Notes on Algebraic Curves

F.Beukers

1 Introduction

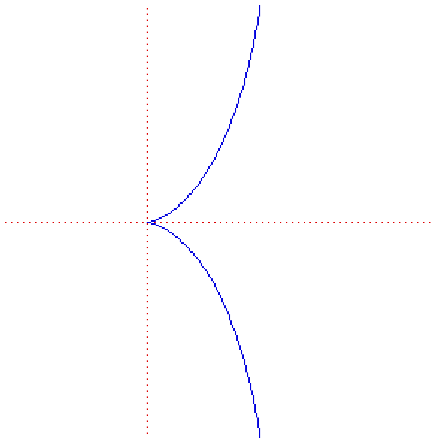
Algebraic curves have been studied since antiquity. We are all familiar with the circle, parabola and ellipse, which are examples of so-called *conic sections*. But also more involved curves were studied already by the ancient Greeks. We recall the conchoid of Nicomedes (180 BC) and the cissoid of Diocles (180 BC) which were both used in solutions of the duplication of the cube problem. As more recent curves we recall the cardioid (Castillon, 1741), the folium (Descartes, 1638) and the lemniscate (Jacob Bernoulli, 1694).
All these curves share the property that, beside their geometrical description, they can be given by algebraic equations in the plane equipped with coordinates x, y. The equation of the conic sections are of course all quadratic. For the cissoid it reads

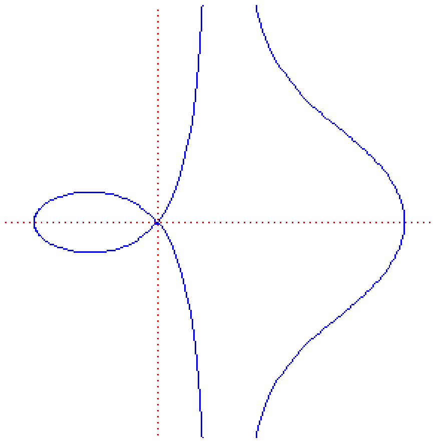
$$y^2(2a - x) = x^3$$

and for the conchoid we have

$$(x - b)^2(x^2 + y^2) - a^2x^2 = 0.$$

In the real plane they look like


Cissoid of Diocles


Conchoid

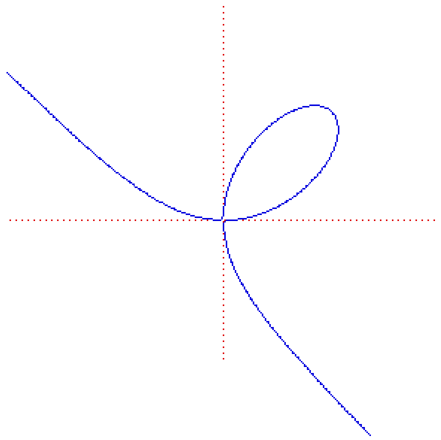
The equation of the Folium reads

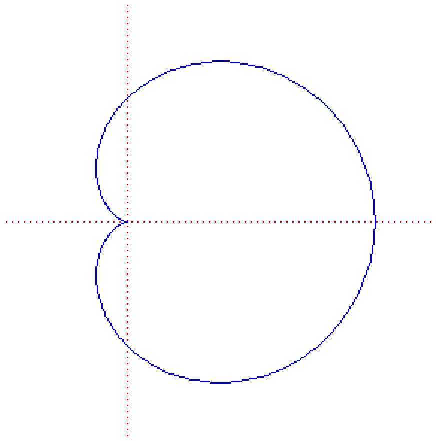
$$x^3 + y^3 = 3axy$$

for the Cardiod we have

$$(x^2 + y^2 - axy)^2 = 4a^2(x^2 + y^2).$$

Their real points look like

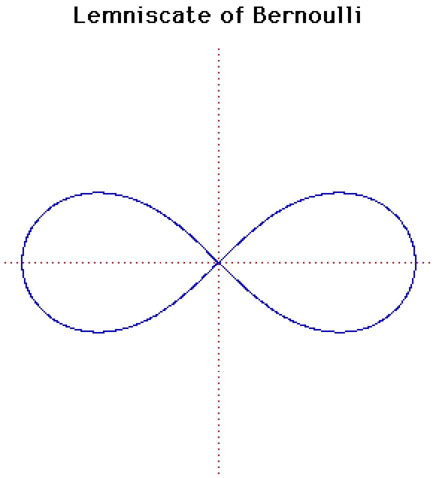

Folium of Descartes


Cardioid

Finally the lemniscate is given by

$$(x^2 + y^2)^2 - a^2(x^2 - y^2) = 0$$

and it looks like



In the above pictures we have basically drawn the curves as subset of $\mathbb{R}^2$. However, it is also possible to consider curves given by equations with complex coeffients or even coefficients from finite fields. They are a little harder to draw though.

Definition 1.1 *Let k be a field. A (plane, affine) algebraic curve defined over k is an equation of the form*

$$F(x,y)=0$$

where $F \in k[X,Y]$.

Above we have considered curves defined over $\mathbb{R}$, which we shall call *real (algebraic) curves*. When the coefficients of the defining equation are in $\mathbb{C}$ we speak of a *complex (algebraic) curve*. We have very formally defined an algebraic curve by an equation. Of course there are also solutions to this equation. We shall call these solutions the points of our curve. More precisely,

Definition 1.2 *Let C be an algebraic curve defined by $F(x,y)=0$ with $F \in k[X,Y]$. Let K be a field containing k (possibly $K=k$). The K-rational points of C are the solutions of $F(x,y)=0$ in $x,y \in K$. Notation: $C(K)$.*

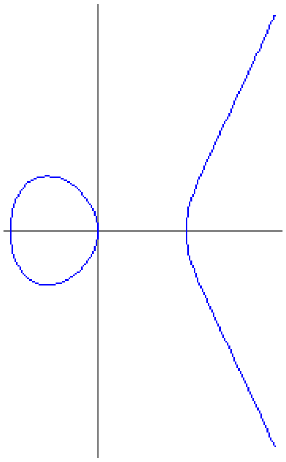
In the pictures above we have drawn the set of real points $C(\mathbb{R})$ of our curves. Of course we can also consider the *complex points* $C(\mathbb{C})$ which is what we shall do later on.

Definition 1.3 *Let C be a curve given by $F(x,y) = 0$ with $F \in k[X,Y]$. We shall call C irreducible over k if F is an irreducible polynomial in the ring $k[X,Y]$. We shall call C absolutely irreducible, or geometrically irreducible, if F is irreducible in $\overline{k}[X,Y]$, where $\overline{k}$ is the algebraic closure of k.*

For example, let C be the curve given by $x^3+y^3+1-3xy = 0$. It is irreducible over $\mathbb{Q}$ because $x^3+y^3+1-3xy$ is irreducible in $\mathbb{Q}[x,y]$. It is reducible over $\mathbb{Q}(\sqrt{-3})$ however, because

$$x^3+y^3+1-3xy = (x+y+1)(x+\omega y+\omega^2)(x+\omega^2 y+\omega)$$

where $\omega = (-1+\sqrt{-3})/2$ is a cube root of unity.
On the other hand, the curve $x^3+y^3+1 = 0$ is absolutely irreducible because x^3+y^3+1 is irreducible in $\mathbb{C}[x,y]$.
Although many of the things we discuss in this course hold for general fields k we shall confine ourselves to real and complex curves, together with their real and/or complex points. At this point it is interesting to note that the real points of a real curve do not always reflect the properties of the curve (that is: its defining equation). For example, the equations $x^2+y^2+1 = 0$ and $x^2+2y^2+3 = 0$ are clearly distinct curves, yet they have the same set of real points, namely the empty one. Another observation, the polynomial $y^2-(x^3-x)$ is absolutely irreducible, whereas the real points of $y^2 = x^3-x$ look like



In other words, $C(\mathbb{R})$ consists of two topological components, but we tagged the curve as being irreducible. All this will prompt us to look at the complex points of an algebraic curve rather than the real ones. In the next section we will find some more motivation for this.

