Complex Projective Cubic Plane Curves

Abdullah Ahmed, Ahmer Nadeem Khan, Arhum Naseem Khwaja

Lahore University of Management Sciences,
Mathematics Department
May 15, 2023

Abstract

This report aims to classify the study of all irreducible cubic curves in $\mathbb{C}(\mathbb{P}^2)$ (complex projective 2-space). To do so, it builds up the necessary foundational ideas about algebraic plane curves needed to prove two primary theorems in order: Bezout's Theorem, followed by the Cayley-Bacharach Theorem. Using these two significant results, it will finally move towards classification, with a specific emphasis on the algebraic and topological study of elliptic curves.

Key words and Phrases: Complex projective 2-space, Classification, Bezout's Theorem, Caley-Bacharach Theorem, Elliptic Curves

Contents

1 Plane Curves

Definition 1.1. (Algebraic Plane Curves): Algebraic plane curves are curves defined by a polynomial equation that lie entirely in a plane. Affine plane curves are defined by polynomials $f(x, y) = 0$, $f \in k[x, y]$. Similarly, projective plane curves are defined by homogenous polynomials $f(x : y : z) = 0$, $f \in k[x : y : z]$

This section will continue to explore algebraic plane curves, whose properties can often be extended to projective plane curves. Further, for ease of classification, we can consider algebraic plane curves to be the equivalence classes of the following relation: $f(x, y)\ g(x, y) \iff f(x, y) = \lambda g(x, y)$, for some $\lambda \in k$.

Definition 1.2. (Degree of a Plane Curve): The degree of an algebraic plane curve f is the degree of the leading term of f when f is ordered with respect to graded lexicographic order.

Remark. The degree of a plane curve is used to ascribe labels onto it. Curves of degree 2 are conic sections, curves of degree 3 are cubic curves, curves of degree 4 are quartic curves and so on.

Example. $y^2 + x = 0$ - *Conic section*
$x^3y + 2xy = 0$ - *Quartic curve*
$x^3 + x^2y + 2x + y = 0$ - *Cubic curve*

Remark. This definition of degree is equivalent to the following:

Definition 1.3. Let $f \in k[x_1, x_2, ..., x_n]$ be an algebraic curve where k is an algebraically closed field. The degree of f is given by the intersections between f and a general hyperplane.

Here, a general hyperplane is a hyperplane that does not contain the curve, nor lie 'tangent' to it. In the case of algebraic plane curves, our hyperplane is a straight line.

Definition 1.4. (Irreducible Plane Curves): $f(x, y)$ is irreducible if and only if $f \neq gh$ for some g ,$h \in k[x, y]$. It follows that any $f \in k[x, y]$ can be written as $\prod_{i=1}^{n} f_i^{\alpha}$, where each f_i is an irreducible component of f with multiplicity α.

Definition 1.5. (Simple and Singular Points): A point on a curve $f \in k[x_1, x_2, ..., x_n]$ is simple if $\frac{\partial f}{\partial x_i} \neq 0$ for some $1 \leq i \leq n$. A point on f is singular if it is not simple (i.e $\frac{\partial f}{\partial x_i} = 0\ \forall i$).

Further, we seek to explore the multiplicity of $f(x, y)$ at a point p. To begin, we take the point $p = (0, 0)$.

$f(x, y) = a + m_1 + m_2 + ... + m_n$ where m_i is a non-constant monomial in f and a is constant. Then, $m_{(0,0)}(f) = \min(\deg(m_1), \deg(m_2), ..., \deg(m_n))$. [2]

Remark. If $m_{(0,0)}(f) = 1$ then p is simple, since at least one of the partial derivatives of f at (0,0) is constant and non-zero.

In order to extend this definition to an arbitrary point $p = (a, b)$, we define the linear transformation $T(x, y) = (x + a, y + b)$, then $f^T = f(x + a, x + b)$.

Definition 1.6. (Multiplicity of f at a Point p): $m_p(f) = m_{(0,0)}(f^T)$. By convention, if $p \notin f$ then $m_p f = 0$. [2]

The multiplicity of f at a point p denotes the number of tangents to the curve at p. Equivalently, it denotes the number of smooth monotone arcs in which p is contained. These arcs are known as branches.

Singular points have a multiplicity greater than 1 and can further be classified into nodes and cusps. If the tangents at p are distinct, then f has a node at p, and if the tangents are equal, then f has a cusp at p.

2 Intersection of Plane Curves

Now that the preliminaries of algebraic plane curves have been established, this section aims to study the intersection of two plane curves. We aim to use the resultant of two polynomials to compute the intersection and, we aim to use the properties of the resultant to prove more general results like Bezout's theorem.

Definition 2.1. Given two polynomials $f(x)$, $g(x) \in k[x]$. The resultant is given by the determinant of the following matrix:

$$\begin{bmatrix}
a_0 & a_1 & \dots & a_s & & & \dots & 0 \\
 & a_0 & a_1 & \dots & a_s & & \dots & 0 \\
 & & \ddots & \ddots & \ddots & \ddots & & \\
 & & & a_0 & a_1 & \dots & a_s & \dots & 0 \\
b_0 & b_1 & \dots & b_t & & & & \dots & 0 \\
 & b_0 & b_1 & \dots & b_t & & & \dots & 0 \\
 & & \ddots & \ddots & \ddots & \ddots & & \\
 & & & b_0 & b_1 & \dots & b_t & \dots & 0
\end{bmatrix}$$

where $f = a_0x^s + a_1x^{s-1} + \dots + a_s$ and $g = b_0x^t + b_1x^{t-1} + \dots + b_t$,
$a_0 \neq 0$, $b_0 \neq 0$. [3]

Example. *Resultant of* $f = 4x^3 + 2x$, $g = 3 - 4x$*:*

$$Res(f, g) = \begin{vmatrix}
4 & 0 & 2 & 0 \\
-4 & 3 & 0 & 0 \\
0 & -4 & 3 & 0 \\
0 & 0 & -4 & 3
\end{vmatrix} = 204$$

Corollary 2.1. $gcd(f,g) = 1 \iff Res(f,g) \neq 0$
It is fairly straightforward to see that since a_0 and b_0 are non-zero, the determinant of the resultant matrix will be zero if and only if there is a common root (which in turn, happens if and only if f and g share a common factor).

Corollary 2.2. $Res(f,g) = (-1)^{st} Res(g,f)$

Given algebraic plane curves $f(x,y)$, $g(x,y) \in k[x,y]$, we can re-arrange f and g as follows:

$$f(x,y) = f_0(x)y^s + f_1(x)y^{s-1} + ... + f_s(x)$$
$$g(x,y) = g_0(x)y^t + g_1(x)y^{t-1} + ... + g_t(x)$$

Definition 2.2. (Resultant of f and g With Respect to Y):

$$Res_y(f,g)(x) = \begin{vmatrix} f_0(x) & f_1(x) & ... & f_s(x) & & & ... & 0 \\ & f_0(x) & f_1(x) & ... & f_s(x) & & ... & 0 \\ & & \ddots & \ddots & \ddots & \ddots & & \\ & & & f_0(x) & f_1(x) & ... & f_s(x) & ... & 0 \\ g_0(x) & g_1(x) & ... & g_t(x) & & & & ... & 0 \\ & g_0(x) & g_1(x) & ... & g_t(x) & & & ... & 0 \\ & & \ddots & \ddots & \ddots & \ddots & & & \\ & & & g_0(x) & g_1(x) & ... & g_t(x) & ... & 0 \end{vmatrix}$$

