1. Del

Elliptic curves — Basics

Version 1.0 — last update: 10/20/14 9:54:28 AM
This is hopefully the final version. I have corrected a lot of errors, mostly misprints but also a few mathematical ones (in the formulas for the addition on curves on general Weierstrass form) and added some examples, some exercises and some figures.

There are several ways to start this story. We skip the historical background (which is in self very interesting) and jump directly to the definition of the main object of our studies in this first part of this course, namely the *elliptic curves*.

The elliptic curves live over fields, so we let k denote a field. We do *not* assume it to algebraically closed. The most popular field will be the field $\mathbb{Q}$ of rational numbers; indeed elliptic curves over $\mathbb{Q}$ are the center of our interest. Other frequently used fields are the finite fields $\mathbb{F}_q$ with $q = p^n$ elements (the letter p will without exceptions denote a prime number) and the p-adic complete fields $\mathbb{Q}_p$. And not to forget our old acquaintances the reals $\mathbb{R}$ and the complex numbers $\mathbb{C}$. We shall need an algebraically closed field Ω that contains k, any will do, but a natural choice is the algebraic closure of k. Some times, *e.g.,* if $k = \mathbb{Q}$, it is convenient to use a bigger field, *e.g.,* $\mathbb{C}$ in stead of the field $\overline{\mathbb{Q}}$ of algebraic numbers.

The projective plane A few words about the projective plane $\mathbb{P}^2$. In contemporary algebraic geometry the projective plane is a scheme over $\mathbb{Z}$ representing a certain functor, but we shall follow a much more modest approach. The points in $\mathbb{P}^2(\Omega)$ are the lines through the origin in the vector space Ω^3.

The coordinates of any point on a line L, but different from the origin, are called *homogenous coordinates* of the point in $\mathbb{P}^2(\Omega)$ corresponding to L, and we shall write homogenous coordinates as $(x; y; z)$. They are of course not unique—there are many points on a line—but two sets of coordinates representing the same point are related by a homotethy; one is a multiple of the other by a non-zero scalar. Thus $(x; y; z) =$

$(x';y;z')$ if and only if $x' = cx$, $y' = cy$ and $z' = cz$ for some non-zero $c \in \Omega$. The triple $(0;0;0)$ is forbidden; at least one of the coordinates of a point in $\mathbb{P}^2$ must be non-zero.

If $z \neq 0$, one may normalize the homogenous coordinate since $(x;y;z) = (x/z;y/z;1)$. Renaming x/z and y/z as x and y, the points where $z \neq 0$ are identified with points (x,y) in Ω^2. This subset is called the *affine piece where $z \neq 0$* , and when we use coordinate (x,y) we alway work in that affine piece.

Of course one can do the same with any of the coordinates, and for that matter with any linear functional $l(x,y,z)$, and thus obtain different affine pieces.

A point $P \in \mathbb{P}^2(\Omega)$ is said to be *rational over k* if homogenous coordinates may be chosen from k, that is $P = (x;y;z)$ with $x,y,z \in k$. For example, the point $P = (i;i;i)$ is rational over $\mathbb{Q}$ since scaling by i gives $P = (1;1;1)$. The points over k will be denoted by $\mathbb{P}^2(k)$.

A curve E in $\mathbb{P}^2(\Omega)$ is given by a *homogenous* equation $f(x,y,z) = 0$—this is a meaningful since $f(cx,cy,cz) = c^d f(x,y,z)$, and hence the condition $f(x,y,z) = 0$ does not depend on the choice of homogenous coordinates of a point. The integer d is called the *degree* of the curve. It may happen that the coefficients of $f(x,y,z)$, after a suitable rescaling, all lie in k. We then say that *E is defined over k* or that *E is a curve in $\mathbb{P}^2(k)$*. The last notion is slightly misleading since it may very well happen that no points in $\mathbb{P}^2(k)$ satisfy the equation $f(x,y,z) = 0$, like *e.g.,* $x^2 + y^2 + z^2 = 0$ which is defined over $\mathbb{R}$, but has no points in $\mathbb{P}^2(\mathbb{R})$.

There are higher dimensional analogs $\mathbb{P}^n$ of $\mathbb{P}^2$ where n is any natural number (this includes $\mathbb{P}^1$, which one would not call a higher dimensional analog!). They are the spaces of lines through the origin in the vector space Ω^{n+1}. Homogenous coordinates of a point L is just the coordinates of any point of the corresponding line different from the origin. The homogenous coordinates are denote as $(x_0;\ldots;x_n)$ and they are only unique up to a non-vanishing scalar factor.

The definition of an elliptic curve

There are many equivalent characterizations of elliptic curves, and which one to chose as the definition depends on the intentions. In a purely scientific context the language of schemes is the obvious and only choice, but in a pedagogical text a simpler and more down to earth approach is better. Hence, for us, an elliptic curve is defined as follows:

Defenition 1.1 *An elliptic curve E over k is a smooth, cubic curve E in $\mathbb{P}^2(\Omega)$ defined over k together with one of the points of inflexion O which is rational over k.*

Recall that *an inflection point*, or *a flex* for short, is a point P on E such that the tangent to E at P has a contact order that exceeds two. For a cubic curve, which is given by a cubic equation $f(x,y,z) = 0$, this means that the contact order is three, and that P is *the only* intersection point between the curve and the tangent. Indeed, if

$(x(t); y(t); z(t))$ is a linear parametrization[1] of the tangent line with P corresponding to $t = 0$, the polynomial $f(x(t), y(t), z(t))$ is of degree three. It has at most three zeros, and in the case of P being a flex, it has a triple zero at the origin.

For example, the curve

$$y^2z = x^3 + axz^2 + bz^3 \tag{1.1}$$

has a flex at the point $(0; 1; 0)$. The line $z = 0$ has triple contact, since putting $z = 0$ reduces the equation to $x^3 = 0$ (the line may be parametrized as $(x; 1; 0)$).

Over an algebraically closed field Ω one may prove that every cubic curve has 9 flexes, but none of them need to be rational over k, it might even happen that the curve has no rational point over k at all. The definition specifically ask for one of flexes being k-rational. In case there are several, we require one to be singled out; the rational inflection point is part of the structure. The same curve E, but equipped with two different inflection points constitutes two different elliptic curves. The current usage is just to call E *a cubic curve* when no flex is specified.

When the flex is located at the point $(0; 1; 0)$, there is a strong historical precedence, and indeed it is very convenient, to work in the affine piece where $z \neq 0$. The equation of the curve in that part of $\mathbb{P}^2$ is $f(x, y, 1) = 0$. For example the equation (1.1) above becomes

$$y^2 = x^3 + ax + b.$$

Doing this, one should always remember that there is *one point* at infinity, the flex $(0; 1; 0)$.

Recall that the curve is *smooth* if the the three partials f_x, f_y and f_z do not have a common zero in $\mathbb{P}^2(\Omega)$.

There are, as we remarked in the beginning, several ways of defining elliptic curves; here are two other ways:

□ a pair (E, O) where E is a complete and smooth curve of of genus one over k, and O is a k-rational point on it.

□ a pair (E, O) where E is a smooth cubic curve i $\mathbb{P}^2(\Omega)$ defined over k, and O is a k-rational point on it.

That these are equivalent to our definition hinges on two facts. Firstly, every smooth and complete curve of genus one which is defined over k and has a k-point, say O, may be embedded in $\mathbb{P}^2(\Omega)$ as a cubic curve defined over k with O being a flex, and secondly, every smooth cubic curve is of genus one.

Equivalent or isomorphic elliptic curves

The first of the alternative approaches in the previous section has the advantage of offering a natural definition of when two elliptic curves are considered to be same,

[1] Strictly speaking, this is a local parametrization valid in an affine piece containing P. To get a global one, one needs two homogenous parameters $(t; u)$.

i.e., when the two elliptic curves (E, O) and (E', O') are *isomorphic*. This is to be the case when there is an isomorphism $\phi\colon E \to E'$ of the two curves defined over k respecting the chosen points, that is one has $\phi(O) = O'$. Among other things, that ϕ is defined over k, implies that it maps k-points to k-points, and therefore induces a map $E(k) \to E'(k)$.

It is important that the map ϕ should be defined over k. It is a frequently occurring phenomenon that two curves non-isomorphic over k become isomorphic over a bigger field, *e.g.,* the algebraic closure Ω of k. For example, the real quadric curves $x^2+y^2 = 4$ and $x^2 + y^2 = -4$ are certainly not isomorphic as curves over $\mathbb{R}$, one being a circle and the other without real points, but they are isomorphic over $\mathbb{C}$ (use the map $x \mapsto ix$ and $y \mapsto iy$). In the same way one defines a *morphism*, or a *mapping* for short, between two elliptic curves. One just weakens the requirement that ϕ be an isomorphism; it is merely required to be a regular map. That is, is a regular map $\phi\colon E \to E'$ satisfying $\phi(O) = O'$. Such maps between elliptic curves are usually called *isogenies*.

EXAMPLE 1.1. For example, the two curves with equations

$$y^2 = x^3 + 64x + 64 \quad\text{and}\quad y^2 = x^3 + 4x + 1,$$

both with the flex at $(0; 1; 0)$, are isomorphic over $\mathbb{Q}$. Indeed, the map $(x; y; z) \mapsto (2^2x, 2^3y; z)$ leaves $(0; 1; 0)$ untouched, and it takes the equation $y^2 = x^3 + 64x + 64$ into

$$2^6y^3 = 2^6x^3 + 64 \cdot 4x + 64.$$

Remembering that $2^6 = 64$, we cancel 64 throughout and get $y^2 = x^3 + 4x + 1$. ❋

EXAMPLE 1.2. The isomorphism in the previous example is one instance of a general contstruction. Two curves whose equations are

$$y^2 = x^3 + ax + b \text{ and } y^2 = x^3 + ac^{-4}x + bc^{-6}$$

where $a, b, c \in k$ and $c \neq 0$ are isomorphic, one easily checks that the map $(x; y; z) \mapsto (c^2x; c^3y; z)$ does the job. ❋

PROBLEM 1.1. Show that the $y^2 = x^3+1/9x+1/27$ is isomorphic to $y^2 = x^3+9x+27$. HINT: Scale x and y appropriately. ✷

Weierstrass normal form

By a clever choice of coordinates on $\mathbb{P}^2(k)$ one may simplify the equation of a cubic curve and bring it on a standard form. There are of course several standard forms around, their usefulness depends on what one wants to do, but the most prominent one is the one called the *Weierstrass normal form*. This is also the one most frequently used in the arithmetic studies. In the case the characteristic of k is not equal to 2 or 3, it is particularly simple.

