137 NOTES, PART 4: STUDY'S LEMMA AND APPLICATIONS

Z. RAN

1. Study's Lemma

As it turns out, the resultant is the key that opens many doors in the study of plane curves. As a first application, we will show that a plane curve 'essentially' determines its equation. In fact, we will prove a rather more general result. First a definition. A field k is said to be *algebraically closed* if every nonconstant polynomial in $k[x]$ has at least one root. The standard example of an algebraically closed field is the field $\mathbb{C}$ of complex numbers (thanks to the Fundamental Theorem of Algebra). An important fact whose proof goes back to Euclid is the following:

Theorem 1.1. *Any algebraically closed field is infinite.*

Proof. If k is a finite field, $k = \{a_1, ..., a_n\}$, then

$$f(x) = (x - a_1) \cdots (x - a_n) + 1$$

has no roots in k, so k is not algebraically closed. □

Exercise 1.1. *Modify the above argument to prove*
(i) there are infinitely many prime numbers in $\mathbb{Z}$;
(ii) for any field k (even finite), there are infinitely many non-associate irreducible polynomials in $k[x]$.

Theorem 1.2. *(Study's Lemma) Let k be an algebraically closed field, $f, g \in k[x_1, ..., x_n]$ polynomials with f irreducible. Assume*

$$\text{Zeros}_k(f) \subseteq \text{Zeros}_k(g). \tag{1}$$

Then

$$f|g.$$

The idea of the proof is based on projection, i.e. the resultant with respect to, say, x_n. Assuming, for contradiction, that $f \nmid g$, the resultant $r = r(g, f)$ with respect to x_n will be nonzero. We can then find a point

Date: March 19, 2006.

$a. = (a_1, ..., a_{n-1})$ such that $r(a.) \neq 0$. This means $f(a., x_n), g(a., x_n)$ have no common factor. But that is absurd: by algebraic closedness $f(a., x_n)$ has some zero in x_n and by (1) that zero is also a zero of $g(a., x_n)$. This contradiction will prove the theorem.

Turning to the details, we start with

Lemma 1.3. *Let D be an infinite integral domain and $h \in D[x_1, ..., x_n]$ a nonzero polynomial. Then there exist $a_1, ..., a_n \in D$ such that*

$$h(a_1, ..., a_n) \neq 0.$$

Proof. Proof of Lemma: If $n = 1$ this follows from the fact that h has only finitely many zeros (even in K, the fraction field in D), while D is infinite. For general n we use induction. Write h as

$$h(x_1, ..., x_n) = b_0 + b_1 x_n + ... + b_r x_n^r,$$

$$b_0, ..., b_r \in D[x_1, ..., x_{n-1}], b_r \neq 0.$$

By induction, there exist $a_1, ..., a_{n-1} \in D$ such that $b_r(a_1, ..., a_{n-1} \neq 0$. Then

$$h(a_1, ..., a_{n-1}, x_n) \in D[x]$$

is not the zero polynomial, therefore there exists $a_n \in D$ such that $h(a_1, ..., a_n) \neq 0$, as claimed.

□

Remark 1.1. If D is finite, there do exist nonzero polynomials $h \in D[x]$ such that the value $h(a) = 0$ for all $a \in D$. For example $D = \mathbb{Z}_2 = \{0, 1\}, h(x) = x^2 + x$.

Proof. *(of Study's Lemma)*: Permuting variables, we may assume x_n occurs in f, i.e. $f \notin k[x_1, ..., x_{n-1}]$. Write

$$f = b_0 + b_1 x_n + ... + b_m x_n^m,$$

where

$$b_0, ..., b_m \in k[x_1, ..., x_{n-1}], b_m \neq 0, m > 0.$$

Now suppose, to start with, that g does not involve x_n, i.e. $g \in k[x_1, ..., x_{n-1}]$. By the lemma, choose $a_1, ..., a_{n-1} \in k$ such that

$$b_r(a_1, ..., a_{n-1}) g(a_1, ..., a_{n-1}) \neq 0.$$

Then

$$\deg(f(a_1, ..., a_{n-1}, x_n)) = r > 0$$

so this is a nonconstant polynomial. As k is algebraically closed, there exists $a_n \in k$ such that $f(a_1, ..., a_n) = 0$, therefore $g(a_1, ..., a_n) =$

$g(a_1, ..., a_{n-1}) = 0$ by our hypothesis $\text{Zeros}(f) \subseteq \text{Zeros}(g)$. This is a contradiction. Thus, g is nonconstant as polynomial of x_n. Write

$$g = e_0 + ... + e_j x_n^j,$$

$$e_0, ..., e_j \in k[x_1, ..., x_{n-1}], e_j \neq 0, j > 0$$

Now consider f, g as polynomials in x_n with coefficients in $D = k[x_1, ..., x_{n-1}]$. Because f is irreducible in $k[x_1, ..., x_n]$, it has no factors besides itself and elements of k. Therefore, as element of $D[x_n]$, f has no factor besides itself which has degree > 0 in x_n. Consequently, if $f \nmid g$, then f, g have no common factor in $D[x_n]$ of positive degree in x_n, therefore by Theorem 2.1 of Part 3, the resultant

$$r = r(f, g) = r_{m,j}(f, g; x_n) \in k[x_1, ..., x_{n-1}]$$

is nonzero. Therefore

$$b_m e_j r \neq 0.$$

Now pick $c_0, ..., c_{n-1} \in k$ such that

$$b_m(c_1, ..., c_{n-1}) e_j(c_1, ..., c_{n-1}) r(c_1, ..., c_{n-1}) \neq 0. \tag{2}$$

Now

$$f(c_1, ..., c_{n-1}, x_n) \in k[x_n]$$

is a nonconstant polynomial. k being algebraically closed, this polynomial has at least one zero, say c_n. Thus

$$f(c_1, ..., c_n) = 0.$$

by our main assumption (1), we have

$$g(c_1, ..., c_n) = 0$$

as well. Thus $x_n = c_n$ is a common zero, and $x_n - c_n$ is a common factor of the two polynomials

$$f(c_1, ..., c_{n-1}, x_n), g((c_1, ..., c_{n-1}, x_n) \in k[x_n],$$

which have respective degrees m, j exactly. Therefore the resultant of these polynomials is zero. But that resultant is non other than the result of plugging $x_1 = c_1, ..., x_{n-1} = c_{n-1}$ into r. Therefore

$$r(c_1, ..., c_{n-1}) = 0.$$

But this contradicts (2). Therefore $f|g$ and we are done. □

Corollary 1.4. *Let k be an algebraically closed field, $f, g \in k[x_1, ..., x_n]$ polynomials such that*

$$\text{Zeros}_k(f) = \text{Zeros}_k(g).$$

Then f, g have the same sets of irreducible factors (not necessarily with the same multiplicities). If f, g are moreover irreducible, then f, g differ by a constant in k

