THE J-INVARIANT OF ELLIPTIC CURVES AND COMPLEX MULTIPLICATION

George Wellen

April 4, 2003

Introduction

The j-invariant of an elliptic curve with complex multiplication is an algebraic integer. For a proof of this fact see [Si2, Thm.II.6.1]. For every $z \in \mathbb{C}$ there exists an elliptic curve E s.t. $j(E) = z$. If we pick an arbitrary algebraic integer z does the corresponding elliptic curve have complex multiplication? In this project we show that the answer is no. In fact only finitely many rational integers (i.e. elements of $\mathbb{Z}$) correspond to elliptic curves with complex multiplication.

Chapter 1 contains a discussion of plane curves. Many of the proofs are contained in [Kn] but I have partly simplified them and added steps for clarity.

Chapter 2 defines an elliptic curve as a nonsingular cubic in Weierstrass Form. We define the j-invariant of an elliptic curve in Chapter 2.

Chapter 3 shows that an elliptic curve is topologically a torus. There is a correspondence between complex tori and elliptic curves. The j-invariant allows us to explicitly forge a bijection between classes of complex tori and classes of elliptic curves. Thus we regard complex tori as elliptic curves.

Chapter 4 defines complex multiplication. We look at complex multiplication from the perspective of plane curves and from the perspective of complex tori.

Chapter 5 contains a lot of algebraic number theory. We need results about algebraic number fields in order to understand the proof that the j-invariant of a curve with complex multiplication is an algebraic integer. To show that only finitely many rational integers correspond to curves with complex multiplication we need the fact that there are exactly nine quadratic imaginary fields of class number 1. This was originally conjectured by Gauss and was proved by Heegner. See [He] for a proof.

1 Plane Curves

Summary

The set of zeroes of a nonzero homogeneous polynomial is a well-defined subset of the projective plane $\mathbb{P}^2_{\mathbb{C}}$. For a discussion of projective space see [Re1, 1.4]. I think of $\mathbb{P}^2_{\mathbb{R}}$ as $\mathbb{R}^2$ together with points on the horizon "at infinity". A projective change of coordinates is an invertible linear map. We regard two plane curves as the same if they are projectively equivalent.

A curve is nonsingular if we can sensibly define a tangent line at every point of the curve. The tangent line at a point is the unique line through that point with intersection multiplicity greater than 1. Nonsingularity is preserved by a projective change of coordinates. A flex (or point of inflection) is a nonsingular point of the curve where the intersection multiplicity of the tangent line is greater than 2. Of course at school we learn that an inflection point of the curve in $\mathbb{R}^2$ given by $y = f(x)$ is a point where $\frac{\partial^2 f}{\partial x^2} = 0$.

1.1 A Few Definitions

$\mathbb{P}^2_{\mathbb{C}} := (\mathbb{C}^3 \setminus \{0\})/\sim$ where $(\alpha, \beta, \gamma) \sim (\alpha', \beta', \gamma')$ if $\exists\, \lambda \in \mathbb{C} \setminus \{0\}$ s.t. $(\alpha, \beta, \gamma) = \lambda(\alpha', \beta', \gamma')$

A plane curve is a non-zero homogeneous polynomial $F \in \mathbb{C}[X, Y, Z]$. The set of zeroes of F in $\mathbb{P}^2_{\mathbb{C}}$ is well-defined since F is homogeneous. We write $F(\mathbb{C})$ or $E : (F = 0)$ to denote this locus. If deg(F)=1, 2 or 3 we say F is a line, conic or cubic respectively. A plane curve F is called irreducible if F is an irreducible polynomial. We regard F and αF as the same curve $\forall \alpha \in \mathbb{C} \setminus \{0\}$ since $F(\mathbb{C}) = \alpha F(\mathbb{C})$.

A projective transformation (or projective change of coordinates) is a linear map $\phi \in Gl_3(\mathbb{C})$. If $\phi_1 = \lambda \phi_2$ for some $\lambda \in \mathbb{C} \setminus \{0\}$ then
$\phi_1(\alpha, \beta, \gamma) = \phi_2(\alpha, \beta, \gamma) \,\forall\, (\alpha, \beta, \gamma) \in \mathbb{P}^2_{\mathbb{C}}$.

This leads us to define the projective group,
$PGl_3(\mathbb{C}) := (Gl_3(\mathbb{C}))/\{\text{scalar matrices}\}$
where a scalar matrix is a matrix of the form λI for some $\lambda \in \mathbb{C} \setminus \{0\}$. Note that $PGl_3(\mathbb{C})$ acts transitively on $\mathbb{P}^2_{\mathbb{C}}$ (ie.$\forall\, X, Y \in \mathbb{P}^2_{\mathbb{C}} \,\exists\, \phi \in PGl_3(\mathbb{C})$ s.t. $\phi(X) = Y$) since $Gl_3(\mathbb{C})$ acts transitively on $\mathbb{C}^3 \setminus \{0\}$.

We say two curves, F_1 & F_2, are projectively equivalent if $\exists\, \phi \in PGl_3(\mathbb{C})$ s.t. $F_1(X, Y, Z) = F_2(\phi^{-1}(X, Y, Z))$. Note that $F_1(\mathbb{C}) = \phi(F_2(\mathbb{C}))$.
Define $F^\phi := F \circ \phi^{-1}$. Then $F^\phi(\mathbb{C}) = \phi(F(\mathbb{C}))$.

1.2 Definition

Let $(\alpha, \beta, \gamma) \in \mathbb{P}^2_{\mathbb{C}}$. Choose $\phi \in PGl_3(\mathbb{C})$ s.t. $\phi(\alpha, \beta, \gamma) = (0, 0, 1)$. We define local affine coordinates at (α, β, γ) with the map:

$$\begin{aligned} \varphi : \phi^{-1}(\mathbb{C} \times \mathbb{C} \times \{1\}) &\rightarrow \mathbb{C}^2 \\ \varphi(\phi^{-1}(X, Y, 1)) &= (X, Y) \end{aligned}$$

φ is a bijection. The most familiar example is $\phi = I$:

$$\begin{aligned} \varphi : \{(X, Y, Z) \in \mathbb{P}^2_{\mathbb{C}} \,|\, Z = 1\} &\rightarrow \mathbb{C}^2 \\ \varphi(X, Y, 1) &= (X, Y) \end{aligned}$$

φ defines local coordinates at (0,0,1) and φ^{-1} gives us an imbedding of $\mathbb{C}^2$ in $\mathbb{P}^2_{\mathbb{C}}$ as the affine piece (Z=1). In this case the (Z=0) part of $\mathbb{P}^2_{\mathbb{C}}$ is often referred to as "the line at infinity".

If F is a plane curve then about any point $(\alpha, \beta, \gamma) \in \mathbb{P}^2_{\mathbb{C}}$ we can define affine local coordinates by choosing $\phi \in PGl_3(\mathbb{C})$ as in Definition 1.2. We have the corresponding affine curve f defined by $f(x, y) = F(\phi^{-1}(x, y, 1)) \in \mathbb{C}[x, y]$.

$$f(x, y) = f_0(x, y) + f_1(x, y) + ... + f_d(x, y)$$

where $f_i(x, y)$ is a homogeneous polynomial of degree i in x & y, $d = \deg(F)$. $f_0(x, y) = 0 \Leftrightarrow (\alpha, \beta, \gamma) \in F(\mathbb{C})$

1.3 Definition

Let $(\alpha, \beta, \gamma) \in F(\mathbb{C})$. We say (α, β, γ) is a singular point of F if f_1 is the zero polynomial. (α, β, γ) is a nonsingular point iff it is not a singular point. F is a nonsingular curve if all the points in $F(\mathbb{C})$ are nonsingular points of F.

We need to check that singularity is well-defined (i.e. independent of the choice of ϕ).

1.4 Theorem

Let F be a plane curve, $(\alpha, \beta, \gamma) \in F(\mathbb{C})$. Let $\phi, \psi \in PGl_3(\mathbb{C})$ be projective transformations s.t. $\phi(\alpha, \beta, \gamma) = \psi(\alpha, \beta, \gamma) = (0, 0, 1)$. Let

$$\begin{aligned} f(x, y) = F(\phi^{-1}(x, y, 1)) = f_1(x, y) + ... + f_d(x, y) \\ g(x, y) = F(\psi^{-1}(x, y, 1)) = g_1(x, y) + ... + g_d(x, y) \end{aligned}$$

where f_i, g_i are homogeneous of degree i, d = $\deg(F)$.
Then f_1 and g_1 are either both zero or both non-zero.

Proof [Kn, p.26]

$f(x,y) = (F \circ \psi^{-1})(\psi \circ \phi^{-1})(x,y,1)$.
Now $\psi \circ \phi^{-1} \in PGl_3(\mathbb{C})$ and $\psi \circ \phi^{-1}(0,0,1) = (0,0,1)$.
Thus $\psi \circ \phi^{-1} = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ r & s & 1 \end{pmatrix}$.
Expanding the determinant by the third column, we see that
$det(\psi \circ \phi^{-1}) = det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$. Thus $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible. So

$$\begin{aligned} f(x,y) &= (F \circ \psi^{-1})(ax+by, cx+dy, rx+sy+1) \\ &= (F \circ \psi^{-1})(rx+sy+1)\left(\frac{ax+by}{rx+sy+1}, \frac{cx+dy}{rx+sy+1}, 1\right) \\ &= (rx+sy+1)^d g\left(\frac{ax+by}{rx+sy+1}, \frac{cx+dy}{rx+sy+1}\right) \\ &= (rx+sy+1)^{d-1} g_1(ax+by, cx+dy) + \ldots + g_d(ax+by, cx+dy) \end{aligned}$$

By regrouping into homogeneous terms we see that $f_1(x,y) = g_1(ax+by, cx+dy)$.
Similarly $g_1(x,y) = f_1(\alpha x + \beta y, \gamma x + \delta y)$ where $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$.
Thus f_1 is the zero polynomial $\Leftrightarrow f_1(x,y) = 0 \, \forall x,y \in \mathbb{C} \Leftrightarrow g_1(x,y) = 0 \, \forall x,y \in \mathbb{C}$ $\Leftrightarrow g_1$ is the zero polynomial. □

Recall in Definition 1.1 we defined $F^\phi = F \circ \phi^{-1}$ and noted that $F^\phi(\mathbb{C}) = \phi(F(\mathbb{C}))$. Corollary 1.5 will show that nonsingularity is preserved by a projective change of coordinates, so F is nonsingular iff F^ϕ is nonsingular.

1.5 Corollary

If (α, β, γ) is a nonsingular point of F then $\phi(\alpha, \beta, \gamma)$ is a nonsingular point of F^ϕ.

Proof

Choose ψ s.t. $\psi(\alpha,\beta,\gamma) = (0,0,1)$ and φ s.t. $\varphi \circ \phi(\alpha,\beta,\gamma) = (0,0,1)$. Then ψ and $\varphi \circ \phi$ satisfy the hypothesis of Theorem 1.4. In the notation of Theorem 1.4 $f(x,y) = F(\psi^{-1}(x,y,1))$ and $g(x,y) = f^\phi(x,y) = F((\varphi \circ \phi)^{-1}(x,y,1))$. Thus by Theorem 1.4 f_1 and f_1^ϕ are either both zero or both non-zero. □

At a nonsingular point $(\alpha,\beta,\gamma) \in F(\mathbb{C})$ choose ϕ s.t. $\phi(\alpha,\beta,\gamma) = (0,0,1)$ as in Definition 1.2. The affine curve f has a tangent line in $\mathbb{C}^2$ at (0,0). The line is given by $f_1(x,y) = 0$. Note that this line is defined iff f_1 is not the zero polynomial iff (α,β,γ) is a nonsingular point of F. This motivates our next definition.

1.6 Definition

Let (α,β,γ) be a nonsingular point of a plane curve F and choose $\phi \in PGl_3(\mathbb{C})$ s.t. $\phi(\alpha,\beta,\gamma) = (0,0,1)$. The tangent line L to F at (α,β,γ) is defined $L := \widetilde{f_1} \circ \phi$ where $\widetilde{f_1} \in \mathbb{C}[X,Y,Z]$ is just f_1 considered as a polynomial in 3 variables independent of Z.

We need to check that the tangent line is well-defined (i.e. independent of the choice of $\phi \in PGl_3(\mathbb{C})$).

1.7 Theorem

Let $\phi,\psi \in PGl_3(\mathbb{C})$ and suppose $\phi(\alpha,\beta,\gamma) = \psi(\alpha,\beta,\gamma) = (0,0,1)$.
Let $L_\phi = \widetilde{f_1} \circ \phi$ & $L_\psi = \widetilde{g_1} \circ \psi$ where f_1 and g_1 are as in Theorem 1.4. Then $L_\phi = L_\psi$.

Proof [Kn, p.28]

$\psi \circ \phi^{-1}(0,0,1) = (0,0,1)$ so $\psi \circ \phi^{-1} = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ r & s & 1 \end{pmatrix}$
with $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ invertible (as in proof of 1.4).

$$\begin{array}{rcl}
\widetilde{f_1}(x,y,z) & = & f_1(x,y) \\
& \overset{*}{=} & g_1(ax+by, cx+dy) \\
& \overset{**}{=} & \widetilde{g_1}(ax+by, cx+dy, rx+sy+z) \\
& = & \widetilde{g_1}(\psi \circ \phi^{-1}(x,y,z)) \\
L_\psi(x,y,z) & = & \widetilde{g_1}(\psi(x,y,z)) = \widetilde{g_1}(\psi \circ \phi^{-1}(\phi(x,y,z))) \\
& = & \widetilde{f_1}(\phi(x,y,z)) = L_\phi(x,y,z)
\end{array}$$

* by the proof of 1.4.
** since $\widetilde{g_1}$ is independent of the last coordinate. □

1.8 Theorem

$P = (\alpha,\beta,\gamma) \in F(\mathbb{C})$ is a nonsingular point of F iff at least one of $\frac{\partial F}{\partial X}$, $\frac{\partial F}{\partial Y}$, $\frac{\partial F}{\partial Z}$ is nonzero at P. At a nonsingular point the tangent line L is given by $L = X\frac{\partial F}{\partial X}(P) + Y\frac{\partial F}{\partial Y}(P) + Z\frac{\partial F}{\partial Z}(P)$.

Proof [Kn, Prop.II.2.6]

Choose $\phi \in PGl_3(\mathbb{C})$ s.t. $\phi(\alpha,\beta,\gamma) = (0,0,1)$.
$(\alpha,\beta,\gamma) \in F(\mathbb{C})$ so $F \circ \phi^{-1}(0,0,1) = 0$.
As in Definition 1.2, let

$$\begin{aligned} f(x,y) &= F(\phi^{-1}(x,y,1)) = F\left(\phi^{-1}\left((x,y) \mapsto (x,y,1)\right)\right). \\ &= f_0(x,y) + ... + f_d(x,y) \end{aligned}$$

$F \circ \phi^{-1}(0,0,1) = f_0 \equiv 0$. $f_1(x,y) = ax + by$ where $a = \frac{\partial f}{\partial x}(0,0)$, $b = \frac{\partial f}{\partial y}(0,0)$.

By the Chain Rule

$$\begin{aligned} (a,b) &= \left(\frac{\partial f}{\partial x}(0,0), \frac{\partial f}{\partial y}(0,0)\right) \\ &= \left(\frac{\partial F}{\partial X}(\alpha,\beta,\gamma), \frac{\partial F}{\partial Y}(\alpha,\beta,\gamma), \frac{\partial F}{\partial Z}(\alpha,\beta,\gamma)\right) \phi^{-1} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

(ϕ^{-1} is a linear map so is equal to its derivative. $\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$ is the derivative of $(x,y) \mapsto (x,y,1)$).

$$\begin{aligned} \widetilde{f_1}(x',y',z') &= f_1(x',y') = \left(\frac{\partial f}{\partial x}(0,0), \frac{\partial f}{\partial y}(0,0)\right) \begin{pmatrix} x' \\ y' \end{pmatrix} \\ &= \left(\frac{\partial F}{\partial X}(\alpha,\beta,\gamma), \frac{\partial F}{\partial Y}(\alpha,\beta,\gamma), \frac{\partial F}{\partial Z}(\alpha,\beta,\gamma)\right) \phi^{-1} \begin{pmatrix} x' \\ y' \\ 0 \end{pmatrix}. \end{aligned}$$

Thus if all partial derivatives are zero at P, then $\widetilde{f_1} \equiv 0$ (i.e. P is a singular point). Now $F \circ \phi^{-1}(0,0,1) = 0$, so $F \circ \phi^{-1}$ is a polynomial with no monomials just in Z. So

$$\begin{aligned} \frac{\partial F}{\partial Z}(\alpha,\beta,\gamma)\,\phi^{-1}(0,0,1) &= \frac{\partial F}{\partial Z}\left(\phi^{-1}(0,0,1)\right)\phi^{-1}(0,0,1) \\ &= \frac{\partial}{\partial Z}(F \circ \phi^{-1})(0,0,1) \\ &= 0. \end{aligned}$$

By linearity this means we can put anything we like for the third entry of the vector:

$$\begin{aligned} \widetilde{f_1}(x',y',z') &= \left(\frac{\partial F}{\partial X}(\alpha,\beta,\gamma), \frac{\partial F}{\partial Y}(\alpha,\beta,\gamma), \frac{\partial F}{\partial Z}(\alpha,\beta,\gamma)\right) \phi^{-1} \begin{pmatrix} x' \\ y' \\ 0 \end{pmatrix} \\ &= \left(\frac{\partial F}{\partial X}(\alpha,\beta,\gamma), \frac{\partial F}{\partial Y}(\alpha,\beta,\gamma), \frac{\partial F}{\partial Z}(\alpha,\beta,\gamma)\right) \phi^{-1} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}. \end{aligned}$$

Let $(x', y', z') = \phi(X, Y, Z)$ so that

$$L(X,Y,Z) = \widetilde{f_1}(x',y',z') = \left(\tfrac{\partial F}{\partial X}(\alpha,\beta,\gamma), \tfrac{\partial F}{\partial Y}(\alpha,\beta,\gamma), \tfrac{\partial F}{\partial Z}(\alpha,\beta,\gamma)\right)\begin{pmatrix} X \\ Y \\ Z \end{pmatrix}.$$

Thus if at least one of the partial derivatives is nonzero at P, then $\widetilde{f_1} \neq 0$ (i.e. P is a nonsingular point).

