$,

$$\rho_{E,\ell} = \rho_T \otimes \rho_0 : \mathrm{Gal}\left(\bar{K}/K\right) \to \mathrm{Aut}(T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell) \cong \mathrm{Aut}(\mathbb{Q}_\ell \otimes \mathbb{Q}_\ell) = \mathrm{GL}_2\left(\mathbb{Q}_\ell\right)$$

and we take the $\mathbb{Q}_\ell$ vector space,

$$V_\ell E = T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong (\mathbb{Z}_\ell \oplus \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = \mathbb{Q}_\ell \oplus \mathbb{Q}_\ell$$

□

Remark 10.2. We have seen here an interesting ℓ-adic representation arising naturally from algebraic geometry. It is a truly remarkable fact that a very large class of all ℓ-adic Galois representations arise from geometric objects.

10.3 Complex Multiplication

We have discussed how ℓ-adic representations can give information about the underlying geometry. Galois representations can also be used to determine algebraic properties of Galois groups from geometric structures.

Definition: An elliptic curve E has complex multiplication, is CM for short, if there exists an endomorphism of E which is not a multiplication by n map.

Remark 10.3. From the complex analytic viewpoint, such a map is multiplication by $c \in \mathbb{C}$ hence the name. Note, an endomorphism of an elliptic curve is required to be an isogeny i.e. given by rational functions over $\bar{K}$.

Lemma 10.6. Let E be an elliptic defined over K with complex multiplication and denote the exceptional endomorphism by $\phi : E \to E$. There exists a finite extension K^{CM}/K such that $\forall \sigma \in \mathrm{Gal}\left(\bar{K}/K^{\mathrm{CM}}\right) : \phi \circ \sigma = \sigma \circ \phi$

Proof. Because ϕ is an isogeny, it is given by rational functions with coefficients in $\bar{K}$. Let $K^{\mathrm{CM}} = K(S)$ where S is the set of coefficients of ϕ. Then for any automorphism $\sigma \in \mathrm{Gal}\left(\bar{K}/K^{\mathrm{CM}}\right)$ we know that σ preserves the coefficients of ϕ and thus, because σ is a field homomorphism and ϕ is a rational function, $\sigma \circ \phi(P) = \phi \circ \sigma(P)$ for any point $P \in E$. □

Definition: The field $K^{\mathrm{CM}}(E[n])$ is the field extension of K^{CM} generated by the coordinates of all points in $E[n]$. Furthermore define the ℓ^∞-torsion,

$$E[\ell^\infty] = \bigcup_n E[\ell^n]$$

and the field,

$$K^{\mathrm{CM}}(E[\ell^\infty]) = \bigcup_n K^{\mathrm{CM}}(E[\ell^n]) = \varinjlim K^{\mathrm{CM}}(E[\ell^n])$$

Lemma 10.7. For each $n \in \mathbb{Z}^+$ the extension $K^{\mathrm{CM}}(E[\ell^n])/K^{\mathrm{CM}}$ is finite Galois and therefore $K^{\mathrm{CM}}(E[\ell^\infty])/K^{\mathrm{CM}}$ is Galois.

Proof. Take $\sigma \in \mathrm{Gal}\left(\bar{K}/K^{\mathrm{CM}}\right)$ and consider $\sigma(K^{\mathrm{CM}}(E[\ell^n]))$. Since σ fixes K^{CM} the image of $K^{\mathrm{CM}}(E[\ell^n])$ is entirely determined by where σ maps the generators which are coordinates of $E[\ell^n]$. However, we have shown that σ is an automorphism of E and thus must take ℓ^n-torsion to ℓ^n-torsion. Therefore, for each $P \in E[\ell^n]$ we have $\sigma(P) \in E[\ell^n]$ so σ must map coordinates of $E[\ell^n]$ to coordinates of $E[\ell^n]$. Therefore, $\sigma(K^{\mathrm{CM}}(E[\ell^n])) = K^{\mathrm{CM}}(E[\ell^n])$ proving that $K^{\mathrm{CM}}(E[\ell^n])$ is Galois over K^{CM}. Furthermore, since $E[\ell^n]$ is finite, there are only finitely many possible permutations and thus finitely map automorphisms of $K^{\mathrm{CM}}(E[\ell^n])$ proving the extension is finite. □

Theorem 10.8. Let E be an elliptic curve defined over K with complex multiplication $\phi : E \to E$ such that ϕ restricted to $E[\ell]$ is not the multiplication by n map for any $n \in \mathbb{Z}$. Then the extension $K^{\mathrm{CM}}(E[\ell^\infty])/K^{\mathrm{CM}}$ is abelian.

