BASIC ALGEBRAIC GEOMETRY AND THE 27 LINES ON A CUBIC SURFACE

SIMON LAZARUS

Abstract. We present an elementary proof of the fact that any nonsingular cubic surface in $\mathbb{P}^3$ over an algebraically closed field not of characteristic 2 will contain exactly 27 lines. During the course of this proof, we present a way to label these lines in terms of a fixed line l and another fixed line m which is disjoint from l in such a way that we can determine which of the 26 other lines a given line will intersect. In order to present the proof, we first develop without proof some of the basic theory of algebraic geometry and also prove several facts about quadric surfaces and lines in $\mathbb{P}^3$.

Contents

1. Preliminaries

Throughout this paper, let K be a field. We shall mostly be interested in the case where K is algebraically closed and not of characteristic 2, but to begin we can consider any field K.

1.1. Affine Algebraic Varieties.

Definition 1.1. Let C be any collection of polynomials in $K[x_1, \dots, x_n]$. Define the *affine algebraic variety associated to C* to be

$$\mathcal{V}(C) = \{p \in K^n : \forall f \in C, f(p) = 0\},$$

the common zero set of all polynomials in C. More generally, an *affine algebraic variety* is any subset of K^n of the form $\mathcal{V}(D)$ for some collection D of polynomials.

For the sake of brevity, we shall sometimes use the term *affine variety* or simply *variety* to describe an affine algebraic variety.

Intuitively, an affine algebraic variety is a subset of K^n which is "cut out" from K^n by some collection of polynomials.

Date: September 16, 2014.

It is easy to check that the finite union or arbitrary intersection of affine algebraic varieties is an affine algebraic variety. Specifically, the union of two varieties is given by

$$\mathcal{V}(\{f_i\}_{i\in I}) \cup \mathcal{V}(\{g_j\}_{j\in J}) = \mathcal{V}(\{f_i g_j\}_{i\in I, j\in J}) \tag{1.1}$$

and the intersection of arbitrarily many varieties associated to collections C_i of polynomials is given by

$$\bigcap_{i\in I} \mathcal{V}(C_i) = \mathcal{V}\left(\bigcup_{i\in I} C_i\right). \tag{1.2}$$

Additionally, the sets $K^n = \mathcal{V}(\emptyset)$ and $\emptyset = \mathcal{V}(1)$, where 1 denotes the constant polynomial with value 1, are clearly affine algebraic varieties. Thus, we can naturally place a topology on K^n.

Definition 1.2. The *Zariski topology* on K^n is the topology whose closed sets are the affine algebraic varieties in K^n. Under this topology, we denote K^n by $\mathbb{A}^n_K$, or simply $\mathbb{A}^n$ when the underlying field K is clear. $\mathbb{A}^n$ is called *Affine n-space*.

Any affine algebraic variety V is a subset of $\mathbb{A}^n$ and therefore inherits the subspace topology from $\mathbb{A}^n$. Under this topology, the closed sets of V are precisely the *subvarieties* of V, i.e. any subset of V which is the common zero set of some collection of polynomials on V.

We now describe a correspondence between varieties and ideals in the polynomial ring $K[x_1, \dots, x_n]$ which is of great importance.

Definition 1.3. Let $V \subseteq \mathbb{A}^n$ be an affine algebraic variety. Define the *ideal of V* to be

$$\mathcal{I}(V) = \{f \in K[x_1, \dots, x_n] : \forall p \in V, f(p) = 0\},$$

the set of polynomials vanishing on V.

The set $\mathcal{I}(V)$ is clearly an ideal of $K[x_1, \dots, x_n]$: the sum of polynomials vanishing on V also vanishes on V, and the product of a polynomial vanishing on V with any other polynomial must still vanish on V. Additionally, by definition $\mathcal{I}(V)$ is always a *radical* ideal. (Recall that the *radical* of an ideal I in a ring R is defined to be $\sqrt{I} = \{x \in R : x^n \in I \text{ for some } n \in \mathbb{Z}^+\}$ and that I is said to be *radical* if $I = \sqrt{I}$.)

We now observe that if V is any affine algebraic variety, then $V = \mathcal{V}(\mathcal{I}(V))$. For first, $V \subseteq \mathcal{V}(\mathcal{I}(V))$ is obvious. Second, let $p \in \mathcal{V}(\mathcal{I}(V))$. Then by definition for each $f \in \mathcal{I}(V)$ we have that $f(p) = 0$. So writing $V = \mathcal{V}(\{f_i\}_{i\in I})$, we certainly have that $f_i(p) = 0$ for each $i \in I$ since necessarily each f_i vanishes on V and hence is in $\mathcal{I}(V)$. That is, $p \in \mathcal{V}(\{f_i\}_{i\in I}) = V$.

We might now similarly expect that if I is any radical ideal of $K[x_1, \dots, x_n]$ then $I = \mathcal{I}(\mathcal{V}(I))$. As it turns out, this is not always the case: for example, if $K = \mathbb{R}$ and $I = (x^2 + 1)$ then we have that $\mathcal{V}(I) = \emptyset$ and hence $\mathcal{I}(\mathcal{V}(I)) = \mathbb{R}[x] \neq (x^2 + 1)$. However, if K is algebraically closed, then our conjecture is in fact true:

Hilbert's Nullstellensatz. *Suppose K is algebraically closed. Then for each ideal I of $K[x_1, \dots, x_n]$ we have that $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$. Thus, if I is radical then we have that $\mathcal{I}(\mathcal{V}(I)) = I$.*

For a proof, see [1]. Note that by definition, if V is any affine algebraic variety then $\mathcal{I}(V)$ is radical. Thus, when combined with the above observation that for any variety V we have $\mathcal{V}(\mathcal{I}(V)) = V$, the Nullstellensatz gives us a bijective correspondence between the set A of radical ideals in $K[x_1, \ldots, x_n]$ and the set B of affine algebraic varieties in $\mathbb{A}^n$. For we have functions $\mathcal{V} : A \to B$ and $\mathcal{I} : B \to A$ which are inverse to each other.

We now note that every affine algebraic variety can in fact be written as $\mathcal{V}(C)$ for some *finite* collection C of polynomials. This follows from the following theorem, whose proof also appears in [1].

Hilbert's Basis Theorem. *Let R be a Noetherian ring. Then the polynomial ring $R[x]$ is also Noetherian.*

Inductively, we see that if R is Noetherian, then $R[x_1, \ldots, x_n]$ is Noetherian. Since any field is trivially Noetherian, we thus have that $K[x_1, \ldots, x_n]$ is always Noetherian. So letting V be any affine algebraic variety in $\mathbb{A}^n$, we see that the ideal $\mathcal{I}(V)$ must be finitely generated; say $\mathcal{I}(V) = (f_1, \ldots, f_k)$. Therefore

$$V = \mathcal{V}(\mathcal{I}(V)) = \mathcal{V}((f_1, \ldots, f_k)) = \mathcal{V}(f_1, \ldots, f_k),$$

where the last equality follows from the fact that if $f_1, \ldots, f_k$ all vanish at a point $p \in \mathbb{A}^n$ then every polynomial in the ideal generated by $f_1, \ldots, f_k$ must also vanish at p.

Having defined our objects of interest, namely affine algebraic varieties, we now describe their morphisms.

Definition 1.4. Let $V \subseteq \mathbb{A}^m, W \subseteq \mathbb{A}^n$ be affine algebraic varieties. A *morphism of affine algebraic varieties* is a function $F : V \to W$ which is the restriction to V of some polynomial map $G : \mathbb{A}^m \to \mathbb{A}^n$ (that is, the restriction of a map $G = (g_1, \ldots, g_n)$ where each $g_i \in K[x_1, \ldots, x_m]$). Such a function is an *isomorphism* if it has an inverse $F^{-1} : W \to V$ which is also a morphism of affine algebraic varieties.

Since an affine algebraic variety is by definition simply the common zero set of some collection C of polynomials, we would expect polynomial maps to be the functions which preserve the structure in which we are interested. However, we cannot make this intuition rigorous under out initial notion of a variety as simply being a set corresponding to a collection of polynomials. For example, consider the varieties $V_1 \subseteq \mathbb{A}^1$ and $V_2 \subseteq \mathbb{A}^2$ given by $V_1 = \mathbb{A}^1 = \mathcal{V}(\emptyset)$ and $V_2 = \{(x, 0) : x \in K\} = \mathcal{V}(x_2)$. Clearly projection onto the first coordinate is an isomorphism of affine algebraic varieties from V_2 to V_1. However, no collection of polynomials cutting out V_1 from $\mathbb{A}^1$ can ever be equivalent to a collection of polynomials cutting out V_2 from $\mathbb{A}^2$: the only collections cutting out V_1 from $\mathbb{A}^1$ are the empty collection and the collection $\{0\}$ of the zero polynomial, while any collection cutting out V_2 from $\mathbb{A}^2$ must generate an ideal containing the nontrivial polynomial x_2. That is, although the two varieties V_1 and V_2 are isomorphic under our proposed definition of isomorphism, there is no way to make their defining collections of polynomials equivalent. To fix this problem, we introduce the following notion.

Definition 1.5. Let $V \subseteq \mathbb{A}^n$ be an affine algebraic variety. The *coordinate ring* of V is defined to be

$$K[V] = K[x_1, \ldots, x_n]/\mathcal{I}(V).$$

The coordinate ring of V is simply the collection of polynomials on V. For in $K[x_1, \ldots, x_n]/\mathcal{I}(V)$, two polynomials $f, g \in K[x_1, \ldots, x_n]$ (that is, two polynomials on $\mathbb{A}^n$) are equivalent precisely when their difference vanishes on V. That is, two polynomials on $\mathbb{A}^n$ are equivalent in $K[x_1, \ldots, x_n]/\mathcal{I}(V)$ precisely when the two polynomials are the same on V.

We note immediately that in our example above of the isomorphic varieties V_1 and V_2, we have that $\mathcal{I}(V_1) = \{0\}$ and $\mathcal{I}(V_2) = (x_2)$. Thus, the coordinate ring of V_1 is $K[x_1]/\{0\} \cong K[x_1]$, and the coordinate ring of V_2 is $K[x_1, x_2]/(x_2) \cong K[x_1]$. That is, the coordinate rings of V_1 and V_2 are isomorphic.

As it turns out, there is an equivalence of categories between the set of affine algebraic varieties and the set of finitely generated K-algebras without nilpotent elements. (Note that the coordinate ring of a variety V is always such a K-algebra). In this equivalence, a variety V is mapped to its coordinate ring $K[V]$. For a proof of this fact, see [3]. As a result of this equivalence, we can observe that two varieties V and W are isomorphic if and only if their corresponding coordinate rings are isomorphic as K-algebras. Therefore our initial notion of a morphism of affine algebraic varieties is justified.

Example 1.6. An *affine change of coordinates* is a map $\phi : \mathbb{A}^n \to \mathbb{A}^n$ given by $\phi(x) = Ax+b$, where A is an $n\times n$ invertible matrix, b and x are $n\times 1$ column vectors, and all matrix/vector entries are in K. It is clear that such a map is a polynomial map from $\mathbb{A}^n$ to $\mathbb{A}^n$ and hence is a morphism of affine varieties. Additionally, since A is invertible, ϕ has an inverse on $\mathbb{A}^n$ given by $\phi^{-1}(y) = A^{-1}y - A^{-1}b$, which is also an affine change of coordinates and hence is a morphism of affine varieties. Thus, we observe that an affine change of coordinates is an automorphism of the affine variety $\mathbb{A}^n$.