We have shown that at least one of the partial derivatives is nonzero at P iff P is a nonsingular point and that

$$L = X\tfrac{\partial F}{\partial X}(P) + Y\tfrac{\partial F}{\partial Y}(P) + Z\tfrac{\partial F}{\partial Z}(P). \qquad \square$$

Fix a curve F and a line L in $\mathbb{C}[X, Y, Z]$.
Let $P = (\alpha, \beta, \gamma) \in (F = 0) \cap (L = 0)$. As usual choose $\phi \in PGl_3(\mathbb{C})$ s.t. $\phi(\alpha,\beta,\gamma) = (0,0,1)$ and let $f(x,y) = F(\phi^{-1}(x,y,1)) = f_1(x,y) + ... + f_d(x,y)$, $l(x,y) = L(\phi^{-1}(x,y,1))$.
$l(0,0) = 0$ so $l(x,y) = bx - ay$ for some $a, b \in \mathbb{C}$.
$\varphi(t) = \begin{pmatrix} at \\ bt \end{pmatrix}$ parametrizes $l(x,y) = 0$.
$f(\varphi(t)) = f_1(at,bt) + ... + f_d(at,bt) = tf_1(a,b) + ... + t^d f_d(a,b)$.

1.9 Definition

The intersection multiplicity of L with F at P, $i(P, L, F)$, is defined to be the order of the zero of $f(\varphi(t))$ at $t = 0$. (We say $i(P, L, F) = +\infty$ if $f \circ \varphi \equiv 0$ and $i(P, L, F) = 0$ if $P \notin (F = 0) \cap (L = 0)$).

1.10 Theorem

At a nonsingular point $P \in (F = 0)$ the tangent line, L_T, to F at P is the unique line with $i(P, L, F) > 1$.

Proof [Kn, p.35]

Let L be a line through P.
$i(P, L, F) = 1 \Leftrightarrow \frac{df(\varphi(t))}{dt} \neq 0$ at $t = 0 \Leftrightarrow f_1(a,b) \neq 0 \Leftrightarrow (a,b) \notin (L_T = 0)$
since $L_T = \widetilde{f_1} \circ \phi$ by Definition 1.6.
So $(P, L, F) = 1 \Leftrightarrow image(\varphi) \nsubseteq L_T(\mathbb{C}) \Leftrightarrow L \neq L_T$. $\square$

1.11 Definition

A nonsingular point $P \in F(\mathbb{C})$ is called a flex or inflection point of F if
$3 \leqslant i(P, L, F) < \infty$.

We have that a point P is on the curve $\Leftrightarrow f_0 = 0$. Given a point P on the curve, P is a nonsingular point $\Leftrightarrow f_1(x, y) \neq 0$. Given a nonsingular point P on the curve, $l(x, y) = bx - ay$ where $f_1(x, y) = bx - ay$, and P is a flex $\Leftrightarrow f_2(a, b) = 0$.

Let $f_2(x, y) = cx^2 + dxy + ey^2$. If $f_1 \mid f_2$ then $f_2(a, b) = 0$. Conversely if $f_2(a, b) = 0$ then (when $a, b \neq 0$) $f_2(x, y) = cx^2 + dxy + ey^2 = (bx - ay)(rx + sy)$ where $r = c/b$, $s = -e/a$. So $f_1 \mid f_2$. The cases $a = 0$,$b = 0$ can be checked separately.

Thus a nonsingular point is a flex $\Leftrightarrow f_1 \mid f_2$.

1.12 Definition

The Hessian matrix of F is defined to be
$$H := \begin{pmatrix} \frac{\partial^2 F}{\partial x^2} & \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial x \partial z} \\ \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial y^2} & \frac{\partial^2 F}{\partial y \partial z} \\ \frac{\partial^2 F}{\partial x \partial z} & \frac{\partial^2 F}{\partial y \partial z} & \frac{\partial^2 F}{\partial z^2} \end{pmatrix}$$

1.13 Theorem

A nonsingular point $P \in F$ is a flex $\Leftrightarrow detH(P) = 0$.

To prove this we need a few results first.

1.14 Lemma

Let $F, G \in \mathbb{C}[X, Y, Z]$ be plane curves and $P = (\alpha, \beta, \gamma) \in F(\mathbb{C}) \cap G(\mathbb{C})$. Then P is a singular point of the curve FG.

Proof [Kn, Prop.II.2.3]

Choose $\phi \in PGl_3(\mathbb{C})$ s.t. $\phi(P) = (0, 0, 1)$. Let

$$\begin{aligned} f(x,y) &= F(\phi^{-1}(x, y, 1)) = f_1(x, y) + ... + f_d(x, y) \\ g(x, y) &= G(\phi^{-1}(x, y, 1)) = g_1(x, y) + ... + g_d(x, y). \end{aligned}$$

Then

$$\begin{aligned} fg(x, y) = FG(\phi^{-1}(x, y, 1)) &= F(\phi^{-1}(x, y, 1))G(\phi^{-1}(x, y, 1)) \\ &= f_1g_1(x, y) + ... + f_dg_d(x, y). \end{aligned}$$

So fg has no first degree terms and hence P is a singular point of FG. □

1.15 Theorem - Bézout's Theorem

Let $F, G \in \mathbb{C}[X, Y, Z]$, $deg(F) = m$, $deg(G) = n$. Then $F(\mathbb{C}) \cap G(\mathbb{C})$ is nonempty and contains more than mn points iff F and G have a common factor. In fact, if F and G have no common factor, then $F(\mathbb{C}) \cap G(\mathbb{C})$ contains exactly mn points if they are counted with the correct multiplicities.

Proof

For a complete proof see advanced texts on Algebraic Geometry. For a proof in the case when one of the curves is a line or a conic see [Re1, Thm.1.9].

1.16 Corollary

A reducible plane curve F is singular.

Proof [Kn, Cor.II.2.5]

Let $F = F_1F_2$ be plane curves and let d_i & e_i be the highest and lowest degrees of terms in F_i. Now the product of the d_1 terms in F_1 with the d_2 terms in F_2 is the d_1d_2 part of F_1F_2. Similarly the product of the e_1 terms in F_1 with the e_2 terms in F_2 is the e_1e_2 part of F_1F_2. Since F is homogeneous $d_1d_2 = e_1e_2$. So $d_1 > e_1 \Leftrightarrow d_2 < e_2$ which is a contradiction as by definition $d_2 \geq e_2$. Thus $d_1 = e_1$ and $d_2 = e_2$.
We have shown that F_1 and F_2 are homogeneous, ie. they are plane curves. Theorem 1.15 (Bézout's Theorem) tells us that $F_1(\mathbb{C}) \cap F_2(\mathbb{C})$ is nonempty and Lemma 1.14 says that any point in this intersection is singular. □

1.17 Lemma

Let $A = (a_{ij})$ be a 3×3 symmetric matrix over $\mathbb{C}$. Then the conic

$$C(X,Y,Z) := (X,Y,Z)\,A\begin{pmatrix}X\\Y\\Z\end{pmatrix}$$

is reducible iff $detA = 0$.

Proof [Kn, Lem.II.2.11]

If C is reducible then C is singular by Corollary 1.16. Let $P \in C(\mathbb{C})$ be a singular point. By Theorem 1.8 $\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = \frac{\partial f}{\partial z} = 0$ at P. A is symmetric so $A(P) = 0$. $0 \neq P \in Ker(A)$ so $det(A) = 0$.

Conversely we can diagonalise A since it is symmetric. One of the diagonal entries must be zero since $det(A) = 0$. so we find that the conic C is projectively equivalent to the curve $X^2 + Y^2 = (X + iY)(X - iY)$ which is reducible. □

Proof of Theorem 1.13 [Kn, Prop.II.2.12]

Let L be the tangent line to F at P. Choose ϕ with $\phi(P) = (0,0,1)$. Let $f(x,y) = F(\phi^{-1}(x,y,1))$. We know that P is a flex $\Leftrightarrow$ $f_1 \mid f_2$. Now consider the conic $Q_\phi(x,y,z) := \widetilde{f_2} \circ \phi(x,y,z)$. $f_1 \mid f_2 \Leftrightarrow L \mid Q_\phi$.

P is a flex $\Rightarrow L \mid Q_\phi \Rightarrow L$ divides the conic defined by $H(P) \Rightarrow detH(P) = 0$

(by Lemma 1.17).

Conversely $detH(P) = 0 \Rightarrow$ conic C defined by $H(P)$ is reducible (by Lemma 1.17). $C = L_1 L_2$ say. Now L is the tangent line to C at P so $L = L_1$ or $L = L_2$. $L \mid C \Rightarrow L \mid Q_\phi \Rightarrow P$ is a flex. □

1.18 Corollary

A nonsingular plane curve F with $d = deg(F) > 2$ has at least one flex.

Proof

By Theorem 1.13 flex points are solutions of $F = 0 = det(H)$. $det(H)$ is a plane curve of degree $3(d-2)$. Bézout's Theorem tells us that the intersection $F(\mathbb{C}) \cap det(H)(\mathbb{C})$ is non-empty. □

1.19 Remarks

Bézout's Theorem tells us that F has $3d(d-2)$ flex points (if they are counted with correct multiplicities) unless F and $det(H)$ have a common factor. It turns out that this cannot happen unless F is a product of lines. But then of course F is reducible and hence singular by Corollary 1.16.

Every point of $F(\mathbb{C})$ has a tangent line - the unique line with intersection multiplicity $i(P, L, F) > 1$ by Theorem 1.10. Note that $i(P, L, F) = 2$ except at the finite number of flex points.

1.20 Summary of Key Points from Chapter 1

1. Let $P \in F(\mathbb{C})$. P is a nonsingular point iff at least one of the partials $\frac{\partial F}{\partial X}$, $\frac{\partial F}{\partial Y}$, $\frac{\partial F}{\partial Z}$ is not zero at P. The tangent line at P is $X\frac{\partial F}{\partial X}|_P + Y\frac{\partial F}{\partial Y}|_P + Z\frac{\partial F}{\partial Z}|_P$ which is defined iff P is a nonsingular point. Nonsingularity is preserved by projective change of coordinates.

2. A flex is a nonsingular point at which the tangent line has intersection multiplicity greater than or equal to 3. A nonsingular point P of a curve F is a flex iff $det(H(P)) = 0$ where H is the Hessian of F.

3. Every nonsingular cubic contains a flex point. A nonsingular cubic has at most 9 flex points.

2 Elliptic Curves

Overview

A cubic is a non-zero homogeneous polynomial $F \in \mathbb{C}[X,Y,Z]$ of degree 3. An elliptic curve is a nonsingular cubic in Weierstrass Form. A cubic is projectively equivalent to a cubic in Weierstrass Form iff it contains a flex. We showed in Corollary 1.18 that every nonsingular cubic contains a flex. Since we regard projectively equivalent curves as the same, elliptic curves are precisely nonsingular cubics. The j-invariant assigns a different complex number to each projective equivalence class of elliptic curves.

2.1 Definition

A cubic in the form $(Y^2Z + a_1XYZ + a_3YZ^2) - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3)$, $a_i \in \mathbb{C}$ is said to be in <u>Weierstrass Form</u>.

A nonsingular cubic in Weierstrass Form is called an <u>Elliptic Curve</u>.

Let F be a cubic in Weierstrass Form. Plug in $Z = 0$ and we are left with $-X^3$. So $(0,1,0)$ is the only point of $F(\mathbb{C})$ at infinity.

$$\begin{aligned}
\frac{\partial F}{\partial X} &= a_1YZ - 3X^2 - 2a_2XZ - a_4Z^2 \\
\frac{\partial F}{\partial Y} &= 2YZ + a_1XZ + a_3Z^2 \\
\frac{\partial F}{\partial Z} &= Y^2 + a_1XY + 2a_3YZ - a_2X^2 - 2a_4XZ - 3a_6Z^2
\end{aligned}$$

At $(0,1,0)$, $\frac{\partial F}{\partial X} = \frac{\partial F}{\partial Y} = 0$, $\frac{\partial F}{\partial Z} = 1$. By Theorem 1.8 $(0,1,0)$ is a nonsingular point of F and the tangent line to F at $(0,1,0)$ is $Z = 0$. We calculate the Hessian matrix H.

$$\begin{aligned}
H &= \begin{pmatrix} -6X - 2a_2Z & a_1Z & a_1Y - 2a_2X - 2a_4Z \\ a_1Z & 2Z & 2Y + a_1X + 2a_3Z \\ a_1Y - 2a_2X - 2a_4Z & 2Y + a_1X + 2a_3Z & 2a_3Y - 2a_4X - 6a_6Z \end{pmatrix} \\
H &\quad (0,1,0) = \begin{pmatrix} 0 & 0 & a_1 \\ 0 & 0 & 2 \\ a_1 & 2 & 2a_3 \end{pmatrix}
\end{aligned}$$

$detH(0,1,0) = 0$, so by Theorem 1.13 $(0,1,0)$ is a flex of $F(\mathbb{C})$.

2.2 Theorem

A cubic F is projectively equivalent to a cubic in Weierstrass Form $\Leftrightarrow$ $F(\mathbb{C})$ contains a flex.

Proof [Kn, pp.40-42]

($\Rightarrow$) is done above.

($\Leftarrow$) Let P be a flex of F. Choose $\phi_1 \in PGl_3(\mathbb{C})$ s.t. $\phi_1(P) = (0,1,0)$. Then F^{ϕ_1} has a flex at $(0,1,0)$. (Recall that $F^{\phi}(X,Y,Z) = F(\phi^{-1}(X,Y,Z)))$.

Let $L = \alpha X + \beta Z$ (α,β not both zero) be the tangent line to F^{ϕ_1} at $(0,1,0)$. Note there is no term in Y since the line passes through $(0,1,0)$.

We want to make a projective change of coordinates ϕ_2 which leaves the flex at (0,1,0) and so that $L^{\phi_2} = Z$. If $\alpha = 0$ we are done. If $\beta = 0$ then just take $\phi_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. If α,$\beta \neq 0$ choose ϕ_2 with $\phi_2^{-1} = \begin{pmatrix} a & 0 & b \\ 0 & 1 & 0 \\ c & 0 & d \end{pmatrix}$ s.t. $det(\phi_2)^{-1} = ad - bc \neq 0$ and $\alpha a + \beta c = 0$.

$$\begin{aligned} L^{\phi_2}(X,Y,Z) &= L(aX + bZ, Y, cX + dZ) = \alpha(aX + bZ) + \beta(cX + dZ) \\ &= (\alpha a + \beta c)X + (\alpha b + \beta d)Z = (\alpha b + \beta d)Z \end{aligned}$$

since $\alpha a + \beta c = 0$. Now if $\alpha b + \beta d = 0$ then $\alpha\beta ad = \alpha\beta bc$ so $ad - bc = 0$. Contradiction. So $\alpha b + \beta d \neq 0$ and $L^{\phi_2}(X,Y,Z) = Z$.

So, $(F^{\phi_1})^{\phi_2} = F^{\phi_1} \circ \phi_2^{-1} = F \circ \phi_1^{-1} \circ \phi_2^{-1} = F \circ (\phi_2\phi_1)^{-1} = F^{\phi_2\phi_1}$ has a flex at (0,1,0) and (Z=0) is the tangent line at (0,1,0).

Now consider the most general form of a cubic F:

$$\begin{aligned} F &= a_{X^3}X^3 \\ &+ a_{X^2Y}X^2Y + a_{X^2Z}X^2Z \\ &+ a_{XY^2}XY^2 + a_{XYZ}XYZ + a_{XZ^2}XZ^2 \\ &+ a_{Y^3}Y^3 + a_{Y^2Z}Y^2Z + a_{YZ^2}YZ^2 + a_{Z^3}Z^3 \end{aligned}$$

1. $(0,1,0) \in F^{\phi_2\phi_1}(\mathbb{C}) \Rightarrow a_{Y^3} = 0$.

2. $(0,1,0)$ is a nonsingular point of $F^{\phi_2\phi_1}(\mathbb{C})$. As in Definition 1.2, consider $f(x,y) = F^{\phi_2\phi_1}(\mathbb{C})(\phi^{-1}(x,y,1))$ where $\phi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, $\phi(0,1,0) = (0,0,1)$. $f_1(x,y) = a_{XY^2}x + a_{Y^2Z}y \neq 0$ by the definition of a nonsingular point (Definition 1.3). So a_{XY^2} and a_{Y^2Z} are not both zero.

3. The tangent line to $F^{\phi_2\phi_1}(\mathbb{C})$ at $(0,1,0)$ is $L = Z$. But $L = \widetilde{f}_1(\phi(X,Y,Z)) = a_{XY^2}X + a_{Y^2Z}Z$. So $a_{XY^2} = 0$ and by 2, $a_{Y^2Z} \neq 0$.

4. $(0,1,0)$ is a flex of $F^{\phi_2\phi_1}(\mathbb{C})$. Now $f_1(x,y) = a_{Y^2Z}y$ and $f_2(x,y) = a_{X^2Y}x^2 + a_{XYZ}xy + a_{Y^2Z}y^2$. By the comments after Definition 1.11 $f_1 \mid f_2$. Hence $a_{X^2Y} = 0$.

We have

$$\begin{aligned} F^{\phi_2\phi_1} &= a_{X^3}X^3 + a_{X^2Z}X^2Z + a_{XYZ}XYZ \\ &+ a_{XZ^2}XZ^2 + a_{Y^2Z}Y^2Z + a_{YZ^2}YZ^2 + a_{Z^3}Z^3 \end{aligned}$$

¿From Definition 1.11 $i((0,1,0),L,F) < \infty$. Now L=Z is the tangent line so Z does not divide F. Thus $a_{X^3} \neq 0$. We know from 3. that $a_{Y^2Z} \neq 0$.

Finally we let $\phi_3 = \begin{pmatrix} -a_{Y^2Z}/a_{X^3} & 0 & 0 \\ 0 & a_{Y^2Z}/a_{X^3} & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Then the coefficient of Y^2Z in $F^{\phi_3\phi_2\phi_1}$ is $(a_{Y^2Z})^3/(a_{X^3})^2$ and the coefficient of X^3 is $-(a_{Y^2Z})^3/(a_{X^3})^2$. Thus after multiplying through by a constant we obtain
$F^{\phi_3\phi_2\phi_1} = (Y^2Z + a_1XYZ + a_3YZ^2) - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3)$
as required. □

Every nonsingular cubic contains a flex by Corollary 1.18. By Theorem 2.2 every nonsingular cubic is projectively equivalent to a curve in Weierstrass Form and by Corollary 1.5 nonsingularity is preserved by a projective change of coordinates. Every nonsingular cubic is projectively equivalent to an Elliptic Curve.