Proof. If p is any irreducible factor of f, then $\mathrm{Zeros}(p) \subset \mathrm{Zeros}(f) = \mathrm{Zeros}(g)$, hence by Study, $p|g$. Similarly, every irreducible factor of g divides f. □

In light of the Cor. we shall define an *affine plane curve C of degree d* as the zero-set $C = \mathrm{Zeros}(f)$ where f is a polynomial of degree d without multiple factors; f is said to be an *equation* for C, and is uniquely determined by C up to a constant factor, by the Cor. C is said to be *irreducible* if its equation is an irreducible polynomial. As we have seen (as a consequence of the result D factorial $\Rightarrow D[x]$ factorial), any polynomial $f \in \mathbb{C}[x, y]$ is uniquely a product of irreducibles $p_1 \cdots p_k$. Since

$$\mathrm{Zeros}(p_1 \cdots p_k) = \mathrm{Zeros}(p_1) \cdots \mathrm{Zeros}(p_k)$$

it follows:

Corollary 1.5. *Every affine plane curve C is uniquely expressible as a union of irreducible curves (called the* components *of C).*

2. Homogeneous case

D denotes an integral domain.

Proposition 2.1. *If $F, G \in D[X_0, ..., X_n]$, F is homogeneous and $G|F$, then G is homogeneous.*

Proof. Write $F = GH$ and decompose G, H in homogeneous components:

$$G = G_k + ... + G_{k+l}, H = H_r + ... + H_{r+s}$$

with $G_k, G_{k+l}, H_r, H_{r+s} \neq 0$. Assume to start with that l, s are both nozero, i.e. nither G nor H is homogeneous. Then

$$F = G_k H_r + ... + G_{r+s} H_{k+l}$$

where the first summand is homogeneous of degree $k + r$ and the last is homogenous of degree $k + r + l + s$ and all other summands are homogenous with degrees strictly between $k+r$ and $k+r+l+s$. Since F is homogenous, this is a contradiction. Thus at least one of G, H, say $G = G_k$, is homogenous.

Then if H is not homogeneous we have

$$GH = G_k H_r + ... + G_k H_{r+s}$$

and again we get a contradiction as above. Therefore G, H are homogenous. □

As a consequence of this result, the obvious analogues of Study's Lemma and its consequences hold for homogeneous polynomials and their zero-sets:

Corollary 2.2. *(Homogeneous Study's Lemma) Let k be an algebraically closed field.*

(i) *If $F, G \in k[X_0, ...X_n]$ are homogenous polynomials with F irreducible,such that*

$$\mathrm{Zeros}_{\mathbb{P}^n}(F) \subseteq \mathrm{Zeros}_{\mathbb{P}^n}(G).$$

Then $F|G$.

(ii) *If $F, G \in k[X_0, ..., X_n]$ are homogenous polynomials such that*

$$\mathrm{Zeros}_{\mathbb{P}^n}(F) = \mathrm{Zeros}_{\mathbb{P}^n}(G).$$

Then F, G have, up to constant factors, the same sets of irreducible factors (not necessarily with the same multiplicities). If F, G have no multiple factors, then F, G differ by a constant in k.

(iii) *Every projective plane curve C is uniquely expressible as a union of irreducible curves (called the* components *of C).*

Proof. We have the tautological projection

$$\pi : \mathbb{A}^{n+1} \setminus 0 \to \mathbb{P}^n$$

so that for any homogeneous polynomial F,

$$\text{Zeros}_{\mathbb{A}^{n+1}}(F) = \pi^{-1}(\text{Zeros}_{\mathbb{P}^n}(F)) \cup \{0\}.$$

In light of this, our assertions follow immediately from the corresponding assertions in the affine case, proved previously. □

For any n, the zero-set

$$C = \text{Zeros}_{\mathbb{P}^n}(F)$$

of a homogenous polynomial F of degree d without multiple factors is called a *projective hypersurface of degree d with reduced equation F.* The corresponding zero-set

$$\tilde{C} = \text{Zeros}_{\mathbb{A}^{n+1}}(F)$$

is called the *affine cone* over C. Note that if $n = 2$, C is just a plane curve while $\tilde{C} \subset \mathbb{A}^3$ would more appropriately be called a surface. So the foregoing proof illustrates the idea that studying a curve sometimes involves studying other types of geometric objects, like surfaces.

Exercise 2.1. *Give another proof of the Homogenous Study's Lemma using dehomogenization and homogenization, in lieu of the affine cone.*

Theorem 2.3. *Let $F, G \in D[x_0, ..., x_n]$ be homogenous polynomials of degrees s, t, respectively, and let*

$$r = r_{s,t}(F, G, x_n) \in D[x_0, ..., x_{n-1}]$$

be the resultant of F, G as polynomials of degrees s, t in x_n. Then
(i) r is homogenous of degree st.
(ii) If

$$F(0, ..., 0, 1), G(0, ..., 0, 1) \neq 0. \tag{3}$$

Then F, G have a nonconstant common factor iff $r = 0$.

Proof. Let's write

$$F = a_0 x_n^s + ... + a_s, G = b_0 x_n^t + ... + b_t$$

where each $a_i, b_i \in D[x_0, ..., x_{n-1}]$ is homogenous of degree i.

