5 Bézout's Theorem

Throughout this section we will assume that K is an algebraically closed field.

Suppose $f, g \in K[X, Y]$ are nonconstant. Our goal in this section is to analyze $|V(f) \cap V(g)|$. One possibility is that f and g have a common nonconstant factor h. In that case $V(h) \subseteq V(f) \cap V(g)$ and $V(f) \cap V(g)$ is infinite. In case f and g have no common nonconstant factor we will prove that $V(f) \cap V(g)$ is finite and

$$|V(f) \cap V(g)| \leq \deg f \deg g.$$

We begin by describing the main idea of the proof. Suppose $f, g \in K[X, Y]$ are nonconstant polynomials with no common nonconstant factors, $\deg f = n$ and $\deg g = m$. By applying an affine transformation if necessary, we may assume that $f(0,0) \neq 0$ and $g(0,0) \neq 0$. The following proposition is the key to the proof.

Proposition 5.1 *There are at most mn lines L through $(0,0)$ such that $L \cap V(f) \cap V(g) \neq \emptyset$.*

We first argue that $V(f) \cap V(g)$ is finite. Let $L_1, \ldots, L_s$ be the lines through $(0,0)$ that intersect $V(f) \cap V(g)$. If $p \in V(f) \cap V(g)$, then there is a unique line L containing p and $(0,0)$ and L must be one of the L_i. Thus

$$V(f) \cap V(g) = \bigcup_{i=1}^{s} (V(f) \cap V(g) \cap L_i).$$

If L is a line and $V(f) \cap V(g) \cap L$ is infinite, then $V(f) \cap L$ is infinite and, by Theorem 3.16 $L \subseteq V(f)$. Similarly, $L \subseteq V(g)$. If $h = 0$ is the linear equation for L, then, by Study's Lemma, h is a common factor of f and g. Thus each L_i intersects $V(f) \cap V(g)$ in at most finitely many points and $V(f) \cap V(g)$ is finite.

Suppose $|V(f) \cap V(g)| = N$. For each pair of distinct points $p, q \in V(f) \cap V(g)$ let $L_{p,q}$ be the unique line containing p and q. Note that

$$|\{L_{p,q} : p, q \in V(f) \cap V(g) \text{ distinct}\}| = \frac{N(N-1)}{2}.$$

By doing a second affine transformation we may assume that $(0,0)$ is not on $V(f)$, $V(g)$ or any of the lines $L_{p,q}$. Let $L_1, \ldots, L_s$ be all lines through $(0,0)$ containing a point of $V(f) \cap V(g)$. Since $(0,0) \in L_i$, $L_i \neq L_{p,q}$ for any distinct $p, q \in V(f) \cap V(g)$. Thus $|L_i \cap V(f) \cap V(g)| = 1$ and

$$|V(f) \cap V(g)| = s \leq mn.$$

In fact, we will not prove the proposition in the form we have stated it. It is somewhat easier to work in projective space rather than affine space and by working in projective space we will be able to prove the following stronger result.

For $F \in K[X, Y, Z]$ homogeneous, we let

$$V_{\mathbb{P}}(F) = \{p \in \mathbb{P}_2(K) : F(p) = 0\}.$$

Theorem 5.2 (Bézout's Theorem) *Let $F, G \in K[X,Y,Z]$ be nonconstant homogeneous of degree m and n respectively. Either F and G have a common nonconstant factor or $|V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)| \leq mn$.*

Moreover, if F and G have no common nonconstant factor, there is a natural way to assign intersection multiplicities $m_p(F,G)$ for each $p \in V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)$ such that

$$\sum_{p \in V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)} m_p(F,G) = mn.$$

Resultants of Homogeneous Polynomials

The key to proving Bézout's Theorem is a result about resultants of homogeneous polynomials. We need one basic fact about homogeneous polynomials.

