1.14 07/10/24 - Proof(s) of Bézout's Theorem

We are now finally ready to prove Bézout's Theorem, which we state here.

Theorem 1.14.1 (Bézout). If k is an algebraically closed field, and $C, D \subset \mathbb{P}_k^2$ algebraic curves that do not share a common component, then

$$\sum_{P \in C \cap D} i_P(C, D) = (\deg C)(\deg D).$$

We showed in Theorem 1.11.20 that if C and D do not share a component, then C and D intersect in finitely many points. We will give two proofs of Theorem 1.14.1 below. The proof strategy in both case is going to be to choose a suitable coordinate system in which C and D do not intersect at infinity–that it all what we will need the projective plane for. Having done that, the rest of the proof becomes a computation in the affine plane.

1.14.1 Proof 1: Dimension Count

Proof 1 of Theorem 1.14.1. Pick a line L not meeting $C \cap D$ (this is possible by Theorem 1.11.20 and the correct salvage to Exercise 2.6.7), and choose a system of coordinates such that (i.e. assume by a projective change of coordinates that) $L = L_\infty$. Then neither C nor D contains L as a component–indeed, if, say, $L \subset C$, then it would follow from Theorem 1.12.12 that $L \cap D$ is nonempty, and then $L \cap C \cap D$ is nonempty, contrary to assumption. In particular, if F (resp. G) is a minimal polynomial for C (resp. D), and we let $f := F^{\mathrm{i}}$ (resp. $g := G^{\mathrm{i}}$) and $\deg C = n \geq 1$ (resp. $\deg D = m \geq 1$), then we have by Theorem 1.11.21 that

$$\deg f = \deg F = \deg C = m \text{ and } \deg g = \deg G = \deg D = n.$$

If we write $f = f_0 + \cdots + f_m$ and $g = g_0 + \cdots + g_n$, where each f_i and g_i is homogeneous of degree i in x and y, then $f_m g_n \neq 0$, and it follows from the assumption that $L \cap C \cap D = \emptyset$ that $f_m, g_n \in k[x, y]$ are relatively prime (for instance, thanks to Lemma 1.8.3). Finally, the fact that C and D do not share a common component implies that f and g are relatively prime. We now divide the rest of the proof into two lemmas, whose proofs we postpone for a moment.

Lemma 1.14.2. If k is an algebraically closed field and $f, g \in k[x, y]$ are relatively prime, then the following map is an isomorphism:

$$k[x, y]/(f, g) \xrightarrow{\sim} \prod_{P \in C_f \cap C_g} \mathcal{O}_P/(f, g)\mathcal{O}_P.$$

Lemma 1.14.3. If k is a field and $f, g \in k[x, y]$ have degree $m, n \geq 1$ such that f and g are relatively prime and the leading terms f_m and g_n are relatively prime, then

$$\dim_k k[x, y]/(f, g) = mn.$$

By our definition of intersection multiplicity (as in the existence part of the proof of Theorem 1.9.9), the two lemmas above combined prove Theorem 1.14.1. ∎

The first lemma is a local-to-global principle (often called Max Noether's $af + bg$ theorem), and is a sort of Chinese Remainder Theorem for curves, if you will. The second result is the global dimension computation that proves the result. Let's now prove the lemmas.

Lemma 1.14.2. If k is an algebraically closed field and $f, g \in k[x,y]$ are relatively prime, then the following map is an isomorphism:

$$k[x,y]/(f,g) \xrightarrow{\sim} \prod_{P \in C_f \cap C_g} \mathcal{O}_P/(f,g)\mathcal{O}_P.$$

Proof. To show surjectivity, note that we showed in the proof of existence in Theorem 1.9.9 that if $f, g \in k[x,y]$ are relatively prime and if $P = (p,q) \in C_f \cap C_g$, then there is an $N \geq 1$ such that $(x-p)^N, (y-q)^N \in (f,g)\mathcal{O}_P$. Since, by Theorem 1.6.6, the intersection $C_f \cap C_g$ is finite, there is an $N \geq 1$ that works for all $P \in C_f \cap C_g$. In other words, there is an $N \geq 1$ such that if we enumerate $C_f \cap C_g = \{P_i\}$ with $P_i = (p_i, q_i)$, then $(x-p_i)^N, (y-q_i)^N \in (f,g)\mathcal{O}_{P_i}$ for all i. Now, to show injectivity, it suffices to show that for each i, there is a polynomial $f_i \in k[x,y]$ such that f_i maps to 0 in $\mathcal{O}_{P_j}/(f,g)\mathcal{O}_{P_j}$ for all $j \neq i$, but to a unit in $\mathcal{O}_{P_i}/(f,g)\mathcal{O}_{P_i}$; for this, simply take

