Elementary projective geometry and the structure of the geometric group on an elliptic curve

Jonathan Keogh

Hillary Term 2020

A proof of Bézout's Theorem for arbitrary projective curves over an algebraically closed field is given, along with a discussion of the intersection multiplicity. With it we show that all nonsingular projective cubics can be put into Weierstrass form in the case of our field having characteristic different from two or three, and are therefore elliptic curves. From this we lead into a description of the group law on an elliptic curve and show that it is well defined by previous constructions. Afterwards we investigate the structure of the group $E(\mathbb{C})$. With the aim of keeping everything self-contained, we give full proofs.

I have read and I understand the plagiarism provisions in the General Regulations of the University Calendar for the current year, found at http://www.tcd.ie/calendar.

I have also completed the Online Tutorial on avoiding plagiarism 'Ready Steady Write', located at http://tcd-ie.libguides.com/plagiarism/ready-steady-write.

Signed: Jonathan Keogh

Date: 30/03/20

Contents

1 Introduction

Definition. *Let k be a field. An algebraic curve (or simply a curve) is the zero set in k^2 of a non-constant polynomial in $k[x, y]$. We also define the affine space $\mathbb{A}^n(k)$ as the n-fold cartesian product of k. Finally, the projective n-space over k is defined as*

$$\mathbb{P}^n(k) = (k^{n+1} - \{0\})/\sim$$

where we are taking the quotient with respect to the equivalence relation $a \sim b$ if $a = \lambda b$, with $a, b \in k^{n+1}$ and $\lambda \in k$.

In this paper we are mainly interested in the *projective plane* $\mathbb{P}^2(k)$ and curves therein. We denote its elements by $[a : b : c]$ to emphasise that they are equivalence classes. It is instructive to think of the projective plane as the regular affine plane with the added property that that all parallel lines intersect exactly once "at infinity". Specifically, we can write it as the disjoint union of sets $A = \{[a : b : 1] \mid a, b \in k\}$ and $B = \{[a : b : 0] \mid a, b \in k,\ a \neq 0 \neq b\}$, where we identify all $[x : y : 1] \in A$ with $(x, y) \in \mathbb{A}^2(k)$ and $[u : w : 0] \in B$ with the unique line $wx - uy = 0$. In this identification, B consists of lines which indicate in what direction the points "at infinity" are (both directions of a line being considered equivalent).

Every algebraic curve in the affine plane can be represented as the image of a homogeneous polynomial over the projective plane. Throughout, our discussions and constructions mainly focus on the polynomials defining the zero sets we call curves. On reflection, this gives rise to an important subtlety: what if two entirely *different* polynomials define the same zero set, and by extension the same curve? We can answer this question with a version of *Hilbert's Nullstellensatz*:

Two curves in the projective plane are equal (as sets) if and only if the polynomials defining them have the same irreducible factors, possibly with different multiplicities.

Since this result is only true in general over an algebraically closed field, we assume our base field is algebraically closed throughout. For the reader that is comfortable with basic commutative algebra, we have included a direct proof of this important fact in the Appendices.

With this in mind, we make the implicit assumption throughout that the polynomials defining our curves have *no repeated factors*; that is, that they are non-constant polynomials $P \in k[x_1, \ldots, x_n]$ that cannot be written in the form

$$P = Q^2 R,$$

where $Q, R \in k[x_1, \ldots, x_n]$ and Q is non-constant. Therefore, up to a multiplication by a constant, we have a unique polynomial associated to each curve; for if another polynomial has the same zero set, it must have the same irreducible factors by the Nullstellensatz, and so must have repeated factors being different to the original polynomial.

Definition. *1. A homogeneous polynomial of degree d is a polynomial such that $P(\lambda x_1, \ldots, \lambda x_n) = \lambda^d P(x_1, \ldots, x_n)\ \forall \lambda \in k$.*

2. Let $P \in k[x, y, z]$ be a homogeneous polynomial; then its zero set in $\mathbb{P}^2(k)$ is well-defined. Given such a polynomial, we define the projective curve of P to be the set

$$C = \{[x : y : z] \in \mathbb{P}^2(k) \ : \ P(x, y, z) = 0\}.$$

Consider an algebraic curve defined by an irreducible homogeneous polynomial of degree d. If $d = 1$ then we call it a *line*; when $d = 2$ a *conic*; when $d = 3$ a *cubic*; and so on. Note by our above correspondence between curves and their polynomials we may assign a unique degree for each curve as the degree of its polynomial.

If we have the plane algebraic curve defined by $P(x, y)$ of degree d then we can homogenise P by introducing the auxiliary variable z by $P'(x, y, z) := z^d P(\frac{x}{z}, \frac{y}{z})$; conversely, a homogenous polynomial can be de-homogenised by setting $z = 1$. This gives a bijection $[x : y : 1] \leftrightarrow (x, y)$ between points defined by a homogenous polynomial in the projective plane not at infinity and points in the affine plane defined by the de-homogenised polynomial.

Bézout's Theorem essentially states that the special property of the projective plane - of any two lines intersecting exactly once - extends to any two curves, as long as the field k is algebraically closed, with additional nice properties. Therefore, from now on we assume k is an algebraically closed field.

Example 1.1. Consider the lines $\alpha x + \beta y + \gamma = 0$ and $\delta x + \zeta y + \eta = 0$, where we assume they have unequal slope. We may choose a coordinate system such that they have the form $y = m_1 x + b_1$ and $y = m_2 x + b_2$; then they intersect exactly once at the point $(\frac{b_1 - b_2}{m_2 - m_1}, \frac{b_1 m_2 - b_2 m_1}{m_2 - m_1})$. If we perturb either lines by a constant then the perturbation is absorbed into the constants b_1 and b_2, giving still exactly one intersection point.

Example 1.2. Consider the curves $y = x^2$ and $y = 0$ in the complex plane, then they intersect exactly once at the origin. This intersection has a special property. If we perturb the first curve by an arbitrary constant $y_\epsilon = x^2 - \epsilon$, then we have exactly two intersection points $(\pm\sqrt{\epsilon}, 0)$, no matter how small ϵ is.

The difference between these examples is that the first has multiplicity one at its intersection, while the second has multiplicity two. We need to be able to

capture this property for arbitrary curves in the projective plane. This is done with resultants.

2 Resultants

Our exposition follows Kirwan. Throughout, k is an arbitrary field.

Definition. *Let $P(x) = a_0 + a_1 x + \ldots + a_n x^n, Q(x) = b_0 + b_1 x + \ldots + b_m x^m \in k[x]$ be such that $a_n b_m \neq 0$. The resultant $R_{P,Q}$ of P and Q is defined as the determinant of the $(n+m) \times (n+m)$ matrix*

$$\begin{pmatrix} a_0 & a_1 & \cdots & \cdots & \cdots & a_n & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & \cdots & a_{n-1} & a_n & 0 & \cdots & 0 \\ \vdots & & \ddots & & & \vdots & & & \vdots & \vdots \\ 0 & \cdots & 0 & a_0 & \cdots & \cdots & \cdots & \cdots & \cdots & a_n \\ b_0 & b_1 & \cdots & \cdots & b_m & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & & \vdots & & & & \vdots & \\ 0 & \cdots & b_0 & b_1 & \cdots & & & & \cdots & b_m \end{pmatrix}$$

where the first m rows consists of shifts of $(a_0, \ldots, a_n)$ to the right, and the remaining n rows consists of the same for $(b_0, \ldots, b_m)$.

For $P(x,y,z) = \sum_{i=0}^{n} a_i(y,z)x^i, Q(x,y,z) = \sum_{n=i}^{m} b_i(y,z)x^i \in k[x,y,z]$, we define $R_{P,Q}(y,z)$ similarly.

The next three propositions give our required understanding of resultants. For the second one, we shall require the following version of Gauss' Lemma:

Gauss' Lemma. *Let R be a UFD and K field containing R such that every element of K can be written xy^{-1} where $x, y \in R$; then $P, Q \in R[x]$ have a non-constant common factor in $R[x]$ if and only if that have a non-constant common factor in $K[x]$.*

A proof can be found in any standard algebra text.

Proposition 1. *1. Let $P, Q \in h[x]$ be monic, where h is an arbitrary field; then $R_{P,Q} = 0$ if and only if P and Q have a common factor in $k[x]$.*

2. Let $P, Q \in h[x,y,z]$ be homogeneous polynomials with $P(1,0,0)Q(1,0,0) \neq 0$ and h an arbitrary field; then $R_{P,Q} = 0$ if and only if P and Q have a non-constant homogeneous common factor in $h[x,y,z]$.

Proof. 1. Suppose R, Q have a common factor, i.e. $P(x) = S(x)\phi(x), Q(x) = S(x)\psi(x)$, where $\deg S \geq 1$ (otherwise S is constant and not a common

factor). Assume $\phi(x) = c_0 + \ldots + c_{n-1}x^{n-1}$ and $\psi(x) = d_0 + \ldots + d_{m-1}x^{m-1}$ (the higher coefficients of either can be zero, but ϕ and ψ are not identically zero), then the relation $P\psi = S\phi\psi = Q\phi$ gives a non-trivial linear dependence on the rows of the matrix that defines $R_{P,Q}$,

$$\sum_{j=1}^{m} d_{j-1} \cdot (j\text{-th row}) - \sum_{i=1}^{n} c_{i-1} \cdot (m + i\text{-th row}) = 0$$

(note that we are identifying the rows as in the span of the basis $\{x^i\}$). Therefore, we have $R_{P,Q} = 0$. Conversely, the exact reverse of this derivation gives polynomials ϕ and ψ such that $P\psi = Q\phi$ when $R_{P,Q} = 0$, with $\deg \psi \leq m-1$, $\deg \phi \leq n-1$. Since $h[x]$ is a UFD, this implies they have a common factor.

2. We can assume that $P(1,0,0) = Q(1,0,0) = 1$; in this case we can regard P and Q as monic polynomials in x with coefficients in $h[y,z]$. By above, we have $R_{P,Q} = 0$ if and only if P, Q have a common factor in $h[y,z][x]$. By Gauss' Lemma, this is itself equivalent to P and Q having a common factor in $(h[y,z])[x]$. We finally note that every factor of a homogeneous polynomial is homogeneous; see Appendix B.

□

Proposition 2. *If $P, Q \in k[x,y,z]$ are homogeneous of degree n and m, then $R_{P,Q}$ is homogeneous of degree nm if it is not identically zero.*

Proof. Let $r_{i,j}(y,z)$ be the (i,j)-th element of the resultant matrix, and $d_{i,j}$ be its degree. After staring at the resultant matrix for long enough, we find

$$d_{i,j} = \begin{cases} n+j-i, & \text{if } 1 \leq i \leq m,\ i \leq j \leq n+i \\ j-i, & \text{if } m+1 \leq i \leq m+n,\ i-m \leq j \leq i \\ -\infty, & \text{otherwise.} \end{cases}$$

Each summand of the determinant is $\prod_i r_{i,\sigma(j)}(y,z)$, where $\sigma \in S_{n+m}$. Each of the non-zero summands have degree

$$\sum_{i=1}^{n+m} d_{i,\sigma(j)} = \sum_{i=1}^{m} n + i - \sigma(j) + \sum_{i=1}^{n} i - \sigma(j) = nm,$$

and so does $R_{P,Q}$ □

Proposition 3. *If $P(x) = \prod_{i=1}^{n}(x-\lambda_i), Q(x) = \prod_{j=1}^{m}(x-\mu_i) \in k[x]$, then*

$$R_{P,Q} = \prod_{i,j}(\lambda_i - \mu_j).$$

Proof. By definition, the resultant $R_{P,Q}$ can be identified as a polynomial in $k[\lambda_1, \ldots, \lambda_n, \mu_1, \ldots \mu_m]$. For any λ_i of we have

$$R_{P,Q} \in k(\lambda_1 \ldots \lambda_{i-1}, \lambda_{i+1}, \ldots, \lambda_n, \mu_1, \ldots, \mu_m)[\lambda_i].$$

The resultant vanishes whenever $\lambda_i = \mu_j$ for some j; therefore $R_{P,Q}$ is seen to be divisible by $(\lambda_i - \mu_j)$. Since λ_i, μ_j were arbitrary, k is algebraically closed, and these are the only possible roots of P, we have by comparison of degrees

$$R_{P,Q} = c \prod_{i,j} (\lambda_i - \mu_j),$$

for some scalar $c \in k$. To determine the constant, put $P = (x - \lambda_i)^n, Q = x^m$ so that $\mu_j = 0 \; \forall j$. In this case the matrix is upper triangular and can be evaluated as

$$\det \begin{pmatrix} a_0 & a_1 & \cdots & \cdots & \cdots & 1 & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & \cdots & a_{n-1} & 1 & 0 & \cdots & 0 \\ \vdots & & \ddots & & & \vdots & & & \vdots & \vdots \\ 0 & \cdots & 0 & a_0 & \cdots & \cdots & \cdots & \cdots & \cdots & 1 \\ 0 & 0 & \cdots & \cdots & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & & \vdots & & & & \vdots & \\ 0 & \cdots & 0 & 0 & \cdots & & & & \cdots & 1 \end{pmatrix} = a_0^m = (\prod_{i=1}^{n} (-\lambda_i))^m$$

$$= \prod_{i=1}^{n} (-\lambda_i)^m;$$

therefore $c = 1$.

□

Corollary. $R_{P,QS} = R_{P,Q} R_{P,S}$

Proof. Obvious from above. □

3 Intersection Multiplicity and Bézout's Theorem

We can already prove a very strong statement about projective curves easily. Two algebraic curves are said to have a *common component* if the unique polynomials defining them have a non-constant greatest common divisor. Conceptually, if $P, Q, H \in k[x, y]$ and H is a non-constant greatest common divisor of P and Q, then the set of (x, y) such that $H(x, y) = 0$ is a curve that is a subset of both of the curves defined by P and Q.