Exercise 5.3 Suppose $F \in K[X,Y,Z]$ is nonzero. Consider the polynomial $F(TX,TY,TZ) \in K[X,Y,Z,T]$. Then F is homogeneous of degree d if and only if

$$F(TX,TY,TZ) = T^d F(X,Y,Z).$$

[Hint: See 3.6]

Theorem 5.4 *If $F, G \in K[X,Y,Z]$ are nonconstant homogeneous polynomials with no common nonconstant factors such that $F(0,0,1) \neq 0$ and $G(0,0,1) \neq 0$, then $R_{F,G}$ is homogeneous of degree* deg $F \cdot$ deg G.

Proof By Theorem 4.19, if F and G have no common factor, then $R_{F,G}$ is a nonzero polynomial. We will prove that $R_{F,G}$ is homogeneous of degree d by showing that

$$R_{F,G}(TX,TY) = T^{nm} R_{F,G}(X,Y).$$

Let

$$F = \sum_{i=0}^{n} a_i Z^i \text{ and } G = \sum_{i=0}^{m} b_i Z^i$$

where $a_i, b_i \in K[X,Y]$, a_i is homogeneous of degree $n-i$, b_i is homogeneous of degree $m-i$. Since $F(0,0,1) \neq 0$, $a_n \neq 0$. Similarly, $b_m \neq 0$. Thus $R_{F,G}(TX,TY) =$

$$\begin{vmatrix}
a_0T^n & a_1T^{n-1} & \dots & \dots & \dots & a_n & 0 & \dots & \dots & 0 \\
0 & a_0T^n & a_1T^{n-1} & \dots & \dots & \dots & a_n & 0 & \dots & 0 \\
 & & & \ddots & \ddots & & & & & \\
0 & \dots & \dots & 0 & a_0T^n & a_1T^{n-1} & \dots & \dots & \dots & a_n \\
b_0T^m & b_1T^{m-1} & \dots & \dots & b_m & 0 & \dots & \dots & \dots & 0 \\
0 & b_0T^m & b_1T^{m-1} & \dots & \dots & b_m & 0 & \dots & \dots & 0 \\
 & & & \ddots & \ddots & & & & & \\
0 & \dots & \dots & \dots & 0 & b_0T^m & b_1T^{m-1} & \dots & \dots & b_m
\end{vmatrix}.$$

We modify the determinant by multiplying the ith row by T^{m+1-i} for $i = 1...m$ and the $m+i$th row by T^{n+1-i} for $i = 1...n$.

The first m lines now look like:

$$\begin{array}{cccccccccc}
a_0T^{n+m} & a_1T^{n+m-1} & \dots & \dots & \dots & a_nT^m & 0 & \dots & \dots & 0 \\
0 & a_0T^{n+m-1} & a_1T^{n+m-2} & \dots & \dots & \dots & a_nT^{m-1} & 0 & \dots & 0 \\
 & & & \ddots & \ddots & & & & & \\
0 & \dots & \dots & 0 & a_0T^{n+1} & a_1T^n & \dots & \dots & \dots & a_nT
\end{array}$$

while the last n lines look like:

$$\begin{array}{cccccccccc}
b_0T^{m+n} & b_1T^{m+n-1} & \dots & \dots & b_mT^n & 0 & \dots & \dots & \dots & 0 \\
0 & b_0T^{m+n-1} & b_1T^{m+n-2} & \dots & \dots & b_mT^{n-1} & 0 & \dots & \dots & 0 \\
 & & & \ddots & \ddots & & & & & \\
0 & \dots & \dots & \dots & 0 & b_0T^{m+1} & b_1T^m & \dots & \dots & b_mT
\end{array}.$$

