KTH Teknikvetenskap

Institutionen för matematik, KTH.

Contents

Chapter 4

Curves in the projective plane

We will in this chapter study different aspects of *plane curves* by which we mean curves in the projective plane defined by polynomial equations. Here we will start with the more classical setting and consider a plane curve as the set of solutions of one *homogenous* equation in three variables.

We will start by choosing a field, k, which in most cases can be thought of as either $\mathbb{R}$ or $\mathbb{C}$, but sometimes, it is interesting also to look at $\mathbb{Q}$ or finite fields.

The first definition we might try is the following.

Definition 4.0.1. *A* plane curve *C is the set of solutions in $\mathbb{P}^2_k$ of a non-zero homogeneous equation*

$$f(x, y, z) = 0.$$

Example 4.0.2. The equation $x^2 + y^2 + z^2 = 0$ defines a degree two curve over $\mathbb{C}$ but over $\mathbb{R}$ it gives the empty set.

The equation $x^2 = 0$ has a solution set consising of the line $(0 : s : t)$ while the degree of the equation is two.

The example above shows us that there are curves that the definition does not give us any one-one correspondance between curves and equations.

4.1 Lines

We will start by the easiest curves in the plane, namely *lines*. These are defined by linear equations

$$ax + by + cz = 0 \tag{4.1}$$

where $(a, b, c) \neq (0, 0, 0)$. Observe that any non-zero scalar multiple of (a, b, c) has the same set of solutions, which show us that we can *parametrize* all the lines in $\mathbb{P}^2_k$ by another projective plane with coordinates $[a : b : c]$.

Theorem 4.1.1. *Any two distinct lines in $\mathbb{P}^2$ intersect at a single point.*

Proof. The condition that the lines are distinct is the same thing as the equations defining them being linearly independent, which gives a unique solution to the system of equations. □

Theorem 4.1.2. *Any line in $\mathbb{P}^2$ is isomorphic to $\mathbb{P}^1$.*

Proof. By a change of coordinates the equation of a line can be written as $x = 0$ and the solutions are given by $[0 : s : t]$ where $(s, t) \neq (0, 0)$, which as a set equals $\mathbb{P}^1$.

In fact, using this parametrization, we can define a map $\mathbb{P}^1 \longrightarrow \mathbb{P}^2$, which has the given line as the image.

We will come back to what we mean by *isomorphism* later on in order to make this more precise. □

4.1.3 The dual projective plane $(\mathbb{P}^2)^*$

As mentioned above, the coefficients a, b, c of Equation 4.1, give us natural coordinates on the space of lines in $\mathbb{P}^2$ and we will call this the *dual projective plane*, denoted by $(\mathbb{P}^2)^*$.

Theorem 4.1.4. *The set of lines through a given point in $\mathbb{P}^2$ is parametrized by a line in $(\mathbb{P}^2)^*$.*

Proof. Equation 4.1 is symmetric in the two sets of variables, $\{x, y, z\}$ and $\{a, b, c\}$. Thus, fixing $[x : y : z]$ gives a line in $(\mathbb{P}^2)^*$. □

4.1.5 Automorphisms of $\mathbb{P}^2$

A linear change of coordinates on $\mathbb{P}^2_k$ is given by a non-singular 3×3-matrix with entries in k:

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix}.$$

Because of the identification $[x : y : z] = [\lambda x : \lambda y : \lambda z]$, the scalar matrices correspond to the identity. The resulting group of automorphisms is called $\mathrm{PGL}(3, k)$.

4.2 Conic sections

We will now focus on quadratic plane curves, or *conics*. These are defined by a homogeneous quadratic equation

$$ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0.$$

4.2.1 Conics as the intersection of a plane and a cone

The name *conic* is short for *conic section* and comes from the fact that each such curve can be realized as the intersection of a plane and a circular cone

$$x^2 + y^2 = z^2$$

in $\mathbb{P}^3$.

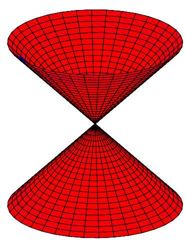

Figure 4.1: The circular cone

4.2.2 Parametrization of irreducible conics

The conic section is *irreducible* if the polynomial defining it is not a product of two non-trivial polynomials.