Note that some cubics in Weierstrass Form are singular, eg. $F = Y^2Z - X^3$ is singular at $(0,0,1)$. Note also that $(0,1,0)$ is always a flex of a cubic in Weierstrass Form. As was remarked earlier this is the only point of $F(\mathbb{C})$ on the line at infinity. So singularity is determined on the affine piece (Z=1).

With this in mind, from now on we write $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ to represent a cubic in Weierstrass Form, taking the flex at $(0,1,0)$ as read.

2.3 Lemma

Every cubic in Weierstrass Form is projectively equivalent to a curve in the form $y^2 = x^3 - 27c_4x - 54c_6$ for some c_4,$c_6 \in \mathbb{C}$.

Proof

We first complete the square on the left-hand-side of the equation:

$$\begin{aligned}
y^2 + a_1xy + a_3y &= x^3 + a_2x^2 + a_4x + a_6 \\
\left(y + \frac{a_1}{2}x + \frac{a_3}{2}\right)^2 &= y^2 + a_1xy + a_3y + \frac{a_1^2}{4}x^2 + \frac{a_1a_3}{2}x + \frac{a_3^2}{4} \\
&= x^3 + a_2x^2 + a_4x + a_6 + \frac{a_1^2}{4}x^2 + \frac{a_1a_3}{2}x + \frac{a_3^2}{4}
\end{aligned}$$

$$\text{Let} \quad Y := 2y + a_1x + a_3, \quad X := x$$

$$\begin{aligned}
\text{Then} \quad Y^2 &= 4X^3 + 4a_2X^2 + 4a_4X + 4a_6 + a_1^2X^2 + 2a_1a_3X + a_3^2 \\
&= 4X^3 + (4a_2 + a_1^2)X^2 + 2(2a_4 + a_1a_3)X + (a_3^2 + 4a_6) \\
&= 4X^3 + b_2X^2 + 2b_4X + b_6
\end{aligned}$$

where $b_2 = (4a_2 + a_1^2)$, $b_4 = (2a_4 + a_1a_3)$, $b_6 = (a_3^2 + 4a_6)$.

Now we complete the cube on the right-hand-side of the equation:

$$\begin{aligned}
\frac{Y^2}{4} &= X^3 + \frac{b_2}{4}X^2 + \frac{b_4}{2}X + \frac{b_6}{4} \\
\left(\frac{Y}{2}\right)^2 &= \left(X + \frac{b_2}{12}\right)^3 + \left(\frac{b_4}{2} - \frac{3b_2^2}{12^2}\right)X + \left(\frac{b_6}{4} - \frac{b_2^3}{12^3}\right).
\end{aligned}$$

Now let $y' := 108Y$ and $x' := 36X + 3b_2$. Then

$$\begin{aligned}
\left(\frac{y'}{216}\right)^2 &= \left(\frac{x'}{36}\right)^3 + \left(\frac{b_4}{2} - \frac{3b_2^2}{12^2}\right)\left(\frac{x'}{36} - \frac{3b_2}{36}\right) + \left(\frac{b_6}{4} - \frac{b_2^3}{12^3}\right) \\
y'^2 &= x'^3 - 6^6\left(\frac{3b_2^2}{12^2} - \frac{b_4}{2}\right)\left(\frac{x'}{36}\right) + 6^6\left(\frac{3b_2^2}{12^2} - \frac{b_4}{2}\right)\frac{3b_2}{36} - 6^6\left(\frac{b_2^3}{12^3} - \frac{b_6}{4}\right).
\end{aligned}$$

The coefficient of the x' term is

$$\begin{aligned}
-6^4\left(\frac{3b_2^2}{12^2} - \frac{b_4}{2}\right) &= -2^43^4\left(\frac{3b_2^2}{2^43^2} - \frac{b_4}{2}\right) \\
&= -3^3\left(\frac{2^43^2b_2^2}{2^43^2} - \frac{2^43b_4}{2}\right) = -27\left(b_2^2 - 24b_4\right).
\end{aligned}$$

And the constant term is

$$\begin{aligned} 6^6\left(\frac{3b_2^2}{12^2}-\frac{b_4}{2}\right)\frac{3b_2}{36} \quad - \quad & 6^6\left(\frac{b_2^3}{12^3}-\frac{b_4}{4}\right) \\ = \quad & 2^6 3^6\left(\frac{3b_2^2}{2^4 3^2}-\frac{b_4}{2}\right)\frac{3b_2}{2^2 3^2} - 2^6 3^6\left(\frac{b_2^3}{2^6 3^3}-\frac{b_6}{2^2}\right) \\ = \quad & (3^4-3^3)b_2^3 - 2^3 3^5 b_2 b_4 + 2^4 3^6 b_6 \\ = \quad & -54\left(-b_2^3+36b_2b_4-216b_6\right) \end{aligned}$$

Thus $y'^2 = x'^3 - 27c_4x' - 54c_6$
where $c_4 = b_2^2 - 24b_4$ and $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$. □

2.4 Definition

$y^2 = x^3 - 27c_4x - 54c_6$ is called Normal Form.

2.5 Definition

Let $f(x) \in \mathbb{C}[x]$. Define the discriminant of f,

$$d := \prod_{1\leq i<j\leq deg(f)} (\alpha_i - \alpha_j)^2$$

where α_i are the roots of f in $\mathbb{C}$. Clearly $d = 0 \Leftrightarrow f(x)$ has a multiple root.

2.6 Lemma

$y^2 = ax^3 + bx^2 + cx + d$ is a nonsingular cubic if and only if $ax^3 + bx^2 + cx + d$ has three distinct roots in $\mathbb{C}$.

Proof [Kn, Prop.III.3.5]

We are considering the curve $F = Y^2Z - (aX^3 + bX^2Z + cXZ^2 + dZ^3)$. This is in Weierstrass Form so as was remarked in the comments before Lemma 2.3, singularity is determined on the affine piece (Z=1). This means that any singular point of F will be of the form $(x_0, y_0, 1)$.

By Theorem 1.8 F is singular $\Leftrightarrow \exists P = (x_0, y_0, 1) \in F(\mathbb{C})$ s.t.

$$\frac{\partial F}{\partial X} = \frac{\partial F}{\partial Y} = \frac{\partial F}{\partial Z} = 0 \text{ at } P.$$

We require (at P):

$$\begin{aligned}
F &= Y^2Z - aX^3 - bX^2Z - cXZ^2 - dZ^3 = 0 \\
\frac{\partial F}{\partial X} &= -3aX^2 - 2bXZ - cZ^2 = 0 \\
\frac{\partial F}{\partial Y} &= 2YZ = 0 \\
\frac{\partial F}{\partial Z} &= Y^2 - bX^2 - 2cXZ - 3dZ^2 = 0
\end{aligned}$$

Plug in Z=1:

$$\begin{aligned}
y^2 - ax^3 - bx^2 - cx - d &= 0 \\
3ax^2 + 2bx + c &= 0 \\
2y &= 0 \\
y^2 - bx^2 - 2cx - 3d &= 0
\end{aligned}$$

So if P is a singular point then $y_0 = 0$. Let $f(x) = ax^3 + bx^2 + cx + d$. We are left with:

$$\begin{array}{rclcl}
f(x_0) & = & ax_0^3 + bx_0^2 + cx_0 + d & = & 0 \\
f'(x_0) & = & 3ax_0^2 + 2bx_0 + c & = & 0 \\
bx^2 + 2cx + 3d & = & 3f(x_0) - x_0 f'(x_0) & = & 0
\end{array}$$

We see these equations are linearly dependent - the third equation is redundant. We have shown that $P = (x_0, y_0, 1)$ is a singular point of F $\Leftrightarrow$ $y_0 = f(x_0) = f'(x_0) = 0$. Such a point exists $\Leftrightarrow$ $f(x) = ax^3 + bx^2 + cx + d$ has a multiple root. □

2.7 Calculating the Discriminant of a Cubic

Let $f(x) \in \mathbb{C}[x]$ be a cubic polynomial. We know that $y^2 = f(x)$ is a singular curve iff $f(x)$ has a multiple root by Lemma 2.6. ¿From Definition 2.5 $f(x)$ has a multiple root iff the discriminant of f is zero. This gives us a convenient way of checking if a curve in the Normal Form (defined in 2.4) $y^2 = x^3 - 27c_4x - 54c_6$ is singular.

At the moment the discriminant of f is defined in terms of the roots of f. It will be useful to a have a description of the discriminant in terms of the coefficients of f. Let r_1, r_2, r_3 be the roots of f. Then

$$f(x) = (x - r_1)(x - r_2)(x - r_3) = x^3 - \alpha x^2 + \beta x - \gamma$$

where $\alpha = r_1 + r_2 + r_3$, $\beta = r_1r_2 + r_1r_3 + r_2r_3$, $\gamma = r_1r_2r_3$ are the three elementary symmetric polynomials in r_1, r_2, r_3. A Theorem of Newton tells us that every symmetric polynomial is expressible as a polynomial of the elementary symmetric polynomials. The discriminant is a symmetric polynomial in r_1, r_2, r_3 so we can express it as a polynomial in α, β, γ. To do this we use a cunning determinant trick (see [Kn, Prop.III.3.3]):

Let $M = \begin{pmatrix} 1 & 1 & 1 \\ r_1 & r_2 & r_3 \\ r_1^2 & r_2^2 & r_3^2 \end{pmatrix}$. Then $det(M) = (r_3 - r_2)(r_3 - r_1)(r_2 - r_1)$.

The discriminant of f is given by

$$\begin{aligned} d &= \prod_{1 \le i < j \le deg(f)} (r_i - r_j)^2 \\ &= (det(M))^2 = det(M)det(M^T) = det(MM^T) \end{aligned}$$

Now $MM^T = \begin{pmatrix} 1 & 1 & 1 \\ r_1 & r_2 & r_3 \\ r_1^2 & r_2^2 & r_3^2 \end{pmatrix} \begin{pmatrix} 1 & r_1 & r_1^2 \\ 1 & r_2 & r_2^2 \\ 1 & r_3 & r_3^2 \end{pmatrix} = \begin{pmatrix} 3 & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_2 & \sigma_3 & \sigma_4 \end{pmatrix}$

where $\sigma_i = r_1^i + r_2^i + r_3^i$.

$$\begin{aligned} \sigma_1 &= r_1 + r_2 + r_3 = \alpha \\ \sigma_2 &= r_1^2 + r_2^2 + r_3^2 = (r_1 + r_2 + r_3)^2 - 2(r_1r_2 + r_1r_3 + r_2r_3) = \alpha^2 - 2\beta \\ \sigma_3 &= r_1^3 + r_2^3 + r_3^3 \\ &= (r_1 + r_2 + r_3)^3 - 3(r_1 + r_2 + r_3)(r_1r_2 + r_1r_3 + r_2r_3) + 3r_1r_2r_3 \\ &= \alpha^3 - 3\alpha\beta + 3\gamma \\ \sigma_4 &= \alpha^4 - 2\alpha^2\beta + 2\beta^2 + 4\alpha\gamma. \end{aligned}$$

We have expressed the discriminant of a cubic polynomial f in terms of its coefficients. Let's use this to find the discriminant, d, of $x^3 - 27c_4x - 54c_6$ in terms of c_4 and c_6.

$\alpha = 0, \beta = -27c_4, \gamma = 54c_6$

$$\begin{aligned} \sigma_1 &= \alpha = 0 \\ \sigma_2 &= \alpha^2 - 2\beta = 2 \cdot 3^3 c_4 \\ \sigma_3 &= \alpha^3 - 3\alpha\beta + 3\gamma = 2 \cdot 3^4 c_6 \\ \sigma_4 &= \alpha^4 - 2\alpha^2\beta + 2\beta^2 + 4\alpha\gamma = 2 \cdot 3^6 c_4^2 \\ d &= det \begin{pmatrix} 3 & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_2 & \sigma_3 & \sigma_4 \end{pmatrix} \\ &= det \begin{pmatrix} 3 & 0 & 2 \cdot 3^3 c_4 \\ 0 & 2 \cdot 3^3 c_4 & 2 \cdot 3^4 c_6 \\ 2 \cdot 3^3 c_4 & 2 \cdot 3^4 c_6 & 2 \cdot 3^6 c_4^2 \end{pmatrix} \\ &= 3(2^2 \cdot 3^9 c_4^3 - 2^2 \cdot 3^8 c_6^2) + 2 \cdot 3^3 c_4(-2^2 3^6 c_4^2) \\ &= 2^2 \cdot 3^9 (c_4^3 - c_6^2). \end{aligned}$$

2.8 More About Discriminants

The roots of the quadratic polynomial $ax^2 + bx + c$ are $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$ and the discriminant is $b^2 - 4ac$.

Let $x^3 + ax^2 + bx + c$ be a cubic. Complete the cube to bring it to the form $X^3 + pX + q$. If $p = 0$ we have $X^3 + q$ which has discriminant $-27q^2$. If $q = 0$ we have $X(X^2 + p)$ which has discriminant $-4p^3$.

Now assume that $pq \neq 0$. Note that $X = 0$ is a solution iff $q = 0$.
$f : \mathbb{C}\backslash\{0\} \to \mathbb{C}\backslash\{0\}$, $Z \mapsto Z - \frac{p}{3Z}$ is a 2-to-1 function since for each $X \in \mathbb{C}\backslash\{0\}$, $\frac{X\pm\sqrt{X^2+4p/3}}{2} \mapsto X$. We find the roots of the cubic by substituting $Z - \frac{p}{3Z}$ for X and solving for Z. We get $Z^3 + q - \frac{p^3}{27Z^3}$. So solve $Z^6 + qZ^3 - \frac{p^3}{27}$ which is a quadratic in Z^3: $Z^3 = \frac{-q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$. The six solutions for Z must yield the three solutions for X (i.e. the solutions for Z pair off). We can calculate that the discriminant of $X^3 + pX + q$ is therefore $-4p^3 - 27q^2$.

Above we showed that the discriminant of the cubic $x^3 - 27c_4x - 54c_6$ is $2^2 \cdot 3^9(c_4^3 - c_6^2)$. Plug $p = -27c_4$, $q = 54c_6$ into $-4p^3 - 27q^2$ and we do indeed get $2^2 \cdot 3^9(c_4^3 - c_6^2)$.

2.9 Definition

Recall from Lemma 2.3 that any curve in Weierstrass Form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ is projectively equivalent to a curve in the Normal Form $y^2 = x^3 - 27c_4x - 54c_6$. The discriminant of a curve in Weierstrass Form is

$$\Delta := \frac{c_4^3 - c_6^2}{1728}$$

Singularity is preserved by projective changes of coordinates so a curve in Weierstrass Form is singular iff the corresponding curve in Normal Form from Lemma 2.3 is singular. By Lemma 2.6 the curve in Normal Form is singular iff $x^3 - 27c_4x - 54c_6$ has repeated roots. $x^3 - 27c_4x - 54c_6$ has repeated roots iff its discriminant (Definition 2.5), $d = 2^2 \cdot 3^9(c_4^3 - c_6^2)$ is zero. d is zero iff Δ is zero by the definition of Δ.

So a curve in Weierstrass Form is singular iff its discriminant, $\Delta = 0$. We see that elliptic curves are precisely curves in Weierstrass Form with non-zero discriminant.

2.10 Definition

An admissable change of coordinates is a projective change of coordinates of the form

$\phi = \begin{pmatrix} u^2 & 0 & r \\ su^2 & u^3 & t \\ 0 & 0 & 1 \end{pmatrix}$ where $r,\, s,\, t,\, u \in \mathbb{C},\, u \neq 0$.
Note that $det(\phi) = u^5 \neq 0$ so $\phi \in PGl_3(\mathbb{C})$.

2.11 Lemma

The set of admissable changes of coordinates is a subgroup of $PGl_3(\mathbb{C})$.

Proof

Inverse:
$$\phi^{-1} = \begin{pmatrix} u^{-2} & 0 & -ru^{-2} \\ -su^{-3} & u^{-3} & u^{-3}(rs-t) \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} U^2 & 0 & R \\ SU^2 & U^3 & T \\ 0 & 0 & 1 \end{pmatrix}$$
where $R = -ru^{-2}$, $S = -su^{-1}$, $T = u^{-3}(rs-t)$, $U = u^{-1} \neq 0$.

Closure:
$$\begin{pmatrix} u_1^2 & 0 & r_1 \\ s_1u_1^2 & u_1^3 & t_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} u_2^2 & 0 & r_2 \\ s_2u_2^2 & u_2^3 & t_2 \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} u_1^2u_2^2 & 0 & r_2u_1^2 + r_1 \\ s_1u_1^2u_2^2 + s_2u_1^3u_2^2 & u_1^3u_2^3 & r_2s_1u_1^2 + u_1^3t_2 + t_1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} U^2 & 0 & R \\ SU^2 & U^3 & T \\ 0 & 0 & 1 \end{pmatrix}$$
where $R = r_2u_1^2 + r_1$, $S = s_1 + s_2u_1u_2$, $T = r_2s_1u_1^2 + u_1^3t_2 + t_1$, $U = u_1u_2 \neq 0$. □

2.12 Theorem

Let $F(X,Y,Z) = (Y^2Z + a_1XYZ + a_3YZ^2) - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3)$ be a curve in Weierstrass Form and $\phi^{-1} = \begin{pmatrix} u^2 & 0 & r \\ su^2 & u^3 & t \\ 0 & 0 & 1 \end{pmatrix}$ be an admissable change of coordinates. Then F^ϕ is a curve in Weierstrass Form. Under this change of coordinates the flex at (0,1,0) remains at (0,1,0) and the tangent line at (0,1,0) remains $(Z = 0)$.

Admissable changes of coordinates are the only projective changes of coordinates that keep F in Weierstrass Form, send the flex at $(0,1,0)$ to itself and preserve its tangent line $(Z = 0)$.