To prove (i) Note

$$r = \det \begin{bmatrix} a_s & & \dots & a_0 & 0 & \dots & 0 \\ 0 & a_s & \dots & & a_0 & \dots & 0 \\ & & & \dots & & & \\ & & & & a_s & \dots & a_0 \\ b_t & & \dots & b_0 & 0 & \dots & 0 \\ 0 & b_t & \dots & & b_0 & \dots & 0 \\ & & & \dots & & & \\ & & & & b_t & \dots & b_0 \end{bmatrix} \tag{4}$$

Then

$$r(ux_0, ..., ux_{n-1}) = \det \begin{bmatrix} u^s a_s & & \dots & u^0 a_0 & 0 & \dots & 0 \\ 0 & u^s a_s & \dots & & u^0 a_0 & \dots & 0 \\ & & & \dots & & & \\ & & & & u^s a_s & \dots & u^0 a_0 \\ u^t b_t & & \dots & u^0 b_0 & 0 & \dots & 0 \\ 0 & u^t b_t & \dots & & u^0 b_0 & \dots & 0 \\ & & & \dots & & & \\ & & & & u^t b_t & \dots & u^0 b_0 \end{bmatrix} \tag{5}$$

Now multiply the 1st row by u^t, the 2nd by u^{t-1} etc. Then the $(t+1)$st row by u^s, the $(t+2)$nd by u^{s-1}, etc. This yields

$$u^{s(s+1)/2+t(t+1)/2} r = \det \begin{bmatrix} u^{s+t} a_s & & \dots & u^0 a_0 & 0 & \dots & 0 \\ 0 & u^{s+t-1} a_s & \dots & & u^0 a_0 & \dots & 0 \\ & & & \dots & & & \\ & & & & u^s a_s & \dots & u^0 a_0 \\ u^{s+t} b_t & & \dots & u^0 b_0 & 0 & \dots & 0 \\ 0 & u^{s+t-1} b_t & \dots & & u^0 b_0 & \dots & 0 \\ & & & \dots & & & \\ & & & & u^t b_t & \dots & u^0 b_0 \end{bmatrix}$$
$$= u^{(s+t)(s+t+1)/2} r$$

(because we can factor $u^{s+t+1-i}$ from the ith column for $i = 1, ..., s+t$ and get the matrix whose determinant is r). Therefore

(6)
$$r(ux_0, ..., ux_{n-1}) = u^{(s+t)(s+t+1)/2 - s(s+1)/2 - t(t+1)/2} r = u^{st} r(x_0, ..., x_{n-1})$$

so r is homogenous of degree st.

For the proof of (ii), note that a_0, b_0 are nonzero constants by our assumption (3) so as polynomials in x_n, F, G have degrees exactly s, t and r is their resultant. So as we have seen, F, G have a nonconstant common factor in $D[x_0, ..., x_{n-1}][x_n] = D[x_0, ..., x_n]$ iff $r = 0$. □

Theorem 2.4. *Any two curves in $\mathbb{P}^2_{\mathbb{C}}$ intersect.*

Proof. We may assume the curves in question have respective homogeneous equations F, G of degrees $m, n > 0$. Applying a suitable projective transformation, we may assume that

$$F(0,0,1), G(0,0,1) \neq 0.$$

This implies that, as polynomials in X_2, both F and G are of degree m, n exactly. Let

$$R = r_{m,n}(F, G; X_2)$$

be the resultant of F, G with respect to X_2. Thus, $R \in \mathbb{C}[X_0, X_1]$ is homogeneous of degree $mn > 0$ and therefore admits a nontrivial zero $[a_0, a_1]$. Then

$$0 = R(a_0, a_1) = r_{m,n}(F(a_0, a_1, X_2), G(a_0, a_1, X_2), X_2) \tag{7}$$

This means one of two things: either

(i) $F(a_0, a_1, X_2)$ is of degree $< m$ in X_2; or

(ii) $G(a_0, a_1, X_2)$ is of degree $< n$ in X_2 or

(iii) $F(a_0, a_1, X_2)$ and $G(a_0, a_1, X_2)$ have a common zero $X_2 = a_2$.

Of course, in Case (iii) we have our desired common zero $[a_0, a_1, a_2]$ for F and G. But Case (i) can happen only if $F(0,0,1) = 0$, which we assumed is not the case; similarly, Case (ii) is impossible too. This proves the Theorem. □

Exercise 2.2. *Prove that for any curve $C \subset \mathbb{P}^2_k$, k algebraically closed, there are infinitely many points on C and infinitely many points in $\mathbb{P}^2_k \setminus C$.*

Theorem 2.5. *('Litle Bézout') Let C, D be projective plane curves of degree m, n, respectively, with no common components. Then*

$$1 \leq |C \cap D| \leq mn \tag{8}$$

Proof. Let $F, G \in \mathbb{C}[X_0, X_1, X_2]$ be respective equations for C, D. Then F, G are homogenous polynomials of degree m, n, respectively with no nonconstant common factors and our claim is that

$$1 \leq |\,\mathrm{Zeros}(F) \cap \mathrm{Zeros}(G)| \leq mn \tag{9}$$

The first inequality is of course just a restatement of the previous Theorem. For the second, we follow closely the notations and argument of that Theorem's proof. Note that $R \neq 0$ thanks to our hypothesis that F, G have no common factors. Since R has degree mn, it follows that R has at most mn zeros $[a_0, a_1]$. The proof shows that any common zero of F, G must lie on one of the lines

$$L_{[a_0,a_1]} = \{[a_0, a_1, *]\} = \mathrm{Zeros}(a_1 X_0 - a_0 X_1) \tag{10}$$

where $[a_0, a_1] \in \text{Zeros}(R)$. Moreover, neither F nor G can vanish identically on any of these lines, because they don't vanish at $[0, 0, 1]$. This shows, at the very least, that the number of common zeros of F, G is *finite*, and can exceed mn only if F, G have > 1 common zero on one of the lines $L_{[a_0,a_1]}$ as above.

Now the last problem is easy to fix: simply restart the proof and make sure in advance that we choose our coordinates so that the point $[0, 0, 1]$ does not lie on any of the finitely many lines joining any pair of common zeros of F, G, since we now know that there are only finitely many such zeros. This completes the proof. □

Corollary 2.6. *Let C, D be affine plane curves of degree m, n, respectively, with no common components. Then*

$$|C \cap D| \leq mn. \tag{11}$$

Proof. It suffices to note that the projective completions C', D' of C, D have no common components: indeed the equations for the components of C', D' are obtained by homogenizing the equations the components of C, D, so if C', D' had a common componet, its affine part would be a common component of C, D. □

Proposition 2.7. *Suppose C, D are projective plane curves, both of degree n, meeting in exactly n^2 points, and that E is an irreducible curve of degree $m < n$ containing exactly mn points of $C \cap D$. Then there exists a curve A of degree $m-n$ containing the remaining $n(n-m)$ points of $C \cap D$.*