Theorem 4.2.3. *If C is a plane irreducible conic with at least two rational points, then C is isomorphic to $\mathbb{P}^1_k$.*

Proof. Let P be a rational point of C and let L denote the line in $(\mathbb{P}^2)^*$ parametrizing lines through P. In the coordinates of each line, the polynomial equation reduces to a homogeneous quadratic polynomial in two variables with at least one rational root. Without loss of generality, we may assume that P is $[0:0:1]$ and the equation of C has the form

$$ax^2 + bxy + cy^2 + dxz + eyz = 0.$$

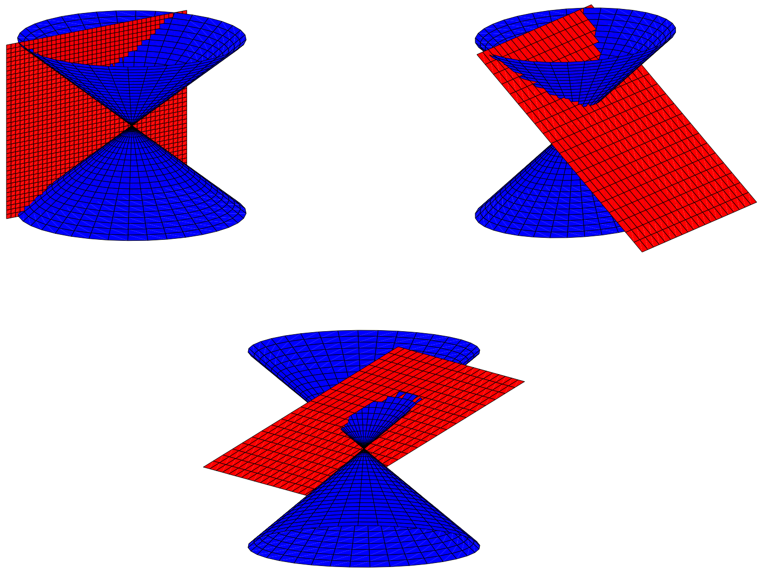

Figure 4.2: The hyperbola, parabola and ellips as a plane sections of a cone

The lines through P are parametrized by a $\mathbb{P}^1$ with coordinates $[s : t]$ and we ge the residual intersection between the curve and the line $sx + ty = 0$ as

$$R = [est - dt^2 : dst - es^2 : cs^2 - bst + at^2].$$

Since C has another rational point, Q, we cannot have $d = e = 0$ since C is irreducible. Hence the residual point R is not equal to P except for one $[s, t]$. Moreover, by the next exercise, we get that the three coordinates are never zero at the same time. Hence we have a non-trivial map from $\mathbb{P}^1$ to $\mathbb{P}^2$ whose image is in C. If the image was a line, C would be reducible and we conclude that C is the image of the map. □

Excercise 4.2.4. Let C be a conic passing throught the point $[0 : 0 : 1]$, i.e., having equation of the form

$$ax^2 + bxy + cy^2 + dxz + eyz = 0.$$

Show that C has is reducible if and only if $cd^2 - bde + ae^2 = 0$ under the assumption that C has at least two rational points.

Example 4.2.5. The example $x^2 + y^2 = 0$ with k a field with no square root of -1 shows that we cannot drop the condition that C has at least two rational points.

4.2.6 The parameter space of conics

Exactly as for the lines, we have that the equation

$$ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0$$

defines the same curve when multiplied with a non-zero constant. Hence all the conics can be parametrized by a $\mathbb{P}^5$ with coordinates $[a : b : c : d : e : f]$.

In this *parameter space* we can look at loci where the conics have various properties. For example, we can look at the locus of degenerate conics that are double lines. These are parametrized by a $\mathbb{P}^2$ and the locus of such curves is the image of the *Veronese* embedding of $\mathbb{P}^2$ in $\mathbb{P}^5$ defined by

$$[s : t : u] \mapsto [s^2 : 2st : t^2 : 2su : 2tu : u^2].$$

If we want to look at all the curves that are degenerate as a union of two lines, we look at the image of a map

$$\Phi\colon \mathbb{P}^2 \times \mathbb{P}^2 \longrightarrow \mathbb{P}^5$$

given by

$$([s_1 : t_1 : u_1], [s_2 : t_2 : u_2]) \mapsto (s_1s_2 : s_1t_2+t_1s_2 : t_1t_2 : s_1u_2+u_1s_2 : t_1u_2+u_1t_2 : u_1u_2].$$

The image of Φ is a *hypersurface* in $\mathbb{P}^5$ which means that is is defined by one single equation in the coordinates $[a : b : c : d : e : f]$.