Proof

For the first part Z is preserved by an admissable change of coordinates. As was remarked in Definition 1.1 $F^\phi(\mathbb{C}) = \phi(F(\mathbb{C}))$. So the only point at infinity in $F^\phi(\mathbb{C})$ is $\phi(0,1,0) = (0,1,0)$. So instead of plugging in $\phi(X,Y,Z)$ for (X,Y,Z) and then putting Z=1, we can work in the affine piece (Z=1), taking

$x' = u^2x + r, y' = u^3y + su^2x + t$ as our admissable change of coordinates.

$$\begin{aligned}
&\{y'^2 + a_1x'y' + a_3y'\} - \{x'^3 + a_2x'^2 + a_4x' + a_6\} \\
&\quad = \{(u^3y + su^2x + t)^2 + a_1(u^2x + r)(u^3y + su^2x + t) + a_3(u^3y + su^2x + t)\} \\
&\qquad - \{(u^2x + r)^3 + a_2(u^2x + r)^2 + a_4(u^2x + r) + a_6\} \\
&\quad = \{y^2 + u^{-1}(2s + a_1)xy + u^{-3}(2t + a_1r + a_3)y\}u^6 \\
&\qquad - \{x^3 + u^{-2}(-s^2 - a_1s + 3r + a_2)x^2 \\
&\qquad\qquad + u^{-4}(-2st - a_1t - rs - a_3s + 3r^2 + 2a_2r + a_4)x \\
&\qquad\qquad + u^{-6}(-t^2 - a_1rt - a_3t + r^3 + a_2r^2 + a_4r + a_6)\}u^6
\end{aligned}$$

We have the curve

$$\begin{aligned}
&y^2 + u^{-1}(2s + a_1)xy + u^{-3}(2t + a_1r + a_3)y \\
&= x^3 + u^{-2}(-s^2 - a_1s + 3r + a_2)x^2 \\
&\quad +u^{-4}(-2st - a_1t - rs - a_3s + 3r^2 + 2a_2r + a_4)x \\
&\quad +u^{-6}(-t^2 - a_1rt - a_3t + r^3 + a_2r^2 + a_4r + a_6)
\end{aligned}$$

so Weierstrass Form is preserved. We know (0,1,0) was sent to (0,1,0) and by the comments after Definition 2.1 it is still a flex with tangent line ($Z = 0$).

Note that the coefficients are powers of u (multiplied by a lot of junk). This explains the mysterious subscripts chosen for the a_i coefficients in Weierstrass Form. After an admissable change of coordinates they are multiples of u^{-i}. In the case that $r = s = t = 0$, i.e. $\phi = \begin{pmatrix} u^2 & 0 & 0 \\ 0 & u^3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, the curve

$$\begin{aligned}
y^2 + a_1xy + a_3y &= x^3 + a_2x^2 + a_4x + a_6 \quad \text{becomes the curve} \\
y^2 + a_1u^{-1}xy + a_3u^{-3}y &= x^3 + a_2u^{-2}x^2 + a_4u^{-4}x + a_6u^{-6}.
\end{aligned}$$

It remains to show that admissable changes of coordinates are the only projective changes of coordinates that keep F in Weierstrass Form, send the flex at $(0, 1, 0)$ to itself and preserve the tangent line $Z = 0$.

Let $\phi^{-1} = \begin{pmatrix} \alpha & \beta & \gamma \\ \delta & \epsilon & \zeta \\ \eta & \theta & \iota \end{pmatrix}$.

$\phi^{-1}(0, 1, 0) = (0, 1, 0)$ so $\beta = \theta = 0$.

We also require that the tangent line to $F(\phi^{-1}(X, Y, Z))$ at (0,1,0) be ($Z = 0$). Thus $\frac{\partial(F\circ\phi^{-1})}{\partial X} = 0$ at (0,1,0). We know from multi-variable calculus that:

$\frac{\partial(F\circ\phi^{-1})}{\partial X} |_{(0,1,0)}= D(F \circ \phi^{-1})_{(0,1,0)}(e_1)$ where $DG |_P$ is the total derivative of G at P and $e_1 = (1, 0, 0)$. So

$$\frac{\partial(F\circ\phi^{-1})}{\partial X} |_{(0,1,0)}= D(F \circ \phi^{-1})_{(0,1,0)}(e_1) = DF|_{\phi^{-1}(0,1,0)} \circ D\phi^{-1}|_{(0,1,0)}(e_1)$$

$$= DF|_{(0,1,0)} \circ \phi^{-1}(e_1) = \begin{pmatrix} \frac{\partial F}{\partial X} & \frac{\partial F}{\partial Y} & \frac{\partial F}{\partial Z} \end{pmatrix} |_{(0,1,0)} \begin{pmatrix} \alpha \\ \delta \\ \eta \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \delta \\ \eta \end{pmatrix} = \eta$$

(Recall from 2.1 that $\begin{pmatrix} \frac{\partial F}{\partial X} & \frac{\partial F}{\partial Y} & \frac{\partial F}{\partial Z} \end{pmatrix} |_{(0,0,1)} = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}$).

Thus $\eta = 0$ and $\phi^{-1} = \begin{pmatrix} \alpha & 0 & \gamma \\ \delta & \epsilon & \zeta \\ 0 & 0 & \iota \end{pmatrix}$. We are working in $PGL_3(\mathbb{C})$ so we can multiply ϕ^{-1} by ι^{-1}. This shows that ϕ^{-1} preserves Z. So again we can work in the affine piece $(Z = 1)$ and consider the change of coordinates $x' = \alpha x + \gamma$, $y' = \delta x + \epsilon y + \zeta$. Take the curve $y'^2 = x'^3$. Our change of coordinates must preserve Weierstrass Form so we see that $\alpha^3 = \epsilon^2$. Thus $\phi^{-1} = \begin{pmatrix} u^2 & 0 & \gamma \\ \delta & u^3 & \zeta \\ 0 & 0 & \iota \end{pmatrix}$ where $u = \alpha^{1/2} = \epsilon^{1/3}$. After multiplying by ι^{-1} this is an admissable change of coordinates. Note that the δ term is OK because we can choose s so be anything we like. □

2.13 Definition

The mysterious subscripts of the coefficients of a curve in Weierstrass Form were discussed in the proof of Theorem 2.12. Define i to be the weight of a_i.

Note that the product $a_i a_j$ has weight $i + j$ since if a_i is sent to a multiple of u^{-i} by an admissable change of coordinates and a_j is sent to a multiple of u^{-j} then the product of what they are sent to is a multiple of $u^{-(i+j)}$. Similarly a_i^{-1} has weight $-i$ and the sum $\alpha a_i + \beta b_i$ has weight i for any $0 \neq (\alpha, \beta) \in \mathbb{C}^2$.

2.14 Remark

Let $F = Y^2Z + YZ^2 - X^3$, $\phi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. Then $F^\phi = F$, but ϕ is not an admissable change of coordinates. In this example the Weierstrass Form is preserved, but (0,1,0) is taken to (0,0,1). In fact the curve has flexes at $(0, 1, 0)$ and $(0, 0, 1)$. ϕ simply swaps them.

So there are projective changes of coordinates which preserve Weierstrass Form that are not admissable changes of coordinates, but these do not satisfy the conditions that the flex at (0,1,0) be preserved and the tangent line remain (Z=0).

2.15 Definition

Two elliptic curves F_1 and F_2 are isomorphic if there is an admissable change of coordinates ϕ such that $F_1^\phi = F_2$. We write $F_1 \cong F_2$.

2.16 Definition

The j-invariant of an elliptic curve is

$$j := \frac{c_4^3}{\Delta} = \frac{1728c_4^3}{c_4^3 - c_6^2},$$

where Δ is the discriminant as defined in 2.9.
Note that j is defined because $\Delta \neq 0$ for a nonsingular curve.

By the remarks after Definition 2.13 c_4 has weight 4, c_6 has weight 6, Δ has weight 12 and j has weight 0. We justify the name invariant in the next Theorem.

2.17 Theorem

Two elliptic curves are isomorphic iff they have the same j-invariant. For every $j \in \mathbb{C}$ there exists an elliptic curve with that j-invariant.

Thus j : {isomorphism classes of elliptic curves} $\to \mathbb{C}$ is a bijection.

Proof

Consider two elliptic curves in Normal Form:

$$\begin{aligned} C &: (y^2 = x^3 - 27c_4x - 54c_6) \\ D &: (y^2 = x^3 - 27d_4x - 54d_6) \end{aligned}$$

Claim $C \cong D \Leftrightarrow \exists u \neq 0$ s.t. $c_4 = u^4 d_4$ and $c_6 = u^6 d_6$.

($\Rightarrow$) Recall from the first underlined section of Theorem 2.12 that admissable changes of coordinates are $x' = u^2x + r$,$y' = u^3y + su^2x + t$ where $r, s, t, u \in \mathbb{C}$, $u \neq 0$. Plug this into C:

$$\begin{aligned} (u^3y + su^2x + t)^2 &= (u^2x + r)^3 - 27c_4(u^2x + r) - 54c_6 \\ u^6y^2 + 2su^5xy + 2tu^3y &= u^6x^3 + (3ru^4 - s^2u^4)x^2 \\ &+ (3r^2u^2 - 2stu^2 - 27c_4u^2)x + (r^3 - t^2 - 27c_4r - 54c_6) \end{aligned}$$

$C \cong D$ so there is a choice of r, s, t, u bringing this mess to the form of D.

The coefficient of $xy = 0$ so $s = 0$ (because $u \neq 0$)
And the coefficient of $y = 0$ so $t = 0$.
And the coefficient of $x^2 = 0$ so $r = 0$.

So we have $u^6y^2 = u^6x^3 - 27c_4u^2x - 54c_6$, which is the same curve as $y^2 = x^3 - 27u^{-4}c_4x - 54u^{-6}c_6$. This is the only way we can get to this form so $\exists u \neq 0$ s.t. $c_4 = u^4d_4$ and $c_6 = u^6d_6$.

($\Leftarrow$) Just take $x' = u^2x^2$, $y' = u^3y$ as the admissable change of coordinates.

Now let E be an elliptic curve. We showed in Lemma 2.3 that E is projectively equivalent to a curve in Normal Form. In one step the change of coordinates used was

$$x' = 36x + 3b_2, y' = 216y + 108a_1x + 108a_3.$$

This is an admissable change of coordinates with $u = 6$. So we showed in Lemma 2.3 that every elliptic curve E is isomorphic to a curve in Normal Form.

Let E be an elliptic curve isomorphic to C and F an Elliptic Curve isomorphic to D. By Lemma 2.11 the set of admissable changes of coordinates is a group so $E \cong F \Leftrightarrow C \cong D$. The claim above showed that $C \cong D \Leftrightarrow \exists u \neq 0$ s.t. $c_4 = u^4 d_4$ and $c_6 = u^6 d_6$.

The j-invariant of E is defined to be $j_E = \frac{1728 c_4^3}{c_4^3 - c_6^2}$.

$E \cong F \Rightarrow C \cong D \Rightarrow \exists u \neq 0$ s.t. $c_4 = u^4 d_4$ and $c_6 = u^6 d_6$.
So the j-invariant of F is $j_E = \frac{1728 c_4^3}{c_4^3 - c_6^2} = \frac{1728(d_4 u^4)^3}{(d_4 u^4)^3 - (d_6 u^6)^2} = \frac{1728 d_4^3}{d_4^3 - d_6^2} = j_F$.

Conversely if $j_E = j_F$ then (assuming c_4,$d_4 \neq 0$), $\frac{1728}{1 - c_6^2/c_4^3} = \frac{1728}{1 - d_6^2/d_4^3}$. So $\frac{c_6^2}{c_4^3} = \frac{d_6^2}{d_4^3}$. Now $\exists v \neq 0$ s.t. $c_4 = v^4 d_4$. But then $c_6^2 d_4^3 = d_6^2 v^{12} d_4^3$ so $c_6^2 = v^{12} d_6^2 \Rightarrow c_6 = \pm v^6 d_6$. If $c_6 = +v^6 d_6$ let $u = v$. If $c_6 = -v^6 d_6$ let $u = \sqrt{-1}v$. Then $c_4 = u^4 d_4$ and $c_6 = u^6 d_6$. So $C \cong D$ and thus $E \cong F$.
If $c_4 = 0$ then $j_E = 1728 = j_F$ so $d_4 = 0$. Similarly if $d_4 = 0$ then $c_4 = 0$. In this case $C : (y^2 = x^3 - 54c_6)$, $D : (y^2 = x^3 - 54d_6)$. There exists $u \neq 0$ s.t. $c_6 = u^6 c_6$ so $C \cong D$ and thus $E \cong F$.

We have shown that $j : \{\text{isomorphism classes of elliptic curves}\} \to \mathbb{C}$ is a well-defined injection. It remains to show that it is a surjection. Fix $j \in \mathbb{C}$.

If $j = 0$ then take $c_4 = 0$ and $c_6 \neq 0$. That is take the curve $y^2 = x^3 - 54c_6$. If $j = 1728$ then take $c_6 = 0$ and $c_4 \neq 0$. Note that in both cases $\Delta \neq 0$ so these are indeed nonsingular and hence elliptic curves.

If $j \neq 0, 1728$ take $c_4 = c_6 = \frac{j}{j - 1728}$. The curve $y^2 = x^3 - 27c_4 x - 54c_6$ has $\Delta = \frac{j^2}{(j-1728)^3}$ and j-invariant j as required. □

It will be useful to have a formula for the discriminant and j-invariant of the curve $y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$. Recall this was the intermediate curve used in the proof of Lemma 2.3.

$$\begin{aligned}
c_4^3 &= b_2^6 - 2^3 \cdot 3^2 b_2^4 b_4 + 2^6 \cdot 3^3 b_2^2 b_4^2 - 2^9 \cdot 3^3 b_4^3 \\
c_6^2 &= b_2^6 - 2^3 \cdot 3^2 b_2^4 b_4 + 2^4 \cdot 3^3 b_2^3 b_6 + 2^4 \cdot 3^4 b_2^2 b_4^2 - 2^6 \cdot 3^5 b_2 b_4 b_6 + 2^6 \cdot 3^6 b_6^2 \\
\Delta &= \frac{c_4^3 - c_6^2}{1728} = b_2^2 b_4^2 - 2^3 b_4^3 - \frac{b_2^3 b_6}{2^2} - \frac{3 b_2^2 b_4^2}{2^2} + 3^2 b_2 b_4 b_6 - 3^3 b_6^2 \\
&= b_2^2 (\frac{b_4^2}{4} - \frac{b_2 b_6}{4}) - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6
\end{aligned}$$

We define $b_8 := \frac{b_2 b_6}{4} - \frac{b_4^2}{4}$ so that $\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6$. $j = \frac{c_4^3}{\Delta}$.

If we had started with a curve in general Weierstrass Form with coefficients a_i then we could express b_8 in terms of the a_i as follows.

$$\begin{aligned} b_8 &= \frac{b_2 b_6}{4} - \frac{b_4^2}{4} \\ &= \frac{(a_1^2 + 4a_2)(a_3^2 + 4a_6)}{4} - \frac{(2a_4 + a_1 a_3)^2}{4} \\ &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2. \end{aligned}$$

2.18 Summary of Key Points from Chapter 2

1. An elliptic curve is a nonsingular cubic in Weierstrass Form $(y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6)$.

2. $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$. $(y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6)$.

3. $c_4 = b_2^2 - 24b_4$, $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$. Normal Form: $(y^2 = x^3 - 27c_4x - 54x_6)$.

4. The discriminant, $\Delta = \frac{c_4^3 - c_6^2}{1728}$. The j-invariant, $j = \frac{c_4^3}{\Delta} = \frac{1728c_4^3}{c_4^3 - c_6^2}$.

5. An admissable change of coordinates, $x' = u^2x + r$, $y' = u^3y + su^2x + t$ where $u \neq 0$. Two elliptic curves are isomorphic if they are related by an admissable change of coordinates. $j : \{\text{isomorphism classes of elliptic curves}\} \to \mathbb{C}$ is a bijection.

6. The subscripts of the coefficients of a curve in Weierstrass Form are called weights. a_i, b_i, c_i have weight i. Δ has weight 12 and j has weight 0.

3 Complex Tori

In this chapter we look at elliptic curves from a different perspective. Define a lattice $\Lambda := \omega_1\mathbb{Z} + \omega_2\mathbb{Z} \subset \mathbb{C}$ where $\omega_1, \omega_2 \in \mathbb{C}\backslash\{0\}$ and $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$. That is ω_1 and ω_2 are linearly independent over $\mathbb{R}$. A complex torus is defined to be $\mathbb{C}/\Lambda$. Topologically it is a torus. We are going to show there is a correspondence between complex tori and elliptic curves.

3.1 Definition

Fix a lattice $\Lambda \subset \mathbb{C}$. Define

$$\begin{aligned} \wp : \mathbb{C}\backslash\Lambda &\to \mathbb{C} \\ \wp(z) &= \frac{1}{z^2} + \sum_{\omega\in\Lambda\backslash\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) \end{aligned}$$

This is called the Weierstrass $\wp$ - function.

$\wp$ is a meromorphic function with double poles at the points of Λ. The $-\frac{1}{\omega^2}$ term in the sum insures that the sum converges absolutely. $\wp$ is an example of an elliptic function - a doubly periodic meromorphic function. We can view an elliptic function as a well-defined meromorphic function from $\mathbb{C}/\Lambda \to \mathbb{C}$.

$$\begin{aligned} \frac{1}{\omega - z} &= \frac{1/\omega}{1 - z/\omega} = \frac{1}{\omega}(1 + \frac{z}{\omega} + \frac{z^2}{\omega^2} + ...) \\ \frac{1}{(\omega - z)^2} &= \frac{1}{\omega^2}(1 + \frac{2z}{\omega} + \frac{3z^2}{\omega^2} + ...) = (\frac{1}{\omega^2} + \frac{2z}{\omega^3} + \frac{3z^2}{\omega^4} + ...) \\ \wp(z) - \frac{1}{z^2} &= \sum_{\omega\in\Lambda\backslash\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) \\ &= \sum_{k=1}^{\infty} (k+1)G_{k+2}z^k \\ \text{where } G_k &:= \sum_{\omega\in\Lambda\backslash\{0\}} \frac{1}{\omega^k}. \text{ Note that for odd } k,\ G_k = 0, \text{ and hence} \\ \wp(z) &= \frac{1}{z^2} + 3G_4z^2 + 5G_6z^4 + ... \\ \wp'(z) &= \frac{-2}{z^3} + 6G_4z + 20G_6z^3 + 42G_8z^5 + ... \end{aligned}$$

By direct computation we can show that
$(\wp'(z))^2 = 4\wp^3(z) - 60G_4\wp(z) - 140G_6 + P(z)$ where $P(z)$ is a polynomial in z with lowest term a multiple of z^7. $P(z)$ is an elliptic function since it is the sum of elliptic functions. $P(z)$ has no poles so is a bounded entire function. By Liouville's Theorem $P(z)$ is a constant but its lowest term is z^7 so it is zero.