1.2. **Projective Algebraic Varieties.** We now describe the context in which we shall be performing most of our analysis in the rest of this paper. It is known as *projective space*, and mutatis mutandis it shares many of the properties of affine space.

Definition 1.7. Projective n-space $\mathbb{P}^n_K$, or just $\mathbb{P}^n$ for short, is the set $K^{n+1} \setminus \{(0, \ldots, 0)\}$ modulo the following equivalence relation: if $x \in K^{n+1}$ is a nonzero scalar multiple of $y \in K^{n+1}$, then x and y are equivalent. We thus write points of $\mathbb{P}^n$ in *homogeneous coordinates*: The point denoted $(x_0 : x_1 : \ldots : x_n)$ denotes the equivalence class of the point $(x_0, x_1, \ldots, x_n)$.

We now wish to define varieties in projective space. It is clear that we cannot do so in precisely the same manner as before: the "zero set" of a polynomial in general need not be well-defined in projective space since, for example, the polynomial $y - x + 1$ has $(1, 0)$ as a zero point but does not have the equivalent point $(2, 0)$ (under the above equivalence relation) as a zero point. However, if we restrict our attention to *homogeneous* polynomials, then this problem no longer exists. Recall that a polynomial f is homogeneous (of degree d) if there is some $d \in \mathbb{N}$ such that in any given monomial of f, the sum of the exponents on the variables in the monomial is d. Such a polynomial is also called a *form* of degree d.

To see that the zero set in $\mathbb{P}^n$ of a homogeneous polynomial is well-defined, let f be homogeneous of degree d and let $c \in K$. Then for each $(x_0, \ldots, x_n) \in K^{n+1}$ we have that $f(cx_0, \ldots, cx_n) = c^d f(x_0, \ldots, x_n)$ since we can factor out a c^d from each monomial of f. So if $c \neq 0$, then we see that $f(cx_0, \ldots, cx_n) = 0$ if and only if $f(x_0, \ldots, x_n) = 0$. Thus, we can make the following definition:

Definition 1.8. Let C be any collection of homogeneous polynomials in $K[x_1, \ldots, x_n]$. The *projective algebraic variety associated to* C is

$$\mathcal{V}(C) = \{p \in \mathbb{P}^n : \forall f \in C, f(p) = 0\}.$$

More generally, a *projective algebraic variety* is any subset of $\mathbb{P}^n$ of the form $\mathcal{V}(D)$ for some collection D of homogeneous polynomials.

As before, we shall often replace the term "projective algebraic variety" by the simpler term *projective variety* or even the term *variety* when the context is clearly projective and not affine.

As we might expect, in addition to the definition of varieties, there are several other similarities between affine and projective spaces.

Definition 1.9. Let $V \subseteq \mathbb{P}^n$ be a projective algebraic variety. The *(homogeneous) ideal of* V is

$$\mathcal{I}(V) = \{f \in K[x_0, \ldots, x_n] : \forall p \in V, f(p) = 0\}.$$

Note that since a point in $\mathbb{P}^n$ is in fact an equivalence class of points of K^{n+1}, the above means that for *any* choice of representative $(y_0, \ldots, y_n)$ for the point $p = (x_0 : \ldots : x_n)$, we must have that $f(y_0, \ldots, y_n) = 0$.

As before, it is easy to observe that for each projective variety V, we have that $\mathcal{I}(V)$ is a radical ideal and that $\mathcal{V}(\mathcal{I}(V)) = V$. Additionally, since any $f \in \mathcal{I}(V)$ must vanish on *any* representative of each point $p \in V$, it is clear that there is always a set of *homogeneous* polynomials which generate $\mathcal{I}(V)$ in $K[x_0, \ldots, x_n]$. This suggests the following result.

Homogeneous Nullstellensatz. *Suppose K is algebraically closed. If I is a radical ideal of $K[x_0, \ldots, x_n]$ which has a set of homogeneous generators and if $I \neq (x_0, x_1, \ldots, x_n)$, then $\mathcal{I}(\mathcal{V}(I)) = I$.*

The reason for the exclusion of the ideal $(x_0, \ldots, x_n)$ is that this ideal cuts out the single point $(0, \ldots, 0)$ from K^{n+1}, and by definition $(0 : \ldots : 0)$ is *not* an element of $\mathbb{P}^n$. As a consequence of the above, we observe that if K is algebraically closed then there is a bijective correspondence between the projective varieties in $\mathbb{P}^n$ and the homogeneously generated radical ideals of $K[x_0, \ldots, x_n]$, excluding the ideal $(x_0, \ldots, x_n)$.

As before, we also have that the set of projective varieties in $\mathbb{P}^n$ is closed under finite unions and arbitrary intersections. Thus, we can define the *Zariski topology* on $\mathbb{P}^n$ by making the projective varieties into the closed sets.

Example 1.10. Fix $i \in \{0, 1, \ldots, n\}$. Let $V_i = \mathcal{V}(x_i) = \{(x_0 : \ldots : x_n) : x_i = 0\}$. The complement of V_i in $\mathbb{P}^n$ is the set $U_i := \{(x_0 : \ldots : x_n) : x_i \neq 0\}$, which by definition is open in the Zariski topology. By dividing by x_i (which is always nonzero in U_i), we can express U_i as

$$U_i = \left\{ \left(\frac{x_0}{x_i} : \ldots : \frac{x_{i-1}}{x_i} : 1 : \frac{x_{i+1}}{x_i} : \ldots : \frac{x_n}{x_i} \right) \;\middle|\; x_0, \ldots, x_n \in K, x_i \neq 0 \right\}.$$

We thus see that each point of U_i has a unique representative in K^{n+1} of the form $(y_0, \ldots, y_{i-1}, 1, y_{i+1}, \ldots, y_n)$ for some $y_0, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n \in K$. By choosing such representatives, we can thus identify U_i with the set of all points in K^{n+1}

whose ith coordinate is 1; that is, we can identify U_i with K^n. In fact, in a more precise sense we can identify each set U_i with $\mathbb{A}^n$, but for our purposes it will suffice to know simply that $\mathbb{P}^n$ is covered by the $n+1$ open sets $U_0, \ldots, U_n$.

Definition 1.11. Let $V \subseteq \mathbb{P}^m, W \subseteq \mathbb{P}^n$ be projective algebraic varieties. A function $F : V \to W$ is a *morphism of projective varieties* if for each $p \in V$, there exist homogeneous polynomials $f_0, \ldots, f_n \in K[x_0, \ldots, x_m]$ all of the same degree d and there exists a Zariski open neighborhood $U \subseteq V$ of p such that for all $x \in U$, (i) not all of $f_0(x), \ldots, f_n(x)$ are zero and (ii) $F(x) = (f_1(x) : \ldots : f_n(x))$.

Note that in the above definition, the polynomials we choose can vary with p. That is, a morphism of projective varieties need only be *locally* polynomial.

Example 1.12. A *projective change of coordinates* is a map $\phi : \mathbb{P}^n \to \mathbb{P}^n$ given by $\phi(x) = Ax$, where $A \in \mathrm{GL}_{n+1}(K)$ and x is considered as an $(n+1)\times 1$ column vector. Such a map is indeed well-defined: for suppose that a point $p \in \mathbb{P}^n$ is represented by $x \in K^{n+1}$, where not all of the coordinates of x are zero. Then since A is invertible and hence has trivial kernel, we see that the coordinates of $\phi(x) = Ax$ in K^{n+1} cannot all be zero, meaning $\phi(x)$ does indeed define a representative for a point in $\mathbb{P}^n$. Additionally, for each $c \in K$, we see that $\phi(cx) = A(cx) = cAx = c\phi(x)$, so that in $\mathbb{P}^n$ the points $\phi(x)$ and $\phi(cx)$ are equivalent. That is, ϕ sends *any* representative of the point p to the same point.

It is clear that a projective change of coordinates ϕ is a polynomial map from $\mathbb{P}^n$ to $\mathbb{P}^n$ and hence is a morphism of projective varieties. Additionally, ϕ has an inverse change of coordinates given by $\phi^{-1}(x) = A^{-1}(x)$. Thus, a projective change of coordinates is an automorphism of the projective variety $\mathbb{P}^n$.

The definition of a morphism of projective varieties is motivated similarly to the definition of a morphism of affine varieties. But, in projective space, it is no longer the case in general that two isomorphic (projective) varieties V and W will have isomorphic coordinate rings. (For an example, see [3], pages 46-47.) However, it *is* true that two projective varieties which are equivalent up to a projective change of coordinates will have isomorphic coordinate rings. Additionally, two projective varieties will always be isomorphic if their coordinate rings are isomorphic. Since changes of coordinates will be the only morphisms which we shall tend to employ, we shall not worry further about the subtleties of coordinate rings.

Before carrying on, we present a few basic definitions and facts about projective space which are motivated by their analogues in affine space.

Definition 1.13. A *hypersurface* of degree d is a subset of $\mathbb{P}^n$ cut out by a single homogeneous polynomial of degree d. A *hyperplane* is a hypersurface of degree 1. In $\mathbb{P}^3$, a hyperplane is simply called a *plane*.

Any plane in $\mathbb{P}^3$ is isomorphic as a projective variety to $\mathbb{P}^2$. In fact, we can always change coordinates in such a way that the defining linear form of a given plane in $\mathbb{P}^3$ is simply the form x_3; that is, we can consider a plane as simply the set of points $(x_0 : x_1 : x_2 : x_3)$ with $x_3 = 0$.

In order to avoid going into too much detail, we shall take a *line* in $\mathbb{P}^3$ to mean a projective variety $l \subseteq \mathbb{P}^3$ which can be defined after a suitable change of coordinates by $l = \mathcal{V}(x_2, x_3)$. This makes sense: such a "line" is simply the intersection of the plane $\mathcal{V}(x_3)$ with the plane $\mathcal{V}(x_2)$. Similarly, a *line* in $\mathbb{P}^2$ is simply a hyperplane of $\mathbb{P}^2$, i.e. the zero set of a single linear form on $\mathbb{P}^2$.

One of the principal reasons to work in projective space as opposed to affine space is that, assuming the field in which we are working is algebraically closed, projective varieties always intersect in the "correct number" of points. This notion is captured in a more precise sense by Bézout's Theorem, but for our purposes we shall only need the following.

Proposition 1.14. *(1) In a projective plane, two distinct lines l_1, l_2 always intersect at a unique point. (2) In $\mathbb{P}^3$, if P is a plane and l is a line such that $l \nsubseteq P$ then l intersects P at a unique point.*

Proof. (1) By a suitable change of coordinates, we can take the projective plane to be $\mathbb{P}^2$. Since $l_1 \neq l_2$, by another suitable change of coordinates we can take l_1 to be $\mathcal{V}(x_2)$ and take l_2 to be $\mathcal{V}(x_1)$. Therefore the point $(1:0:0)$ is the unique point in $l_1 \cap l_2$.

