CHAPTER 15

Some applications of Bézout

We have already put Bézout's theorem to use in proving the genus formula (and in several interesting exercises at the end of Chapters 12 and 14). Now we shall use it to prove a general result on curves through configurations of points, which in particular will yield a short (and rigorous) proof of Pascal's theorem from Chapter 1. We shall also deduce some results on cubics will will come in handy for studying the group law on elliptic curves.

Throughout this Chapter we shall use the following dictionary:

algebraic curve $\subset \mathbb{P}^2$	degree	defining equation (homogeneous polynomial)
C	d	$F \in S_3^d$
D	d	$G \in S_3^d$
E	e	$H \in S_3^e$

Recall the theorem we are wanting to apply:

Bézout. $C \cap E$ *is* 0*-dimensional (consists of points)* $\implies$ $(C \cdot E) = de$.

Part of the content of the (equivalent) contrapositive statement is:

tuozèB. *The number of points* $|C \cap E|$ *exceeds* $de \implies$ *E and C have a common component.*

From Chapter 9, we have:

Study. E irreducible and $E \subset C \implies H$ divides F.

Putting tuozè**B** and **S**tudy together gives:

BS. *E irreducible and $|C \cap E| > de \implies H \mid F$.*

We'll make use of this statement below.

15.1. Cayley-Bacharach theorem

Let $p_1, \dots, p_n \in \mathbb{P}^2$ be distinct points, and define

$$S^d(p_1, \dots, p_n) := \left\{ \begin{array}{c} \text{homogeneous polynomials (of degree } d\text{)} \\ \text{in } [Z : X : Y] \text{ vanishing at } p_1, \dots, p_n \end{array} \right\}.$$

15.1.1. LEMMA. *Suppose E is irreducible and $p_1, \dots, p_a \in E$ for some $a > ed$, while $p_{a+1}, \dots, p_n \notin E$. Then*

$$S^d(p_1, \dots, p_n) = H \cdot S^{d-e}(p_{a+1}, \dots, p_n).$$

PROOF. The inclusion of the RHS into the LHS is easy, since it is just saying that the product of a polynomial vanishing at the last $n - a$ points by a polynomial vanishing at the first a points, vanishes at all of them. So we turn to the reverse inclusion.

Assuming $S^d(p_1, \dots, p_n)$ is nonzero, take a nonzero element F; this defines a degree d curve C containing $p_1, \dots, p_n$. Clearly we have $p_1, \dots, p_a \in C \cap E$, so $|C \cap E| > ed$, and by "BS", $H \mid F$. We can therefore write $F = F_0 \cdot H$ with $F_0 \in S^{d-e}$. Since $F = 0$ but $H \neq 0$ at $p_{a+1}, \dots, p_n$, F_0 must vanish at these points. It follows that $F_0 \in S^{d-e}(p_{a+1}, \dots, p_n)$ as desired. $\square$

15.1.2. THEOREM. *Let E be irreducible, $|C \cap D| = d^2$ with $d > e$, and assume exactly*[1] *ed of the points of $C \cap D$ lie on E. Then the remaining $d(d-e)$ points lie on a (not necessarily irreducible!) curve of degree $\leq d - e$.*

PROOF. Let $[A{:}B{:}C] \in E \backslash \{(C \cap D) \cap E\}$, and set $\lambda = F(A, B, C)$, $\mu = -G(A, B, C)$. Define $P := \lambda G + \mu F \in S^d$; this vanishes on $C \cap D$ *and* at $[A{:}B{:}C]$. Label $(C \cap D) \cap E =: \{p_1, \dots, p_{ed}\}$, $[A{:}B{:}C] =: p_{ed+1}$,

[1] It is enough to check, in applying this, that ed of the points (not "exactly ed of the points") lie on E. This is because by Bézout, more than ed of these points simply *can't* lie on E: we would then have $E \subset C$ and $E \subset D$ hence $|C \cap D| = \infty$.