Proof. Restricting the map given in Theorem 10.5 gives a representation,

$$\rho_{E,\ell}^{\mathrm{CM}} : \mathrm{Gal}\left(\bar{K}/K^{\mathrm{CM}}\right) \to \mathrm{Aut}(V_\ell E) \cong \mathrm{GL}_2\left(\mathbb{Q}_\ell\right)$$

We have that $\rho_{E,\ell}^{\mathrm{CM}}(\sigma) = I \iff \sigma \cdot (P_n) = (\sigma(P_n)) = (P_n)$ for every $(P_n) \in T_\ell(E)$. Therefore, $\sigma \in \ker \rho_{E,\ell}^{\mathrm{CM}}$ if and only if σ acts trivially on $E[\ell^n]$ for each $n \in \mathbb{Z}^+$ or equivalently, since σ acts coordinate-wise on $E[\ell^n]$, acting trivially on the coordinates of $E[\ell^n]$. However, acting trivially on the generators is equivalent to fixing the field $K^{\mathrm{CM}}(E[\ell^n])$ for all n or, equivalently, fixing the compositum $K^{\mathrm{CM}}(E[\ell^\infty])$. Therefore,

$$\ker \rho_{E,\ell}^{\mathrm{CM}} = \mathrm{Gal}\left(\bar{K}/K^{\mathrm{CM}}(E[\ell^\infty])\right)$$

Furthermore, the kernel is closed (because the action is continuous) and normal so the quotient,

$$\mathrm{Gal}\left(\bar{K}/K^{\mathrm{CM}}\right)/\mathrm{Gal}\left(\bar{K}/K^{\mathrm{CM}}(E[\ell^\infty])\right) \cong \mathrm{Gal}\left(K^{\mathrm{CM}}(E[\ell^\infty])/K^{\mathrm{CM}}\right)$$

corresponds to the Galois extension $K^{\mathrm{CM}}(E[\ell^\infty])/K^{\mathrm{CM}}$. The action then injectivly factors through the quotient as,

$$\begin{array}{ccc} \mathrm{Gal}\left(\bar{K}/K^{\mathrm{CM}}\right) & \xrightarrow{\quad\rho_{E,\ell}^{\mathrm{CM}}\quad} & \mathrm{GL}_2\left(\mathbb{Q}_\ell\right) \\ & \searrow \quad \nearrow & \\ & \mathrm{Gal}\left(K^{\mathrm{CM}}(E[\ell^\infty])/K^{\mathrm{CM}}\right) & \end{array}$$

so the group $\mathrm{Gal}\left(K^{\mathrm{CM}}(E[\ell^\infty])/K^{\mathrm{CM}}\right)$ is embedded in $\mathrm{GL}_2\left(\mathbb{Q}_\ell\right)$. However, $\sigma \circ \phi = \phi \circ \sigma$ for all $\sigma \in \mathrm{Gal}\left(\bar{K}/K\right)$ and ϕ is not multiplication by n on $E[\ell]$ so $\phi \in \mathrm{Aut}(V_\ell E) \cong \mathrm{GL}_2\left(\mathbb{Q}_\ell\right)$ corresponds to a non-scalar matrix. However, all matrices in $\mathrm{GL}_2\left(\mathbb{Q}_\ell\right)$ which commute with a fixed non-scalar matrix (which remains non-scalar in the reduction modulo ℓ) commute with each other (technical exercise). Therefore, the image of $\mathrm{Gal}\left(K^{\mathrm{CM}}(E[\ell^\infty])/K^{\mathrm{CM}}\right)$ in $\mathrm{GL}_2\left(\mathbb{Q}_\ell\right)$ is abelian so by the embedding $\mathrm{Gal}\left(K^{\mathrm{CM}}(E[\ell^\infty])/K^{\mathrm{CM}}\right)$ is abelian itself. □

Example 10.9. Consider the elliptic curve over $\mathbb{Q}$ defined by,

$$E : y^2 = x^3 + x$$

which has an exceptional automorphism $\phi : E \to E$ given by,

$$\phi(x, y) = (-x, iy)$$

which preserves the defining equation and the group law. Clearly, $K^{\mathrm{CM}} = \mathbb{Q}(i)$ since i is the only non-rational coefficient defining ϕ. One can easily check that ϕ is not multiplication by n on any torsion subgroup. Therefore, the extensions

$$\mathbb{Q}(i)(E[\ell^\infty])/\mathbb{Q}(i)$$

given by adjoining ℓ^n-torsion points of E are abelian for each ℓ.

Remark 10.4. This is an example of Kronecker's Jugendtraum or "Dream of Youth" which was to generate all abelian extensions of a number field K by adjoining special values of certain interesting functions. For example, the Kronecker-Weber theorem does this for $K = \mathbb{Q}$ saying that the abelian extensions of $\mathbb{Q}$ are exactly the subfields of $\mathbb{Q}(f(\frac{1}{n}))$ where $f(x) = e^{2\pi i x}$ is a very special analytic function. It turns out that, astonishingly, our above construction generated *all* the abelian extensions of $\mathbb{Q}(i)$. That is, the compositum over all primes ℓ of $\mathbb{Q}(i)(E[\ell^\infty])$ gives the maximal abelian extension of $\mathbb{Q}(i)$. Equivalently, every finite abelian extension of $\mathbb{Q}(i)$ is contained in $\mathbb{Q}(i)$ adjoined some finite set of torsion points on the curve E. The theory of elliptic curves using Galois representations has now realized Kronecker's dream for all imaginary quadratic fields. However, the general case remains a mystery.