Theorem 1. *(Weak Bézout's Theorem) Suppose C and D are projective curves (defined by polynomials P and Q) of degree n and m respectively without a common component, then they intersect at most nm times.*

Proof. Make a change of coordinates (see Appendix) such that $[1:0:0]$ does not belong to $C \cup D$ or any line going through two distinct points of intersection; then $P(1,0,0)Q(1,0,0) \neq 0$. If the resultant of P and Q was identically zero then they would share a non-constant common factor by Proposition 1, implying they have a common component. Therefore, the resultant splits into the product of nm linear factors (counting multiplicity) of the form $b_i z - c_i y$ (see Appendix). For each (b_i, c_i) we can find an a_i such that $P(a,b,c) = Q(a,b,c) = 0$, since $R_{C,Q}(b_i, c_i) \equiv 0$; this gives a point of intersection $[a_i : b_i : c_i]$ for each (b_i, c_i). If there was another distinct point of intersection $[\alpha : \beta : \gamma] \neq [a_i : b_i : c_i]$ $\forall i$ then it would be the case that $b_j\gamma - c_j\beta = 0$ for some j (otherwise it would not be a root of the resultant and so would not be a point of intersection). This would imply that $[\alpha : \beta : \gamma], [a_j : b_j : c_j]$ and $[1:0:0]$ all lie on the line

$$b_j z = c_j y,$$

in contradiction to our conditions on $[1:0:0]$; hence, another distinct point of intersection cannot happen. Since there can only be at most nm distinct factors of the resultant, the result follows. □

We now enter into the technical heart of Bézout's Theorem. The most difficult part is in giving a satisfactory definition of intersection multiplicity for arbitrary projective curves and showing it is well-defined. Intuitively when we think of the cubic $y = x^3$, it seems to 'interact' with the x-axis at the origin more intimately than than the line $y = x$. We could formally define the intersection multiplicity of the curve $y = x^n$ with the x-axis at the origin to be n, then extrapolate to other curves through coordinate transformations and the like. Other than some technicalities, this is essentially how we define the intersection multiplicity.

Definition. *An intersection multiplicity $I_p(C, D)$ at a point $p \in \mathbb{P}^2(k)$ is a quantity that satisfies the following axioms:*

1. $I_p(C,D) = \begin{cases} \infty, & p \text{ is in a common component of } C \text{ and } D \\ \in \mathbb{Z}_{>0}, & p \in C \cap D, \text{ not in a common component} \\ 0, & p \notin C \cap D. \end{cases}$
2. $I_p(C,D) = I_p(D,C)$
3. *If C and D are lines and $C \cap D = \{p\}$ then* $I_p(C,D) = 1$
4. $I_p(C_1C_2, D) = I_p(C_1, D) + I_p(C_2, D)$

5. $I_p(C, D) = I_p(C, D + CR)$ *if deg* $R =$ *deg* $D -$ *deg* C *(for homogeneity).*

Theorem 2. *There exists a unique intersection multiplicity defined for all projective curves and points in the projective plane.*

Proof. As with most proofs of this type, uniqueness is the most difficult part to verify. For ease of notation we denote the intersection multiplicity of the curves by their polynomials, $I_p(P, Q)$.

(Existence) Define

$$I_p(P,Q) = \begin{cases} \infty, & p \text{ is in a common component of } C \text{ and } D \\ 0, & p \notin C \cap D. \end{cases}$$

When $p \in C \cap D$ and not in a common component of C and D, we define $I_p(P, Q)$ as follows. Remove any common factor of P and Q and choose a coordinate system such that $[1 : 0 : 0]$ is not in $C \cup D$, any line containing two distinct points of $C \cap D$, or the tangent lines of C or D at any point of $C \cap D$ (this is possible since $C \cap D$ is finite by Weak Bézout's Theorem). For such a $p = [a : b : c] \in C \cap D$, we make $I_p(P, Q)$ equal to the exponent of $bz - cy$ in $R_{P,Q}$. Note that this is invariant under rescaling of P or Q. We verify the axioms:

1. Since $R_{P,Q} = (-1)^{nm} R_{Q,P}$, the exponents coincide.
2. If $p \in C \cap D$ and not in a common component of C and D, then $I_p(P, Q) \in \mathbb{Z}_{>0}$ since the resultant has non-negative exponents.
3. If P and Q are of degree 1 then so is the resultant, hence $I_p(P, Q) = 1$.
4. Since $R_{P_1P_2,Q} = R_{P_1,Q} R_{P_2,Q}$, the exponent of $bz - cy$ on the left hand side is equal to the sum of the its exponents on the right hand side.
5. The resultant matrix of $R_{P,Q+PR}$ can be transformed by elementary row operations into the resultant matrix of $R_{P,Q}$; hence their determinants have the same exponent.

(Uniqueness) This is the hard part. We will show that the intersection multiplicity can be calculated using only the axioms, implying they determine it completely. The cases for $p \notin C \cap D$ and p in a common component of C and D are already determined by axiom 1. Therefore we assume that $p \in C \cap D$ but not in a common component, and that C, D are irreducible by our construction of $I_p(P, Q)$ in removing any common components. The axioms are independent of our choice of coordinates since the multiplicity of the root in the resultant is invariant (see Appendix), so we may assume that $p = [0 : 0 : 1]$. Assume

throughout that P, Q have degree n, m respectively. We will show that the intersection multiplicity $I_p(P, Q)$ can be written $I_p(P, Q) = I_p(R, Q) + q$ where $q > 0$ and the degree of R is less than P; this implies that the axioms can be used continuously to reduce the calculation to the case of P and Q being lines, in which case we can then invoke axiom 3. Put $I_p(P, Q) = c$.

Let

$$\deg P(x, 0, 1) = r \leq s = \deg Q(x, 0, 1)$$

without loss or generality by axiom 2. There are two cases to consider.

1. $r = 0$.
   Write

   $$P(x, y, z) = P(x, 0, z) + yR(x, y, z), Q(x, y, z) = Q(x, 0, z) + yS(x, y, z),$$

   for some R, S both homogeneous. Since $r = 0$, $P(x, 0, 1)$ is constant and identically zero since $P(0, 0, 1) = 0$. This implies the highest power of z has coefficient equal to zero, hence $P(x, 0, z)$ is identically zero.

   Write $Q(x, 0, z) = x^q T(x, z)$, where $T(0, 1) \neq 0$; since then the highest power of z has coefficient equal to zero and would could factor out another x term. Note that $q > 0$ since $Q(0, 0, 1) = 0$ implies again that the term of the highest power of z is zero; and that T is homogeneous of degree $m - q$ since $Q(x, 0, z)$ is homogeneous of degree m. The condition $T(0, 1) \neq 0$ implies that p does not lie on the curve $T(x, z) = 0$, hence $I_p(y, T) = 0$. Putting all of this together we have

   $$\begin{aligned} I_p(P, Q) &= I_p(R, Q) + I_p(y, Q) && \text{by axiom 4} \\ &= I_p(R, Q) + I_p(y, x^q T) && \text{since } Q(x, 0, z) = x^q T \\ &= I_p(R, Q) + qI_p(y, x) + I_p(y, T) && \text{again by axiom 4} \\ &= I_p(R, Q) + q; \end{aligned}$$

2. $r > 0$.
   Multiply P, Q to make $P(x, 0, 1), Q(x, 0, 1)$ monic. Introduce the auxiliary polynomial

   $$G(x, y, z) = z^{n+s-r} Q(x, y, z) - x^{s-r} z^m P(x, y, z),$$

   which is defined so as to be homogeneous and the polynomial in x

   $$G(x, 0, 1) = Q(x, 0, 1) - x^{s-r} P(x, 0, 1)$$

   have degree strictly less that s; this follows from $Q(x, 0, 1), P(x, 0, 1)$ being both monic. Note G is not identically zero since P, Q don't share a

common component. We have,

$$\begin{aligned} I_p(P,Q) &= (n+s-r)\cdot 0 + I_p(P,Q) \\ &= (n+s-r)\cdot I_p(P,z) + I_p(P,Q) && \text{since } p \text{ is not on the line } z=0 \\ &= I_p(P, z^{n+s-r}) + I_p(P,Q) && \text{by axiom 4} \\ &= I_p(P, z^{n+s-r}Q), && \text{again by axiom 4} \\ &= I_p(P, z^{n+s-r}Q - x^{s-r}z^m P) && \text{by axiom 5} \\ &= I_p(P,G). \end{aligned}$$

Since G has degree strictly less than s, this can be used in a finite number of steps (interchanging P and Q is necessary) to reduce the problem to the case $r = 0$.

□

Now we can proceed leisurely once again.

Theorem 3. *(Bézout's Theorem) Suppose C and D are projective curves, with no common component, of degree n and m respectively; then they have exactly nm points of intersection, counting multiplicities.*

Proof. From above and the fact that k is algebraically closed we have that $R_{P,Q}$ splits into linear factors as

$$R_{P,Q} = \prod_{i=1}^{k} (b_i z - c_i y)^{e_i}.$$

By similar arguments used above to prove Weak Bézout's Theorem, after a change of coordinates we can find a unique a_i for each (b_i, c_i) such that $p = [a_i : b_i : c_i] \in C \cap D$; therefore,

$$\sum_{q \in C\cap D} I_q(P,Q) = \sum_{p_i \in C\cap D} I_{p_i}(P,Q) = \sum_i e_i = \deg R_{P,Q} = nm$$

□

Note that distinct linear factors in the resultant do not correspond to distinct intersection points in general! Only after making the change of coordinates such that $[1:0:0] \notin C \cap D$ or any line going through two points of intersections does this become the case. However, the number of distinct intersection points and their multiplicity is invariant, since the intersection multiplicity was defined axiomatically without any reference to polynomials and their coordinates; so Bézout's Theorem still holds.

Example 3.1. Let C_1, C_2 be the *lemniscates* defined by

$$x^4 + y^4 + x^2 - y^2 = 0$$

$$x^4 + y^4 - x^2 + y^2 = 0.$$

In the complex projective plane they are defined by,

$$x^4 + y^4 + x^2z^2 - y^2z^2 = 0$$

$$x^4 + y^4 - x^2z^2 + y^2z^2 = 0.$$

Equating the polynomials, we have the relation

$$z^2(x-y)(x+y) = 0;$$

hence our only candidates for intersections are on the lines $x = \pm y$ and $z = 0$ (the line at infinity). Setting $y = \pm x$ gives $x^4 = 0$ hence the only intersection in this case is at the origin. We calculate its intersection multiplicity by

$$\begin{aligned}
I_{[0:0:1]}(C_1, C_2) &= I_{[0,0,1]}(x^4 + y^4 + x^2z^2 - y^2z^2, x^4 + y^4 - x^2z^2 + y^2z^2) \\
&= I_{[0:0:1]}(x^4 + y^4 + x^2z^2 - y^2z^2, 2y^2 - 2x^2) \\
&= I_{[0:0:1]}(x^4 + y^4, 2y^2z^2 - 2x^2z^2). \\
&= I_{[0:0:1]}(x^4 + y^4, 2(x-y)(x+y)) + I_{(0,0,1)}(x^4 + y^4, z^2) \\
&= I_{[0:0:1]}((x - \zeta_{4,1}y)(x - \zeta_{4,2}y)(x - \zeta_{4,3}y)(x - \zeta_{4,4}y), 2(x-y)(x+y)) \\
&= 4 \cdot 2 = 8,
\end{aligned}$$

where $\zeta_{4,i}$, $i = 1, 2, 3, 4$ are the 4-th roots of unity. Since $(\deg C_1)(\deg C_2) > 8$ we still have some points to find. Setting $z = 0$ we have

$$x^4 + y^4 = (x - \zeta_{4,1}y)(x - \zeta_{4,2}y)(x - \zeta_{4,3}y)(x - \zeta_{4,4}y) = 0;$$

therefore we have four other points at infinity of the form $p_i = [\zeta_{4,i} : 1 : 0]$ (recall scaling of points gives the same point in the projective plane). Calculating the intersection multiplicity gives,

$$\begin{aligned}
I_{p_i}(C_1, C_2) &= I_{p_i}(x^4 + y^4 + x^2z^2 - y^2z^2, x^4 + y^4 - x^2z^2 + y^2z^2) \\
&= I_{p_i}(x^4 + y^4, 2(x-y)(x+y)) + I_{(0,0,1)}(x^4 + y^4, z^2) \\
&= I_{p_i}((x - \zeta_{4,1}y)(x - \zeta_{4,2}y)(x - \zeta_{4,3}y)(x - \zeta_{4,4}y), z^2) \quad = 2 \cdot 1 = 2,
\end{aligned}$$

for each p_i. We have the total intersection multiplicities 16=$(\deg C_1)(\deg C_2)$, as expected by Bézout's Theorem.

4 Classification of Cubic Curves

We can apply the machinery we have developed to a classification of nonsingular curves, and in particular cubic curves.

Proposition 4. *Let be C_1, C_2 be irreducible curves of degree d that intersect $d^2 + 1$ (or more) times at distinct points; then $C_1 = C_2$.*

Proof. By Bézout's Theorem, two such irreducible curves intersect no more than d^2 times. Therefore they must have a common component. Since they are irreducible, this implies they must be equal. □

This very nicely generalises the fact that two points define a line. We see that a curve of degree two is determined by five points (as long as no three are collinear). A curve of degree d is determined by d^2+1 points, as long as no d^2-1 of them are collinear. We can find such curves easily using linear algebra; every point imposes a linear constraint on the coefficients of the equations, which can be used to find the coefficients of each homogeneous term. Since no $d^2 - 1$ are collinear, the systems will not be degenerate.

For example with the quadric curve $ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0$, since there are 6 terms, we can evaluate it at the five points to determine the coefficients up to scaling.

The next theorem will be utilised to great effect in the next section.

Theorem 4. *(Cayley-Bacharach) Let C_1 and C_2 be two cubic curves that intersect in exactly nine points. Let C be a cubic passing through eight of the nine intersection points of C_1 and C_2; then C passes through the ninth intersection point as well.*

Proof. Let A_i, $i = 1, \ldots, 9$ be the intersection points. We will show that C must be defined by a homogeneous polynomial that is a linear combination of the polynomials that define C_1, C_2. Suppose this is not the case. We work on preliminary cases before making the final argument.

No four of the points are collinear; for if they were, then both C_1, C_2 would intersect the line four times, in contradiction to Bézout's Theorem. Any five of these points determine a quadric curve by the above proposition. This curve is unique; for if two different quadric curves shared these same five points, then they would again contradict Bézout's Theorem.