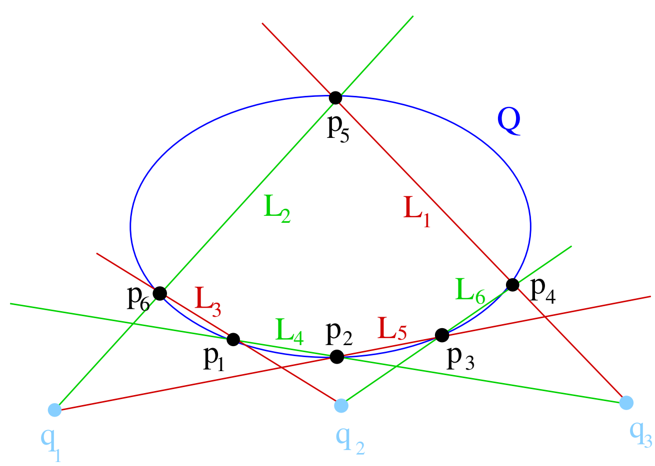
and $(C \cap D) \backslash \{(C \cap D) \cap E\} = \{p_{ed+2}, \ldots, p_{d^2+1}\}$; set $a := ed + 1$ and $n = d^2 + 1$.

Since $a > ed$, Lemma 15.1.1 tells us that $S^d(p_1, \ldots, p_{d^2+1}) = H \cdot S^{d-e}(p_{ed+2}, \ldots, p_{d^2+1})$. But then, since $P \in S^d(p_1, \ldots, p_{d^2+1})$, we have $P = HP_0$ for some $P_0 \in S^{d-e}(p_{ed+2}, \ldots, p_{d^2+1})$. This P_0 defines the required curve. □

Here is the nice application to Pascal:

15.1.3. COROLLARY. *The (three) intercepts of opposite sides of a hexagon inscribed in a conic are collinear.*

PROOF. Referring to the picture



we put $C := L_1 \cup L_3 \cup L_5$, $D = L_2 \cup L_4 \cup L_6$, and $E = Q$. Clearly this means $d = 3$ and $e = 2$, and we do indeed see that $de = 6$ points of $C \cap D = \{p_1, \ldots, p_6\} \cup \{q_1, q_2, q_3\}$ lie on E. So the last three points of $C \cap D$, which are the intercepts, lie on a curve of degree $d - e = 1$ by the Theorem. □

15.1.4. REMARK. If one wanted instead to plug the technical gap in the proof of Pascal suggested in Chapter 1, part of what one needs is the statement: if $p_1, \ldots, p_8 \in \mathbb{P}^2$ are distinct and in "general position" in the sense that no 4 are collinear and no 7 conconic (lying on an irreducible conic), then $\dim S^3(p_1, \ldots, p_8) = 2$. This is proved in Reid's book.

15.2. Intersections of cubics

The results of §15.1 dealt with the case where all intersections of curves have multiplicity one (the "transversal" case), since we required $|C \cap D| = d^2 = (C \cdot D)$. To deal with the general case, at least assuming E is smooth and irreducible (so that we may view it as a Riemann surface), write

$$C \cdot E := \sum_{p \in E \cap C} (E \cdot C)_p [p] \ \in \ \mathrm{Div}(E).$$

If E is irreducible but singular, with a single node or cusp[2] $\hat{p}$, the same definition gives a divisor $C \cdot E \in \mathrm{Div}(\tilde{E})$ (on the normalization) provided $\hat{p} \notin E \cap C$.

15.2.1. THEOREM. *Let C, D, E be distinct cubics, with E irreducible. (If E is singular, assume moreover that $\hat{p} \notin E \cap C$, $E \cap D$.) Writing by Bézout*

$$D \cdot E \ = \ \sum_{i=1}^{9} [q_i] \ \in \ \mathrm{Div}(\tilde{E})$$

where the q_i need not be distinct, and assuming

$$C \cdot E \ = \ \sum_{i=1}^{8} [q_i] \ + \ [q] \ \in \mathrm{Div}(\tilde{E}),$$

we have $q = q_9$.