Excercise 4.2.7. Find the equation of the hypersurface definied by the image of the map $\Phi\colon \mathbb{P}^2 \times \mathbb{P}^2 \longrightarrow \mathbb{P}^5$ defined above.

4.2.8 Classification of conics

When we want to classify the possible conics up to projective equivalence, we need to see how the group of linear automorphisms acts. One way to go back to our knowledge of quadratic forms. If 2 is invertible in k, i.e., if k does not have characteristic 2, we may write the equation

$$ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0$$

as $Q(x, y, z) = 0$, where Q is the *quadratic form* associated to the matrix

$$A = \frac{1}{2}\begin{bmatrix} 2a & b & d \\ b & 2c & e \\ d & e & 2f \end{bmatrix}.$$

Now, a matrix P from $\mathrm{PGL}(3, k)$ acts on A by

$$Q \mapsto P^T AP.$$

Theorem 4.2.9. *Up to projective equivalence, the equation of a conic can be written in one of the three forms*

$$x^2 = 0, \quad x^2 + \lambda y^2 = 0 \quad \textit{and} \quad x^2 + \lambda y^2 + \mu z^2 = 0.$$

Proof. The first thing that we observe is invariant is the rank of the matrix. If the rank is one, we can choose two of the columns of P to be in the kernel of A and hence after a change coordinates, the equation is $\lambda x^2 = 0$, but this is equivalent to $x^2 = 0$.

If the rank is two, we choose one of the columns to be a generator of the kernel and we get that we can assume that $d = e = f = 0$. By completing the square, we can change it into $\kappa x^2 + \mu y^2$, which is equivalent to $x^2 + \lambda y^2$, where $\lambda = \mu/\kappa$.

If the rank is three, proceed by completing the squares in order to write the form as $x^2 + \lambda y^2 + \mu z^2$. □

Remark 4.2.10. In order to further characterize the conics, we need to know about the multiplicative group of our field. In particular, we need to know the quotient of k^* by the subgroup of squares.

Theorem 4.2.11. *Let $k = \mathbb{C}$. Then there are only three conics up to projective equivalence:*

$$x^2 = 0, \quad x^2 + y^2 = 0 \quad \textit{and} \quad x^2 + y^2 + z^2 = 0.$$

Proof. Since every complex number is a square, we can change coordinates so that $\lambda = \mu = 1$ in Theorem 4.2.9. □

Theorem 4.2.12. *Let $k = \mathbb{R}$. Then there are four conics up to projective equivalence:*

$$x^2 = 0, \quad x^2 + y^2 = 0 \quad x^2 - y^2 = 0, \quad x^2 + y^2 - z^2 = 0.$$

Proof. Here, only the positive real numbers are squares and we have to distinguish between the various signs of λ and μ. If $\lambda = \mu = 1$ we get the empty curve, so there is only one non-degenerate curve $x^2 + y^2 = z^2$. □

4.2.13 The real case vs the complex case

4.2.14 Pascal's Theorem

We will look at a classical theorem by Pascal about conics.

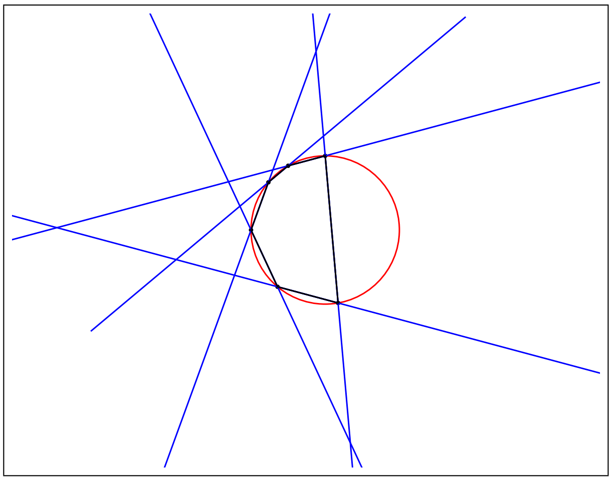

Figure 4.3: Pacsal's Theorem

Theorem 4.2.15 (Pascal's Theorem)**.** *Let C be a plane conic and H be a hexagon with its vertices on C. The three pairs of opposite sides of the hexagon meet in three collinear points.*

There are several ways to understand this theorem and we will now look at one way.

Proof. Start by dividing the lines into two groups of three lines so that no two lines in the same group intersect on the conic C.