2 Bezout's inequality

In this section we consider the intersection of two algebraic curves. Suppose the curves are given by $F(x,y)=0$ and $G(x,y)=0$, then we shall be interested in their common solutions. In order to solve this system of equations we need to introduce some elimination theory for polynomial equations. In general this is done using so-called Gröbner basis techniques, but here we can confine ourselves to introducing the *resultant* of two polynomials.
In the section we let R be an integral domain. This is a commutative ring with $1(\neq 0)$ and no zero-divisors. To such a ring we can associate its field of quotients which we denote by K. To fix ideas we can think of the pairs $R=\mathbb{Z}, K=\mathbb{Q}$ or $R=\mathbb{Q}[y], K=\mathbb{Q}(y)$. The ring of polynomials with coefficients in R is denoted by $R[x]$. We recall the following theorem.

Theorem 2.1 *Suppose R is a unique factorisation ring. Then the same holds for $R[x]$.*

As a consequence we have unique factorisation in $\mathbb{Z}[x]$. By induction on n we can also show that we have unique factorisation in any polynomial ring $K[x_1,x_2,\ldots,x_n]$ where K is a field.
Consider two polynomials $F(x),G(x)\in R[x]$ and write them in the form $F(x)=p_mx^m+p_{m-1}x^{m-1}+\cdots+p_1x+p_0,\ G(x)=q_nx^n+\cdots+q_1x+q_0$. The *resultant* of F and G is given by the determinant of the so-called *Sylvester matrix*

$$\mathrm{Res}(F,G)=\det\begin{pmatrix}
p_0 & p_1 & \cdots & p_m & 0 & \cdots & 0\\
0 & p_0 & \cdots & p_{m-1} & p_m & \cdots & 0\\
\vdots & & & & & & \vdots\\
0 & 0 & \cdots & p_0 & p_1 & \cdots & p_m\\
q_0 & q_1 & \cdots & q_n & 0 & \cdots & 0\\
0 & q_0 & \cdots & q_{n-1} & q_n & \cdots & 0\\
\vdots & & & & & & \vdots\\
0 & 0 & \cdots & q_0 & & q_{n-1} & q_n
\end{pmatrix}$$

As a rule of thumb, the row with the entries p_i occurs n times, the row with the q_j occurs m times.
Examples,

$$\mathrm{Res}(x^4-4x^2+3x-2, x^4+5x^3-2x+1) = -4457, \text{ where } R = \mathbb{Z}$$

and

$$\mathrm{Res}(x^2+2y^2x+y, x^3-yx^2-y^3) = y^3(1+y-5y^3+4y^5+8y^6), \text{ where } R = \mathbb{Q}[y]$$

Theorem 2.2 *Let $F(x), G(x) \in R[x]$ be two polynomials of degree n and m respectively. Then there exist polynomials $A(x), B(x) \in R[x]$ of degrees $< m$ and $< n$ respectively, such that*

$$\mathrm{Res}(F, G) = A(x)F(x) + B(x)G(x).$$

Moreover, assuming that R is a unique factorisation ring, we have $\mathrm{Res}(F, G) = 0$ *if and only if F, G have a common divisor of positive degree in x.*

Proof To the first column of the determinant we add x times the second column, x^2 times the third column, etc until x^{m+n-1} times the last column. After these additions the first column looks like

$$(F(x), xF(x), \ldots, x^{n-1}F(x), G(x), \ldots, x^{m-1}G(x))^t.$$

All entries of the other columns are in R. Develop the determinant along this first column and we obtain a relation of the form $A(x)F(x) + B(x)G(x) = \mathrm{Res}(F, G)$, where A, B are polynomials of degrees at most $n-1, m-1$ respectively.
Suppose F, G have a common divisor of positive degree. Then this divisor divides $\mathrm{Res}(F, G)$ which is only possible if $\mathrm{Res}(F, G) = 0$. Suppose conversely that $\mathrm{Res}(F, G) = 0$. Then the rows of the Sylvester matrix satisfy a non-trivial linear dependence relation with coeffcients in K, hence coefficients in R. Denote the coefficients of such a dependence relation by

$$(a_0, a_1, \ldots, a_{n-1}, b_0, b_1, \ldots, b_{m-1}).$$

Write $\tilde{A}(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ and $\tilde{B}(x) = b_0 + b_1x + \cdots + b_{m-1}x^{m-1}$ and notice that the dependence relation implies that $\tilde{A}(x)F(x) + \tilde{B}(x)G(x) = 0$. So $G(x)$ divides $\tilde{A}(x)F(x)$. Since $\deg(G) = n > n-1 \geq \deg(\tilde{A})$ we see that F, G must have a common divisor. Notice that we could not use the polynomials $A(x), B(x)$ since we cannot assure that they are non-trivial.

qed

Proposition 2.3 *Let notations be as above. Consider the resultant of* F, G *as polynomial in their coefficients* p_i, q_j. *Then, for any monomial*

$$p_0^{n_0} \cdots p_m^{n_m} q_0^{m_0} \cdots q_n^{m_n}$$

occurring in $\mathrm{Res}(F, G)$ *we have that*

1. $\sum_{i=0}^m n_i = n$ *and* $\sum_{j=0}^n m_j = m$
2. $\sum_{i=0}^m i n_i + \sum_{j=0}^n j m_j = mn$

Proof. The first property follows immediately from the shape of the Sylvester matrix. To see the second property we consider $\mathrm{Res}(F(\lambda x), G(\lambda x))$. In the Sylvester matrix for $F(\lambda x), G(\lambda x)$ we multiply the the second row with λ, the third with λ^2 untill the n-th row with λ^{n-1}. Then we multiply the $n+2$-nd row with λ, the $n+3$-rd with λ^2, etcetera untill the $n+m$-th with λ^{m-1}. The value of this new determinant is $\lambda^{n(n-1)/2+m(m-1)/2}\mathrm{Res}(F(\lambda x), G(\lambda x))$. On the other hand we see that the same determinant can be obtained from the Sylvester determinant of $F(x), G(x)$ by multiplication of the second column with λ, the third column with λ^2, etcetera, untill the $m+n$-th column with λ^{m+n-1}. Thus we see that the new determinant equals $\lambda^{(m+n)(m+n-1)/2}\mathrm{Res}(F(x), G(x))$ as well. Since $(m+n)(m+n-1)/2 - n(n-1)/2 - m(m-1)/2 = mn$ we conclude that

$$\mathrm{Res}(F(\lambda x), G(\lambda x)) = \lambda^{mn}\mathrm{Res}(F, G),$$

which proves our second statement.

qed

As illustration we consider the resultant of the quadratric polynomials $F = p_0 + p_1 x + p_2 x^2$ and $G = q_0 + q_1 x + q_2 x^2$ which is defined as

$$\begin{vmatrix} p_0 & p_1 & p_2 & 0 \\ 0 & p_0 & p_1 & p_2 \\ q_0 & q_1 & q_2 & 0 \\ 0 & q_0 & q_1 & q_2 \end{vmatrix}$$

and whose value is

$$p_2^2 q_0^2 - p_1 p_2 q_0 q_1 + p_0 p_2 q_1^2 + p_1^2 q_0 q_2$$

$$-2p_0 p_2 q_0 q_2 - p_0 p_1 q_1 q_2 + p_0^2 q_2^2.$$

You can easily verify our Proposition in the case of this resultant. In each term there are two factor p_i and two factors q_j and the weighted degree of each term is 4. Notice that if we replace p_i by $p_i\lambda^i$ and q_j by $q_j\lambda^j$ in each term, each such term is multiplied by λ^4. This can be seen directly from the Sylvester determinant expression,

$$\mathrm{Res}(F(\lambda x), G(\lambda x)) = \begin{vmatrix} p_0 & p_1\lambda & p_2\lambda^2 & 0 \\ 0 & p_0 & p_1\lambda & p_2\lambda^2 \\ q_0 & q_1\lambda & q_2\lambda^2 & 0 \\ 0 & q_0 & q_1\lambda & q_2\lambda^2 \end{vmatrix} = \lambda^{-2} \begin{vmatrix} p_0 & p_1\lambda & p_2\lambda^2 & 0 \\ 0 & p_0\lambda & p_1\lambda^2 & p_2\lambda^3 \\ q_0 & q_1\lambda & q_2\lambda^2 & 0 \\ 0 & q_0\lambda & q_1\lambda^2 & q_2\lambda^3 \end{vmatrix}.$$

Note that the second column in the last determinant is divisible by λ, the third by λ^2 and the fourth by λ^3. Hence $\mathrm{Res}(F(\lambda x), G(\lambda x)) = \lambda^4 \mathrm{Res}(F(x), G(x))$. We now apply our theory of resultants to the ring $R = k[y]$ where k is a field, usually $\mathbb{R}$ or $\mathbb{C}$. Polynomials in $R[x]$ are then polynomials in two variables x, y. Let $F(x, y)$ and $G(x, y)$ be two such polynomials and suppose they have no common non-constant factor. The resultant of F, G, when considered as polynomials in x, is denoted by $\mathrm{Res}_x(F, G)$. But F, G can also be considered as polynomials in y. The resultant is then denoted by $\mathrm{Res}_y(F, G)$.