Suppose three of the given points A_1, A_2, A_3 are collinear on the line l. The remaining five determine a unique quadric $\sigma$by above. Let P be another point on l, and Q a point not on l or σ. Let p_1, p_2 and p_3 and q_1, q_2 and q_3 denote the

values the cubics C_1, C_2 and C take at the points P and Q respectively. The system of equations

$$p_1x + p_2y + p_3z = 0$$

$$q_1x + q_2y + q_3z = 0$$

has a non-trivial solution by linear algebra. If (a, b, d) is a solution then we have a non-trivial combination $D = aC_1 + bC_2 + dC$, and D vanishes at P and Q. Further, D is not constant since by assumption C is not a linear combination of C_1, C_2. Now, since l intersects D at four points A_1, A_2, A_3 and P, Bézout's Theorem forces D to contain the line l. Thus D is the product of l and σ by above; but then Q lies on either l or σ, a contradiction. No three points are collinear.

Similarly, suppose six of the first eight points - say $A_1, \ldots, A_6$ - lie on a quadric σ. Since no three points can be collinear by above, the quadric must be an irreducible conic. As before, let l be the line going through A_7, A_8, P another point on σ, and Q and point on neither l or σ. By the same argument as above we can find a non-trivial cubic $D = aC_1 + bC_2 + dC$ vanishing on P and Q. As D vanished on seven points of σ; since σ is a conic D must contain σ entirely. Therefore D is the union of σ and the line l; but then this curve cannot pass through C by assumption, which is a contradiction.

Finally, let l be the line going through A_1, A_2 and σ going through $A_3, \ldots, A_7$; from the above arguments σ is a conic, and A_8 cannot lie on l (no three points are collinear) or σ(no five points like on on a quadric curve). As before pick two points P, Q on l but not σ; then there exists $D = aC_1 + bC_2 + dC$ vanishing on P, Q. Since D is a cubic that vanishes at four points of l and five points of the conic σ it must be the union of these two; but then A_8 does not pass through D, a contradiction. Therefore C must be a linear combination of C_1, C_2 and so must pass through all nine intersection points. □

We continue in our classification of nonsingular and irreducible curves.

Definition. 1. *We formally define the partial derivatives* $P_x = \frac{\partial P}{\partial x}, P_y = \frac{\partial P}{\partial y}$, $P_z = \frac{\partial P}{\partial z}$ *of a polynomial formally so that they coincide with the usual definition of partial derivatives. A projective curve* C *defined by a homogeneous polynomial* $P \in k[x, y, z]$ *is called singular if there exists a point* $[a : b : c] \in C$ *such that*

$$P_x(a, b, c) = P_y(a, b, c) = P_z(a, b, c) = 0.$$

2. *The tangent line to* C *at a nonsingular point* $p = [a : b : c]$ *is the line given by*

$$xP_x(a, b, c) + yP_y(a, b, c) + zP_z(a, b, c) = 0.$$

Proposition 5. *1. Every nonsingular projective curve is irreducible*

2. If a projective curve is irreducible then it has finitely many singular points

Proof. 1. Suppose C is reducible, then its defining polynomial can be written as a product of non-constant polynomials $P = RS$. By Bézouts Theorem, both R and S have a common zero $p = [a : b : c]$ with

$$P(a,b,c) = P_x(a,b,c) = R_x(a,b,c)S(a,b,c) + S_x(a,b,c)R(a,b,c) = 0,$$

and similarly for $P_y(a,b,c) = 0 = P_z(a,b,c)$, in contradiction to C being nonsingular.

2. Suppose C is defined by P of degree n. By a change of coordinates, we can assume that $[1:0:0] \notin C$, which implies that the coefficient of the x^n term is non-zero; therefore P_x is of degree $n-1$ and does not have a common factor with P since its irreducible. By Bézout's Theorem, they have at most $n(n-1)$ distinct roots in common, implying C can have at most $n(n-1)$ singular points.

□

Example 2.3 Let C be an irreducible conic curve in the projective plane. Write its defining polynomial as

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz.$$

Since there are only finitely many singular points we can perform a change of coordinates so that $[0:1:0] \in C$ and is nonsingular, with its tangent line given by $z = 0$. This implies that the coefficient of the y^2 term is zero, and that

$$P_x(0,1,0) = P_y(0,1,0) = 0;$$

implying $d = 0$. Our conic is reduced to

$$ax^2 + cz^2 + exz + fyz.$$

Apply the projective transformation $[x' : y' : z'] = [\sqrt{a}x : fy + ex + cz, -z]$ to obtain,

$$(\sqrt{a}x)^2 + z(cz + ex + fy) = x'^2 - z'y',$$

a parabola. Conclusion: the classic conic sections are equivalent up to projective transformations in the projective plane.

In fact we can do one better; we show all nonsingular cubics can be put into a particularly nice form. From now on we assume k is algebraically closed with $\mathrm{char}(k) \neq 2, 3$ (this is so that transformations involving their reciprocals are well-defined).

Definition. *Let $P(x,y,z)$ be a homogeneous polynomial of degree d, then the Hessian H_P is defined as the degree $3(d-1)$ (if $d \leq 1$, then $-\infty$) polynomial*

$$H_P(x,y,z) = \det \begin{pmatrix} P_{xx} & P_{xy} & P_{xx} \\ P_{yx} & P_{yy} & P_{yz} \\ P_{zx} & P_{zy} & P_{zz} \end{pmatrix}.$$

A nonsingular point $[a : b : c] \in C$ is called a point of inflection of C if $H_P(a,b,c) = 0$.

Proposition 6. *(Euler's relation) If $R(x,y,z)$ is a homogeneous polynomial of degree m then*

$$x\frac{\partial R}{\partial x} + y\frac{\partial R}{\partial y} + z\frac{\partial R}{\partial z} = mR.$$

Proof. Each term of R is of the form $x^i y^j z^k$ with $i+j+k = m$. For any such term we have

$$x\frac{\partial}{\partial x}(x^i y^j z^k) + y\frac{\partial}{\partial y}(x^i y^j z^k) + z\frac{\partial}{\partial z}(x^i y^j z^k) = m x^i y^j z^k.$$

The general result follows by the linearity of the derivative. □

Lemma. *If $d = deg\ P > 1$ and $d - 1 \neq 0$ in k, then*

$$y^2 H_P(x,y,z) = (d-1)^2 \det \begin{pmatrix} P_{xx} & P_x & P_{xz} \\ P_x & \frac{d}{d-1}P & P_z \\ P_{zx} & P_z & P_z \end{pmatrix}.$$

Proof. From Euler's relation above we have,

$$dP = xP_x + yP_y + zP_z$$

$$(d-1)P_x = xP_{xx} + yP_{yx} + zP_{zx}$$
$$(d-1)P_y = xP_{xy} + yP_{yy} + zP_{zy}$$
$$(d-1)P_z = xP_{xz} + yP_{yz} + zP_{zz}.$$

Expanding out the right hand side and using these relations, then collecting terms, gives the desired result. □

Theorem 5. *Every nonsingular cubic curve C in the projective plane under a projective transformation can be transformed into a cubic of the form*

$$y^2 z = x(x-z)(x-\lambda z),$$

where $\lambda \in k - \{0,1\}$.

Proof. Let P be the polynomial that defines C. Since $\deg H_P = 3(3-2) = 3$ $= \deg P$, H_P and P have a point of intersection; which implies C has a point of inflection $p = [a : b : c]$. By a change of coordinates we can assume that $p = [0 : 1 : 0]$ and that the tangent line at p is $z = 0$. By the definition of the tangent line at a point on the curve, we have

$$P(0,1,0) = P_x(0,1,0) = P_y(0,1,0) = H_P(0,1,0) = 0;$$

while

$$P_z(0,1,0) \neq 0,$$

since C is nonsingular. By the above lemma we have,

$$y^2 H_P(x,y,z) = 4 \det \begin{pmatrix} P_{xx} & P_x & P_{xz} \\ P_x & \frac{3}{2}P & P_z \\ P_{zx} & P_z & P_z \end{pmatrix};$$

therefore,

$$0 = y^2 H_P(0,1,0) = 4 \det \begin{pmatrix} P_{xx} & 0 & P_{xz} \\ 0 & 0 & P_z \\ P_{zx} & P_z & P_z \end{pmatrix} = -4(P_z(0,1,0))^2 P_{xx}(0,1,0),$$

implying $P_{xx}(0,1,0) = 0$. Putting this together, this means that the coefficients of following terms are zero: y^3, xy^2, x^2y. Rewrite P without these terms as

$$\begin{aligned} P(x,y,z) &= Q(x,z) + \alpha xyz + \beta y^2 z + \gamma y z^2 = Q(x,z) + yz(\alpha x + \beta y + \gamma z) \\ &= Q(x,z) + z(\beta y^2 + (\alpha x + \gamma z)y) \\ &= Q(x,z) + z((\sqrt{\beta}y + \frac{\alpha x + \gamma z}{2\sqrt{\beta}})^2 - \frac{(\alpha x + \gamma z)^2}{4\beta}) \\ &= Q'(x,z) + z(\sqrt{\beta}y + \frac{\alpha x + \gamma z}{2\sqrt{\beta}})^2 \end{aligned}$$

where Q, Q' are homogeneous of degree 3 and $\beta = P_z(0,1,0) \neq 0$. Therefore, we can perform the change of coordinates

$$[x : y : z] \mapsto [x' : \sqrt{\beta}y' + \frac{\alpha x' + \gamma z'}{2\sqrt{\beta}} : z'],$$

to have C defined by a polynomial of the form

$$R(x,z) + y^2 z,$$

where R is homogeneous of degree 3. Since C is nonsingular, z does not divide R, which implies the x^3 term is nonzero. We can split R as

$$R(x,z) = u(x - az)(x - bz)(x - cz),$$

where $u \neq 0$ and a, b, c being distinct by nonsingularity of C. To facilitate the final change of coordinates, write the full expression defining C as,

$$\left(\frac{y}{\sqrt{u(b-a)^3}}\right)^2 z = \left(\frac{x-az}{b-a}\right)\left(\frac{x-az}{b-a} - z\right)\left(\frac{x-az}{b-a} - \frac{b-c}{b-a}z\right),$$

then perform $[x : y : z] \mapsto [\frac{x'-az'}{b-a} : \frac{y'}{\sqrt{u(b-a)^3}} : z']$ to obtain

$$y^2 z = x(x-z)(x-\lambda z),$$

for $\lambda = \frac{b-c}{b-a} \in k$. □

Corollary. *If C is a nonsingular projective cubic curve with a point of inflection $p = [a : b : c]$ then under a projective transformation it may be written as a cubic of the form*

$$y^2 z = x^3 + \alpha x z^2 + \beta z^3,$$

with the image of p being $[0 : 1 : 0]$. Equivalently, every such nonsingular cubic is equivalent in the affine plane to the depressed cubic

$$y^2 = x^3 + \alpha x + \beta.$$

Proof. Compose the above transformation with

$$[x : y : z] \mapsto [x' + \frac{\lambda+1}{3} z' : y' : z']$$

to obtain

$$y^2 z = x^3 + xz^2(-\frac{1}{3}\lambda^2 + \frac{1}{3}\lambda - \frac{1}{3}) + (-\frac{2\lambda^3}{27} + \frac{\lambda^2}{9} + \frac{\lambda}{9} - \frac{2}{27}).$$

□

This form of a cubic curve is very special. A cubic that be put into this form is called an *elliptic curve*.

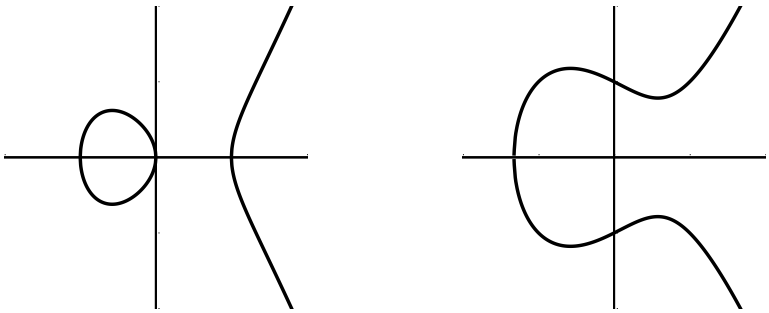
5 The Group Law on Elliptic Curves

Definition. *An elliptic curve is a nonsingular cubic curve.*

For simplification[1] we assume all of our elliptic curves are in the form $y^2 z = x^3 - \alpha x z^2 - \beta z^3$ with an inflection point at $p = [0 : 1 : 0]$. Note

[1] Our subsequent constructions are invariant under projective change of variables and so our elliptic curve is not required to be in Weierstrass form to derive them; however the proof of this (that a change of variables is a group homomorphism) would take us too far afield.

that in this form they are symmetric about the x-axis, and that its only point at infinity is the point $[0:1:0]$. Since they're nonsingular, their discriminant $\Delta = (4a^3 - 27b^2)$ is non-zero. Over $\mathbb{A}^2(\mathbb{R})$ they will always look like one of the two figures below, depending on whether their roots of the right hand terms include a complex conjugate pair.



$\Delta < 0$ $\Delta > 0$

Elliptic curves are rich in structure and are very important. They are the source of a great amount of ongoing research throughout the mathematical community. This is largely because of the following theorem.

Theorem 6. *Given two points P, Q on an elliptic curve E, construct the unique line l going through them. By Bézout's Theorem the line must meet the cubic in a third point, counting multiplicity (ie. this third point may be P or Q). Reflect this third point about the x-axis (ie. $[x:y:z] \mapsto [x:-y:z]$) and define this point to be the formal sum $P+Q$. This definition is well-defined and defines an abelian group on our elliptic curve E we denote by $E(\mathbb{C})$, with identity element $[0:1:0]$.*

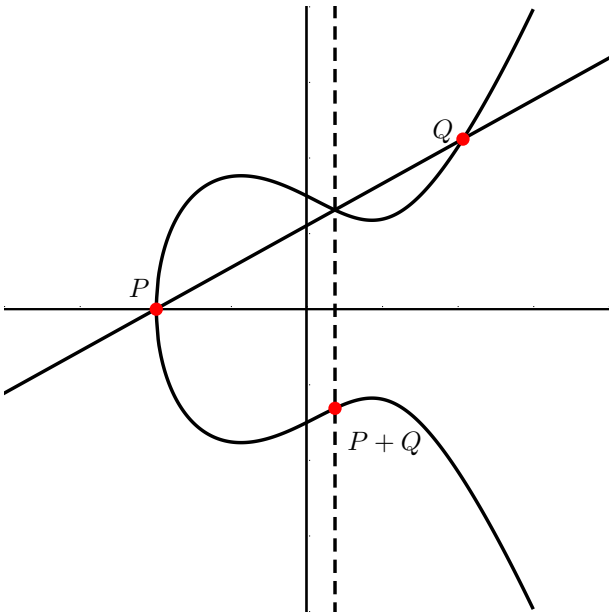
Proof. Its clear from the results we have proved above that the construction is well-defined and gives a unique point on the elliptic curve for each sum of points. We prove the group axioms - associativity is the hardest part.