The name refers to the differential equation

$$\wp' = 4\wp^3 - g_2\wp - g_3$$

discovered by Weierstrass, and one of whose solution—the famous Weierstrass $\wp$-function—was used by him to parametrize complex elliptic curves. It seems that the norwegian mathematician Trygve Nagell was the first[2] to show that genus one curves over $\mathbb{Q}$ with a given $\mathbb{Q}$-rational point O, can be embedded in $\mathbb{P}^2$ with the point O as a flex.

The idea behind the Weierstrass normal form is to place the specified inflection point of the curve at infinity, at the point $(0;1;0)$, and chose the z-coordinate in a manner that $z = 0$ is the inflectionally tangent.

Proposition 1.1 *Assume that E is as smooth, cubic curve defined over k with a flex at $P = (0;1;0)$. Then then there is linear change of coordinates with entries in k, such that E has the affine equation*

$$y^2 + a_1xy + a_3 = g(x) \tag{WW}$$

where a_1 and a_3 are elements in k, and $g(x)$ is a monic, cubic polynomial with coefficients in k.

There is a standard notation for the coefficients of the polynomial $g(x)$, which goes like this:

$$y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6 \tag{WWb}$$

There is a very good reason for the particular choice of the numbering the coefficients which will become clear later on (see example 1.1 on page 4).

PROOF: First we choose coordinates on $\mathbb{P}^2$ such that the point $P = (0;1;0)$ is the flex and such that the tangent to E at P is the line $z = 0$. That the curve passes through $(0;1;0)$ amounts to there being no term y^3 in the equation $f(x,y,z)$, and that $z = 0$ is the inflectionally tangent amounts to there being no terms y^2x or yx^2. Indeed, in affine coordinates round P the dehomogenized polynomial defining E—that is $f(x,1,z)$—has the form

$$f(x,1,z) = z + q_2(x,z) + q_3(x,z),$$

where the $q_i(x,z)$'s are homogenous polynomials of degree i, and where the coefficient of the z-term has been absorbed in the z-coordinate. Now we exploit that $z = 0$ is the inflectionally tangent. Putting $z = 0$, we get

$$f(x,1,0) = q_2(x,0) + q_3(x,0),$$

[2] This is what J. W.S. Cassels writes in his obituary of Nagell.

and $f(x,1,0)$ has a triple root at the origin so $q_2(x,0)$ must vanish identically. Hence

$$f(x,1,z) = z + a_1xz + a_3z^2 + q_3(x,z)$$

with $a_1, a_3 \in k$. The homogeneous equation of the curve is thus

$$y^2z + a_1xyz + a_3yz^2 = G(x,z) \tag{1.2}$$

where $G(x,z) = -q_3(x,z)$. Write $G(x,z)$ as $G(x,z) = \gamma x^3 + zr(x,z)$ where $r(x,z)$ is homogenous of degree two. Since the curve is irreducible, we have $\gamma \neq 0$ and may change the coordinate z to γz. By cancelling γ throughout the equation, we see that we can take $\gamma = 1$, and then $g(x) = G(x,1)$ will be a monic polynomial. ❏

With some restrictions on the characteristic of k the equation can be further simplified. If the characteristic is different from two, one may complete the square on left the side of 1.2, that is, replace y by $y - a_1x/2 - a_2z/2$. This transforms (1.2) into an equation of the form

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

where G is a homogenous polynomial of degree three (different from the G above), and after a scaling of the z-coordinate similar to the one above it will be monic in x.

In case the characteristic is not equal to three there is a standard trick to eliminate the quadratic term of a cubic polynomial. One replaces x by $x - \alpha/3$ where α is the sum of the three roots of $g(x)$, that is the negative of the coefficient of x^2. We therefore have

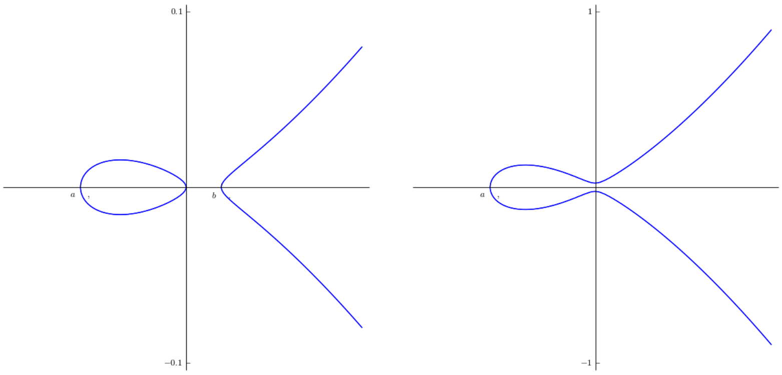
Proposition 1.2 *Assume that k is a field whose characteristic is not 2 or 3. If E is a smooth, cubic curve defined over k having a k-rational inflection point, then there is linear change of coordinates with entries in k, such that the affine equation becomes*

$$y^2 = x^3 + ax + b \tag{W}$$

where $a, b \in k$.

Sometimes the coefficients a and b are denoted by a_4 and a_6 respectively. The equation shows that a point (x,y) lies on the curve if and only if $(x,-y)$ lies there. Hence there is a regular map $\iota\colon E \to E$ with $\iota(x,y) = (x,-y)$. It is called *the canonical involution of E*. (It is common usage to call maps whose square is the identity for involutions).

The real case Over the reals the elliptic curves may topologically be divided into two classes according to the real cubic polynomial $g(x)$ having one or three real roots. In former case the set of real points $E(\mathbb{R})$ is connected and homeomorphic to the circle $\mathbb{S}^1$ in the strong topology (*i.e.*, the one inherited from $\mathbb{R}^2$) and in the latter is is homeomorphic to the disjoint union of two circles. We underline that this is a topological division, many non-isomorphic curves have homeomorphic sets of real points. Real curves may be depicted, and here follow two pictures, one from each of the two classes. We remind you that only the affine piece where $z \neq 0$ is drawn, so there is a point at infinity making circles out of the infinite branches.



Curves with $E(\mathbb{R})$ having one and two components.

Curves on extended Weierstrass form The extended Weierstrass form WWb is not only useful in characteristic two. Many curves have a simpler equation on that form than on the simple Weierstrass form; for example $y^2 - y = x^3 - x$ has the simple Weierstrass equation $y^2 = x^3 - 16x + 16$; and there are cases where the general form serves a special purpose.

Departing from a Weierstrass equation (WWb) and completing the square on the left side of the equation, one arrives at an equation on the form

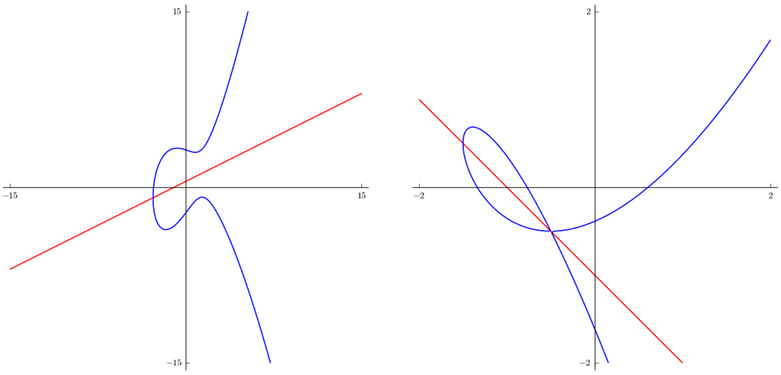
$$\big(y + (a_1 x + a_3)/2\big)^2 = g_1(x)$$

where $g_1(x)$ is monic cubic polynomial.

It thus appears that the line $y = -(a_1x + a_3)/2$ is a line of symmetry for the curve—in the sense that (x, y) lies on E if and only if $\big(x, -y - (a_1x + a_3)\big)$ does. The canonical involution ι is in this case given by

$$(x, y) \mapsto \big(x, -y - (a_1x + a_3)\big). \tag{1.3}$$

Below we show pictures of two such curves, one non-singular and one with a node; the node is forced to lie on the symmetry line being the sole singularity. The symmetry is not an orthogonal symmetry about the line, so the curves appear somehow skew.



Curves with line of symmetry other than the x-axis

PROBLEM 1.2. *(Legendre's normal form).* Assume that k is algebraically closed of characteristic not equal to 2. Show that the equation of any elliptic curve over k can be brought on the form

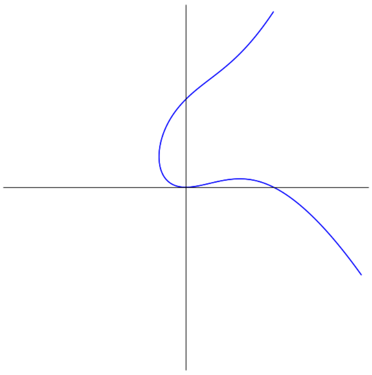
$$y^2 = x(x-1)(x-\lambda)$$

where $\lambda \in k$ and $\lambda \neq 0, 1$. HINT: Start with a Weierstrass normal form $y^2 = g(x)$. Translate the x-coordinate to make one of the roots of $g(x)$ equal to zero, then scale x to make another root equal to 1. ✷

PROBLEM 1.3. *(Tate's normal form).* Show that the equation of any elliptic curve may be brought on the form

$$y^2 + sxy - tx = x^3 - tx.$$

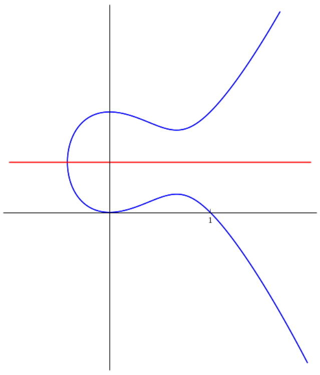
Show that origin $(0,0)$ lies on E and that the tangent to E at the origin is the x-axis. Show that the origin is *not* a flex; that is, the tangent has contact order 2. ✷



The curve $y^2 - xy - y = x^3 - x^2$ on Tate's normal form.
The x-axis is tangent at he origin, but the origin is not a flex.