Proposition 2.4 *Let $F, G \in k[x, y]$ and suppose the total degree of F is m and the total degree of G is n. Then $\mathrm{Res}_x(F, G)$ is either zero or a polynomial of degree $\leq mn$ in y.*

Proof. We will use Proposition 2.3. Write $F(x, y) = \sum_{i=0}^m p_i(y)x^i$. Then $p_i(y)$ is a polynomial of degree at most $m - i$ in y. Similarly, when we write $G(x, y) = \sum_{j=0}^n q_j(y)x^j$, the polynomials $q_j(y)$ have degree at most $n - j$. The resultant is a sum of monomials $p_0^{n_0} \cdots p_m^{n_m} q_0^{m_0} \cdots q_n^{m_n}$. The degree of such a monomial is at most

$$\begin{aligned} & \sum_{i=0}^m n_i(m - i) + \sum_{j=0}^n m_j(n - j) \\ = \; & m\sum_{i=0}^m n_i + n\sum_{j=0}^n m_j - \sum_{i=0}^m in_i - \sum_{j=0}^n jm_j \\ = \; & mn + mn - mn = mn \end{aligned}$$

The last line follows from application of Proposition 2.3. So if $\mathrm{Res}_x(F, G) \neq 0$ it is a polynomial of degree $\leq mn$.

qed

Let $F, G \in k[x,y]$ be two polynomials without common non-constant factor. Let x_0, y_0 satisfy $F(x_0,y_0) = G(x_0,y_0) = 0$. Then $\mathrm{Res}_x(F,G)(y_0) = 0$ as well. Since $\mathrm{Res}_x(F,G)$ has degree at most mn we see that at most mn values of y_0 are possible. Similarly at most mn values of x_0 are possible. As a consequence the set of points x_0, y_0 satisfying $F(x_0,y_0) = G(x_0,y_0) = 0$ is at most finite.

We can phrase this alternatively. Consider two algebraic curves C, D given by the equations $F(x,y) = 0$ and $G(x,y) = 0$. We shall say that C, D have a *common component* if F, G have non-constant common divisor $H \in k[x,y]$. The common component is then the curve given by the equation $H(x,y) = 0$. If F, G do not have a non-constant common factor we say that the curves do not have a common component.

Any point x_0, y_0 satisfying $F(x_0,y_0) = G(x_0,y_0) = 0$ can be seen as an intersection point of C and D. So we see that two algebraic curves without common component intersect in finitely many points. We can say a bit more though.

Theorem 2.5 (Bezout inequality) *Let C, D be two algebraic curves of degree m, n respectively. Suppose that the curves have no common component. Then the number of intersection points of C, D is at most mn.*

Proof. We have seen that the number of intersection points is finite. Choose $\lambda \in k$ (extend k a bit if necessary) so that the coordinate u given by $u = y + \lambda x$ has distinct values for every two intersection points of C, D. Let C, D be given by the polynomial equations $F(x,y) = 0$ and $G(x,y) = 0$. Consider $\mathrm{Res}_x(F(x, u - \lambda x), G(x, u - \lambda x))$. This is a non-zero polynomial of degree $\le mn$ in u. So it has at most mn zeros u. To every such zero there corresponds at most one intersection point by our choice of λ. This proves our Theorem.

qed

Finally we note that we can compute the points of intersection of two curves C, D by use of the resultant. In general, let $F(x,y) = 0$ and $G(x,y) = 0$ be their equations. The zeros of the resultant $\mathrm{Res}_x(F,G) \in k[y]$ are the y-coordinates of the points of intersection. To each such zero y we like to compute the x-coordinate(s) of the intersection points. In general this can easily be done using Gröbner basis computation, but in this case the following observation may also help.

Proposition 2.6 *Let $P, Q \in R[x]$ and let $L(P,Q)$ be the determinant of the matrix which we get from the Sylvester matrix by replacing the first row by $(x, -1, 0, 0, \ldots, 0)$. Then $L(P,Q)$ is a polynomial in $R[x]$ of degree at most 1 and it can be written in the form $L(P,Q) = U(x)P(x) + V(x)Q(x)$ where $U, V \in R[x]$.*

The proof is an exercise which follows exactly the same lines as the proof of Theorem 2.2.
We illustrate with an example to intersect two conics, although this particular case could be handled much more easily in a straightforward manner. We intersect the curves

$$P(x,y) := -3 - 4x - x^2 + 6xy + 3y^2 = 0, \qquad Q(x,y) := 1 + y - x^2 + xy = 0.$$

The resultant of P, Q reads $-24y(y-1)(y+1)(y-2)$ so we see that the y-coordinates of the intersection points are $0, 1, -1, 2$. To find the corresponding x values we compute

$$L(P,Q) = \det \begin{pmatrix} x & -1 & 0 & 0 \\ 0 & 3y^2-3 & 6y-4 & -1 \\ 1+y & y & -1 & 0 \\ 0 & 1+y & y & -1 \end{pmatrix}$$

which equals $-4 + y + 5y^2 + (8y^2 - 5y - 4)x$. It belongs to the ideal generated by P, Q. Notice that

$$L(P,Q)|_{y=0} = -4 - 4x, \;\; L(P,Q)|_{y=1} = 2 - x$$

$$L(P,Q)|_{y=-1} = 9x, \;\; L(P,Q)|_{y=2} = 18 + 18x.$$

From this we find the intersection points $(-1,0), (2,1), (0,-1), (-1,2)$. We note however that this method may not always work since $L(P,Q)$ may vanish identically when substituting values for y.

3 Bezout's theorem for projective curves

It turns out that Bezout's inequality is actually an equality if we take the right precautions.
Let C, D be two curves defined over $\mathbb{R}$. Then we must look at their complex intersection points $C(\mathbb{C}) \cap D(\mathbb{C})$. For example, consider the circle $x^2 + y^2 = 2$

intersected with the line $y = x + 2c$. We compute the intersection points by solving $(x + 2c)^2 + x^2 = 2$ which gives us the solutions

$$x = -c \pm \sqrt{1 - c^2}.$$

So in general (that is, if $c \neq \pm 1$) there are two intersection points if we are willing to consider complex points. So most of the time there are two solutions, exactly the upper bound in Bezout's inequality.

Another reason for failure of a Bezout equality is the following simple one. Consider the parallel lines $y = x$ and $y = x + 1$. They have clearly no intersection in the plane. However, they do have an intersection at infinity which becomes visible if we are willing to extend our (affine) plane to the *projective plane*.

The projective plane over a field k is defined as the set of triples $(X, Y, Z) \in k^3$, not all zero modulo the equivalence relation

$$(X, Y, Z) \sim (X', Y', Z') \iff \exists \lambda \in k : \; X' = \lambda X, \; Y' = \lambda Y, \; Z' = \lambda Z.$$

Notation $\mathbb{P}^2(k)$. Very often, to emphasize that we are actually looking at ratios between the three coordinates, we write a projective point as $(X : Y : Z)$.

In particular, any point of the projective plane is equivalent to at least one point of the following form: $(x : y : 1), (x : 1 : y)$ or $(1 : y : z)$. The affine plane k^2 (or more officially, $\mathbb{A}^2(k)$) can be embedded in $\mathbb{P}^2$ via $(x, y) \mapsto (x : y : 1)$. The set of points not covered by this embedding, i.e. those with $z = 0$, is called the *line at infinity*. The embeddings $(x, y) \mapsto (x : 1 : y)$ and $(x, y) \mapsto (1 : x : y)$ give two more embeddings. Together these three embeddings provide us with a cover of $\mathbb{P}^2$ with affine planes $\mathbb{A}^2$.