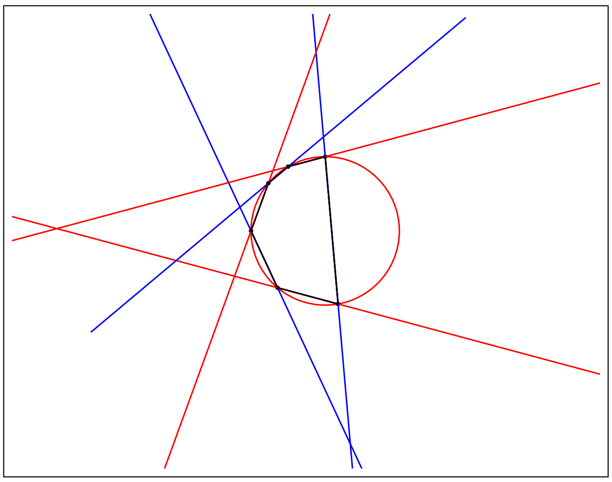

Figure 4.4: The two groups of lines

Each group of three lines defines a cubic plane curve, given by the product of the three linear equations defining the lines. Since each line in one group meets each of the lines from the other group, we have nine points of intersections of lines from the two groups. Six of these are on the conic and it remains for us to prove that the remaining three are collinear.

Choose two of the points and take the line L through them. Together with the conic, the line defines a cubic curve, i.e., there is a cubic polynomial vanishing on the line and the conic. In particular, this cubic curve passes through eight of our nine points. We already have two cubic curves passing through all nine points. If the last cubic didn't pass through all nine points, we would have three linearly independent cubic polynomials passing through our eight points.

Denote the three cubic polynomials by f_1, f_2 and f_3. They can generate seven or eight linearly independent polynomials of degree four. If they generate eight, we get that it will generate a space of codimension 7 in all higher degree, by multiplication by a linear form not passing through any of the points. If they generate only seven linearly independent forms of degree four, we must have two linearly independent syzygies, i.e., relations of the form

$$\begin{cases} \ell_1 f_1 & + & \ell_2 f_2 & + & \ell_3 f_3 & = & 0, \\ \ell_4 f_1 & + & \ell_5 f_2 & + & \ell_6 f_3 & = & 0. \end{cases}$$

Since there is a unique solution to this system up to multiplication by a polynomial, we get that

$$(f_1, f_2, f_3) = \ell(\ell_2\ell_6 - \ell_3\ell_5, \ell_3\ell_4 - \ell_1\ell_6, \ell_1\ell_5 - \ell_2\ell_4)$$

showing that the three cubics share a common linear factor. However, this cannot be the case, since the two original cubics did not have a common factor.

We conclude that the cubic passing throug eight of the nine point also pass throug the ninth, which shows that the three that were not on the conic have to be collinear. □

The property that any cubic passing through eight of the nine points also has to pass through the ninth point is known as the Cayley-Bacharach property and similar consequences occur in much more general situations.

Chapter 5

Cubic curves

When we move to cubic curves, we have ten coefficients of the equation

$$a_0x^3+a_1x^2y+a_2x^2z+a_3xy^2+a_4xyz+a_5xz^2+a_6y^3+a_7y^2z+a_8yz^2+a_9z^3=0.$$

Thus, as in the case of lines and conics, we can use a projective space to parametrize all cubics and in this case we get $\mathbb{P}^9$. As the group of automorphisms of $\mathbb{P}^2$ has dimension 8, we expect that there should be at least a one-dimensional family of non-isomorphic cubics.

As in the case of conics, we have a number of degenerate cases where the cubic is reducible. We get several different ways the cubic polynomial could factor. If we have linear factors, they could all be equal, two distinct or three distinct. In the case when there are three distinct factors, they can share a common zero or not. This can be summarized as

$$x^3=0, \qquad x^2y=0 \qquad , xy(x+y)=0 \qquad \text{or} \qquad xyz=0.$$

When the cubic polynomial has a linear and an irreducible quadratic factor, we get different cases depending on whether the line is tangent to the conic or not which gives the two possibilities

$$x(x^2+y^2-z^2) \qquad \text{and} \qquad (x-z)(x^2+y^2-z^2).$$

5.1 Normal forms for irreducible cubics

Definition 5.1.1. *L is a tangent line to C at P if the restriction of the equation of C to L has a root of multiplicity at least two at P.*

Definition 5.1.2. *A point P on a curve C is* non-singular *if there is a unique tangent line of C at P.*

Definition 5.1.3. *A non-singular point P of a curve C is a* flex *point of C if the tangent of C at P intersect C with multiplicity at least three at P.*

Theorem 5.1.4. *The equation of an irreducible cubic with at flex point can be written as*

$$y^2z = x^3 + ax^2z + bxz^2 + cz^3$$

after a change of coordinates.

