Algebraic Geometry

Zandi

November 19, 2013

THIS IS A DRAFT. Expect inaccuracte and incomplete information.

Introduction

Algebraic Geometry is a field of mathematics with roots as far back as at least the 19^{th} century, and with major advancement and applications in recent years. At its core, Algebraic Geometry is concerned with studying the sets of zeroes of a system of polynomials, in particular their algebraic structure. Though real polynomials are surely the first that come to mind, much of the power in Algebraic Geometry comes from the generalization to polynomials with coefficients in arbitrary fields.

The undergraduate mathematics student would hopefully find this paper accessible, but experience with algebra and geometry would help. A "Basics" section is included, but will not be exhaustive. As unhelpful as it seems, it's recommended to do independent research as necessary using Wikipedia, YouTube (videotaped lectures) and the referenced textbooks.

This paper draws heavily from "Undergraduate Algebraic Geometry" by Miles Reid, with the primary addition being annotated proofs. Where Reid's proofs left details to the reader, these details are mostly provided, although the proofs remain the same.

1 Basics

The undergraduate math student would be well prepared for this paper with prior experience in algebra, linear algebra and geometry. However, there are still various concepts and terms which may be unfamiliar. These will be briefly discussed here before the main content, which will make heavy use of them. Note that a central concept to algebraic geometry, the *variety*, is not covered here, nor elsewhere in this paper. It seems to be abstract enough that such introductory materials don't bother with it. Despite this, the following should provide enough background for the following sections. Let's begin with what is surely the most widely used and foundational concept; *Projective Space*.

Definition 1.1. *Given a Field k, the* Projective Space of Degree n over k*, denoted* $\mathbb{P}_k^n$ *is the quotient* $(k^{n+1} \setminus \{\mathbf{0}\})/\sim$*, where* $\sim$ *is the equivalence relation defined as*

$$(x_0, ..., x_n) \sim (y_0, ..., y_n) \text{ if } \exists \lambda \in k \text{ s.t. } \lambda \neq 0, (x_0, ..., x_n) = (\lambda y_0, ..., \lambda y_n)$$

Given this, points in projective space are often denoted $P = [x_0 : ... : x_n]$*, with the colons and brackets indicating this is an equivalence class. So then,* $[y_0 : ... : y_n] = P = [x_0 : ... : x_n]$ *if* $(y_0, ..., y_n) \sim (x_0, ..., x_n)$*.*

The definition is abstract to purposely highlight the fact that, given a field k we can create a projective space. Effectively, the projective space is the set of all lines in k^{n+1} through the origin. This is also why the projective space has one fewer dimension than its corresponding vector space.

So, the "points" in projective space are lines in the corresponding vector space. Another interesting feature of projective space is that parallel lines intersect at a "point at infinity". This can be thought of as making partitions of lines in the projective space pased on parallelism, as if we were defining an equivalence relation. Now, each equivalence class is assigned a unique "point at infinity" that each line in the equivalence class intersects. Thus, if two lines are parallel, they intersect at some point at infinity. Likewise, if two lines aren't parallel, they'll have their own points at infinity, but they won't be the same, thus they will only have the usual intersection normally expected of non-parallel lines.

This may seem very strange, but can be illustrated with a stereographic projection. Suppose we're in $\mathbb{R}^3$, and picture two things: the plane $z = 1$ and a sphere of radius 1 centered at the origin. Now, we can map any point p on $z = 1$ to a unique point on the upper hemisphere of our sphere; simply note that the line passing through p and the origin $(0, 0, 0)$ intersects the specified hemisphere precisely once at some point q. Knowing this, we can see that lines on our plane $z = 1$ are mapped to great circles on our sphere. In the case of two parallel lines, they will never intersect in $z = 1$, but the great circles they're mapped to will approach a point of intersection on the equator of the hemisphere.

Definition 1.2. *A function* $f(x)$ *is* Homogenous of Degree n *if, for some constant* λ*, we have* $f(\lambda x) = \lambda^n f(x)$*. If* f *is a homogenous polynomial of degree n, it is known as a* form of degree n.

Homogenous functions are particularly useful when considering their sets of zeroes in projective space. If f is homogenous of degree n, and some point $x = (x_0, ..., x_n)$ is a zero of f, then $f(\lambda x) = \lambda^n f(x) = \lambda^n 0 = 0$. Thus, we can say that, if f is homogenous, then we can indeed have zeroes of f in $\mathbb{P}^n_k$, assuming k is algebraically closed.