1. (Existence of identity) Define $O := [0:1:0]$. It is obvious that O is the identity - O is the point infinitely far away in the y-direction, which means any line connecting it with a point on our curve is vertical and so reflects our point about the x-axis; reflecting again gives us the same point.
2. (Closure) Clear from our definition of $P + Q$.
3. (Commutativity) Follows from the fact that there is only one line going through any two points so the third intersection point is unique.
4. (Existence of inverse) For every point $P = [a:b:c]$ define

$-P := [a : -b : c]$. The line joining these two points is vertical and so intersects the curve at infinity, implying $P - P = O$.

5. (Associativity) Let P, Q, R lie on our curve E. Consider the points P, Q, R, $P+Q, -(P+Q), Q+R, -(Q+R), -((P+Q)+R)$ and $-(P+(Q+R))$. If any of them were equal to the identity then associativity would follow. Assume this is not the case. Let l_1, l_2, l_3 be the lines joining the points P & Q, Q & R, and P & $(Q+R)$ respectively; and likewise denote the lines joining the points $(P+Q)$ & R, O & $(Q+R)$, and O & $(P+Q)$ by l_4, l_5, and l_6. Let C be the cubic curve consisting of the lines l_1, l_4, and l_5 and D be the cubic curve consisting of l_2, l_3 and l_6. The cubic curves E, C, D meet at eight points; by the Cayley Bacharach Theorem they must intersect at nine points, implying the points $-((P+Q)+R)$ and $-(P+(Q+R))$ coincide.

□



Since the only the point O is gained when embedding E in the projective plane we can identify our curve as the set

$$E = \{(x, y) \in \mathbb{C} \mid y^2 = x^3 - \alpha x - \beta\} \cup \{O\}.$$

What is the structure of this group? Well first let's see explicitly how addi-

tion is calculated. Consider the points

$$P = (x_p, y_p),\ Q = (x_q, y_q)$$

and $S = (x_s, y_s)$ the third intersection with the elliptic curve before reflection about the x-axis, and assume $x_p \neq x_q$ (in this case, $P = Q$). Putting $\lambda = \frac{y_p - y_q}{x_p - x_q}$ then the line between P, Q is $y = y_p + \lambda(x - x_p)$; subbing back into $y^2 = x^3 - \alpha x - \beta$ gives

$$x^3 - \lambda^2 x^2 + (-\alpha + 2\lambda^2 x_p - 2\lambda y_p) - \beta - (\lambda x_p - y_p)^2 = 0.$$

The three solutions to this cubic are x_p, x_q, x_s, hence from Vieta's formulae we have $x_p + x_q + x_s = \lambda^2$ and from the equation of the line we also have $y_s = y_p + \lambda(x_s - x_p) = y_p + \lambda(x_s - x_p)$; therefore

$$P + Q = (x_s, -y_s) = (\lambda - x_p - x_q, \lambda(x_p - x_r) - y_p).$$

So addition is done by rational combinations of the coordinates! This immediately gives us two subgroups

$$E(\mathbb{R}) := \{(x, y) \in E(\mathbb{C}) \ : \ x, y \in \mathbb{R}\} \cup \{O\}$$
$$E(\mathbb{Q}) := \{(x, y) \in E(\mathbb{C}) \ : \ x, y \in \mathbb{Q}\} \cup \{O\},$$

when α and β are real or rational numbers respectively.

For the remainder of this paper we will investigate the properties of these groups.

6 Elliptic Functions

Definition. *1. A lattice is a set $\Lambda = w_1\mathbb{Z} \oplus w_2\mathbb{Z}$ where $w_1, w_2 \in \mathbb{C}$ are $\mathbb{R}$-independent. We make it into a group through component-wise addition.*

2. Given a lattice Λ over $\mathbb{C}$ we define a torus as the quotient $\mathbb{C}/\Lambda$.

Our aim is to prove that for every elliptic curve we have $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ as groups for some Λ; this leads us to the theory of elliptic functions.

Definition. *1. An elliptic function f is a meromorphic function on $\mathbb{C}$ which is periodic with respect to a lattice Λ.*

2. A fundamental parallelogram for a lattice Λ is a parallelogram of the form

$$D = \{x_1 w_1 + x_2 w_2 \ : \ x_1, x_2 \in [0, 1)\} \subset \mathbb{C}$$

where $a \in \mathbb{C}$ such that the natural map of sets $D \to C/\Lambda$ is bijective.

If we know what values an elliptic function f takes on a fundamental parallelogram D we know what values it takes on anywhere else. Note that since the set of poles of a meromorphic function is discrete we can always choose a fundamental parallelogram that has no zeroes or poles on its boundary.

Throughout, f is an elliptic function relative to a given $\Lambda = w_1\mathbb{Z} \oplus w_2\mathbb{Z}$ and D is a fundamental parallelogram with this property.

Proposition 7. *Every non-constant elliptic function must have a pole (and hence a zero).*

Proof. If not then our function is holomorphic. Since it's periodic we have $|f| \leq \sup_{z\in\bar{D}} |f(z)|$, implying by Liouville's Theorem that it's constant. If it had no zeroes, consider $\frac{1}{f}$. □

So every non-trivial elliptic function must have some zeros and poles. What about their orders and residues?

Proposition 8.
1. $\sum_{w\in D} res_w(f) = 0$
2. $\sum_{w\in D} ord_w(f) = 0$
3. $\sum_{w\in D} ord_w(f)w \in \Lambda$*; equivalently, the sum of poles minus the sum of zeros of an elliptic function is zero mod* Λ *counting multiplicity.*

Note that the summation here makes sense since the set of zeros and poles of a meromorphic function on a compact set are finite, for otherwise D *would have an accumulation point which would not be isolated.*

Proof. Recall the generalized argument principle, that says

$$\frac{1}{2\pi i}\int_C \frac{f'(z)}{f(z)} g(z)dz = \sum_{w\in C'} g(w)\mathrm{ord}_w(f)$$

when g is analytic in a region, C is a closed contour inside that region, and C' is the region enclosed by C.

1. We have
$$\sum_{w\in D} \mathrm{res}_w(f) = \frac{1}{2\pi}\int_{\partial D} f(z)dz.$$
Since f is periodic, integrating along opposite sides of the parallelogram cancel.

2. Since f is periodic, so is f'; from above we have
$$\sum_{w\in D} \mathrm{ord}_w(f) = \frac{1}{2\pi}\int_{\partial D} \frac{f'(z)}{f(z)}dz = 0.$$

3. Let $a = \inf_{z\in D} |z|$ so that $D = \{b + w_1 n_1 + w_2 n_2 \mid n_1, n_2 \in \mathbb{Z}\}$ for some b with $|b| = a$; then

$$\sum_{w\in D} \mathrm{ord}_w(f)w = \frac{1}{2\pi i}\left(\int_a^{a+w_1} + \int_{a+w_1}^{a+w_1+w_2} + \int_{a+w_1+w_2}^{a+w_2} + \int_{a+w_2}^{a}\right) z\frac{f'(z)}{f(z)}dz.$$

Making the change of variable $z \mapsto z - w_1$ in the second integral and $z \mapsto z - w_2$ in the third and using periodicity yields

$$\sum_{w\in D} \mathrm{ord}_w(f)w = \frac{w_2}{2\pi i}\int_a^{a+w_1} \frac{f'(z)}{f(z)}dz + \frac{w_1}{2\pi i}\int_a^{a+w_2} \frac{f'(z)}{f(z)}dz.$$

Both integrals are winding numbers around the origin of a path; and since $\frac{f'(z)}{f(z)}$ is periodic, it has equal values at the end points, implying the integrals divided by $2\pi i$ are integers. Therefore $\sum \mathrm{ord}_w(f)$ has the desired form.

□

By the second part of above, an elliptic function has the same number of zeros and poles counting multiplicity in a fundamental parallelogram.

It's easy to see that the set of elliptic functions on a lattice is a field $\mathbb{C}(\Lambda)$ under the usual operations. As it turns out, there's a special function which entirely determines it. We will introduce it, and show how it links complex tori and elliptic curves. We set $\Lambda^* = \Lambda\backslash\{0\}$.

Proposition 9. *1. The series $\sum_{w\in\Lambda^*} \frac{1}{w^3}$ is absolutely convergent. It follows that the series*

$$G_{2k}(\Lambda) = \sum_{w\in\Lambda^*} w^{-2k}$$

is absolutely convergent also for $k > 1$.

2. The series

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{w\in\Lambda^*}\left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right)$$

converges absolutely and uniformly on every compact subset of D.

3. The series $\wp_\Lambda(z)$ given above defines an even elliptic function relative to Λ having a double pole with residue 0 at each lattice point, and no other poles.

Proof. 1. Consider the parallelograms for $n \leq 1$

$$P_n = \{t_1 w_1 + t_2 w_2 \in \Lambda \mid t_1, t_2 \in \mathbb{Z}, \max\{|t_1|, |t_2|\} = n, \} \subset \Lambda.$$

If we enumerate

$$(-n,-n),(-n,-n+1),\ldots,(-n,n)$$
$$(n,-n),(-n,-n+1),\ldots,(n,n)$$
$$(-n,-n),(-n+1,-n),\ldots,(n,-n)$$
$$(-n,n),(-n+1,n),\ldots,(n,n)$$

this accounts for all points of P_n. Each line has $2n+1$ points, and $(-n,-n),(n,-n),(-n,n),(n,n)$ are double counted, hence $\#P_n = 8n$. Let l be the least distance between points from P_1 and the origin, then each point of P_n has a distance at least ln between it and the origin; therefore

$$\sum_{w\in\Lambda^*}\frac{1}{|w|^3} = \sum_{\substack{w\in P_n\\ n>0}}\frac{1}{|w|^3} \leq \sum_{n>0}\frac{8n}{l^3n^3} = \frac{8}{l^3}\sum_{n>0}\frac{1}{n^2},$$

implying the sum converges.

2. For each z in disk of radius r centred at the origin, we have $|w| > 2|z|$ for all but finite many $w \in \Lambda$. For those w's we have

$$\left|\frac{1}{(z-w)^2}-\frac{1}{w^2}\right| = \left|\frac{z(2w-z)}{w^2(z-w)^2}\right| \leq \frac{|z|(2+|\frac{z}{w}|)}{|w|^3(1-|\frac{z}{w}|)^2} < \frac{|z|(2+\frac{1}{2})}{|w|^3(1-\frac{1}{2})^2} \leq \frac{10r}{9|w|^3}$$

with the second inequality following from $|1-\frac{z}{w}|^2 \geq (1-|\frac{z}{w}|)^2$; hence this series converges absolutely uniformly on every compact subset of $\mathbb{C}\backslash\Lambda$.

3. By above the series defines a holomorphic function on $\mathbb{C}\backslash\Lambda$; by inspection it is meromorphic on $\mathbb{C}$ with a double pole at each point of Λ^*. It's even, since

$$\begin{aligned}\wp_\Lambda(-z) &= \frac{1}{(-z)^2}+\sum_{w\in\Lambda^*}\left(\frac{1}{(-z-w)^2}-\frac{1}{(-w)^2}\right)\\ &= \frac{1}{z^2}+\sum_{-w\in\Lambda^*}\left(\frac{1}{(z-w)^2}-\frac{1}{w^2}\right) = \wp_\Lambda(z).\end{aligned}$$

It remains to show it's periodic with respect to Λ. We have

$$\wp'_\Lambda(z) = \sum_{-w\in\Lambda^*}\frac{-2}{(z-w)^3},$$

implying that $\wp'_\Lambda$ is periodic. Integrating we find that $\wp_\Lambda(z+w)$ $= \wp_\Lambda(z)+c(w)$. Finally, we have

$$\wp_\Lambda\left(\frac{-w}{2}\right) = \wp_\Lambda\left(\frac{-w}{2}+w\right) = \wp_\Lambda\left(\frac{-w}{2}\right)+c(w)$$

since it's even; therefore $c(w)=0$, as desired.

□

The function $\wp_\Lambda$ is called the *Weierstrass $\wp$-function* relative to Λ, and $G_{2k}(\Lambda)$ is the *Eisenstein series of weight* $2k$ for Λ. For ease of notation we shall write $\wp_\Lambda = \wp$ for the rest of our exposition, where Λ is a fixed lattice.

Theorem 7. *If f is an elliptic function relative to Λ then $f \in \mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$.*

Proof. Since

$$f(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2}$$

we may reduce to the case where f is even or odd. But $\wp'$ is odd, implying $f \cdot \wp'$ is even if f is odd; therefore we may assume that f is even; note that this implies $\text{ord}_w f = \text{ord}_{-w} f \ \forall w \in \mathbb{C}$. Since f is elliptic it has the same number of zeros and poles counting multiplicity. Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be its zeros and poles, where $a_i, b_j \in D \ \forall i, j$. Define the function

$$g(z) = f(z) \left(\prod_{i=1}^{n} \frac{\wp(z) - \wp(a_i)}{\wp(z) - \wp(b_i)} \right)^{-1}.$$

Suppose first that 0 is neither a zero or a pole of f. We claim g is a holomorphic elliptic function, in which case the result follows since g must be constant. We know that for every k, $\wp(z) - \wp(a_k)$ and $\wp(z) - \wp(b_k)$ only has singularities at each point of Λ and they are double poles; hence g has removable singularities at each $z \in \Lambda$. For each k, $\wp(z) - \wp(b_k)$ has zeros of order 1 at $\pm b_k$ since $\wp$ is even and $b_k \neq 0$. Since multiplicity is counted in our product, g has a removable singularity at each $\pm b_k$, by comparison with the zeros of f. By an analogous argument, g has a removable singularity at each $\pm a_k$. This accounts for all poles, so g must be holomorphic. Since it's clearly elliptic, the claim follows.