Proof. Let C be the curve defined by the equation

$$a_0x^3+a_1x^{2y}+a_2x^2z+a_3xy^2+a_4xyz+a_5xz^2+a_6y^3+a_7y^2z+a_8yz^2+a_9z^3 = 0.$$

Assume that $[0 : 1 : 0]$ is a flex point with tangent line $z = 0$. Then, when restricting the equation to the line, we need to get $x^3 = 0$, forcing $a_1 = a_3 = a_6 = 0$.
If $a_7 = 0$ we get that the restriction of the equation of C to the line $x = 0$ is $a_8yz^2 + a_9z^3 = 0$. Thus $x = 0$ is a second tangent line to C at P. Since P is a flex point, it is non-singular and we deduce that $a_7 \neq 0$.
We can now change change variables with $y = y' + \alpha x + \beta z$ so that there will be no other terms involving y' than $(y')^2$. Thus we get to the desired normal form.
The irreducibility gives that $a_0 \neq 0$ since otherwize $z = 0$ would be a component. Thus we can get the leading term on the right hand side to be x^3. □

Excercise 5.1.5. Find the normal form for the Fermat cubic $x^3 + y^3 = z^3$.

5.2 Elliptic curves

Definition 5.2.1. *A non-singular cubic curve is called en* elliptic curve.

Theorem 5.2.2. *The cubic curve defined by the equation*

$$y^2z = f(x, z)$$

is non-singular if and only if $f(x, z)$ has no multiple factors.

Proof. Without loss of generality, we can assume that the point is $P = [0 : y_0 : 1]$. The lines though P are $sx + t(y - y_0z) = 0$, for $[s : t]$ in $\mathbb{P}^1$. When $t = 0$ we get the line $x = 0$ which is tangent to C if and only if $c = y_0 = 0$.

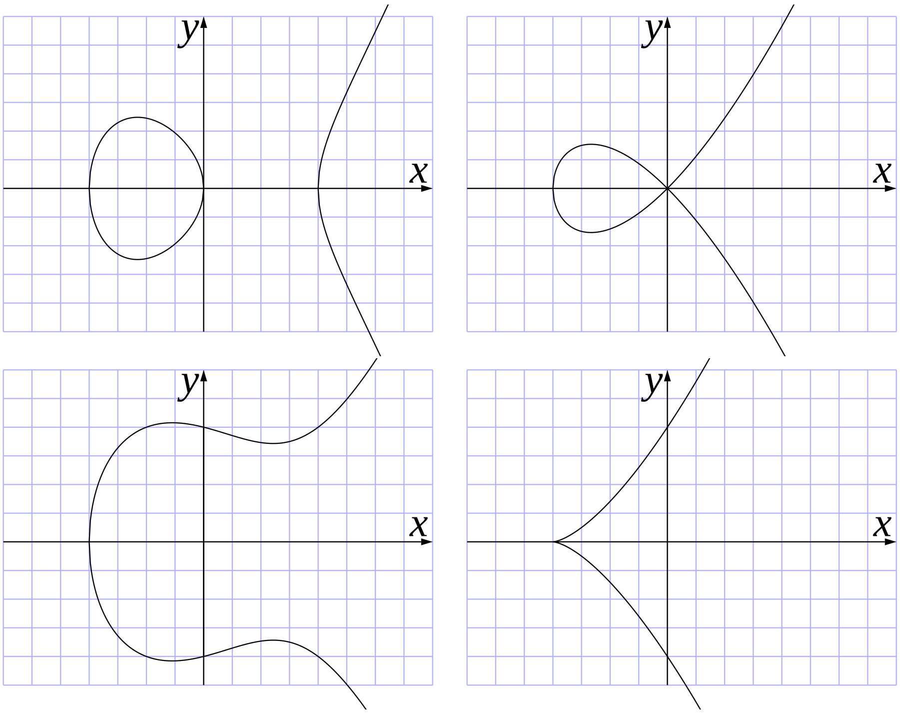

Figure 5.1: Different kinds of cubics in normal form

For $t \neq 0$ we substitute in $y^2z = x^3 + ax^2z + bxz^2 + z^3$ to get

$$x(t^2x^2 + (at^2 - s^2)xz + (bt + 2sy_0)tz^2) = 0$$

which has a double root at P if and only if $(bt + 2sy_0)t = 0$. Thus we get a unique tangent line, unless $c = y_0 = b = 0$, where we get $x = 0$ and $y = y_0$ as tangent lines. □

5.2.3 The group law on an elliptic curve

The elliptic curves are special in many ways. One of them is that there is a commutative group law on the set of rational points of an elliptic curve.

