Introduction to Algebraic Geometry

Bézout's Theorem and Inflection points

1. The resultant.

Let K be a field. Then the polynomial ring $K[x]$ is a unique factorisation domain (UFD). Another example of a UFD is the ring of integers $\mathbb{Z}$. There is a strong analogy between primes and irreducible polynomials. In general, given an integral domain A, one has the concepts of *prime* and *irreducible*: let $p \in A$, $p \neq 0$, p not a unit, then p is *irreducible* if $p = ab$ implies a or b is a unit, and p is *prime* if $p|ab$ implies $p|a$ or $p|b$. Every prime element is irreducible, but the converse is false in general.

Example. Let $A = \mathbb{C}[x,y,z]/(z^2 - xy)$. The class of z is irreducible, but not prime, as $z|xy$ but neither $z|x$ nor $z|y$. The ring A is an integral domain, but not a UFD: the element z^2 has two different factorisations: $z^2 = z \cdot z$ and $z^2 = x \cdot y$.

In a UFD every irreducible element is prime. If A is a UFD, also $A[x]$ is a UFD, and by induction we obtain $K[x_1, \dots, x_n]$ is a UFD (K a field), see exercises.

Let A be a unique factorisation domain. We are interested in the question when two polynomials $f(x)$, $g(x) \in A[x]$ have a common factor. Cases of interest are $A = K$, but also $A = K[y,z]$ (cf. Ex. 1). Let:

$$\begin{aligned} f =& a_0x^m + a_1x^{m-1} + \dots + a_m, \\ g =& b_0x^n + b_1x^{n-1} + \dots + b_n, \end{aligned}$$

where the case that either $a_0 = 0$ or $b_0 = 0$ is allowed.

Proposition 1. *The polynomials f and g have a non-constant factor h in common, if and only there exist polynomials u and v of degree less than m, resp. n, not both vanishing, such that $vf + ug = 0$.*

Proof. We may suppose that $a_0 \neq 0$. All irreducible factors of f have to occur in ug, and not all can occur in u, because $\deg u < \deg f$; therefore f and g have a factor in common. Conversely, given h one finds a v and w, such that $f = wh$ and $g = vh$, so the equation $vf + ug = 0$ is satisfied with $(u,v) = (-w, v)$. $\square$

Now put:

$$\begin{aligned} u =& u_0x^{m-1} + \dots + u_{m-1}, \\ v =& v_0x^{n-1} + \dots + v_{n-1}, \end{aligned}$$

and consider the coefficients as indeterminates. Comparison of coefficients of powers of x in $vf + ug = 0$ gives the system of linear equations:

$$\begin{aligned} a_0v_0 + b_0u_0 \qquad\qquad &= 0 \\ a_1v_0 + a_0v_1 + b_1u_0 + b_0u_1 &= 0 \\ &\vdots \\ a_mv_{n-1} + b_nu_{m-1} &= 0\,. \end{aligned}$$

This system has a solution if and only if its determinant vanishes. After transposing we get the following determinant, which is called the *Resultant* of f and g:

$$R_{f,g} = \begin{vmatrix} a_0 & a_1 & a_2 & \dots & a_m & & & & \\ & a_0 & a_1 & a_2 & \dots & a_m & & & \\ & & \dots & \dots & \dots & \dots & \dots & & \\ & & & a_0 & a_1 & a_2 & \dots & a_m & \\ b_0 & b_1 & \dots & b_{n-1} & b_n & & & & \\ & b_0 & b_1 & \dots & b_{n-1} & b_n & & & \\ & & \dots & \dots & \dots & \dots & \dots & & \\ & & & b_0 & b_1 & \dots & b_{n-1} & b_n & \end{vmatrix}.$$

We have shown:

Proposition 2. *The polynomials f and g have a non-constant factor h in common, if and only $R_{f,g} = 0 \in A$.*

Now suppose that $R_{f,g} \neq 0$. Leaving out the last equation $a_m v_{n-1} + b_n u_{m-1} = 0$ describes the condition that $vf + ug$ does not involve x. The maximal minors of the matrix yield a solution (v, u) such that $vf + ug = R_{f,g}$ (Cramer's rule!). So for any two polynomials f and g there exist u and v with $\deg u < \deg f$ and $\deg v < \deg g$, such that:

$$vf + ug = R_{f,g}.$$

Remark. If A is a polynomial ring, and a_i and b_i are homogeneous polynomials of degree i, then $R_{f,g} \in A$ is a polynomial of degree mn.