Corollary 2.3. $Res_y(f,g)(x) \neq 0 \iff gcd_y(f,g) = 1$

Theorem 2.1. *There exists a solution to the following system:*
$f(x,y) = 0$, $g(x,y) = 0$ *(where $f_0(x) \neq 0$ or $g_0(x) \neq 0$) if and only if $Res_y(f,g)(a) = 0$. [3]*

Proof. " $\implies$ "
Suppose $f(a,b) = g(a,b) = 0$. This implies that $f(a,y) = f_a(y)$ has a common root b with $g(a,y) = g_a(y)$.
Case 1:
If $f_0(a)$ and $g_0(a)$ are both non-zero, then by Corollary 3.1, $Res(f,g)(a) = 0$. *Case 2:*
If $g_0(a) = 0$, let $g_a^*(y) = g_k(a)y^{s-k} + g_{k+1}y^{s-k-1} + ... + g_s(a)$ such that k is the index o the first non-zero coefficient of y^α.

$$Res(f_a, g_a^*) = g_0^k Res(f_a, g_a)$$

$$= f_0^k \begin{vmatrix} f_0(x) & f_1(x) & ... & f_s(x) & & & ... & 0 \\ & f_0(x) & f_1(x) & ... & f_s(x) & & ... & 0 \\ & & \ddots & \ddots & \ddots & \ddots & & \\ & & & f_0(x) & f_1(x) & ... & f_s(x) & ... & 0 \\ g_k(x) & g_{k+1}(x) & ... & g_t(x) & & & & ... & 0 \\ & g_k(x) & g_{k+1}(x) & ... & g_t(x) & & & ... & 0 \\ & & \ddots & \ddots & \ddots & \ddots & & & \\ & & & g_k(x) & g_{k+1}(x) & ... & g_t(x) & ... & 0 \end{vmatrix}$$

Since f_a and g_a^* share a common root, $Res(f_a, g_a^*) = 0$ and since $f_0(a) \neq 0$, $Res(f_a, g_a) = 0$.

Case 3:

If $f_0(a) = 0$, then, similarly, $Res(g, f_a^*) = g_0^l Res(g, f) = (-1)^{tl} g_0^l Res(f, g)$, where l is the smallest index for which $f_l(a) \neq 0$. Since f_a^* and g_a share a common root, $Res(f, g) = 0$.

" $\Longleftarrow$ "

Suppose $Res_y(f, g) = 0$.

Case 1:

If $f_0(a)$ and $g_0(a)$ are both non-zero. By Corollary 3.1, they have a common factor, and therefore, a common root (the root of the factor).

Case 2:

If $g_0(a) = 0$, $Res(f_a, g_a) = f_0(a)^k Res(f_a, g_a^*) = 0$. Since $f_0(a) \neq 0$, f_a, g_a^* share a common factor, which implies f_a and g_a share a common factor, and therefore, a common root b. Consequently, $f(a, b) = g(a, b) = 0$.

Case 3:

If $f_0(a) = 0$ then $g_0^k Res(f_a, g_a) = (-1)^{tl} Res(g_a, f_a^*) = 0$, which implies f_a and g_a share a common factor, and therefore, a common root b. Consequently, $f(a, b) = g(a, b) = 0$. ■

We can now use Theorem 3.1 to develop a methodology to solve the system $f(x, y) = 0$, $g(x, y) = 0$. Solving $Res_y(f, g) = 0$ will give the x values for the solution, and solving $Res_x(f, g) = 0$ will give the y values for the solution. Then, the values can be paired and each pair tested using substitution.

Example. $f(x, y) = x^2 - 2xy + 3x$, $g(x, y) = y^2 - 4x$

$$Res_y(f, g)(x) = \begin{vmatrix} -2x & x^2 + 3 & 0 \\ 0 & -2x & x^2 + 3 \\ 1 & 0 & -4 \end{vmatrix} = x^2(x^2 - 10x + 9) = 0$$

$\Longrightarrow$ $x = 0, 1, 9$

$$Res_x(f, g)(y) = \begin{vmatrix} 1 & 3 - 2y & 0 \\ 0 & 1 & 3 - 2y \\ 0 & -4 & y^2 \end{vmatrix} = y^2(y^2 - 8y + 12 = 0$$

$\implies y = 0, 2, 6$
Substituting all the possible pairs and testing them gives us the following solutions: $(0,0)$, $(1,2)$, $(9,6)$.

Remark. Theorem 3.1 however, requires that $f_0(a)$ and $g_0(a)$ are not both zero. For example, given $f(x,y) = xy^2 - y + x^2 + 1$ and $g(x,y) = x^2y^2 + y - 1$, $Res_y(f,g) = 0$ implies that f and g intersect at $x = 0$ but since $f_0(x) = g_0(x) = 0$, we cannot know using the theorem if a root $(0, \beta)$ exists.

2.1 Bezout's Theorem

Having established resultants, we can establish some lemmas regarding their properties and use them to prove Bezout's theorem, giving us more information about the intersection of 2 given plane curves.

Theorem 2.2. *(**Bezout's Theorem**): Let $f(x,y)$, $g(x,y) \in k[x,y]$ with degrees s and t respectively. If f and g have no common factor of non-zero degree, then f and g intersect, at most, st times. [3]*

Lemma 2.1. *Let f, $g \in k[x_1, ..., x_r, y_1, ..., y_s, t] \subset k(x_1, ..., x_r, y_1, ..., y_s)[t]$ such that:*

$$f(t) = a_0t^s + ... + a_s$$
$$g(t) = b_0t^r + ... + b_r$$
where each $a_i \in k[x_1, ..., x_r]$ and each $b_j \in k[y_1, ..., y_s]$.

Then, $Res(f,g)$ is a monic polynomial of degree $rs - km$ where k is the smallest index such that $a_k \neq 0$ and m is the smallest index such that $b_m \neq 0$. [3]

Lemma 2.2. *Let f, $g \in k(x_1, ..., x_r, y_1, ..., y_s)[t]$ such that:*

$$f(t) = (t - x_1)(t - x_2)...(t - x_r)$$
$$g(t) = (t - y_1)(t - y_2)...(t - y_s)$$
$$\text{Then, } Res(f,g) = \prod_{j=1}^{r} \prod_{k=1}^{s} (x_j - y_k).$$

[3]

Proof. By the Vieta formula for plane curves:

$$f(t) = t^r - s_1(x_1, ..., x_r)t^{r-1} + ... + (-1)^r S_r(x_1, ..., x_r),$$
$$g(t) = t^s - s_1(y_1, ..., y_s)t^{s-1} + ... + (-1)^s S_s(y_1, ..., y_s),$$
where S_i are non-zero, monic, symmetric polynomials in r or s variables. [3]

By Lemma 3.1, $Res(f,g)$ is a monic polynomial of degree rs. By Corollary 3.1, $Res(f,g) = 0$ when $x_j = y_k$ for some j, k. Therefore $Res(f,g)$ is divisible by $x_j - y_k$. Since $x_j - y_k$ and $x_l - y_p$ are relatively prime if $j \neq l$ or $k \neq p$, $Res(f,g)$ is divisible by the product of all $x_j - y_k$:

$$Res(f,g) = \prod_{j=1}^{r}\prod_{k=1}^{s}(x_j - y_k)$$

■

Lemma 2.3. *Let f, $g \in k[t]$ such that:*

$$f(t) = a_0t^r + ... + a_r = a_0(t-c_1)...(t-c_r) = a_0\prod_{j=1}^{r}(t-c_j)$$
$$g(t) = b_0t^s + ... + b_s = b_0(t-d_1)...(t-d_s) = b_0\prod_{k=1}^{s}(t-d_k).$$

Then, $Res(f,g) = a_0^s b_0^r \prod_{j=1}^{r}\prod_{k=1}^{s}(c_j - d_k) = a_0^s\prod_{j=1}^{r} g(c_j) = (-1)^{rs}b_0^s\prod_{k=1}^{s} f(d_k)$

Proof. If $a_0 = b_0 = 1$, then by Lemma 3.2: $Res(f,g) = \prod_{j=1}^{r}\prod_{k=1}^{s}(c_j - d_k)$. Otherwise, $Res(\frac{f_0}{a_0}, \frac{g_0}{b_0}) = \prod_{j=1}^{r}\prod_{k=1}^{s}(c_j - d_k) \iff Res(\frac{f_0}{a_0}, \frac{g_0}{b_0}) = a_0^s b_0^r Res(f,g) \iff Res(f,g) = a_0^s b_0^r \prod_{j=1}^{r}\prod_{k=1}^{s}(c_j - d_k)$.