PROBLEM 1.4. Let E be the curve $y^2 - y = x^3 - x^2$. This is a very famous curve with the denotation $Y_0(11)$ in the nomenclatur of the so called *modular curves*. The exercise is to bring it on simple Weierstrass form. Which one of the two equations is simplest? List five points in $E(\mathbb{Q})$. ✷

PROBLEM 1.5. Show that the symmetry line of a curve on general Weierstrass form but with $a_1 = 0$ is the horisontalline $y = -a_1/2$. ✷



The curve $y^2 - y = x^3 - x^2$ with a horisontal symmetry line.

Problem 1.6. Show that the Weierstrass equation of $x^3 + y^3 = \alpha$ is $y^2 = x^3 - 432\alpha^2$. ✸

Singularities and the discriminant

It is fundamental to be able to decide whether a curve given by an equation on Weierstrass form is non-singular or not, and the discriminant is an efficient tool in that respect. It is an element Δ in the field k one associates to the elliptic curve, or rather to its Weierstrass equation, that vanishes if and only if the curve is singular. The discriminant is easily computable, just given as a polynomial (although rather complicated) in the coefficients of the Weierstrass equation.

We start with the simplest case when k is not of characteristic 2 or 3, and assume that the equation is on the simple Weierstrass form given by (W). First of all, the point $P = (0; 1; 0)$ is never a singular point, and this holds whether the Weierstrass equation is simple or not. Indeed, the affine equation of the curve round that point P is obtained by putting $y = 1$ in (WW), which gives en equation of the type

$$z + q_2(x, z) + q_3(x, z) = 0,$$

where each q_i is homogeneous of degree i in x and z. Since there is always the non-zero linear term z, the points P at infinity is not a singular point on E.

For the other points of E, where $z \neq 0$, we compute the two partial derivatives of $f(x, y, 1) = y^2 - x^3 - ax - b$. They are

$$f_y = 2y \qquad f_x = g'(x) = -3x^2 - a.$$

One sees immediately that f_y never vanishes off the x-axis (in characteristic different than two). Hence the curve E is singular precisely at points where $a = -3x^2$ and $x^3 + ax + b = 0$. From this one derives that $x^3 = b/2$, and hence $(b/2)^2 = -(a/3)^3$; or in other words $27b^2 + 4a^3 = 0$.

The expression $\Delta = 27b^2 + 4a^3$ is called *the discriminant*. It is a fundamental invariant of the curve, or rather an invariant of *the equation* of E on should say. If one performs the changes $x \mapsto c^2x$ and $y \mapsto c^3y$, as in example 1.2, the coefficients of the new equation for E become $a_4' = c^{-4}a_4$ and $a_6' = c^{-6}a_6$. This shows that the discriminant transforms as $\Delta' = c^{-12}\Delta$.

There are several normalizations around, and for serious, but so far for us mysterious grounds, the expression $-16(27b^2+4a^3)$ is the most natural choice, and it is this number that is *the discriminant*.

The discriminant of a polynomial.

There is also the notation of the discriminant of a polynomial in one variable. It measures if the polynomial has double roots or not. In the case of a polynomial $g(x)$ of degree d over an algebraically closed field Ω it is given as

$$\Delta(g) = \prod_{i \leq j}(e_i - e_j)^2$$

where e_i's are the d roots of $g(x)$ in Ω (possibly with repetitions). This is a simple way of getting an expression that vanishes if and only if $g(x)$ has a double root, and the main point is that $D(g)$ can expressed polynomial in terms of *the coefficients* of g. No solution of equations is therefore needed in its calculation, and as important, if E is defined over a field k, then it has an equation with $\Delta \in k$.

In principle this follows from Newton's result that any symmetric function in the roots e_i's (and the discriminant is one, due to the squares) is a polynomial in the *elementary symmetric functions* of the e_i's, and those elementary symmetric functions of the roots are exactly the coefficients of $g(x)$. In practise however, the expression becomes horribly long and complicated but in a few cases. If the degree is two, the discriminant of $g(x) = x^2 + ax + b$ is the good old $a^2 - 4b$, and if $g(x) = x^3 + ax + b$ one has $\Delta(g) = -27b^2 - 4a^3$.

With this we have another explanation of the coupling between the discriminant and the singularities of E. Since $f_y = 2y = 2g(x)$, a point (x_0, y_0) can be a singularity only if $y_0 = 0$ and x_0 is one of the roots of $g(x)$. Now $f_x = g'(x)$, which vanishes at x_0 if and only if x_0 is a double root of $g(x)$.

Problem 1.7. Show by calculation that the discriminant of $g(x) = x^3 + ax$ is $-4a^3$ and that of $g(x) = x^3 + b$ is $-27b^2$. ✷

Problem 1.8. Show that the discriminant of $g(x) = x^3 + ax^2 + bx$ equals $b^2(a^2 - 4b)$. ✷

Problem 1.9. Every polynomial $g(x)$ has a discriminant, which may be expressed as a linear combination of $g(x)$ and $g'(x)$ with coefficients from $k[x]$. Show, by brute force, that with $g(x) = x^3 + ax + b$ and $\Delta = 27b^2 + 4a^3$ one has

$$\Delta = -27(x^3 + ax - b)g(x) + (3x^2 + 4a)g'(x)^2.$$

✷

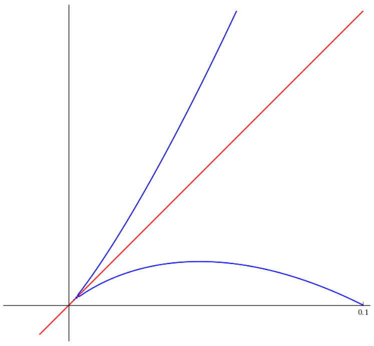
The types of singularities

In case the discriminant of a curve E vanishes the curve is singular. The singularity is either a cusp, which is a singularity with just one branch, or a node. A node is simple double point, and over an algebraically closed field it has two distinct tangent, while over a general field the two tangents may split or not. A cusp is often called an additive singularity and a node a multiplicative one that can be split or not. All together, there are three possible scenarios, which we proceed to describe. For simplicity, we work only with curves on simple Weierstrass form.

So we assume that $\Delta = 27b^2 + 4a^3 = 0$. Then $(b/2)^2 = -(a/3)^3$, and putting $x_0 = -(3/2)ba^{-1}$ if $a \neq 0$ and $x_0 = 0$ in case $a = 0$, one has $-3x_0^2 = a$ and $2x_0^3 = b$. This gives immediately the factorization

$$x^3 + ax + b = (x + 2x_0)(x - x_0)^2. \tag{✘}$$

□ The cuscpidal case In this case $x_0 = 0$, and the polynomial $g(x)$ has a triple zero at the orgin. The curve is given by $y^2 = x^3$, and the singularity is a *cusp* located at the origin. The curve E has just one tangent line there, the x-axis. Of course curves not on simple Weierstrass form can have other cusp tangents and their cusp need not be located at the origin.



The curve $y^2 - 2xy = 10x^3 - x^2$ with cusp tangent $y = x$.

□ The nodal case This is the case when $x_0 \neq 0$. As we shall see, there are two subcases. The polynomial $g(x)$ has a double zero at x_0, and the singularity is a *node*. Over the algebraically closed field Ω, the curve has two distinct tangent lines $y = \pm\sqrt{3x_0}(x - x_0)$ at the singular point; indeed, this is seen by writing the equation as

$$y^2 = 3x_0(x - x_0)^2 + (x - x_0)^3.$$

If E is defined over a smaller field k either $3x_0$ has a square root in k or it has not. In the former case the two nodal tangents to E are both defined over k, and we say the node is *a split node*. In the latter, they are not, and the node is called *non-split*. These two notions are of course relative to the ground field k; for example, a non-split node becomes split over the quadratic extension $k(\sqrt{3x_0})$. We have established the following proposition

Proposition 1.3 *Assume k is a field whose characteristic is different from 2 and 3. Assume that the cubic curve E is given by the Weierstrass equation*

$$y^2 = x^3 + ax + b$$

with $a, b \in k$.

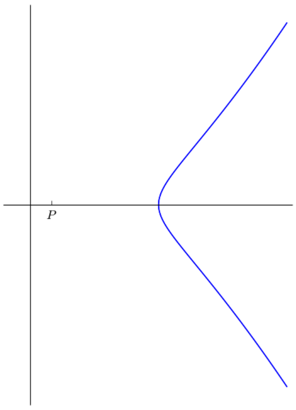
- □ *The curve is non-singular if and only if the discriminant $\Delta = 27b^2 + 4a^3$ is non-zero.*
- □ *If $\Delta = 0$ and $a \neq 0$, then for $x_0 = -(3/2)ba^{-1}$, the curve E has a node at the point $(x_0, 0)$ as its only singular point, the nodal tangents being $y = \pm\sqrt{3x_0}(x - x_0)$. If $\sqrt{3x_0} \in k$, the node is split, and the two tangent are defined over k. Otherwise it is non-split, and the tangents are defined over $k(\sqrt{3x_0})$.*
- □ *If $\Delta = 0$ and $a = 0$, the equation is reduced to $y^2 = x^3$ and the curve has a cusp at the origin as the only singular point.*

The first remark, is that a curve on Weierstrass normal form alwyas is *irreducible*, a reducible cubic has either a triple point or at least two double points. The second remark concerns curves in characteristic two. A curve E on simple Weierstrass normal form W can never be smooth in characteristic two. Indeed, the partial f_y vanishes identically in that case, so the point with x-coordinate $\sqrt{a}$ (there is only one since the characteristic of k is two) will be singular. This is one good reason for including the factor -16 in the discriminant (but not the fourth power).