$$f_i := \prod_{j : p_j \neq p_i} (x - p_j)^N \prod_{j : q_j \neq q_i} (y - q_j)^N,$$

which maps to zero in each $\mathcal{O}_{P_j}/(f,g)\mathcal{O}_{P_j}$ for $j \neq i$ because of our choice of N, while it is a unit already in $\mathcal{O}_{P_i}$ and hence also in $\mathcal{O}_{P_i}/(f,g)\mathcal{O}_{P_i}$.[36]

To show injectivity, we have to show that if $h \in k[x,y]$ is such that $h \in (f,g)\mathcal{O}_P$ for all $P \in C_f \cap C_g$, then $h \in (f,g)k[x,y]$. For that, given an h, consider the ideal

$$I := \{q \in k[x,y] : qh \in (f,g)\} \subset k[x,y].$$

Then $I \supset (f,g)k[x,y]$, and we want to show that $1 \in I$, i.e. that $I = k[x,y]$.[37] If I is not a proper ideal, then by Proposition 1.7.6, there is a prime ideal $Q \subset k[x,y]$ containing I.[38] Since Q cannot be 0 or of the form (r) for some irreducible $r \in k[x,y]$ (because $f, g \in Q$ are nonzero and relatively prime), by Exercise 2.3.3, we must have $Q = (x-p, y-q)$ for some $p, q \in k$ (this uses that k is algebraically closed). Now $f, g \in Q = (x-p, y-q)$ implies that if $P = (p,q)$, then $P \in C_f \cap C_g$. Since, by hypothesis, we have $h \in (f,g)\mathcal{O}_P$, we conclude that there are $a, b, c \in k[x,y]$ such that $ch = af + bg$ with $c|_P \neq 0$. But this implies that $c \in I \setminus Q$, which is a contradiction, finishing the proof. ∎

Lemma 1.14.3. If k is a field and $f, g \in k[x,y]$ have degree $m, n \geq 1$ such that f and g are relatively prime and the leading terms f_m and g_n are relatively prime, then

$$\dim_k k[x,y]/(f,g) = mn.$$

Proof. For each integer $d \geq 0$, let $k[x,y]_{\leq d}$ denote the k-vector subspace of $k[x,y]$ consisting of polynomials of degree at most d, which has dimension $\binom{d+2}{2}$ over k. The proof idea is to approximate $\dim_k k[x,y]/(f,g)$ by the images of the projections of $k[x,y]_d$ for $d \gg 1$. To do this, for any $d \geq m+n$, consider the sequence of k-vector spaces and k-linear maps given by

$$0 \to k[x,y]_{\leq d-m-n} \xrightarrow{\alpha} k[x,y]_{\leq d-m} \times k[x,y]_{\leq d-n} \xrightarrow{\beta} k[x,y]_{\leq d} \xrightarrow{\pi_d} k[x,y]/(f,g), \tag{1.2}$$

[36] The surjectivity result does not actually need k to be algebraically closed.

[37] The ideal I is often called the ideal quotient of (f,g) by (h) and is denoted $(f,g) : (h)$.

[38] In our case, we did not quite need a fact this general, since we already have $f, g \in I$ and so we may conclude from this that there are polynomials in x only and y only in I, but Proposition 1.7.6 (which is a good fact to know in general) simplifies things tremendously.

where

$$\begin{aligned}\alpha : c \quad &\mapsto (cg, -cf),\\ \beta : (a,b) &\mapsto af + bg,\end{aligned}$$

and π_d is the restriction of the natural projection map $\pi : k[x,y] \to k[x,y]/(f,g)$ to the subspace $k[x,y]_{\leq d}] \subset k[x,y]$. In the sequence (1.2), the compositions of each pair of successive maps are all zero, i.e. $\beta \circ \alpha = 0$ and $\pi_d \circ \beta = 0$. The key claim is that, under our hypotheses, this sequence (1.2) is exact, i.e. α is injective, and we have $\operatorname{im}\alpha = \ker\beta$ and $\operatorname{im}\beta = \ker\pi_d$. Assuming this, we conclude from repeated applications of the Rank-Nullity Theorem that