The restriction to any line of the equation of a cubic curve gives a homogeneous cubic equation in two variables. If this equation has two rational solutions, the third has to be rational as well.

Definition 5.2.4. *Choose a flex point O of the elliptic curve C. If P and Q are points on C we define the sum $P + Q$ to be the third point on the line throug O and the third point on the line through P and Q. Observe that if $P = Q$, we take the tangent line at P.*

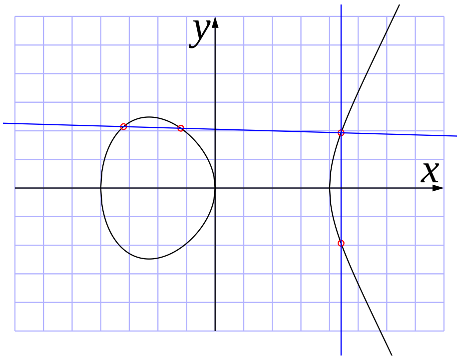

Figure 5.2: The addition on an elliptic curve

Theorem 5.2.5. *The addition defines a commutative group law on the set of points of C.*

Proof. The commutativity is clear from the defnition. The identity element is given by O since the line through O and P meets the curve in a point Q and then the line through O and Q is the same as the line before, which shows that $O + P = P$. The inverse of P is given as the point Q on the line through O and P.

The associativity is more involved and we will refer to other sources for a proof of that. □

5.2.6 A one-dimensional family of elliptic curves

The normal form $y^2z = x^3 + ax^2z + bxz^2 + cz^3$ does not specify an elliptic curve up to isomorphism. As we have seen before, we have that the right hand side has distinct factors. We can translate one of them to $x = 0$ and scale one of them to $x = z$. This leaves us with the normal form

$$y^2z = x(x - z)(x - zw)$$

where $w \neq 0$ and $w \neq 1$.

5.2.7 Flex points on an elliptic curve

Theorem 5.2.8. *The set of flex points on C form an elementary* 3*-group.*

Proof. The flex points can be shown to be zeroes of the Hessian form (cf. Exercise 5.2.14), which shows that there are at most finitely many flex points.

If P is a flex point, we have that $3P = 0$ since the tangent through P meets C only at P. The sum of two flex points is again a flex point as $3P = 0$ and $3Q = 0$ implies that $3(P+Q) = 0$. Thus the set of flex points on an elliptic curve form a finite subgroup where all non-trivial elements have order 3, i.e, an elementary 3-group. □

Excercise 5.2.9. Show that an elliptic curve over $\mathbb{R}$ cannot have more than three flex points.

5.2.10 Singularities and the discriminant

Among the irreducible cubics, there are two kinds of singular curves; nodal cubics and cuspidal cubics. Both of these singular curves are rational curves and are images of a degree three map $\mathbb{P}^1 \longrightarrow \mathbb{P}^3$. In the normal form they can be written as

$$y^2z = x^3 \quad \text{and} \quad y^2z = x^3 - x^2z$$

We can localize the singularities of C by the Jacobian ideal since they correspond to zeroes of the gradient of the polynomial defining C.

Example 5.2.11. Let C be then nodal cubic defined by $F(x, y, z) = y^2z - x^3 + x^2z$. The gradient is given by

$$\nabla F = (-3x^2 + 2xz, 2yz, y^2 + x^2)$$

which is zero only at $[0 : 0 : 1]$.

Example 5.2.12. Let C be the cuspidal cubic defined by $F(x, y, z) = y^2z - x^3$. Then we get

$$\nabla F = (-3x^2, 2yz, y^2)$$

which again is zero only at $[0 : 0 : 1]$.

Excercise 5.2.13. Define the rational cubic curve C as the image of the map $\Phi\colon \mathbb{P}^1 \longrightarrow \mathbb{P}^2$ given by

$$\Phi([s : t]) = [s^3 : st^2 : t^3], \qquad [s : t] \in \mathbb{P}^1.$$

Find the singular point of C and determine whether C is nodal or cuspidal.