Now, f being even implies that its Laurent series at the origin $f(z) = \sum_{k=-\infty}^{\infty} a_k z^k$ consists only of even powers since

$$0 = f(z) - f(-z) = \sum_{k=-\infty}^{\infty} (1 - (-1)^k) a_k z^k \implies a_k = 0 \text{ for odd } k.$$

Suppose f vanishes at the origin with order $2m$, then since $\wp^m$ has a pole of order $2m$ the function $f \cdot \wp^m$ has a removable singularity at the origin and so doesn't vanish there. Therefore we reduce to the case above. If f has a pole at the origin then analogously we find that the function $\frac{f}{\wp^m}$ reduces to the case above for some m. □

Now we can use the Laurent expansion of $\wp$ around the origin to investigate the connection with elliptic curves.

Proposition 10. *1. The Laurent series for $\wp$ around the origin is*

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+1} z^{2k}.$$

2. *For every* $z \in \mathbb{C}\backslash\Lambda$,

$$\wp'^2 = 4\wp^3 - 60G_4\wp - 140G_6.$$

3. *Put* $g_2 = g_2(\Lambda) = 60G_4(\Lambda)$ *and* $g_3 = g_3(\Lambda) = 140G_6(\Lambda)$, *then the polynomial*

$$4x^3 - g_2x - g_3$$

has distinct roots; equivalently, $\Delta(\Lambda) = g_2^3 - 27g_3^2 \neq 0$.

Proof. 1. For all z with $|z| < |w|, w \in \Lambda^*$ write

$$\frac{1}{(z-w)^2} - \frac{1}{w^2} = \frac{1}{w^2}\left(\frac{1}{(1-\frac{z}{w})^2} - 1\right) = \sum_{n=1}^{\infty}(n+1)\frac{z^n}{w^{n+1}};$$

then

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + \sum_{\Lambda*}\left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right) \\
&= \frac{1}{z^2} + \sum_{\Lambda*}\left(\sum_{n=1}^{\infty}(n+1)\frac{z^n}{w^{n+2}}\right) \\
&= \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)\sum_{\Lambda*}\frac{z^{2k}}{w^{2k+2}}, \text{ since for odd } n \text{ the terms } \frac{1}{w^{n+2}} \text{ and } \frac{1}{-w^{n+2}} \text{ cancel} \\
&= \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k}.
\end{aligned}$$

2. Computing the Laurent series of various terms we have

$$\begin{aligned}
\wp'(z)^2 &= 4z^{-6} - 24G_4z^{-2} - 80G_6 + \dots \\
\wp(z)^3 &= z^{-6} + 9g_4z^{-2} + 15G_6 + \dots \\
\wp(z) &= z^{-2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k}.
\end{aligned}$$

Comparing terms we see that the elliptic function

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

is holomorphic around the origin and on $\mathbb{C}\backslash\Lambda$; therefore it must be holomorphic everywhere (by periodicity), and so is identically constant since it's elliptic. By noting the constant terms in the Laurent series, evaluating at the origin gives $f(0) = -g_3 + g_3 = 0$, implying the result.

3. Let $w_3 = w_1 + w_2$; each w_i is distinct since w_1, w_2 is $\mathbb{R}$-independent. Since $\wp'$ is odd and periodic we have

$$\wp'\left(\frac{w_i}{2}\right) = -\wp'\left(-\frac{w_i}{2}\right) = -\wp'\left(\frac{w_i}{2}\right) \Longrightarrow \wp'\left(\frac{w_i}{2}\right) = 0,$$

hence each $\wp'\left(\frac{w_i}{2}\right)$ is a root of $4x^3 - g_2x - g_3$; it remains to show that they are distinct. Consider the elliptic function $g_i(z) = \wp(z) - \wp\left(\frac{w_i}{2}\right)$. Since $\wp$ is even and has a double zero at each lattice point and no other zeros, $g_i(w)$ has $\frac{w_i}{2}$ as a double zero and no other zeros, implying each $\wp\left(\frac{w_i}{2}\right)$ is distinct since $\frac{w_i}{2} \neq \frac{w_j}{2} \mod \Lambda \; \forall i \neq j$.

□

7 Elliptic Curves as Complex Tori

We see that $y^2 = 4x^3 - g_2x - g_3$ is always an elliptic curve since it has non-zero discriminant. Now we can show the first direction of the desired equivalence.

Theorem 8. *Let $E(\mathbb{C})$ be the elliptic curve*

$$y^2 = 4x^3 - g_2x - g_3;$$

then the map

$$\phi : \mathbb{C}/\Lambda \to E(\mathbb{C})$$

given by

$$z \mapsto \begin{cases} (\wp(z), \wp'(z)) & z \neq 0 \ mod\ \Lambda \\ O & z = 0 \ mod\ \Lambda. \end{cases}$$

is a group isomorphism.

Proof. Note that the map makes sense since we already proved $\wp'^2 = 4\wp^3 - g_2\wp - g_3$. Suppose $z_1, z_2 \in \mathbb{C}/\Lambda$ and let $x + ay = b$ be the line between $(\wp(z_1), \wp'(z_1))$ and $(\wp(z_2), \wp'(z_2))$ such that

$$\wp(z_1) + a\wp'(z_1) = b$$

$$\wp(z_2) + a\wp'(z_2) = b.$$

The function $\wp(a) + a\wp'(z) - b$ has a triple pole at the origin and no other poles mod Λ. By proposition 8 we know that $\sum \mathrm{ord}_w(f)w = 0 \mod \Lambda$, hence z_1, z_2 being simple zeros implies the only other zero is $-z_1 - z_2$. Thus, the point

$$(\wp(z_1 + z_2), -\wp'(z_1 + z_2)) = (\wp(-z_1 - z_2), \wp'(-z_1 - z_2))$$

is collinear with $(\wp(z_1), \wp'(z_1)), (\wp(z_2), \wp'(z_2))$, since all three being on the line $x + ay - b = 0$. Therefore

$$\begin{aligned}\phi(z_1 + z_2) &= (\wp(z_1 + z_2), \wp'(z_1 + z_2)) = (\wp(z_1), \wp'(z_1)) + (\wp(z_2), \wp'(z_2)) \\ &= \phi(z_1) + \phi(z_2)\end{aligned}$$

For surjectivity, let $(x, y) \in E(\mathbb{C})$. The elliptic function $\wp(z) - x$ is non-constant and so has a zero, say $z = a$. It follows that $\wp'(a)^2 = y^2$ and by replacing a with $-a$ if need be, and noting that $\wp$ is even and $\wp'$ is odd, we obtain $\wp'(a) = y$. Therefore, $\phi(a) = (x, y)$.

Finally, suppose $\phi(z_1) = (\wp(z_1), \wp'(z_1)) = (\wp(z_2), \wp'(z_2)) = \phi(z_2)$. The function $\wp(z) - \wp(z_1)$ has a pole of order 2 and so can only have two other zeros mod Λ counting multiplicity. It vanishes at $z_1, -z_1$ and z_2 so two of these must be congruent. Suppose $2z_1 \notin \Lambda$ so that $z_1 \neq -z_1 \bmod \Lambda$ and $z_2 = \pm z_1 \bmod \Lambda$. Then

$$\wp'(z_1) = \wp'(z_2) = \wp'(\pm z_1) = \pm \wp'(z_1)$$

implies either $z_2 = z_1 \bmod \Lambda$ or $\wp'(z_1) = 0$. However from the proof of proposition 10, we know that the only zeros of $\wp'$ are $\frac{w_i}{2}$, so if $\wp'(z_1) = 0$ then we must have $2z_1 \in \Lambda$, a contradiction. Hence in this case $z_1 = z_2 \bmod \Lambda$. If $2z_1 \in \Lambda$ then $\wp(z) - \wp(z_1)$ has a double zero at z_1; as above it can only have two zeros counting multiplicity, so we must have $z_1 = z_2 \bmod \Lambda$. This completes the proof.

□

Remark. *This gives a cleaner proof of associativity for the group law on $E(\mathbb{C})$. We can also see that, by pulling back the group law onto the elliptic curve, requiring the addition of two points to be the reflection through the x-axis of the third intersection point follows from the fact that the derivative of the Weierstrass function is odd.*

We have proved that there is a well defined mapping

$$\{\text{Complex Tori}\} \longrightarrow \{\text{Elliptic Curves over } \mathbb{C}\}.$$

All that remains is to prove that this map is in fact surjective. To this end we introduce a very special function on the set of lattices called the *j-invariant* given by

$$j(\Lambda) = \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2} = \frac{g_2(\Lambda)^3}{\Delta(\Lambda)},$$

where we are also considering g_2, g_3 as functions with lattices as arguments. Note that lattices are entirely determined by their periods, so we may instead consider these functions as acting on the set of complex periods. Inspecting the

Eisenstein series, we see that g_2 and g_3 are homogeneous of degree -4 and -6 respectively; that is

$$g_2(\lambda w_1, \lambda w_2) = \lambda^{-4} g_2(w_1, w_2) \text{ and } g_3(\lambda w_1, \lambda w_2) = \lambda^{-6} g_3(w_1, w_2)$$

for all $\lambda \neq 0$. It easily follows that $j(\lambda w_1, \lambda w_2) = j(w_1, w_2)$. Writing $\lambda = \frac{1}{w_1}$ and $\tau = \frac{w_2}{w_1}$ we obtain

$$j(1, \tau) = j(w_1, w_2);$$

hence, j is a function of τ only, and we may rewrite $j(\tau) = j(1, \tau)$. Since w_1, w_2 are $\mathbb{R}$-independent if and only if $\frac{w_2}{w_1}$ is non-real, and j is invariant under reflection about the real axis, we may consider j as a function of the upper-half plane.

Before we continue, we note that

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

has a quotient group

$$\mathrm{SL}_2(\mathbb{Z})/\{\pm 1\} = \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \ : \ a, b, c, d \in \mathbb{Z} \text{ and } ad - bc = 1 \};$$

such elements in this quotient are called *unimodular*.

Proposition 11. *1. $j(\tau)$ is invariant under the action of the group $SL_2(\mathbb{Z})/\{\pm 1\}$.*

2. $j(\tau)$ is analytic in the upper-half plane

Proof. 1. Two lattices with bases $\alpha = \left(\begin{smallmatrix} \alpha_1 \\ \alpha_2 \end{smallmatrix}\right)$ and $\omega = \left(\begin{smallmatrix} \omega_1 \\ \omega_2 \end{smallmatrix}\right)$ respectively are equivalent if and only if $\alpha = U\omega$ for some unimodular matrix $U \in SL_2(\mathbb{Z})$.

To show this, suppose first that $\alpha = A\omega$ with A unimodular; then A^{-1} is also unimodular. Both A and A^{-1} then have integer entries, so α_1 and α_2 are linear integral combinations of ω_1 and ω_2 and so all of their linear integral combinations are elements of Λ_1. The same argument with A^{-1} shows that all linear integral combinations of ω_1 and ω_2 are elements of Λ_2, and so $\Lambda_1 = \Lambda_2$.

Conversely, suppose that Λ_1 and Λ_2 are equivalent; then $\alpha_1, \alpha_2 \in \Lambda_2$ and $\omega_1, \omega_2 \in \Lambda_1$ so

$$\alpha = A\omega, \text{ and } \omega = B\alpha$$

where A and B are integer matrices. This implies $\alpha = AB\alpha$ or equivalently $(AB - I)\alpha = 0$; but α_1 and α_2 are $\mathbb{R}$-independent by definition, so we must have $AB = I$. Therefore $\det A \det B = 1$, which implies $\det A = \pm 1$ and $\det B = \pm 1$ since they have integer entries.

All that remains to be shown is that the domain remains in the upper half plane under the action of a unimodular matrix; but this is obvious, since if $U \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ with $ad - bc = 1$ then

$$\mathrm{Im}\ U\tau = \mathrm{Im}\ \frac{a\tau + b}{c\tau + d} = \frac{ad - bc}{|c\tau + d|^2} \mathrm{Im}\ \tau = \frac{\mathrm{Im}\ \tau}{|c\tau + d|^2} > 0.$$

2. Since we have already shown that $\Delta = g_2^3 - 27g_3^2$ is always non-zero, we need only show that $g_2(\tau)$ and $g_3(\tau)$ are both analytic in the upper-half plane. Both are given by series of the form

$$\sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} \frac{1}{(m+n\tau)^{\alpha}},$$

where $\alpha > 0$. We know from above that this series converges for fixed τ. We shall prove that in each strip of the form

$$S = \{x + iy \ : \ |x| \leq A, \ y \geq \delta\},$$

where $A, \delta > 0$, we have uniform convergence, from which the assertion that the series are analytic on the open upper-half plane follows. To do this prove this we will give an $M > 0$ depending on A and δ such that

$$\frac{1}{|m+n\tau|^{\alpha}} \leq \frac{M}{|m+ni|^{\alpha}}$$

for $\tau \in S$ and $(m,n) \neq (0,0)$. This in turn will follow if

$$|m+n\tau|^2 > M|m+ni|^2,$$

or

$$(m+nx)^2 + (ny)^2 > M(m^2+n^2)$$

if $\tau = x + iy$. For $n = 0$, any M such that $0 < M < 1$ will do. If $n \neq 0$, put $q = \frac{m}{n}$, then this is equivalent to

$$\frac{(q+x)^2 + y^2}{1+q^2} > M.$$

Now, set

$$M = \frac{\delta}{1+(a+\delta)^2}.$$

If $|q| \leq A + \delta$ then since $(q+x)^2 \geq 0$ and $y \geq \delta^2$ we have

$$\frac{(q+x)^2 + y^2}{1+q^2} > \frac{\delta}{1+(A+\delta)^2} = M.$$

If $|q| > A + \delta$ then $|\frac{x}{q}| < \frac{|x|}{A+\delta} \leq \frac{A}{A+\delta} < 1$ so

$$\left|1 + \frac{x}{q}\right| \geq 1 - \left|\frac{x}{q}\right| > 1 - \frac{A}{A+\delta} = \frac{\delta}{A+\delta}$$

hence

$$|q+x| \geq \frac{q\delta}{A+\delta}$$

and

$$\frac{(q+x)^2+y^2}{1+q^2} > \frac{\delta^2}{(A+\delta)^2}\frac{q^2}{1+q^2}.$$

Now $\frac{q^2}{1+q^2}$ is increasing as a function of q^2 so

$$\frac{q^2}{1+q^2} \geq \frac{(A+\delta)^2}{1+(A+\delta)^2} > M$$

when $q^2 > (A+\delta)^2$. This is what was required to prove.