We now define algebraic curves in $\mathbb{P}^2$.

Definition 3.1 *Let k be a field. A (plane, projective) algebraic curve defined over k is an equation of the form*

$$F(X, Y, Z) = 0$$

where $F \in k[X, Y, Z]$ is a homogeneous polynomial.

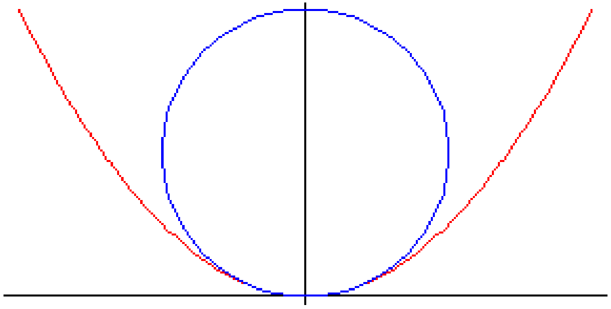
In the same way as with affine curves we can define points on a projective curve. Since the defining polynomial F of a projective curve is homogeneous we have $F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x, y, z)$. Hence $F(x, y, z) = 0 \iff$

$F(\lambda x, \lambda y, \lambda z) = 0$ for any non-zero λ. Actually, this is precisely the reason we consider homogeneous polynomials when speaking about projective algebraic curves.

Any affine curve C can be extended to a projective curve as follows. Let $F(x, y) = 0$ be the defining equation of C and suppose it has degree n. Then we homogenize by taking the projective equation $Z^n F(X/Z, Y/Z) = 0$. For example, the affine curve $y^2 = x^3 - 2x - 1$ can be extended as projective curve by writing it as $(Y/Z)^2 = (X/Z)^3 - 2X/Z - 1$ and then multiply by Z^3, to get $Y^2 Z = X^3 - 2XZ^2 - Z^3$. This process is called homogenization of the affine equation. We can reverse the procedure simply by setting $X = x, Y = y, Z = 1$. In that way we discard the line at infinity.

Let us turn to our parallel affine lines $y = x, y = x + 1$. Projectively they can be written as $Y = X$ and $Y = X + Z$. Solving these equations gives us $Z = 0$ and $X = Y$. These solutions all represent the same projective point $(1 : 1 : 0)$, which is a point at infinity.

Consider the two affine curves $y = x^2, y = x^2 + 1$. Clearly they have no intersection in the affine plane. So let us homogenize to the projective curves $YZ = X^2, YZ = X^2 + Z^2$. Solution of this system gives us $Z = 0, X = 0$. So there is only one point of intersection ,namely $(0 : 1 : 0)$. Let us put $Y = 1$. Then we get the affine curve $z = x^2, z = x^2 + z^2$. In a picture,



Thus we see that the curves have 1 point of intersection, but we have higher order intersection, the curves are tangent in the point $x = 0, z = 0$. In order to get a Bezout equality we should also count intersection points with suitable multiplicities.

Let C, D be two plane projective algebraic curves and let P be a point in the intersection of C and D. When C and D do not have a common component we shall define an *intersection multiplicity* at P in the next section. We denote it by $\nu_P(C, D)$. It is a positive integer measuring the order of intersection of C and D at the point P. Using this intersecting multiplicity we can state the following theorem.

Theorem 3.2 (Bezout) *Let C, D be two plane projective curves defined over a field k of degrees m, n. Suppose that they have no common components. Let S be the set of intersection points $C(\overline{k}) \cap D(\overline{k})$. Here $\overline{k}$ denotes the algebraic closure of k. Then*

$$\sum_{P \in S} \nu_P(C, D) = mn.$$

Note that if we look at real or complex curves (that is, $k = \mathbb{R}$ or $k = \mathbb{C}$) then Bezout's theorem is a statement about the complex intersection points ($\overline{k} = \mathbb{C}$).

4 Singularities and intersection multiplicities

Let C be an algebraic curve given by $F(x, y) = 0$ and $P = (p, q)$ a point on C. The tangent of C at the point P is given by $(x-p)F_x(p, q) + (y-q)F_y(p, q) = 0$. Notice that this defines a straight line if and only if at least one of $F_x(p, q), F_y(p, q)$ is non-zero. When $F_x(p, q) = F_y(p, q) = 0$ we call P a *singular point* of the curve C. Here are some examples where $(0, 0)$ is a singular point. Of course this is no restriction since we can always perform a change of coordinates such that $P = (0, 0)$.

To compute the singular points of an affine curve we must solve the simultaneous equations $F(p, q) = F_x(p, q) = F_y(p, q) = 0$ in the unknowns p, q. However, since we shall often deal with projective curves, it is better to look at the projective version of this calculation.

Suppose F has degree n. We define $\mathcal{F} = Z^n F(X/Z, Y/Z)$. This is the homogenized version of F. Notice that

- $\mathcal{F}_X = Z^{n-1} F_x(X/Z, Y/Z),\ \mathcal{F}_Y = Z^{n-1} F_y(X/Z, Y/Z)$
- $Z\mathcal{F}_Z = n\mathcal{F} - X\mathcal{F}_X - Y\mathcal{F}_Y$

Using these relations we see that finding projective singular points of the form $(p : q : 1)$ comes down to solving

$$\mathcal{F}_X(p, q, 1) = \mathcal{F}_Y(p, q, 1) = \mathcal{F}_Z(p, q, 1) = 0.$$

Furthermore, if $(p,q,1)$ is a non-singular point of C the tangent line is given by

$$X\mathcal{F}_X(p,q,1)+Y\mathcal{F}_Y(p,q,1)+Z\mathcal{F}_Z(p,q,1)=0.$$

Since any projective point lies in one of the three affine spaces $Z\neq 0, Y\neq 0$ or $X\neq 0$, this gives us the following statement.

Theorem 4.1 *Let C be a projective curve given by the homogeneous equation $F(X,Y,Z)=0$. Let $P=(p:q:r)$ be a point on C. Then C is singular if and only if*

$$F_X(p,q,r)=F_Y(p,q,r)=F_Z(p,q,r)=0.$$

If P is non-singular, the tangent of C at P is given by

$$XF_X(p,q,r)+YF_Y(p,q,r)+ZF_Z(p,q,r)=0.$$

Here is an example where we compute the singular points of the cardioid $(x^2+y^2-xy)^2-4(x^2+y^2)=0$. In homogeneous form,

$$F(X,Y,Z):=(X^2+Y^2-XY)^2-4Z^2(X^2+Y^2)=0.$$

Consider the equations

$$\begin{aligned}F_X &= 2(X^2+Y^2-XY)(2X-Y)-8XZ^2=0\\ F_Y &= 2(X^2+Y^2-XY)(2Y-X)-8YZ^2=0\\ F_Z &= -8Z(X^2+Y^2)=0\end{aligned}$$

From the last equation it follows that either $Z=0$ or $X=\pm iY$. In the first case our equations reduce to

$$(X^2+Y^2-XY)(2X-Y)=0,\qquad (X^2+Y^2-XY)(2Y-X)=0.$$

The assumption $X^2+Y^2-XY\neq 0$ leads to $2X-Y=2Y-X=0$, hence $X=Y=0$, which is no solution. Hence $X^2+Y^2-XY=0$ and we get $X=\rho Y$ or $X=\rho^{-1}Y$ where ρ is a primitive 6-th root of unity. So we find the points $(\rho:1:0)$ and $(\rho^{-1}:1:0)$. Now suppose that $X=iY$. The first two equations become