Proof. Let F, G, H be respective equations of C, D, E; thus F, G have no multiple factors and H is irreducible. Since E is infinite, we can find a point $P = [a, b, c] \in E \setminus C \cap D$. Set

$$\lambda = -G(a, b, c), \mu = f(a, b, c), B = \lambda F + \mu G.$$

Then $B(a, b, c) = 0$ and B also vanishes on $C \cap D$. Then $\text{Zeros}(B) \cap E$ has at least $mn+1$ points. Therefore B and H have a common factor, and since H is irreducible, it follows that $H|B$, i.e. $B = HK$ for some homogeneous polynomial K of degree $n - m$. Since B vanishes on $C \cap D$, those points of $C \cap D$ not on $E = \text{Zeros}(H)$ must lie on $A = \text{Zeros}(K)$. □

Remark 2.1. Analyzing the above proof, we see that it is still valid when $E = E_1 \cup E_2$ with E_1, E_2 irreducible and there exists a point $P \in E_1 \cap E_2 \setminus C \cap D$. This is because we can still define B as above using P and conclude, as above, that each of the equations H_1, H_2 of E_1, E_2 divides B. Since H_1, H_2 are distinct irreducibles, it follows that $H_1 H_2 | B$ and we can conclude as above.

Exercise 2.3. Fill in the details in the above remark

An obvious special case of this is the following

Corollary 2.8. *If C, C' are cubics meeting in 9 points $P_1, ..., P_9$ and if Q is a nondegenerate conic containing $P_1, ..., P_6$ but not the rest, then P_7, P_8, P_9 are collinear.*

A classic consequence is the following

Theorem 2.9. *(Pascal's mystic hexagon) The opposite sides of a hexagon inscribed in a nondegenrate conic meet in 3 collinear points.*

Proof. By assumption, we have an irreducible conic Q, points $P_1, ..., P_6$ on Q, and the inscribed hexagon comprised of the lines

$$L_1 = \overline{P_1P_2}, ..., L_6 = \overline{P_6P_1}.$$

The pairs of opposite sides are $(L_1, L_4), (L_2, L_5), (L_3, L_6)$. Now consider the cubics

$$C = L_1L_3L_5, C' = L_2L_4L_6.$$

Their intersection points are precisely $P_1, ..., P_6$ together with $L_1 \cap L_4, L_2 \cap L_5, L_3 \cap L_6$. Therefore our claim follows from the previous result. □

Remark 2.2. Given 6 points $P_1, ..., P_6 \in \mathbb{P}^2$, we do not expect that there exist a conic through all of them. To see why, notice that the set of all quadratic forms $F(X_0, X_1, X_2)$ is a 6-dimensional vector space with basis $X_0^2, X_2^2, X_2^2, X_0X_1, X_0X_2, X_1X_2$. For F to vanish at P_i is one linear equation on the coefficients of F, so in total there are 6 such, and we don't expect them to have a nontrivial common solution, in general. In fact, it can be shown that there do exist 6-tuples not on any conic.

Theorem 2.10. *(Pappus) Let L_1, L_2 be distinct lines in $\mathbb{P}^2$,*

$$P_1, P_2, P_3 \in L_1 \setminus L_2, Q_1, Q_2, Q_3 \in L_2 \setminus L_1.$$

Set

$$L_{ij} = \overline{P_iQ_j}, i \neq j \in \{1, 2, 3\},$$

$$L_{12} \cap L_{21} = R_3, L_{13} \cap L_{31} = R_2, L_{23} \cap L_{32} = R_1.$$

Then R_1, R_2, R_3 are collinear.

Proof. Apply Prop 2.7 and the following remark in case

$$C = L_{12}L_{23}L_{31}, D = L_{21}L_{32}L_{13}, E_1 = L_1, E_2 = L_2.$$

Since $E_1 \cap E_2 \notin C \cap D$, we can conclude that the part of $C \cap D$ not on $E_1 \cup E_2$ is on a line, which is precisely Pappus' assertion. □

Proposition 2.11. *(Cayley-Bachrach) Let C be an irreducible cubic, C_1, C_2 cubics. Suppose for $i = 1, 2$, C_i meets C in 9 distinct points $P_1, ..., P_8, Q_i$. Then $Q_1 = Q_2$.*

Lemma 2.12. *If 2 cubics C, C_1 meet in exactly 9 points and Q is one of these points, then all but finitely many lines through Q meet C residually in exactly 2 points.*

[The proof of the Lemma uses concepts to be discussed later; briefly, one shows first that Q is a simple (nonsingular) point on C, and second that any simple point Q on C has the asserted property.]

Proof. (of Prop) If false, let L be a line through Q_1 not through Q_2. Thus

$$L \cap C = \{Q_1, R, S\}.$$

Choose another line M not through any of the previously designated points. Then

$$\begin{aligned}(L \cup C_2) \cap (C \cup M) &= \{P_1, ..., P_8, Q_1, Q_2, R, S\} \cup ((L \cup C_2) \cap M) \\ &= C_1 \cap C \cup \{Q_2, R, S\} \cup ((L \cup C_2) \cap M).\end{aligned}$$

Of these 16 points, the 12 points $C_1 \cap C \cup \ ((L \cup C_2) \cap M)$ are on $C_1 \cup M$. By Prop 2.7 and the following remark, Q_2, R, S are collinear, i.e. $Q_2 \in L$, which is a contradiction. □

3. Singular and nonsingular points

The notions of singular and nonsingular point P on a curve C have do do with the *local* geometry of C near P. We begin with some deinitions. Let $C \subset \mathbb{A}^2$ be an affine curve with reduced equation $f(x, y)$, and let P be a points on C. Then P is said to be a *singular* point or a *singularity* of C if

$$\nabla f(P) = 0,$$

i.e.

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

Similarly, a point P on a projective curve $C \subset \mathbb{P}^2$ with reduced homogenous equation F is said to be a singular point of C if

$$\nabla F(P) = 0$$

i.e.

$$\frac{\partial F}{\partial X_0}(P) = \frac{\partial F}{\partial X_1}(P) = \frac{\partial F}{\partial X_2}(P) = 0.$$

A point of C that is not singular is said to be *nonsingular* or *smooth.* C itself is said to be a *singular curve* if it has at least one singular point; otherwise C is said to be *nonsingular* or *smooth.*

Example 3.1. Any projective conic C is equivalent to one with equation $F = X_0^2 + X_1^2 + X_2^2$. Thus $\nabla F = (2X_0, 2X_1, 2X_2)$ and this is never zero on $\mathbb{P}^2$. Therefore C is nonsingular.