In the intersection multiplicity one case, the Theorem gives immediately:

15.2.2. COROLLARY. *Let C, D, E be distinct cubics, E irreducible. If $D \cap E = \{q_1, \ldots, q_9\}$ (distinct points) and C passes through $q_1, \ldots, q_8$, then it passes through q_9.*

Actually this is true without assuming E irreducible (provided E doesn't share any components with D or C), but we won't prove that.

[2]See the paragraph immediately preceding §16.1 below.

PROOF OF THEOREM 15.2.1. First assume E is smooth. Recall that the quotient of two homogeneous polynomials — say, F/G — yields a meromorphic function on $\mathbb{P}^2$. By Example 7.3.6, since E intersects $D = \{G = 0\}$ only in points, we may pull this back to E:

$$f := \left.\frac{F}{G}\right|_E \in \mathcal{K}(E)^*.$$

Suppose (for a contradiction) that $q \neq q_9$. Since $C = \{F = 0\}$ and $D = \{G = 0\}$, the divisor of f is evidently

$$(f) = C \cdot E - D \cdot E = [q] - [q_9] \in \mathrm{Div}(E).$$

This says that f has one zero (at q) and one pole (at q_9); hence, as a holomorphic map of Riemann surfaces $E \to \mathbb{P}^1$, f has mapping degree 1. That is, f is 1-to-1; and since (using the open mapping theorem) its image must be open and closed (and $\mathbb{P}^1$ is connected), f is surjective. So f gives an isomorphism $E \cong \mathbb{P}^1$. On the other hand, being a smooth cubic, E has genus 1 (by the genus formula), whereas the genus of $\mathbb{P}^1$ is zero — so they can't be isomorphic for purely topological reasons! This contradication tells us that, indeed, our assumption $q \neq q_9$ was wrong, and so they are equal.

To extend this argument to the case where E is singular with ODP $\hat{p}$, first pull back $\frac{F}{G}$ along the normalization $\sigma : \tilde{E} \to \mathbb{P}^2$ (of E) to obtain $f \in \mathcal{K}(\tilde{E})$. We regard f as a map from $\tilde{E} \to \mathbb{P}^1$. As before, assuming $q \neq q_9$ leads to $\deg(f) = 1$. However, a different objection to "$\deg(f) = 1$" will be required as there is no topological obstruction: indeed, $\tilde{E} \cong \mathbb{P}^1$ by the genus formula (a nodal cubic has genus zero normalization). So argue as follows: since $\hat{p} \notin C, D$, we find that $\frac{F}{G} \in \mathcal{K}(\mathbb{P}^2)$ is well-defined at $\hat{p}$, so its pullback via σ cannot "separate" the two branches of E there. That is, at the two points of $\tilde{E}$ mapping to $\hat{p}$ (under σ), f will take the same value. But then, the mapping degree of f cannot be 1.

The other possibility is that $\hat{p}$ is a cusp. We may assume that $\hat{p} = [1 : 0 : 0]$ and the equation of E is of the form $x^3 = y^2$ (parametrized by $t \mapsto (t^2, t^3)$). Again we need to show that $f = \sigma^* \frac{F}{G}$, if nonconstant, cannot have mapping degree 1. Let $\tilde{p} = \sigma^{-1}(\hat{p})$, and write $R(x,y) := \frac{F(1,x,y)}{G(1,x,y)} - \frac{F(1,0,0)}{G(1,0,0)}$. Then $f(t) - f(0) = (\sigma^* R)(t) = R(t^2, t^3)$, and

$$\begin{aligned} \deg(f) &= \deg f^{-1}([f(0)]) \\ &\geq \mathrm{ord}_0(R(t^2, t^3)) \\ &\geq \mathrm{ord}_{(0,0)}(R(x,y)) \cdot \min\{\mathrm{ord}_0(t^2), \mathrm{ord}_0(t^3)\} \\ &\geq 1 \cdot 2 = 2. \end{aligned}$$ $\square$

The first three exercises use ideas from this chapter; the remaining ones make further use of divisors and intersection numbers.

