Lecture 18: Some consequences of Bézout's theorem

1 Elementary consequences

We start with some very elementary consequences of Bézout's theorem:

Corollary 47.

1. *A plane curve has finitely many singular points.*
2. *A nonsingular plane curve is irreducible.*
3. *The intersection multiplicity $m_p(C, D) = 1$ if and only if p is a nonsingular point of both C and D, and the tangent lines T_pC and T_pD are distinct.*

Proof.

1. Given $C = \mathbb{V}(f)$ of degree d, we know that $\operatorname{sing}(C) \subseteq \mathbb{V}(f) \cap \mathbb{V}(\frac{\partial f}{\partial x})$. By Bézout's theorem, this is a set of $\leq d(d-1)$ points.
2. Suppose C has a decomposition $C = C_1 \cup C_2$ with $\deg C_1, \deg C_2 \geq 1$. Then by Bézout's theorem there is at least one point $p \in C_1 \cap C_2 \subset C$, and C must be singular at p.
3. Omitted. See Kirwan's textbook *Complex algebraic curves.* □

2 The Cayley–Bacharach theorem

Definition 48. The *linear system* $L_d(p_1, \ldots, p_m) \subset \mathbb{C}[x, y, z]$ is the $\mathbb{C}$-vector space of homogeneous polynomials of degree d that vanish at $p_1, \ldots, p_m \in \mathbb{P}^2$.

If $f \in L_d(p_1, \ldots, p_m)$ then each point p_i imposes at most one extra condition on the coefficients of f, so

$$\dim L_d(p_1, \ldots, p_m) \geq \binom{d+2}{2} - m$$

where $\binom{d+2}{2}$ is the dimension of the space of all homogeneous polynomials of degree d in $\mathbb{C}[x, y, z]$. The dimension may be larger than expected if the points don't impose independent conditions—for example $\dim L_1(p, q, r) = 0$ if p, q, r are non-collinear, but if p, q, r lie on a line $L = \mathbb{V}(f)$ then $\dim L_1(p, q, r) = 1$ (where $L_1(p, q, r)$ is spanned by f).

Theorem 49. *Suppose we have eight points $p_1, \ldots, p_8 \in \mathbb{P}^2$, no four of which are collinear and no seven of which lie on any conic. Then*

$$\dim L_3(p_1, \ldots, p_8) = 2$$

(i.e. the eight points all impose independent conditions on $f \in L_3(p_1, \ldots, p_8)$).

Proof. We have $\dim L_3(p_1, \ldots, p_8) \geq \binom{5}{2} - 8 = 2$, so we only have to prove that the dimension cannot be bigger. Suppose that $\dim L_3(p_1, \ldots, p_8) \geq 3$. We will find a contradiction.

Case 1. *Suppose no three points lie on a line and no six points lie on a conic.* Let p_9, p_{10} be two more points on the line $L = \overline{p_1 p_2}$. Then

$$\dim L_3(p_1, \ldots, p_8, p_9, p_{10}) \geq \dim L_3(p_1, \ldots, p_8) - 2 \geq 1$$

and therefore there is a (possibly degenerate) cubic curve X passing through $p_1, \ldots, p_{10}$. Since $\#X \cap L \geq 4$, by Bézout's theorem we must have $L \subset X$, so that $X = C \cup L$ where C is a conic. But now the six points $p_3, \ldots, p_8 \in X \setminus L$ must live on the conic C—a contradiction!

Case 2. *Suppose that p_1, p_2, p_3 lie on a line L.* Let p_9 be a fourth point on L. By a similar argument to before, any cubic curve through $p_1, \ldots, p_9$ breaks up as $C \cup L$ for some conic curve C passing through $p_4, \ldots, p_8$. Since

$$L_3(p_1, \ldots, p_8, p_9) \geq \dim L_3(p_1, \ldots, p_8) - 1 \geq 2,$$

there are two distinct conics C_1, C_2 through the five points $p_4, \ldots, p_8$. But now $\#C_1 \cap C_2 \geq 5$ and $C_1 \neq C_2$, so Bézout's theorem implies that C_1 and C_2 share a common line L'. Therefore $C_1 = L_1 \cup L'$ and $C_2 = L_2 \cup L'$. Since no four of the points lie on L', at least two of the points (p_7 and p_8 say) must lie on L_1, and also on L_2. But now $\#L_1 \cap L_2 \geq 2$ and $L_1 \neq L_2$—another contradiction!