Exercise 3.1. *(i) If C, C' are projectively or affine equivalent then C is singular iff C' is.*

(ii) Determine the singularities of the affine curves

$$y^2 = x^3 + x + 1, \tag{12}$$

$$y^2 = x^3 + x^2, \tag{13}$$

$$y^3 = x^3. \tag{14}$$

We begin by checking that the affine and projective notions are compatible:

Lemma 3.2. *If $P \in U_0 = \{X_0 \neq 0\} \subset \mathbb{P}^2$, then for any projective curve C, P is singular on C iff P is singular on $C_0 = C \cap U_0 \subset U_0 \simeq \mathbb{A}^2$.*

Proof. Let F be a homogeneous equation for C, so that

$$f(x, y) = F(1, x, y)$$

is an affine equation for C_0. Then

$$\frac{\partial f}{\partial x}(P) = \frac{\partial F}{\partial X_1}(P), \frac{\partial f}{\partial y}(P) = \frac{\partial F}{\partial X_2}(P) \tag{15}$$

From this it is immediate that a singular point on C is singular on C_0. Conversely, if P is singular on C_0 then

$$\frac{\partial F}{\partial X_1}(P) = \frac{\partial F}{\partial X_2}(P) = 0.$$

If $d = \deg(F)$, then

$$F(X_0, X_1, X_2) = X_0^d f(X_1/X_0, X_2/X_0)$$

therefore by the chain rule,

$$\frac{\partial F}{\partial X_0}(P) = dX_0 f(X_1/X_0, X_2/x_0) + X_0^d \frac{\partial f}{\partial x}(P)(\frac{-X_1}{X_0^2}) + X_0^d \frac{\partial f}{\partial y}(P)(\frac{-X_2}{X_0^2}).$$

The first term is zero because $P \in C_0$, while the other two are zero because P is singular on C_0.

□

Note that given a point P on a projective curve C, one can always choose coordinates so that $P \in U_0$, so one can study the singularity or nonsingularity of C at P via the affine curve $C \cap U_0$.

The set of singular points of a curve C is denoted $\text{sing}(C)$. Thus, the foregoing Lemma is the statement that $\text{sing}(C \cap U_0) = \text{sing}(C) \cap U_0$ for any projective curve C.

Proposition 3.3. *For any curve C, $\text{sing}(C)$ is finite.*

Proof. We do the proof in the projective case; the affine case is similar. Suppose first that $C = \text{Zeros}(F)$ is irreducible. Thus F is irreducible, say of degree d. We may assume $F_1 = \frac{\partial F}{\partial X_1} \neq 0$. Then F_1 is homogenous of degree d_1 and since F is irreducible, F and F_1 have no common factor. Then by Little Bézout, $\text{Zeros}(F) \cap \text{Zeros}(F_1)$ is finite (in fact, has at most $d(d-1)$ points. But the latter intersection obviously contains $\text{sing}(C)$, to $\text{sing}(C)$ is finite too.

Now suppose C is reducible, say $C = C_1 \cup C_2$, so the homogeneous equation F of C splits as $F = F_1F_2$ with $C_i = \text{Zeros}(F_i), i = 1, 2$. By the product rule,

$$\nabla(F_1F_2)(P) = F_1(P)\nabla F_2(P) + F_2(P)\nabla F_1(P).$$

If this is zero and $F(P) = 0$, either $F_2(P) = 0, F_1(P) \neq 0$, in which case $\nabla F_2(P) = 0$; or $F_1(P) = 0, F_2(P) \neq 0$, in which case $\nabla F_1(P) = 0$; or $F_1(P) = F_2(P) = 0$. Therefore

$$\text{sing}(C_1 \cup C_2) = \text{sing}(C_1) \cup \text{sing}(C_2) \cup C_1 \cap C_2 \tag{16}$$

From this, an obvious induction on the number of irreducible components of C proves our assertion. □

Remark 3.1. For $k = \mathbb{C}$, some of the significance of nonsingular points comes from the *implicit function theorem* which says that if f is a polynomial such that $f(x_0, y_0) = 0, \partial f/\partial x(x_0, y_0) \neq 0$, then there is an analytic function (not a polynomial in general) $y(x)$ defined in some disc D around x_0, such that if $x \in D$, then $f(x, y) = 0$ iff $y = y(x)$; similarly if $\partial f/\partial y(x_0, y_0) \neq 0$. In terms of the corresponding curve $C = \mathrm{Zeros}(f)$, this says that if P is a nonsingular point on C, then there is a piece of C that is a graph of an analytic function $y = y(x)$ or $x = x(y)$. This implies that this piece of C is an 'analytic manifold'.

The singularity of an affine curve C with equation f at a point $P = (a, b) \in C$ is closely related to the Taylor expansion of f at P: we can write

$$f(x,y) = \sum_{k=1}^{m} \sum_{i+j=k} \frac{1}{i!j!} \frac{\partial^k f(a,b)}{\partial x^i \partial y^j} (x-a)^i (y-b)^j \tag{17}$$

$$= \sum_{k=1}^{m} f_k \tag{18}$$

with each f_k homogenous of degree k in $x - a, y - b$ (and $f_0 = 0$ because $P \in C$). Note that C is nonsingular at P iff $f_1 \neq 0$. In this case the (affine) line with equation f_1 is called the *tangent line* to C at P, denoted $T_P C$. In general, the smallest k such that $f_k = 0$ is called the *multiplicity* of C at P (or the multiplicity of P on C). Note that in that case we can factor the homogenous polynomial f_k (which is known as the *leading form* of f at P) as

$$f_k = \prod_{i=1}^{k} [\alpha_i (x-a) + \beta_i (y-b)] \tag{19}$$

The lines L_i with equations

$$\alpha_i (x-a) + \beta_i (y-b) = 0$$

are called the *generalized tangent lines* of C at P. The union of these lines (i.e. the zero-set of f_k) is known as the *tangent cone* to C at P.

Points of multiplicity 2 are known as *double points* or *nodes*. A node or double point (more generally, a singular point of multiplicity k) is said to *ordinary* if the tangent cone consists of k *distinct* lines (i.e. the leading form splits as a product of distinct linear factors).