□

There is quite a lot that can be said about this function, but for our purposes we need only prove that it takes every complex value; hence we take a more direct approach than what is usually taken.

The first crucial insight is that since j is invariant under unimodular transformations we have that

$$j(\tau) = j(\tau+1) = j\left(\frac{-1}{\tau}\right)$$

so that we may restrict j to a 'fundamental domain' in the same way we have done for elliptic functions. To that end, we consider the set

$$\mathfrak{H} = \{z \in \mathbb{C} \ : \ -\frac{1}{2} < \Re(z) < \frac{1}{2},\ |z| > 1,\ \Im(z) > 0\}$$

and note that by the property of j above this accounts for all τ in the upper-half plane.

The second insight is that after a change variable $q = e^{2\pi i\tau}$ we may write $j(\tau) = \frac{1}{q} + h(q)$ where h is holomorphic. This requires a detailed proof, however.

Lemma 1. *If τ is in the upper-half plane and $n > 0$ then*

$$\sum_{m=-\infty}^{+\infty} \frac{1}{(m+n\tau)^4} = \frac{8\pi^4}{3}\sum_{r=1}^{\infty} r^3 q^{rn}$$

and

$$\sum_{m=-\infty}^{+\infty} \frac{1}{(m+n\tau)^6} = -\frac{8\pi^6}{15}\sum_{r=1}^{\infty} r^5 q^{rn},$$

where $q = e^{2\pi i\tau}$.

Proof. First note the partial fraction decomposition of the cotangent is

$$\pi\cot\pi\tau = \frac{1}{\tau} + \sum_{\substack{m=-\infty \\ m\neq 0}}^{+\infty}\left(\frac{1}{\tau+m} - \frac{1}{m}\right).$$

However, if $q = e^{2\pi i\tau}$ then $|q| < 1$ and

$$\pi \cot \pi\tau = \pi \frac{\cos \pi\tau}{\sin \pi\tau} = \pi i \frac{e^{2\pi i\tau} + 1}{e^{2\pi i\tau} - 1} = \pi i \frac{q+1}{q-1} = -\pi i \left(\frac{q}{1-q} + \frac{1}{1-q} \right)$$
$$= -\pi i \left(\sum_{r=1}^{\infty} q^r + \sum_{r=0}^{\infty} q^r \right) = -\pi i \left(1 + 2 \sum_{r=1}^{\infty} q^r \right).$$

Hence, we have

$$\frac{1}{\tau} + \sum_{\substack{m=-\infty \\ m\neq 0}}^{+\infty} \left(\frac{1}{\tau + m} - \frac{1}{m} \right) = -\pi i \left(1 + 2 \sum_{r=1}^{\infty} q^r \right)$$

and so differentiating repeatedly we obtain

$$-\frac{1}{\tau^2} - \sum_{\substack{m=-\infty \\ m\neq 0}}^{+\infty} \frac{1}{(\tau + m)^2} = -(2\pi i)^2 \sum_{r=1}^{\infty} r q^r,$$

$$-3! \sum_{m=-\infty}^{+\infty} \frac{1}{(\tau + m)^4} = -(2\pi i)^4 \sum_{r=1}^{\infty} r^3 q^r$$

and

$$-5! \sum_{m=-\infty}^{+\infty} \frac{1}{(\tau + m)^6} = -(2\pi i)^6 \sum_{r=1}^{\infty} r^5 q^r.$$

Replacing τ by $n\tau$ gives us the desired result. □

Theorem 9. *If τ is in the upper-half plane then*

1. $$g_2(q) = \frac{4\pi^4}{3} \left(1 + 240 \sum_{k=1}^{\infty} p_3(k) q^k \right)$$

2. $$g_3(q) = \frac{8\pi^6}{27} \left(1 - 504 \sum_{k=1}^{\infty} p_5(k) q^k \right)$$

3. $$\Delta(q) = (2\pi)^{12} \sum_{n=1}^{\infty} \tau(n) q^n,$$

where $p_i(k) = \sum_{d|k} d^i$ and $\tau(n)$ are integers.

Proof. 1. We have

$$\begin{aligned} g_2(\tau) &= 60 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} \frac{1}{(m+n\tau)^4} \\ &= 60 \sum_{\substack{m,n=-\infty \\ m\neq 0}}^{\infty} \frac{1}{m^4} + 60 \sum_{n=1}^{\infty} \sum_{m=-\infty}^{+\infty} \left(\frac{1}{(m+n\tau)^4} + \frac{1}{(m-n\tau)^4} \right) \\ &= 60 \left(2\zeta(4) + 2 \sum_{n=1}^{\infty} \sum_{m=-\infty}^{+\infty} \frac{1}{(m+n\tau)^4} \right) \\ &= 60 \left(\frac{2\pi^4}{90} + \frac{16\pi^4}{3} \sum_{n=1}^{\infty} \sum_{r=1}^{\infty} r^3 q^{nr} \right). \end{aligned}$$

In the last line we obtain the required expression after collecting together terms in the last double sum in which nr is constant.

2. The form for g_3 is similarly derived as aboved.

3. Note that the sums involving $p_i(k)$ are polynomials with integer coefficients since $p_i(k) \neq 0$ for only finitely many k. If we put

$$A = \sum_{n=1}^{\infty} p_3(n) q^n \text{ and } B = \sum_{n=1}^{\infty} p_5(n) q^n,$$

then by above

$$\Delta(q) = g_2(q)^3 - 27 g_3(q)^2 = \frac{64\pi^{12}}{12}((1+240A)^3 - (1-504B)^2).$$

We can rewrite

$$(1+240A)^3 - (1-504B)^2 = 12^2(5A+7B+12^3(100A^2 - 147B^2 + 8000A^3));$$

but since $5A + 7B = \sum_{n=1}^{\infty}(5p_3(n) + 7p_5(n))q^n$ and

$$\begin{aligned} 5d^3 + 7d^5 = d^3(5+7d^2) &\equiv d^3(d^2-1) \equiv 0 \bmod 3 \\ &\equiv d^3(1-d^2) \equiv 0 \bmod 4 \\ \implies \quad 5d^3 + 7d^5 &\equiv 0 \bmod 12, \end{aligned}$$

we have that 12^3 is a factor in each coefficient of the polynomials $(1+240A)^3 - (1-504B)^2$. Therefore

$$\Delta(q) = \frac{64\pi^{12}}{27} \left(12^3 \sum_{n=1}^{\infty} \tau(n) q^n \right) = (2\pi)^{12} \sum_{n=1}^{\infty} \tau(n) q^n$$

where $\tau(n)$ are integers

□

Corollary. *After the change of variable $q = e^{2\pi i\tau}$ the j invariant may be written as*

$$12^3 j(q) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c(n)q^n$$

where $c(n)$ are integers.

Proof. Let S denote any power series in q with integer coefficients, then

$$g_2(q)^3 = \frac{64}{27}\pi^{12}(1 + 240q + S)^3 = \frac{64}{27}\pi^{12}(1 + 720q + S), \text{ and}$$

$$\Delta(q) = \frac{64}{27}\pi^{12}(12^3 q(1 - 24q + S));$$

and so we have

$$j(q) = \frac{g_2(q)^3}{\Delta(q)} = \frac{1}{12^3 q}(1 + 720q + S)(1 + 24q + S),$$

implying the result. □

Now we can show the j-invariant is surjective.

Theorem 10. *The j-invariant takes on every complex value on the set*

$$\mathfrak{H} = \{z \in \mathbb{C} \ : \ -\frac{1}{2} < \Re(z) < \frac{1}{2}, \ |z| > 1, \ \Im(z) > 0\}.$$

Proof. Let $h > 0$ and

$$F_h = \{z \in \mathbb{C} \ : \ -\frac{1}{2} < \Re(z) < \frac{1}{2}, \ |z| > 1, \ \Im(z) > h\} \subset \mathfrak{H},$$

where we let its boundary ∂F_h have counter-clockwise orientation. Suppose $j(\tau) \neq j_0$ for all $\tau \in \mathfrak{H}$; then by the argument principle

$$\frac{1}{2\pi i}\int_{\partial F_h} \frac{j'(\tau)}{j(\tau) - j_0} d\tau = 0.$$

Let us calculate this a different way. Write $\partial F_h = A \cup B \cup C \cup D \cup E$ where

$$A = \partial F_h \cap \{\tau \in \mathbb{C} \ : \ \Re(\tau) = \tfrac{1}{2}\}$$

$$B = \partial F_h \cap \{\tau \in \mathbb{C} \ : \ \Re(\tau) = -\tfrac{1}{2}\}$$

$$C = \partial F_h \cap \{\tau \in \mathbb{C} \ : \ \Im(\tau) = h\}$$

$$D = \partial F_h \cap \{\tau \in \mathbb{C} \ : \ |\tau| = 1 \text{ and } \Re(\tau) \leq 0\}$$

$$E = \partial F_h \cap \{\tau \in \mathbb{C} \ : \ |\tau| = 1 \text{ and } \Re(\tau) > 0\}$$

so that this is a disjoint union. The integration along A and B cancel by opposing orientation; while the same happens for D and E since the identity $j(\tau) = j(-\frac{1}{\tau})$ transforms E into D with the opposite orientation. Now considering C, we have by the expansion proved previously

$$\frac{1}{2\pi i}\int_C \frac{j'(\tau)}{j(\tau)-j_0}d\tau = \frac{1}{2\pi i(12)^3}\int_{|q|=h} \frac{-\frac{2\pi i}{q} + 2\pi i q f'(q)}{\frac{1}{q} + f(q) - j_0}\frac{dq}{2\pi i q}$$

$$= \frac{1}{2\pi i(12)^3}\int_{|q|=h} -\frac{1}{q} + \tilde{f}(q)dq,$$

where f and $\tilde{f}$ are holomorphic. However, since $\tilde{f} \sim O(1)$, if we take limits we see that

$$\lim_{h\to 0} \frac{1}{2\pi i(12)^3}\int_{|q|=h} -\frac{1}{q} + \tilde{f}(q)dq = \frac{1}{12^3}$$

while the original integral remains 0. This is a contradiction and so we must have surjectivity. □

So we are associating complex tori with elliptic curves as groups by

$$\mathbb{C}/\Lambda \mapsto y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda).$$

The next theorem shows us that we can find such a Λ for any elliptic curve.

Theorem 11. *Given two complex numbers $a_2, a_3 \in \mathbb{C}$ such that $a_2^3 - 27a_3^2 \neq 0$ there exists $w_1, w_2 \in \mathbb{C}$ whose ratio is non-real such that*

$$g_2(w_1, w_2) = a_2, \text{ and } g_3(w_1, w_2) = a_3.$$

Proof. We have three cases:

1. Suppose $a_2 = 0$; then we necessarily have $a_3 \neq 0$. Let $\rho = e^{\frac{2\pi i}{3}}$,

$$w_1^6 = \frac{g_3(1,\rho)}{a_3}, \text{ and } w_2 = \rho w_1.$$

We have $g_2(1,\rho)=0$ since

$$\begin{aligned}\frac{1}{60}g_2(1,\rho) &= \sum_{\substack{m,n=-\infty\\(m,n)\neq(0,0)}}^{\infty}\frac{1}{(m+n\rho)^4} = \sum_{\substack{m,n=-\infty\\(m,n)\neq(0,0)}}^{\infty}\frac{1}{(m\rho^3+n\rho)^4}\\ &= \frac{1}{\rho^4}\sum_{\substack{m,n=-\infty\\(m,n)\neq(0,0)}}^{\infty}\frac{1}{(m\rho^2+n)^4}\\ &= \frac{1}{\rho^4}\sum_{\substack{m,n=-\infty\\(m,n)\neq(0,0)}}^{\infty}\frac{1}{(n-m-m\rho)^4},\ \text{since } \rho^2+\rho+1=0\\ &= \frac{1}{\rho^4}\sum_{\substack{m',n'=-\infty\\(m',n')\neq(0,0)}}^{\infty}\frac{1}{(m'+n'\rho)^4} = \frac{1}{60\rho^4}g_2(1,\rho);\end{aligned}$$

but then $g_3(1,\rho)\neq 0$ for otherwise $a_2^3-27a_3^2=0$. Therefore, we must have w_1 defined above and $\frac{w_2}{w_1}$ non-real; hence

$$g_2(w_1,w_2)=g_2(w_1,\rho w_1)=\frac{1}{w_1^4}g_2(1,\rho)=0=a_2,$$

$$\text{and } g_2(w_1,w_2)=g_2(w_1,\rho w_1)=\frac{1}{w_1^6}g_3(1,\rho)=a_3.$$

2. Suppose $a_3=0$ so that $a_3\neq 0$. Let

$$w_1^4=\frac{g_2(1,i)}{a_3},\ \text{and } w_2=iw_1.$$

Similarly to above, we have $g_3(1,i)=0$ since

$$\begin{aligned}\frac{1}{140}g(1,i) &= \frac{1}{140i^6}\sum_{\substack{m,n=-\infty\\(m,n)\neq(0,0)}}^{\infty}\frac{1}{(m+ni)^6} = \frac{1}{140i^6}\sum_{\substack{m,n=-\infty\\(m,n)\neq(0,0)}}^{\infty}\frac{1}{(mi^3+n)^6}\\ &= \frac{1}{140i^6}\sum_{\substack{m,n=-\infty\\(m,n)\neq(0,0)}}^{\infty}\frac{1}{(-mi+n)^6} = -\frac{1}{140}g_3(1,i).\end{aligned}$$

Therefore,

$$g_2(w_1,w_2)=g_2(w_1,iw_1)=\frac{1}{w_1^4}g_2(1,i)=a_2,$$

$$\text{and } g_3(w_1,w_2)=g_3(w_1,iw_1)=\frac{1}{w_1^6}g_3(1,i)=0=a_3.$$

3. Finally, suppose $a_2 a_3 \neq 0$. Choose τ such that

$$j(1,\tau) = \frac{a_2^3}{a_2^3 - 27a_3^2};$$

then $j(1,\tau) \neq 0$ since $a_2 \neq 0$ implying $g_2(1,\tau) \neq 0$. Now, put

$$w_1^2 = \frac{a_3}{a_2}\frac{g_3(1,\tau)}{g_2(1,\tau)}, \text{ and } w_2 = \tau w_1;$$

then we have

$$\frac{g_2(w_1,w_2)}{g_3(w_1,w_2)} = w_1^2 \frac{g_2(1,\tau)}{g_3(1,\tau)} = \frac{a_2}{a_3},$$

which implies

$$g_3(w_1,w_2) = \frac{a_3}{a_2} g_2(w_1,w_2).$$

Therefore, if we write

$$\frac{27a_3^2}{a_2^3} = \frac{27g_3(w_1,w_2)^2}{g_2(w_1,w_2)^3} = \frac{27a_3^2}{a_2^2 g_2(w_1,w_2)}$$

we obtain $g_2(w_1,w_2) = a_2$ which further implies $g_3(w_1,w_2) = a_3$, as desired.