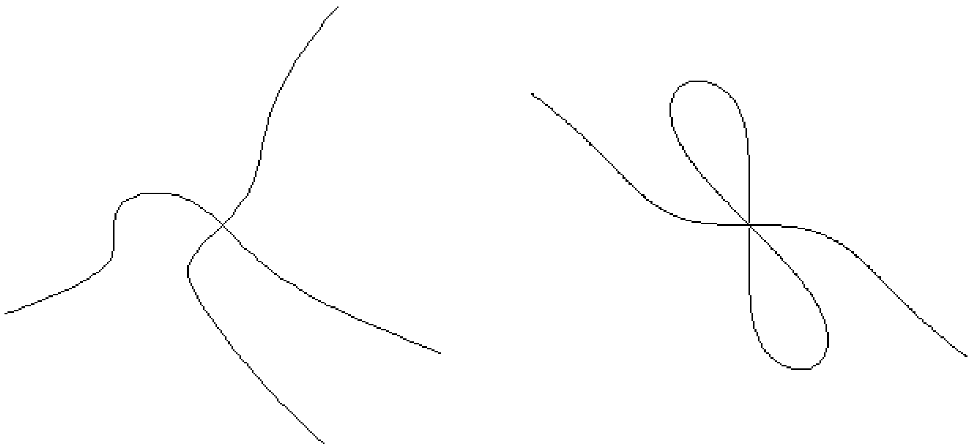
$$-2i(2i-1)Y^3-8iYZ^2=0,\qquad -i2(2-i)Y^3-8YZ^2=0.$$

If $Y\neq 0$ we get $(4+2i)Y^2-8iZ^2=0$ and $(-2-4i)Y^2-8Z^2=0$ which are conflicting equations unless $Y=Z=0$ which does not give a solution.

We are left we the possibility $Y = 0$ which leads us to the third singularity $(0:0:1)$.
For the local study of a singular point it is best to introduce affine coordinates and choose them in such a way that the singular point has coordinates $(0,0)$.

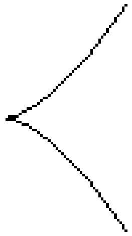
Definition 4.2 *Let P be a point of an affine curve C. Choose affine coordinates such that $P = (0,0)$ and let $F(x,y) = 0$ be the equation of C in these coordinates. Then the multiplicity of P is given by the degree of the lowest degree monomial occurring in F. Notation $\nu_P(C)$.*

Notice that $\nu_P(C) > 0$ since P is a point of C and that $\nu_P(C) = 1$ if and only if P is a non-singular point of C.
Note that one must verify that $\nu_P(C)$ is independent of the choice of affine coordinates.
Although singularities of curves can be quite complicated there are a number of simple types that one distinguishes. Suppose that $P = (0,0)$ is a singular point of the curve given by $F(x,y) = 0$. Here are a number of cases that may occur.
The nodal singularity. Suppose $F = F_n +$ terms of degree $> n$ where F_n is homogeneous of degree n with distinct linear factors. For example, $F = x^2 - y^2 + x^3 + 4xy^3 - y^5$ or $F = xy(x+y) + x^5 - 2x^3y^2 + y^7$. Locally, around P these curves look like

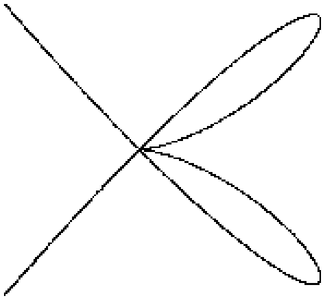


When $n = 2, 3, ...$ we speak of a double node, triple node, etc. Their multiplicity is given $\nu_P(C) = n$.
The cusp. Suppose $F = ax^p - by^q +$ higher degree terms where $p, q \geq 2, ab \neq 0$, $\gcd(p,q) = 1$ and where ”degree” means the weighted degree given by

$\deg(x^a y^b) = qa + pb$. When $p = 2, q = 3$ we say that $(0,0)$ is an ordinary cusp, when $p > 2$ or $q > 3$ we speak of a generalised cusp. The standard example is the curve given by $y^2 = x^3$ which looks like



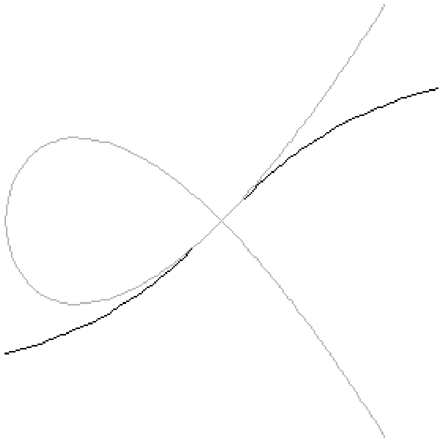
However, mixes of these singularities are also possible, for example the curve $x^5 - x^2y^2 + y^4 = 0$,



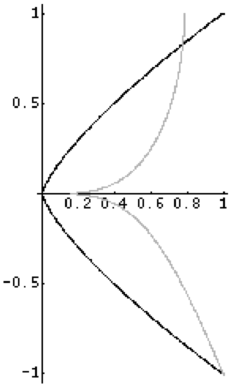
As for intersection multiplicity we point out that we can have several types of intersection. Let C, D be two algebraic curves that intersect in a point P. Suppose first that P is a non-singular point of both C and D. When the tangents at P are different we speak of *transversal intersection* and it makes sense to define the intersection multiplicity as 1.

When the two tangents coincide, we can choose coordinates such that $P = (0,0)$ and the common tangent is the line $y = 0$. Let $y - cx^\gamma + O(x^{\gamma+1}, xy) = 0$ be the local equation for C and $y - dx^\delta + O(x^{\delta+1}, xy) = 0$ the local equation for D. In that case it makes sense to define the intersection multiplicity as $\min(\gamma, \delta)$ when $\gamma \neq \delta$. However, when $\gamma = \delta$ and $c = d$ we must be more careful. For example, the curves $y = x^2 + x^3$ and $y = x^2 + 2x^3$ intuitively should have contact order 3, whereas $\min(\gamma, \delta) = 2$.

When P is a singular point on C or D or both, the situation gets more complicated. For example, when C is given by $y - x + y^2x = 0$ and D by $y^2 = x^3 + x^2$, the point $P = (0,0)$ is non-singular on C and singular on D. The curves look like



Or, when C is given by $y^4 - x^3 = 0$ and D by $x^2y^3 - y^2 + 2x^7 = 0$ the point $P = (0,0)$ is singular on both C and D. The intersecting curves look like



Intuition becomes a bit more complicated in the last example, so we give a formal definition for intersection multiplicity. Suppose that the curves C, D are defined over the field k and that they have no common components. Suppose the curves are given by $F(x,y) = 0$ and $G(x,y) = 0$ and that $P = (p,q) \in k^2$. We consider the local ring

$$\mathcal{O}_P = \{A(x,y)/B(x,y) \mid A, B \in k[x,y],\ B(p,q) \neq 0\}.$$

In that ring we define the ideal $I(F,G)$ generated by F, G. The quotient ring $\mathcal{O}_P/I(F,G)$ can be considered as a k-vector space.

Definition 4.3 *Let notations be as above. The intersection multiplicity of*

C, D in the point P is defined by

$$\nu_P(C,D) = \dim_k(\mathcal{O}_P/I(F,G)).$$

To show how this definition works, we demonstrate a few examples.

1. Suppose we have two straight lines that intersect in $P = (0,0)$ in different directions. We can choose a coordinate system so that the lines are given by $x = 0$ and $y = 0$. One easily checks that any element $A(x,y)/B(x,y)$ of $\mathcal{O}_P$ is modulo $I(x,y)$ equivalent to $A(0,0)/B(0,0)$. Hence the dimension of $\mathcal{O}_P/I(x,y)$ is one.

2. Suppose that $P = (0,0)$ is non-singular on C and D and the tangents are distinct. By a proper choice of coordinates we can see to it that these tangents are given by $x = 0$ and $y = 0$ respectively. Then the equations read $F(x,y) = x +$ higher order terms and $G(x,y) = y +$ higher order terms. Let us write $F(x,y)$ in the form $F(x,y) = xF_1(x,y) + yF_2(x,y)$ where F_1, F_2 are polynomials. Of course there are many ways in which this can be done, but we always have that $F_1(0,0) = 1$ and $F_2(0,0) = 0$ (please check). Similarly $G(x,y) = xG_1(x,y) + yG_2(x,y)$ and $G_1(0,0) = 0, G_2(0,0) = 1$. We can now solve for x and y,

$$x = \frac{1}{\Delta(x,y)}(FG_2 - GF_2), \quad y = \frac{1}{\Delta(x,y)}(-FG_1 + GF_1)$$

   where $\Delta(x,y) = F_1(x,y)G_2(x,y) - F_2(x,y)G_1(x,y)$. Notice that $\Delta(0,0) = 1$, hence $x \in I(F,G)$ and $y \in I(F,G)$. Thus we conclude that $I(F,G) = I(x,y)$ and we are back again in the previous case.