Recall that if we multiply one row of a matrix A by λ, then the determinant of the new matrix is $\lambda \det A$. Thus the determinant above is equal to

$$T^{(\sum_{i=1}^{n} i + \sum_{j=1}^{m} j)} R_{F,G}(TX, TY).$$

To finish the proof we want to show in every element of the jth column the power of T occuring is $T^{m+n+1-j}$. Suppose $i = 1, \dots, m$ in the matrix to compute $R_{F,G}(TX, TY)$ the element in the ith row and jth column is 0 if $j < i$ or $j > i + n + 1$. Otherwise it is

$$a_{j-i}T^{n+i-j}.$$

When we modify the matrix to make the second determinant if $1 \leq i \leq m$ and $i \leq j \leq n + i + 1$, the element in the ith row and jth column is

$$a_{j-i}T^{n+i-j}T^{m+1-i} = a_{j-1}T^{n+m+1-j}.$$

Similarly if $1 \leq i \leq n$ and $i \leq j \leq m + i + 1$ then element in the $(m + i, j)$ position of the first determinant is

$$b_{j-i}T^{m+i-j}$$

while in the second matrix it is

$$b_{j-i}T^{m+i-j}T^{n+1-i} = b_{j-i}T^{n+m+1-j}.$$

Notice that all nonzero entries of the jth column of the second matrix have a $T^{n+m+1-j}$ term. It follows that we could have gotten the second determinant starting with the matrix to compute $R_{F,G}$ and multiplying the first column by T^{n+m}, the second by T^{n+m-1},…,the last by T. Since multiplying a column of a matrix by λ multiplies the determinant by λ. This shows that the second determinant is equal to

$$T^{\sum_{j=1}^{n+m} j} R_{F,G}.$$

Thus

$$T^{\sum_{j=1}^{n+m} j} R_{F,G} = T^{(\sum_{i=1}^{n} i + \sum_{j=1}^{m} j)} R_{F,G}(TX, TY)$$

and

$$R_{F,G}(TX, TY) = T^{(\sum_{j=1}^{n+m} j - \sum_{i=1}^{n} i - \sum_{k=1}^{m} k)} R_{F,G}.$$

But

$$\sum_{i=1}^{s} i = \frac{s(s+1)}{2}.$$

Thus

$$\sum_{j=1}^{n+m} j - \sum_{i=1}^{n} i - \sum_{j=1}^{m} j = \frac{(n+m)^2 + (n+m) - n^2 - n - m^2 - m}{2} = nm$$

and

$$R_{F,G}(TX, TY) = T^{nm} R_{F,G}$$

as desired.

Proof of Bézout's Theorem

We now state and prove the projective version of Proposition 5.1

Proposition 5.5 *Suppose $F, G \in K[X, Y, Z]$ are nonconstant homogeneous polynomials with* $\deg F = n$ *and* $\deg G = m$ *such that* $F(0,0,1) \neq 0$*,* $G(0,0,1) \neq 0$*, and F and G have no common nonconstant factors. Then there are at most mn lines in $\mathbb{P}_2(K)$ through $[0,0,1]$ containing a point of $V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)$.*

Proof Since F and G have no common factor, by Theorem 5.4, $R_{F,G}$ is a homogeneous polynomial of degree mn.

In general, projective lines have equations $aX + bY + cZ = 0$, but lines through $[0,0,1]$ have equations $aX + bY = 0$.

Claim Let L be the line $aX + bY = 0$. Then $V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G) \cap L \neq \emptyset$ if and only if $R_{F,G}(b, -a) = 0$.

If $[x, y, z]$ are homogeneous coordinates for a point on L where $x \neq 0$, then $y = \frac{-a}{b} x$ and

$$F(x, y, z) = 0 \Leftrightarrow F(x, \frac{-a}{b} x, z) = 0 \Leftrightarrow F(b, -a, \frac{bz}{x}) = 0.$$

It follows that $V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G) \cap L \neq \emptyset$ if and only if there is a w such that

$$F(b, -a, w) = G(b, -a, w) = 0.$$

Let $f(X) = F(b, -a, X)$ and $g(X) = G(b, -a, X)$. By Theorem 1.22, f and g have a common zero if and only if $R_{f,g} = 0$. But, as in the proof of Study's Lemma,

$$R_{f,g} = R_{F,G}(b, -a).$$

Thus $V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G) \cap L \neq \emptyset$ if and only if $R_{F,G}(b, -a) = 0$.