Example 1.3. It is instructive to see what can happen over the reals. The curve with equation

$$y^2 = (x - 2)(x - 1)^2$$

has a node at $x_0 = 1$. The tangents are not real, but given by the complex conjugate equations $y = \pm i\sqrt{3}(x - 1)$. The singular point $P = (1, 0)$ is an isolated point of curve; the two branches that pass by it are non-real and do not show up in the real picture.



The curve $y^2 = (x - 6)(x - 1)^2$ with an isolated nodal point at $P = (1, 0)$

❄

For curves on the general Weierstrass form (WWb) there is also a formula for the discriminant, but its awfully long, so we skip it. The interested student can consult *e.g.,* Silverman's book [?] on page 46.

Example 1.4. It is illuminating do to some examples in detail, so let us study the curve $y^2 + y = x^3 - x$, and transform it into a Weierstrass equation of the form (W). We start by completing the square (hence the characteristic is not two) and replace y by $y + 1/2$. The equation then takes the form

$$y^2 = x^3 - x + 1/4.$$

We frequently want equations with integral coefficients, to be able to reduce them modulo primes (which is a good old trick in the world of diophantine equations). Our first equation, can be reduced mod any prime, but the second has no meaning mod 2. To get integral coefficients, we replace y by $2^{-3}y$ and x by $2^{-2}x$ and the equation becomes

$$2^{-6}y^2 = 2^{-6}x^3 - 2^{-2}x + 2^{-2}$$

and after multiplying through by 2^{-6}, we have it on the form

$$y^2 = x^3 - 16x + 16.$$

One computes the discriminant $\Delta = 27b^2 + 4a^3 = 27 \cdot 16^2 + 4 \cdot (-16)^3 = -16^2 \cdot 37$. So in characteristic two, that is over $\mathbb{F}_2$, the curve has a cusp, and if the characteristic is a 37, that is over $\mathbb{F}_{37}$, it has a node at $-3/2 \cdot (16)/(-16) = 3/2 = 20$. The node is non-split over $\mathbb{F}_{37}$ since 15 is not a square i $\mathbb{F}_{37}$.

One remark is that first the equation $y^2 + y = x^3 - x$ defines a smooth curve in characteristic two, indeed $f_y \equiv 1$ and never vanishes! However the last equation gives a curve with a cusp, and the second has not even a meaning. The moral is, things change, and one should give things careful thought. ❄

The group law

It is fundamental that every elliptic curve E over Ω has a group law that makes it into an abelian group. This goes back to Abel and Jacobi— Jacobi was the first to use it systematically in the study of elliptic functions, and it is closely related to Abel's addition theorem.

There is an easy and intuitive geometric way of introducing the group law which hinges on Bezout's theorem; in fact on the very simplest version of Bezout: Any line in $\mathbb{P}^2(\Omega)$ meets E in three points when they are counted with the correct multiplicity.

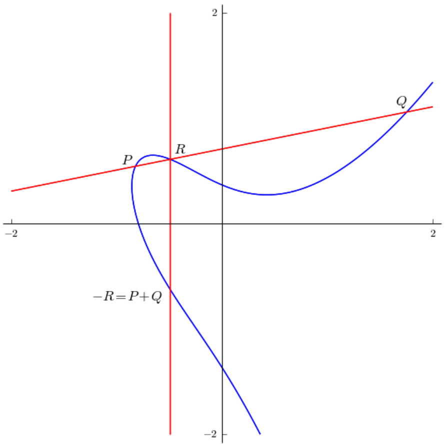
Indeed, if $(x(t,u);x(t,u);z(t,u))$ is a homogenous linear parametrization of the line, the points where it meets E, are the zeros of the homogenous cubic polynomial $g(t,u) = f(x(t,u),y(t,u),z(t,u))$. This polynomial is the product of three linear forms, hence has exactly three zeros (counted with multiplicity) on the line.

To define a group structure one needs an involution—*i.e.,* a map $P \mapsto -P$—and a group law, an associative binary operation on E. It turns out to commutative, and we'll write as $P+Q$.

We start by defining the involution on E.

THE INVOLUTION Take any point $P \in E(\Omega)$ and draw the line from the flex O to P. This line intersects E in a third point which by definition is $-P$. As a consequence, we see that $-O = O$. The flex is the neutral element of the group.

If the curve is on Weierstrass normal form (W), the involution is simply given as $(x;y;z) \mapsto (x;-y;z)$; or in affine coordinates, if $P=(x,y)$, then $-P=(x,-y)$. Indeed, if $P=(x_0,y_0)$, the vertical line through P has equation $x=x_0$, and the intersection points with E other than the flex are $(x_0,\pm y_0)$. If $y_0=0$, these two points coincide and $P=-P$; that is P is a two-torsion point on E.



Addition on the curve $y^2+2xy+y=x^3-1/2$

The general case with Weierstrass equation (WW) requires slightly more work. The intersection between E and the vertical line $x=x_0$ is then given by the equation

$$y^2+a_1x_0y+a_3y=g(x_0).$$

It follows that the y-coordinate of $-P$ satisfies $y_1+y_0=-a_1x_0-a_3$, and the involution operates according to

$$(x,y)\mapsto(x,-y-a_1x-a_3).$$

The points in $\mathbb{P}^2(\Omega)$ not affected by the involution are the points on the line $y = -(a_1x+a_3)/2$, so this line is a symmetry line of the elliptic curve E. It coincides the x-axis when $a_1=a_3=0$.

The group law Let P and Q be two points in $E(\Omega)$. If they are different, they span a line, which by Bezout's theorem intersects E in a third point, and we denote this third point by $l(P,Q)$. If the points are equal, the tangent line of E at P has double contact with E at P, and hence it intersects E in a third point $l(P,P)$. The addition on E is then simply defined by

$$P+Q=-l(P,Q).$$

In short: To add P and Q, draw the line from P to Q (the tangent to E if $P=Q$) and determine the point R where it intersects E. Then reflect R through the symmetry line.

We shall prove the following theorem

Theorem 1.1 *The addition and involution as just defined, give $E(\Omega)$ the structure of a commutative group. The map $E\times E\to E$ sending (P,Q) to $P+Q$ and the one $E\to E$ sending P to $-P$ are both regular maps. If $P,Q\in E(k)$, then $P+Q\in E(k)$ and $-P\in E(k)$, so $E(k)$ is an abelian group.*

Rationality

Our main interest is the rational points of a curve defined over $\mathbb{Q}$, so it is of fundamental importance to see how the group law is related to rationality questions, and luckily, the situation is very satisfactory. If the elliptic curve E is defined over the field k (then the flex by definition is a k-point) and P and Q both are k-rational points of E, then their sum $P+Q$ is rational over k as well.

Finding rational points on a curve, or a variety for that matter, is notoriously difficult, and the group structure of E gives us a nice way of getting new rational points from old ones. There are explicit formulas for the sum, formulas that are not too complicated, so finding new rational points is a matter of computational work.

Proposition 1.4 *Assume that the elliptic curve E is defined over k. Then the set of k-rational points $E(k)$ is a subgroup of $E(\Omega)$.*

Proof: That $P+Q$ is rational is obvious when $Q=-P$ or $P=O$, so we treat only the other cases. The curve E being defined over k, has an equation on the form

$$y^2+a_1xy+a_3y=g(x)$$

where $g(x)$ is a cubic polynomial with coefficients from k.

If the two points P and Q are different and not opposite, the line through them has coefficients in k and is of the form $y=\alpha x+\beta$, where α and β are elements in k. The same applies to the tangent to E at rational point. By implicit derivation, the slope can be found from

$$(2y+a_1x+a_3)y'=g'(x)-a_1y$$

and it is in k (as $2P\neq O$, the point P does not lie on the symmetry-line $2y+\alpha_1x+a_3=0$).

In both cases we find, inserting $y = \alpha + \beta$ in the Weierstrass equation:

$$(\alpha x + \beta)^2 + a_1 x(\alpha x + \beta) + a_3(\alpha x + \beta) = g(x).$$

The sum of the roots of a cubic polynomial being the negative of the coefficient of the quadratic term, the three solutions of this equation—that is the x-coordinates x_1, x_2 and x_3 of P, Q and $P + Q$ — satisfy

$$x_1 + x_2 + x_3 = \alpha^2 + a_1\alpha.$$

Hence if two of them are in k, the third is. And as the y-coordinate y_3 of $P+Q$ satisfies $y_3 = \alpha x_3 + \beta$, one sees that $y_3 \in k$ as well. ❏

Associativity

There is a geometric proof of the associativity of the group law based on the following property of cubic curves in the projective plain. We shall now sketch that proof, assuming the three point from the curve that are the involved, are distinct.

Assume that f and g are two homogeneous cubic polynomials in three variable, defining the curves D and E. Assume that f and g has no common component. According to Bezout's theorem, the two curves intersect in 9 points or they have a common component, which we assume is not the case. We shall use the following lemma:

Lemma 1.1 *If a cubic h passes through eight of the points, it passes through the ninth.*

For a proof see xxx, armed with this result we attack

Proposition 1.5 *The binary operation $P + Q$ on E is associative.*

Proof: Let $L_{P,Q}$ denote the linear form defining the line i $\mathbb{P}^2$ passing through the two points P and Q.

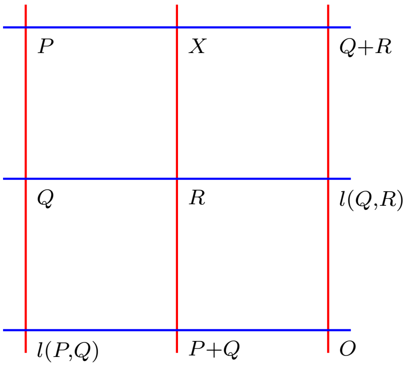
If we pick three points P, Q and R in E, we may consider the two cubics defined by the equations

$$L_{P,Q}L_{P+Q,R}L_{l(Q,R),O} = 0 \tag{1.4}$$

$$L_{Q,R}L_{Q+R,P}L_{l(Q,P),O} = 0 \tag{1.5}$$

Clearly they have the points P, Q, R, $l(Q,P)$,$l(Q,R)$, $Q + P$, $Q + R$ and O in common (check that!). Let X be the ninth intersection point of the two cubics; that is the point common to the two lines $L_{P+Q,R}$ and $L_{Q+R,P}$. Now, the curve E passes through the same eight points, hence it passes through X! From this one sees that $-(P + (Q + R)) = -(R + (P + Q))$, and we are done! ❏

May be you find the diagram (which we have borrowed from Milne, see [?], I. 3 page 28) below enlightening. The three lines whose equations are the linear factors of the cubic in the first line above, that is in (1.4), are drawn vertically and red , and the second triple of lines, those defined by the linear factors in (1.5), are blue and horizontal.