As we have seen, the general cubic curve is non-singular, but there is an eight-dimensional family of singular curves given by the nodal cubics. One way to see that the family of singular cubics is eight dimensional is to look at the curves that are singular at a given point $[x_0 : y_0 : z_0]$. We have a two-dimensional choice of the point and for each point, we have three linear conditions on the coefficients of the cubic giving us a $\mathbb{P}^6$ of curves singular at the given point. We can describe this as a $\mathbb{P}^6$-bundle over $\mathbb{P}^2$.

The locus $X \subseteq \mathbb{P}^9$ parametrizing singular cubics is defined by a single polynomial called the *discriminant*. It is a difficult task to compute this polynomial which is of degree 12.

Excercise 5.2.14. Let C be a cubic plane curve over $\mathbb{C}$. Show that the Hessian, i.e., the determinant of

$$\begin{bmatrix} \frac{\partial^2 F}{\partial x^2} & \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial x \partial z} \\ \frac{\partial^2 F}{\partial y \partial x} & \frac{\partial^2 F}{\partial y^2} & \frac{\partial^2 F}{\partial y \partial z} \\ \frac{\partial^2 F}{\partial z \partial x} & \frac{\partial^2 F}{\partial z \partial y} & \frac{\partial^2 F}{\partial z^2} \end{bmatrix}$$

vanishes exactly at the singular points of C and on the flex points of C.

Chapter 6

Bézout's Theorem

On $\mathbb{P}^1$ we have that any polynomial of degree d has exactly d roots counted with multiplicity, at least when we are working over $\mathbb{C}$ or any algebraically closed field. We will now look at a generalization of this called *Bézouts't Theorem*, which stated that two plane curves of degree d and e with no common component intersect in exactly $d \cdot e$ points counted with multiplicity.

There are a couple of difficulties that we have to overcome in order to prove this. The first is to properly define what *multiplicity* means in the statement of the theorem.

6.0.15 The degree of a projective curve

As we have seen before, when a homogeneous polynomial of degree d defining a plane curce is restricted to a line with coordinates $[s : t]$, we either get zero or a homogeneous polynomial of degree d in s and t. In the first case, the line was a component of C and in the second case, we get a polynomial which factors into a product of d linear factors if our field is algebraically closed. From now on, we will assume that this is the case. Moreover, we will assume that the polynomial defining our curve has the lowest possible degree, so that there are no multiple factors in the factorization into irreducible polynomials. We call such a polynomial *reduced*.

With these conventions, the following definition makes sense.

Definition 6.0.16. *A plane curve C has degree d if a general line in $\mathbb{P}^2$ intersect C in d distinct points.*

6.0.17 Intersection multiplicity

Let C_1 and C_2 be plane curves defined by reduced polynomials f_1 and f_2 with no common factors. In order to define the intersection multiplicity of C_1 and C_2 at their points of intersection, we will first change coordinates in order to move the point common point P to $[0 : 0 : 1]$. When looking locally around this point, we can dehomogenize the polynomials by substituting $z = 1$. Let $F_1 = f_1(x, y, 1)$ and $F_2 = f_2(x, y, 1)$ be the polynomials we obtain in this way. We have $F_1, F_2 \in k[x, y]$, but we can also see them as formal power series in the ring $k[[x, y]]$, which has the advantage that any polynomial which is non-zero at the origin $(0, 0)$ is invertible. In this way, we can concentrate only at what happens at the origin. From F_1 and F_2 we get an ideal $I = (F_1, F_2) \subseteq k[[x, y]]$ and we can define the quotient ring $k[[x, y]]/I$.

Definition 6.0.18. *The intersection multiplicity of C_1 and C_2 at $P = [0 : 0 : 1]$ is given by*

$$I_P(f_1, f_2) = \dim_k k[[x, y]]/(F_1, F_2)$$

We will need a couple of properties of the intersection multiplicity.

Theorem 6.0.19. *If f, g and h are homogeneous polynomials in $k[x, y, z]$ with no common factors, we have*

(1) $I_P(f, gh) = I_P(f, g) + I_P(f, h)$

(2) $I_P(f, g + fh) = I_P(f, g)$ *if* $\deg g = \deg f + \deg h$.

Proof. At the moment, we will refer to other sources for the proof of the first statement, which requires more knowlegde in power series rings.
The second statement follows from the definition since $(f, g) = (f, g + fh)$ as ideals in $k[x, y, z]$ and hence also their images in $k[[x, y]]$ under the map $k[x, y, z] \to k[[x, y]]$ sending z to 1. □

Excercise 6.0.20. Show that if P is a non-singular point of C_1 and C_2 such that the tangents of C_1 and C_2 at P are distinct, then $I_P(f, g) = 1$ where f and g are the homogeneous polynomials defining C_1 and C_2.