Definition 1.3.

$$S_d = \{ \textit{ forms of degree } d \textit{ in } (X, Y, Z)\}$$

So, any element F of S_d can be written in a unique way as:

$$F = \Sigma_{\substack{i+j+k'=d \\ i,j,k'>0}} a_{i,j,k'} X^i Y^j Z^{k'},\ a_{i,j,k'} \in k$$

So, S_d has a basis of

$$\begin{aligned}
&\{X^d, X^{d-1}Y, X^{d-2}Y^2, \dots \\
&\ X^{d-1}Z, X^{d-2}YZ, X^{d-3}Y^2Z, \dots \\
&\ X^{d-2}Z^2, X^{d-3}YZ^2, X^{d-4}Y^2Z^2, \dots \\
&\ \vdots \\
&\ XZ^{d-1}, YZ^{d-1} \\
&\ Z^d\}
\end{aligned}$$

Also, it can be seen that $\dim S_d = \binom{d+2}{2}$. On its own S_d isn't incredibly interesting, but we can make use of it when reasoning about certain sets of geometric objects.

Definition 1.4. *for $p_1, \dots, p_n \in \mathbb{P}^2$, let*

$$S_d(p_1, \dots, p_n) = \{F \in S_d :\ F(p_i) = 0,\ i = 1, \dots, n\}$$

Here, for example, we can augment S_d with specific points to define a set of all forms which are zero at those points. As we will see, zeroes of forms define geometric figures, so reasoning about forms in these sets is very useful for considering various kinds of intersections, an important tool for various proofs.

Definition 1.5. *A* line *in $\mathbb{P}^2$ is defined as the points for which some linear form $aX + bY + cZ$ is zero. This is notated*

$$L : (aX + bY + cZ = 0)$$

As an example, consider S_1, the set of all linear forms in $\mathbb{R}^3$. If $F \in S_1$ then $F = aX + bY + cZ$, so consider $L : (F = 0)$, and examine some point $p_0 = (X_0, Y_0, Z_0) \in L$ with $X_0 \neq 0, Y_0 \neq 0, Z_0 \neq 0$. $p_0 \in L$ so $F(p_0) = aX_0 + bY_0 + cZ_0 = 0$, which is a linear equation in 3 variables. None of the coefficients of p_0 are zero, so we can easily determine one of our coefficients is dependent on the others, thus, $S_1(p_0) \cong \mathbb{R}^2$, hence $\dim S_1(p_0) = 2$.

Definition 1.6. *A* Projective Transformation *on* $\mathbb{P}^2_{\mathbb{R}}$ *is a transformation of the form*

$$T(x) = Mx$$

where x *is some point in* $\mathbb{P}^2_{\mathbb{R}}$ *in homogenous coordinates in vector form, and* M *is a non-singular* 3×3 *matrix.*

More explicitly, if we restrict ourselves to $\mathbb{R}^2 \subset \mathbb{P}^2_{\mathbb{R}}$ (eg: the $Z = 1$ plane) then we can think of this as

$$\begin{bmatrix} x \\ y \end{bmatrix} \mapsto (A \begin{bmatrix} x \\ y \end{bmatrix} + B)/(cx + dy + e)$$

when $cx + dy + e \neq 0$. Thus, we can define the matrix M as follows:

$$M = \left[\begin{array}{cc|c} & A & & B \\ \hline c & & d & e \end{array}\right]$$

Interestingly, this is a somewhat subtle way of demonstrating that certain non-linear transformations (projective and affine translation) in n dimensions can actually be achieved using linear transformations in $n + 1$ dimensions.

2 Conic Sections

Conic sections provide perhaps the simplest geometric figures to study in algebraic geometry. They are fairly well understood within $\mathbb{R}^2$, and extend quite beautifully into $\mathbb{P}^2$. One example of this is examining the classification of conics in both $\mathbb{R}^2$ and $\mathbb{P}^2$. While both have their degenerate cases, it's interesting to note that in $\mathbb{R}^2$ there are 3 non-degenerate cases of a conic section; the ellipse, hyperbola, and parabola. However, in $\mathbb{P}^2$ these can all be described in a single non-degenerate case, thanks to the point at infinity of projective space. Also, algebraic geometry can inform the historically interesting execercise of finding rational or integer roots for the pythagorean equation $X^2 + Y^2 = Z^2$.