Regularity

The explicit formulas just established, show that the addition map μ, given by $(P,Q) \mapsto P+Q$, is a rational map $E \times E \to E$, that is at least regular at the points (P,Q) when P and Q do not have the same x-coordinate. As a set theoretical map μ is of course well defined everywhere, but we have no formula valid in open sets around pair of points with coinciding x-coordinates showing it to be regular.

To show that μ is regular we use a trick to be found in Silverman (see [?]). In general, if $\phi\colon X \to Y$ is a rational map between smooth varieties and $P \in X$ is a point, then ϕ is regular—or can be extended to a regular map—at P if there is an open neigbourhood $U \subseteq X$ of P and a regular map $\phi'\colon U \to Y$ such that ϕ and ϕ' coincide in the points of U where ϕ is defined.

It is a result that any rational map $\phi\colon X \to Y$ can be extended to a regular map whenever X is a smooth curve and Y is a complete (*e.g.,* projective) variety. The translation maps $\tau_Q\colon E \to E$ are set theoretically defined by $\tau_Q(P) = P + Q$, and by the explicit formula they are regular as long as P and Q have x-coordinates that differ. By what we just said, they extend to a regular maps, which we still denote as $\tau_Q\colon E \to E$.

Now fix two points R_1 and R_2 and introduce two auxiliary points Q_1 and Q_2 chosen such that the x-coordinates of $R_1 + Q_1$ and $R_2 + Q_2$ differ. Clearly

$$P_1 + P_2 = (P_1 + Q_1) + (P_2 - Q_2) + (Q_2 - Q_1),$$

or in terms of maps

$$\mu = \tau_{Q_1 - Q_2} \circ \mu \circ \tau_{Q_1} \times \tau_{Q_2}.$$

If we interpret τ_R as the extended map whichever point R is, the maps on the right side are regular whenever the x-coordinates of $P_1 + Q_1$ and $P_2 + Q_2$ differ; but this certainly holds in a neigbourhood of (R_1, R_2). It follows that μ extends to a regular map on $E \times E$, and by a continuity argument, the extension is given by the formulas we have found (the slope m in the duplication formula is the limit of the slope m in the case x-coordinates differ).

Explicit formulas

There are explicit formulas for the coordinates of the sum $P + Q$ in terms of the coordinates of the two points. They are relatively simple and easy to develop, one just translate the geometric recipe for the sum into equations. We shall treat curves with a general Weierstrass equation WW, the formulas are slightly more involved, and we give the simple versions as special cases. Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $P+Q = (x_3, y_3)$.

The first case when $x_1 \neq x_2$ Assume that $x_1 \neq x_2$. The line connecting P_1 and P_2 is given by $y = m(x - x_1) + y_1$ where $m = (y_2 - y_1)/(x_2 - x_1)$. Substituting this in the Weierstrass equation (WW) for E, we obtain the equation

$$\big(m(x - x_1) + y_1\big)^2 + a_1x\big(m(x - x_1) + y_1\big) + a_3\big((m(x - x_1) + y_1\big) = g(x),$$

where $g(x)$ is a cubic polynomial. The solutions of this equation are x_1, x_2 and x_3. The sum of the roots of a cubic polynomial being the negative of the coefficient of the quadratic term, we find

$$x_1 + x_2 + x_3 = m(m + a_1) - a_2.$$

This gives

$$x_3 = m(m + a_1) - x_1 - x_2 - a_2.$$

Substituting back in the equation for the line, gives in view of the general formula for the involution 1.3 on page 7:

$$y_3 = -m(x_3 - x_1) - y_1 - (a_1x + a_3),$$

We have established

Proposition 1.6 *Let E have the Weierstrass equation (WW) and let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on E. If $P + Q = (x_3, y_3)$ and $x_1 \neq x_2$, one has*

$$x_3 = m(m + a_1) - a_2 - x_1 - x_2 \text{ and } y_3 = -m(x_3 - x_1) - y_1 - (a_1x + a_3),$$

where $m = (y_2 - y_1)/(x_2 - x_1)$.

If the curve is on the simple Weierstrass form, these formulas simplify:

Proposition 1.7 *Let E have a simple Weierstrass equation (W) and let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on E. If $P + Q = (x_3, y_3)$ and $x_1 \neq x_2$, one has*

$$x_3 = m^2 - x_1 - x_2 \text{ and } y_3 = -m(x_3 - x_1) - y_1. \tag{1.6}$$

Problem 1.10. Let E be the curve

$$y^2 = x^3 - 4x + 1$$

and let $P_1 = (2, 1)$, $P_2 = (-2, -1)$ and $P_3 = (-2, 1)$. Compute $P_1 + P_2$ and $P_1 + P_3$. (Answer: (1/4,-1/8)). ✱

The duplication formula Now let $P = (x_1, y_1)$, we give a formula for the coordinates of $2P$—hence the name “duplication formula”. The tangent line of E at P has the equation

$$y = y_1'(x - x_1) + y_1$$

where y_1' is the value of the derivative y' (with respect to x) of y at P. It is computed by implicit derivation of the general Weierstrass equation (WW):

$$(2y + a_1x + a_3)y' = g'(x) - a_1y,$$

The same arguments as in the previous paragraph then gives

Proposition 1.8 (The duplication formula) *Assume that k is not of characteristic two and that the elliptic curve E has the general Weierstrass form (WW). If $P = (x_1, y_1)$ and $2P = (x_2, y_2)$ then*

$$x_2 = \Big(\frac{g'(x_1) - a_1y_1}{2y_1 + a_1x_1 + a_3}\Big)\Big(\frac{g'(x_1) - a_1y_1}{2y_1 + a_1x_1 + a_3} + a_1\Big) - a_2 - 2x_1$$
$$y_2 = -\frac{g'(x_1) - a_1y_1}{2y_1 + a_1x_1 + a_3}(x_2 - x_1) - y_1 - (a_1x + a_3).$$

In case the characteristic of k is two, one of the coefficients a_1 and a_3 must be non-zero, else the curve is not smooth, and the formulas are still valid.

The expressions in the proposition are somehow complicated, but if the curve is on Weierstrass form (W), they simplify considerably:

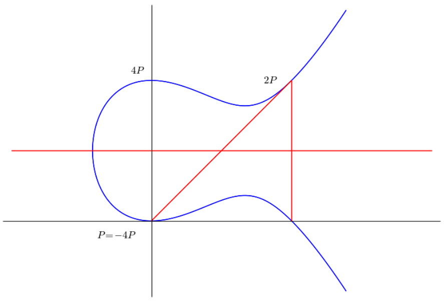
Proposition 1.9 (Duplication—simple form) *Assume that E is an elliptic curve with a simple Weierstrass equation. Let $P = (x_1, y_1)$ and let $2P = (x_2, y_2)$. Then*

$$x_2 = \Big(\frac{g'(x_1)}{2y_1}\Big)^2 - 2x_1 \quad \textit{and} \quad y_2 = -\frac{g'(x_1)}{2y_1}(x_2 - x_1) - y_1. \tag{1.7}$$

Example 1.5. Let us come back to the curve Y with equation $y^2 - y = x^3 - x^2$.

The origin $P = (0, 0)$ lies on Y, and the tangent to Y there is the x-axis. The third intersection point the tangent has with Y is the point $(1, 0)$, and reflected through the symmetry line $y = 1/2$ the point $(1, 0)$ becomes $2P = (1, 1)$.

The derivative y' is found by implicit derivation which gives $2y' - 1 = 3x^2 - 2x^2$. From $x = y = 1$ it follows that $y' = 1$. Hence the tangent to Y at $(1, 1)$ is the line $y = x$, and the third intersection it has with Y is the origin $P = (0, 0)$. It follows that $-4P = P$, and consequently that P is a five torsion point.



The origin $P=(0,0)$ is a five-torsion point on the curve $y^2-y=x^3-x^2$.

❄

Problem 1.11. With the notation from the preceding example, determine $3P$. ✱

Problem 1.12. Let E be an elliptic curve on Tate's normal form, that is $y^2+sxy-ty=x^3-tx^2$, and let $P=(0,0)$.

a) Show that the involution is $(x,y)\mapsto(x,-y-sx+t)$.

b) Show that $-2P=(t,0)$ and that $2P=(t,t(1-s))$. Show that $-3P=(1-s,(1-s)^2)$ and that $3P=(1-s,t-(1-s)^2)$.

✱

Problem 1.13. The equation $y^2-x^3=c$ is often called Bachet's equation or Mordell's equation; let E be the curve it describes. Show that if $P=(x,y)$ is point on E, then $-2P$ is given as

$$-2P=\Big(\frac{x^4-8cx}{4y^2},\frac{-x^6-20cx^3+8c^2}{8y^3}\Big).$$

This formula is called *Bachet's duplication formula* and dates back to 1621. ✱

The two- and the three-torsion points

In any abelian group a *torsion element* is an element of finite order. In our geometric context we call elements of $E(k)$ for points, so we speak about *torsion points* rather than torsion elements. A point $P\in E(k)$ is an m-torsion point if P is killed by the integer m, *i.e.*, $mP=O$. As usual, the smallest such m is called the *order* of P. The subgroup of $E(k)$ consisting of torsion points is denoted by $E_{tors}(k)$, and for a specific natural number n, we denote the subgroup of m-torsion points by $E_n(k)$—the notation $E(k)[n]$ is also common.