(2) Since $l \nsubseteq P$, by a suitable change of coordinates we can take $P = \mathcal{V}(x_3)$ and $l = \mathcal{V}(x_1, x_2)$. Thus, $(1:0:0:0)$ is the unique point in $l \cap P$. □

We shall also frequently find the following fact to be useful:

Proposition 1.15. *Let $f \in K[x, y]$ be a nonzero homogeneous polynomial of degree d. Then f has at most d zeros in $\mathbb{P}^1$. If K is algebraically closed, then f has exactly d zeros in $\mathbb{P}^1$ when these zeros are counted with multiplicity.*

Proof. The points of $\mathbb{P}^1$ are all points of the form $(a:1)$ for $a \in K$ along with the single "point at infinity" $(1,0)$. Thus, the notion of multiplicity of a root of f is very natural: for any root of the form $(a:1)$, the multiplicity of said root is simply the highest power of $(x - ay)$ which divides f (for when we substitute $y = 1$, this is the usual definition); and if f has $(1:0)$ as a root, then the multiplicity of this root is simply the highest power of y dividing f.

Now let k be the multiplicity of the point $(1:0)$ as a root of f, where this multiplicity is 0 if $(1:0)$ is not a root of f. Let g be the (no longer necessarily homogeneous) polynomial in one variable obtained from f by substituting $y = 1$. Then since f is homogeneous of degree d, by definition we have that $\deg(g) = d - k$. Now since g is a polynomial in $K[x]$ of degree $d - k$, we know that g has at most $d - k$ roots in K and has exactly $d - k$ roots counted with multiplicity when K is algebraically closed. Combining all of the above facts with the definition of multiplicity presented above gives the desired result. □

1.3. **Irreducibility and Nonsingularity.**

Definition 1.16. Let V be a variety, affine or projective. We say that V is *reducible* if there exist nonempty subvarieties $V_1, V_2 \subseteq V$ such that $V_1 \neq V_2$ and $V = V_1 \cup V_2$. Otherwise, V is said to be *irreducible*.

Since we know by Equation 1.1 that $\mathcal{V}(f) \cup \mathcal{V}(g) = \mathcal{V}(fg)$, we see that a hypersurface is irreducible precisely when its defining polynomial is some power of an irreducible polynomial. More generally, one can see that a variety is irreducible precisely when its corresponding radical ideal is prime.

We now move on to the other main property of a variety in which we shall be interested, namely nonsingularity. Before defining it, we briefly discuss *tangent spaces*.

Definition 1.17. Let $V \subseteq \mathbb{A}^n$ be an affine variety and let $p \in V$. The *tangent space* to V at $p = (p_1, \ldots, p_n)$ is the affine variety

$$T_pV = \bigcap_{f \in \mathcal{I}(V)} \mathcal{V}\left(\sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(p) \cdot (x_i - p_i)\right),$$

that is, the intersection over all polynomials vanishing on V of the "linear part at p" of the variety corresponding to that polynomial.

Note that in the above definition, the partial derivatives $\frac{\partial f}{\partial x_i}$ are defined purely algebraically, not analytically. We also have an analogous definition of the tangent space of a projective variety:

Definition 1.18. Let $V \subseteq \mathbb{P}^n$ be a projective variety and let $p \in V$. The *tangent space* to V at p is the projective variety

$$T_pV = \bigcap_{f \in \mathcal{I}(V)} \mathcal{V}\left(\sum_{i=0}^{n} \frac{\partial f}{\partial x_i}(p) \cdot x_i\right).$$

Note that each projective variety $\mathcal{V}\left(\sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(p) \cdot x_i\right)$ is indeed well-defined: if f is homogeneous of degree d, then each partial derivative $\frac{\partial f}{\partial x_i}$ will be either identically zero or homogeneous of degree $d-1$, so that choosing a different representative of p, say $(cp_0 : \ldots : cp_n)$ instead of $(p_0 : \ldots : p_n)$, will simply scale each term of $\sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(p) \cdot x_i$ by the constant c^{d-1}; that is, it will scale the polynomial $\sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(p) \cdot x_i$ by a constant and hence will not affect its zero set.

Example 1.19. A projective line l is its own tangent space at any point of l. For after a change of coordinates, any line in $\mathbb{P}^n$ is simply the variety cut out by the $n-1$ polynomials $x_2, \ldots, x_n$; that is, $l = \mathcal{V}(x_2, \ldots, x_n) = \mathcal{V}((x_2, \ldots, x_n))$, where this last quantity denotes the variety associated to the ideal generated by $x_2, \ldots, x_n$. By the homogeneous Nullstellensatz, we thus see that $\mathcal{I}(l) = \mathcal{I}(\mathcal{V}((x_2, \ldots, x_n))) = (x_2, \ldots, x_n)$. Therefore

$$T_pl = \bigcap_{f \in \{x_2, \ldots, x_n\}} \mathcal{V}\left(\sum_{i=0}^{n} \frac{\partial f}{\partial x_i}(p) \cdot x_i\right) = \bigcap_{j=2}^{n} \mathcal{V}(x_j) = \mathcal{V}(x_2, \ldots, x_n) = l.$$

At this point, we could define a projective variety to be singular at a point p if the dimension of $T_p(V)$ (when considered as a vector subspace of K^{n+1}) is "too large." While this definition can be made rigorous, we shall only have occasion to use the following simpler definition, which we state in a way that defines nonsingularity in both the projective and affine cases.

Definition 1.20. Let $V = \mathcal{V}(f)$ be an irreducible hypersurface in $\mathbb{P}^n$ (alternatively, in $\mathbb{A}^{n+1}$). We say V is *singular* at a point $p \in V$ if all of the following hold:

$$\frac{\partial f}{\partial x_0}(p) = 0, \quad \frac{\partial f}{\partial x_1}(p) = 0, \; \ldots \;, \frac{\partial f}{\partial x_n}(p) = 0.$$

If V is nonsingular at each of its points, then we simply say V is *nonsingular*.

It is clear that singularity at $p \in V$ is well-defined even in the projective case (since the partial derivatives of a homogeneous polynomial are homogeneous) and is unchanged if we replace f by any nonzero scalar multiple of f. Therefore our definition of singularity is a property of the hypersurface, not one of our choice of f to define it. We also observe that if $V = \mathcal{V}(f)$ is singular at p under the definition just given, then the tangent space to V at p, namely $\mathcal{V}\left(\sum_{i=0}^{n} \frac{\partial f}{\partial x_i}(p) \cdot x_i\right)$, has full dimension $n+1$. This fits with our earlier idea of nonsingularity.

Finally, it is worth keeping in mind that a change of coordinates in either the affine case or the projective case never affects the irreducibility or nonsingularity of a variety.

2. Miscellaneous Lemmas

In this section, we present several miscellaneous facts which we shall need for our proof that there are exactly 27 lines on a nonsingular cubic surface. Throughout this section, assume that K is algebraically closed and not of characteristic 2.

Additionally, since we shall henceforth be working only in $\mathbb{P}^n$ with n at most 3, we shall write homogeneous coordinates in a fashion such as $(x : y : z : t)$ instead of in the more unwieldy fashion $(x_0 : x_1 : x_2 : x_3)$.

Lemma 2.1. *Let $f \in K[x, y, z, t]$ be a quadratic form cutting out a quadric surface Q in $\mathbb{P}^3$. Then there exists a symmetric matrix $M \in M_4(K)$ such that for each $\mathbf{x} \in K^4$ we have $f(\mathbf{x}) = \mathbf{x}^T M\mathbf{x}$. Additionally, Q is singular if and only if M is singular.*

Proof. Write $f(x, y, z, t) = Ax^2 + By^2 + Cz^2 + Dt^2 + Exy + Fxz + Gxt + Hyz + Iyt + Jzt$. For any matrix $(a_{ij}) \in M_4(K)$ we have that for each $(x, y, z, t) \in K^4$,

$$\begin{aligned}(x,y,z,t)\begin{pmatrix}a_{11} & \dots & a_{14}\\ \vdots & & \vdots \\ a_{41} & \dots & a_{44}\end{pmatrix}\begin{pmatrix}x\\y\\z\\t\end{pmatrix} &= (x,y,z,t)\begin{pmatrix}a_{11}x+\ldots+a_{14}t\\ \vdots \\ a_{41}x+\ldots+a_{44}t\end{pmatrix}\\ &= (a_{11}x+\ldots+a_{14}t)x+\ldots+(a_{41}x+\ldots+a_{44}t)t\end{aligned}$$

$$\begin{aligned}= a_{11}x^2 + a_{22}y^2 + a_{33}z^2 + a_{44}t^2 + (a_{12}+a_{21})xy + (a_{13}+a_{31})xz + (a_{14}+a_{41}xt)\\ +(a_{23}+a_{32})yz + (a_{24}+a_{42})yt + (a_{34}+a_{43})zt.\end{aligned}$$

Thus, taking $a_{11} = A, \ldots, a_{44} = D, a_{12} = a_{21} = \frac{E}{2}, \ldots, a_{34} = a_{43} = \frac{J}{2}$ and letting $M = (a_{ij})$ gives us a symmetric matrix M such that for each $\mathbf{x} \in K^4$ we have $f(x) = \mathbf{x}^T M\mathbf{x}$.

Lastly, note that Q is singular if and only if there exist $x_1, y_1, z_1, t_1 \in K$ not all zero such that

$$\begin{pmatrix}\frac{\partial f}{\partial x}(x_1,y_1,z_1,t_1)\\ \vdots \\ \frac{\partial f}{\partial t}(x_1,y_1,z_1,t_1)\end{pmatrix} = \begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}$$

As one can easily check by computing the partial derivatives, this occurs if and only if there are $x_1, y_1, z_1, t_1 \in K$ not all zero such that

$$\begin{pmatrix}2(a_{11}x_1+\ldots+a_{14}t_1)\\ \vdots \\ 2(a_{41}x_1+\ldots+a_{44}t_1)\end{pmatrix} = \begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}.$$

But this means precisely that there exists a nontrivial vector $(x_1, y_1, z_1, t_1) \in K^4$ such that $2M(x_1, y_1, z_1, t_1)^T = \mathbf{0}$, which means precisely that M has nullity at least 1 and hence is singular. Thus, Q is singular if and only if M is singular. □

Lemma 2.2. *Let Q be a quadric surface in $\mathbb{P}^3$, i.e. let $Q = \mathcal{V}(f)$ for some $f \in K[x, y, z, t]$ homogeneous of degree 2. Let l be a line in $\mathbb{P}^3$. Then l intersects Q. Additionally, $l \subseteq Q$ if and only if $l \cap Q$ contains at least 3 points of $\mathbb{P}^3$.*

Proof. By a suitable change of coordinates, we can assume that $l = \mathcal{V}(z, t)$. Then $Q \cap l$ is a subvariety of l defined by the vanishing of the homogeneous polynomial f modulo the ideal generated by z and t; that is, $Q \cap l$ can be considered as a subvariety of $\mathbb{P}^1$ defined by the vanishing of the polynomial $g \in K[x, y]$ obtained from f by setting $z = t = 0$. Since f was homogeneous of degree 2, we see that either (i) g is the zero polynomial or (ii) g is a homogeneous polynomial of degree 2. In case (i) *any* point $(x : y) \in \mathbb{P}^1$ will be a root g; and in case (ii) we see by Proposition 1.15 that g has either 1 or 2 distinct roots in $\mathbb{P}^1$. So in either case there is certainly a point $(x : y : 0 : 0) \in \mathbb{P}^3$ which satisfies both f and the polynomials defining l (namely z and t). That is, in either case there is a point lying in both Q and l.