2. Bézout's Theorem.

Theorem 3. *Let k be an infinite field. Let $F(X, Y, Z)$ and $G(X, Y, Z)$ be homogeneous polynomials in $k[X, Y, Z]$ of degree m and n, without common factor. Then the number of common zeroes of F and G in $\mathbb{P}^2_k$, counted with multiplicities, is at most mn, and equal to mn, if k is algebraically closed.*

We will use the resultant to define intersection multiplicities in such a way, that the theorem becomes trivial. To this end we consider F and G as polynomials in X, with coefficients in $k[Y, Z]$. By Prop. 1 the resultant $R_{F,G}$ is not identically zero, because F and G have no factor in common. Therefore $R_{F,G}$ is a homogeneous polynomial of degree mn in Y and Z, which vanishes only for a finite number of values $(Y : Z)$. Eliminating X from the equations $F = G = 0$ amounts geometrically to projecting onto the line $X = 0$ (which has homogeneous coordinates (Y, Z)) from the point $(1 : 0 : 0)$. The common zeroes of F and G therefore lie on a finite number of lines through $(1 : 0 : 0)$. It is possible that such a line contains several zeroes, but the total number is finite.

Choose a point P, not on $F = 0$, not on $G = 0$, and outside all lines connecting two common zeroes of F and G; this is possible, because k is infinite. Take new coordinates, in which P is the point $(1 : 0 : 0)$.

Definition. Let $Q = (\xi : \eta : \zeta)$ be a common zero of F and G; by construction it is the only one on the line $\zeta Y - \eta Z = 0$. The *intersection multiplicity* of F and G in the point Q is the multiplicity of $(\eta : \zeta)$ as zero of the resultant $R_{F,G}(Y, Z)$.

Remark. As announced Bézout's theorem now trivially holds. The only remaining problem is that our definition of intersection multiplicity a priori depends on the choice of the point P. Independence can be shown in a number of different ways. The most abstract approach to the definition uses the axiomatic method: one gives a set of postulates for intersection multiplicity and shows that there is at most one intersection theory satisfying them, see [Fulton]. To show existence one has to give somehow an explicit definition (as opposed to implicit by the axioms), and the one with the resultant is an example. One can also argue by continuity, see [Brieskorn-Knörrer]: a 1-parameter family of admissable points P_t gives a family of homogeneous polynomials of degree mn with constant number of zeroes, counted without multiplicity. By the continuous dependence of the roots of a polynomials in $\mathbb{C}[x]$ on the coefficients their multiplicities have to be constant also. As stated this argument uses the topology of $\mathbb{C}$. To make it into a purely algebraic proof one needs the Zariski topology, cf. the remark in [Reid, (2.10)]. Here I want to give a different motivation, using another, analytic definition of the intersection multiplicity of a smooth analytic curve with a plane curve, and show that it coincides with the definition above. This again works only for $k = \mathbb{R}$ or $k = \mathbb{C}$; I restrict myself to the complex case.

Definition. Let $D \subset \mathbb{C}$ be a domain containing 0. Let $\varphi\colon D \to \mathbb{C}^2$ be an analytic map, with $\varphi(0) = 0$, and $\varphi'(0) \neq 0$. Let $f\colon \mathbb{C}^2 \to \mathbb{C}$ be a non constant analytic function with $f(0) = 0$. The intersection multiplicity of the curve $\varphi(t)$ with the curve $f(x, y) = 0$ at the origin is the order in t of the analytic function $f \circ \varphi(t)$.

This definition generalises the definition of intersection multiplicities in the case of the intersection of a line in $\mathbb{P}^2_{\mathbb{C}}$ with an algebraic curve. Note that it is not symmetric in f and φ. I show now that both definitions the intersection multiplicity coincide (if they both apply).

Lemma 4. *If the curve $G = 0$ is smooth in a common zero Q of F and G, and the point P does not lie on the tangent line of $G = 0$ in the point Q, then both definitions give the same result.*