However, we will only briefly cover conic sections, and even then primarily for their application to forthcoming sections. Let's begin by defining what a conic actually is.

Definition 2.1. *A* Conic *in* $\mathbb{R}^2$ *is a plane curve given by the quadratic equation*

$$q(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0$$

To "adapt" this definition into projective space $\mathbb{P}^2$, we simply note that the inhomogenous polynomial q has an associated homogenous polynomial

$$Q(X, Y, Z) = aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2$$

Miles Reid recommends thinking about this as a bijection $q \leftrightarrow Q$ by

$$q(x, y) = Q(\frac{X}{Z}, \frac{Y}{Z}, \frac{Z}{Z}),\ Z \neq 0$$

Thus, a conic in $\mathbb{P}^2$ would be determined by the zeroes of Q.

Theorem 2.1. *Let* k *be any field of characteristic* $\neq 2$*. Then, any quadratic form* Q *in* (X, Y, Z) *has an associated* 3×3 *symmetric matrix* A *s.t.*

$$x^T Ax = Q(X, Y, Z),\ x = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

explicitly, if

$$Q(X, Y, Z) = aX^2 + 2bXY + cY^2 + 2dXZ + 2eYZ + fZ^2$$

Then

$$A = \begin{bmatrix} a & b & d \\ b & c & e \\ d & e & f \end{bmatrix}$$

and the quadratic form (and hence the conic it defines) is non-degenerate if the matrix A *is non-degenerate (non-singular).*

Note that the matrix A from the above theorem is symmetric. Thus, we can apply the Spectral Theorem to see that we can diagonalize it using some orthogonal matrix. This effectively allows us to transform any non-degenerate quadratic form into a homogenous quadratic form through a change of basis.

Theorem 2.2. *Let Q be a quadratic form of X, Y, Z. Then, there exists a change of basis $(X, Y, Z) \mapsto (X', Y', Z')$ s.t. $Q(X, Y, Z) = Q'(X', Y', Z')$ where*

$$Q'(X', Y', Z') = \lambda_1 X'^2 + \lambda_2 Y'^2 + \lambda_3 Z'^2$$

As a corollary, all non-degenerate conics in $\mathbb{P}^2$ are projectively equivalent to the conic defined by $XZ = Y^2$. That is, there is some projective transformation which takes an arbitrary conic C to the conic defined by $XZ = Y^2$.

Proof. Q is a quadratic form, thus Q has an associated symmetric matrix A s.t. $Q(x) = x^T A x$. As A is symmetric, the Spectral Theorem gives that

$$\exists P : \ P \text{ orthogonal}, \ P^T A P \text{ is diagonal}$$

and in fact, the diagonal entries of $B = P^T A P$ are the eigenvalues of A. Thus, it is easy to show, using the transformation $x = Px'$, that

$$Q(X, Y, Z) = x^T A x = (Px')^T A P x' = x'^T P^T A P x' = x'^T B x'$$

Now, letting the eigenvalues of A be $\lambda_1, \lambda_2, \lambda_3$ we see that

$$x'^T B x' = \lambda_1 X'^2 + \lambda_2 Y'^2 + \lambda_3 Z'^2 = Q'(X', Y', Z')$$

Thus, $Q(X, Y, Z) = Q'(X', Y', Z')$. □

Thus, conic sections in $\mathbb{P}^2$ have an interesting sort of unifying characteristic when regarded under projective transformations. Not only is there one case of a non-degenerate conic instead of 3, but any non-degenerate conic is ultimately just a projective transformation of $XZ = Y^2$!. This will come in handy in just a few pages.

3 Bezout's Theorem

One of the most beautiful and powerful theorems in algebraic geometry is Bezout's Theorem. With it we can very precisely link the intersections of geometric structures with the degree of their defining forms, and characterize their intersection. This is quite useful in proofs, as various kinds of intersections occur quite frequently. To start, we'll explore some of the properties of homogenous forms in 2 variables, and the explicit connection between these forms and their associated non-homogenous polynomials. It may be useful here to consider the plane $Z = 1$ when in $\mathbb{P}^2$, and the line $V = 1$ when in $\mathbb{P}^1$.