Further, $a_0^s\prod_{j=1}^{r} g(c_j) = a_0^s\prod_{j=1}^{r}(b_0\prod_{k=1}^{s}(c_j - d_k)) = a_0^s b_0^r\prod_{j=1}^{r}\prod_{k=1}^{s}(c_j - d_k) = Res(f,g)$ and $(-1)^{rs}b_0^s\prod_{k=1}^{s} f(d_k) = (-1)^{rs}b_0^s\prod_{k=1}^{s}(a_0\prod_{j=1}^{r}(d_k - c_j)) = (-1)^{rs}a_0^r b_0^s(-1)^{rs}\prod_{k=1}^{s}\prod_{j=1}^{r}(c_j - d_k) = Res(f,g)$. ■

Definition 2.3. (Discriminant of $f(x)$): $\Delta f(x) = (-1)^{\frac{r(r-1)}{2}}\frac{1}{a_0}Res(f, \frac{\delta f}{\delta x})$, where $r = deg(f)$. [3]

Example. $f = ax^2 + bx + c$
$\Delta(f) = (-1)^1\frac{1}{a}Res(f, \frac{\delta f}{\delta x})$

$$\Delta(f) = \frac{-1}{a}\begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix}$$

$\Delta(f) = \frac{-1}{a}(4a^2c - b^2a) = b^2 - 4ac$

Lemma 2.4. *Let $f \in k[t]$ such that:*

$$f(t) = a_0t^r + ... + a_r = a_0(T-c_1)...(T-cr).$$

Then:

$$\Delta(f) = a_0^{2r-2}\begin{vmatrix} 1 & 1 & ... & 1 \\ c_1 & c_2 & ... & c_r \\ \vdots & \vdots & \ddots & \vdots \\ c_1^{r-1} & c_2^{r-1} & ... & c_r^{r-1} \end{vmatrix}^2 \quad [3]$$

Proof.

$$f'(t) = a_0\sum_{j=1}^{r}(t-c_1)...(t-c_{j-1})(t-c_{j+1})...(t-c_r).$$
$$\implies f'(c_j) = (-1)^{r-j}a_0(c_j - c_1)...(c_j - c_{j-1})(c_{j+1} - c_j)...(c_r - c_j)$$

By Lemma 3.3: $Res(f,f') = a_0^{r-1}\prod_{j=1}^{r} f'(c_j)$. And since every $c_k - c_j$ occurs twice:

$$a_0\Delta(f) = (-1)^{\frac{r(r-1)}{2}} Res(f, f') = a_0^{2r-1} \prod_{k>j}(c_k - c_j)^2. \blacksquare$$

Lemma 2.5. *Let f, $g \in k[x, y]$, then $deg(Res(f, g)) \leq deg(f)deg(g)$. [3]*

Proof. Let $x := \frac{x_1}{x_2}$ and $y := \frac{y}{x_2}$. Then f, $g \in k(x_1, x_2, y)$. Cancelling the common denominator gives us f^+ and $g^+ \in k[x_1, x_2, y]$ where $deg(f^+) = deg(f) = r$ and $deg(g^+) = deg(g) = s$:

$$f^+(x_1, x_2, y) = f_0(x_1, x_2)y^r + ... + f_r(x_1, x_2),$$
$$g^+(x_1, x_2, y) = g_0(x_1, x_2)y^s + ... + g_s(x_1, x_2),$$

where each f_i and g_j are monic polynomials of degrees i and j respectively or 0.

By Lemma 3.1, $Res(f^+, g^+)$ is a monic polynomial (with respect to y) of degree less than or equal to rs. From our substitution, $f(x_1, y) = f^+(x_1, 1, y)$ and $g(x_1, y) = g^+(x, 1, y)$. Since $Res_y(f, g) = Res(f^+(x_1, x_2 = 1, y), g^+(x, x_2 = 1, y))$ we have that $deg(Res(f, g)) \leq rs = deg(f)deg(g)$. $\blacksquare$

Proof of Bezout's Theorem. [3]
Assume on the contrary that there exist f, $g \in k[x, y]$ with degrees r and s respectively, and f and g have no common factor with a non-zero degree, such that there are $rs + 1$ different solutions of the system.
There exists c such that:

$$a_j + cb_j \neq a_k + cb_k,\ 1 \leq j < k \leq rs + 1$$

Substitute: $x := x' - cy'$, $y = y'$

$$f_1(x', y') = f_0(x - cy')y'^r + f_1(x' - cy')y'^{r-1} + ... + f_r(x' - cy'),$$
$$g_1(x', y') = g_0(x - cy')y'^s + g_1(x' - cy')y'^{s-1} + ... + g_s(x' - cy')$$

Set: $(a'_j, b'_j) = (a_j + cb_j, b_j)$, $j \in 1, 2, ..., rs + 1$ where $a'_j \neq a'_k$ for $j \neq k$. Therefore,

$$f_1(a'_j, b'_j) = g_1(a'_j, b'_j) = 0$$

By Theorem 3.1, $a'_1, a'_2, ..., a'_{rs+1}$ are roots of $Res_{y'}(f_1, g_1)(x')$. By Lemma 3.5, $deg(Res_{y'}(f_1, g_1)(x')) \leq rs$ so $Res_{y'}(f_1, g_1)$ must be 0. By Corollary 3.3, this implies that f and g have a common non-zero factor, which is a contradiction to the assumption and f and g cannot intersect $rs + 1$ times. Therefore, Bezout's theorem is proved. $\blacksquare$

2.2 Generalized Bezout's Theorem

Theorem 2.3. ***(Bezout)**: Two projective algebraic plane curves f and g with degrees r and s respectively that have no common factor over an algebraically closed field have rs common points (counted with multiplicities). [3]*

3 Transition

Moving ahead we will begin building up some theory in order to define the group law on elliptic curves, and proving some classical theorems in Euclidean geometry along the way. The main goal of this section is to prove the Cayley-Bacharach Theorem (also known as the 8-point Theorem of cubic curves); we will then be able to prove the famous Pappus' Theorem and Pascal's Theorem using Cayley-Bacharach. Eventually, Cayley-Bacharach will be used to prove the associativity of the group law on elliptic curves.
Firstly let us recall some notions, and restate others discussed prior more precisely now.
Examples of different degree curves that we will reference include:

- ◇ Degree 1 (linear) curves $\{(x, y) \in k^2 : ax + by = c\}$, which are lines in k^2;
- ◇ Degree 2 (quadric) curves $\{(x, y) \in k^2 : ax^2 + bxy + cy^2 + dx + ey + f = 0\}$, which include classical conic sections (circles, hyperbolae, parabolae, ellipses) when $k = \mathbb{R}$, and also the reducible case of a union of two lines;
- ◇ Degree 3 (cubic) curves $\{(x, y) \in k^2 : ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0\}$, which include the elliptic curves $\{(x, y) \in k^2 : y^2 = x^3 + ax + b\}$ (with non-zero discriminant $\Delta := -16(4a^3 + 27b^2)$, so that the curve is smooth) as examples (ignoring some technicalities when k has characteristic two or three), but also include the reducible examples of the union of a line and a conic section, or the union of three lines.