Case 3. *Suppose that $p_1, \ldots, p_6$ lie on a conic C.* Choose a seventh point $p_9 \in C$. Then any cubic X that passes through $p_1, \ldots, p_8, p_9$ has $\#X \cap C \geq 7$, so by Bézout's theorem $X = C \cup L$ for some line L which must pass through p_7 and p_8. Since

$$L_3(p_1, \ldots, p_8, p_9) \geq \dim L_3(p_1, \ldots, p_8) - 1 \geq 2,$$

there are at two such cubics $X_1 = C \cup L_1$ and $X_2 = C \cup L_2$. But then $\#L_1 \cap L_2 \geq 2$ and $L_1 \neq L_2$—contradiction! □

Corollary 50 (Cayley–Bacharach theorem)**.** *Let C_1, C_2 be two cubic curves that intersect at nine distinct points $p_1, \ldots, p_9$. Any cubic curve C that passes through the first eight $p_1, \ldots, p_8$ must also pass through the ninth point p_9.*

Proof. If four of the points lie on a line L then C_1 and C_2 must both contain L and cannot intersect in nine distinct points. If seven of the points lie on a conic C then C_1 and C_2 must both contain C and cannot intersect in nine distinct points. Now the eight points $p_1, \ldots, p_8$ satisfy the conditions of Theorem 49 and hence

$$\dim L_3(p_1, \ldots, p_8) = 2.$$

This means that the equations f_1, f_2 defining C_1, C_2 form a basis for $L_3(p_1, \ldots, p_8)$, and therefore the equation for C is of the form $f = \lambda f_1 + \mu f_2$ for some $\lambda, \mu \in \mathbb{C}$. Since $f(p_9) = \lambda f_1(p_9) + \mu f_2(p_9) = 0$ we have that $p_9 \in C$. □

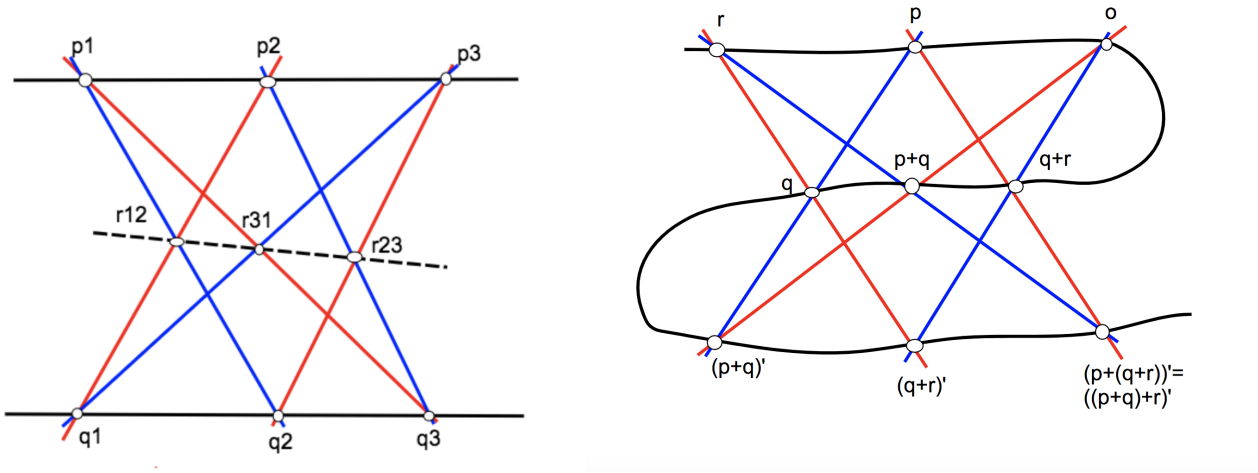
3 Pappus' theorem

Pappus' theorem is a classical theorem in plane Euclidean geometry.