6.0.21 Proof of Bézout's Theorem

Theorem 6.0.22 (Bézout's Theorem)**.** *If C_1 and C_2 are plane curves defined by homogeneous polynomials f and fg of degree d and e, they intersect in*

$d \cdot e$ points, counted with multiplicity, i.e.,

$$\sum_P I_P(f, g) = d \cdot e.$$

Proof. If one of the polynomials splits into a product of linear factors, we can use Theorem 6.0.19 (1) to conclude the theorem.

We will use Theorem 6.0.19 (1) to make reductions until we can assume that one of the polynomial splits into a product of linear factors. By Theorem 6.0.19 (1) we can assume that f and g are irreducible.

The basic step will be the following. Write the polynomials as

$$\begin{aligned} f(x, y, z) &= z^{d'} h_0(x, y) + z^{d'-1} h_1(x, y) + \cdots + h_{d'}(x, y) \\ g(x, y, z) &= z^{e'} k_0(x, y) + z^{e'-1} k_1(x, y) + \cdots + k_{e'}(x, y) \end{aligned}$$

With no loss of generality, we may assume that $d' \geq e'$. Then we can define

$$f_1 = k_0 f - h_0 z^{d'-e'} g$$

which will have lower degree in z than f. We have that

$$I_P(f_1, g) = I_P(k_0 f, g) = I_P(k_0, g) + I_P(f, g), \quad \forall P.$$

Since k_0 is a polynomial in two variables, it splits into a product of linear forms. Since g was assumed to be irreducible we know that k_0 is not a factor of g. Since we know the theorem holds for k_0 and g we can deduce it for f and g if we know it holds for f_1 and g. For this we can use induction on the degree of z in the polynomials. □

Excercise 6.0.23. Follow the proof of Bézout's theorem above starting with the curves $zy^2 = x^3 - xz^2$ and $x^2 + y^2 = z^2$. What are all the intersection points and their multiplicities at the end of the reduction?

6.0.24 The homogeneous coordinate ring of a projective plane curve

As we have seen, the polynomial ring $k[x, y, z]$ plays an important role in the study of $\mathbb{P}^2$. This is the *homogeneous coordinate ring* of $\mathbb{P}^2$.

If C is defined by the homogeneous polynomial $f \in k[x, y, z]$, we get the homogeneous coordinate ring of C as $R_C = k[x, y, z]/(f)$.

Theorem 6.0.25. *(1) C is irreducible if and only if R_C is a domain.*

(2) C is reduced if and only of R_C has no nilpotent elements.

The homogeneous coordinate ring of C is graded, i.e., we can write it as

$$R_C = \bigoplus_{i \geq 0} [R_C]_i$$

so that $[R_C]_i [R_C]_j \subseteq [R_C]_{i+j}$.

Definition 6.0.26. *The* Hilbert function *of C is given by $H_C(i) = \dim_k [R_C]_i$, for $i = 0, 1, 2, \ldots$.*

Theorem 6.0.27. *If C has degree d, the Hilbert function of C is given by*

$$H_C(i) = \binom{i+2}{2} - \binom{i+2-d}{2} = \frac{1}{2}(di + 3d - d^2),$$

for $i \geq d - 1$.

Proof. The Hilbert function of C is given by the vector space dimension of $k[x, y, z]/(f)$ in degree i. We have the following short exact sequence

$$0 \to k[x, y, z] \to k[x, y, z] \to R_C \to 0$$

where the first map is multiplication by f. Thus the dimension of R_C in degree i is the difference between the dimension of $k[x, y, z]$ in degree i and degree $i - d$. If $i \geq d - 1$, these dimensions are given by the formula in the statement of the theorem. □

Lemma 6.0.28. *The homogenous polynomial g defines an injective map $R_C \longrightarrow R_C$ if and only if g doesn't vanish completely on any component of C.*

Proof. Suppose that $gh = 0$ in R_C for some homogeneous polynomial h. This means that $gh = kf$ for some homogeneous polynomial k and since $k[x, y, z]$ is a unique factorization domain, we conclude that each irreducible factor of f must be a factor of either g or h. If non of them divides g, we must have that $h \in (f)$ so $h = 0$ in R_C. Thus g defines an injective map if it doesn't vanish on any component of C.

If g does vanish on some component, we will be able to find $h \neq 0$ in R_C with $gh = 0$ showing that the map is not incjective. □