Since $\lambda aX + \lambda bY = 0$ is the same line as $aX + bY = 0$, lines that contain points of $V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)$ correspond to points of $\mathbb{P}_1(K)$ where $R_{F,G} = 0$. But $R_{F,G} = 0$ has degree mn and at most mn zeros in $\mathbb{P}_1(K)$. Thus there are at most mn lines through $[0, 0, 1]$ intersecting $V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)$.

The proof of Bézout's Theorem now follows the outline at the beginning of the section.

Proof of Bézout's Theorem

Suppose $F, G \in K[X, Y, Z]$ are homogeneous of degree n and m respectively with no common factor. By making a projective transformation we may assume that $F(0, 0, 1) \neq 0$ and $G(0, 0, 1) \neq 0$. Suppose L is a line through $[0, 0, 1]$. If $L \cap V_{\mathbb{P}}(F)$ is infinite, then by Theorem 3.16, $L \subseteq V_{\mathbb{P}}(F)$. By the projective version of Study's Lemma, if $H = 0$ is the homogeneous linear equation for L, then H divides F. Thus if $V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G) \cap L$ is infinite, then H divides F and G, a contradiction. Thus $L \cap V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)$ is finite. Since only finitely many lines through $[0, 0, 1]$ intersect $V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)$, $V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)$ is finite.

Let $C_1, \ldots, C_N$ be all lines containing two or more points of $V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)$. By making a second projective transformation, we may, in addition, assume that $[0, 0, 1] \notin C_i$ for $i = 1, \ldots, N$. Thus if $L_1, \ldots, L_s$ are the lines through $[0, 0, 1]$ intersecting $V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)$, then $|L \cap V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)| = 1$. Thus

$$|V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)| = s \leq mn.$$

It remains to show how to define the intersection multiplicities. Assume, via projective transformations, that we are in the setting where $F(0, 0, 1) \neq 0$, $G(0, 0, 1) \neq 0$ and no line through $[0, 0, 1]$ contains more than one point of $V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)$. There is a one-to-one correspondence between:

i) points of $V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)$;

ii) lines through $[0, 0, 1]$ intersecting $V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)$;

iii) zeros of $R_{F,G}$ in $\mathbb{P}_1(K)$.

Indeed if $p = [a, b, c] \in V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)$, then $R_{F,G}(a, b) = 0$ and c is the unique z such that $[a, b, z] \in V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)$. We let $m_p(F, G)$ be the multiplicity of $[a, b]$ as a zero of $R_{F,G}$. By the remarks after the proof of Theorem 3.16, we see that

$$\sum_{p \in V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)} m_p(F, G) = mn$$

as desired.

Suppose $C = V_{\mathbb{P}}(F)$ is a projective curve. We can factor $F = F_1^{m_1} \cdots F_k^{m_k}$ where $F_1, \ldots, F_k$ are relatively prime irreducible polynomials. Note that

$$C = V(F_1 \cdots F_k).$$

We say that F is a *minimal polynomial for C* if $F = V_{\mathbb{P}}(C)$ and F has no multiple irreducible factors. The previous paragraph shows that every curve has a minimal polynomial.

Exercise 5.6 Suppose F and G are minimal polynomials for a projective curve C. Prove that $F = aG$ for some $a \in K$.

Definition 5.7 If C is a projective curve, the *degree of* C is the degree of a minimal polynomial for C.