A later section is devoted to a rather intensive study of the torsion points of elliptic curves over $\mathbb{Q}$ of all orders, but the two- and three-torsion have an easy and very geometric description that naturally belongs here.

Over *an algebraically closed field* Ω of characteristic zero we shall in a later lecture prove that $E_n(\Omega) \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, so in that case the number of n-torsion points is n^2. The same applies if the characteristic of k is p when n is relatively prime to p.

Over smaller fields some of the torsion points are rational and some are not, but they always form a group. The possibilities are therefore 0, $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.

THE TWO-TORSION A point $P \in E(k)$ is a two-torsion point if and only if $P = -P$ (well, this is true i any group), that is, the vertical line is tangent to E at P. From the simple Weierstrass equation, one finds

$$2yy' = g'(x),$$

hence in that case the tangent is vertical if and only if $y = 0$, and the two-torsion points of $E(k)$ are the intersection points between the curve and the x-axis that are rational over k.

In the general case of a Weierstrass equation of the form (WWb), the points with vertical tangents are found from

$$(2y + a_1x + a_3)y' = g'(x) - a_1y$$

that is, they are the intersections between the curve and the line $2y + a_1x + a_3 = 0$.

EXAMPLE 1.6. For example, $y^2 = x^3 - x$ has three nontrivial 2-torsion points over $\mathbb{Q}$: $(0,0)$,$(0,1)$ and $(0,-1)$. The 2-torsion subgroup of $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. The curve $y^2 = x^3 + x$, on the contrary, only has one non-trivial torsion point namely $(0,0)$. The 2-torsion subgroups is $\mathbb{Z}/2\mathbb{Z}$. ❄

PROBLEM 1.14. Show that for a prime p and natural number v, the curve $y^2 = x^3 + p^v x + p$ has no non-trivial torsion over $\mathbb{Q}$. HINT: Eisenstein's criterion ✷

PROBLEM 1.15. Assume the characteristic k is not two. Let $a \in k$ be an element different from zero, and let E be the elliptic curve $y^2 = x^3 + ax$. Show that $E_2(k) \neq 0$ and that $E_2(k) = \mathbb{Z}/2\mathbb{Z}$ if and only if $-a$ is not a square in k. ✷

PROBLEM 1.16. Determine the two-torsion groups of the curves $y^2 - y = x^3 - x$ and $y^2 - y = x^3 + x^2$. ✷

Proposition 1.10 *Let E be an elliptic curve over k. The 2-torsion subgroup of $E(k)$ is either trivial or isomorphic to$\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. If the characteristic of k is two, the case $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ does not occur.*

PROOF: This amounts to say there is at most 4 two-torsion points (including O), which is clear since the x-axis (or the symmetry line $2y + a_1x + a_3 = 0$) intersects the curve in at most three points.

In characteristic two, the constraint on the 2-torsion becomes $a_1x + a_3 = 0$, so the x coordinate is unique, and there is at most one non-trivial 2-torsion point, namely $(a_3a_1^{-1}, 0)$. ❑

The three-torsion A three torsion point $P \in E(k)$ is by definition a point such that $3P = 0$. In geometric terms this means the the tangent to E at P has triple contact with E, that is, P is an inflection point. The subgroup $E_3(k)$ therefore consist of the inflection points of E that are rational over k.

As in any group a point $P \in E(k)$ satisfy $3P = 0$ if and only if $2P = -P$, and this allows to give equations for the three-torsion points. Assume the curve is on simple Weierstrass form. The duplication formula (1.7) then gives

$$3x = \big(\frac{3x^2 + a}{2y}\big)^2.$$

When we combine that with equation of the curve, we arrive, after some elementary algebra, at the following equation for x-coordinates of a three-torsion point:

$$3x^4 + 6ax^2 + 12bx + a^2 = 0.$$

The only thing that concerns us for the moment, is that the degree is four, so there at most four roots. As $-P$ is three-torsion if P is, there can at most be 8 non-trivial three-torsion points. In characteristic three, term a_2x^2 in $g(x)$ does not necessarily vanish, and the duplication formula yields

$$3x = 0 = \frac{g'(x)^2}{(2y)^2} - a_2 = \frac{(2a_2x + a_4)^2}{(2y)^2} - a_2.$$

With a little algebra one deduces from this that

$$a_2x^3 = a_4.$$

This has at most one solution since the characteristic is three, and there are at most two non-zero three-torsion points.

Proposition 1.11 *Let E be an elliptic curve over k. Then the subgroup $E(k)_3$ of three-torsion points is one the following groups 0, $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. If the characteristic is 3, the group $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ does not occur.*

Problem 1.17. Check the argument for the preceding proposition when k has characteristic two. ✱

Problem 1.18. Assume that the characteristic of k is three. Let E be on Weierstrass form with $a_1 = a_3 = 0$. Show that a_2 or a_4 must be non-zero. ✱

Problem 1.19. Show that $P = (0, 2)$ is a point of order 3 on the curve $y^2 = x^3 + 4$. ✱

Problem 1.20. Show that the point $P = (2, 3)$ is of order 6 on the curve $y^2 = x^3 + 1$. Which point is $3P$? Hint: E has only one two torsion point. ✱

Isomorphisms and uniqueness

It is an absolutely appropriate question to what extent the Weierstrass equation is unique. That is, given a cubic curve with a flex at $(0;1;0)$ and with the flex tangent $z=0$, what are the different coordinate changes that will bring it on a normal Weierstrass form?

EXAMPLE 1.7. — SCALING x AND y. As an example, an example we already approached in example 1.1 on page 4 and that finally is more than just an example, replacing x by c^2x and y by c^3y brings the Weierstrass equation (WWb) into the equation

$$c^6y^2 + c^5xy + c^3y = c^6x^3 + a_2c^4x^2 + a_4c^2x^2 + a_6,$$

and multiplying through with c^{-6} gives us

$$y^2 + c^{-1}a_1xy + c^{-3}a_3y = x^3 + a^2c^{-2}x^2 + a_4c^{-4}x + a_6c^{-6}.$$

We rewrite it as

$$y^2 + a_1'xy + a1_3y = x^3 + a_2'x^2 + a_4'x + a_6'$$

with $a_i' = c^{-i}a_i$. This makes the way of indexing the coefficients more meaningful, and in some sense it shows that the coefficients a_i are homogenous of degree $-i$. ❄

There are several other *admissible coordinate changes*, that is, linear coordinate changes that take a general Weierstrass equation (WWb) with coefficient in k into a general Weierstrass equation with coefficients in k. However it isn't that many more.

Proposition 1.12 *The only linear changes of variables that are admissible, are those of the form*

$$x = c^2x' + r \qquad y^{`} = c^3y' + sc^2x' + t$$

where r, s, t and c are in k, and where c is different from 0.

PROOF: The inflection point $(0;1;0)$ and the flectional tangent $z=0$ must be conserved under the coordinate shift, so $z \mapsto \alpha z$ and $x \mapsto \beta x + rz$, which in affine coordinates reads $x \mapsto \beta x + r$. There is no constraint on what y can be mapped to, so $y \mapsto \gamma y + sx + t$. After the replacements the coefficients of x^3 and y^2 must be equal so they can be cancelled by scaling the equation. Hence $\beta^3 = \gamma^2$. Putting $c = \gamma/\beta$ proves the claim; indeed $c^2 = \gamma^2/\beta^2 = \beta$ and $c^3 = \gamma^3/\beta^3 = \gamma$.

The coefficient sc^2 merits a comment. Since c is invertible, s is well defined, and there is no problem with the statement. The only reason for this apparently aparte notation, is to keep the "homogeneity" of x. ❏

One is as well interested in the coordinate changes that takes a simple Weierstrass equation into a simple one. For that to happen, one must have $s = t = 0$, since there is no way of cancelling a non-zero xy-term nor a y-term. But at that moment, there is no way of cancelling a x^2-term, so $r = 0$ as well. And we have

Proposition 1.13 *The only linear shifts of variables that take a simple Weierstrass equation into a simple one, are the scalings $y \mapsto c^3 y$ and $x \mapsto c^2 x$.*

It is important to see how different invariants of the curve behave when the coordinates are changed. In the case of the simple Weierstrass equation, the discriminant is given as $\Delta = 27a_6^2 + 4a_4^3$, and it becomes $c^{-12}\Delta'$ when we replace y by $y' = c^3 y$ and x by $x' = c^2 x$; indeed, in that case $a_i = c^{-i} a_i$. In the general case, with a general Weierstrass equation and a general coordinate change, the same relation between the two discriminants holds, but in accordance with our principle of not entering into the long and tedious, but trivial, computations (they don't even make you any wiser), we just state

Proposition 1.14 *If one performs an admissible change of coordinates like in proposition 1.12, the discriminants comply to the rule*

$$\Delta' = c^{-12}\Delta.$$

Problem 1.21. Explore what linear coordinate changes take a special Weierstrass equation into a special Weierstrass equation. ✷

Problem 1.22. Assume that k is of characteristic p. Let E have a Weierstarss equation with coefficients a_i. And let $E^{(p)}$ denote the curve having a Weierstrass equation with coefficients a_i^p. Assume that E and $E^{(p)}$ are isomorphic. Show that E is isomorphic to a curve having simple Weierstrass coefficents b_i with $b_i = b_i^p$. ✷

A general isomorphism theorem

The statement in proposition 1.12 may be strengthened considerably to a statement about general isomorphisms of elliptic curves. Given two elliptic curves E and E', both contained in $\mathbb{P}^2$, with inflection points O and O' respectively, and assume that there is an isomorphism $\phi\colon E' \to E$ taking O' to O. There is *a priori* absolutely no reason for this isomorphism to be induced by a linear automorphism of $\mathbb{P}^2$, but miraculously it is:

Proposition 1.15 *Let $E, E' \subseteq \mathbb{P}^2(\Omega)$ be two elliptic curves with inflection points O and O', both defined over k, and both on Weierstrass form (WWb). Assume there is an isomorphism $\phi\colon E' \to E$ defined over k that takes O' to O. Then there is a linear coordinate shift with*

$$x = c^2 x' + r \qquad y^{`} = c^3 y' + sc^2 x' + t$$

with r, s, t and c are in k, and $c \neq 0$, inducing the isomorphism ϕ.