□

Corollary. *Let $E(\mathbb{C})$ be the elliptic curve over $\mathbb{C}$ given by*

$$E \ : \ y^2 = x^3 - \alpha x - \beta;$$

then there exists a lattice $\Lambda \subset \mathbb{C}$ such that there is a group isomorphism

$$\phi : \mathbb{C}/\Lambda \to E(\mathbb{C}).$$

Proof. Since E is non-zero, $\alpha_2^3 - 27\beta a_3^2 \neq 0$. By above here exists w_1, w_2 that span a lattice over $\mathbb{C}$ such that $g_2(w_1,w_2) = \sqrt[3]{4}\alpha$ and $g_3(w_1,w_2) = \beta$. By Theorem 7 we have a group isomorphism

$$\mathbb{C}/\Lambda \xrightarrow{\sim} E'(\mathbb{C})$$

where

$$E' \ : \ y^2 = 4x^3 - \sqrt[3]{4}\alpha x - \beta;$$

but then $E'(\mathbb{C}) \cong E(\mathbb{C})$ by the change of $x \mapsto \frac{x}{\sqrt[3]{4}}$. □

8 Properties of the Group Law

In this section we exploit our understanding of complex tori to derive geometric statements about elliptic curves.

Proposition 12. *Let E be an elliptic curve over $\mathbb{C}$; we have*

$$E(\mathbb{C})^{\text{tors}} \cong \mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}.$$

Proof. Since $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ we have

$$E(\mathbb{C})^{\text{tors}} \cong \mathbb{C}/\Lambda^{\text{tors}} \cong (\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z})^{\text{tors}} \cong (\mathbb{R}/\mathbb{Z})^{\text{tors}} \times (\mathbb{R}/\mathbb{Z})^{\text{tors}} \cong \mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}.$$

□

Proposition 13. *The group law on a elliptic curve $E(\mathbb{C})$ is divisible: given $p \in E(\mathbb{C})$ and any integer $n \geq 1$ there exists $q \in E(\mathbb{C})$ such that*

$$nq := \underbrace{q + \ldots + q}_{n \text{ times}} = p.$$

In fact, there are n^2 such points

Proof. Let $\Lambda \subset \mathbb{C}$ be a lattice such that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$. Suppose $p \in \mathbb{C}/\Lambda$ and $n \geq 1$ is given. Write $p = \lambda_1 w_1 + \lambda_2 w_2 + \Lambda$ where $\lambda_1, \lambda_2 \in [0, 1)$ is unique (i.e. using the projection $D \to C/\Lambda$ for the representation, where D is a fundamental parallelogram). For any integers $k_1, k_2 \in [0, n-1]$ write

$$p_{k_1,k_2} = \frac{k_1 + \lambda_1}{n} w_1 + \frac{k_2 + \lambda_2}{n} w_1 + \Lambda.$$

It is clear then that $np_{k_1,k_2} = q$. There are n^2 of them because they are distinct. To see this, suppose

$$\frac{k_1 + \lambda_1}{n} w_1 + \frac{k_2 + \lambda_2}{n} w_1 + \Lambda = \frac{k_1' + \lambda_1}{n} w_1 + \frac{k_2' + \lambda_2}{n} w_1 + \Lambda;$$

then

$$\frac{k_1 - k_1'}{n} w_1 + \frac{k_2 + k_2'}{n} w_1 = m_1 w_1 + m_2 w_2$$

where $m_1, m_2 \in \mathbb{Z}$, which implies $\frac{k_i - k_i'}{n} = m_i$ by linear independence of w_1 and w_2. Hence, $k_i = k_i'$ since $k_i, k_i' \in [0, n-1]$. To see that these are all such points, suppose $nq = p$ and write $q = a_1 w_1 + a_2 w_2 + \Lambda$.We have

$$na_1 w_1 + na_2 w_2 + \Lambda = \lambda_1 w_1 + \lambda_2 w_2 + \Lambda,$$

which means there are integers m_1, m_2 such that

$$(na_1 - \lambda_1) w_1 + (na_2 - \lambda_2) w_2 = m_1 w_1 + m_2 w_2.$$

Again, by linear independence we have $na_i - \lambda_i = m_i$, which gives $a_i = \frac{m_i+\lambda_i}{n}$. Therefore,

$$q = \frac{k_1 + \lambda_1}{n} w_1 + \frac{k_2 + \lambda_2}{n} w_2 + \Lambda$$

where $k_i \equiv m_i$ with $k_i \in [0, n-1]$. □

Corollary. *For any integer $m \geq 1$ let $E(\mathbb{C})[m]$ be the m-torsion subgroup of $E(\mathbb{C})$; then*

$$E(\mathbb{C})[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

Proof. If we consider the points $q \in \mathbb{C}/\Lambda$ such that $mq = 0$, then by above we see that the defined points p_{k_1,k_2}, when seen as in the m-torsion subgroup, are isomorphic to $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ as

$$\mathbb{C}/\Lambda[m] \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}), \ \frac{k_1 + \lambda_1}{m} w_1 + \frac{k_2 + \lambda_2}{m} w_1 + \Lambda \mapsto (k_1, k_2).$$

This immediately implies the result. □

We can get a better view of this by considering the subgroup $E(\mathbb{R})$ in the case that α and β are real. By above, $E(\mathbb{R})[m] \subset E(\mathbb{C})[m]$ is always finite. The group of 2-torsion points in this case are easily discernible. If $P = (x_p, y_p)$ then $2P = O$ implies that the tangent line to P is parallel to the y-axis; and since $y^2 = x^3 - \alpha x - \beta$ is symmetric about the y-axis, the 2-torsion points are exactly the points at which $y_p = 0$, or $x_p^3 - \alpha x_p - \beta = 0$. There are three such points (not counting the identity element) when $\Delta < 0$ and only one when $\Delta > 0$.

The group $E(\mathbb{R})[3]$ is more tricky. We have the following result.

Proposition 14. *A point $P \in E(\mathbb{C})$ has $3P = O$ if and only if P is an inflection point on the elliptic curve $y^2 = x^3 - \alpha x - \beta$.*

Proof. Let $x(Q)$ denote the x-coordinate for any point Q on the elliptic curve E; then since E is symmetric about the y-axis we have that $2P = -P$ implies $x(2P) = x(-P) = x(P)$. Conversely if $P \neq O$ has $x(2P) = x(P)$ then $2P = \pm P$ implies $3P = 0$. So P is a 3-torsion point if and only if $x(2P) = x(P)$. Using the addition formula we derived earlier, this is equivalent to

$$\psi(x) = 3x^4 - 6\alpha x^2 - 12\beta x - \alpha^2 = 0.$$

Now, going through the algebra, putting $f(x) = x^3 - \alpha x - \beta$ we have

$$\frac{d^2y}{dx^2} = \frac{2f''(x)f(x) - f'(x)^2}{4yf(x)} = \frac{\psi(x)}{4yf(x)}.$$

By definition of an inflection point, we must have then that $\psi(x(P))) = 0$ exactly when P is a point of inflection and vice versa. □

Corollary. *Suppose $y^2 = f(x) = x^3 - \alpha x - \beta$ has $\alpha, \beta \in \mathbb{R}$, then there are exactly two flex points in $E(\mathbb{R})$ (not counting O).*

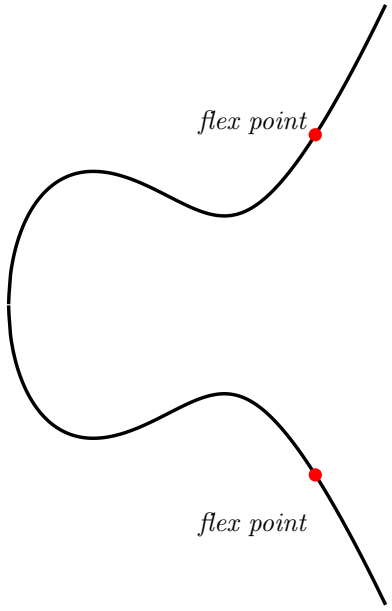
Proof. By above the flex points are exactly those that satisfy $\psi(x) = 3x^4 - 6\alpha x^2 - 12\beta x - \alpha^2 = 0$. Note that a monic quartic polynomial has exactly two real roots if it is negative on the zeroes of its derivative. We have that

$$\psi'(x) = 12f(x) = 12x^3 - 12\alpha x - 12\beta;$$

but

$$\psi(x) = 2f''(x)f(x) - f'(x)^2$$

implies $\psi(x_0) < 0$ when $f(x_0) = 0$ and x_0 is a flex point (so $f'(x_0) \neq 0$). The result follows. □



Assuming the reader knows some Galois theory, we can finish with the following. When $\alpha, \beta \in \mathbb{Q}$, this gives a stringent requirement on all torsion points on an elliptic curve.

Lemma. *Suppose*

$$E: \ y^2 = x^3 - \alpha x - \beta$$

where $\alpha, \beta \in \mathbb{Q}$ and K a Galois extension of $\mathbb{Q}$. For $P = (x, y) \in E(K)$, define $\sigma(P) = (\sigma(x), \sigma(y))$ where $\sigma \in Gal(K/\mathbb{Q})$; then P having order n implies that $\sigma(P)$ has order n.

Proof. Note that this makes sense since

$$y^2 = x^3 - \alpha x - \beta \implies \sigma(y)^2 = \sigma(x)^3 - \alpha\sigma(x) - \beta.$$

Since the addition of coordinates is done by rational combinations, it easily follows that

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

for all $P, Q \in E(K)$; in particular $\sigma(nP) = n\sigma(P)$. Let m be the order of $\sigma(P)$; then $n\sigma(P) = \sigma(nP) = O$ which implies m divides n. However, $O = m\sigma(P) = \sigma(mP)$ implies $O = \sigma^{-1}(\sigma(mP)) = mP$ and so n divides m. Hence $m = n$. □

Theorem 12. *Suppose*

$$E: \ y^2 = x^3 - \alpha x - \beta$$

where $\alpha, \beta \in \mathbb{Q}$ *and let*

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

then

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

is a Galois extension of $\mathbb{Q}$.

Proof. Let $\sigma : K \to \mathbb{C}$ be a field homomorphism. We must verify that $\sigma(K) = K$, for K to be a Galois extension over $\mathbb{Q}$. By above, if $P \in E(\mathbb{C})[n]$, then $\sigma(P) \in E(\mathbb{C})[n]$, and so $\sigma(K) \subset K$. □

Corollary. *Every torsion point of*

$$E: \ y^2 = x^3 - \alpha x - \beta$$

where $\alpha, \beta \in \mathbb{Q}$ *has coordinates that are algebraic over* $\mathbb{Q}$.

Proof. By the same argument as above, there are finitely many field homomorphisms $\sigma : K \to \mathbb{C}$. But if any x_i or y_i was not algebraic over $\mathbb{Q}$, then K would have infinite degree over $\mathbb{Q}$, and so would have infinitely many such homomorphisms. The result follows □

Acknowledgements

I would like to thank my supervisor Mr. Nicolas Mascot for his suggestion of the topic, his continual guidance, and his helpful insights throughout the year, without which this project would not have been possible.

A Hilbert's Nullstellensatz

In this section we show the equivalence the between polynomials and algebraic curves in our discussions. In fact we prove a more general theorem, famously known as *Hilbert's Nullstellensatz* from which our special case is an easy deduction.

We presuppose the reader is acquainted with the algebraic objects studied in basic algebra such as fields, rings, modules etc. and understands their basic properties such as when they are finitely generated and how some fields are algebraic extensions of other fields. All rings are assumed to be commutative.

Definition. *A Noetherian ring R is a ring in which every ideal I is finitely generated; i.e. there exists $a_1, \ldots, a_n$ in I such that $I = Ra_1 + \ldots + Ra_n$.*

We begin our rapid treatment.

Theorem 13. *(Hilbert's Basis Theorem) If A is a Noetherian ring, then so is $A[x]$.*

Proof. Let $I \subset A[x]$ be an ideal, and for any $f \in I$ let $c(f)$ be its leading coefficient. It is obvious that the set

$$J = \{a \ : \ a = c(f) \text{ for some } f \in I\}$$

is an ideal in A, since each $f_i \in I$ and I is an ideal. Since A is Noetherian, J is finitely generated, say by elements $a_1, \ldots, a_n$. For each i let $f_i \in A[x]$ have leading coefficient a_i; then let $r_i = \deg f_i$, $R = \max_{i=1}^{n} r_i$, and $K = (f_1, \ldots, f_n) \subset I$.

Now, if $f \in I$ has $\deg f \geq R$, we can write $c(f) = \sum_i a_i u_i$ where $u_i \in A[x]$; then

$$f - \sum_i u_i f_i x^{\deg f - r_i}$$

is in I and has degree less than $\deg f$. If we continue in this way, we may reduce our polynomial so that we may write $f = g + h$ where $\deg g < R$ and $h \in K$.

For each $r \leq R$ such that there exists polynomials of degree $r \in I$ let $J_r = \{c(f) : f \in I \text{ of degree } r\} = (a_{r,1}, \ldots, a_{r,n_r})$ and $c(f_{r,i}) = a_{r,i}$. In exactly the same way as before, we may repeatedly use the polynomials $f_{\deg g, i}$ where $i = 1, \ldots, n_r$ to reduce the degree of g at each step until we have $g = 0$; then we have written $f = g + h$ as a finite combination of the f_i and $f_{r,i}$, so these generate I. □

Corollary. *If A is a Noetherian ring and B is a finitely generated A-algebra, then B is Noetherian.*

Proof. Let $a_1, \ldots, a_n$ generate B as an A-algebra. This means that every element of $b \in B$ can be written as a polynomial $b = p(a_1, \ldots, a_n) \in A[a_1, \ldots, a_n]$. Consider then the surjective ring homomorphism

$$\phi : A[x_1, \ldots, x_n] \to B,\ p(x_1, \ldots, x_n) \mapsto p(a_1, \ldots, a_n).$$

Since $A[x_1, \ldots, x_n]$ is Noetherian, any of its quotients is also Noetherian (given $J \subset A/I$, let $a_1 \ldots, a_m$ generate the ring given by $\pi^{-1}(J)$; then $\pi(a_1) \ldots, \pi(a_m)$ generate J). Therefore, $B \cong A[x_1, \ldots, x_n]/(\ker \phi)$ is finitely generated. □

Theorem 14. *(Artin-Tate Lemma) Let $R \subset T \subset S$ be rings such that*

1. *R is Noetherian*
2. *S is finitely generated as an R-algebra, and*
3. *S is finitely generated as a T-module.*

Then T is finitely generated as an R-algebra.