Proof. Use affine coordinates, and suppose the intersection point is the origin. Write $f(x, y) = F(X, Y, 1)$, etc. We assume as before that $P = (1 : 0 : 0)$ so we project parallel to the x-axis. The condition on g is that its gradient does not vanish at the origin. The x-axis is not allowed to be the tangent, so $\frac{\partial g}{\partial x}(0, 0) \neq 0$. By the implicit function theorem we can find a parametrisation $x = \varphi(y)$, such that $g(\varphi(y), y) \equiv 0$. From the equation $vf + ug = R$ we get:

$$v(\varphi(y), y) f(\varphi(y), y) = R(y).$$

I claim that $v(0, 0) \neq 0$. Then the order of the zero $y = 0$ of R equals that of the zero $y = 0$ of $f(\varphi(y), y)$. Because $g(0, 0) = 0$, we can write $g(x, 0) = xg_1(x)$, and we have $b_n(0) = 0$ (remember that $g(x, y) = \sum b_i(y)x^{n-i}$). Note that $v(0, 0) = v_{n-1}(0)$ is a certain minor, which is itself a resultant, namely that of $g_1(x)$ and $f(x, 0)$. As the root $x = 0$ of $g(x, 0)$ is a simple root (because $\frac{\partial g}{\partial x}(0, 0) \neq 0$), which is the only common root of $g(x, 0)$ and $f(x, 0)$ by our assumption on the choice of P, this resultant does not vanish. □

3. The Hessian.

Let $F_d(X_0, X_1, X_2)$ be the equation of a plane curve C, and $P = (p_0 : p_1 : p_2)$ a point on it. The *tangent line* at P is given by the equation:

$$\frac{\partial F}{\partial X_0}(P)X_0 + \frac{\partial F}{\partial X_1}(P)X_1 + \frac{\partial F}{\partial X_2}(P)X_2 = 0, \qquad (*)$$

provided this linear form is not identically zero; if $\left(\frac{\partial F}{\partial X_0}(P), \frac{\partial F}{\partial X_1}(P), \frac{\partial F}{\partial X_2}(P)\right) = 0$, then P is a *singular point*, and the tangent line is not defined.
There are several ways to understand the formula $(*)$.

- We can view F as equation on k^3, and describe the tangent plane in any point on the line, which projects onto $P \in (k^3 \setminus \{0\})/k^*$. As this plane passes through the origin, it is given by $(*)$.
- In affine coordinates (x_1, x_2), write $f(x_1, x_2) = F(1, X_1, X_2)$; the tangent line is $\frac{\partial f}{\partial x_1}(P)(x_1 - p_1) + \frac{\partial f}{\partial x_2}(P)(x_2 - p_2) = 0$. By Euler's formula:

$$\sum X_i \frac{\partial F}{\partial X_i} = dF,$$

  and the fact that $F(p_0, p_1, p_2) = 0$, we obtain in homogeneous coordinates the expression $(*)$.
- Finally, the tangent line is the line which intersects F in P with multiplicity at least two. Let $Q = (Q_0, Q_1, Q_2)$, and consider the line $P + tQ$. By Taylor's formula:

$$F(P + tQ) = F(P) + t \sum \frac{\partial F}{\partial X_i}(P) \cdot Q_i + \text{h.o.t.}$$

The condition that $t = 0$ is at least a double root, gives that Q satisfies $(*)$.
Observe that differentiation of a polynomial can be defined purely algebraically (product rule!), and involves no analysis. To avoid funny behaviour in characteristic p we assume from now on that our field k has characteristic 0.

Definition. A tangent line L, tangent to $C\colon F = 0$ in the point P, is an *inflexional tangent*, or flex for short, and P is an *inflexion point*, if the intersection multiplicity of L and C at P is at least 3.

Definition. The *Hessian* H_F of F is the curve, defined by the equation:

$$\det\left(\frac{\partial^2 F}{\partial X_i \partial X_j}\right) = 0.$$

Remarks.

1. The Hessian transforms under a projective transformation $X' = AX$ as a quadratic form (Exercise 7.3.i).
2. The Hessian curve passes through the singular points of F: by Euler's formula $(d-1)\frac{\partial F}{\partial X_j} = \sum X_i \frac{\partial^2 F}{\partial X_i \partial X_j}$, so the columns of the matrix are dependent.

Theorem 5. *Let $F_d(X_0, X_1, X_2)$ define a curve C of degree d without lines as components in $\mathbb{P}^2_k$, with k a field of characteristic zero. A nonsingular point $P \in C$ is an inflexion point with intersection multiplicity of the flex and the curve $r+2$ if and only if the Hessian H_F intersects F in P with multiplicity r.*