Algebraic affine plane curves can also be extended to the projective plane $\mathbb{P}k^2 = \{[x, y, z] : (x, y, z) \in k^3\backslash 0\}$ by homogenising the polynomial. For instance, the affine quadric curve $\mathbb{P}k^2 = \{[x, y, z] : (x, y, z) \in k^3\backslash\{0\}\}$ would become $\{[x, y, z] \in \mathbb{P}k^2 : ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0\}$.

We also now reformulate the definition of *degree* now. We will define the degree of a plane curve as the maximum possible intersection with a linear sub-variety (here, we consider plane curves as varieties in k^2).

Definition 3.1. A linear sub-variety of $\mathbb{P}^n$ is a closed subset of a variety (in the Zariski Topology) defined by linear homogeneous polynomials.

Then, an m-dimensional linear sub-variety of $\mathbb{P}^n$ is a projective sub-variety determined by a $(m + 1)$-dimensional subspace of the vector space $\mathbb{C}^{n+1}$. Furthermore, the projective closure of a linear sub-variety of $\mathbb{A}^n$ is a linear sub-variety in $\mathbb{P}^n$.

Definition 3.2. The degree of a variety $V \subset \mathbb{P}^n$, denoted by $deg(V)$, is defined as

$$deg(V) := max\{\#(V \cap L) < \infty\}$$

where L is linear in $\mathbb{P}^n$ and $dimL + dimV = n$.

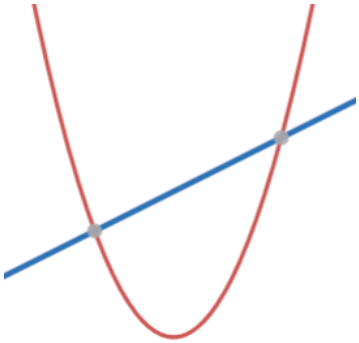

Figure 1: A generic line intersects a conic in two distinct points.

Thus, the degree of V is the number of points common to V and a $(codim V)$-dimensional "generic" linear sub-variety.

We can then prove the following theorem, which ensures us that our two definitions of "degree" are consistent.

Theorem 3.1. *If F is an irreducible homogeneous polynomial of degree d, then the degree of the hypersurface $\mathbb{V}(F) \subset \mathbb{P}^n$ is d.*

Proof. Give an arbitrary line $L \subset \mathbb{P}^n$, the intersection point of V and L can be identified with the zero of the polynomial function on L obtained by restricting F to the line L. The restriction of F to the line L produces a degree d polynomial on $L \cong \mathbb{C}$ which, by the Fundamental Theorem of Algebra, has d roots. For a generic line L, these roots are distinct, and correspond to the d intersection points of V and L. ■

Arguments that follow will also heavily depend on Theorem 2.3, the *The Generalized Bezout's Theorem*. To get some understanding of its implications, see that it ensures two distinct lines intersect in at most one point; a line and a conic section intersect in at most two points; two distinct conic sections intersect in at most four points; a line and an elliptic curve intersect in at most three points; two distinct elliptic curves intersect in at most nine points; and so forth. Now having recalled all the machinery we will utilize ahead, we can move on.

3.1 Building Algebraic Curves

Using facts from Linear Algebra, we can easily build algebraic curves by considering general plane equations and applying constraints to these equations by specifying a particular number of points in the plane through which the curve must pass. For example:

- ◇ For any two points A_1, A_2 one can find a line $\{(x, y) : ax + by = c\}$ passing through the points A_1, A_2, because this imposes two linear constraints on three unknowns a, b, c and is thus guaranteed to have at least one solution;

- ◇ Given any five points $A_1, \ldots, A_5$, one can find a quadric curve passing through these five points (though note that if three of these points are collinear, then this curve cannot be a conic thanks to Bezout's theorem as the line passing through these points and the curve can only intersect in at most two points, and is thus necessarily reducible to the union of two lines);

- ◇ Given any nine points $A_1, \ldots, A_9$, one can find a cubic curve going through these nine points.

Next, we must deal with the uniqueness of algebraic curves that are built through these *polynomial methods.* This will be relevant to our discussion of the Cayley-Bacharach Theorem.
In the linear case, it is clear that the line determined by two distinct points is always unique. The higher degree cases are more complicated. For instance, five collinear points do not determine a unique quadric curve; one can simply take the union of the line containing those five points, and any other arbitrary line; every choice of the other line determines a different quadric. Similarly, eight points on a conic section plus one additional point determine more than one cubic curve, as one can take that conic section plus an arbitrary line going through the additional point.

This issue of uniqueness is resolved if some "general" situation is imposed on these points. For instance, given five points, no three of which are collinear, there can be at most one quadric curve that passes through these points (because these five points cannot lie on the union of two lines, and by Bézout's theorem they cannot simultaneously lie on two distinct conic sections). Here, the general hypothesis is that no three points lie on a hypersurface (a line in this case).

For cubic curves, the situation is more complicated still. Consider for instance two distinct cubic curves $\gamma_0 = \{P_0(x, y) = 0\}$ and $\gamma_\infty = \{P_\infty(x, y) = 0\}$ that intersect in precisely nine points $A_1, \ldots, A_9$ (note from Bézout's theorem that this is an entirely typical situation). Then there is in fact an entire one-parameter family of cubic curves that pass through these points, namely the curves $\gamma_t = \{P_0(x, y) + tP_\infty(x, y) = 0\}$ or any t$\in k \cup \{\infty\}\}$. This leads immediately to the theorem in the next section.

4 Cayley-Bacharach Theorem

Theorem 4.1 (**Cayley-Bacharach Theorem**). *Let* $\gamma_0 = \{P_0(x, y) = 0\}$ *and* $\gamma_\infty = \{P_\infty(x, y) = 0\}$ *be two cubic curves that intersect (over some algebraically closed field* k*) in precisely nine distinct points* $A_1, \ldots, A_9 \in k^2$*. Let* P *be a cubic polynomial that vanishes on eight of these points (say* $A_1, \ldots, A_8$*). Then* P *is a linear combination of* P_0, P_∞*, and in particular vanishes on the ninth point* A_9*.*

Proof. (by Husemöller) We assume for contradiction that there is a cubic polynomial P that vanishes on $A_1, \ldots, A_8$, but is not a linear combination of P_0 and P_∞.

We first make some observations on the points $A_1, \ldots, A_9$. No four of these points can be collinear, because then by Bézout's theorem, P_0 and P_∞ would both have to vanish on this line, contradicting the fact that γ_0, γ_∞ meet in at most nine points. For similar reasons, no seven of these points can lie on a quadric curve.

One consequence of this is that any five of the $A_1, \ldots, A_9$ determine a unique quadric curve σ. The existence of the curve follows from linear algebra as discussed previously. If five of the points lie on two different quadric curves σ, σ', then by Bezout's theorem, they must share a common line; but this line can contain at most three of the five points, and the other two points determine uniquely the other line that is the component of both σ and σ', and the claim follows.