Theorem 51. *Suppose that $\{p_1, p_2, p_3\}$ is one set of three collinear points and $\{q_1, q_2, q_3\}$ is another. Then the points $\{r_{12}, r_{23}, r_{31}\}$, where $r_{ij} = \overline{p_i q_j} \cap \overline{p_j q_i}$, are also collinear.*

Proof. The degenerate cubic curves $C_1 = \overline{p_1 q_2} \cup \overline{p_2 q_3} \cup \overline{p_3 q_1}$ and $C_2 = \overline{p_1 q_3} \cup \overline{p_2 q_1} \cup \overline{p_3 q_2}$ both pass through all nine points $p_1, p_2, p_3, q_1, q_2, q_3, r_{12}, r_{23}, r_{31}$. Now apply Corollary 50 with the degenerate cubic curve $C = \overline{p_1 p_2} \cup \overline{q_1 q_2} \cup \overline{r_{12} r_{23}}$. □

Proof by picture. Picture proof of Pappus' Theorem 51 (on the left) and the associativity of the group law on an elliptic curve (on the right, cf. Theorem 53). In each case the cubic C_1 is drawn in red, C_2 is drawn in blue and C (or E) is drawn in black.



4 The group law on an elliptic curve

Definition 52. An *elliptic curve* is an irreducible nonsingular plane cubic curve $E \subset \mathbb{P}^2$ with a chosen point $o \in E$.

Given an elliptic curve E, we can define an *additive group law* on the points of E with the following properties:

1. For any $p \in E$, the line $\overline{op}$ intersects E at three points o, p, q (counted with multiplicity). Define $p' := q$, and note that $p'' = p$ for all $p \in E$.

2. For any $p, q \in E$, the line $\overline{pq}$ intersects E at three points p, q, r (again, counted with multiplicity). We define $(p+q)' := r$, and hence $p + q = (p+q)'' = r'$ as above.

Theorem 53. *This construction defines an Abelian group law on E with identity element O.*

Proof. First, to show addition is well-defined we need to show that the line $L = \overline{pq}$ is well-defined. This is clearly true if $p \neq q$. If $p = q$ then we let L be the tangent line T_pE, which is well-defined since E is nonsingular and $\dim E = 1$.

Showing that o is the identity and $p + q = q + p$ are easy. To find the inverse of p we let o' be the third intersection point of $T_oE \cap E$. Then $\overline{po'}$ intersects E at three points p, o', q and, by the addition rule applied to $\overline{pq}$, we have $p + q = o'' = o$. Therefore q is the inverse of p.

The hardest part of the theorem is to prove associativity, i.e. that $(p+q)+r = p+(q+r)$. We consider the reducible cubic

$$C_1 = \overline{pq} \cup \overline{o, q+r} \cup \overline{p+q, r}$$

which meets E at the nine points

$$p,\ q,\ (p+q)' \quad o,\ q+r,\ (q+r)', \quad p+q,\ r,\ ((p+q)+r)'$$

and similarly the reducible cubic

$$C_2 = \overline{qr} \cup \overline{o, p+q} \cup \overline{p, q+r}$$

which meets E at the nine points

$$q,\ r,\ (q+r)' \quad o,\ p+q,\ (p+q)', \quad p,\ q+r,\ (p+(q+r))'.$$

Since C_1, C_2 and E have the eight points $o, p, q, r, p+q, q+r, (p+q)', (q+r)'$ in common, the last intersection point is also equal by Corollary 50. Therefore $p+(q+r) = (p+q)+r$. $\square$