In the projective case, if P is a nonsingular point on the projective curve C with homogeneous equation F, we define the tangent line to C at P, denoted $T_P C$, as the projective line with equation

$$\nabla F(P).(X_0, X_1, X_2) = 0.$$

This is denoted by T_PC. This notion is compatible with the affine one because of the following

Lemma 3.4. *If $P \in U_0 \simeq \mathbb{A}^2$, then $T_PC \cap U_0$ is the affine line $T_P(C \cap U_0)$.*

Proof. Write $P = [1, a, b]$ and let f be an affine equation for $C_0 = C \cap U_0$. Then

$$F(X_0, X_1, X_2) = X_0^d f(X_1/X_0.X_2/X_0)$$

hence

$$\nabla F(X_0, X_1, X_2) =$$
$$(dX_0^{d-1} f(X_1/X_0, X_2/X_0) - X_0^{d-2} X_1 \frac{\partial f}{\partial x}(X_1/X_0, X_2/X_0)$$
$$-X_0^{d-2} X_2 \frac{\partial f}{\partial y}(X_1/X_0, X_2/X_0),$$
$$X_0^{d-1} \frac{\partial f}{\partial x}(X_1/X_0, X_2/X_0), \frac{\partial f}{\partial y}(X_1/X_0, X_2/X_0))$$

Plugging in $(X_0, X_1, X_2) = (1, a, b)$, we get

$$\nabla F(P) = (-a\frac{\partial f}{\partial x}(a, b) - b\frac{\partial f}{\partial y}(a, b), \frac{\partial f}{\partial x}(a, b), \frac{\partial f}{\partial y}(a, b)) \tag{20}$$

Thus, T_PC is the line with homogenous equation

$$X_0(-a\frac{\partial f}{\partial x}(a, b) - b\frac{\partial f}{\partial y}(a, b)) + X_1\frac{\partial f}{\partial x}(a, b) + X_2\frac{\partial f}{\partial y}(a, b)$$

Dehomogenizing this yields

$$(x - a)\frac{\partial f}{\partial x}(a, b) + (y - b)\frac{\partial f}{\partial y}(a, b)$$

i.e exactly the affine equation for T_PC_0.

□

Note that for a nonsingular point P on a projective curve $C = \text{Zeros}(F)$, the tangent line T_PC may be viewed as a point in the dual projective plane $\mathbb{P}^{2*}$; it is just the point with homogeneous coordinates

$$[\nabla F(P)] = [\frac{\partial F}{\partial X_0}(P), \frac{\partial F}{\partial X_1}(P), \frac{\partial F}{\partial X_2}(P)].$$

Therefore if C is nonsingular, say of degree d, this yields a well defined mapping, known as the *dual mapping*

$$D : C \to \mathbb{P}^{2*}.$$

It can be shown that the image $C^* := D(C) \subset \mathbb{P}^{2*}$ is itself a curve, and it has degree $d^* = d(d-1)$ (this is known as one of the *Plücker formulas*). If $d > 3$, C^* will always be singular.

As in the affine case, one can talk about the multiplicity and generalized tangent lines of a projective curve C or homogeneous polynomial F at a point $P \in \mathbb{P}^2$. For future reference, we note the following

Lemma 3.5. *(i) The vector space V_n of homogeneous polynomials of degree n in X_0, X_1, X_2 is of dimension $n(n+2)/2$;*

(ii) the subspace $V_n(r, P) \subset V_n$ of polynomials having multiplicity at least r ar P is of codimension $r(r+1)/2$.

(iii) for any collection of points $P_1, ..., P_k$ and natural numbers $r_1, ..., r_k$, the subspace $V_n(r_1, P_1; ... : r_k, P_k)$ of polynomials having multplicity at least r_i at each $P_i, i = 1, ..., k$ is of codimension at most $\sum \binom{r_i+1}{2}$.

Example 3.6. Let C be a nonsingular conic. Then C is projectively equivalent to the conic C_0 with equation $F = X_0^2 + X_1^2 + X_2^2$. For this C_0 the dual mapping is just

$$[X_0, X_1, X_2] \mapsto [2X_0, 2X_1, 2X_2] = [X_0, X_1, X_2]$$

so the dual C_0^* is just C_0 itself. Therefore for any nonsingular conic C, the dual C^* is a conic (not necessarily equal to C; in fact if $C = T_A^*(C_0)$ then $C^* = T_{A^t}^*(C_0) \neq C$). The fact that C^* is a conic means, concretely, that through a general point of $\mathbb{P}^2$ there are just 2 lines tangent to C.

A famous fact from classical projective geometry related to this is known as *Poncelet's porism.* Let C_1, C_2 be two general conics and choose a general point $P_0 \in C_1$. Let L_1 be one of the two tangent lines to C_2 through P_0, and P_1 the other intersection point of L_1 with C_2. Now at P_1 there will be, besides L_1, a second line, say L_2, tangent to C_2; the procedure may be iterated indefinitely. The question is: is this process periodic, i.e. is $P_n = P_0$ for some n (in which can it is easy to see that $P_{n+1} = P_1$ etc.) Poncelet's theorem is that *the process being periodic depends only on the conics C_1, C_2 and not on the choice of starting point P_0.* Interestingly, the proof depends on a certain cubic (elliptic) curve and its group structure, specifically on whether a certain point on this elliptic curve has finite order in the group structure.

4. Intersection numbers and Bézout's theorem

Definition 1. *A point $Q \in \mathbb{P}^2$ is said to be a* good center *with respect to curves C, D (or their equations) if*

(i) $Q \notin C \cup D$
(ii) *Q is not on any line joining two distinct points of $C \cap D$.*

Theorem 4.1. *There exist unique symbols $I_P(F,G) = F \cdot_P G, I_P(C,D) = C \cdot_P D$, where $P \in \mathbb{P}^2$ is a point, F, G are nonzero homogeneous polynomials and $C, D \subset \mathbb{P}^2$ are curves, such that*

$$I_P(C,D) = I_P(F,G)$$

whenever F, G are reduced equations for C, D, and such that

(i) $I_P(C,D) = I_P(D,C)$;
(ii) *$I_P(C,D) = \infty$ iff C, D have a common component through p and otherwise $I_P(C,D)$ is a nonnegative integer;*
(iii) *$I_P(C,D) = 0$ iff $p \notin C \cap D$*
(iv) *if L_1, L_2 are distinct lines through p, then $I_P(L_1, L_2) = 1$;*
(v) $I_P(F_1F_2, G) = I_P(F_1, G) + I_P(F_2, G)$;
(vi) *if $\deg(F) \leq \deg(G)$ and $\deg(H) = \deg(G) - \deg(F)$ then $I_P(F,G) = I_P(F, G + HF)$.*