Now suppose that three of the first eight points, say A_1, A_2, A_3, are collinear, lying on a line ℓ. The remaining five points $A_4, \ldots, A_8$ do not lie on ℓ, and determine a unique quadric curve σ by the previous discussion. Let B be another point on ℓ, and let C be a point that does not lie on either ℓ or σ. By linear algebra, one can find a non-trivial linear combination $Q = aP + bP_0 + cP_\infty$ of P, P_0, P_∞ that vanishes at both B and C. Then Q is a cubic polynomial that vanishes on the four collinear points A_1, A_2, A_3, B and thus vanishes on ℓ, thus the cubic curve defined by Q consists of ℓ and a quadric curve. This curve passes through $A_4, \ldots, A_8$ and thus equals σ. But then C does not lie on either ℓ or σ despite being a vanishing point of Q, a contradiction. Thus, no three points from $A_1, \ldots, A_8$ are collinear.

In a similar vein, suppose next that six of the first eight points, say $A_1, \ldots, A_6$, lie on a quadric curve σ; as no three points are collinear, this quadric curve cannot be the union of two lines, and is thus a conic section. The remaining two points A_7, A_8 determine a unique line $\ell = \overleftrightarrow{A_7 A_8}$. Let B be another point on σ, and let C be another point that does not lie on either ℓ and σ. As before, we can find a non-trivial cubic $Q = aP + bP_0 + cP_\infty$ that vanishes at both B, C. As Q vanishes at seven points of a conic section σ, it must vanish on all of σ, and so the cubic curve defined by Q is the union of σ and a line that passes through A_7 and A_8, which must necessarily be ℓ. But then this curve does not pass through C, a contradiction. Thus no six points in $A_1, \ldots, A_8$ lie on a quadric curve.

Finally, let ℓ be the line through the two points A_1, A_2, and σ the quadric curve through the five points $A_3, \ldots, A_7$; as before, σ must be a conic section, and by the preceding paragraphs we see that A_8 does not lie on either σ or ℓ. We pick two more points B, C lying on ℓ but not on σ. As before, we can find a non-trivial cubic $Q = aP + bP_0 + cP_\infty$ that vanishes on B, C; it vanishes on four points on ℓ and thus Q defines a cubic curve that consists of ℓ and a quadric curve. The quadric curve passes through $A_3, \ldots, A_7$ and is thus σ; but then the curve does not pass through A_8, a contradiction. This contradiction finishes the proof of the proposition. [6] ■

5 Corollaries in Euclidean Geometry

5.1 Pappus' Theorem

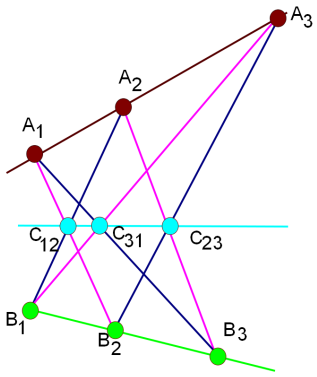

Figure 2: Diagram showing Pappus' Theorem. [5]

Theorem 5.1 (**Pappus' Theorem**). *Let ℓ, ℓ' be two distinct lines, let A_1, A_2, A_3 be distinct points on ℓ that do not lie on ℓ', and let B_1, B_2, B_3 be distinct points on ℓ' that do not lie on ℓ. Suppose that for $ij = 12, 23, 31$, the lines $\overleftrightarrow{A_iB_j}$ and $\overleftrightarrow{A_jB_i}$ meet at a point C_{ij}. Then the points C_{12}, C_{23}, C_{31} are collinear.*

Proof. We may assume that C_{12}, C_{23} are distinct, since the claim is trivial otherwise. Let γ_0 be the union of the three lines $\overleftrightarrow{A_1B_2}$, $\overleftrightarrow{A_2B_3}$, and $\overleftrightarrow{A_3B_1}$ (the purple lines in Figure 2), let γ_1 be the union of the three lines $\overleftrightarrow{A_2B_1}$, $\overleftrightarrow{A_3B_2}$, and $\overleftrightarrow{A_1B_3}$ (the dark blue lines), and let γ be the union of the three lines ℓ, ℓ', and $\overleftrightarrow{C_{12}C_{23}}$ (the other three lines). By construction, γ_0 and γ_1 are cubic curves with no common component that meet at the nine points $A_1, A_2, A_3, B_1, B_2, B_3, C_{12}, C_{23}, C_{31}$. Also, γ is a cubic curve that passes through the first eight of these points, and thus also passes through the ninth point C_{31}, by the Cayley-Bacharach theorem. The claim follows (note that C_{31} cannot lie on ℓ or ℓ').[5] ■

5.2 Pascal's Theorem

Theorem 5.2 (**Pascal's Theorem**). *Let $A_1, A_2, A_3, B_1, B_2, B_3$ be distinct points on a conic section σ. Suppose that for $ij = 12, 23, 31$, the lines $\overleftrightarrow{A_iB_j}$ and $\overleftrightarrow{A_jB_i}$ meet at a point C_{ij}. Then the points C_{12}, C_{23}, C_{31} are collinear.*

Proof. Repeat the proof of Pappus' theorem, with σ taking the place of $\ell \cup \ell'$. (Note that as any line meets σ in at most two points, the C_{ij} cannot lie on σ.) [5] ■

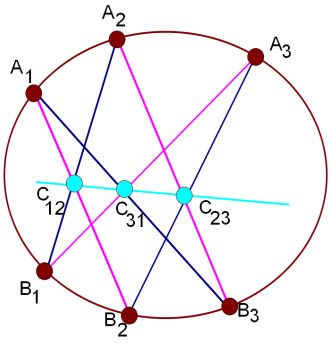

Figure 3: Diagram showing Pascal's Theorem. [5]

One can also view Pappus's theorem as the degenerate case of Pascal's theorem, when the conic section degenerates to the union of two lines.

Having proved all the necessary machinery we now move on to classification of cubics, where it must be taken for granted that our curves live in the complex projective plane, although most of these notions can be generalized to any algebraically closed field. It is only during the topological analysis of elliptic curves that our restriction to $\mathbb{C}$ is important.

6 Singular Cubic Plane Curves

Definition 6.1. *A cubic plane curve containing a singular point is called a singular cubic plane curve.*

There exists an equivalent characterization of a singular point to the one mentioned before: *Given a curve C, a point $S \in C$ is a singular point of C if and only if every line L passing through S intersects C at S with $m_S(C \cap L) \geq 2$.* Also recall a specific case of Bezout's Theorem: *Assume we have two curves C_1, $C_2 \in \mathbb{C}(\mathbb{P}^2)$ of degree d_1 and d_2 respectively that do not share a common irreducible component. Then, accounting for multiplicity, $C_1 \cap C_2$ consists exactly of $d_1 d_2$ points.* Using this, we prove the following lemma.

Lemma 6.1. *Let C be an irreducible singular cubic plane curve. Then C only has one singular point S with $m_S(C) = 2$.*

Proof. Assume $\exists\ S_1, S_2 \in C$ such that both are singular points of C and $S_1 \neq S_2$. Let $L = \overline{S_1 S_2}$ be of degree 1. As $S_1, S_2 \in C \cap L \Rightarrow L$ intersects C with total multiplicity at least 4 at S_1 and S_2. This is a contraction as L and C do not share a common component (as they are irreducible) and thus, by Bezout's Theorem, C must intersect L with total multiplicity only 3. Thus $S_1 = S_2$.