Exercises

(1) Let C, D, and E be as above (defined by $F = 0$, $G = 0$, $H = 0$), of respective degrees d, d, e with $3 \leq e \leq d$. Suppose C and D intersect in d^2 distinct points, and assume that E is smooth (hence irreducible). Show that if E passes through $ed - 1$ of these, it passes through ed of them. (Imitate the argument from the proof of Theorem 15.2.1.)

(2) (*Converse of Pascal*) Suppose that $C := L_1 \cup L_3 \cup L_5$ and $D := L_2 \cup L_4 \cup L_6$ are lines extending the edges of a hexagon, with $|C \cap D| = 9$. Assume the three intersection points which are not vertices of the hexagon (i.e. the intercepts of opposite edges) are collinear. (a) Prove that the vertices are conconic. [The conic may be smooth or degenerate.] (b) Explain how this leads to a *construction* of the conic through 5 points, in the spirit of Prop. 1.2.1.

(3) (*Möbius's generalization of Pascal*) Show that if any $2n$ intercepts of opposite sides of a $(4n+2)$-gon inscribed in a conic are collinear, then all $2n+1$ of the intercepts are collinear.[3] (Notice that for $n = 1$, this is indeed equivalent to Pascal.) [Hint: try $n = 2$

[3] You should make the following "genericity" assumption: if C is the union, going around the polygon, of the odd-numbered lines, and D the union of the even-numbered lines, then they should intersect in $(2n+1)^2$ distinct points.

first, or maybe just do that case; it's already a bit tricky. Start by applying Theorem 15.1.2 with C and D both configurations of 5 lines, and E the conic. This produces a cubic K containing the 15 points $(C \cap D) \setminus (C \cap D \cap E)$. Argue that the line L containing at least 4 of these points is a component of K, and consider the union of E and the *other* component of K. Assume L does *not* contain a fifth point and arrive at a contradiction.]

(4) Show that all (complex analytic) automorphisms of $\mathbb{P}^2$ are projectivities (hence algebraic), i.e. that $\mathrm{Aut}(\mathbb{P}^2) \cong \mathrm{PGL}(3, \mathbb{C})$. [Hint: given an automorphism α, it sends an algebraic curve *a priori* to an analytic one; but we know this is algebraic by Exercise (6) of Chapter 10. By considering intersection numbers for a pair of curves, show that lines are sent to lines. Compose α with an appropriate projectivity to get the identity, using what you know about automorphisms of $\mathbb{P}^1$.]

(5) (*Weil reciprocity*) Given a Riemann surface M and meromorphic functions $f, g \in \mathcal{K}(M)^*$ with disjoint divisors $(f), (g)$ (i.e. the zeroes/poles of f don't intersect those of g), prove that

$$f((g)) = g((f)).$$

(For a divisor $D = \sum m_i[p_i]$, $f(D)$ means $\prod f(p_i)^{m_i}$.) [Hint: consider g as a morphism $M \to \mathbb{P}^1$, and write z for the coordinate on $\mathbb{P}^1$, so that $(g) = g^*(z)$ in the notation of Remark 14.1.3. Write $\mathcal{N} \colon \mathcal{K}^*(M) \to \mathcal{K}^*(\mathbb{P}^1)$ for the *Norm map* sending a function to the product of its values over each point of $\mathbb{P}^1$. Show that $f((g)) = \mathcal{N}f((z))$ and $g((f)) = z((\mathcal{N}f))$, thereby reducing the proof to the case $M = \mathbb{P}^1$; then finish it off.]