By definition, case (i) occurs if and only if $l \subseteq Q$. So first, assume that $l \subseteq Q$. Then since we are in case (i), we see that *any* point of the form $(x : y : 0 : 0)$ will lie on both Q and l, so there are certainly at least 3 points in $l \cap Q$, as desired. Conversely, assume that $l \nsubseteq Q$. Then we are in case (ii), so there are either 1 or 2 distinct points $(x : y : 0 : 0)$ lying on both Q and l. That is, $|Q \cap l| \leq 2$, as desired. □

Lemma 2.3. *Let l_1, l_2, l_3 be pairwise disjoint lines in $\mathbb{P}^3$. Then there exists a nonsingular quadric surface $Q \subseteq \mathbb{P}^3$ which contains all three of l_1, l_2, l_3.*

Proof. For each $i \in \{1, 2, 3\}$, let p_i, p'_i, p''_i be three distinct points on l_i. Then $p_1, p_2, p_3, p'_1, p'_2, p'_3, p''_1, p''_2, p''_3$ constitute 9 distinct points since l_1, l_2, l_3 are disjoint. Write these 9 points as $(x_1 : y_1 : z_1 : t_1), \ldots, (x_9 : y_9 : z_9 : t_9)$. We shall first argue that there exists a quadric surface Q containing these 9 points. Any quadric surface is defined by a homogeneous polynomial of degree 2, i.e. some polynomial $f \in K[x, y, z, t]$ of the form

$$f(x, y, z, t) = Ax^2 + By^2 + Cz^2 + Dt^2 + Exy + Fxz + Gxt + Hyz + Iyt + Jzt$$

with $A, \ldots, D$ not all zero. Thus, there is a quadric surface containing all 9 of our points if and only if there is some choice of coefficients $A, \ldots, J$ (not all zero) such that all 9 of the equations

$$Ax_1^2 + By_1^2 + Cz_1^2 + Dt_1^2 + Ex_1y_1 + Fx_1z_1 + Gx_1t_1 + Hy_1z_1 + Iy_1t_1 + Jz_1t_1 = 0$$

$$\vdots$$

$$Ax_9^2 + By_9^2 + Cz_9^2 + Dt_9^2 + Ex_9y_9 + Fx_9z_9 + Gx_9t_9 + Hy_9z_9 + Iy_9t_9 + Jz_9t_9 = 0$$

hold. (We need not worry about the case where all of $A, \ldots, D$ are zero since finding a polynomial of this kind amounts to finding a *plane* containing all 9 of our points, and the union of such a plane with any other plane defines a quadric surface.) This is a system of 9 homogeneous linear equations in 10 variables: here, the *coefficients* $A, \ldots, J$ are the variables, while $x_1, \ldots, t_9$ are fixed elements of K. Thus, there is a nontrivial solution to this system; that is, there are indeed coefficients $A, \ldots, J$ not all zero such that the above 9 equations all hold. Therefore there certainly exists some quadric surface Q containing all 9 of our points.

In fact, Q must contain all three lines l_1, l_2, l_3. For given $i \in \{1, 2, 3\}$, we have that Q contains 3 distinct points of l_i, and by Lemma 2.2, this means $l_i \subseteq Q$.

Next, we note that Q cannot contain any projective planes and hence is irreducible. For suppose for a contradiction that Q contains a plane P, i.e. suppose we can factor out the defining polynomial of P from f. Then since f is of degree 2, we see that f factors into two possibly equal linear forms. Thus, Q is the union of two possibly equal planes in $\mathbb{P}^3$; call them P_1 and P_2. Since $l_1, l_2, l_3 \subseteq Q$, without loss of generality we can assume that either (i) $l_1, l_2 \subseteq P_1$ and $l_3 \subseteq P_2$ or (ii) $l_1, l_2, l_3 \subseteq P_1$. In either case, we find a projective plane which contains at least two of the lines l_1, l_2, l_3. But these lines are all pairwise disjoint, meaning we have found a projective plane containing two disjoint lines, a contradiction.

Now to see that Q is in fact nonsingular, suppose for a contradiction that Q is singular. Then by Lemma 2.1, there is a symmetric singular matrix $M \in M_4(K)$ such that for each $\mathbf{x} \in K^4$ we have $f(\mathbf{x}) = \mathbf{x}^T M\mathbf{x}$. In particular, there is some nonzero $\mathbf{y} \in K^4$ such that $M\mathbf{y} = \mathbf{0}$. Since M is symmetric, this also means that $\mathbf{y}^T M = \mathbf{0}$. Thus, for each $\mathbf{x} \in K^4$ we certainly have that $\mathbf{x}^T M\mathbf{y} = 0 = \mathbf{y}^T M\mathbf{x}$.

Next, note that since l_1, l_2, l_3 are disjoint, there must exist $i \in \{1, 2, 3\}$ such that $\mathbf{y} \notin l_i$ (here treating $\mathbf{y}$ as a point in $\mathbb{P}^3$ rather than one in K^4). Without loss of generality, assume $\mathbf{y} \notin l_1$. Then we observe that for each point $\mathbf{x} \in K^4$ whose equivalence class (that is, whose corresponding point in $\mathbb{P}^3$) is in l_1 and for each $a, b \in K$ not both zero we have that $f(a\mathbf{x} + b\mathbf{y}) = 0$, as follows. We know

$$f(a\mathbf{x}+b\mathbf{y}) = (a\mathbf{x}+b\mathbf{y})^T M(a\mathbf{x}+b\mathbf{y}) = a\mathbf{x}^T Ma\mathbf{x}+a\mathbf{x}^T Mb\mathbf{y}+b\mathbf{y}^T Ma\mathbf{x}+b\mathbf{y}^T Mb\mathbf{y}.$$

The first term of the right-hand side is zero since it equals $f(a\mathbf{x})$ and since any scalar multiple of $\mathbf{x}$ satisfies f since the equivalence class of $\mathbf{x}$ is in l_1. The remaining terms are zero by the end of the previous paragraph.

Now by a suitable change of coordinates, it is easy to see that the set of all equivalence classes of points of the form $a\mathbf{x} + b\mathbf{y}$ as above is in fact a projective plane and is the unique projective plane containing $\mathbf{y}$ and l_1. Thus, f is zero on the unique projective plane containing $\mathbf{y}$ and l_1. But as established above, Q cannot contain any projective planes. This contradiction means that Q must be nonsingular. □

Lemma 2.4. *Let $Q = \mathcal{V}(f)$ be a nonsingular quadric surface in $\mathbb{P}^3$. Then by a suitable change of coordinates we have $Q = \mathcal{V}(xy - zt)$.*

Proof. By Lemma 2.1, we know there is a nonsingular symmetric matrix $M \in M_4(K)$ such that for each $\mathbf{x} \in K^4$ we have $f(\mathbf{x}) = \mathbf{x}^T M\mathbf{x}$. Now change coordinates to diagonalize M into a matrix M'. Then the only possible nonzero entries of M' are the four along the diagonal; say from top-left to bottom-right these are a, b, c, d. Since M is nonsingular, M' is nonsingular, meaning none of a, b, c, d can be zero. Under this change of coordinates, we have for each $(x, y, z, t) \in K^4$ that

$$f(x, y, z, t) = (x, y, z, t)M'(x, y, z, t)^T = ax^2 + by^2 + cz^2 + dt^2$$
$$= (\sqrt{a}x + i\sqrt{b}y) \cdot (\sqrt{a}x - i\sqrt{b}y) - i(\sqrt{c}z + i\sqrt{d}t) \cdot i(\sqrt{c}z - i\sqrt{d}t),$$

where here we are employing the fact that K is algebraically closed to let $\sqrt{a}$ denote a zero of the polynomial $x^2 - a$ and let i denote a zero of the polynomial $x^2 + 1$.

Now let

$$A = \begin{pmatrix} \sqrt{a} & i\sqrt{b} & 0 & 0 \\ \sqrt{a} & -i\sqrt{b} & 0 & 0 \\ 0 & 0 & i\sqrt{c} & -\sqrt{d} \\ 0 & 0 & i\sqrt{c} & \sqrt{d} \end{pmatrix}.$$

Then

$$\det A = \det \begin{pmatrix} \sqrt{a} & i\sqrt{b} \\ \sqrt{a} & -i\sqrt{b} \end{pmatrix} \cdot \det \begin{pmatrix} i\sqrt{c} & -\sqrt{d} \\ i\sqrt{c} & \sqrt{d} \end{pmatrix} = -2i\sqrt{ab} \cdot 2i\sqrt{cd} = 4\sqrt{abcd} \neq 0$$

(since $a, b, c, d \neq 0$ and K is not of characteristic 2), so that A is invertible and hence defines a change of coordinates ϕ on $\mathbb{P}^3$. But this change of coordinates is precisely $x \mapsto \sqrt{a}x + i\sqrt{b}y$, $y \mapsto \sqrt{a}x - i\sqrt{b}y$, $z \mapsto i(\sqrt{c}z + i\sqrt{d}t)$, $t \mapsto i(\sqrt{c}z - i\sqrt{d}t)$, so that under the change of coordinates ϕ^{-1} we have that $f(x, y, z, t) = xy - zt$, as desired. $\square$

Lemma 2.5. *Let Q be a nonsingular quadric surface in $\mathbb{P}^3$. Then the set of lines of $\mathbb{P}^3$ which are contained in Q is divided into two disjoint families, F_1 and F_2, such that (i) no two distinct lines from the same family intersect, (ii) if $l_1 \in F_1$ and $l_2 \in F_2$ then $l_1 \cap l_2 \neq \emptyset$, and (iii) $\bigcup_{l_1 \in F_1} l_1 = Q = \bigcup_{l_2 \in F_2} l_2$.*

Proof. By Lemma 2.4, we can write $Q = \mathcal{V}(xy - zt)$. Now consider the *Segre map* $g : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ given by $g((p : q), (r : s)) = (pr : qs : qr : ps)$. This map is well-defined since it doesn't depend on our choice of representatives for $(p : q)$ or $(r : s)$ and since at least one of pr, qs, qr, ps will not vanish as long as at least one of p, q and at least one of r, s do not vanish. One can easily check that the image of this map is precisely $Q = \mathcal{V}(xy - zt)$: for example, under the notation of Example 1.10, we see that $g(U_0 \times U_0) = \{(1 : qs : q : s) : q, s \in K\} = Q \cap U_0$, $g(U_1 \times U_1) = \{(pr : 1 : r : p) : p, r \in K\} = Q \cap U_1$, and similarly the other possible combinations of products of U_0 and U_1 map to the other possible intersections of Q with U_0, U_1, U_2, U_3. Additionally, g has an inverse since it has an inverse on each of the sets $Q \cap U_0, \ldots, Q \cap U_3$: for example on $Q \cap U_0$, the map $(1 : qs : q : s) \mapsto ((1 : q), (1 : s))$ is its inverse. g is thus an isomorphism of $\mathbb{P}^1 \times \mathbb{P}^1$ with Q.

Now by an argument similar to the one which appears in Lemma 3.2 below, we know that given any point $p \in Q$ and any line $l \subseteq Q$ such that $p \in l$, we have that l is contained in the *plane* T_pQ. Furthermore, since Q is cut out from $\mathbb{P}^3$ by a quadratic form, we know similarly to the proof of Lemma 3.1 below that the intersection of Q with any plane forms a plane conic; therefore certainly for each point $p \in Q$ we know that $Q \cap T_pQ$ contains at most two lines. Combining the above, we see that there can be at most two distinct lines $l \subseteq Q$ through any given point $p \in Q$.