$$\begin{aligned}\dim_k \operatorname{im}\pi_d &= \binom{d+2}{2} - \dim_k \ker\pi_d\\ &= \binom{d+2}{2} - \dim_k \operatorname{im}\beta\\ &= \binom{d+2}{2} - \binom{d-m+2}{2} - \binom{d-n+2}{2} + \dim_k \ker\beta\\ &= \binom{d+2}{2} - \binom{d-m+2}{2} - \binom{d-n+2}{2} + \dim_k \operatorname{im}\alpha\\ &= \binom{d+2}{2} - \binom{d-m+2}{2} - \binom{d-n+2}{2} + \binom{d-m-n+2}{2}\\ &= mn,\end{aligned}$$

where the last step is a trivial simplification. In particular, for all $d \geq m+n$, the dimension of $\operatorname{im}\pi_d$ is independent of d. Since the $\operatorname{im}\pi_d \subset k[x,y]/(f,g)$ for $d \geq 0$ form an increasing sequence of subspaces with union $\operatorname{im}\pi = k[x,y]/(f,g)$, it follows from this constancy of dimensions that

$$\operatorname{im}\pi_{m+n} = \operatorname{im}\pi_{m+n+1} = \operatorname{im}\pi_{m+n+2} = \cdots = \operatorname{im}\pi = k[x,y]/(f,g),$$

and hence

$$\dim k[x,y]/(f,g) = \dim \operatorname{im}\pi_{m+n} = mn.$$

It remains to show that under our hypothesis, the sequence (1.2) is exact, which we do now.

(a) The map α is visibly injective, since $k[x,y]$ is a domain and $f, g \neq 0$.

(b) Clearly, $\operatorname{im}\alpha \subset \ker\beta$. Conversely, if $(f,g) \in \ker\beta$, then $af + bg = 0$. Since f and g are relatively prime, it follows from this that $g \mid a$ and $f \mid b$, and in fact that there is a $c \in k[x,y]$ such that $a = cg$ and $b = -cf$. If $\deg a \leq d - m$ and $\deg b \leq d - n$, then we must also have $\deg c \leq d - m - n$. This proves that $\ker\beta \subset \operatorname{im}\alpha$.

(c) Again, clearly $\operatorname{im}\beta \subset \ker\pi_d$. Conversely, if $h \in \ker\pi_d$, then $h \in (f,g)$. Write $h = af + bg$ for some $a, b \in k[x,y]$ and suppose that this representation is chosen so that $\deg a$ is minimal (here we take $\deg 0 = 0$). We will show that $\deg a \leq d - m$ and $\deg b \leq d - n$, from which it follows that $h \in \operatorname{im}\beta$, finishing the proof. Suppose to the contrary that $p := \deg a > d - m$ or that $q := \deg b > d - n$, so that either af or bg contains a term of degree greater than d. Since $\deg h \leq d$ and $h = af + bg$, it follows that the leading terms of af and bg must cancel, i.e. $p + m = q + n$ and if we write $a = a_0 + \cdots + a_p$ and $b = b_0 + \cdots + b_q$, where each a_i, b_i is homogeneous of degree i with $a_p b_q \neq 0$, then

$$a_p f_m + b_q g_n = 0.$$

Now, since the terms f_m and g_n are relatively prime, it follows as before that there is some nonzero $c \in k[x,y]$ of degree $p - n = q - m$ such that $a_p = gc_n$ and $b_q = -cf_m$. Then

$$h = (a - cg)f + (b + cf)g$$

is another representation of h with $\deg(a - cg) < \deg a$, contrary to our choice of a.

■

1.14.2 Proof 2: Resultants

Sketch of Proof 2 of Theorem 1.14.1. Consider the finite set S consisting of all lines that join two or more points of $C \cap D$ and all tangent lines to C and D at all the points of intersection $C \cap D$. Pick a point $P_0 \in \mathbb{P}^2_k$ that is not on $C \cup D$ and not on any line in S. Pick a coordinate system so that $P_0 = [1 : 0 : 0]$. It follows from this choice that each "horizontal" line $Z_0 Y - Y_0 Z = 0$ meets at most one point of $C \cap D$, i.e. all the points of intersection have distinct y-coordinates. The idea of the proof is to project the intersection points $C \cap D$ onto the y-axis, and use this to count then number intersection points (with multiplicity).