We have shown that $\wp$ satisfies the differential equation $(\wp')^2 = 4\wp^3 - g_2\wp - g_3$ where $g_2 := 60G_4$ and $g_3 := 140G_6$. Define

$$\begin{array}{rcl} \varphi : \mathbb{C}/\Lambda & \rightarrow & \mathbb{P}^2_{\mathbb{C}} \\ \varphi(z) & = & \begin{cases} (\wp(z), \wp'(z), 1) & \text{if } z \notin \Lambda, \\ (0,1,0) & \text{if } z \in \Lambda. \end{cases} \end{array}$$

Because of the differential equation satisfied by $\wp$,
$\varphi(\mathbb{C}/\Lambda) \subset E : (Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3) \subset \mathbb{P}^2_{\mathbb{C}}$.

3.2 Theorem

$\varphi : \mathbb{C}/\Lambda \rightarrow E(\mathbb{C})$ is a holomorphic bijection with holomorphic inverse.

Proof [Kn, Thm.VI.6.14]

$\mathbb{C}/\Lambda$ is a 1-dimensional complex manifold; $\mathbb{P}^2_{\mathbb{C}}$ is a 2-dimensional complex manifold. We want to show φ is holomorphic as a map of manifolds. Let $(x, y, 1) \in \varphi(\mathbb{C}/\Lambda)$. Use the chart map $(x, y, 1) \mapsto (x, y)$ in a neighbourhood of this point. We then have $z \mapsto (\wp(z), \wp'(z))$ which is holomorphic. In a nbhd of $(0, 1, 0)$ use the chart map $(x, 1, y) \mapsto (x, y)$. In this nbhd we have the map $0 \neq z \mapsto \left(\frac{\wp(z)}{\wp'(z)}, \frac{1}{\wp'(z)}\right)$ and $0 \mapsto (0, 0)$. $\wp$ and $\wp'$ have finitely many poles and zeroes in a compact subset of $\mathbb{C}$. So there is a punctured disc around 0 where this map has no zeroes or poles. Thus it is holomorphic on a punctured disc around 0 and is continuous at 0, so it is holomorphic at 0 too. This shows φ is holomorphic as map of complex manifolds.

Suppose $\varphi(z_1) = \varphi(z_2)$. That is $\wp(z_1) = \wp(z_2)$ and $\wp'(z_1) = \wp'(z_2)$. $\wp$ has a pole of order 2 at 0 and no other poles. Let Π be the parallelogram in $\mathbb{C}$ with vertices at 0, ω_1, ω_2 and $\omega_1 + \omega_2$. Translate Π in the complex plane to a parallelogram Π' s.t. $\wp$, $\wp'$ have no zeroes or poles on its boundary. From Complex Analysis $\int_{\partial\Pi'} \frac{z\wp'(z)}{\wp(z)}dz = \sum$ zeroes of $\wp - \sum$ poles of $\wp$. Now the integral is zero since $\wp$ is periodic so $z_1 = \overline{z_2}$ where $\overline{z}$ denotes complex conjugate. Thus $\wp'(z_1) = \wp'(\overline{z_2}) = \wp'(-z_2) = -\wp'(z_2)$ since
$\wp'(z) = -2\sum_{\omega\in\Lambda} \frac{1}{(z-\omega)^3}$ is an odd function. But by assumption $\wp'(z_1) = \wp'(z_2)$ so $\wp'(z_1) = \wp'(z_2) = 0$. Now $\wp'$ has a pole of order 3 at 0 and no other poles. $\int_{\Pi'} \frac{\wp'}{\wp}$ = (no. of zeroes of $\wp'$) $-$ (no. of poles of $\wp'$). So $\wp'$ has 3 zeroes. Since it is a periodic odd function $\omega_1/2$, $\omega_2/2$ and $(\omega_1 + \omega_2)/2$ are zeroes and therefore the only zeroes of $\wp'$. Thus z_1 is one of these three points and so $z_1 = \overline{z_1}$ and by the above $z_2 = \overline{z_1}$. Hence $z_1 = z_2$. Thus φ is injective.

To show φ is surjective fix $(a, b, 1) \in E(\mathbb{C})$. Since
$\int_{\Pi'} \frac{\wp'-a}{\wp-a}$ = (no. of zeroes of $\wp - a$) $-$ (no. on poles of $\wp - a$) and $\wp - a$ has a double pole at 0 we see $\exists\, z$ s.t. $\wp(z) = a$. Because of the differential equation satisfied by $\wp$, $b^2 = \wp'(z)^2$. If $\wp'(z) = -b$ then $\wp'(\overline{z}) = b$. Thus φ is surjective.

We have shown φ is a holomorphic bijection. We can show that it has a holomorphic inverse using the Inverse Function Theorem. $\square$

3.3 Corollary

With notations as in Theorem 3.2 $\varphi(\mathbb{C}/\Lambda)$ is an elliptic curve.

Proof

By the proof of Theorem 3.2 the zeroes of $\wp'$ are $\omega_1/2$, $\omega_2/2$ and $\omega_3 := (\omega_1 + \omega_2)/2$. Now $\wp(z) - \wp(\omega_i)$ has a double zero at $\omega_i/2$. By the proof of Theorem 3.2 $\wp(z) - \wp(\omega_i)$ has the same number of zeroes and poles. So $\omega_i/2$ are its only zeroes. Thus $\wp(\omega_i) \neq \wp(\omega_j)$ for $i \neq j$. This shows that $4\wp^3 - g_2\wp - g_3$ has distinct zeroes in $\mathbb{C}$.

By Lemma 2.6, $\varphi(\mathbb{C}/\Lambda)$ is a nonsingular cubic. Thus $\varphi(\mathbb{C}/\Lambda)$ is an elliptic curve except for the factor of $4X^3$ instead of X^3. This is a minor point and defining an elliptic curve to have $4X^3$ would not affect the content of Section 2 very much. In fact the only change would be to substitute $y/2$ for y in the normal form. It was presented in that way because the notation is absolutely standard. $\square$

In the remarks before Summary 2.18 we looked at Δ and j for a curve in the form $y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$.
We have the curve $y^2 = 4x^3 - g_2x - g_3$. Using notation as in the remarks before Summary 2.18, $b_2 = 0$, $b_4 = \frac{-g_2}{2}$, $b_6 = -g_3$ so $\Delta = -8b_4^3 - 27b_6^2 = g_2^3 - 27g_3^2$ and $c_4 = -2^9 \cdot 3^3 b_4^3 = 2^6 \cdot 3^3 g_2^3$. Thus $j = \frac{c_4^3}{\Delta} = \frac{1728 g_2^3}{g_2^3 - 27g_3^2}$.

3.4 Definition

The j-invariant of a lattice $\Lambda \subset \mathbb{C}$ is defined to be $j(\Lambda) := \frac{1728 g_2^3}{g_2^3 - 27g_3^2}$.

A holomorphic bijection with holomorphic inverse is a homeomorphism so by Corollary 3.3 a complex torus is topologically equivalent to an elliptic curve. Given any elliptic curve in $\mathbb{P}^2_{\mathbb{C}}$ we can bring it to the form $E : (y^2 = 4x^3 - ax - b)$ and to this we can associate a complex torus, although this is not trivial. The Uniformization Theorem says that there exists a unique lattice $\Lambda \subset \mathbb{C}$ s.t. $g_2(\Lambda) = a$ and $g_3(\Lambda) = b$. For a proof see [Sh, 4.2].

We say two complex tori are conformally equivalent if there is an analytic bijection between them. Conformal equivalence is an equivalence relation. We want to know when two complex tori are conformally equivalent.

3.5 Theorem

Two complex tori $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are conformally equivalent iff $\exists\, G \in Aut(\mathbb{C}) = \{\text{bijective analytic } \mathbb{C} \to \mathbb{C}\}$ s.t. $\Lambda_1 = G^{-1}\Lambda_2 G$.

Proof

Let $p_i : \mathbb{C} \to \mathbb{C}/\Lambda_i$ be the natural covering maps and let $f : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ be an analytic bijection. Fix $z \in \mathbb{C}$ and pick $w \in \mathbb{C}$ such that $p_2(w) = f(p_1(z))$. Set $G(z) = w$. Take $z' \in \mathbb{C}$. Let γ be a curve with $\gamma(0) = z$ and $\gamma(1) = z'$. We get a curve $f \circ p_1 \circ \gamma$ from $f(p_1(z))$ to $f(p_1(z'))$. Let Γ be the lift of $f \circ p_1 \circ \gamma$ starting at w. Let $w' = \Gamma(1)$ and set $G(z') = w'$. If $\widetilde{\gamma}$ is a different curve from z to z' then $\widetilde{\gamma}$ is homotopic to γ. So $f \circ p_1 \circ \widetilde{\gamma}$ is homotopic to $f \circ p_1 \circ \gamma$ and so by the Monochromy Theorem their lifts Γ and $\widetilde{\Gamma}$ are homotopic as $\Gamma(0) = \widetilde{\Gamma}(0) = w$. Hence $\Gamma(1) = \widetilde{\Gamma}(1) = w'$ so G is well-defined. $p_2 \circ G = f \circ p_1$. This shows that $G : \mathbb{C} \to \mathbb{C}$ is analytic. Because of uniqueness of lifting and because f is invertible Γ determines γ uniquely. In particular $\Gamma(1) = w'$ determines $\gamma(1) = z'$. Hence G is injective and surjective. $G \in Aut(\mathbb{C})$.

We now show $\Lambda_1 = G^{-1}\Lambda_2 G$. Take $g_1 \in Aut(\mathbb{C})$ with $g_1 = (z \mapsto z + \lambda_1)$ for some $\lambda_1 \in \Lambda_1$. Let $z' = g_1(z)$. Then $p_1(z') = p_1(z)$ so $f(p_1(z')) = f(p_1(z))$. In particular $f(p_1(\gamma(1))) = f(p_1(\gamma(0)))$ so $p_1 \circ \gamma$ and $f \circ p_1 \circ \gamma$ are closed loops. Hence $\exists g_2 \in \Lambda_2$ such that $\Gamma(1) = g_2\Gamma(0)$. ie. $G(g_1(z)) = g_2(G(z))$.
In fact, the same choices work for $\widetilde{z} \in$ (neighbourhood of z). By the Identity Principle $G \circ g_1 = g_2 \circ G : \mathbb{C} \to \mathbb{C}$. That is $\Lambda_1 = G^{-1}\Lambda_2 G$. □

3.6 Corollary

Two tori $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are conformally equivalent iff $\exists\, \alpha \in \mathbb{C}^*$ s.t. $\alpha\Lambda_1 = \Lambda_2$.

Proof

Suppose that $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are conformally equivalent. By Theorem 3.5, $\exists$ $G \in Aut(\mathbb{C}) = \{\text{bijective analytic } \mathbb{C} \to \mathbb{C}\}$ s.t. $\Lambda_1 = G^{-1}\Lambda_2 G$. It can be shown that $Aut(\mathbb{C}) = \{\alpha z + \beta | \alpha \neq 0\}$. With notation as in Theorem 3.5, $G(z) = \alpha z + \beta$, $\alpha \neq 0$. $G^{-1}(z) = \frac{z}{\alpha} - \frac{\beta}{\alpha}$.
$\forall \lambda_1 \in \Lambda_1$, $g_1 = (z \mapsto z + \lambda_1)$, $\exists\, g_2 = (z \mapsto z + \lambda_2)$ such that $g_1 = G^{-1} g_2 G$.
$(z \mapsto z + \lambda_1) = \left(z \mapsto \frac{1}{\alpha}((\alpha z + \beta) + \lambda_2) - \frac{\beta}{\alpha}\right) = \left(z \mapsto z + \frac{\lambda_2}{\alpha}\right)$
i.e. $\lambda_2 = \alpha\lambda_1$ so $\alpha\Lambda_1 \subset \Lambda_2$. By the symmetry of the argument $\Lambda_2 \subset \alpha\Lambda_1$.

Conversely if $\exists\, \alpha \in \mathbb{C}^*$ s.t. $\alpha\Lambda_1 = \Lambda_2$ then $f : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$, $z \mapsto \alpha z$ is an analytic bijection. □

3.7 Corollary

Two elliptic curves are isomorphic iff the associated complex tori are conformally equivalent.

Proof

By Corollary 3.6 two complex tori $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are conformally equivalent iff $\exists\, \alpha \in \mathbb{C}^*$ such that $\alpha\Lambda_1 = \Lambda_2$. Observe that $g_2(\alpha\Lambda) = \alpha^{-4}g_2(\Lambda)$ and $g_3(\alpha\Lambda) = \alpha^{-6}g_3(\Lambda)$. By the proof of Theorem 2.17 the corresponding elliptic curves $y^2 = x^3 - g_2(\Lambda_1)x - g_3(\Lambda_1)$ and $y^2 = x^3 - g_2(\Lambda_2)x - g_3(\Lambda_2)$ are isomorphic iff $\exists\, \alpha \in \mathbb{C}^*$ such that $g_2(\Lambda_2) = \alpha^{-4}g_2(\Lambda_1)$ and $g_3(\Lambda_2) = \alpha^{-6}g_3(\Lambda_1)$. □

The j-invariant is therefore a bijection from the set of conformal equivalence classes of complex tori to the set of isomorphism classes of elliptic curves. Each conformal equivalence class contains exactly one lattice $\mathbb{Z} + \tau\mathbb{Z}$ where $Im(\tau) > 0$. We aim now to find a subset of the upper half plane containing exactly one element from each conformal equivalence class of complex tori. Let $\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$.

3.8 Lemma

Two lattices $\omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ and $\omega_1'\mathbb{Z} + \omega_2'\mathbb{Z}$ are conformally equivalent $\Leftrightarrow$ $\exists\, M \in \mathrm{PSL}_2(\mathbb{Z})$ s.t. $M\begin{pmatrix}\omega_1'\\ \omega_2'\end{pmatrix} = \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$

Proof

($\Leftarrow$) We can express ω_1' and ω_2' in terms of ω_1 and ω_2. Now $M^{-1}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} = \begin{pmatrix}\omega_1'\\ \omega_2'\end{pmatrix}$ so we can also express ω_1 and ω_2 in terms of ω_1' and ω_2'. Hence the lattices are the same.

($\Rightarrow$) After multiplying through by some constant α we can write $\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\omega_1'\\ \omega_2'\end{pmatrix}$ for some $a, b, c, d \in \mathbb{Z}$.
Similarly $\begin{pmatrix}\omega_1'\\ \omega_2'\end{pmatrix} = \begin{pmatrix}e & f\\ g & h\end{pmatrix}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ for some $e, f, g, h \in \mathbb{Z}$.
Thus $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}e & f\\ g & h\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ so $det\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \pm 1$.
Hence $M := \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z})$. □

3.9 Definition

The Fundamental Domain, D is defined to be
$D := \{\tau \in \mathbb{C} : -1/2 \leq Re(\tau) \leq 1/2 \text{ and } |\tau| \geq 1\}$.

3.10 Theorem

For every z in the upper half plane $\exists\ g \in \mathrm{PSL}_2(\mathbb{Z})$ s.t. $gz \in D$ and this point is unique (except for identifications on the boundary).

Proof [Kn, Thm.VIII.8.5]

Existence

Fix z in the upper half plane. Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z})$. Then $Im(gz) = \frac{Im(z)}{|cz+d|^2}$. Since c and d are integers there are are only finitely many choices such that $|cz+d|$ is less than a given number. Thus $\exists g \in \mathrm{PSL}_2(\mathbb{Z})$ s.t. $Im(gz)$ is a minimum. Choose $n \in \mathbb{N}$ s.t. $z' := \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} z$ has real part between $-1/2$ and $1/2$. If $|z'| < 1$ then $-1/z'$ would have imaginary part strictly greater than $Im(gz)$ contradicting the choice of g. Thus $|z'| \geq 1$ and $z' \in D$.

Uniqueness

Let z and gz be in D and $g \neq id$. We show they are both on the boundary of D. We can assume $Im(gz) \geq Im(z)$ and thus $|cz+d| \leq 1$. Thus $c \in \{0, \pm 1\}$. If $c = 0$ then $g = \begin{pmatrix} \pm 1 & b \\ 0 & \pm 1 \end{pmatrix}$ so both points lie on the boundary. If $c = \pm 1$ then since $|cz+d| \leq 1$, $d = 0$ except when $z = e^{\pi i/3}$ or $z = e^{2\pi i/3}$. If $d = 0$ then $|z| = 1$. We can explicitly check the cases $z = e^{\pi i/3}$ and $z = e^{2\pi i/3}$. □

j is a bijection from D to $\mathbb{C}$ except for identifications along the boundary. These identifications are $z \sim z+1$; and when $x^2 + y^2 = 1$, $x + iy \sim -x + iy$. Given a conformal equivalence class of complex tori j takes the unique representative $\mathbb{Z} + \tau\mathbb{Z}$ with $\tau \in D$ and gives the j-invariant of the corresponding isomorphism class of elliptic curves. The identifications along the boundary make $j : \overline{D/\sim} \to \mathbb{P}^1_{\mathbb{C}}$ a homeomorphism. $\overline{D/\sim}$ denotes the compactification of $D/\sim$,which is just $D/\sim$ plus one point, and $\mathbb{P}^1_{\mathbb{C}}$ is of course $\mathbb{C}$ plus one point.

In the proof of Corollary 3.7 we saw that $g_i(\alpha\Lambda) = \alpha^{-2i} g_i(\Lambda)$. By Lemma 3.8 and Theorem 3.10 this tells us that $g_i\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{2i} g_i(\tau)$. g_i is an example of a Modular Form of weight i. This ties in nicely with the notion of weight defined in 2.13. j has weight 0 which corresponds to it being invariant under a projective change of coordinates/conformal equivalence. Any modular form of weight 0 is actually a rational function of j.

3.11 Summary of Key Points from Chapter 3

1. An elliptic function is a doubly periodic meromorphic function. The Weierstrass $\wp$ function is an elliptic function. The $\wp$ function allows us to

forge a correspondence between complex tori and elliptic curves.

2. Lattices Λ_1 and Λ_2 are conformally equivalent iff $\exists\, \alpha \neq 0$ s.t. $\alpha\Lambda_1 = \Lambda_2$.

3. For a lattice Λ, $j(\Lambda) := \frac{1728 g_2^3}{g_2^3 - 27 g_3^2}$. j defines a bijection from the set of conformal equivalence classes of complex tori to the set of isomorphism classes of elliptic curves.