Now taking S to be our singular point, assume that $m_S(C) \geq 3$. Take any point $M \neq S$

on C. The line $L = \overline{MS}$ intersects C with total multiplicity at least 4 at M and S. This is again a contradiction to Bezout's Theorem for the same reason as before. Thus $m_S(C) = 2$. ■

Now we can use the above lemma to prove the first classification:

Theorem 6.1. *Let C be an irreducible singular cubic plane curve. Then C is rational, i.e, birationally equivalent to $\mathbb{P}^1$.*
Proof. Let S be the singular point of C and L be any line in $\mathbb{P}^2$ such that $S \notin L$. Take any point in $L \setminus C$, say Q; then the line $\overline{QS}$ intersects C at only one other point besides S to give total multiplicity 3 (This follows from the previous lemma and Bezout's Theorem). Denote this point by Q', and define the following rational map:

$$\phi : L \dashrightarrow C, \quad Q \longmapsto Q' = \overline{QS} \cap (C \setminus \{S\}).$$

Note that this map is by construction the quotient of two polynomials, as it is formed through the intersection of two polynomial curves: a straight line and a cubic. Coupling this with the fact that it is defined on the Zariski dense open subset $(L \setminus C) \subseteq L$, we can define a rational inverse $\phi^{-1} : C \dashrightarrow L$, where any point $Q' \in C$ is mapped to the single point in $(\overline{Q'S}) \cap L$ (will be a single point as total intersection multiplicity of two lines equals 1 by Bezout's Theorem). We can see that ϕ^{-1} is defined on the Zariski dense open subset $(C \setminus \{S\}) \subseteq C$, and includes $\phi(L \setminus C)$. Also $\phi^{-1}(C \setminus \{S\}) \subseteq (L \setminus C)$ as $((\overline{Q'S}) \cap L) \notin C$ by Bezout's theorem (would otherwise give total intersection multiplicity of $\overline{QS} \cap C$ to be ≥ 4). Thus both compositions $(\phi \circ \phi^{-1})$, and $(\phi^{-1} \circ \phi)$ are defined, and both equal identity on their respective domains by construction. Thus we have a birational mapping between $L \cong \mathbb{P}^1$ and $C \Rightarrow$ C is rational. ■

7 Non-Singular Cubic Plane Curves

Definition 7.1. *A non-singular/smooth projective cubic plane curve is called a general elliptic curve.*

7.1 Weierstrass Normal Form

We can see that the definition of an elliptic curve does not, at least obviously, impose any conditions on the cubic polynomial itself. To make any such impositions clear, we introduce the notion of the Weierstrass Normal Form of a cubic–which is in simple words just a cubic of the type: $y^2 = x^3 + cx + d$, where we are looking at the affine projection of our cubic plane curve, and $c, d \in \mathbb{C}$.

Proposition 7.1.1. *Every elliptic curve is projectively equivalent (i.e related by a set of projective transformations) to a curve of the Weierstrass Normal Form.*
Proof. Starting with the general form of a homogenized cubic polynomial for a cubic

curve in $\mathbb{C}(\mathbb{P}^2)$, these transformations can be sketched out as follows: Fix any point $\mathcal{O}$ on the elliptic curve E. Set $Z = 0$ to be the tangent to E at $\mathcal{O}$. This axis then intersects E at exactly one other point, K. Set $X = 0$ to be the tangent to E at K, and $Y = 0$ to be any line that passes through $\mathcal{O}$ apart from $Z = 0$. Now dehomogenize by setting $x = X/Z$ and $y = Y/Z$. Once in this form, a simple set of linear transformations and algebraic manipulations gets one to the final Weierstrass Normal Form. The details of the proof can be found in Silverman.[4] ■

One should note the key role played by the smoothness of an elliptic curve in the proof above. We can also see that the above curve in Weierstrass Normal form contains the point at infinity $\sigma = [0 : 1 : 0]$, and has $Z = 0$ as the tangent to E at σ. Also note that this curve is symmetric about the x-axis. All of these properties heavily restrict the family of curves we need to focus on, and we can safely assume, from now on, that our elliptic curves will be given exclusively in the Weierstrass Normal Form.

7.2 Chord-and-Tangent Group Law

It is possible to define a group structure on every *general* elliptic curve. This is done by introducing an appropriate binary operation on the points of the elliptic curve. We will move to define this now: Take any two points P and Q on our elliptic curve E. Set $P \star Q = \overline{PQ} \cap (E \setminus \{P, Q\})$, which is well defined by Bezout's Theorem. If $P = Q$, then the line $\overline{PQ}$ is taken to be the tangent to E at P. If $Q = \sigma$, then $\overline{P\sigma}$ is a vertical line at P, and $P \star \sigma = P_r$, where P_r is the reflection of P across the x-axis. If $P = \sigma$, then $\sigma \star Q = Q_r$.

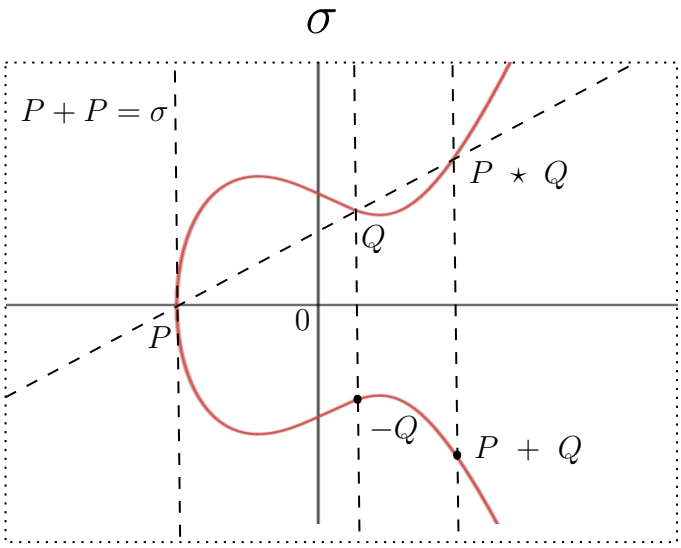

Figure 4: The group law exhibited on the elliptic curve given by $y^2 = x^3 - 4x + 9$. Note that here we are specifically looking at its real projection on the affine plane. The point at infinity σ lies outside the affine plane marked by the dotted boundary.

Theorem 7.2.1. *Given the following binary operation:*

$$+ : E \times E \longrightarrow E \quad \textit{such that} \quad P + Q = (P \star Q) \star \sigma,$$

$(E, +)$ *is an abelian group.*

Proof. We must check that the group axioms hold for $(E, +)$:
Identity: We can easily see that for any $P \in E$:

$$P + \sigma = (P \star \sigma) \star \sigma = (P_r)_r = P = (P_r)_r = (\sigma \star P) \star \sigma = \sigma + P,$$

hence σ is identity in $(E, +)$.
Inverse: We can see that for any $P \in E$:

$$P + P_r = (P \star P_r) \star \sigma = \sigma \star \sigma = \sigma = \sigma \star \sigma = (P_r \star P) \star \sigma = P_r + P,$$

hence P_r (which always exists in E due to symmetry of E about the x-axis given by the Weierstrass Normal form) is the inverse of P.
Commutativity: Is can easily be seen geometrically, that as for any P, $Q \in E$, $\overline{PQ} = \overline{QP} \Rightarrow P + Q = Q + P$.
Associativity: As is the case for most group structures, this proof is the most involved one. Firstly, we can see that for any P, Q, $R \in E$, $(P + Q) + R = P + (Q + R) \Leftrightarrow (P + Q) \star R = P \star (Q + R)$. Thus we focus on proving the latter instead. Here we will also assume we are ignoring some special cases where either some of the points are equal to each other, or equal to some others' reflection, etc–associativity can be proved trivially in these cases.