Proof. Let $x_1, \ldots, x_n$ generate S as an R-algebra and $y_1, \ldots, y_m$ generate S as a T-module. For each $1 \leq i \leq n$ write

$$x_i = \sum_{j=1}^{m} a_{ij} y_j,\ a_{ij} \in T.$$

Similarly write

$$y_i y_j = \sum_{k=1}^{m} b_{ijk} y_k,\ b_{ijk} \in T$$

for all $1 \leq i, j \leq m$. Let T_0 be the R-subalgebra of T generated by the a_{ij} and b_{ijk}. By the above corollary it is itself a Noetherian ring. Now since each element of S may be expressed as a polynomial in the x_i's with coefficients in R, making substitutions using the two equations above shows that S is finitely generated T_0-module. Since T_0 is a Noetherian, the submodule T is also finitely generated as a T_0 module (considering T as a subalgebra). This immediately implies T is a finitely generated T_0-algebra, and so it is finitely generated as a R-algebra. □

Now we can prove the main result in which the rest will follow.

Theorem 15. *(Zariski's Lemma) Let k be a field. If $\mathfrak{m}$ is a maximal ideal of $k[t_1, \ldots, t_n]$ then $k[t_1, \ldots, t_n]/\mathfrak{m}$ is a finite field extension of k.*

Proof. It suffices to prove that if K is a field extension of k that is finitely generated as a k-algebra, then K is a finite algebraic extension. This is because an algebra is finitely generated if and only if it is isomorphic to a quotient of a polynomial ring over its base field; and so since $k[t_1, \ldots, t_n]/\mathfrak{m}$ is exactly that, it is finitely generated as a k-algebra, and so would be a finite degree algebraic extension.

Let $K = k[x_1, \ldots, x_n]$ and suppose K was not a finite algebraic extension. Renumber the x_i so that $x_1, \ldots, x_r$ is algebraically independent over k and each $x_{r+1}, \ldots, x_n$ is algebraic over $F = k(x_1, \ldots, x_r)$. Hence K if a finite algebraic extension of F and is finitely generated as a F-module. Applying the Artin-Tate Lemma to the rings $k \subset F \subset K$ shows that F is finitely generated as a k-algebra; hence $F = k[y_1, \ldots, y_s]$ for some y_j. By the definition of F, each y_i is of the form $\frac{f_j}{g_j}$ where $f_j, g_j \in k[x_1, \ldots, x_r]$. There are infinitely many irreducible polynomials in $k[x_1, \ldots, x_r]$ (let $p_1, \ldots, p_m$ be a finite collection of them, then an irreducible factor of $l = p_1 p_2 \cdots p_m + 1$ cannot be any of those in the finite collection). Hence take h to be an irreducible polynomial that does not divide any of the g_j; then the element $h^{-1} \in F = k(x_1, \ldots, x_r)$ cannot be a polynomial in the y_j's. This is a contradiction. Therefore, K is a finite algebraic extension of k. □

Now let's build our definitions.

Definition. *Let k be an algebraically closed field. Consider the polynomial ring $k[x_1, \ldots, x_n]$ and let J be an ideal of this ring.*

1. *The set $V(J)$, called the variety generated by J, is the set of all n-tuples $x = (x_1, \ldots, x_n) \in k^n$ such that $f(x) = 0$ for all $f \in J$.*
2. *We define $I(V(J))$ to be the ideal of all polynomials that vanish on the set $V(J)$.*
3. *We define the set*

$$\sqrt{J} = \{x \in k[x_1, \ldots, x_n] \ : \ x^r \in J, \text{ for some } r \in \mathbb{N}\},$$

called the radical of J.

Note that in general $k[x_1, \ldots, x_n]$ is a UFD, and so if $J \subset k[x_1, \ldots, x_n]$ is generated by a polynomial P that factors as $P = \prod_i P_i^{e_i}$ then $\sqrt{J}$ is generated as an ideal by the polynomial $\prod_i P_i$.

As a simple example of how all of this fits into our discussion, consider the ideal $J = (p)$ where $p \in k[x, y]$. In this case, our definition of an algebraic curve is equivalent to the variety $V(J)$. In this case the Nullstellensatz says that any polynomial $q \in k[x, y]$ that has the same zero set as $V(J)$, that is

a member of the set $I(V(J))$, should just be the product of those irreducible factors with certain multiplicities. This is what we prove in what follows, in greater generality.

Now we may prove the weak Nullstellensatz, from which the general (or 'strong') Nullstellensatz will follow.

Proposition 15. *(Weak Nullstellensatz) If J is a proper ideal of $k[x_1, \ldots, x_n]$ then $V(J) \neq \emptyset$.*

Proof. We may assume J is a maximal ideal, for if $I \subset J$ then $V(J) \subset V(I)$.

Put $R = k[x_1, \ldots, x_n]$ and consider R/J. By Zariski's Lemma, R/J is a finite field extension of k; but k is algebraically closed, so $R/J \cong k$. Hence we have a surjective map

$$\phi : R \xrightarrow{proj.} R/J \xrightarrow{\sim} k.$$

Put $a_i = \phi(x_i)$, then $x_i - a_i \in \ker \phi = J$. Now, let $f \in J$ then $f(a_1, \ldots, a_n) = f(\phi(x_1), \ldots, \phi(x_n)) = \phi(f(x_1, \ldots, x_n)) = 0$, implying $(a_1, \ldots, a_n)$ is a zero of J; therefore $V(J) \neq \emptyset$. □

Theorem 16. *(Hilbert's Nullstellensatz) Let k be an algebraically closed field and $J \subset k[x_1, \ldots, x_n]$ a proper ideal, then*

$$I(V(J)) = \sqrt{J}.$$

Proof. It is clear that $\sqrt{J} \subset I(V(J))$; for if $p \in \sqrt{J}$ then $p^r \in J$ for some r, and so if $x \in V(J)$ is such that $p(x)^r = 0$ then $p(x) = 0$.

Conversely (this is the so-called 'Rabinowitsch trick'), suppose $J \subset k[x_1, \ldots, x_n]$ is a proper ideal and $g \in I(V(J))$. Let $f_1, \ldots, f_m$ generate J (justified since $k[x_1, \ldots, x_n]$ is Noetherian) and consider the ideal $J' \subset k[x_1, \ldots, x_n, x_{n+1}]$ generated by J and the element $1 - x_{n+1}f \in k[x_1, \ldots, x_n, x_{n+1}]$. By construction the polynomials $f_1, \ldots, f_m$ and the polynomial $1 - x_{n+1}g$ have no zeroes in common. By the Weak Nullstellensatz, we must then have $J' = k[x_1, \ldots, x_n, x_{n+1}]$; hence we may write

$$1 = p_1 f_1 + \cdots + p_m f_m + p_{m+1}(1 - x_{n+1}g),$$

where each $p_i \in k[x_1, \ldots, x_n, x_{n+1}]$. Evaluating this expression through the ring homomorphism

$$k[x_1, \ldots, x_n, x_{n+1}] \to k(x_1, \ldots, x_n),\ x_{n+1} \mapsto \frac{1}{g}$$

we obtain

$$1 = p_1(x_1, \ldots, x_n, \frac{1}{g})f_1 + \cdots + p_m(x_1, \ldots, x_n, \frac{1}{g})f_m.$$

After multiplying by a power of g throughout to clear denominators we obtain $g^r \in J$ for some $r \in \mathbb{N}$, implying $I(V(J)) \subset \sqrt{J}$. This proves the theorem. $\square$

Corollary. *If $P, Q \in k[x, y]$ where k is algebraically closed then*

$$\{(x, y) \in k^2 \ : \ P(x, y) = 0\} = \{(x, y) \in k^2 \ : \ Q(x, y) = 0\}$$

if and only if P and Q have the same irreducible factors, possible occurring with different multiplicities.

Proof. Put $I = (P)$ and $T = (Q)$. We have $\sqrt{J} = I(V(J)) = I(V(T)) = \sqrt{T}$, implying $P^r = Q^m$ for some $n, m \in \mathbb{N}$. $\square$

Note that this generalises nicely to the case of homogeneous polynomials defining curves in projective space by considering points in $\mathbb{P}^n(k)$ to be embedded in $\mathbb{A}^{n+1}(k)$ and applying the Nullstellensatz for the $n + 1$ case.

B Homogenous Polynomials

An equivalent definition of a homogenous polynomial P of degree d over a ring R is an element of $R[x_1, \ldots, x_n]$ that can be written in the form

$$P = \sum_{k_1+\ldots+k_n=d} a_{k_1,\ldots k_n} x^{k_1} x^{k_2} \cdots x^{k_n},$$

where each $a_{k_1,\ldots k_n} \in R$.

Proposition. *Every factor of a homogenous polynomial is homogeneous.*

Proof. Let P be a homogeneous polynomial. Omitting the trivial case where P is irreducible, factor $P = QS$ where neither Q or S is constant. Write $Q = U+V$ where only U is homogenous and $\deg V < \deg U = \deg Q$ and similarly with $S = K + L$ and $\deg L < \deg K = \deg S$; then

$$P = (U + V)(K + L) = UK + UL + VK + VL,$$

but $\deg UL + VK + VL = \max\{\deg UL, \deg VK, \deg VL\} < \deg UK = \deg P$ implying $UL + VK + VL = 0$. □

Proposition. *A homogenous polynomial in $k[x, y]$ splits into linear factors $b_i x - c_i y$ where $b, c \in k$.*

Proof. Let $P \in k[x, y]$ be homogenous of degree d; write

$$P(x, y) = \sum_{i=0}^{d} a_i x^i y^{n-i} = y^d \sum_{i=0}^{d} a_i (\frac{x}{y})^i,$$

where at least one a_i is not zero. Let e be the largest element of $\{0, \ldots, d\}$ such that $a_e \neq 0$; then $\sum_{i=0}^{d} a_i (\frac{x}{y})^i$ splits over k as

$$\sum_{i=0}^{d} a_i (\frac{x}{y})^i = a_e \prod_{i=0}^{e} (\frac{x}{y} - \gamma_i).$$

Therefore, P splits over k as

$$P(x, y) = \sum_{i=0}^{d} a_i (\frac{x}{y})^i = a_e y^d \prod_{i=0}^{e} (\frac{x}{y} - \gamma_i) = a_e y^{d-e} \prod_{i=0}^{e} (x - \gamma_i y).$$

□

We cannot strengthen this result to the case of a homogeneous polynomial in more than two variables; otherwise algebraic curves in the projective plane would be a union of lines.

C Projective Transformations

Definition. *A projective transformation is a bijection $f : \mathbb{P}^2(k) \to \mathbb{P}^2(k)$ such that for some linear isomorphism $\alpha : k^{2+1} \to k^{2+1}$ we have $f \circ \Pi = \Pi \circ \alpha$, where $\Pi : k^{2+1} \to \mathbb{P}^2(k)$ is the canonical projection.*

This is a generalisation of a linear change of coordinates. We interchangeably call a projective transformation a change of coordinates throughout the main body of the text.

Proposition. *Given four distinct points p_0, p_1, p_2 and q in $\mathbb{P}^2(k)$, no three of which are are span a subspace of dimension two when viewed as points in k^{2+1}, there exists a projective transformation sending p_0, p_1 and p_2 to $[1:0:0], [0:1:0]$ and $[0:0:1]$, and q to $[1:1:1]$.*

Proof. Let u_0, u_1, u_2 and v be the points p_0, p_1, p_2 and q as they are represented in k^{2+1}. The points u_i are linearly independent, since our original points are distinct in $\mathbb{P}^2(k)$ and are not collinear in k^{2+1}. Therefore, there exists a linear transformation sending them to the standard basis. This defines a projective transformation f sending p_0, p_1 and p_2 to $[1:0:0], [0:1:0]$ and $[0:0:1]$. Moreover, the conditions on our points imply that $q = [\lambda_1, \lambda_2, \lambda_3]$ where $\lambda_1, \lambda_2, \lambda_3$ are all nonzero. The composition of f with the diagonal matrix

$$\begin{pmatrix} \frac{1}{\lambda_1} & 0 & 0 \\ 0 & \frac{1}{\lambda_2} & 0 \\ 0 & 0 & \frac{1}{\lambda_3} \end{pmatrix}$$

is our required projective transformation. □

In particular, since lines in $\mathbb{P}^2(k)$ are defined by two points, we can send a point and its tangent line to wherever we need.

Lemma. *The resultant being zero is invariant under a projective change of coordinates.*

Proof. Let P, Q be of degree m, n respectively. The result follows from the following relations:

- $R_{P(x+a),Q(x+a)} = R_{P(x),Q(x)}\ \forall a \in k$
- $R_{P(ax),Q(ax)} = a^{mn} R_{P(x),Q(x)}$
- $R_{x^m P(\frac{1}{x}),x^n Q(\frac{1}{x})} = (-1)^{mn} R_{P(x),Q(x)}$

$\forall a \in k$. □

References

[1] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 2009.

[2] Joseph H. Silverman and John T. Tate. *Rational Points on Elliptic Curves*. Springer International Publishing, Switzerland, 2015.

[3] Frances Kirwan. *Complex Algebraic Curves*. Cambridge University Press, Cambridge, 1992.

[4] Dale Husemöller. *Elliptic Curves*. Springer-Verlag, New York, 1987.

[5] M. F. Atiyah and I. G. MacDonald. *Introduction To Commutative Algebra*. Avalon Publishing, 1994.

[6] Tom M. Apostol. *Modular Functions and Dirichlet Series in Number Theory*. Springer-Verlag, New York, 1990.