4 Complex Multiplication

Every additive abelian group G has trivial homomorphisms $g \mapsto ng \, \forall n \in \mathbb{Z}$. Elliptic curves come equipped with the structure of an additive abelian group. An elliptic curve $E(\mathbb{C})$ has complex multiplication if it has any nontrivial analytic homomorphisms $E(\mathbb{C}) \to E(\mathbb{C})$. We begin this section with a key lemma.

4.1 Lemma

If $f : \mathbb{C}/\Lambda \times \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ is a continuous function and is analytic in each variable then there exist $a, b, c \in \mathbb{C}$ such that $f(z_1, z_2) \equiv az_1 + bz_2 + c \bmod \Lambda$ for all $z_1, z_2 \in \mathbb{C}$.

Proof [Kn, Lem.VI.6.18]

Let $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. Lift to a function $F : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$.
Then for all $m, n \in \mathbb{Z}$ there exist $m', n' \in \mathbb{Z}$ such that $F(z_1 + m\omega_1 + n\omega_2, z_2) = F(z_1, z_2) + m'\omega_1 + n'\omega_2$.

$$\frac{\partial F}{\partial z_1}(z_1 + m\omega_1 + n\omega_2, z_2) = \frac{\partial F}{\partial z_1}(z_1, z_2),$$
$$\frac{\partial F}{\partial z_2}(z_1 + m\omega_1 + n\omega_2, z_2) = \frac{\partial F}{\partial z_2}(z_1, z_2).$$

$\frac{\partial F}{\partial z_1}$ and $\frac{\partial F}{\partial z_2}$ are periodic in the first variable. Thus they are bounded analytic functions and so by Liouville's Theorem they are constant.
Similarly they are constant in the second variable. We have $\frac{\partial F}{\partial z_1} = a$ and $\frac{\partial F}{\partial z_2} = b$.
Thus $f(z_1, z_2) = az_1 + bz_2 + c$ as required. □

We use this Lemma to show that the group defined on an elliptic curve $E(\mathbb{C})$ is isomorphic to the group on a torus. The group law on a torus is just addition mod Λ.

4.2 Theorem

$$\begin{aligned} \varphi : \mathbb{C}/\Lambda &\to E(\mathbb{C}) \\ z &\mapsto \begin{cases} (\wp(z), \wp'(z), 1) & \text{if } z \notin \Lambda, \\ (0, 1, 0) & \text{if } z \in \Lambda. \end{cases} \end{aligned}$$

is a group isomorphism.

Proof

Recall that φ is an analytic bijection with analytic inverse.
Define $f : \mathbb{C}/\Lambda \times \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ by $f(z_1, z_2) := \varphi^{-1}(\varphi(z_1) + \varphi(z_2))$. f satisfies the hypothesis of Lemma 4.1 so $f(z_1, z_2) \equiv az_1 + bz_2 + c \bmod \Lambda$.
Now $f(0,0) = 0$ and $f(z,0) = f(0,z) = z$. Thus $c = 0$ and $a = b = 1$. $f(z_1, z_2) = \varphi^{-1}(\varphi(z_1) + \varphi(z_2)) = z_1 + z_2$. Hence $\varphi(z_1 + z_2) = \varphi(z_1) + \varphi(z_2)$. □

4.3 Definition

An isogeny is an analytic map $h : E(\mathbb{C}) \to E(\mathbb{C})$ which fixes the identity of the group. That is $h(0,1,0) = (0,1,0)$.

4.4 Theorem

If $h : E(\mathbb{C}) \to E(\mathbb{C})$ is an isogeny then $h(\varphi(z)) = \varphi(az)$ for some $a \in \mathbb{C}$.

Proof

Let $f(z_1, z_2) := \varphi^{-1} \circ h \circ \varphi(z_1)$. f satisfies the hypothesis of Lemma 4.1 so $f(z_1, z_2) = az_1 + bz_2 + c$. f is constant w.r.t. z_2 and $h(\varphi(0)) = \varphi(0)$ so $f(z_1, z_2) = az_1$.
Thus $h(\varphi(z_1)) = \varphi(az_1)$ as required. □

Now $h(\varphi(z_1) + \varphi(z_2)) = \varphi(az_1 + az_2) = \varphi(az_1) + \varphi(az_2) = h(\varphi(z_1)) + h(\varphi(z_2))$ so an isogeny is a group homomorphism. An elliptic curve always has the trivial isogenies with $a \in \mathbb{Z}$. These are the trivial homomorphisms $G \to G$, $g \mapsto ng$ where $n \in \mathbb{Z}$, which exist for any additive abelian group.

4.5 Definition

An elliptic curve with any non-trivial isogenies is said to have
complex multiplication (or CM for short).

That is, there exist isogenies $h : E(\mathbb{C}) \to E(\mathbb{C})$, $h(\varphi(z)) = \varphi(az)$ with $a \in \mathbb{C} \backslash \mathbb{Z}$.

Note that if $a \in \mathbb{R} \backslash \mathbb{Z}$ then h is not well-defined as $h(\varphi(\omega_1)) = h(0,1,0) = (0,1,0) \neq \varphi(a\omega_1)$, since $a\omega_1 \notin \Lambda$. Thus any non-trivial isogenies are given by multiplication by a number $a \in \mathbb{C} \backslash \mathbb{R}$. Hence the name complex multiplication.

4.6 Theorem

An elliptic curve $\mathbb{Z} + \tau\mathbb{Z}$ has complex multiplication $h(\varphi(z)) = \varphi(az)$ iff τ lies in a quadratic imaginary extension field of $\mathbb{Q}$.

Proof

If $h : E(\mathbb{C}) \to E(\mathbb{C})$ is well-defined then $\forall z \in \Lambda$
$\varphi(az) = h(\varphi(z)) = h((0,1,0)) = (0,1,0)$.
Thus $az \in \Lambda\ \forall z \in \Lambda$ and so $a\Lambda \subset \Lambda$.
Conversely, if $a\Lambda \subset \Lambda$ then define $h(\varphi(z)) = \varphi(az)$. Let $z_1 \equiv z_2 \mod \Lambda$. Say $z_1 = z_2 + \omega$. Then $az_1 = az_2 + a\omega \in az_2 + \Lambda$. Thus $az_1 \equiv az_2 \mod \Lambda$. So h is well-defined. Thus $h(\varphi(z)) = \varphi(az)$ is an isogeny iff $a\Lambda \subset \Lambda$.

Suppose that $E(\mathbb{C})$ has complex multiplication. $1 \in \Lambda$ so $a = m + n\tau$ for some $m, n \in \mathbb{Z}$. Also by the above $a\tau = m' + n'\tau$ for some $m', n' \in \mathbb{Z}$.
Now $a\tau = (m + n\tau)\tau$, so $n\tau^2 + (m - n')\tau - m' = 0$.
τ satisfies a quadratic polynomial over $\mathbb{Z}$ and $\tau \in \mathbb{C}\backslash\mathbb{R}$ so τ lies in a quadratic imaginary extension of $\mathbb{Q}$.
Conversely, if τ lies in a quadratic imaginary extension of $\mathbb{Q}$ then $\exists \alpha, \beta, \gamma \in \mathbb{Z}$ such that $\alpha\tau^2 + \beta\tau + \gamma = 0$. Define $a = \alpha\tau \in \Lambda$. Then $a\tau = -\beta\tau - \gamma \in \Lambda$ and thus $a\Lambda \subset \Lambda$. Also $a \in \mathbb{C}\backslash\mathbb{R}$ as required. □

4.7 Corollary

The following categories are equivalent:

Objects:	Elliptic curves up to isomorphism	$\leftrightarrow$	Lattices up to homothety
Maps:	Isogenies	$\leftrightarrow$	$\{a \in \mathbb{C} \mid a\Lambda \subset \Lambda\}$

4.8 Definition

The set of isogenies of an elliptic curve E forms a ring with multiplication being composition of maps. This is called the Endomorphism Ring of E, denoted $End(E)$.

We know that $End(E)$ always contains $\mathbb{Z}$ as a subring. An elliptic curve has complex multiplication precisely when $End(E) \supsetneq \mathbb{Z}$.
With notation as in Theorem 4.6 $a = m + n\tau$, $a\tau = m' + n'\tau$.

$$\begin{aligned}
a^2 &= n^2\tau^2 + 2mn\tau + m^2 = -mn\tau + nn'\tau + m'n + 2mn\tau + m^2 \\
&= (m + n\tau)(m + n') + m'n - mn' = (m + n')a - (mn' - m'n) \\
a^2 &- (m + n')a + (mn' - m'n) = 0
\end{aligned}$$

Thus a is in the ring of integers of a quadratic imaginary extension field of $\mathbb{Q}$. Since $a \in \mathbb{Q}(\tau)$, $End(E)$ is a subring of the ring of integers of $\mathbb{Q}(\tau)$. $End(E)$ strictly contains $\mathbb{Z}$ and therefore has rank 2 as an additive abelian group. Thus $End(E)$ is an order of $\mathbb{Q}(\tau)$ (a subring of the ring of integers of $\mathbb{Q}(\tau)$ containing $\mathbb{Z}$ with rank 2 as an additive abelian group).

4.9 Summary of Key Points from Chapter 4

1. An isogeny is an analytic map $E(\mathbb{C}) \to E(\mathbb{C})$ which fixes $(0, 1, 0)$.

2. Let h be an isogeny. Then $h(\varphi(z)) = \varphi(az)$ for some $a \in \mathbb{C}$. An isogeny is a group homomorphism.

3. The set of isogenies of an elliptic curve E form a ring called the endomorphism ring of E, denoted $End(E)$. $End(E)$ always contains $\mathbb{Z}$ as these correspond to the trivial homomorphisms $g \mapsto ng$ which any additive abelian group possesses.

4. An elliptic curve is said to have complex multiplication if $End(E) \underset{\neq}{\supset} \mathbb{Z}$. Any nontrivial isogeny is given by $h(\varphi(z)) = \varphi(az)$ for some a in the ring of integers of a quadratic imaginary field.

5. An elliptic curve has complex multiplication iff τ lies in a quadratic imaginary extension field of $\mathbb{Q}$.

5 Complex Multiplication and the j-invariant

In this final Chapter we are going to show that every CM elliptic curve has an algebraic integer for its j-invariant. Since the algebraic integers are countable (see Appendix on Cardinality) this shows that CM curves are very rare. We will also show that the converse is false. That is not all choices of algebraic integers for the j-invariant give CM curves. Some algebraic number theory is required and is built up first.

5.1 Definition

Let R be a commutative ring with 1 and K the field fractions of R. An element $k \in K$ is said to be integral over R if there is a monic polynomial $f(X) \in R[X]$ s.t. $f(k) = 0$. The set of elements of K which are integral over R is called the integral closure of R. R is said to be integrally closed if it is its own integral closure.

5.2 Definition

An integral domain with 1 is called a Dedekind Domain if it is noetherian, integrally closed, and every nonzero prime ideal is maximal.

5.3 Definition

Let I, J be nonzero proper ideals of a Dedekind domain R. We say I divides J, written $I|J$, if $\exists\, H \lhd R$ such that $J = IH$.

5.4 Lemma

Let I be an ideal of a Dedekind domain R. Then I contains a product of prime ideals. If $I \neq R$ then $\exists\, k \in K \backslash R$ s.t. $kI \subseteq R$ (where K denotes the field of fractions of R).

Proof [Mo, Lem.3.13 and 3.14]

For the first part let S be the set of ideals which do not contain a product of prime ideals. If $S \neq \emptyset$ then since R is noetherian S contains a maximal element M. M cannot be prime so $\exists\, r, s \notin M$ s.t. $rs \in M$. Now $M \subsetneqq M + rM, M + sM$ so these ideals contain products of prime ideals. But $(M + rM)(M + sM) \subseteq M$ so M contains a product of primes. Contradiction so $S = \emptyset$.

For the second part let $a \in I$. Let $P_1 ... P_n \subseteq aR$ be a product of primes with n as small as possible. Now I is contained in a maximal ideal by Zorn's Lemma.

(Let $T = \{R \neq J \lhd R : I \subseteq J\}$ ordered by inclusion. Then if $\{J_\lambda\}$ is a totally ordered subset of T, $\cup J_\lambda \in T$ is an upper bound of $\{J_\lambda\}$, so T contains a maximal element).

Now maximal ideals are prime so $I \subseteq P$ for some prime ideal P. $P_1...P_n \subseteq P$ so since P is prime $P_i \subseteq P$ for some i, say $i = 1$ for convenience. Since R is a Dedekind domain prime ideals are maximal so $P_1 = P$. By assumption aR does not contain products of fewer than n primes so $\exists\, b \in P_2...P_n \backslash aR$. Thus $\frac{b}{a} \in \frac{1}{aR}P_2...P_n \backslash R \subseteq K\backslash R$. Now $bP \subseteq PP_2...P_n \subseteq aR$, so if $d \in I \subseteq P$ then $bd \in aR$ and so $\frac{b}{a}d \in R$. That is $\frac{b}{a}I \subseteq R$ and we have found our $k(= \frac{b}{a})$. □

5.5 Lemma

Let R be a Dedekind domain and $0 \neq A \lhd R$. Then $\exists\, 0 \neq B \lhd R$ s.t. AB is principal.

Proof [Mo, Thm.3.15]

Let $0 \neq a \in A$ and let $B := \{b \in R : Ab \subseteq aR\} \lhd R$. Then $AB \subseteq aR$.
Let $M := \frac{1}{a}AB \lhd R$. We show $M = R$ which implies $AB = aR$.
If $M \subsetneqq R\ \exists\, k \in K\backslash R$ s.t. $kM \subseteq R$ by Lemma 5.4. R is a Dedekind domain so is integrally closed. We show k is the root of a monic polynomial over R obtaining a contradiction. $b = \frac{1}{a}ab\ \forall b \in B$ so $B \subseteq M$.
Thus $kB \subseteq kM \subseteq R \Rightarrow kAB \subseteq aR \Rightarrow kB \subseteq B$.
R is noetherian so take a finite set of generators $\{b_1, ..., b_r\}$ for B,
that is $B = \mathbb{Z}b_1 + ... + \mathbb{Z}b_r$.
$kb_i = \sum_{j=1}^{r} n_{ij}b_j$ for some integers n_{ij}. We see that

$$\det \begin{pmatrix} n_{11} - k & n_{12} & \cdots & n_{1r} \\ n_{21} & n_{22} - k & \cdots & n_{2r} \\ \vdots & \vdots & \vdots & \vdots \\ n_{r1} & n_{r2} & \cdots & n_{rr} - k \end{pmatrix} = 0$$

since $0 \neq (b_1, \cdots, b_r)$ is in its kernel. By expanding the determinant we have found a monic polynomial over R of which k is a root. □

5.6 Lemma

Let I, J be nonzero proper ideals of a Dedekind domain R. Then $I|J \Leftrightarrow I \supseteq J$.

Proof

($\Rightarrow$) By the definition of an ideal $I \supseteq IH = J$.

($\Leftarrow$) By Lemma 5.5 $\exists\, 0 \neq L \lhd R$ and $a \in I$ s.t. $LI = aR$. Let $H := \frac{1}{a}LJ$. Since $J \subseteq I$ by assumption, H is an ideal of R and $LIH = LJ$. By Lemma 5.5 $\exists\, 0 \neq N \lhd R$, $b \in L$, s.t. $NL = bR$. Then $bRIH = NLIH = NLJ = bRJ$.
So $bRIH = bRJ \Rightarrow IH = b^{-1}RbRIH = b^{-1}RbRJ = J$. □

5.7 Theorem

Let I be a nonzero proper ideal of a Dedekind domain R. Then $\exists\, P_1, ..., P_r$ distinct prime ideals of R and $n_1, ..., n_r \in \mathbb{N}$ s.t. $I = P_1^{n_1} ... P_r^{n_r}$ and this expression is unique (up to the order of the factors).

Proof [**Mo, Thm.3.19**]

Existence
Let $S = \{0, R \neq I \lhd R : I$ is not expressible as a product of primes$\}$. Suppose $S \neq \emptyset$. By Zorn's Lemma S has a maximal element M (w.r.t. inclusion). By Zorn's Lemma M is contained in a maximal ideal P (see proof of Lemma 5.4). P is prime and $M \subseteq P$. By Lemma 5.6 $\exists\, I \lhd R$ s.t. $M = IP$. Thus $I \supseteq M$. Suppose $I = M$. Then $IR = I = IP$. By Lemma 5.5 $\exists\, L \lhd R$, $a \in I$, s.t. $LI = aR$. So $R = a^{-1}aRR = a^{-1}LIR = a^{-1}LIP = P$. Hence $P = R$ but P is a maximal ideal. This is a contradiction so $I \supsetneq M$. I is then a product of primes but $M = IP$ so M is a product of primes. Contradiction so $S = \emptyset$.

Uniqueness
Suppose $P_1...P_r = Q_1...Q_s$ are products of (not necessarily distinct) primes. $P_1 \supseteq Q_1...Q_s$ so $P_1 \supseteq Q_i$ for some i. Say $i = 1$ for convenience since we can reorder anyway. R is a Dedekind domain so prime ideals are maximal. Thus $P_1 = Q_1$. By Lemma 5.5 $\exists\, 0 \neq L \lhd R$, $a \in P_1$, s.t. $LP_1 = LQ_1 = aR$. Thus $P_2...P_r = a^{-1}LP_1P_2...P_r = a^{-1}LQ_1Q_2...Q_r = Q_2...Q_R$. By induction we have uniqueness. □

5.8 Definition

Let R be Dedekind domain and K its field of fractions. A fractional ideal of R is a nonzero finitely generated R-submodule of K.

Let M be a fractional ideal with generators $m_1, ..., m_k$. Each m_i is in K so there exists $s \in R$ such that $m_i s \in R$ for all i. Thus $Ms \subset R$. This explains the name fractional ideal.

5.9 Definition

Let M be a fractional ideal of a Dedekind domain R.
Define $M^{-1} := \{x \in K | xM \subseteq R\}$. A fractional ideal M is said to be invertible if $MM^{-1} = R$.

We aim to define an abelian group structure on the set of fractional ideals of R. The product of two fractional ideals M and N is the set $MN := \{\sum_{\text{finite}} m_i n_i | m_i \in M, n_i \in N\}$. If $\{x_i\}$ and $\{y_j\}$ are sets of generators for M and N then the set of products $\{x_i y_j\}$ is a set of generators for MN. Thus MN is finitely generated and so is a fractional ideal. The identity element is R.