3. Let C be given by $F = y^2 - x^3 - x^2 = 0$ and D by $G = y - x + xy^2 = 0$. Denote the ideal $I(F,G)$ by I. Notice that $G - xF = y - x + x^3 + x^4$. Hence $y \equiv x - x^3 - x^4 (\text{mod } I)$. Combining this with the first equation we get $(x - x^3 - x^4)^2 - x^3 - x^2 \equiv 0 (\text{mod } I)$ and after simplification, $x^3(-1 - 2x - 2x^2 + x^3 + 2x^4 + x^5) \equiv 0(\text{mod } I)$. The factor between parentheses is invertible, hence $x^3 \equiv 0(\text{mod } I)$. So $x^3 \in I$ and this implies that $y - x \in I$. It is now straightforward to see that $I(F,G) = I(y - x, x^3)$ and $\dim \mathcal{O}_P/I(F,G) = 3$.

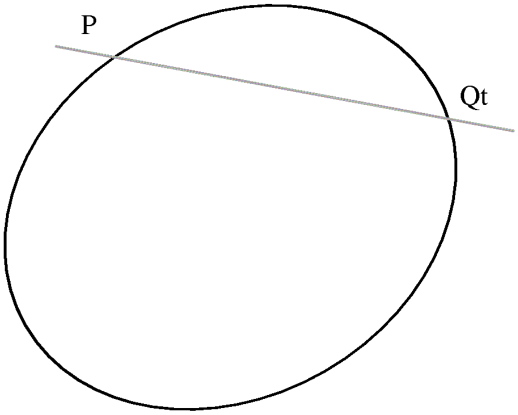
5 Rational parametrisation

It is well known that the circle $x^2 + y^2 = 1$ has a parametrisation by rational functions given by

$$x = \frac{1-t^2}{1+t^2}, \quad y = \frac{2t}{1+t^2}.$$

Conversely, given any point on the unit circle, the corresponding parameter value is given by $(1-x)/y$.

More generally, any non-singular algebraic curve of degree 2 can be parametrised by rational functions. We call such curves conics (from conic sections, i.e. circles, ellipses, hyperbolae, parabolae). The idea is to use the so-called chord-method. Let C be a conic and $P = (p, q)$ a point on C. Consider the line L_t given by $y - q = t(x - p)$. It passes through P and has direction t. Since a line intersects a conic in two points, there is a second point of interscetion we denote by Q_t. The coordinates of Q_t depend on t in a rational way. Conversely, given any point Q on C, the direction of the line connecting P and Q is the parameter value corresponding to Q.



The question arises which algebraic curves can be parametrised rationally. So, given an algebraic curve $F(x, y) = 0$, do there exist non-constant rational functions $r(t), s(t)$ of t such that $F(r(t), s(t)) = 0$?

In general the answer is ”no”, as can be seen from the case of cubic curves.

Proposition 5.1 *Let $f(x)$ be a polynomial of degree 3 with three simple zeros. Then the curve $y^2 = f(x)$ has no rational parametrisation.*

Proof. Suppose we do have a parametrisation,

$$s(t)^2 = f(r(t)).$$

We consider the rational function $r'(t)/s(t)$. Let a be a pole of this rational function. Then either a is a pole of $r(t)$, or $s(a) = 0$.
Suppose a is a pole of order n of $r(t)$. Then a is a pole of order $3n$ of $f(r(t))$ and thus $s(t)$ must have a pole of order $3n/2$ at a. In particular we see that n must be even, say $n = 2m$. So $r(t)$ has a pole of order $2m$ and $s(t)$ a pole of order $3m$ at a. This means that $r'(t)/s(t)$ has a zero of order $m-1$ at a, so r'/s has no pole at a.
Suppose that $s(a) = 0$ and that $s(t)$ has a zero of order n at a. We differentiate $s^2 = f(r)$ to obtain $2ss' = f'(r)r'$. Notice that $f(r(a)) = s(a)^2 = 0$. Since f has only simple zeros this means that $f'(r(a)) \neq 0$. Therefor, from the relation $2ss' = f'(r)r'$ it follows that $r'(t)$ has a zero of order $2n-1$ at a. Hence $r'(t)/s(t)$ has a zero of order $n-1$ at a, again no pole.
Since $r'(t)/s(t)$ does not have poles in finite points a, it must be a polynomial. Let us now study its behaviour when $t = \infty$. Since $r(t), s(t)$ is a parametrisation of $y^2 = f(x)$ the same is true for $\rho(\tau) = r(1/\tau)$, $\sigma(\tau) = s(1/\tau)$. By the same argument we can show that $\rho'(\tau)/\sigma(\tau)$ has no pole in $\tau = 0$. Notice that $r'(t)/s(t) = -\tau^2\rho'(\tau)/\sigma(\tau)$. So $r'(t)/s(t)$ vanishes when $t = \infty$ (i.e $\tau = 0$).
We conclude that $r'(t)/s(t) = 0$ and hence that $r(t)$ is constant. So we do not have a rational parametrisation.

qed

We also show

Proposition 5.2 *The curve given by $x^n + y^n = 1$ cannot be parametrised rationally when $n > 2$. In particular this means that Fermat's equation in polynomials has no non-constant solution.*

Proof. We proceed in almost the same way. Suppose there is a parametrisation $r(t)^n + s(t)^n = 1$ with non-constant rational functions $r(t), s(t)$. We consider the rational function $r'(t)/s(t)^{n-1}$. Suppose a is a pole of this rational function. Then either $s(a) = 0$ or a is a pole of $r(t)$. Suppose the latter holds. Then from the equation it follows that $r(t)$ and $s(t)$ have the same pole order. Hence, because $n-1 \geq 2$, the quotient $r'(t)/s(t)^{n-1}$ has no pole in a. Suppose that $s(a) = 0$. Then $r(a) \neq 0$. Differentiate the relation $r^n + s^n = 1$ to obtain $r^{n-1}r' + s^{n-1}s' = 0$. Since $r(a) \neq 0$ we see that $r'(t)$ has a zero of order $n\mathrm{ord}_a(s) - 1$. Hence $r'(t)/s(t)^{n-1}$ has zero order $\mathrm{ord}_a(s) - 1$. We conclude that r'/s^{n-1} has no finite poles, so it must be a polynomial in t. Let us now look in $t = \infty$. Define $\rho(\tau) = r(1/\tau), \sigma(\tau) = s(1/\tau)$. Clearly this is also a parametrisation of the curve $x^n + y^n = 1$. Hence $\rho'(\tau)/\sigma(\tau)^{n-1}$ has no pole in $\tau = 0$. Since $r'(t)/s(t)^{n-1} = -\tau^2\rho'(\tau)/\sigma(\tau)^{n-1}$ we see that $r'(t)/s(t)^{n-1}$ vanishes at $t = \infty$. Therefore $r'(t)/s(t)^{n-1} = 0$ and $r(t)$ is constant. So there is no parametrisation.

qed

6 Rational functions and maps

Let C be a geometrically irreducible curve given by the equation $F(x,y) = 0$, where $F \in k[x,y]$ is absolutely irreducible. We like to consider functions on C and do this as follows. Any polynomial $P(x,y)$ can be considered as function on C simply by restricting its domain to C. However, the polynomial $P(x,y)$ and any polynomial $Q(x,y)$ such that $P \equiv Q(\text{mod } F)$ will give us the same function on C. Therefore it is more natural to consider the ring

$$\mathcal{O}_k(C) = k[x,y]/(F(x,y))$$

and call this the *ring of regular functions* on C. The suffix k is put in $\mathcal{O}_k$ to indicate that the polynomials are taken from $k[x,y]$. We drop it if the fields of definition are clear from the context. Note that $\mathcal{O}_k(C)$ is an integral domain because F is irreducible. Its quotient field is called the *field of rational functions* on C. Notation: $k(C)$. To emphasize that the functions have their coefficients in k, we sometimes speak of the field of k-rational functions. The subfield k is called the *field of constant functions.* Note that $k(C)$ is generated by the coordinate functions x, y on C.