Corollary 5.8 *If C and D are projective curves with no common component, then $|C \cap D| \leq \deg C \cdot \deg D$.*

Three Example

Example 1 Let $F(X,Y,Z) = Z^3 - XY^2$ and $G(X,Y,Z) = Z^3 + XY^2$. Using the MAPLE command

```
resultant(F,G,Z);
```

We find that

$$R_{F,G} = 8X^3Y^6.$$

Suppose $[x,y,z] \in V_{\mathbb{P}}(F) \cap V_{\mathbb{P}}(G)$ then $x = 0$ or $y = 0$. If $x = 0$, then $z = 0$. While if $y = 0$, $z = 0$. Thus $[0,1,0]$ and $[1,0,0]$ are the unique points of intersection. We have

$$m_{[0,1,0]}(F,G) = 3 \text{ and } m_{[1,0,0]}(F,G) = 6.$$

What does this mean in $\mathbb{A}_2(\mathbb{C})$. Let $f(X,Y) = F(X,Y,1) = 1 - XY^2$ and $g(X,Y) = G(X,Y,1) = 1 + XY^2$. The affine curves $V(f)$ and $V(g)$ have no points of intersection. But there are two points of intersection "at infinity".

Example 2 Let $F(X,Y,Z) = X^2 - 2XZ - YZ + Z^2$ and $G(X,Y,Z) = X^2 - 4XZ - YZ + 4Z^2$. In this case the resultant is

$$R_{F,G} = -X^3(6Y - X).$$

Since $R_{F,G}(0,1) = 0$, there must be a point of intersection with homongeneous coordinates $[0,1,z]$. But then $-z + z^2 = 0$ and $-z + 4z^2 = 0$. Thus $z = 0$. Thus $[0,1,0]$ is the unique point of intersection on the line $X = 9$ and this point has multiplicity 3.

We also need to look for a point of intersection on the line $X = 6Y$. We look for a point with homogeneous coordinates $[6,1,z]$. Then

$$0 = 36 - 12z - z + z^2 = (z - 9)(z - 4)$$

and

$$0 = 36 - 24z - z + 4z^2 = (4z - 9)(z - 4).$$

Thus $z = 4$ and $[6,1,4]$ is the point of intersection. This point has multiplicity 1.

Let's look at what this means in $\mathbb{A}_2(\mathbb{C})$. Let $f(X,Y) = F(X,Y,1) = X^2 - 2X - Y + 1$ and $g(X,Y) = G(X,Y,1) = X^2 - 4X - Y + 4$. Then these two parabolas have a unique point of interesection in $\mathbb{A}_2(K)$. Since $(6,1,4) \sim (\frac{3}{2}, \frac{1}{4}, 1)$. The point of intersection is $(\frac{3}{2}, \frac{1}{4})$. There is an additional point of intersection "at infinity".

We still must address the question of what the intersection multiplicity means. The next example begins to shed some light.

Example 3 Consider the affine curves $Y = X^2 + 1$ and $Y = 1$. We investigate their intersection by first homogenizing them to

$$F(X, Y, Z) = X^2 - YZ + Z^2 \text{ and } G(X, Y, Z) = Y - Z.$$

Then $R_{F,G} = X^2$. If $x = 0$ and $y = 1$, then $z = 1$. Thus $[0, 1, 1]$ is the unique point of intersection and it has multiplicity 2.

Considering the affine equations this is not surprising since the paraboloa $Y = X^2 + 1$ and the line $Y = 1$ intersect at (0,1) and the line is tangent at this point.

Suppose we change the previous problem by taking the line $Y = a$ for any $a \neq 1$. Then

$$F(X, Y, Z) = X^2 - YZ + Z^2 \text{ and } G(X, Y, Z) = Y - aZ.$$

Then

$$R_{F,G} = aX^2 - (a-1)Y^2$$

If $a \neq 0$ and $\alpha^2 = \frac{a-1}{a}$, then

$$R_{F,G} = a(X - \alpha Y)(X + \alpha Y).$$

Since $Y = aZ$, there are two distinct solutions $[\alpha, a, 1]$ and $[-\alpha, a, 1]$.

Thus is we move the line $Y = 1$ to the line $Y = 1 \pm \epsilon$ for small $\epsilon > 0$, we get two points of intersection. This is the right intuition. If two curves point of intersection of multiplicity > 1 and we perturbe the curves slightly, than we get p distinct points of intesection.