Another way of stating this, is the there is linear map $\Phi\colon \mathbb{P}^2 \to \mathbb{P}^2$ such that $\Phi(P) = \phi(P)$ whenever $P \in E$. The proof of this requires some preparations. Before starting with that, we formulate a corollary which in some sense is astonishing:

Corollary 1.1 *Let E and E' be two elliptic curve over k and let $\phi\colon E \to E'$ be an isomorphism. If $\phi(O) = O'$, then ϕ is a group homomorphism.*

Proof: The isomorphism can be realized as the restriction of a linear map $\Phi\colon \mathbb{P}^2 \to \mathbb{P}^2$. As the group laws are defined by lines, and Φ takes lines to lines, it holds that $\phi(P + Q) = \phi(P) + \phi(Q)$. ❑

Quick review of poles and zeros First of all, a quick review of the local behavior regular function on plane smooth curve. So assume that $C \subseteq \mathbb{A}^2 = k^2$ is a smooth curve given by the equation $f(x, y) = 0$. We pick a point P on C, which we by an appropriate choice of coordinates can assume to be $P = (0, 0)$. Adjusting the coordinates if necessary, the tangent to C at P will be given by $y = 0$. The polynomial $f(x, y)$ may then be brought on the form

$$f(x, y) = y(\alpha + r(x, y)) + x^n(\beta + s(x)) = yu - x^n v$$

where $u = u(x, y)$ and $v = v(x)$ are polynomials that do not vanish in $(0, 0)$ and n is a natural number (which by the way is the contact order of the tangent; for an ordinary tangent $n = 2$). Recall the local ring $\mathcal{O}_{C,P}$ of C at P. It is the localized ring

$$\mathcal{O}_{C,P} = (k[x, y]/(f(x, y)))_{\mathfrak{m}}$$

where $\mathfrak{m}$ is the maximal ideal in $k[x, y]$ consisting of polynomials vanishing at P. In this ring the polynomial u above is invertible, and one can write $y = x^n vu^{-1}$. Any element in $\mathcal{O}_{C,P}$ is therefore of the form $x^m w$ with w is a unit and $m \geq 0$ an integer. More or less the same applies to any rational function ϕ on C, that is, an element in the fraction field of $\mathcal{O}_{C,P}$; It can be expressed as $x^m w$ where now $m \in \mathbb{Z}$ and w is a unit in $\mathcal{O}_{C,P}$. The integer m is uniquely associated to ϕ; it does not depend on the coordinate x as long as the line $x = 0$ is not tangent to C. We call it *the order of ϕ at P*, and x is called a *parameter at p*.

If $m < 0$ one says that ϕ has a *pole* at P and if $m > 0$ it has *zero*. The order of ϕ at P will be is usually denoted by $\operatorname{ord}_P(\phi)$.

Elliptic curves at the flex For any curve on Weierstrass form

$$zy^2 = x^3 + axz^2 + bz^3 \tag{1.8}$$

the affine equation round the inflection point $(0; 1; 0)$ is

$$z = x^3 + axz^2 + bz^3,$$

where we continue our notorious abuse of language writing z for z/y and x for x/y. The tangent is $z = 0$, and we can use x as parameter. We find

$$z = x^3/(1 - axz - bz^2),$$

so $\text{ord}_O(z) = 3$; that is z/y (no abuse of language!) has a zero of order 3 at O, and of course z/x has a zero of order 2. Inverting the two we find:

Lemma 1.2 *If the elliptic curve is given on general Weierstrass form, then y/z and x/z has poles of order respectively 3 and 2 at O.*

Proof: There is just one remark to make: Above we worked solely with the special Weierstrass equation to make the presentation simpler, but every thing goes through with obvious and trivial modifications in the general setting. ❏

Problem 1.23. Carry through the computation above in the general case, that is when the curve is given by (WWb). ✷

A very mild Riemann-Roch In the proof we shall use a very mild form of the Riemann-Roch theorem. We will state it, but not prove it. It is mild in the sense that it is formulated in very specific situation. The general Riemann-Roch theorem for curves (there is one for all smooth, complete varieties) applies to any smooth and complete curve C and any divisor D on C (a divisor is just a formal finite integral linear combination $D = \sum_p n_p P$ of points in of the curve). In our mild version the curve is elliptic and the divisor confined to the form nP.

Let E be any elliptic curve over k and let $P \in E(k)$ be a k-rational point on E. We are interested in rational functions on E regular away from P and with a limited pole-order at P. Specifically, if n is a natural number, we require that $\text{ord}_P(\phi) \geq -n$. These rational functions form a linear subspace of the fraction field $K(E)$ (you can't make a pole worse by adding two functions) which we denote by $L(nP)$. It is a theorem that these space are finite-dimensional, and the Riemann-Roch theorem gives a formula for the dimensions $\dim L(nP)$.

Theorem 1.2 $\dim L(nP) = n$ *if* $n \geq 2$ *and* $\dim L(P) = 1$.

If $n = 0$, the functions in $L(0P)$ are just the constants, and the constant functions are contained in any of the $L(nP)$, so the statement that $\dim L(P) = 1$, means that any non-constant rational function regular outside P must at least have a double pole at P. We also note that $L(mP) \subseteq L(nP)$ whenever $m \leq n$.

Finally we come to the proof of the proposition:

Proof of proposition 1.15: We first concentrate on E'. There is an increasing sequence $k \subseteq L(2O') \subseteq L(3O')$ of vector space of dimensions 1, 2 and 3 respectively. Hence[3] y' (which by lemma 1.2 lies in $L(3O')$ but not in $L(2O')$), x' (which lies in $L(2O')$ but not in k) and the constant function 1 form a basis for $L(3O')$. And similarly, x' and 1 form a basis for the subspace $L(2O')$.

The rational function $x \circ \phi$ on E' has a double pole at O' and is regular elsewhere (the map ϕ is an isomorphism and takes O' to O where x has its only pole which is

[3] As usual we shorten the notation and write y' for y'/z' and x' for x/z, and ditto for the coordinates x, y on E)

double). Hence one may write $x \circ \phi = \alpha x' + r$. In an analogous manner, $y \circ \phi$ has a triple pole at O' and is regular elsewhere so it belongs to $L(3O')$ and may expressed in the basis: $y \circ \phi = \beta y' + sx' + t$.

This means that the linear map $(x', y') \to (\alpha x' + r, \beta y' + sx' + t)$ takes a point $P' \in E'$ to $\phi(P')$. As in the proof of proposition 1.12 above one sees that $\alpha^3 = \beta^2$, and $c = \alpha/\beta$ does the job. ❑

Comment on RR

Having stated the mild Riemann-Roch theorem we take the opportunity to sketch the argument that any smooth, connected curve of genus one with a rational point, can be brought on Weierstrass form; a result that apparently first was written down by Nagell. We shall need a slightly wilder Riemann-Roch theorem than the one above, and begin with a few words about Riemann-Roch.

To any curve k which is smooth and complete, one may associate a fundamental invariant g called the genus of the curve. The very first trace of this invariant is found in Niels Henrik Abels work, although he did not call it the genus, and seemingly it must have been rather nebulous to him. The genus can be defined in several mostly subtle ways, and most of need some kind of cohomology to be done a proper way. De do not intend to go into that, but shall sketch an argument with differential forms for the genus of an elliptic curve being one.

So this is just to say that there is the notion of the genus of a curve and give you some feeling for the invariant in the context of elliptic curves. (If you don't care, you can think about genus one curves as curves for which theorem 1.2 is valid). For smooth plane curves of degree d the genus is given by the formula $(d-1)(d-2)/2$.

The notion of the genus of a curve is closely related to the differential forms on the curve. If ω is a (rational) form and x is a parameter at the point P, one may write $\omega = f(x)dx$ in a neigbourhood round P with $f(x)$ a rational function. One defines $\operatorname{ord}_P(\omega)$ as $\operatorname{ord}_P(f)$, that is one has $\omega = x^\nu v dx$ where v does not vanish at P and $\nu = \operatorname{ord}_P(f)$.

A priori this depends on the choice of the parameter x, but if $x = ux_1$ where u does not vanish at P, one finds $dux = udx_1 + x_1du = (u + xu')dx_1$ so $f(x)dx = f(ux_1)(u + x_1u')dx_1 = x_1^\nu u^n v(u + x_1u1)dx_1$ where $u^n v(u + x_1u_1)$ does not vanish at P. This gives us the possibility to defined the degree of a differential form just by summing up the orders of ω at the different points, that is $\deg \omega = \sum_P \operatorname{ord}_P(\omega)$ (this is a finite sum, since locally the orders of ω are the orders of a rational function). It is a result that this degree is the same for all ω, and one defines the genus as the number g with $\operatorname{ord}_P(\omega) = 2g - 2$.

In the case of an elliptic curve given by the Weierstrass equation

$$y^2 = x^3 + ax + b = g(x)$$

one finds upon derivation

$$\frac{2dy}{g'(x)} = \frac{dx}{y}$$

and this defines a global regular differential form; off the x-axis the right side is well defined, and near by the points on the curve lying on the x-axis the left side is well defined, indeed in those points the derivative $g'(x)$ does not vanish, $g(x)$ having simple zeros.

Off the x-axis the tangent to E is never vertical, that is we may use x as a parameter and at the intersection points with the x-axis the tangent is vertical and we may use y as a parameter at those points. So ω is regular and never vanishes. Hence $\deg\omega = 0$ and $g = 1$.

Recall that a divisor D on the curve E is a formal linear combination $D = \sum_{P\in E} n_p P$ where $n_P \in \mathbb{Z}$ and where only finitely many of the n_P's are non-zero. The *degree* of D is simply $\sum_P n_P$. Just as we defined $L(nO)$ above, we let $L(D)$ be the space of those rational functions $f \in k(E)$ whose order at a point P is bounded below by $-n_p$, that is $\mathrm{ord}_P(f) \geq -n_P$ for all P. As $\mathrm{ord}_P(f+g) \geq \min\{\mathrm{ord}_P(f), \mathrm{ord}_P(g)\}$ this is a vector space (cancellation can only increase the order). If $n_P \leq 0$ the functions in $L(D)$ are regular at P, and in case $n_P < 0$ they vanish there (to an order larger than $-n_P$).