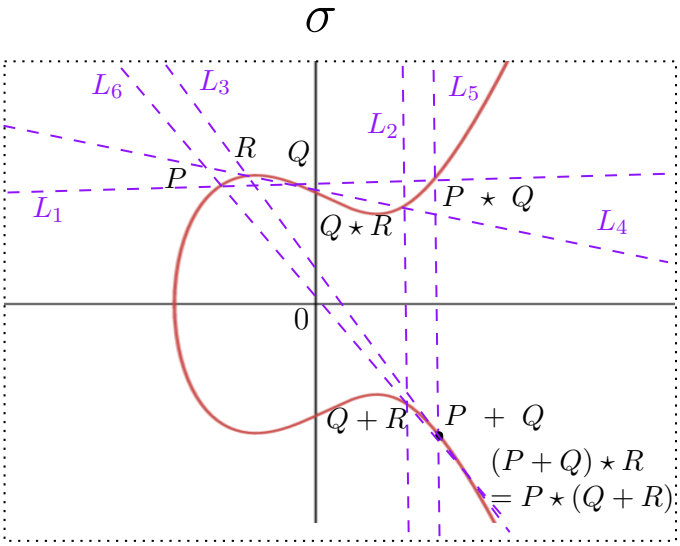

Figure 5: Geometric visualization of associativity of the group law.

Consider the following 8 points: σ, P, Q, R, $P \star Q$, $P + Q$, $Q \star R$, and $Q + R$. Construct the following six lines: $L_1 = \overline{PQ}$, $L_2 = \overline{(Q \star R)\sigma}$, $L_3 = \overline{(P + Q)R}$, $L_4 = \overline{RQ}$,

$L_5 = \overline{(P \star Q)\sigma}$, $L_6 = \overline{P(Q+R)}$.
Note that $C_1 = L_1 \cup L_2 \cup L_3$ and $C_2 = L_4 \cup L_5 \cup L_6$ form two degenerate cubics that pass through the 8 points mentioned before by definition, and, assuming that the points were chosen generally, an additional distinct ninth point given by $L_3 \cap L_6$. As E is a cubic curve that passes through the first 8 points by definition, by the *Cayley-Bacharach Theorem* it must pass through the ninth point, i.e, $L_3 \cap L_6 \Rightarrow (E \cap L_3) \setminus \{P+Q, R\} = L_2 \cap L_6 = (E \cap L_6) \setminus \{P, Q+R\}$. But we know, by definition, $(P+Q) \star R = (E \cap L_3) \setminus \{P+Q, R\}$ and $P \star (Q+R) = (E \cap L_6) \setminus \{P, Q+R\} \Rightarrow (P+Q) \star R = P \star (Q+R)$. Hence we are done and $(E, +)$ is an abelian group. ■

Now we can use the tools of abstract algebra to study elliptic curves, an instance of which is discussed below.

Proposition 7.2.1. *If E is an elliptic curve defined over a field L that has coefficients in a sub-field K of L, then the set of K-rational points $E(K) \leq E(L)$.*
Proof. It suffices to show that for any $P, Q \in E(K)$, we must also have $(P \star Q) \in E(K)$. Let $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, $P \star Q = R = (x_R, y_R)$ and $E : y^2 = x^3 + ax + b$ be an arbitrary elliptic curve where $a, b \in K$.
Assume $x_P \neq x_Q$. Then $\overline{PQ} : y = sx + d$, where $s = \dfrac{y_P - y_Q}{x_P - x_Q} \in K$. At $\overline{PQ} \cap E$ we have $sx + d = x^3 + ax + b \Rightarrow x^3 - s^2x^2 - 2sdx + ax + b - d^2 = 0$. By construction we have that x_P, x_Q and x_R are solutions to this cubic, i.e:

$$x^3 - s^2x^2 - 2sdx + ax + b - d^2 \equiv (x - x_P)(x - x_Q)(x - x_R)$$

Thus we can equate the coefficients of x^2 to get $s^2 - x_P - x_Q = x_R \in K$. Now using the equation for $\overline{PQ}$, we get $y_P + s(x_R - x_P) = y_R \in K \Rightarrow R \in E(K)$.
If $x_P = x_Q \Rightarrow y_P = \pm y_Q$. If $y_P = -y_Q$, then $R = \sigma \in E(K)$. If $y_P = y_Q$, then $P = Q$ and we consider the tangent at P, $T_P : gx + l$, where $g = \dfrac{3x_P^2 + a}{2y_P} \in K$. Using similar arguments as before, we can see that $T_P \cap E$ will give points in $E(K) \Rightarrow R \in E(K)$. Thus $E(K) \leq E(L)$. ■

There are also certain important results specifically for rational points on elliptic curves, one of which is stated here:

Theorem 7.2.2 (Mordell's Theorem, 1922). *If an elliptic curve E in the Weierstrass Normal form has integer coefficients, $E(\mathbb{Q})$ is a finitely generated abelian group.*

There are also some other important results regarding this finitely generated abelian group including the Nagell-Lutz Theorem(1935) and Mazur's Theorem(1977).

7.3 The Topology of an Elliptic Curve

We proved earlier that all singular cubic plane curves were rational. One question of great importance is whether any such parameterisation in terms of the projective line exists for elliptic curves. Turns out, it does not. One can prove this is many different ways, but the argument we choose to make here is a topological one. If we can show that the the elliptic curve is not topologically equivalent to $S^2 \overset{\text{hom}}{\cong} \mathbb{P}^1$ upto addition or removal of finitely many points (courtesy of a *birational equivalence* to $\mathbb{P}^1$, which is only *almost* an isomorphic equivalence), then that is equivalent to showing that elliptic curves are not rational. In fact, we will prove something stronger, and that is *every elliptic curve is homeomorphic to the torus*. For this argument, we introduce some new objects of interest:

Definition 7.3.1. A *lattice* Λ generated by $\omega_1,\ \omega_2 \in \mathbb{C}$ (where ω_1 and ω_2 are linearly independent over $\mathbb{R}$) is the set of all *integral* linear combinations of ω_1 and ω_2. It can also be denoted by $\Lambda(\omega_1, \omega_2)$, i,e, $\Lambda(\omega_1, \omega_2) = \{m\omega_1 + n\omega_2 : m,\ n \in \mathbb{Z}\}$.

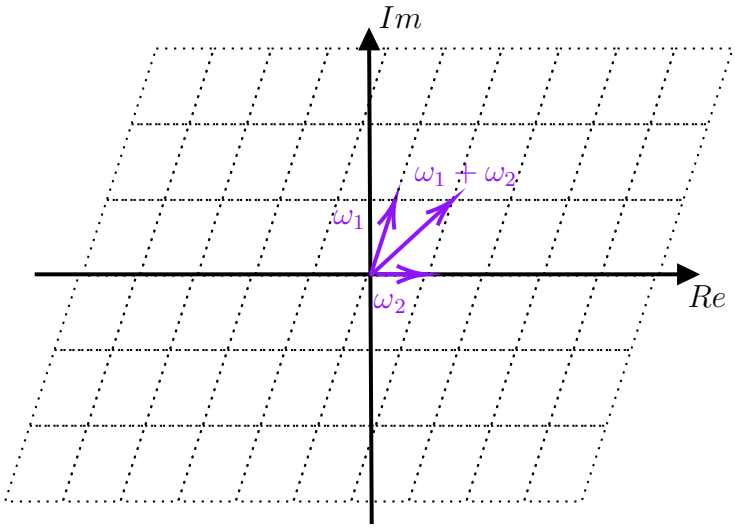

Figure 6: The lattice $\Lambda(\omega_1, \omega_2)$ shown on $\mathbb{C}$. More specifically, Λ consists of all the vertices of the parallelograms shown.