It remains to show that every fractional ideal has an inverse. We do this by showing every fractional ideal is invertible (as defined in Definition 5.9). First let's check that M^{-1} is a fractional ideal. M^{-1} is a non-zero R-submodule of K. Choose $0 \neq m \in M$. Then $M^{-1}m \subset R$ so $M^{-1} \subset Rm^{-1}$. Rm^{-1} is a finitely generated R module and because R is noetherian, the submodule M^{-1} is also finitely generated. Hence M^{-1} is a fractional ideal.

5.10 Definition

Let R be a Dedekind domain and K its field of fractions.
A principal fractional ideal of R is a fractional ideal of the form Rx for some $0 \neq x \in K$.

$(Rx)^{-1} = Rx^{-1}$ so $(Rx)(Rx)^{-1} = Rxx^{-1} = R$. Thus a principal fractional ideal is invertible.

5.11 Lemma

Let R be an integral domain with 1 and $\emptyset \neq S \subseteq R$ a multiplicative set. That is $0 \notin S$ and S is closed under multiplication. Then there is a ring R_S which contains R as a subring such that every element of S has a multiplicative inverse.

Proof [Ja, Prop.1.1]

Define an equivalence relation on $R \times S$ by $(a, b) \sim (c, d)$ iff $ad = bc$. Let $R_S = R \times S/ \sim$. Addition and multiplication are defined in the same way as for the field of fractions of R. R is isomorphically imbedded in R_S by fixing $s \in S$ and using the mapping $r \mapsto (rs, s)$. □

We write r/s to denote (r, s). Note that $R_S = R_{S \cup \{1\}}$ so we can assume $1 \in S$ and the mapping of R into R_S can be taken as $r \mapsto r/1$.

5.12 Definition

The ring R_S is called the localization of R at S.

5.13 Lemma [Ja, Prop.1.2]

There is a one-to-one correspondence between prime ideals of R_S and prime ideals of R which have empty intersection with S.

Proof

Define

$$\begin{aligned}\varphi : \{\text{prime ideals of } R_S\} &\rightarrow \{\text{prime ideals } P \lhd R : P \cap S = \emptyset\}\\ \varphi(Q) &:= Q \cap R\\ \psi : \{\text{prime ideals } P \lhd R : P \cap S = \emptyset\} &\rightarrow \{\text{prime ideals of } R_S\}\\ \psi(P) &:= PR_S\end{aligned}$$

We show φ and ψ are inverse maps. That is

$$\begin{aligned}PR_S \cap R &= P \text{ for every prime ideal } P \lhd R \text{ s.t. } P \cap S = \emptyset\\ (Q \cap R)R_S &= Q \text{ for every prime ideal } Q \lhd R_S.\end{aligned}$$

Let Q be a prime ideal of R_S. $Q \cap R$ is a prime ideal of R and $(Q \cap R)R_S \subseteq Q$ is an ideal of R_S. Let $q/s \in Q$ then $q = (q/s)s \in Q \cap R$ so $q(1/s) = q/s \in (Q \cap R)R_S$. Thus $Q \subseteq (Q \cap R)R_S$.

Let P be a prime ideal of R with $P \cap S = \emptyset$. PR_S is an ideal of R_S. It is prime since if $(r_1/s_1)(r_2/s_2) \in PR_S$ with $(r_1/s_1), (r_2/s_2) \in R_S$ then $(r_1/s_1)(r_2/s_2) = x/s$ for some $x \in P$ and $s \in S$. Now $r_1 r_2 s = x s_1 s_2 \in P$ and P is prime so r_1 or $r_2 \in P$. So (r_1/s_1) or $(r_2/s_2) \in PR_S$ and PR_S is prime. If $u \in PR_S \cap R$ then $u = x/s$ with $x \in P$. But $u \in R$ so since P is prime, $x = us \Rightarrow u \in P$. Thus $PR_S \cap P \subseteq P$. $P \subseteq PR_S \cap P$ is clear. □

Take a prime ideal $P \lhd R$ and let $S = R \backslash P$. We write R_P to denote the localization of R at S. Since $0 \in P$ a prime ideal can never be a multiplicative set so this notation is not ambiguous. The prime ideals of R which have empty intersection with $S = R \backslash P$ are those prime ideals contained in P. By Lemma 5.12 the only ideals of R_P are those contained in PR_P. Maximal ideals are always prime so PR_P is the only maximal ideal in R_P.

5.14 Definitions

An integral domain with 1 with only one maximal ideal is called a Local Ring.
By the above comments if we localize at a prime ideal we get a local ring.
A local ring which is also a principal ideal domain is called a Discrete Valuation Ring (DVR).

5.15 Lemma

Let R be a Dedekind domain. Then R_P is a DVR for every nonzero prime ideal P of R.

Proof [Ja, Prop.3.20]

R is Noetherian by definition. Let $J_1 \subseteq J_2 \subseteq ...$ be an ascending chain of ideals of R_P. Then $J_1 \cap R \subseteq J_2 \cap R \subseteq ...$ is an ascending chain of ideals of R which therefore terminates. That is $\exists n \in \mathbb{N}$ s.t. $J_n \cap R = J_{n+1} \cap R = ...$
Observe that $(J_i \cap R)R_P \subseteq J_i$. Let $r/s \in J_i$. Then $r = (r/s)s \in J_i \cap R$
so $r(1/s) = r/s \in (J_i \cap R)R_P$. Thus $J_i \subseteq (J_i \cap R)R_P$.
So $J_n = J_{n+1} = ...$ and R_P is Noetherian.

By the comments after Lemma 5.13 the only maximal ideal of R_P is PR_P. Since R is a Dedekind domain there is no distinction between prime and maximal ideals. So PR_P is the only prime ideal of R_P. Also R_P is integrally closed because R is.

Fix $0 \neq a \in R_P$. Let $M = R_P/aR_P$. For each $m \in M$ let
$null(m) = \{r \in R_P : rm = aR_P\}$. This is an ideal of R_P for each $m \in M$. Choose $m \in M$ s.t. $null(m)$ is maximal in the set of ideals
$\{null(m) : 0 \neq m \in M\}$. Pick a representative of this coset, $m = b + aR_P$ with $b \in R_P$. $Q := null(b + aR_P)$ is nonzero because $a \in Q$. Q is prime for suppose $x, y \notin Q$ but $xy \in Q$. Then $y(b + aR_P) \neq aR_P$ so $null(yb + aR_P)$ contains Q and x which contradicts the maximality of Q. Q is therefore the unique prime ideal, i.e. $Q = PR_P$.

We have shown $bPR_P \subseteq aR_P$ but $b \notin aR_P$ since $b + aR_P \neq R_P$. So $\frac{b}{a} \notin R_P$ and $\frac{b}{a}PR_P \subseteq R_P$. Suppose $\frac{b}{a}PR_P \subsetneq R_P$. Then since PR_P is the unique maximal ideal we have $\frac{b}{a}PR_P \subseteq PR_P$. By exactly the same determinant trick as used in Lemma 5.5 $\frac{b}{a}$ is integral over R_P. R_P is integrally closed by definition so $\frac{b}{a} \in R_P$ contradicting the above. Thus $\frac{b}{a}PR_P = R_P$ and so $PR_P = \frac{a}{b}R_P$. This shows the unique maximal ideal is principal. Write $PR_P = xR_P$.

Let U be a nonzero ideal of R_P. Consider the chain $U \subseteq x^{-1}U \subseteq x^{-2}U \subseteq ....$ If $x^{-n}U = x^{-n-1}U$ then by the determinant trick x^{-1} is integral over R_P which is impossible because $x^{-1} \notin R_P$ and R_P is integrally closed. Since R_P is noetherian the part of the chain which falls into R_P must be finite. There exists n s.t. $x^{-n}U \subseteq R_P$ but $x^{-n-1}U \nsubseteq R_P$. If $x^{-n}U \subseteq PR_P$ then $x^{-n-1}U \subseteq R_P$ so $x^{-n}U = R_P$ and $U = x^n R_P$. U is a principal ideal as required. □

5.16 Theorem

Let R be a Dedekind domain. Any nonzero prime ideal of R is invertible.

Proof

Let P be a nonzero prime ideal of R. Then $PP^{-1} = U$ is an ideal of R. For any maximal ideal Q we know that R_Q is a PID by Lemma 5.15 so PR_Q is principal and hence invertible by the remarks after Definition 5.10. Thus $UR_Q = (PP^{-1})_Q = R_Q$. This holds for all maximal ideals Q of R. Let $b \in R$. $bR_Q \subseteq UR_Q$ so $\exists\, a \in U$ and $s \in R\backslash Q$ s.t. $b = a/s$. The ideal of

R, $\{y \in R : by \subseteq U\}$ contains s so does not belong to Q. The ideal must then be the whole of R. So $b \in U$ and so $R \subseteq U$ and thus $R = U$ as required. □

5.17 Corollary

Let R be a Dedekind domain. Let M be a fractional ideal of R. Then $\exists P_1, ..., P_n$ distinct prime ideals of R and $a_1, ..., a_n \in \mathbb{Z}$ s.t. $M = P_1^{a_1} ... P_n^{a_n}$ and this expression is unique (up to the order of the factors).

Proof [Ja, Thm.4.2]

Let M be a fractional ideal with generators $m_1, ..., m_k$. Each m_i is in K so there exists $s \in R$ such that $m_i s \in R$ for all i. Thus $Ms \subset R$. By Theorem 5.7 there exist factorizations of the ideals Rs and Ms as $Rs = \prod Q_j^{b_j}$, $Ms = \prod P_i^{a_i}$ where the P_i and Q_j are prime ideals of R. It follows $M \prod Q_j^{b_j} = \prod P_i^{a_i}$. Prime ideals are invertible so $M = \prod P_i^{a_i} \prod Q_j^{-b_j}$. This establishes existence.

For uniqueness suppose $M = \prod P_i^{a_i} \prod Q_j^{-b_j} = \prod X_i^{c_i} \prod Y_j^{-d_j}$ where
P_i, Q_j, X_i, Y_j are prime ideals and a_i, b_j, c_i, d_j are positive integers.
Thus $\prod P_i^{a_i} \prod Y_j^{d_j} = \prod X_i^{c_i} \prod Q_j^{b_j}$ is a factorization of ideals in R so we have uniqueness by Theorem 5.7. □

We have shown that the set of all fractional ideals is a group with respect to multiplication and inverses described above. The uniqueness statement of Corollary 5.17 shows that it is a free abelian group with the set of nonzero prime ideals as generators. The collection of all principal fractional ideals is a subgroup.

5.18 Definition

Let R be a Dedekind domain. The group of fractional ideals is called the ideal group of R and is denoted $I(R)$. The subgroup of principal fractional ideals is denoted $P(R)$.
The class group of R is defined to be $C(R) := I(R)/P(R)$.

We now apply this theory to algebraic number fields. An algebraic number field $K \subseteq \mathbb{C}$ is a finite field extension of $\mathbb{Q}$. The ring of algebraic integers in $\mathbb{C}$ is denoted $\mathbb{A}$. Define the ring of integers in K to be $R_K := K \cap \mathbb{A}$.

5.19 Theorem

If K is an algebraic number field then R_K is a Dedekind domain.

Proof

R_K is an integral domain finitely generated as an abelian group. Therefore every ideal of R_K is finitely generated and so R_K is noetherian.

Suppose $a/b \in K$ is the root of a monic polynomial over R_K. Then $a/b \in \mathbb{A}$ so $a/b \in K \cap \mathbb{A} = R_K$. R_K is integrally closed.

Let $0 \neq I \lhd R_K$ and $0 \neq r \in I$. Let R_K have rank n as a free abelian group and choose a basis $f_1, ..., f_n$ of R_K. Then $\exists\, b_{i,j} \in \mathbb{Z}$ s.t.

$$\begin{pmatrix} r \\ \vdots \\ \vdots \\ r^{n+1} \end{pmatrix} = \begin{pmatrix} b_{1,1} & b_{1,2} & \dots & b_{1,n} \\ b_{2,1} & b_{2,2} & \dots & b_{2,n} \\ \vdots & \vdots & \vdots & \vdots \\ b_{n+1,1} & b_{n+1,2} & \dots & b_{n+1,n} \end{pmatrix} \begin{pmatrix} f_1 \\ \vdots \\ \vdots \\ f_n \end{pmatrix}$$

Now $rank(b_{i,j}) \leqslant n$ so $\exists\, a_i \in \mathbb{Z}$ s.t. $a_{n+1}r^{n+1} + a_n r^n + ... + a_0 = 0$. Then $a_0 = -r(a_{n+1}r^n + ... + a_1)$.

Choose a polynomial over $\mathbb{Z}$ with smallest degree possible of which r is a zero. Then $a_0 \neq 0$ because $a_{n+1}r^n + ... + a_1 \neq 0$.

Now $a_0 = -r(a_{n+1}r^n + ... + a_1) \in I$ so $I \supseteq a_0 R_K$.

$R_K/a_0R_K \cong \mathbb{Z}/a_0\mathbb{Z} \bigoplus ..... \bigoplus \mathbb{Z}/a_0\mathbb{Z}$ and R_K/I is a homomorphic image of this, so has the same number of elements or fewer. $|R_K/I| \leqslant |R_K/a_0R_K| = a_0^n$. If we take I to be a prime ideal then R_K/I is a finite integral domain and hence a field. Therefore I is a maximal ideal of R_K. □

5.20 Theorem

Let K be an algebraic number field and R_K its ring of integers. Then $C(R_K)$ is finite.

Proof

Let I be a nonzero proper ideal of R_K. By Theorem 5.7 $\exists\, P_1, ..., P_r$ prime ideals of R_K and $n_1, ..., n_r \in \mathbb{N}$ s.t. $I = P_1^{n_1} ... P_r^{n_r}$ and this expression is unique up to the order of the factors.

For a prime ideal P of R_K the ideal $rad(P)$ is prime. By Theorem 5.19 R_K is a Dedekind domain so $rad(P)$ is maximal. $P \subseteq rad(P)$ so $P = rad(P)$. Now $rad(IJ) = rad(I \cap J) = rad(I) \cap rad(J)$ so $rad(P^n) = rad(P)$. We have

$\prod_{i=1}^r P_i = rad(\prod_{i=1}^r P_i) = \bigcap_{i=1}^r rad(P_i) = \bigcap_{i=1}^r P_i$

If $P_i^{n_i} + P_j^{n_j} = A \subsetneq R_K$, then $A | P_i^{n_i}$ and $A | P_j^{n_j}$ which contradicts P_i, P_j distinct primes so $P_i^{n_i} + P_j^{n_j} = R_K$.

By the Chinese Remainder Theorem

$R/I = R/\prod_{i=1}^r P_i^{n_i} = R/\bigcap_{i=1}^r P_i^{n_i} \cong \prod R/P_i^{n_i}$.

By the proof of Theorem 5.19 these sets are finite so
$|R/I| = \prod |R/P_i|^{n_i}$.
Define the norm of an ideal to be $N(I) := |R_K/I|$.
Note that $N(IJ) = N(I)N(J)$.

It can be shown by an argument using lattice theory that every class in $C(R_K)$ contains an ideal I of R s.t. $N(I) \leqslant M$ where M is a finite number called the Minkowski Bound. See [Ja, Thm.11.8]. Now I is expressible as a product of primes so there are only finitely many ideals of R that divide I. Namely they are products of subsets of the ideals that compose I. It follows that there are only finitely many ideals with a given norm and so there are only finitely many choices for the classes in $C(R_K)$. $\square$

5.21 Definition

Let K be an algebraic number field. The cardinality of the class group of R_K is called the class number of K.

5.22 Lemma

Let R be a Dedekind domain. Then R is a UFD iff the class group of R has cardinality 1.

Proof [Mo, Thm.3.32]

¿From the definition of the $C(R)$ we see that $|C(R)| = 1 \Leftrightarrow R$ is a PID. A PID is always a UFD. It remains to show that in a Dedekind domain a UFD is a PID.

Suppose R is a UFD and $I \lhd R$ is not a principal ideal. I is expressible as a product of primes by Theorem 5.7 so there is a prime ideal P which is not a principal ideal. Let S be the set of ideals $I \lhd R$ s.t. PI is principal. We know S is non-empty by Lemma 5.5. By Zorn's Lemma S has a maximal element M. $PM = (a)$ and a must be irreducible by the maximality of M. There exist nonzero $b \in P \backslash (a), c \in M \backslash (a)$ s.t. $bc \in PM \subseteq (a)$. So $a|bc$ but a does not divide b or c. a is irreducible but not prime. This contradicts R being a UFD. $\square$

5.23 Theorem

Let K be a quadratic imaginary field. There is a one-to-one correspondence between ideal classes in $C(R_K)$ and isomorphism classes of elliptic curves with $End(E) \cong R_K$.

Proof

Take an ideal Λ of R_K. The elliptic curve $\mathbb{C}/\Lambda$ has $End(\mathbb{C}/\Lambda) \cong \{a \in \mathbb{C} : a\Lambda \subset \Lambda\} = R_K$. Two elliptic curves are isomorphic precisely if they are homothetic and this corresponds to multiplication by a principal fractional ideal. $\square$

5.24 Corollary

Let E be an Elliptic Curve with $End(E) \cong R_K$. Then $j(E)$ is an algebraic number.

Proof

By Theorem 5.20 $C(R_K)$ is finite so there are only finitely many isomorphism classes of elliptic curves with $End(E) \cong R_K$.
Let $\sigma \in Aut(\mathbb{C}/\mathbb{Q})$. $End(E^\sigma) \cong End(E) \cong R_K$. By the above $\{j(E)^\sigma : \sigma \in Aut(\mathbb{C}/\mathbb{Q})\}$ is finite. We have a finite field extension which from Galois theory we know is algebraic. □

5.25 Theorem

Let E be an elliptic curve with complex multiplication such that $End(E)$ is the ring of integers in a quadratic imaginary field. Then $j(E)$ is an algebraic integer.

Proof

A complex analytic proof of this is given in [Si2, Thm.II.6.1]. □

5.26 Corollary

Let E be an elliptic curve with complex multiplication. Then $j(E)$ is an algebraic integer.