For genus one one has

Theorem 1.3 *Let E be a genus one curve over k and let D be a divisor. If $\deg D > 0$, then $\dim(D) = \deg D$.*

We are now ready for:

Proposition 1.16 *Let E a smooth, complete curve of genus one over k with a rational point O. Then E is isomorphic over k with a curve on Weierstrass form with O corresponding to the flex.*

Proof: The main point is that Riemann-Roch theorem, as stated above, holds true for genus one curves without any reference to any ambient space. So if O is the rational point, there is the ascending series of vector spaces of rational functions on E:

$$k \subseteq L(2O) \subseteq L(3O),$$

where the dimension in each step jumps by one. There k stands for the space of constant functions. As above, there is a basis $y, x, 1$ for $L(3O)$ with $y \notin L(2O)$ and with $x \in L(2O)$ but being not constant—this choice is of course inspired by lemma 1.2.

Using the functions x and y as respectively the x- and the y-coordinate, give a rational map $C \to \mathbb{P}^2$. Away from O it is defined by sending P to $(x(P); y(P); 1)$, and this map extends to the whole of C by sending P to the point $(x(P)/y(P); 1; 1/y(P))$ on the piece of C where $y(P) \neq$. In particular, $O \mapsto (0; 1; 0)$.

The image of E under this map is a cubic. Indeed, the space $L(6O)$ is of dimension 6 so there must be a linear relation among the following 7 members: y^2, x^3, x^2, x, y, xy and 1 giving

$$a_0y^2 + a_1xy + a_3y = a_0'x^3 + a^2x^2 + a^4x + a^6.$$

There is a lot of checking to do.

First of all both the coefficients a_0 and a_0' are non-zero: The terms x^3 and y^2 are the only terms respectively on the right and on the left side with coinciding pole orders (the other terms on the right are of even order and those on the left of odd). Hence these terms are forced to be non-zero, and $a_0a_0' \neq 0$. We may as well assume that both equal one, so the image is on Weierstrass form.

We shall not give a full proof of the map being an isomorphism, just check that it is injective. For that, let P and Q be two different points on E. We shall exhibit a coordinate —that is a rational function in $L(3O)$— vanishing in P but not in Q (one says that "linear system" $L(3O)$ separates points). Then the images of P and Q must be different.

Now $L(3O-P)$ and $L(3O-Q)$ are the subspaces of $L(3O)$ consisting of functions that vanish respectively at P and Q. Hence their intersection equals the subspace $L(3O-P-Q)$ of functions vanishing at both P and Q. Now $\deg(3O-P) = \deg(3O-Q) = 2$ and RR give us the dimensions $\dim L(3O-P) = L(3O-Q) = 2$. On the other hand, $\deg(3O-P-Q) = 1$, and therefore $\dim L(3O-Q-P) = 1$. Since $L(3O-Q-P) = L(3O-P) \cap L(3O-Q)$ it follows that $L(3O-P) \neq L(3O-Q)$, and we can find a function lying in one of the spaces but not in the other. ❏

Problem 1.24. Show that at every point P in E there is a function in $L(3O)$ that vanishes at P but whose derivative does not. This is basically the step that is missing in the proof of proposition 1.16. ✷

1.1 The j-invariant

There is a very convenient devise to decide if two curves E and E' are isomorphic over an algebraically closed field Ω, called the j-invariant. It is a number $j(E)$ in Ω one associates to any elliptic curve E, the point being that E and E' are isomorphic over Ω if and only if they have the same j-invariant. It is mostly an easy task to compute the j-invariant, for example if E is given by the simple Weierstrass equation

$$y^2 = x^3 + ax + b$$

one has $j = 1728 \cdot 4a^3/(4a^3 + 27b^2)$. To decide if two curves with the same j-invariant are isomorphic over k, however, can be a most delicate matter; sometimes they are and sometimes they aren't.

If we perform a scaling operation of the usual type as in 1.1 on page 4 where x is replaced by c^2x and y by c^3x, the coefficient a changes to $c^{-4}a$ and b to $c^{-6}b$. Both the enumerator and the denominator in the expression for j above change by the factor c^{-12}, and hence the j-invariant itself does not change; it is, well, invariant. An elementary but rather involved calculation shows that j is invariant under any admissible change of coordinates.

One may wonder why the constant 1728 appears. This is not because Copenhagen was on fire that year, but because there is a complex function closely related to the j-invariant that has a Fourier expansion

$$j(q)?\frac{1}{q}+744+196884q+21493760q^2+864299970q^3+\dots$$

where $q=\exp(2\pi i\tau)$. And the 1728 is there to make all the Fourier coefficients integers! Which is really an amazing thing!! (Even more amazing is that 196884 is the rank of the smallest representation of the biggest sporadic simple group, the big monster. This goes under the name of "moonshine".)

There is also an expression for the j-invariant of curves whose Weierstrass equation is on the general form (WWb). It is however long and complicated and we don't give it. If you insist on seeing it, you'll find it at page 46 of Silverman's book [**?**].

As we indicated, the *raison d'être* of the j-invariant is the following proposition:

Proposition 1.17 *It E and E_1 are two isomorphic elliptic curve, one has $j(E)=j(E_1)$.*

Proof: In the general case, this is just a tedious and not very enlightening computation. However in the special case when the curve is on the simple Weierstrass form W and the isomorphism is just a scaling as in example 1.7, replacing y by c^3y and x by c^2x, it follows all by it self that $j(E)$ is invariant since a_i is changed to $c^{-i}a_i$ and $j(E)$ in that case is

$$j(E)=1728\cdot 4a^3/(4a^3+27b^2).$$

❑

Example 1.8. — Curves with $j=1728$. Elliptic curves with equation $y^2=x^3+ax$ where $a\neq 0$ all have j-invariant 1728.

Over an algebraically closed field one can perform the usual scaling as in 1.1 on page 4 with a factor c satisfying $c^{-4}=a$, and thus transform the equation into $y^2=x^3+x$. This shows that these curves all are isomorphic to the one given by $y^2=x^3+x$.

However, over a non-algebraically closed field this is no more true. A simple example being $y^2=x^3-x$ and $y^2=x^3+x$. They are not isomorphic over the reals $\mathbb{R}$; see exercise **??** on page **??**. ❄

Example 1.9. — Curves with $j=0$. Elliptic curves with Weierstrass equation $y^2=x^3+b$ have $j=0$, and they are isomorphic over an algebraically closed field. Indeed, one has $b\neq 0$, otherwise the curve would have a cusp, and scaling by a factor c with $c^{-6}=b$ shows they all are isomorphic to $y^2=x^3+1$. ❄

Proposition 1.18 *Let E and E_1 be two elliptic curves over the algebraically closed field Ω. If $j(E)=j(E_1)$, the elliptic curves E and E_1 are isomorphic (over Ω).*

Proof: We shall only give the proof in the case the curves are given by Weierstrass equations of the simple form. Since the j-invariants are equal, one has

$$a^3/(4a^3+27b^2) = a_1^3/(4a_1^3+27b_1^2)$$

and after a trivial manipulation one arrives at

$$a^3b_1^2 = a_1^3b^2. \tag{$\star$}$$

Assume first that $bb_1 \neq 0$. Since Ω is algebraically closed, we may an element $c \in \Omega$ such that $c^{-6} = bb_1^{-1}$. Then the scaling $y \mapsto c^3y$ and $x \mapsto c^2x$ brings the equation $y^2 = x^3 + ax + b$ on the form $y^2 = x^3 + a'x + b'$ with coefficients satisfying $a' = c^{-4}a$ and $b' = c^{-6}b$. By choice, $c^{-6} = b_1b^{-1}$, and hence $b' = b_1$. The relation ($\star$) above shows that $c^{-4} = (bb_{-1})^{-2/3} = a_1a^{-1}$, and it follows that $a' = a_1$.

The case $b = 0$ or $b_1 = 0$, is just example 1.8 above. ❑

It is worth while remarking that two curves E and E_1 defined over k and having the same j-invariant, are not necessarily isomorphic over k if k is not algebraically closed. However, they will be isomorphic over a finite extension K of k which is cyclic and of degree at most 6.

It is a natural question if every element from Ω is the j-invariant of some elliptic curve (the answer is yes), and just as natural is the question over which field that curve is defined.

For example, if $j \in \mathbb{Q}$ is a rational number, can one find an elliptic curve defined over $\mathbb{Q}$ having j as j-invariant? The answer is yes. If E is defined over $\mathbb{Q}$, clearly $j(E)$ is rational, and hence it holds true that $j(E) \in \mathbb{Q}$ if and only if E is defined over $\mathbb{Q}$.

One may think about this in the following way: The elliptic curves, up to isomorphism, are parametrized by a line (called *the moduli space*) with the coordinate j. The rational points on that line correspond to curves defined over $\mathbb{Q}$, and more generally if K is a number field, K-points of the curve correspond to elliptic curves defined over K.

Let $\mathbb{F} \subseteq \Omega$ denote the prime field. That is $\mathbb{F} = \mathbb{Q}$ in case Ω is of characteristic zero, and if Ω is of characteristic p, then $\mathbb{F} = \mathbb{F}_p$. As usual, we shall only give the proof in case $p \neq 2, 3$ which is somehow simpler than the proof in the general case.

Proposition 1.19 *Let E be an elliptic curve over Ω. Then E is defined over $\mathbb{F}(j(E))$. Every $j \in \Omega$ is the j-invariant of a curve.*

Proof: We need to find one curve whose equation

$$y^2 = x^3 + ax + b$$

has coefficients in $\mathbb{F}(j)$; that is, we must solve the equation

$$j = 1728 \cdot 4a^3/(4a^3 + 27b^2).$$

We have the freedom to chose $b = a$, that simplifies the equation

$$j(4a + 27) = 1728 \cdot 4a.$$

This gives $a = 27j/4(j - 1728)$ as long as $j \neq 1728$, but in that case $b = 0$ will do. ❑