Theorem 3.1. Homogenous Forms in 2 Variables*:*

Let $F(U, V)$ be a non-zero homogenous polynomial of degree d in U, V, with coefficients from a fixed field k. Then, we call F a form of degree d*, and can see that*

$$F(U,V) = a_d U^d + a_{d-1}U^{d-1}V + \cdots + a_i U^i V^{d-i} + \cdots + a_0 V^d$$

Now, if we apply $u = U/V$ and hold $V = 1$ we have an associated non-homogenous polynomial

$$f(u) = a_d u^d + a_{d-1}u^{d-1} + \cdots + a_i u^i + \cdots + a_0$$

This may not seem incredibly important, but this observation allows us to explore the zeroes of forms by examining the zeroes of relatively simpler polynomials. Similar constructions can be made for forms in more variables, but this two-variable form gives us a relatively simple example to explore.

Exploring this further, for some $\alpha \in k$

$$f(a) = 0 \iff (u-a)|f(u) \iff (U - \alpha V)|F(U,V)$$

As f must contain at least a linear term whose root is a, and thus applying $u = U/V$, we get $(U/V - a)$ and thus $(U - \alpha V)$. Now, holding $V = 1$ like earlier, we see that

$$(U - \alpha V)|F(U,V) \iff F(\alpha, 1) = 1$$

So, zeroes of the simpler polynomial f correspond to zeroes of F on $\mathbb{P}^1_k$ so long as $V \neq 0$. However, if F had a root of the form $(\beta, 0)$ then certainly by homogeneity F also has $(1, 0)$ as a root, giving:

$$F(1,0) = 0 \iff a_d \cdot 1 + a_{d-1} \cdot 1 \cdot 0 + \cdots + a_0 \cdot 0 = 0 \iff a_d = 0$$

which would force $deg f < d$, as then the highest power of U in F is strictly less than d. In this situation, $(1, 0)$ is effectively a "root at ∞" in $\mathbb{P}^1_k$.

Now, we can define the *multiplicity* of a zero of F as:

$$\text{The multiplicity of } f \text{ at the corresponding } a \in k \tag{i}$$
$$d - deg f \text{ if } (1,0) \text{ is the zero} \tag{ii}$$

Equivalently, the multiplicity of a zero of F at a point $(a,1)$ is the greatest power of $(U - \alpha V)$ dividing F, and at $(1,0)$ is the greatest power of V dividing F.

So, we have an interesting relationship between forms of 2 variables and their related polynomials in a single variable. Assuming k is algebraically closed, we are in fact bridging the zeroes of F in $\mathbb{P}^1_k$ with the zeroes of f in k by examining the restriction of F to the line $V = 1$. Later we'll see a similar approach where third-degree forms with roots $(X, Y, Z) \in \mathbb{P}^2_k$ are examined by restricting F to the $Z = 1$ plane, giving us some simpler f with roots in k^2.

Theorem 3.2. Bezout's Theorem*:*

If C and D are plane curves of degree m and n (respectively) then $C \cap D$ contains precisely mn points, provided:

The field we're working over is algebraically closed (i)
Points of intersection are counted with multiplicity (ii)
We work in $\mathbb{P}^2_k$ to account for points at infinity (iii)

Instead of proving the general theorem, we'll only cover a special case of particular importance to us; intersections involving lines and conics.

Theorem 3.3. *Let $L \subset \mathbb{P}^2_k$ be a line (respectively, $C \subset \mathbb{P}^2_K$ a non-degenerate conic) and $D \subset \mathbb{P}^2_k$ a curve defined by $D : (G_d(X, Y, Z) = 0)$ where G is a form of degree d in the 3 variables X, Y, Z. Also, assume that $L \not\subset D$ (resp. $C \not\subset D$). Then*

$$|L \cap D| \leq d$$

and respectively

$$|C \cap D| \leq 2d$$

And in fact, once accounting for multiplicity, points at infinity, and if k is algebraically closed, we have equality.