In fact, we already know how to find two lines of Q through any given point $p \in Q$. Say $p = g(p_1, q_1)$ for some $p_1, q_1 \in \mathbb{P}^1$. Then one easily checks that the images $g(\mathbb{P}^1 \times \{q_1\})$ and $g(\{p_1\} \times \mathbb{P}^1)$ are distinct lines in Q which both contain $p = g(p_1, q_1)$. These two lines are therefore the *only* lines of Q through p.

We therefore see that the set of lines of Q is divided into two disjoint families: $F_1 = \{g(\{p_1\} \times \mathbb{P}^1) : p_1 \in \mathbb{P}^1\}$ and $F_2 = \{g(\mathbb{P}^1 \times \{q_1\}) : q_1 \in \mathbb{P}^1\}$. No two lines from the same family can intersect: for example in F_1, if p_1, p_1' are distinct points in $\mathbb{P}^1$ then $\{p_1\} \times \mathbb{P}^1$ and $\{p_1'\} \times \mathbb{P}^1$ are disjoint and hence their images $g(\{p_1\} \times \mathbb{P}^1)$ and $g(\{p_1'\} \times \mathbb{P}^1)$ under the isomorphism g must be disjoint.

Additionally, if $l_1 \in F_1$ and $l_2 \in F_2$ we see that l_1 must intersect l_2. For writing $l_1 = g(\{p_1\} \times \mathbb{P}^1)$ and $l_2 = g(\mathbb{P}^1 \times \{q_1\})$, we see that $g(p_1, q_1) \in l_1 \cap l_2$. This proves (ii). Finally, to prove (iii) let $p \in Q$. Write $p = g(p_1, q_1)$. Then we see that $p \in g(\{p_1\} \times \mathbb{P}^1)$ and $p \in g(\mathbb{P}^1 \times \{q_1\})$. □

Lemma 2.6. *Let $l_1, \ldots, l_4$ be pairwise disjoint lines in $\mathbb{P}^3$ such that $l_1, \ldots, l_4$ do not all lie on any given nonsingular quadric surface $Q \subseteq \mathbb{P}^3$. Then the number of lines in $\mathbb{P}^3$ which intersect all of $l_1, \ldots, l_4$ is either 1 or 2.*

Proof. By Lemma 2.3 above, let Q be a nonsingular quadric surface containing l_1, l_2, and l_3. Then by hypothesis $l_4 \not\subseteq Q$, so by Lemma 2.2 above, we know that $|l_4 \cap Q| \in \{1, 2\}$. So write $l_4 \cap Q = \{p, q\}$ with the possibility that $p = q$. Let F_1, F_2 be the two families of lines of Q as in Lemma 2.5.

Now recall that l_1, l_2, l_3 are *disjoint* lines which are contained in Q. Since all of the lines of Q are either in F_1 or in F_2, by the above we can assume without loss of generality that $l_1, l_2, l_3 \in F_1$. Now any line m in $\mathbb{P}^3$ which intersects $l_1, \ldots, l_3$ must contain at least three points of Q (as $l_1, l_2, l_3 \subseteq Q$ and l_1, l_2, l_3 have no points in common), so by Lemma 2.2, any such line m must be contained in Q. Therefore, any such line m can only intersect l_4 at either p or q. So letting N be the number of lines of $\mathbb{P}^3$ which intersect all of l_1, l_2, l_3, l_4, we see that N is the same as the number of lines m of Q which intersect all of l_1, l_2, l_3 and intersect p or q.

Now any line m of Q lies in either F_1 or F_2. If m lies in F_1, it cannot intersect *any* of l_1, l_2, l_3; if instead m lies in F_2, it must intersect *all* of l_1, l_2, l_3. Therefore N is precisely the number of elements of F_2 which intersect p or q. So since there is a *unique* element of F_2 through a given point of Q, we see that N is either 1 or 2 ($N = 1$ precisely when either (i) $p \neq q$ and the unique line through p and q lies in Q or (ii) $p = q$), as desired. □

In the following lemma, we shall call a plane conic curve *nondegenerate* if its defining polynomial is irreducible.

Lemma 2.7. *Let $f \in K[x, y, z]$ be a quadratic form on $\mathbb{P}^2$. Then f cuts out one of the following from $\mathbb{P}^2$: (A) a nonsingular, nondegenerate conic curve, (B) two distinct lines (necessarily intersecting at a unique point), or (C) a "double" line.*

Proof. First, suppose f factors as $f = gh$ for some linear forms $g, h \in K[x, y, z]$. If g is a nonzero multiple of h, then f is a nonzero constant times the square of a single linear form and hence its zero set is simply that of this linear form, namely a line. This is case (C). If instead g is not a multiple of h, then by Equation (1.1) we know that f cuts out from $\mathbb{P}^2$ the union of the two distinct lines defined by g and h respectively. This is case (B). So we need only consider the case when f does not factor into the product two linear forms, namely when f is irreducible.

Somewhat similarly to the proof of Lemma 2.4, by employing an analogue of Lemma 2.1 and then diagonalizing, we find that under an appropriate change of coordinates we can write

$$f(x, y, t) = ax^2 + by^2 + cz^2$$

for some $a, b, c \in K$ not all zero. If at least one of a, b, c is 0, then we can employ the fact that K is algebraically closed to see that we can factor f. For example, $ax^2 + by^2$ factors as $(\sqrt{a}x + i\sqrt{b}y)(\sqrt{a}x - i\sqrt{b}y)$, and ax^2 factors as $(\sqrt{a}x)^2$. Thus, in the case where f is irreducible, we know that f is equivalent up to a change of coordinates to $ax^2 + by^2 + cz^2$ with all three of a, b, c nonzero. But in this case, by taking the partial derivatives with respect to x, y, and z it is easy to observe that f is nonsingular. This is case (A). □

Lemma 2.8. *Let $f \in K[x, y, t]$ be a quadratic form on $\mathbb{P}^2$; say*

$$f(x, y, t) = Ax^2 + Bxy + Cy^2 + Dxt + Eyt + Ft^2.$$

Then the conic curve $c = \mathcal{V}(f) \subseteq \mathbb{P}^2$ is nonsingular if and only if the "discriminant"

$$\Delta = 4ACF + BDE - AE^2 - B^2F - CD^2$$

is nonzero.

Proof. Let

$$M = \begin{pmatrix} A & B/2 & D/2 \\ B/2 & C & E/2 \\ D/2 & E/2 & F \end{pmatrix}.$$

By the same argument as in Lemma 2.1, we see that we can write

$$f(x, y, t) = (x, y, t)M \begin{pmatrix} x \\ y \\ t \end{pmatrix}$$

and that c is nonsingular if and only if M is nonsingular. But one easily checks that Δ is precisely 4 times the determinant of M, so that Δ is nonzero precisely when M is nonsingular, which is precisely when c is nonsingular. □

3. The 27 Lines on a Nonsingular Cubic Surface

Throughout this section, $f \in K[x, y, z, t]$ will be an irreducible homogeneous cubic polynomial defining a nonsingular hypersurface $S = \mathcal{V}(f)$ in $\mathbb{P}^3$. Assume that K is algebraically closed and of characteristic different from 2.

We wish to demonstrate the remarkable fact that regardless of its shape, the nonsingular cubic surface S will always contain precisely 27 lines of $\mathbb{P}^3$. We do so following the method presented in Chapter 7 of [2].

Lemma 3.1. *Let $P \subseteq \mathbb{P}^3$ be a plane. Then the intersection of the surface S with the plane P forms one of the following in the plane P: (1) a nondegenerate cubic curve (namely, a cubic curve defined by an irreducible cubic form), (2) the union of a nondegenerate conic curve and a line, or (3) three distinct lines.*

Proof. By a suitable change of coordinates, we can assume that P is the plane $\mathcal{V}(t)$. Under this change of coordinates, S is cut out from $\mathbb{P}^3$ by some polynomial g which is homogeneous of degree 3. The intersection of S with P is the plane cubic whose defining polynomial h is the polynomial in $K[x, y, z]$ which is obtained from g by substituting 0 for t. Such a polynomial h either (i) is irreducible, (ii) factors as a product of an irreducible quadratic form and a linear form, or (iii) factors as a product of three linear forms. Case (i) clearly corresponds to case (1) in the statement of the lemma. By Equation (1.1), we see that case (ii) corresponds to case (2). Lastly, again by Equation (1.1) we see that case (iii) corresponds to case (3) except for the fact that a priori we do not know that all three linear terms must be distinct; that is, we do not know that $S \cap P$ will always be the union of three *distinct* lines whenever it is a union of lines. Therefore, it suffices to show that whenever h factors into three linear forms, these linear forms must all be distinct from each other.

So letting l be an arbitrary line in $S \cap P$, it suffices to show that the linear form in $K[x, y, z]$ defining l does not factor out of the cubic h more than once. Now further change coordinates such that $l = \mathcal{V}(z, t)$, i.e. such that the linear form defining l in P is simply z. Next, assume for a contradiction that we can in fact write $h(x, y, z) = z^2 \cdot a(x, y, z)$ for some linear form a. Then reversing the process from which we obtained h from g, we see that g can be expressed as $g(x, y, z, t) = z^2 \cdot b(x, y, z, t) + t \cdot c(x, y, z, t)$ for some linear form b and some quadratic form c. Computing the partial derivatives of g, we see that $g_x = z^2 b_x + tc_x$, $g_y = z^2 b_y + tc_y$, $g_z = 2zb + z^2 b_z + tc_z$, and $g_t = z^2 b_t + c + tc_t$. Thus, at any point $(x : y : z : t)$ such that $z = t = 0$ and such that $c(x, y, z, t) = 0$ we will have that $S = \mathcal{V}(g)$ is singular.