Proposition 6.1 *Let notations be as above. Then the field $k(C)$ is an extension of k of transcendence degree 1. Moreover, for any non-constant $f \in k(C)$ the extension $k(C)/k(f)$ is finite.*

Let D be another absolutely irreducible curve defined over k by the equation $G(x,y) = 0$. A *rational map* from C to D is a pair of functions $f, g \in k(C)$ such that $G(f,g) = 0$. The map is called constant if f, g are both constant and *non-constant* otherwise. Strictly speaking a rational map can only be seen as a map of points of C to points of D if we limit ourselves to the domain of f and g.
Furthermore, any rational map $\psi : C \to D$ defines an embedding $\phi^* : k(D) \to k(C)$ given by

$$\xi \mapsto f, \qquad \eta \mapsto g$$

where ξ, η are the standard coordinate functions on D. Note that ϕ^* fixes the constant field k.
Conversely, any field embedding $\phi : k(D) \to k(C)$ fixing k defines a rational map from C to D by taking $f = \phi(\xi)$ and $g = \phi(\eta)$.

Definition 6.2 *Let notation be as above and let $\psi : C \to D$ a non-constant rational map. Then the degree of the extension $k(C)/k(f,g)$ is called the degree of the rational map ψ.*

Proposition 6.3 *Let C, be absolutely irreducible curves defined over k. Let $\psi : C \to D$ be a rational map. Suppose that its degree is one. Then there is a rational map $\chi : D \to C$ such that $\chi \circ \psi = \mathrm{id}$.*

Definition 6.4 *A rational map $\psi : C \to D$ is called a birational map if it has an inverse. The curves C, D are called birationally equivalent if there exists a birational map $\psi : C \to D$.*

Notice that the curves C, D are birationally equivalent if and only if the function fields $k(C)$ and $k(D)$ are k-isomorphic. This means that there is a field isomorphism $\phi : k(D) \to k(C)$ which fixes k.
Notice that a rational parametrisation of a curve C can be seen as a rational map from the line to C. So if an irreducible conic C is defined over k and contains a point in $C(k)$ it is birationally equivalent over k to the line.
Similarly we can apply the chord method to a cubic curve C with a double point S. Any line through S, not tangent to the branches at the singularity, intersects C in one more point. The dependence of this point on the slope of the line gives us again a rational parametrisation.

7 The genus of a curve

One of the first problems in the study of absolutely irreducible algebraic curves is to find a classification for them. One such classification might be according to the degree of the curve. Although this is a reasonable idea for very low degree curves, it turns out to be unsatisfactory for higher degree curves. Instead of the degree there is a more interesting quantity, namely the *genus of a curve*. This is a non-negative integer that can be associated to any absolutely irreducible curve and which, most importantly, is a birational invariant.

To define the genus of a curve would lead us too far for this short course. We can give a number of indications. Let C be an absolutely irreducible curve of degree d. Suppose it has singular points $S_1, \ldots, S_k$. To any singular point we assign a certain quantity δ which depends on the complexity of the singularity. If the singularity is an ordinary n-fold node we have $\delta = n(n-1)/2$. For a cusp we take $\delta = 1$. In general $\delta \geq \nu_P(C)(\nu_P(C)-1)/2$ where $\nu_P(C)$ is the multiplicity of the singularity. The genus of the curve C is defined by

$$g(C) = \frac{(d-1)(d-2)}{2} - \sum_{i=1}^{k} \delta_i$$

where δ_i corresponds to the singularity S_i. We mention the following theorems.

Theorem 7.1 *Let C be an absolutely irreducible curve of degree d with singular points $S_1, \ldots, S_k$ with multiplicities $\nu_1, \ldots, \nu_k$. Then*

$$(d-1)(d-2) - \sum_{i=1}^{k} \nu_i(\nu_i - 1) \geq 0.$$

Moreover, if we have equality, then C is a rational curve.

Theorem 7.2 *Suppose we have two absolutely irreducible curves C, D and a non-constant rational map $\psi : C \to D$ then $g(D) \leq g(C)$. In particular the genus of a curve is a birational invariant.*

We now list algebraic curves according to their degree d and make some comments on their genus.
The case $d = 1$. This is a straight line, no singularities and by our definition we have $g = 0$. For every curve C that can be parametrised rationally we have $g(C) \leq 0$, hence $g(C) = 0$.
The case $d = 2$. When there is no singularity the genus definition gives us $g(C) = 0$. This corresponds to the fact that conics can be parametrised rationally.
The case $d = 3$. Without singularities we have $g(C) = 1$. So we see immediately that nonsingular cubic curves cannot be parametrised rationally. Suppose we have a double point or cusp, then $g(C) = 0$ and we do have a rational parametrisation.

The case $d = 4$. In general, when there is no singularity, the genus is 3. In case the curve has a double point or cusp we get $g(C) = 2$. Since the genus of a non-singular degree d curve equals $(d-1)(d-2)/2$ we see that a non-singular plane curve can never have genus 2. So plane genus 2 curves always have singular points.
Only for very special values of g there exist plane non-singular curves of genus g. For the study of algebraic curves we can assume however that the singularities are only double points on the basis of the following theorem.

Theorem 7.3 *Any plane absolutely irreducible curve is birationally equivalent (over* $\overline{k}$*) to a plane curve having only double points.*

If one really wants to have non-singular curves that are birationally equivalent to a plane curve we should consider models in higher dimensional spaces which are obtained by blowing up the singular points.

8 Problems

1. Suppose we are given 5 distinct points $P_1, \ldots, P_5$ in the plane, not all on a line.

   (a) Show that there is a curve C of degree 2 (conic) which passes through them (hint: how many coefficients does an arbitrary quadratic polynomial have?).

   (b) Suppose that three of the points P_i lie on the straight line L. Show that L is a component of C.

   (c) It turns out that if we make the assumption that no 4 of the points P_i lie on a straight line, the conic C we found is unique. We prove this in the following manner. Suppose we have two different conics passing through the P_i. Suppose they are given by $F(x, y) = 0$ and $G(x, y) = 0$. For every choice of λ, ν the curve $C_{\lambda,\nu} : \lambda F + \nu G = 0$ passes through the P_i. Show this.

   (d) Now choose a point A on the line through P_1, P_2 and choose λ, ν not both zero such that $C_{\lambda,\nu}$ passes through A. Show that $C_{\lambda,\nu}$ is reducible and show that there are three points among the P_i that lie on a line.

(e) Show that $F = 0$ and $G = 0$ represent the same curve, contradicting our assumption that they are different.

2. Suppose we are given 9 disctinct points $P_1, \ldots, P_9$ in the plane, not all on a line or conic.

   (a) Show that there is a cubic curve C passing through these points.

   (b) Can you think of a situation where C is not uniquely determined?

   (c) Suppose that no 7 of the points P_i lie on a conic and no 3 of them lie on a straight line. Show that the curve C is irreducible.

3. In this problem we prove the so-called *nine point theorem*:

   Let C_1, C_2 be two cubic curves intersecting in precisely 9 distinct points $P_1, \ldots, P_9$. Then every cubic curve C passing through 8 of these points also passes through the ninth

   Let us suppose that C contains the points $P_1, \ldots, P_8$. In the following steps we show that P_9 also lies on C. First we make some preparations.

   (a) Suppose a cubic curve D contains four points that lies on a straight line L. Show that L is a component of D.

   (b) Suppose a cubic curve D contains 7 points which also lie on an irreducible conic Q. Then Q is a component of D.

   (c) Using the above two parts show that of the points $P_1, \ldots, P_9$ no 4 can lie on a straight line and no 7 points on a conic.

   (d) We now prove our theorem. Suppose C_1, C_2, C are given by the equations $F_1 = 0, F_2 = 0, F = 0$ respectively. Since C_1, C_2 intersect in exactly nine points, the polynomials F_1, F_2 are linearly independent over the constant. Our proof consists in showing that F depends linearly on F_1, F_2, hence $F = \alpha F_1 + \beta F_2$. As a result we see that F also vanishes in P_9, i.e. P_9 lies on C.