Moreover, if $Q = [0,0,1]$ is a good center with respect to F, G, $p = [a,b,c] \neq Q$ and $\bar{p} = [a,b]$, then

- *$I_P(F,G)$ is the multiplicity at $\bar{p}$ of the resultant $r(F,G;X_2)$ of F, G with respect to X_2.*

Proof. We first show that the properties (i)-(vi) characterize I_P uniquely. To simplify notation, we may assume $P = [1,0,0]$. We may assume that F, G are irreducible, distinct, and both vanish at P. Set $k = I_P(F,G)$. By induction on k, we may assume I_P is already uniquely determined if its value is $< k$. Set

$$f(y) = F(1,0,y), r = \deg f, g(y) = G(1,0,y), s = \deg g.$$

By symmetry (axiom (i)), we may assume $r \leq s$. Suppose first that $f = 0$. This clearly means that $X_1 | F$, so write $F = X_1 H$, hence

$$I_P(F,G) = I_P(X_1, G) + I_P(H,G).$$

Write

$$G = G(X_0, 0, X_2) + X_1 Q(X_0, X_1, X_2)$$

(i.e. $G(X_0, 0, X_2)$ is the part of G not involving X_1), and

$$G(X_0, 0, X_2) = X_2^q T$$

where $X_2 \nmid T$ which means precisely $T(1,0,0) \neq 0$. Note $q > 0$. Then

$$I_P(X_1, G) = I_P(X_1, G(X_0, 0, X_2)) = I_P(X_1, X_2^q T) = I_P(X_1, X_2^q) = q.$$

Moreover $I_P(H, G) = k - q < k$, so inductively it is already uniquely determined. Therefore so is $I_P(F, G)$.

Now suppose $f \neq 0$. Since $f(0) = 0$, this implies $r > 0$. We may assume f, g both monic. Set

$$S = X_0^{N-\deg(G)} G - X_0^{N-\deg(F)-s+r} X_2^{s-r} F$$

for some sufficiently large integer N. Then

$$S(1, 0, y) = g - y^{s-r} f$$

is of degree $< s$. Moreover since F, G are distinct irreducible, $S \neq 0$. Then

$$I_P(F, S) = I_P(F, X_0^{N-\deg(G)} G) = I_P(F, G).$$

If S is reducible, $I_P(F, S)$ is determined by additivity (property (v)); else, an induction on s shows $I_P(F, G)$ is uniquely determined.

We now prove existence of I_P.

(a) If P is in a common component of the zero-sets of F, G, set $I_P(F, G) = \infty$.

(b) If P is not a common zero of F, G, set $I_P(F, G) = 0$.

(c) Otherwise, remove all common factors from F, G, choose coordinates so that $[0, 0, 1]$ is a good center with respect to F, G and $P = [1, 0, 0]$ and define $I_P(F, G)$ according to $\bullet$ above.

Then (i) above follows from $\pm$ symmetry of the resultant; (ii) follows from the fact that in case (c) F, G have no common factor so their resultant $r \neq 0$. (iii) follows from the fact that in case (c), using notation as above $f(y), g(y)$ have the same degrees as F, G and have no common zeros $y \neq 0$. Therefore F, G both vanish at p iff f, g have a common zero iff $r(1, 0) = 0$ iff the multiplicity of $[1, 0]$ as zero of r is > 0.

Now (iv) is the following easy calculation: if $F = a_1 X_1 + a_2 X_2, G = b_1 X_1 + b_2 X_2$, then

$$r = \det \begin{bmatrix} a_1 X_1 & a_2 \\ b_1 X_1 & b_2 \end{bmatrix} = (a_1 b_2 - a_2 b_1) X_1$$

and the coefficient is clearly $\neq 0$.

Finally, (v)-(vi) follow from standard properties of the resultant. □

An immediate consequence of the defining axioms of the Intersection Number I_P is the following

Corollary 4.2. *If L is a line through p with equation F and $F \nmid G$ then*

$$I_P(F, G) = \mathrm{mult}_P(G|_L).$$

Proof. We may assume $F = X_2, P = [1, 0, 0,]$. Write

$$G = G_0(X_0, X_1) + X_2G_1 = X_1^r G_0'(X_0, X_1) + X_2G_1, G_0'(1, 0) \neq 0.$$

Then

$$I_P(F, G) = I_P(X_2, G_0) = I_P(X_2, X_1^r) = r = \mathrm{mult}_P(G|_L).$$

□

As an immediate consequence of the definition via resultants, we obtain

Theorem 4.3. *(Bézout) If F, G are homogeneous polynomials of degrees m, n with no common factor, then*

$$\sum_P I_P(F, G) = mn. \tag{21}$$

If C, D are curves in $\mathbb{P}^2$ of degrees m, n with no common component, then

$$\sum_P I_P(C, D) = mn. \tag{22}$$

Proof. It suffices to prove the polynomial version. Applying a suitable projective transformation- which doesn't affect either side of the claimed equality- we may assume $Q = [0, 0, 1]$ is good center with respect to F, G. As F, G have no common factor, their resultant r is a nonzero homogeneous polynomial of degree mn, hence r has mn zeros, counting multiplicities. On the other hand, by the above proof, those multiplicities correspond exactly to the intersection numbers of F, G. Therefore the result follows. □

As in the case of $\mathbb{P}^1$, we can define the group of cycles

$$Z(\mathbb{P}^2) = \{\sum n_i[P_i] : n_i \in \mathbb{Z}\}$$

and its subset (closed under addition) $Z_+(\mathbb{P}^2)$ of cycles with nonnegative coefficients. The *degree* of a cycle is defined as

$$\deg(\sum n_i[P_i]) = \sum n_i \in \mathbb{Z}.$$

Given curves C, D without common component, we can define their *intersection cycle* $C \cdot D$ or $I(C, D)$ as

$$C \cdot D = \sum_{P \in \mathbb{P}^2} I_P(C, D)[P] \tag{23}$$

We similarly define $F \cdot G$ or $F \cdot C$. Then Bézout's Theorem is just the statement that

$$\deg(C \cdot D) = \deg(C) \deg(D).$$

Theorem 4.4. *(Local intersection inequality) If F, G have multiplicities r, s at P, then*

$$I_P(F,G) \geq rs.$$

Proof. We may assume $P = [1,0,0]$ and dehomogenize as usual. Write

$$f = f_0x^r + f_1x^{r-1}y + ... + f_r y_r + f_{r+1}y^{r+1}...$$

$$g = g_0x^s + g_1x^{s-1}y + ... + g_s y^s + g_{s+1}y^{s+1}...$$

with f_i, g_i polynomials in x. Then we have the resultant

$$(24) \qquad r = \det \begin{bmatrix} f_0x^r & & \dots & f_r & f_{r+1} & \dots & \dots & 0 \\ 0 & f_0x^r & \dots & & f_r & f_{r+1}\dots & \dots & 0 \\ & & & \dots & & & & \\ & & & & f_0x^r & & \dots & f_m \\ g_0x^s & & \dots & g_s & g_{s+1} & \dots & \dots & 0 \\ 0 & g_0x^s & & \dots & g_s & g_{s+1}\dots & \dots & 0 \\ & & & \dots & & & & \\ & & & & g_0x^s & & \dots & g_n \end{bmatrix}$$