Proof. Choose coordinates such that $P = (0:0:1)$ and the tangent line in P is the line $X = 0$. Now we can write the equation of the curve in the form $F = XU(X,Y,Z) + Y^{r+2}G(Y,Z)$ with $U(0,0,1) \neq 0$ and $G(0,1) \neq 0$. For the Hessian we do the same thing, collecting all terms containing X in a first summand. The result is $H_F = XV(X,Y,Z) + Y^r H(Y,Z)$, where the second summand is computed by putting $X = 0$ in the determinant, defining H_F:

$$Y^r H(Y,Z) = \begin{vmatrix} 2U_X & U_Y & U_Z \\ U_Y & (r+2)(r+1)Y^r G + 2(r+2)Y^{r+1}G_Y + Y^{r+2}G_{YY} & (r+2)Y^{r+1}G_Z + Y^{r+2}G_{YZ} \\ U_Z & (r+2)Y^{r+1}G_Z + Y^{r+2}G_{YZ} & Y^{r+2}G_{ZZ} \end{vmatrix}.$$

As $(\deg U)U = XU_X + YU_Y + ZU_Z$, one has $U(0,0,1) \neq 0$ if and only if $U_Z(0,0,1) \neq 0$, and therefore $H(0,1) = -U_Z^2(0,0,1)G(0,1) \neq 0$ (here we use $\operatorname{char} k = 0$). This shows that $P \in H_F$ if and only if $r > 0$.

To compute the intersection multiplicity of F and H_F, we compute the resultant to be of the form $Y^{r+2}GQ_1 + Y^r HQ_2$ with $Q_2(0,1)$ itself the resultant of $U(X,0,Z)$ and $XV(X,0,Z)$. By choosing suitable coordinates we can ensure that P is the only intersection point of F and H_F on $Y = 0$. □

Corollary 6. *A nonsingular cubic curve over an algebraically closed field k with $\operatorname{char} k = 0$ has exactly nine distinct inflexion points.*

Exercises.

1 ($\sim$ 3.3). i) Prove Gauß' Lemma: if A is a UFD and $f, g \in A[x]$ are polynomials with coefficients in A, then a prime element of A that is a common factor of the coefficients of the product fg is a common factor of the coefficients of f or g.
ii) Let A be a UFD. Prove that $A[x]$ is a UFD. For this you need to compare factorisations in $A[x]$ with factorisations in $Q[x]$, where Q is the field of fractions of A, using Gauß' lemma to clear denominators.
iii) If K is a field then $K[x]$ is a UFD. Prove by induction on n that $K[x_1, \ldots, x_n]$ is a UFD.

2. Let $f(x,y)$ be the affine equation of a real or complex plane curve, and $P = (p,q)$ a point on it; suppose that $\frac{\partial f}{\partial y}(P) \neq 0$, so by the implicit function theorem $y = \varphi(x)$ in a neighbourhood of P. Prove that P is an inflexion point (in the sense that $\varphi''(p) = 0$) if and only if:

$$\begin{vmatrix} f_{xx} & f_{xy} & f_x \\ f_{xy} & f_{yy} & f_y \\ f_x & f_y & 0 \end{vmatrix} = 0.$$

(Hint: differentiate $f(x,\varphi(x)) \equiv 0$ twice. Compute also the determinant) Use Euler's formula and $f(p,q) = 0$ to translate this condition into the condition on the vanishing of the Hessian of the associated homogeneous function $F(X,Y,Z)$.

3 (= 2.10). Let $C \subset \mathbb{P}^2_k$, $\operatorname{char} k \neq 2$, be a plane cubic with inflexion point P. Prove that a change of coordinates can be used to bring C in the normal form $Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$. Hint: take coordinates such that $P = (0:1:0)$, and its tangent is $Z = 0$; get rid of the linear term in Y by completing the square.

4. A real plane cubic with one inflexion point has two other inflexion points. Hint: use the result of the previous exercise in affine coordinates, express y as function of x and show that $y''(x)$ has to have a zero.

5. Find the inflexion points of the singular cubics $ZY^2 = X^2(X+Z)$ and $Y^2Z = X^3$, both in $\mathbb{P}^2_{\mathbb{R}}$ and in $\mathbb{P}^2_{\mathbb{C}}$.

6. Let P and Q be inflexion points on a cubic curve C. Show that the third intersection point of the line $\overline{PQ}$ with C is also an inflexion point. Hint: use coordinates in which $P = (0:1:0)$, $Q = (0:0:1)$ and the flexes are $Y = 0$ and $Z = 0$.

7. Consider the cubic curve C in $\mathbb{P}^2_{\mathbb{C}}$ with equation:

$$X^3 + Y^3 + Z^3 - 3\lambda XYZ = 0,$$

where $\lambda^3 \neq 1$. Find its inflexion points. Compute the inflexion lines. What are all lines joining inflexion points? Determine the singular elements of the pencil of cubics $\mu(X^3 + Y^3 + Z^3) - 3\lambda XYZ$.