But at least one such point $(x : y : z : t)$ does indeed exist on S: for requiring that $z = t = 0$ simply means restricting to the line l in the plane P, and when we substitute $z = t = 0$ into c we obtain a polynomial c_1 which either (A) is identically zero or (B) is a homogeneous quadratic in the two variables x, y. In the first case, *any* point $(x : y)$ is a root of c_1. In the second case, by Proposition 1.15 we know that c_1 has at least one root $(x : y)$. That is, in all cases $\mathcal{V}(c_1) \neq \emptyset$, i.e. c has some root $(x : y : 0 : 0)$ along l. Therefore S has a singular point, giving a contradiction. □

Lemma 3.2. *Let p be a point of S. Then the number of lines which are contained in S and contain p is at most 3. Additionally, the tangent space to S at p is a plane containing all such lines.*

Proof. Let l be a line contained in S. By Example 1.19, we know $l = T_p l$. Also, since $l \subseteq S$ we have that $\mathcal{I}(S) \subseteq \mathcal{I}(l)$. Thus (taking $x_0 = x, x_1 = y, x_2 = z, x_3 = t$),

$$T_p l = \bigcap_{g \in \mathcal{I}(l)} \mathcal{V}\left(\sum_{i=0}^{3} \frac{\partial g}{\partial x_i}(p) \cdot x_i\right) \subseteq \bigcap_{g \in \mathcal{I}(S)} \mathcal{V}\left(\sum_{i=0}^{3} \frac{\partial g}{\partial x_i}(p) \cdot x_i\right) = T_p S$$

since the intersection on the left is over a larger set than the one on the right. Additionally, since $S = \mathcal{V}(f) = \mathcal{V}((f))$, by the homogeneous Nullstellensatz we have that $\mathcal{I}(S) = (f)$, meaning that

$$T_p S = \mathcal{V}\left(\sum_{i=0}^{3} \frac{\partial f}{\partial x_i}(p) \cdot x_i\right).$$

That is, the projective variety $T_p S$ is cut out from $\mathbb{P}^3$ by a single linear form, and this form is nonzero since at least one of the derivatives $\frac{\partial f}{\partial x_i}(p)$ must be nonzero since S is nonsingular. This is the very definition of $T_p S$ being a plane. In summary: $l \subseteq T_p l \subseteq T_p S$, so that l is a line through p which is contained in the plane $T_p S$. But also $l \subseteq S$, so that $l \subseteq T_p S \cap S$. That is, *any* line through p which is contained in S must also be contained in $T_p S \cap S$. And by 3.1, we know that there are at most 3 lines in $T_p S \cap S$. So there are certainly at most 3 lines through P which are contained in S. □

We now proceed to demonstrate that there are exactly 27 lines on S. In order to do so, however, we shall need to assume that there exists at least one line on S. An elementary proof of this fact involves a quite detailed and not very illustrative calculation; such a proof appears in [2]. Those who are deeply concerned about the omission of such a proof here can simply consider this section as a proof that there are exactly 27 lines on any nonsingular cubic surface which contains at least 1 line.

Lemma 3.3. *Let l be a line contained in S. Then there are exactly 10 lines on S which intersect l. We can write these 10 lines as $\{l_1, \ldots, l_5, l'_1, \ldots, l'_5\}$ in such a way that for each $i \in \{1, \ldots, 5\}$, (1) l, l_i, and l'_i all lie in some plane P_i and (2) if $j \in \{1, \ldots, 5\} \setminus \{i\}$ then $(l_i \cup l'_i) \cap (l_j \cup l'_j) = \emptyset$.*

Proof. Any line $m \neq l$ which intersects l determines a unique plane P_m containing l and m. We thus observe that if $m \subseteq S$ is any line such that $m \neq l$ and such that $l \cap m \neq \emptyset$, then P_m must contain exactly *three* distinct lines of S (as two lines is impossible by Lemma 3.1): l, m, and some other line m'. And since any two lines in a projective plane will always intersect, we see that both m and m' intersect l. In summary: (i) any line m contained in S and intersecting l gives rise to another line m' which also intersects l and in such a way that l, m, m' are coplanar, and (ii) any plane containing l and at least one other line of S must contain exactly 3 lines of S. To establish (1) and (2) as desired, we thus have two facts left to prove: (I) there are exactly 5 planes containing l which also contain another line of S, meaning we can number all the possible pairs of lines (m, m') above as $(l_1, l'_1), \ldots, (l_5, l'_5)$; and then (II) if $i \neq j$ then $(l_i \cup l'_i) \cap (l_j \cup l'_j) = \emptyset$.

Before proving (I), we shall assume (I) and prove (II). Renumbering if necessary, suppose for a contradiction that $(l_1 \cup l'_1) \cap (l_2 \cup l'_2) \neq \emptyset$ and let p be a point in this intersection. Then p lies on either l_1 or l'_1; without loss of generality assume that p lies on l_1. Additionally, without loss of generality assume that p lies on l_2. Then l_1 intersects l_2, and by hypothesis both l_1 and l_2 intersect l. I claim that this means l_1, l_2, l are coplanar. For let P be the unique plane containing l_1 and l_2. If $l \subseteq P$ then we are done, so assume that $l \nsubseteq P$. Then since l can only intersect P in one point, necessarily we have that l intersects P at p. That is, $p \in l_1 \cap l_2 \cap l$. But by Lemma 3.2, this means that T_pS is a plane which contains all three of l_1, l_2, l. That is, l_1, l_2, l are coplanar, a contradiction. So indeed l_1, l_2, l must be coplanar. But we know that l'_1 is a line which is coplanar to l and to l_1, meaning that l'_1 is a line of S lying in the plane containing l, l_1 and l_2 such that l'_1 is (by hypothesis) distinct from all three of l, l_1, l_2. This means that the plane containing l, l_1, l_2 contains at least *four* distinct lines of S, a contradiction to (ii).

We now must prove (I). First, suppose P is a plane containing l. Changing coordinates so that $P = \mathcal{V}(t)$, we see that $S \cap P$ is a subvariety of $P = \mathbb{P}^2$ cut out by a cubic form; and since $l \subseteq S \cap P$, we see that we can factor out the linear form defining l from this cubic form. By equation (1.1), we thus have that $S \cap P$ is the union of the line l and a plane conic c. Now by Lemma 2.7, we know that c is exactly one of the following: (A) a nonsingular, nondegenerate conic curve, (B) the union of two distinct lines, or (C) a single line. Since $S \cap P = l \cup c$, by Lemma 3.1 we know that case (C) is impossible. Thus, precisely one of the following is true: (a) c is nonsingular and contains no lines, or (b) c is the union of two distinct lines and hence is singular.

Now *any* plane P containing l gives rise to a corresponding conic c such that $S \cap P = l \cup c$. Since (I) asks us to prove that there are exactly 5 planes P such that $S \cap P$ contains a line distinct from l, by the conclusion of the previous paragraph it thus suffices to prove that there are exactly 5 planes P in which the corresponding conic c is singular. Therefore, to prove (I), and hence complete the proof of this lemma, it suffices to prove the following:

Lemma 3.4. *Let $\mathcal{P}$ be the set of planes in $\mathbb{P}^3$ which contain l. Then there are exactly 5 elements $P \in \mathcal{P}$ such that $S \cap P$ is the union of l and a plane conic c such that c is singular.*

Proof. Change coordinates such that $l = \mathcal{V}(z,t)$. Note that l will still equal $\mathcal{V}(z,t)$ under a further change of coordinates as long as this change of coordinates replaces z and t by some linear combination of z and t. In particular, the change of coordinates sending z to t and t to z will not affect the defining polynomials of l.

Now since $\mathcal{V}(z,t) = l \subseteq S$, we know $f(x,y,z,t)$ is identically zero whenever $z = 0$ and $t = 0$. Therefore, under our coordinate system we can write

$$f(x,y,z,t) = A(z,t)x^2 + B(z,t)xy + C(z,t)y^2 + D(z,t)x + E(z,t)y + F(z,t), \tag{3.1}$$

where $A, B, C, D, E, F \in K[z,t]$ such that A, B, C are linear forms, D, E are quadratic forms, and F is a cubic form.

It follows from our definition of $\mathcal{P}$ that $\mathcal{P}$ is precisely the set of all varieties of the form $\mathcal{V}(a_0 z - b_0 t)$ with $a_0, b_0 \in K$ not both zero. Let $\mathcal{Q}$ be the set of all varieties of the form $\mathcal{V}(a_0 z - b_0 t)$ with $a_0 \neq 0$ and let $\mathcal{Q}' = \{\mathcal{V}(t)\}$ so that $\mathcal{P} = \mathcal{Q} \cup \mathcal{Q}'$ and $\mathcal{Q}, \mathcal{Q}'$ are disjoint. We first consider the case where $P \in \mathcal{Q}$.

So let $P \in \mathcal{Q}$ and write $P = \mathcal{V}(a_1 z - b_1 t)$. Since $a_1 \neq 0$, we have $P = \mathcal{V}(z - \frac{b_1}{a_1} t)$. Let $b = \frac{b_1}{a_1}$ so that $P = \mathcal{V}(z - bt)$. Observe that b is uniquely determined by our choice of $P \in \mathcal{Q}$: the only choices of (a_0, b_0) such that $\mathcal{V}(a_0 z - b_0 t) = \mathcal{V}(a_1 z - b_1 t)$ are pairs of the form $(a_0, b_0) = (c_0 a_1, c_0 b_1)$ for some nonzero $c_0 \in K$, in which case the quotient $\frac{b_0}{a_0}$ is simply $\frac{c_0 b_1}{c_0 a_1} = \frac{b_1}{a_1} = b$. Also observe that different values of $b \in K$ correspond to different planes $P \in \mathcal{Q}$, and conversely: for we see that $\mathcal{V}(z - bt) = \mathcal{V}(z - b't)$ if and only if $b = b'$.

Since $P = \mathcal{V}(z - bt)$, we see that in P, we always have $z = bt$. Thus, by substituting $z = bt$, we observe that in the plane P, the line l is given simply by $t = 0$. Furthermore, the restriction of f to P is given by substituting $z = bt$ into the expression for f given in Equation (3.1). That is,

$$f|_P(x,y,z,t) = A(bt,t)x^2 + B(bt,t)xy + C(bt,t)y^2 + D(bt,t)x + E(bt,t)y + F(bt,t).$$

Since A, B, C are linear forms, D, E are quadratic forms, and F is a cubic form we can factor out powers of t to see that

$$f|_P(x,y,z,t) = tA(b,1)x^2 + tB(b,1)xy + tC(b,1)y^2 + t^2 D(b,1)x + t^2 E(b,1)y + t^3 F(b,1).$$

That is,

$$f|_P(x,y,z,t) = t[A(b,1)x^2 + B(b,1)xy + C(b,1)y^2 + tD(b,1)x + tE(b,1)y + t^2 F(b,1)].$$

Since t is the defining polynomial of l in P and $f|_P$ is the defining polynomial of $S \cap P$, we see by Equation (1.1) that $S \cap P$ is the union of l and the conic curve c in P defined by

$$g_b(x,y,t) = A(b,1)x^2 + B(b,1)xy + C(b,1)y^2 + D(b,1)xt + E(b,1)yt + F(b,1)t^2.$$

In summary: every plane $P \in \mathcal{Q}$ gives rise to a unique value $b \in K$ such that the defining polynomial of the "conic part" c of $S \cap P$ is $g_b(x,y,t)$; furthermore, the values of $b \in K$ are in bijective correspondence with the possible planes $P \in \mathcal{Q}$.

Now by Lemma 2.8, we know that the conic c will be singular precisely when the discriminant of g_b is zero, i.e. when

$$0 = 4A(b,1)C(b,1)F(b,1) + B(b,1)D(b,1)E(b,1) - A(b,1)E^2(b,1) \\ -B^2(b,1)F(b,1) - C(b,1)D^2(b,1).$$

Now let h be the homogeneous quintic in $K[z,t]$ given by

$$h(z,t) = 4A(z,t)C(z,t)F(z,t) + B(z,t)D(z,t)E(z,t) - A(z,t)E^2(z,t) \\ -B^2(z,t)F(z,t) - C(z,t)D^2(z,t).$$

Then by the above, we see that different planes $P \in \mathcal{Q}$ in which the conic part of $S \cap P$ is singular correspond bijectively to different roots of h (in K^2, or in this case equivalently in $\mathbb{P}^1$) of the form $(b,1)$ for some $b \in K$.