   We now assume that F_1, F_2, F are linearly independent over the constants and arrive at a contradiction. For any λ, μ, ν, not all zero, we consider the cubic curve $C(\lambda, \mu, \nu) : \lambda F_1 + \mu F_2 + \nu F = 0$. Show that every curve $C(\lambda, \mu, \nu)$ contains the points $P_1, \ldots, P_8$. We distinguish the following cases:

i. Three of the points $P_1, \ldots, P_8$ lie on a straight line L. Let us assume the points are P_1, P_2, P_3. Let Q be the unique conic through the remaining five points $P_4, \ldots, P_8$. Choose a point A on the line L and a point B not on L and not on Q. Determine λ, μ, ν, not all zero such that $C(\lambda, \mu, \nu)$ contains both A and B. Show that this curve is the union of L and Q and derive a contradiction.

ii. Six of the points $P_1, \ldots, P_8$ lie on a conic Q. Let us assume the points are $P_1, \ldots, P_6$. Let L be the line through the remaining points P_7, P_8. Show how we can again arrive at a contradiction.

iii. Of the points $P_1, \ldots, P_8$ no three lie on a line and no six lie on a conic. Choose two points A, B on the line through P_1, P_2 and construct a cubic curve $C(\lambda, \mu, \nu)$ which passes through A, B. Again derive a contradiction.

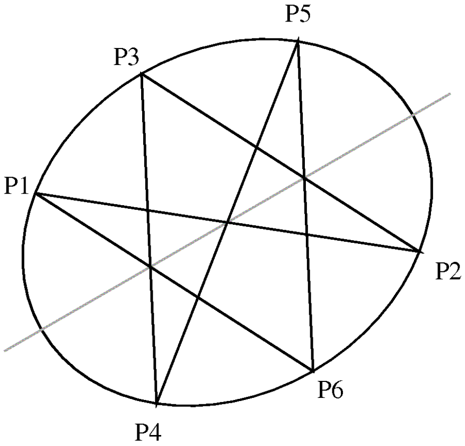
4. The nine point theorem can be used to prove *Pascal's theorem.* Roughly speaking it says the following.

   Consider a hexagon whose vertices all lie on a conic. Then the three intersection points of the three pairs of opposite sides lie on a straight line.

   A more precise formulation is the following one.

   Let Q be a conic and let $P_1, \ldots, P_6$ be 6 distinct points on the conic. Let R_1 be the intersection of P_1P_2 and P_4P_5, R_2 the intersection of P_2P_3 and P_5P_6 and R_3 the intersection of P_3P_4 and P_6P_1. Then R_1, R_2, R_3 lie on one line.

   Here is a picture of a sample situation.



We use the nine point theorem in the notation of the previous problem. For C_1 we choose the union of the lines P_1P_2, P_3P_4, P_5P_6, for C_2 we take the union of P_2P_3,P_4P_5,P_6P_1 and for C we take the union of Q and the line through R_1R_2. Now prove Pascal's theorem.

5. Let d be a positive integer. Suppose we are given $d(d+3)/2$ distinct points in the plane. Show that there is at least one algebraic curve of degree $\leq d$ passing through these points.

6. Let C be an irreducible curve of degree d. Let S be a set of d^2+1 distinct points on C. Show that C is the only curve of degree d passing through these points. This shows that an algebraic curve is determined by its points if there are enough of them.

7. Consider the projective algebraic curves $z^2y = x^3$ and $z^2y - x^3 + y^3 = 0$. They are both non-singular curves. Show that they have only one point of intersection. What is the intersection multiplicity at that point?

8. Find the intersection points of the following pairs of projective curves.

   (a)
$$\begin{aligned} x(y^2 - xz)^2 - y^5 &= 0 \\ y^4 + y^3z - x^2z^2 &= 0 \end{aligned}$$

   (b)
$$\begin{aligned} x^3 - y^3 - 3xyz &= 0 \\ 2x^3 - 4x^2y - 3xy^2 - y^3 - 2x^2z &= 0 \end{aligned}$$

(c)

$$\begin{aligned} x^4 + y^4 - y^2z^2 &= 0 \\ x^4 + y^4 - 2y^3z - 2x^2yz - xy^2z + y^2z^2 &= \end{aligned}$$

9. Find the singular points of the following projective curves.

   (a) $xz^2 - y^3 + xy^2 = 0$

   (b) $(x + y + z)^3 - 27xyz = 0$

   (c) $x^2y^2 + 36xz^2 + 24yz^3 + 108z^4 = 0$

10. For which values of λ is the projective curve

    $$x^3 + y^3 + z^3 - \lambda xyz = 0$$

    non-singular?

11. We can use the calculation of singular points to decide if an algebraic curve is irreducible. Suppose C is a reducible projective curve consisting of two distinct irreducible components C_1, C_2.

    (a) Show that any intersection point of C_1, C_2 is a singular point of C. In particular, if we have simple intersection (multiplicity 1) at a point P, show that P is a double point of C.

    (b) Suppose that the degree of C is equal to $d \geq 2$ and suppose that in all points of $C_1 \cap C_2$ we have simple ($\nu = 1$) intersection. Show that the number of singular points of C is at least $d - 1$.

    (c) Determine the singular points of the curve D given by

    $$x^2y^2 + yz^3 - 4x^2z^2 + z^4 = 0$$

    and determine their nature. Conclude that D is irreducible.

12. Suppose we have a birational map from the line to a curve C given by

    $$t \mapsto R(t)/T(t), S(t)/T(t)$$

    where $R(t), S(t), T(t) \in k[t]$ are polynomials with $\gcd(R, S, T) = 1$, not all constant and their maximum degree is d. Show that the degree of the resulting curve is also d.

13. Show that any projective straight line defined over $\mathbb{Z}/p\mathbb{Z}$ contains precisely $p+1$ points with coordinates in $\mathbb{Z}/p\mathbb{Z}$.

14. Let p be a prime and a an integer not divisible by p. Consider the projective conic $C_a : x^2 + y^2 = az^2$ modulo p.

    (a) Let $a = 1$. Show that there are precisely $p+1$ points modulo p on C_1. (Hint: use chord method).

    (b) Let a be arbitrary. Show that there is at least one point on C_a with coordinates in $\mathbb{Z}/p\mathbb{Z}$. (Hint: how many distinct values are there for $x^2(\text{mod } p)$, and for $a - y^2(\text{mod } p)$?)

    (c) Show that there are precisely $p+1$ points on C_a.

15. How many points does $\mathbb{P}^2(\mathbb{Z}/p\mathbb{Z})$ contain?

16. Count the number of solutions of $y^2 \equiv x^3 - x(\text{mod } p)$ for $p = 3, 5, 7, 11, 13$ and verify if the Hasse inequality is satisfied. Can you explain the answer when $p \equiv -1(\text{mod } 4)$? (we are given that -1 is not a square modulo p if $p \equiv -1(\text{mod } 4)$).

17. Use the chord method to determine all rational points on the curve $x^2 - 3xy + 3y^2 - x - y = 0$.

18. Consider $y^2 = x^3 + 17$ in the unknowns $x, y \in \mathbb{Q}$. The solutions $P = (-1, 4)$ and $Q = (-2, 3)$ are given.

    (a) Check for all integers x with $|x| < 10$ if there exists $y \in \mathbb{Z}$ such that $y^2 = x^3 + 17$.

    (b) Draw the line through P, Q and intersect with $y^2 = x^3 + 17$. Determine the third point of intersection R.

    (c) Change the sign of the y-coordinate of R and repeat the construction with the new point and Q.

    (d) Determine the third point of intersection of the tangent in Q with $y^2 = x^3 + 17$. Do the same with P.

19. Here we describe a construction due to Fermat to construct rational points on curves of the for $y^2 = x^4 + A$. Given two points (x_1, y_1) and (x_2, y_2) construct a parabola $y = x^2 + \alpha x + \beta$ passing through these points. Then intersect it with $y^2 = x^4 + A$.

Apply the method to $y^2 = x^4 + 9$ and the points $(0, 3), (2, -5)$.

Construct a new rational point by choosing the parabola tangent to $y^2 = x^4 + 9$ in $(2, 5)$.