Now as in the proof of Thm 2.3, multiply the 1st row by x^s, the 2nd by x^{s-1} etc., then the sth row by x^r etc. Then the 1st column becomes divisible by x^{r+s}, the 2nd by x^{r+s-1} etc. Then the same computation as in the proof of Thm 2.3 yields that the x-multiplicity of r, i.e. $I_P(F,G)$, is at least rs.

□

Corollary 4.5. *If F, G have no common factors then*

$$\deg F \deg G \geq \sum \mu_P(F)\mu_P(G).$$

Corollary 4.6. *If F of degree n has no multiple factors then*

$$n(n-1) \geq \sum \mu_P(F)(\mu_P(F) - 1).$$

Proof. Choosing coordinates properly, we may assume F has no irreducible factor R independent of X_0, hence $F_0 = \partial F/\partial X_0 \neq 0$.

Lemma 4.7. *If G is a common factor of $F, \partial F/\partial X_0$ then either G is a multiple factor of F or $\partial G/\partial X_0 = 0$.*

Proof. We may assume G is irreducible. Write

$$F = G^m H, G \nmid H.$$

Then

$$F_0 = G^m H_0 + mG_0G^{m-1}H$$

Since this is divisible by G, $G|G_0G^{m-1}H$ so either $m > 1$ or $G_0 = 0$.

□

To prove the corollary, notice that

$$\mu_P(F_0) \geq \mu_P(F) - 1$$

By the Lemma, F and F_0 cannot have any common factor in our case, so we are done by the previous Corollary.

□

The local intersection inequality yields quite a bit more information on the 'amount of singularity' a curve can have. For example, suppose C is a cubic with 2 singular points P_1, P_2 and apply the above Cor. 4.5 to C and the line $L = \overline{P_1, P_2}$. We get a contradiction unless L is a component of C. In particular, *an irreducible can have at most one singular point P, and P must be a double point.* This reasoning can be generalized as follows.

Note that the vector space V_n of homogeneous polynomials of degree n in X_0, X_1, X_2 is of dimension $\binom{n+2}{2}$. Moreover, it is easy to check that the subspace $V_n(r, P)$ of polynomials having multiplicity at least r at p is of codimension $\binom{r+1}{2}$. It follows that for any collection of points $P_1, ..., P_k$ and natural numbers $r_1, ..., r_k$, the subspace $V_n(r_1, P_1; ... : r_k, P_k)$ of polynomials having multplicity at least r_i at each $P_i, i = 1, ..., k$ is of codimension *at most* $\sum \binom{r_i+1}{2}$.

Theorem 4.8. *Let F be an irreducible polynomial of degree n having points P_i of multiplicity $r_i, i = 1, ..., k$. Then*

$$\sum r_i(r_i - 1) \leq (n-1)(n-2) \tag{25}$$

Proof. We have

$$\sum r_i(r_i - 1)/2 \leq n(n-1)/2 \leq (n-1)(n+2)/2 = \dim V_{n-1} - 1.$$

Therefore there exists a polynomial G of degree $n-1$ having multiplicity at least $r_i - 1$ at each P_i, and through $(n-1)(n+2)/2 - \sum r_i(r_i - 1)/2$ further points on C. Since F, G can have no common factor, Bézout's Theorem and the intersection inequality yield

$$n(n-1) \geq \sum r_i(r_i - 1) + (n-1)(n+2)/2 - \sum r_i(r_i - 1)/2$$

which is the inequality claimed. □

Example 4.9. For $n = 2$ the Theorem says that an irreducible conic is nonsingular, which we knew already. For $n = 3$ it says an irreducible cubic has at most 1 singular point of multiplicity 2 (double point). Example: $X_0 X_2^2 = X_1^3 + X_1^2 X_0$.

For $n = 4$ it says an irreducible quartic either has 3 or fewer double points, or a triple point and no other singularities. All these cases actually occur. Examples: $X_0^2X_1^2 + X_1^2X_2^2 + X_0^2X_2^2$ (3 double points), $X_0(X_1^3 + X_2^3) + X_1^4 + X_2^4$ (1 triple point).

Theorem 4.10. *Let C be an irreducible curve of degree n having points P_i of multiplicity $r_i, i = 1, ..., k$ such that*

$$\sum r_i(r_i - 1) = (n-1)(n-2) \tag{26}$$

Then there is a homogeneous parametrization

$$f : \mathbb{P}^1 \to C.$$

Proof. (Sketch) As in the preceding proof, consider the vector space $V_{n-1}(r_1 - 1, P_1; ...; r_k - 1, P_k)$ which by our hypothesis has dimension at least

$$\binom{n}{2} - \binom{n-2}{2} = 2n - 1.$$

Choose $2n - 3$ further distinct points $Q_1, ..., Q_{2n-3}$ on C. Then

$$\dim V_{n-1}(r_1 - 1, P_1; ...; r_k - 1, P_k; 1, Q_1 :, ...; 1, Q_{2n-3}) \geq 2.$$

Choose a 2-dimensional subspace W of this vector space. W may be identified with k^2. Note that

$$n(n-1) - \sum r_i(r_i - 1) - (2n - 3) = 1$$

Now for $F \in W$, we have

$$F.C - \sum r_i(r_i - 1)P_i - \sum Q_i$$

is a nonnegative cycle on C of degree 1, hence of the form Z_F so defining

$$f : \mathbb{P}^1 \to C,$$
$$F \mapsto Z_F$$

yields a nonconstant map. Now results of general algebraic geometry, not covered in this course, show that f is automatically a homogeneous parametrization. □