We now consider the other case, namely if $P \in \mathcal{Q}'$. Then necessarily $P = \mathcal{V}(t)$, so that the line $l = \mathcal{V}(z,t)$ is defined in P simply by $z = 0$. And similarly to before, we find $f|_P$ by substituting $t = 0$ into f as given in Equation (3.1). That is,

$$f|_P(x,y,z,t) = A(z,0)x^2 + B(z,0)xy + C(z,0)y^2 + D(z,0)x + E(z,0)y + F(z,0).$$

By factoring out powers of z from A, B, C, D, E, F according to their degrees, we find that

$$f|_P(x,y,z,t) = z[A(1,0)x^2+B(1,0)xy+C(1,0)y^2+D(1,0)xz+E(1,0)yz+F(1,0)z^2]$$

so that the conic part c of $S \cap P$ is simply given by

$$g(x,y,z) = A(1,0)x^2 + B(1,0)xy + C(1,0)y^2 + D(1,0)xz + E(1,0)yz + F(1,0)z^2.$$

By Lemma 2.8, we know that the conic c will be singular precisely when

$$0 = 4A(1,0)C(1,0)F(1,0) + B(1,0)D(1,0)E(1,0) - A(1,0)E^2(1,0) \\ -B^2(1,0)F(1,0) - C(1,0)D^2(1,0).$$

Thus, we see that the (unique) plane $P \in \mathcal{Q}'$ will result in a singular conic part c of $S \cap P$ precisely when the polynomial h has $(1,0) \in K^2$ as a root. But since h is homogeneous, we know that h will have $(1,0)$ as a root if and only if it has every point of the form $(d,0)$ with $d \in K \setminus \{0\}$ as a root. That is, the plane $P \in \mathcal{Q}'$ will result in c being singular precisely when h has $(1:0) \in \mathbb{P}^1$ as a root.

Combining this with the case when $P \in \mathcal{Q}$ and recalling that $\mathcal{P} = \mathcal{Q} \cup \mathcal{Q}'$, we see that the distinct planes $P \in \mathcal{P}$ in which the conic part c of $S \cap P$ will be singular correspond bijectively to the distinct roots in $\mathbb{P}^1$ of the homogeneous quintic $h(z,t)$. Since we wish to prove that there are exactly 5 distinct planes $P \in \mathcal{P}$ in which c is singular, it thus suffices to prove that there are exactly 5 distinct roots of h in $\mathbb{P}^1$. Now by Proposition 1.15, we know that h has exactly 5 roots in $\mathbb{P}^1$ when these roots are counted with multiplicity; thus, it suffices to show that h has no multiple roots. That is, we must only prove the following:

Lemma 3.5. *Under the notation above, the homogeneous quintic h has no multiple roots in $\mathbb{P}^1$.*

Proof. Note that each element of $\mathbb{P}^1$ has a representative of the form $(b,1)$ (for some $b \in K$) or of the form $(1,0)$. Recalling Proposition 1.15, we know that whenever h has a root of the form $(b:1)$, we can factor out the term $z - bt$ from h; similarly, whenever h has the root $(1:0)$, we can factor out a t from h. Thus, to prove our desired result it suffices to show that for any given $b \in K$, we cannot factor out more than one power of the term $z - bt$ or of the term t from h.

Note that as stated in the first paragraph of the proof of Lemma 3.4, changing coordinates such that z and t are switched will not affect the fact that $l = \mathcal{V}(z,t)$ and hence will not affect the fact that $h(z,t) = 4A(z,t)C(z,t)F(z,t) + B(z,t)D(z,t)E(z,t) - A(z,t)E^2(z,t) - B^2(z,t)F(z,t) - C(z,t)D^2(z,t)$ for some A, B, C linear forms, D, E quadratic forms, and F a cubic form. So by changing coordinates such that z and t are switched if necessary, we need only demonstrate that no term of the form $z - bt$ can be factored out from h more than once.

Now given some specific $b \in K$, we can further change coordinates such that $z - bt$ becomes z and t becomes t. This is the inverse change of coordinates of a change simply sending z to a linear combination of z and t, so by the first paragraph of the proof of Lemma 3.4 this change of coordinates will also not affect anything we know. Thus, it in fact suffices to simply demonstrate that we cannot factor out more than one power of z from h.

Since we can factor out a z (namely factor out $z - bt$ with $b = 0$) from h, we know h has $(0 : 1)$ as a root. Recalling the correspondence established in the proof of Lemma 3.4, we know that this root corresponds to the plane $P \in \mathcal{P}$ given by $P = \mathcal{V}(z)$, in which l is given simply by $\mathcal{V}(t)$. That is, we know that the intersection of S with this particular plane P is the union of l and a *singular* conic c. By Lemma 3.1 we thus know that $S \cap P$ is a set of 3 distinct lines in P which includes l; say l, m, m' are these lines.

We obviously have that either (A) l, m, m' all intersect at some point $p \in P$ or (B) $l \cap m \cap m' = \emptyset$. Since l, m, m' all lie in the projective plane P, we know that the pairwise intersections of l, m, m' are nonempty. Thus, in case (B), necessarily there are three distinct points $p_1, p_2, p_3 \in P$ such that $l \cap m = p_1$, $l \cap m' = p_2$, and $m \cap m' = p_3$. We now change coordinates in P in order to arrange l, m, m' in a simple fashion. Specifically, in case (A), we can change coordinates such that in P we have $m = \mathcal{V}(x)$ and $m' = \mathcal{V}(x - t)$; in case (B), we can change coordinates such that in P we have $m = \mathcal{V}(x)$ and $m' = \mathcal{V}(y)$. Such changes of coordinates occur only in the plane P and do not affect the fact that $P = \mathcal{V}(z)$; furthermore, they also do not affect the fact that $l = \mathcal{V}(t)$ in P. Thus, such changes of coordinates will not affect anything we know about h.

We consider case (B); we omit case (A) since it is similar. Since $l, m, m' \subseteq S = \mathcal{V}(f)$, we see that whenever (i) $t = 0$ or $x = 0$ or $y = 0$ and (ii) $z = 0$ both occur, we must have that $f(x,y,z,t) = 0$. So since f is a homogeneous cubic, we thus know that we can write

$$f(x,y,z,t) = xyt + z \cdot q(x,y,z,t)$$

for some quadratic form q. Under our notation from Equation (3.1), we thus have that $B(t,z) = t + az$ for some $a \in K$ and that z divides each of A, C, D, E, F. Now using this very last fact and recalling that

$$h(z,t) = 4A(z,t)C(z,t)F(z,t) + B(z,t)D(z,t)E(z,t) - A(z,t)E^2(z,t) \\ - B^2(z,t)F(z,t) - C(z,t)D^2(z,t),$$

we see immediately that each term of h except possibly $-B^2(z,t)F(z,t)$ is divisible by z^2. Then using the fact that $B(t,z) = t + az$, we see that

$$-B^2(z,t)F(z,t) = -(t^2 + 2azt + a^2z^2)F(z,t).$$

Thus, to show that z^2 does not divide $-B^2F$ (and hence does not divide h, as desired) it suffices to show that z^2 does not divide F. To do so, note that under our coordinate system, the point $p = (0 : 0 : 0 : 1)$ satisfies f and hence lies in S. Since S must be nonsingular at p, we therefore know that at least one of the partial derivatives of f at $(0, 0, 0, 1)$ must be nonzero. Now using the fact that $f(x, y, z, t) = xyt + z \cdot q(x, y, z, t)$, one easily sees that the partial derivatives of f with respect to each of x, y, and t vanish at $(0, 0, 0, 1)$. Therefore we know that $f_z(0, 0, 0, 1)$ must be nonzero. Now recalling the expression for f in Equation (3.1), we know that

$$f_z(x, y, z, t) = A_z(z, t)x^2 + B_z(z, t)xy + C_z(z, t)y^2 + D_z(z, t)x + E_z(z, t)y + F_z(z, t).$$

Evaluating at $(0, 0, 0, 1)$ and recalling that $f_z(0, 0, 0, 1)$ must be nonzero gives that

$$0 \neq f_z(0, 0, 0, 1) = F_z(0, 1).$$

Now since F is a homogeneous cubic and is divisible by z, we can write $F(z, t) = \alpha z^3 + \beta z^2 t + \gamma z t^2$ for some $\alpha, \beta, \gamma \in K$. Then we see that $F_z = 3\alpha z^2 + 2\beta z t + \gamma t^2$, so that $0 \neq F_z(0, 1)$ gives that $\gamma \neq 0$. That is, F has a nonzero zt^2 term and hence is not divisible by z^2, as desired. □

Corollary 3.6. *There exists a pair (m, n) of lines of S such that $m \cap n = \emptyset$.*

Proof. Under the notation of Lemma 3.3, simply take $m = l_1$ and $n = l_2$. Then the result follows from Lemma 3.3 (2). □

Now by the corollary above, fix lines l, m of S such that $l \cap m = \emptyset$. By Lemma 3.3, we know that the only other lines of S intersecting l are the corresponding 10 lines $l_1, \ldots, l_5, l'_1, \ldots, l'_5$. We now ask: how many lines of S are there which do *not* intersect l? In order to answer this question, first note that in the notation of Lemma 3.3, m cannot lie in any of the 5 planes $P_1, \ldots, P_5$: for by Lemma 3.1 this would mean $m \in \{l, l_i, l'_i\}$, a contradiction to $l \cap m = \emptyset$. Therefore, m intersects each of $P_1, \ldots, P_5$ in exactly one point. Since $m \subseteq S$ and since for each $i \in \{1, \ldots, 5\}$ we know that $S \cap P_i = l \cup l_i \cup l'_i$, we see that for each $i \in \{1, \ldots, 5\}$, the line m must intersect l_i or intersect l'_i since it does not intersect l. Additionally, for any particular $i \in \{1, \ldots, 5\}$ we know that m cannot intersect both l_i and l'_i, as this would mean that either (i) m lies in P_i or (ii) m does not lie in the same plane P_i as l_i and l'_i but there is a point p which lies on all three of l_i, l'_i, and m. Conclusion (i) contradicts $S \cap P_i = l \cup l_i \cup l'_i$, and conclusion (ii) contradicts Lemma 3.2 since we have found 3 *noncoplanar* lines of S which contain the point $p \in S$. Thus, we observe that for each $i \in \{1, \ldots, 5\}$, there is a unique element of $\{l_i, l'_i\}$ which m intersects. By relabeling if necessary, we can assume that for each $i \in \{1, \ldots, 5\}$, the line m intersects l_i and does not intersect l'_i.

Now by applying Lemma 3.3 to the line m, we know that there are 10 distinct lines of S which meet m. We have already accounted for the 5 lines $l_1, \ldots, l_5$, and we know that if $i \neq j$ then the lines l_i and l_j cannot be coplanar since $l_i \cap l_j = \emptyset$. By Lemma 3.3 with m in place of l, then, we know that for each $i \in \{1, \ldots, 5\}$, there must be a line (call it l''_i) distinct from all of the lines $l_1, \ldots, l_5$ which is coplanar with m and l_i. More specifically, under our notation we have the following:

Corollary 3.7. *There are exactly 10 lines on S which intersect m. Five of these lines are $l_1, \ldots, l_5$; the other 5 are $l''_1, \ldots, l''_5$. We have that for each $i \in \{1, \ldots, 5\}$,* *(1) m, l_i, and l_i'' all lie in some plane Q_i and (2) if $j \in \{1, \dots, 5\} \setminus \{i\}$ then $(l_i \cup l_i'') \cap (l_j \cup l_j'') = \emptyset$.*

We also observe that for no $i, j \in \{1, \dots, 5\}$ can we have that $l_i'' = l_j'$. For suppose for a contradiction that $l_i'' = l_j'$ for some $i, j \in \{1, \dots, 5\}$. First, suppose $i \neq j$. Then by Lemma 3.3 (2), we know that $l_i \cap l_j' = \emptyset$ and therefore that l_j' cannot be coplanar to l_i. That is, l_i'' cannot be coplanar to l_i. But we know that the plane Q_i contains both l_i and l_i'', a contradiction. So suppose instead that $i = j$, namely suppose that $l_i'' = l_i'$. Then since l_i'' intersects m, we know l_i' intersects m. But this contradicts the fact that we labelled $l_1, \dots, l_5, l_1', \dots, l_5'$ in such a way that for each $i \in \{1, \dots, 5\}$, m intersects l_i but *not* l_i'.