Proof. The line L is defined as the set of zeroes of some linear form λ; $L : (\lambda = 0)$ in X, Y, Z. Well, as a line we can certainly paramaterize L using

$$X = a(U, V),\ Y = b(U, V),\ Z = c(U, V)$$

where a, b, c are linear forms of U, V. As an example, if $\lambda = \alpha X + \beta Y + \gamma Z$ with $\gamma \neq 0$ then we could paramaterize L as

$$X = U,\ Y = V,\ Z = -\frac{\alpha}{\gamma}U - \frac{\beta}{\gamma}V$$

by simply noting that $\lambda = 0 \implies 0 = \alpha X + \beta Y + \gamma Z$ and solving for Z. If $\gamma = 0$ we have the simpler case of $0 = \alpha X + \beta Y$. Similarly, a non-degenerate conic can be parameterized as follows

$$X = a(U,V),\ Y = b(U,V),\ Z = c(U,V)$$

where a, b, c are quadratic forms in U, V. This is because C is a projective transformation of $XZ = Y^2$, which is can be parameterized by $(X, Y, Z) = (U^2, UV, V^2)$. Thus, C is given by

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = M \begin{bmatrix} U^2 \\ UV \\ V^2 \end{bmatrix}$$

Where M is a non-singular 3x3 matrix. Hence, C can be parameterized by quadratic forms a, b, c in U, V.

So, in order to find the points of intersection of L (resp. C) with D, we simply need to evaluate $G_d|_L = 0$ (resp. $G_d|_C = 0$) using the above parameterizations. Explicitly, to find the points of $L \cap D$ we want to find the solutions to

$$G_d(a(U,V), b(U,V), c(U,V)) = 0$$

Now we can see that, as G_d is a form of degree d in X, Y, Z, and a, b, c are forms of degree 1 (resp. 2) in U, V then by composition $G_d|_L$ is of degree d (resp. 2d) in U, V.

Now, if k is algebraically closed, then $G_d \in k[X, Y, Z]$ and so all roots of $G_d|_L$ are elements (U, V) of $k \times k$. Likewise, all roots of $G_d|_C$ are elements of $k \times k$. Thus, accounting for multiplicities and points at infinity, $G_d|_L$ has precisely d roots in (U, V) and $G_d|_C$ has precisely $2d$ roots in (U, V). Using the parameterizations a, b, c we can easily find the corresponding roots in $\mathbb{P}^2_k$.

Thus, accounting for multiplicities of zeroes and points at infinity, the intersection $L \cap D$ has d elements, and the intersection $C \cap D$ has $2d$ elements. Thus, the curve L (resp. C) meets D in precisely d (resp. $2d$) points. □

Now, we formally know that given two distinct lines in $\mathbb{P}^2$, they will intersect in precisely one point. Likewise, the intersection of a line with a conic that doesn't contain it will have precisely 2 points. This is a useful tool when combined with examining the dimension of S_d. For example, the intersection of any two conics $C_1,\ C_2$ has 4 points, so given 5 points, what do we know about the conics which lie on them? If no 4 of these 5 points are collinear, then in fact there is only one conic C which passes through all of them. This can be shown by assuming the contrary; that two distinct conics pass through such 5 points; and then examining the intersection of these conics. Another interesting consequence is that, with distinct $p_0, \ldots, p_n \in \mathbb{P}^2_{\mathbb{R}}$, then $\dim S_2(p_0, \ldots, p_n) \geq 6 - n$. This can be seen by considering some $Q \in S_2(p_0, \ldots, p_n)$, and treating each of $Q(p_i) = 0$ as a linear equation in 6 coefficients, since each p_i is fixed. Then we have a system of n equations in 6 variables, and we can easily apply linear algebra techniques.

4 Elliptic Curves

One of the more beautiful applications of algebra to geometry can be seen on elliptic curves. Here, it is in fact possible to form a group using points on non-singular cubic curves. Where previous material was primarily focused with algebra *of* geometric structures, homogenous polynomials and projective space, now we focus on algebra *on* a geometric structure. This is similar to the definition of the Dihedral group in that the structure of the object in question is fundamental to the structure of the group, but the group on the elliptic curve is more complicated. We'll begin by stating some theorems which will be used to prove that the structure which arises is indeed a group.