For this, let $\deg C = m$ (resp. $\deg D = n$), and let F (resp. G) be a minimal polynomial for C (resp. D). Write

$$F = F_0 X^m + \cdots + F_m \text{ and } G = G_0 X^n + \cdots + G_n,$$

where each F_i (resp. G_i) is a polynomial only of Y and Z and homogeneous of degree i. The assumption that $P_0 \notin C \cup D$ implies that $F_0 G_0 \neq 0$. Since F, G are relatively prime in $k[X, Y, Z]$, by Lemma 1.6.2(b) there are $A, B \in k[X, Y, Z]$ and $0 \neq R \in k[Y, Z]$ such that $AF + BG = R$. In fact, we can choose R to be the resultant

$$R = \operatorname{Res}_X(F, G) \in k[Y, Z]_{mn}$$

with A and B homogeneous as well.[39] Then a point $[Y_0 : Z_0]$ is a root of R iff the polynomials $F(X, Y_0, Z_0)$ and $G(X, Y_0, Z_0)$ have common root X_0 over k (Exercise 2.2.4(d)), which happens iff the horizontal line $Z_0 Y - Y_0 Z = 0$ intersects the curve. In other words, the roots of R correspond exactly to the projection of the intersection of F and G to the y-axis, since we chose our coordinate system so that no two points of intersection lie on the same horizontal line.

Since R has exactly mn roots counted with multiplicity, to complete the proof, it suffices to show that for each root $[Y_0 : Z_0]$ of R, the intersection multiplicity of C and D at the unique point of intersection on the line $Z_0 Y - Y_0 Z = 0$ is exactly the multiplicity of $[Y_0 : Z_0]$ as a root of R. There are many ways to do this. One way to show this is to prove that this definition satisfies (with respect to any choice of P_0) satisfies the axioms (1)-(7), and use the uniqueness result from Theorem 1.9.9; this is, for instance, the approach followed in [6, Theorem 3.18]. Another way to do this is to note that the problem is local at P, so by an affine translation (so preserving P_0), we may assume that $P = (0, 0)$ is the point of intersection on line $y = 0$. Since resultants are stable under dehomogenization, we conclude that if f and g are the dehomogenizations of F and G, then we have to show that $i_P(f, g)$ is the multiplicity $m_0(r)$ of $r = \operatorname{Res}_x(f, g)$ at 0, which is the highest power of y dividing r. Let this highest power be N. The claim then follows from the observation in the local ring $\mathcal{O}_P$, we have $(f, g)\mathcal{O}_P = (x + yq, y^N)\mathcal{O}_P$ for some $q \in k[x, y]$. The result follows from this from because then

$$i_P(f, g) = \dim_k \mathcal{O}_P/(f, g)\mathcal{O}_P = i_P(x + yq, y^N) = N \cdot i_P(x + yq, y) = N \cdot i_p(x, y) = N.$$

To show that $(f, g)\mathcal{O}_P = (x + yq, y^N)\mathcal{O}_P$, note first that $r \in (f, g)k[x, y]$ can be written as $y^N r_0$ for some $r_0 \in k[y]$ with $r_0(0) \neq 0$, whence $y^N \in (f, g)\mathcal{O}_P$. Also, we can write $f = x f_1 + y f_2$ and $g = x g_1 + y g_2$ for some polynomials $f_1, g_1 \in k[x]$ and $f_2, g_2 \in k[x, y]$. Then the assumption that P is the only intersection point of C and D on $y = 0$ implies that f_1 and g_1 are coprime, whence from Bézout's *Lemma* it follows that there are $a, b \in k[x]$ such that $a f_1 + b g_1 = 1$. It follows then that $af + bg = x + yq$ for $q = a f_2 + b g_2$, and hence $x + yq \in (f, g)\mathcal{O}_P$. This shows $(x + yq, y^N)\mathcal{O}_P \subset (f, g)\mathcal{O}_P$. The other inclusion is similar, but needs more work of reconstructing the polynomials f and g from the resultant and powers of x. ■

[39] We haven't quite shown this, but it is not very hard to do with the tools that we have developed. A fuller discussion of the theory of resultants would include this result. The resultant R is homogeneous of degree mn precisely because $F_0 G_0 \neq 0$.