Given any lattice Λ generated by ω_1 and ω_2, one can define a special function known as the *Weierstrass-$\wp$ function* as follows:

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

This series converges *uniformly absolutely* in $\mathbb{C} \setminus \Lambda$, and has a *pole* of order 2 at each

lattice point.[1] Also:

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

There are some other properties of the Weierstrass-$\wp$ function and its derivative that are important to note.

Lemma 7.3.1. *$\wp(z)$ is an even function and $\wp'(z)$ is an odd function.*
Proof. We can see that,

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

where the last step follows as the summation preceeding it is merely a rearrangement of the orginal summation (for all $\lambda \in \Lambda \Leftrightarrow -\lambda \in \Lambda$), and thus converges to the same value as before due to absolute uniform convergence. Thus $\wp$ is even, and using a similar argument, one can show that $\wp'$ is odd. ■

Lemma 7.3.2. *$\wp(z)$ and $\wp'(z)$ are doubly periodic, that is, $\wp(z+\omega_1) = \wp(z) = \wp(z+\omega_2)$ and $\wp'(z+\omega_1) = \wp'(z) = \wp'(z+\omega_2)$, for all $z \in \mathbb{C} \setminus \Lambda$.*
Proof. We can see that,

$$\wp(z+\omega_1) = \frac{1}{(z+\omega_1)^2} + \sum_{\lambda\in\Lambda\setminus\{0\}} \left(\frac{1}{(z+\omega_1-\lambda)^2} - \frac{1}{\lambda^2}\right) = \wp(z),$$

where the summation again is just a rearrangement of the summation in the original definition for $\wp(z)$ (as for all $\lambda \in \Lambda \Leftrightarrow (\omega_1 - \lambda) \in \Lambda$). One can see that the same holds if we replace ω_1 by ω_2, and hence $\wp(z+\lambda) = \wp(z)$, $\forall\lambda \in \Lambda$. One can similarly show that this property holds for $\wp'(z)$ too. ■

Note: Such meromorphic and doubly periodic functions are called *elliptic functions*. Elliptic functions are inverse functions of *elliptic integrals*, which is a class of integrals that was encountered while calculating the arc length of an ellipse. As we shall also see, elliptic curves have a close relationship to the Weierstrass-$\wp$ elliptic function–hence where they get their name from!

Lemma 7.3.3. *An entire elliptic function is constant.*
Proof. Assume we have an elliptic function f that is entire. Furthermore, as it is continuous, it is bounded over the closure of a *period parallelogram* (the area enclosed by $\{\mu\omega_1 + \nu\omega_2 : 0 \leq \mu, \nu \leq 1\}$)$\Rightarrow$ it is bounded over all of $\mathbb{C}$ by periodicity $\Rightarrow$ By *Liouville's Theorem*, as f is a bounded and entire function, it must be constant. ■

We can now use this lemma to prove an important property of the Weierstrass-$\wp$

function.

Proposition 7.3.1. *The Weierstrass-$\wp$ function satisfies the following differential equation:*

$$\wp'(z)^2 - 4\wp(z)^3 + g_1\wp(z) = g_2$$

where g_1, g_2 are constants that depend on ω_1 and ω_2.

Proof. Firstly, one can easily calculate the *Laurent* series of $\wp$ centered around $z = 0$ to give:

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

where G_{2k+2} directly depends on the periods ω_1 and ω_2 for all k.[1] This enables one to write out the first few terms comprising the *principal* part in the Laurent series of the following functions:

$$\begin{aligned}\wp(z) &= z^{-2} + \ldots..,\\ \wp(z)^3 &= z^{-6} + 9G_4z^{-2} + \ldots..,\\ \wp'(z)^2 &= 4z^{-6} - 24G_4z^{-2} + \ldots..,\end{aligned}$$

where we can see that through an appropriate choice of a constant g_1 (will depend on G_{2k+2} and hence on ω_1 and ω_2), one gets that the principal part in the Laurent series of $P(z) = \wp'(z)^2 - 4\wp(z)^3 + g_1\wp(z)$ vanishes$\Rightarrow$ $P(z)$ is analytic at $z = 0$. It is also easy to see that $P(z)$ is an elliptic function with the same periods ω_1 and ω_2, and has inherited analyticity at all $z \in \mathbb{C} \setminus \Lambda$. As it is analytic at $z = 0$, by periodicity, it is also analytic at all $z \in \Lambda$, and hence is entire. Thus, by the above lemma, $P(z) = g_2$ for some appropriate constant g_2 and we are done. ■

Now we move prove the main topological characterization of elliptic curves.

Theorem 7.3.1. *Every elliptic curve is topologically equivalent to the torus.*
Proof. We can see by the above corollary that given a certain lattice Λ, the related Weierstrass-$\wp$ function and its derivative satisfy an equation identical to the Weierstrass Normal form, i.e, for all z we have $(\wp(z), \wp'(z), 1)$ lies in an elliptic curve of appropriate coefficients determined by Λ. Thus we can define the following well-defined map:

$$\Phi : \mathbb{C}/\Lambda \overset{\text{hom}}{\cong} \tau \to E \subseteq \mathbb{P}^2(\mathbb{C})$$

such that,

$$\Phi(\bar{z}) = \begin{cases} (\wp(z) : \wp'(z) : 1) & \text{if } \bar{z} \neq 0 \\ [0:1:0] & \text{if } \bar{z} = 0 \end{cases}.$$

The proof that this function is a *biholomorphy* extensively utilises techniques from complex analysis, and thus, in interest of not diverting attention from the topic at hand, it is only sketched here:
Firstly, one can use the cubic polynomial analogous to the differential equation from Proposition 7.3.1 to prove that $\wp'(z)$ has only three roots at ω_1, ω_2, and $\omega_3 = \dfrac{\omega_1 + \omega_2}{2}$. Then one can use this to prove the injectivity of Φ where the inputs are $\text{mod}(\Lambda)$. Surjectivity of Φ can be proved primarily using Lemma 7.3.1. Finally, one can show that $\Phi'(\bar{z})$ does not vanish by showing $\wp''(\omega_i) \neq 0$ for all $i = 1, 2, 3$, and hence use the *inverse function theorem for holomorphic maps* to show that a bijective holomorphic inverse of Φ exists. This concludes that Φ is a biholomorphy. One can even prove that this map is a *group homomorphism*, where the group structure on E is induced by the chord-and-tangent group law, and the natural *Lie group* structure is imposed on the torus τ. Details of the proof can be found here.[1] This gives us that elliptic curves are not rational, and instead have a parameterisation through the torus. ■

References

[1] Béatrice; I. Chetard. *"Elliptic curves as complex Tori"*. University of Western Ontario, Oct 2017.

[2] William Fulton. *"Algebraic curves: An Introduction to Algebraic Geometry"*. Addison-Wesley, 2008.

[3] Pawel Gladki. *"Resultants and the Bezout theorem"*. University of Silesia in Katowice.

[4] Joseph H. Silverman and John Torrence Tate. *"Rational points on elliptic curves"*. Springer, 2015.

[5] Terence Tao. *"Pappus's theorem and elliptic curves"*. July 2011.

[6] Wikipedia. *"Cayley-Bacharach Theorem"*. Aug 2022.