Theorem 4.1. *Let k be an infinite field, and let $p_1, \ldots, p_8 \in \mathbb{P}^2_k$ be distinct points. Additionally, suppose that no 4 of $p_1, \ldots, p_8$ are collinear, and no 7 lie on a non-degenerate conic (no 7 are con-conic). Then:*

$$\dim S_3(p_1, \ldots, p_8) = 2$$

That is, the set of all cubics which pass through $p_1, \ldots, p_8$ can in fact be considered a vector space, with a basis of the defining equations F_1, F_2 of the 2 cubic curves. Thus

$$D \in S_3(p_1, \ldots, p_8) \implies \exists \alpha, \beta : D = \alpha F_1 + \beta F_2$$

Theorem 4.2. Corrollary: *Let C_1, C_2 be two cubic curves whose intersection contains 9 distinct points; $C_1 \cap C_2 = \{p_1, \ldots, p_9\}$. Then, a cubic D which passes through $\{p_1, \ldots, p_8\}$ also passes through p_9.*

Proof. If 4 of the points were collinear on some line L, then each of C_1, C_2 contain L. by Bezout's Theorem, any intersection of C_1 (resp. C_2) with L has precisely $3 \cdot 1 = 3$ points. So, the only way to have more points of intersection is if the line L were contained in C_1 (resp. C_2). But then, $L \subset C_1 \cap C_2$, so $C_1 \cap C_2$ would contain infinitely many points, a contradiction. Thus, no 4 points of intersection can be collinear.

Likewise, no 7 points can be con-conic. Bezout's theorem forces precisely $3 \cdot 2 = 6$ points of intersection. Thus, if 7 points lied on a common conic E then $E \subset C_1 \cap C_2$, thus $C_1 \cap C_2$ has more than 9 points, a contradiction.

Thus, WLOG $\{p_1, \ldots, p_8\}$ satisfy the hypotheses of theorem 4.1, so we now know that

$$\dim S_3(p_1, \ldots, p_8) = 2$$

So, the defining equations F_1, F_2 of C_1, C_2 form a basis of $S_3(p_1, \ldots, p_8)$. Thus, the cubic D which passes through $\{p_1, \ldots, p_8\}$ is defined by some equation G $(D : (G = 0))$, thus $G \in S_3(p_1, \ldots, p_8)$ so $G = \alpha F_1 + \beta F_2$. But now, we know that $F_1(p_9) = 0 = F_2(p_9)$, thus $G(p_9) = \alpha \cdot 0 + \beta \cdot 0 = 0$, so D passes through p_9. □

Definition 4.1. Group Law on a Plane Cubic: *Suppose $k \subset \mathbb{C}$ is a subfield of $\mathbb{C}$, and $F \in k[X,Y,Z]$ is a cubic form defining a non-empty plane curve $\mathfrak{C} : (F = 0) \subset \mathbb{P}^2_k$. Additionally, assume that F satisfies the following:*

$$F \text{ is irreducible, so } \mathfrak{C} \text{ won't contain a line or conic} \tag{a}$$

$$\forall P \in \mathfrak{C},\ \exists!\ \text{line } L \subset \mathbb{P}^2_k \text{ s.t. } P \text{ is a repeated zero of } F|_L \tag{b}$$

Now, fix any point $O \in \mathfrak{C}$ and make the following construction:

$$\text{for } A \in \mathfrak{C},\ \text{let } \bar{A} \text{ be the third point of intersection of } \mathfrak{C} \text{ with } \overleftrightarrow{OA} \tag{i}$$

$$\text{for } A, B \in \mathfrak{C} \text{ let } R \text{ be the third point of intersection of } \mathfrak{C} \text{ with } \overleftrightarrow{AB} \text{ and define } A + B = \bar{R} \tag{ii}$$

Geometrically, the uniqueness in (b) says that $\mathfrak{C}$ should be non-singular (no cusps, self-intersections), and we can see that this line L is in fact the tangent line to $\mathfrak{C}$ at P. Likewise, (a) prevents somewhat degenerate cases.

As you may have noticed, we've defined an operation on points of this cubic curve $\mathfrak{C}$, so naturally we're curious what sort of structure then arises. It turns out that this actually defines an Abelian Group on $\mathfrak{C}$, as we will now prove.