Proof

We follow the proof in [Si2, Cor.II.6.3.1] and use the same notations. Let $End(E) \cong R$, an order in K. Let $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ be a lattice for E. Now $K = \mathbb{Q}(\omega_1/\omega_2)$. By multiplying by a suitable $\lambda \in \mathbb{C}^*$, we may assume $\Lambda \subset R_K = \mathbb{Z} + \tau\mathbb{Z}$.
Then there exist integers a, b, c, d such that

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

Let $n = ad - bc$. After switching ω_1 and ω_2 if necessary we may assume $n \geq 1$. The matrix $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in D_n$ so $j \circ \alpha$ is integral over the ring $\mathbb{Z}[j]$. Now $F_n(j, X) = 0$ so evaluating at τ we find that $j(\alpha\tau)$ is integral over $\mathbb{Z}[j(\tau)]$. But $j(\alpha\tau) = j(E)$ and $j(\tau)$ is integral over $\mathbb{Z}$ by the above Theorem. Hence $j(E)$ is integral over $\mathbb{Z}$. □

Since the algebraic integers are countable this implies that the number of elliptic curves (up to isomorphism) with CM is countable. Complex multiplication is therefore a rare property of an elliptic curve. See the Appendix for a discussion of cardinality.

The converse of the above theorem is false. That is, given an algebraic integer for j the corresponding elliptic curve is not always CM. We show this below in 5.29 onwards. We know that an elliptic curve is CM iff τ is in a quadratic imaginary extension field of $\mathbb{Q}$. We show now that if $3 \leq [\mathbb{Q}(\tau) : \mathbb{Q}] < \infty$ then $j(\tau)$ is transcendental. This will mean that any τ whose elliptic curve is not CM, but for who $j(\tau)$ an algebraic integer, must be transcendental.

5.27 Theorem

Let K be a finite field extension of $\mathbb{Q}$ and let f_1,...f_n be meromorphic functions of finite order. Suppose that the ring $K[f_1, ..., f_n]$ is mapped to itself by differentiation and has transcendence degree at least 2 over K. Then there are only finitely many numbers z at which $f_1, ..., f_n$ simultaneously assume values in K.

Proof

See [Ba, Thm.6.1]. □

A meromorphic function f is said to have finite order if $f = g/h$ where g,h are entire functions and $\exists \rho > 0$ s.t. $\forall R \geq 2$, $\forall z$ with $|z| \leq R$, $max(|g(z)|, |h(z)|) < exp(R^\rho)$. The transcendence degree of the ring $K[f_1, ..., f_n]$ is the maximum number of elements in an algebraically independent subset.

5.28 Corollary [Ba, Thm.6.3]

Let τ be an algebraic number with $3 \leq [\mathbb{Q}(\tau) : \mathbb{Q}]$, then $j(\tau)$ is transcendental.

Proof

Suppose $j(\tau)$ is algebraic. Then there is a $\wp$-function with algebraic invariants g_2, g_3 and fundamental periods ω_1, ω_2 such that $\tau = \omega_2/\omega_1$. When $z = 3\omega_1/2$ the functions $f_1 = \wp(z)$, $f_2 = \wp(\tau z)$, $f_3 = \wp'(z)$, $f_4 = \wp'(\tau z)$ assume the same values in an algebraic number field, say K. By the above Theorem $K[f_1, f_2, f_3, f_4]$ has transcendence degree at most 1. f_1 and f_2 are thus algebraically dependent. This implies that $l\omega_2$ is a period of $\wp(\tau z)$ for some $l \in \mathbb{N}$. $l\tau\omega_2 = m\omega_1 + n\omega_2$ for some $m, n \in \mathbb{Z}$, so $l\tau^2 - n\tau - m = 0$ and τ is a quadratic irrational. □

5.29 Lemma

Every quadratic field is of the form $\mathbb{Q}(\sqrt{d})$ where d is a square-free integer.

Proof

Let $K = \mathbb{Q}(\alpha)$ be a quadratic field and α be a solution of $x^2 + ax + b$ for some $a, b \in \mathbb{Z}$. Thus $K = \mathbb{Q}\left(\frac{-a \pm \sqrt{a^2-4b}}{2}\right) = \mathbb{Q}(\sqrt{a^2-4b})$. By uniqueness of factorization in $\mathbb{Z}$, $a^2 - 4b = p_1^{e_1}...p_r^{e_r}$ for primes p_i with powers e_i. Thus

$a^2 - 4b = \prod_{e_i \text{ odd}} p_i \left(\prod_{e_i \text{ odd}} p_i^{(e_i-1)/2}(\prod_{e_j \text{ even}} p_j^{(e_j)/2}\right)^2 = dr^2$ for some $d, r \in \mathbb{Z}$, d square-free. Thus $K = \mathbb{Q}(r\sqrt{d}) = \mathbb{Q}(\sqrt{d})$. □

5.30 Theorem

The ring of integers in a quadratic field $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}(\sqrt{d})$ if $d \equiv 2$ or $3 \bmod 4$ and $\mathbb{Z}(\frac{1}{2} + \frac{1}{2}\sqrt{d})$ if $d \equiv 1 \bmod 4$.

Proof

This proof is taken from the 2nd year essay "Algebraic Number Fields" by John Hudson, an undergraduate at the University of Warwick. Let $z \in \mathbb{Q}(\sqrt{d})$ be an algebraic integer. Then $z = \frac{a+b\sqrt{d}}{c}$ for some $a, b, c \in \mathbb{Z}$. We may assume the highest common factor of a,b and c is 1. The coefficients of the minimum polynomial of z, $\left(x - \frac{a+b\sqrt{d}}{c}\right)\left(x - \frac{a-b\sqrt{d}}{c}\right)$ are integers. Thus $\frac{a^2-b^2d}{c^2} \in \mathbb{Z}$ and $\frac{2a}{c} \in \mathbb{Z}$. If a and c have a common prime divisor p then p^2 divides b^2d and since d is square-free, p^2 divides b^2. Thus p divides b contradicting the highest common factor of a, b, c being 1. Hence c is 1 or 2. This shows that the ring of integers is either $\mathbb{Z}(\sqrt{d})$ or $\mathbb{Z}(\frac{1}{2} + \frac{1}{2}\sqrt{d})$.

Consider the case $c = 2$. Now $\frac{a^2-b^2d}{c^2} \in \mathbb{Z}$ so $a^2 - b^2d \equiv 0 \bmod 4$. a must be odd since it does not have a common prime divisor with c. Thus b must be odd. Thus $a^2 \equiv b^2 \equiv 1 \bmod 4$ and therefore $d \equiv 1 \bmod 4$. Conversely if $d \equiv 1 \bmod 4$ then $\frac{a+b\sqrt{d}}{2}$ for a, b odd is an algebraic integer since $\frac{a^2-b^2d}{4} \in \mathbb{Z}$. □

5.31 Corollary

An order θ in a quadratic imaginary field K is given by $\theta = \mathbb{Z} + fR_K$ for some $f \in \mathbb{Z}$. f is called the <u>conductor</u> of θ.

Proof

Suppose $R_K = \mathbb{Z}(\sqrt{d})$. θ has a basis 1,β for some $\beta \in R_K$. $\beta = e + f\sqrt{d}$ for some $e, f \in \mathbb{Z}$ so $\theta = \{m + n\beta | m, n \in \mathbb{Z}\} = \{m + ne + nf\sqrt{d} | m, n \in \mathbb{Z}\} = \mathbb{Z} + f\mathbb{Z}(\sqrt{d})$.

Suppose $R_K = \mathbb{Z}(\frac{1}{2} + \frac{1}{2}\sqrt{d})$. θ has a basis 1,β for some $\beta \in \mathbb{R}_K$. $\beta = \frac{x}{2} + f\frac{y}{2}\sqrt{d}$ for some integers x and y and by a similar argument we have the result. □

5.32 Theorem

Let K be a quadratic imaginary field and let E be an elliptic curve with endomorphism ring an order in K. By Corollary 5.26 $j(E)$ is an algebraic integer. The degree of the minimum polynomial of $j(E)$ over $\mathbb{Z}$ is greater than or equal to the class number of K.

Proof

See [Si2, Thm.II.4.3] for a proof that if $End(E)$ is the full ring of integers then the degree of the minimum polynomial of $j(E)$ over $\mathbb{Z}$ equals the class number of K. By [Si2, Thm.II.6.3] and Exercise 2.28 in [Si2] we have the result. □

Note that the endomorphism ring of a CM curve $\mathbb{C}/\Lambda$ is the lattice Λ. By Theorem 5.32 the only candidates for CM elliptic curves with j-invariant in $\mathbb{Z}$ are therefore those with $End(E)$ an order in a quadratic imaginary field of class number 1. By Lemma 5.22 this is the same as asking that the ring of integers be a UFD. We use the classification of all quadratic imaginary fields whose ring of integers is a UFD. There are 9 of them. They are $\mathbb{Q}(\sqrt{d})$ where $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$. It can be shown that as the size of the conductor goes up, the degree of the minimum polynomial of j goes up. In fact only finitely many orders in each of these fields have j with minimum polynomial of degree 1 over $\mathbb{Z}$. There are precisely 13 of them.

Only 13 j-invariants in $\mathbb{Z}$ correspond to CM elliptic curves. They are listed in [Si2, App.A.3]. Pick any other integer and we have an example of j an algebraic integer but the corresponding elliptic curve not CM. In particular $j = 1$ gives a non-CM curve.

5.33 A non-CM elliptic curve with integer j-invariant

$j = 1$ does not correspond to a CM curve. Let's find an elliptic curve with j-invariant 1. As in the proof of Theorem 2.17 the curve
$y^2 = x^3 - 27\frac{j}{j-1728}x - 54\frac{j}{j-1728}$ has j-invariant j. Thus
$y^2 = x^3 + \frac{27}{1727}x + \frac{54}{1727}$ has j-invariant 1.

It would be nice to find τ for such a curve. I have written computer programs in BASIC which approximate j from τ and τ from j for $j > 1728$ using a method of Gauss involving the arithmetic-geometric mean. $j > 1728$ corresponds precisely to $\tau = it$ with $t > 1$. j grows rapidly with t. In fact we know that $j(i) = 1728$, $j(\sqrt{2}i) = 8000$, $j(\sqrt{3}i) = 54000$ and $j(2i) = 287496$ as these are CM curves listed in [Si2, App.A.3]. My programs calculate these values accurately so we can be confident that they give me an accurate numerical approximation for τ with $j(\tau) = 1729$. The Gauss method is summarized in Section VI.9 in [Kn, VI.9].

5.34 Summary of Key Points from Chapter 5

1. A Dedekind domain is a noetherian, integrally closed integral domain with 1 in which every prime ideal is maximal.

2. A fractional ideal of a Dedekind domain, R, is a nonzero finitely generated R-submodule of K, the field of fractions of R. A principal fractional ideal of R is a fractional ideal of the form Rx for some $0 \neq x \in K$.

3. The class group of R, $C(R) := I(R)/P(R)$ where $I(R)$ is the group of fractional ideals of R and $P(R)$ is the subgroup of principal fractional ideals of R.

4. The ring of integers R_K of an algebraic number field K is a Dedekind domain. The class group $C(R_K)$ is finite. The cardinality of $C(R_K)$ is called the class number of K.

5. There is a one-to-one correspondence between ideal classes in $C(R_K)$ and isomorphism classes of elliptic curves with $End(E) \cong R_K$.

6. The j-invariant of a CM elliptic curve is an algebraic integer.

7. The elliptic curve $y^2 = x^3 + \frac{27}{1727}x + \frac{54}{1727}$ does not have complex multiplication and its j-invariant is 1.

Suggestions for Further Study

1. $j = 1$ is an attractive example of a curve that is not CM. It would be nice to explicitly have $\tau \in \mathbb{C}$ s.t. $j(\mathbb{Z} + \tau\mathbb{Z}) = 1$. ¿From Corollary 5.28 we know that such a τ must be transcendental. One such τ is near $e^{2\pi i/3}$ and satisfies $|\tau| = 1$.

2. For any integer greater than 1728 we can use the Gauss method to approximate an appropriate $\tau = it$ for some $t > 1$. It might be possible to find such a τ whose continued fraction expansion does not recur. This implies that τ does not lie in a quadratic extension of $\mathbb{Q}$ and therefore that the curve $\mathbb{Z} + \tau\mathbb{Z}$ is not CM by Theorem 4.6. One idea is to try out strictly increasing continued fraction expansions, e.g. $2 - \frac{1}{1-\frac{1}{2-\frac{1}{3-\frac{1}{4-\dots}}}}$.

3. It is known that there are only finitely many quadratic imaginary fields with any given class number. See [Ba, 5.5]. The quadratic imaginary fields with class number 2 have been completely classified. The next step is to find all choices j with $[\mathbb{Q}(j){:}\mathbb{Q}]= 2$ s.t. the corresponding elliptic curve is CM.

4. We know that when the endomorphism ring of an elliptic curve E is the full ring of integers R_K, $[\mathbb{Q}(j(E)) : \mathbb{Q}]= |C(R_K)|$. When $End(E)$ is an order of K, $[\mathbb{Q}(j(E)) : \mathbb{Q}] \geq |C(R_K)|$. The degree of the field extension seems to go up as the conductor goes up. This needs verifying. If this is true then it is possible to prove that for any $n \in \mathbb{N}$ there are only finitely many algebraic integers j with $[\mathbb{Q}(j) : \mathbb{Q}]= n$ s.t.the corresponding elliptic curve is CM. In this project we have only proved this for $n = 1$.

6 Appendix on Cardinality

Two sets have the same cardinality if there is a bijection between them. The Schröder-Bernstein Theorem says that given two sets A and B, if there exist well-defined injections $f : A \to B$ and $g : B \to A$ then there is a bijection between A and B. We say a set is countable if it has the same cardinality as $\mathbb{N}$.

6.1 Theorem

$\mathbb{R}$ is uncountable.

Proof

Assume for contradiction that $|\mathbb{R}| = |\mathbb{N}|$. Then there exists a numeration $\mathbb{R} = \{a_n | n \in \mathbb{N}\}$. Consider a decimal expansion for each a_n: $a_n = m_n + \sum_{i=1}^{\infty} \frac{b_{ni}}{10^i}$ for some $m_n \in \mathbb{Z}, b_{ni} \in \{0, ..., 9\}$.
Let $c_i := \begin{cases} 1 & \text{if } b_{ii} \neq 1 \\ 5 & \text{if } b_{ii} = 1 \end{cases}$
$c_i \neq b_{i_i}, 0, 9 \ \forall i \in \mathbb{N}$ so $\sum_{i=1}^{\infty} \frac{c_i}{10^i} \notin \mathbb{R}$. Contradiction. □

6.2 Theorem

(a) $|\mathbb{R}| = |(0,1)|$ and (b) $|[0,1]| = |[0,1] \times [0,1]|$.

Proof

(a) $f : (0,1) \to \mathbb{R}$, $f(x) = tan\left(\pi x - \frac{\pi}{2}\right)$ is a bijection.

(b) By the Schröder-Bernstein Theorem we just have to find a well-defined injection $f : [0,1] \times [0,1] \to [0,1]$. To do this we use a cunning trick. We use binary expansions for the elements of $[0,1] \times [0,1]$ and decimal expansions for the elements of $[0,1]$. That is
$[0,1] \times [0,1] = \{\left(\sum_{n=1}^{\infty} \frac{a_n}{2^n}, \sum_{n=1}^{\infty} \frac{b_n}{2^n}\right) | a_n, b_n \in \{0,1\}\}$
$[0,1] = \{\sum_{n=1}^{\infty} \frac{c_n}{10^n} | c_n \in \{0, ..., 9\}\}$
We have to be careful here and choose recurring zeroes if there is a choice (recall 0.19999... = 0.20000...). We define
$f\left(\sum_{n=1}^{\infty} \frac{a_n}{2^n}, \sum_{n=1}^{\infty} \frac{b_n}{2^n}\right) := \sum_{n=1}^{\infty} \frac{c_n}{10^n}$ where $c_n = 2a_n + b_n + 1$. □

Using Schröder-Bernstein it is not hard to see that if $|A| = |A'|$ and $|B| = |B'|$ then $|A \times B| = |A' \times B'|$. Therefore $|\mathbb{C}| = |\mathbb{R}^2| = |\mathbb{R}|$.

The algebraic numbers $\overline{\mathbb{Q}}$ are the complex numbers which are zeroes of a polynomial over $\mathbb{Z}$.

6.3 Theorem

$\overline{\mathbb{Q}}$ is countable.

Proof

For a polynomial $f(t) = a_0 + a_1 t + ... + a_n t^n \in \mathbb{Z}[t]$ define its height to be $h(f) := n + |a_0| + ... + |a_n|$. There are only a finite number of polynomials over $\mathbb{Z}$ of a given height h.
Now each height h polynomial has less than h roots in $\mathbb{C}$.
So $|\overline{\mathbb{Q}}| \leq \sum_{h=0}^{\infty} h.$(number of height h polynomials), which is a countable infinity. □

References

[Ba] A. Baker, *Transcendental Number Theory*, Cambridge University Press, 1975.

[Bo] A. Borel, S. Chowla, C.S. Herz, K. Iwasawa, J-P. Serre, *Seminar on Complex Multiplication*, Springer-Verlag, Berlin - Heidelberg - New York, 1966.

[He] K. Heegner, *Diophantische Analysis and Modulfunktionen*, Math. Zeit. 56, 1952.

[Ja] G.J. Janusz, *Algebraic Number Fields*, New York, London: Academic Press, 1973 (Pure and Applied Mathematics: Vol. 55).

[Kn] A.W. Knapp, *Elliptic curves*, Mathematical Notes, Princeton University Press, Princeton, New Jersey, 1992.

[Ku] R. Kumanduri & C. Romero, *Number Theory with Computer Applications*, Prentice Hall, Upper Saddle River, New Jersey 07458, 1998.

[Ma] D. Masser, *Elliptic Functions and Transcendence*, Springer-Verlag, Berlin - Heidelberg - New York, 1975.

[Mo] R.A. Mollin, *Algebraic Number Theory*, Chapman & Hall/CRC, Boca Raton - London - New York - Washington, D.C., 1999.

[Re1] M. Reid, *Undergraduate Algebraic Geometry*, London Mathematical Society Student Texts 12, Cambridge University Press, 1988.

[Re2] M. Reid, *Undergraduate Commutative Algebra*, London Mathematical Society Student Texts 29, Cambridge University Press, 1995.

[Sh] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, 1971.

[Si1] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.

[Si2] J.H. Silverman, *Advanced Topics in the Arithmethic of Elliptic Curves*, Springer-Verlag, New York - Berlin - Heidelberg -London - Paris - Tokyo Hong Kong - Barcelona - Budapest, 1994.