We thus conclude that each line of the form l_i'' is distinct from every line of the form l_j'. Combining this with the facts established in Corollary 3.7 that each line l_i'' is disjoint form each l_j when $i \neq j$ and that each line l_i'' is distinct from l_i, we thus observe that each of the lines in the list $l, m, l_1, \dots, l_5, l_1', \dots, l_5', l_1'', \dots, l_5''$ is distinct from all other lines in this list. That is, the set

$$A := \{l, m, l_1, \dots, l_5, l_1', \dots, l_5', l_1'', \dots, l_5''\}$$

has 17 elements.

Corollary 3.8. *Let $i, j \in \{1, \dots, 5\}$ such that $i \neq j$. Then $l_j'' \cap l = \emptyset$ and $l_j'' \cap l_i = \emptyset$. However, l_j'' must intersect l_i'.*

Proof. First, if l_j'' were to intersect l, then by Lemma 3.3 we would have that $l_j'' \in \{l_1, \dots, l_5, l_1', \dots, l_5'\}$, a contradiction to the fact that the set A above has 17 distinct elements. Second, the fact that $l_j'' \cap l_i = \emptyset$ follows immediately from Corollary 3.7 (2). Third, since l_j'' does not intersect l, by the same argument we used to show that m intersects exactly one of l_i or l_i' for each $i \in \{1, \dots, 5\}$, we see that l_j'' must intersect exactly one of l_i or l_i' for each $i \in \{1, \dots, 5\}$. So since $l_j'' \cap l_i = \emptyset$, we see that l_j'' must intersect l_i'. □

Lemma 3.9. *Let $A = \{l, m, l_1, \dots, l_5, l_1', \dots, l_5', l_1'', \dots, l_5''\}$ as above. Let n be a line of S such that $n \notin A$. Then n intersects exactly three of the lines $l_1, \dots, l_5$.*

Proof. First, note that given any four disjoint lines $m_1, \dots, m_4$ of S, we cannot have that $m_1, \dots, m_4$ all lie in some nonsingular quadric surface Q. For suppose for a contradiction that $m_1, \dots, m_4$ did in fact lie on a nonsingular quadric Q.

I claim that $Q \subseteq S$, as follows. We wish to prove that $f|_Q$ is identically zero. Since Q is nonsingular, we know by Lemma 2.5 that its lines are divided into two families F_1 and F_2. Since m_1, m_2, m_3, m_4 are disjoint, by Lemma 2.5 (ii) they must all lie in the same family, so without loss of generality assume $m_1, m_2, m_3, m_4 \in F_1$. Since by Lemma 2.5 (iii) we know $Q = \bigcup_{k \in F_2} k$, to show that f is identically zero on all of Q it suffices to show that f is identically zero along any line $k \in F_2$. So let $k \in F_2$. By a suitable change of coordinates, we can assume $k = \mathcal{V}(z, t)$. Therefore $f|_k$ is a cubic form in x, y; that is, f is a cubic form on $\mathbb{P}^1$. Now since $m_1, m_2, m_3, m_4 \subseteq S = \mathcal{V}(f)$, we know that f is identically 0 along each of m_1, m_2, m_3, m_4. Since by Lemma 2.5 (ii) k intersects each of the distinct lines m_1, m_2, m_3, m_4, we thus see that $f|_k$ has at least 4 distinct zeros. But by Proposition 1.15, this means $f|_k$ must be identically zero, as desired.

Thus, $Q \subseteq S$. So we can divide f by the polynomial defining Q, meaning S is the union of Q and the plane defined by the other factor of f, a contradiction to the fact that S is irreducibile and nondegenerate. Therefore no four lines of S lie on the same nonsingular quadric surface.

Now note that l and m are distinct lines in $\mathbb{P}^3$ such that both l and m intersect each of the lines $l_1, \dots, l_5$. So if n intersects at least four of the lines $l_1, \dots, l_5$, then by Lemma 2.6 we know that $n \in \{l, m\}$, a contradiction to $n \notin A$. Thus, we must only rule out the case when n intersects 2 or fewer of $l_1, \dots, l_5$. Now since we know (by the same argument we used to prove that m intersects exactly one of each of l_i or l'_i for $1 \le i \le 5$) that n intersects exactly one of l_i, l'_i for each $i \in \{1, \dots, 5\}$, we see that if n intersects at most 2 of $l_1, \dots, l_5$ then necessarily n intersects at least 3 of $l'_1, \dots, l'_5$. So in this case, assume without loss of generality that n intersects l'_1, l'_2, and l'_3. Now exactly one of the following must hold: (i) n intersects l_4 and l_5, (ii) n intersects l'_4 and l'_5, (iii) n intersects l'_4 and l_5, or (iv) n intersects l_4 and l'_5.

Note that by Lemma 3.3, l intersects all of l'_1, l'_2, l'_3, l'_4, and l_5. Additionally, by Corollary 3.7 l''_5 intersects l_5, as these two lines both lie in the plane Q_5. And by Corollary 3.8, l''_5 also intersects all of l'_1, l'_2, l'_3, l'_4. Thus, by Lemma 2.6 we know that if n intersects at least 4 of the lines $l'_1, l'_2, l'_3, l'_4, l_5$ then $n \in \{l, l''_5\}$. So in all of cases (i)-(iii) we have that $n \in \{l, l''_5\}$, a contradiction to $n \notin A$.

So we must only consider case (iv). By a similar argument to the one in the previous paragraph, we know that both l and l''_4 intersect all of $l'_1, l'_2, l'_3, l_4, l'_5$. Therefore by Lemma 2.6 we know that in case (iv) we must have $n \in \{l, l''_4\}$, a contradiction to $n \notin A$. ☐

Lemma 3.10. *(i) Any line of S which is not in A intersects exactly three of the five lines $l_1, \dots, l_5$ and is uniquely determined by which three of these lines it intersects. Furthermore, (ii) for every possible choice of distinct $i, j, k \in \{1, \dots, 5\}$, there does indeed exist a line of S which is not in A and which intersects l_i, l_j, and l_k.*

Proof. By Lemma 3.9 above, we know that any line of S which is not in A will intersect exactly three of $l_1, \dots, l_5$. Now let $i, j, k \in \{1, \dots, 5\}$ be pairwise distinct. To prove (i), we must show that if n_1, n_2 are lines of S which are not in A and which both intersect all of l_i, l_j, l_k then we must have $n_1 = n_2$. Without loss of generality, we can assume that $\{i, j, k\} = \{1, 2, 3\}$.

We know that both n_1 and n_2 intersect l'_4 and l'_5: for any line n not intersecting l will intersect a unique element of $\{l_i, l'_i\}$ for each $i \in \{1, \dots, 5\}$, and any such line n will intersect exactly three of $l_1, \dots, l_5$. Specifically, this means that each of l, n_1, and n_2 intersects all four of the pairwise disjoint lines l_1, l_2, l_3, l'_4. By the proof of Lemma 3.9 we know l_1, l_2, l_3, l'_4 do not all lie on any quadric surface; therefore, by Lemma 2.6 we know that at most two distinct lines in $\mathbb{P}^3$ can intersect all of l_1, l_2, l_3, l'_4. Thus, the set $\{l, n_1, n_2\}$ contains at most two elements. But by our assumption that $n_1, n_2 \notin A$, we know $n_1, n_2 \neq l$. Therefore we must have that $n_1 = n_2$, as desired.

We now prove (ii). Fix $i \in \{1, \dots, 5\}$. It suffices to show that for each choice of $j, k \in \{1, \dots, 5\}$ such that i, j, k are all distinct, we have that there is a line of S which is not in A and which intersects l_i, l_j, and l_k. Note that there are exactly $\binom{4}{2} = 6$ choices of $j, k \in \{1, \dots, 5\}$ such that i, j, k are all distinct. Thus, it will suffice to prove that there are exactly 6 lines of S which are not in A and which intersect l_i: for each such line intersects exactly two of $l_1, \dots, l_{i-1}, l_{i+1}, \dots, l_5$ and is uniquely determined by which two it intersects, so that if there are exactly 6 such lines then these 6 lines must cover all $\binom{4}{2}$ choices of l_j and l_k to intersect. We therefore now prove that there are exactly 6 lines of S which are not in A and which intersect l_i.

We know that l, m, l'_i, l''_i all intersect l_i: l'_i intersects l_i since they are coplanar, and similarly for l''_i. Additionally, by Lemma 3.3 we know that for each $j \neq i$, the lines l_j and l'_j do not intersect l_i; and similarly by Corollary 3.7 we know that if $j \neq i$ then l''_j does not intersect l_i. Thus, l, m, l'_i, l''_i are all of the elements of A which intersect l_i. That is, there are 4 elements of A which intersect l_i. Now by Lemma 3.3, we know there are exactly 10 lines of S which intersect l_i. This means that there are exactly $10 - 4 = 6$ lines of S which are not in A and intersect l_i, as desired. □

Theorem 3.11. *There are exactly 27 lines on S.*

Proof. The set of lines on S splits into two subsets: the set

$$A = \{l, m, l_1, \ldots, l_5, l'_1, \ldots, l'_5, l''_1, \ldots, l''_5\}$$

and the set B of those lines of S which are not in A. Now by Lemma 3.9, every element of B intersects exactly three of $l_1, \ldots, l_5$. And by Lemma 3.10, the different elements of B correspond precisely to different choices of distinct $l_i, l_j, l_k \in \{l_1, \ldots, l_5\}$ to intersect; that is, they correspond to different choices of distinct $i, j, k \in \{1, \ldots, 5\}$. Now there are exactly $\binom{5}{3} = 10$ choices of three distinct elements of $\{l_1, \ldots, l_5\}$, so there must be exactly 10 elements of B. This gives that the number of lines on S is $|A| + |B| = 17 + 10 = 27$. □

Acknowledgments. I would like to thank Benjamin Gammage for recommending the subject of algebraic geometry to me, capturing my interest by demonstrating some of its fascinating results, and patiently answering my questions and recommending exercises as I studied the subject. I would like to thank Sergei Sagatov for greatly assisting me in assembling this paper, including giving detailed answers to many of my questions and carefully reading drafts of this paper and suggesting improvements. Lastly, I would like to thank Peter May and all of the instructors and organizers of the 2014 University of Chicago Mathematics REU for making the program as valuable and engaging as it was.

References

[1] George Kemper. *A Course in Commutative Algebra.* Springer, 2011.
[2] Miles Reid. *Undergraduate Algebraic Geometry.* Cambridge University Press, 1990.
[3] Karen E. Smith et al. *An Invitation to Algebraic Geometry.* Springer, 2004.