Theorem 4.3. *The above construction (Definition 4.1) defines an Abelian Group $(\mathfrak{C}, +)$ with O as the identity element.*

Proof. Well, to prove this is an abelian group, we have a few conditions we must satisfy:

1. Well-definedness of the operation and inverses
2. Existence of an identity element
3. Existence of unique inverses
4. Commutativity
5. Associativity

Well-Definedness:
Let $P, Q \in \mathfrak{C}$. Then, we have two simple cases:

case 1: $P \neq Q$. Then $\exists! L \subset \mathbb{P}^2_k$ such that $L = \overleftrightarrow{PQ}$.

case 2: $P = Q$. Then, part (b) of the definition gives that $\exists! L \subset \mathbb{P}^2_k$ such that P is a repeated root of $F|_L$.

Note, however, that in both cases $F|_L$ is a cubic form in 2 variables. So, as $F|_L$ is a 3rd degree form, it has precisely 3 roots, 2 of which are the k-valued

points P and Q. Well, $P \in \mathbb{P}_k^2,\ Q \in \mathbb{P}_k^2$, so $F|_L$ is the product of 3 linear terms from $k[X,Y,Z]$. Thus, the third root of $F|_L$ is certainly defined, and must also be from $\mathbb{P}_k^2$, and of course from $\mathfrak{C}$.

So, given any two points on $\mathfrak{C}$, the line they determine intersects $\mathfrak{C}$ at some third point. Thus our construction, which relies on such a third point existing, is well defined. That is, Given any $A \in \mathfrak{C},\ \bar{A}$ is a unique element of $\mathfrak{C}$, and given any $A, B \in \mathfrak{C},\ A+B$ is a unique point of $\mathfrak{C}$.

Commutativity:
Well, need to show that $A+B = B+A$. Miles Reid chooses to "leave this to the reader", and likewise we won't elaborate on this. Simply note that $\overleftrightarrow{AB} = \overleftrightarrow{BA}$, so they share the same 3rd point of intersection with $\mathfrak{C}$.

Identity:
Let $A \in \mathfrak{C}$ be some arbitrary point of $\mathfrak{C}$, and consider $O + A$. Well, by our construction, we first find the third point of intersection of $\overleftrightarrow{OA}$ with $\mathfrak{C}$, which by (i) is $\bar{A}$. From here, to find $O + A$ we must now find the third point of intersection of $\overleftrightarrow{O\bar{A}}$ with $\mathfrak{C}$. However, note that $O,\ A,\ \bar{A}$ are all collinear. Thus, this third point of intersection of $\overleftrightarrow{O\bar{A}}$ with $\mathfrak{C}$ is A. Hence, $O + A = A,\ \forall A \in \mathfrak{C}$.

Inverses:
Let L be the line tanget to $\mathfrak{C}$ at O. That is, L is the unique line s.t. $F|_L$ has O as a repeated zero. Now, let $\bar{O}$ be the 3rd root of $F|_L$. Now, given any point $A \in \mathfrak{C}$, we can see that the third point of intersection of $\overleftrightarrow{A\bar{O}}$ with $\mathfrak{C}$ is the inverse of A.

Call this third point of intersection A'. Now, consider $A + A'$. By definition, $A,\ A',\ \bar{O}$ are all collinear, so the third point of intersection of $\overleftrightarrow{AA'}$ with $\mathfrak{C}$ is $\bar{O}$. Now, by how we defined $\bar{O}$, we know that the third point of intersection of $\mathfrak{C}$ with $\overleftrightarrow{O\bar{O}}$ is O, as O is a repeated root of this line. Thus, $A + A' = O$, so in the future we'll refer to such an A' as A^{-1}.

Finally, note that as A^{-1} was picked as the third point of intersection of $\mathfrak{C}$ with $\overleftrightarrow{A\bar{O}}$, it is well-defined.

Associativity:
Associativity is by far the most difficult part of this proof. We'll first prove Associativity for one case, and then reduce the general case to this special case.

Suppose that $A, B, C \in \mathfrak{C}$. We want to show that $(A+B)+C = A+(B+C)$. Well, in the construction of $(A+B)+C$ we use the 4 lines

$$L_1 : \overleftrightarrow{AB\bar{R}},\ L_2 : \overleftrightarrow{RO\bar{R}},\ L_3 : \overleftrightarrow{C\bar{R}S},\ L_4 : \overleftrightarrow{SOS}$$

Likewise, the construction of $A + (B + C)$ involves

$$M_1 : \overleftrightarrow{BCQ},\ M_2 : \overleftrightarrow{QOQ},\ M_3 : \overleftrightarrow{A\bar{Q}S'},\ M_4 : \overleftrightarrow{S'OS'}$$

Clearly, $(A+B)+C = A+(B+C) \iff \bar{S} = \bar{S}' \iff S = S'$. We'll prove $S = S'$ by inspecting the two cubics

$$D_1 = L_1 \cup M_2 \cup L_3 \text{ and } D_2 = M_1 \cup L_2 \cup M_3$$

Thus, by construction we have

$$\mathfrak{C} \cap D_1 = \{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S\}$$

and

$$\mathfrak{C} \cap D_2 = \{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S'\}$$

Now, assuming all 9 points of $\mathfrak{C} \cap D_1$ are distinct, then $\mathfrak{C}$ and D_1 satisfy the conditions of proposition 2.7 (TODO: add prop. 2.7 from book to earlier sections), so D_2 must pass through the 9th point S, which is only possible if $S' = S$. Hence, $\bar{S} = \bar{S}'$ and, so long as our construction involves 9 distinct points, $+$ is Associative.

Now, to extend to the more general case of points $A, B, C \in \mathfrak{C}$ which don't necessarily involve only distinct points in the construction of $(A + B) + C$ or $A + (B + C)$. We'll make use of some concepts from calculus here.

First, some useful lemmas:

Lemma 4.1. *$+$ is a continuous function. Thus, as the composition of continuous functions, both*

$$(A, B, C) \mapsto (A + B) + C$$

$$(A, B, C) \mapsto A + (B + C)$$

are continuous

Lemma 4.2. *$\forall A, B, C \in \mathfrak{C}, \exists A', B', C' \in \mathfrak{C}$ arbitrarily near A, B, C such that the 9 points $\{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S\}$ are distinct.*

Specifically, there exist sequences $(A_n), (B_n), (C_n)$ s.t.

$$A_n \to A,\ B_n \to B,\ C_n \to C \text{ as } n \to \infty.$$

Thus, $\forall n \in \mathbb{N}$ the previous limited proof of associativity gives that

$$(A_n + B_n) + C_n = A_n + (B_n + C_n) \qquad (*)$$

Now, by the continuity in Lemma 4.1, we have the following limits using the sequences from Lemma 4.2:

$$\lim_{n\to\infty} (A_n + B_n) + C_n = (A + B) + C$$

$$\lim_{n\to\infty} A_n + (B_n + C_n) = A + (B + C)$$

But, by the above noted equality (*) gained from Lemma 4.2, we know that

$$\lim_{n\to\infty} (A_n + B_n) + C_n = \lim_{n\to\infty} A_n + (B_n + C_n)$$

Thus, by uniqueness of limits

$$(A + B) + C = A + (B + C)$$

More specifically, we can see from Lemma 4.2 that the set of such points (A, B, C) where the 9 involved points of the construction are distinct is in fact dense in $\mathfrak{C} \times \mathfrak{C} \times \mathfrak{C}$. Thus, as the two functions from Lemma 4.1 agree on this dense set, they agree everywhere on $\mathfrak{C} \times \mathfrak{C} \times \mathfrak{C}$, giving us Associativity $\forall A, B, C \in \mathfrak{C}$.

Therefore, $(\mathfrak{C}, +)$ is an Abelian Group. □

It should be noted that the fact the curve is cubic is quite important. This allows us to have precisely 3 points of intersection when intersecting our curve with a line, letting us define a relatively natural operation based on this. On the contrary, a quartic curve would have 4 points of intersection with a line, and an increasing number of points if we were to consider intersections with conics and cubics, so it's even less clear how we would define an operation here to get a group. Likewise, intersections of a line with another line are so trivial it's hard to imagine such an interesting structure arising.

Also note curves of the form $y^2 = x^3 + ax + b$ fulfill the requirements of our theorem, and are symmetric about the x-axis. In practice, the identity O is taken to be the ideal point at infinity (since we are really in $\mathbb{P}^2_k \subset \mathbb{P}^2_{\mathbb{C}}$), allowing for all vertical lines to intersect O. As our curve tends towards infinity, it also intersects O, so everything is still well-defined. The benefit of this approach is that calculating inverses is trivial: $A = (x, y) \implies A^{-1} = (x, -y)$. Once we pair this with a field k with desirable number-theoretic properties, we enter the realm of cryptography using elliptic curves, and travel far outside the scope of this short paper.