MATH-GA 2150.001 : Advanced Topics in Algebra (Introduction to Algebraic Geometry and Elliptic Curves)

ALENA PIRUTKA

Contents

Chapter 1

Affine and projective algebraic varieties

1.1 Affine varieties, Nullstellensatz

In this section we introduce affine algebraic varieties : the base objects of study in algebraic geometry. The main theorem of this section is the famous Hilbert's Nullstellensatz on zero locus of a system of polynomial equations over an algebraically closed field.

Let k be a field. The main cases of interest for this course is $k = \mathbb{C}$, k algebraically closed, $k = \mathbb{R}$, $k = \mathbb{Q}$ or a finite extension (a number field), k finite.

We identify the affine space $\mathbb{A}^n_k$ with the set k^n.

An *affine algebraic variety* over k is the subset of k^n defined as zero locus of a system of polynomials in $k[x_1, \ldots, x_n]$:

Definition 1.1.1. For I an ideal in $k[x_1, \ldots, x_n]$ we denote

$$V(I) = \{x = (x_1, \ldots, x_n) \in k^n \mid f(x) = 0 \, \forall f \in I\}$$

the **affine algebraic variety** defined by I.

If $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ is a finite family of polynomials, we write $V(f_1, \ldots, f_m)$ instead of $V((f_1, \ldots, f_m))$ for the affine variety defined by the ideal generated by $f_1, \ldots, f_m$.

Recall that the ring $k[x_1, \ldots, x_n]$ is noetherian : any ideal I of this ring is generated by a finite number of elements, so that any algebraic variety is of the form $V(f_1, \ldots, f_m)$ as above.

Example 1.1.2. In the affine plane $\mathbb{A}^2_k$ we have $V(x, y) = (0, 0)$, $V(x - 1, y - 2) = (1, 2)$, $V(y^2 - x^3 + x)$ is a curve (we will see that it is an example of an elliptic curve).

Remark 1.1.3. In a more advanced course on algebraic geometry an affine variety corresponds to an ideal in $k[x_1, \ldots, x_n]$; saing that $X = V(I)$ is an affine variety means that we recall the data of X and I. Speaking about the *set of rational points* $X(k) \subset k^n$ of X means that we consider the set $X(k) = V(I)$ but we «forget» the data of I. If K/k is an extension of k we denote $X(K) = V(I_K) \subset K^n$ for $I_K \subset K[x_1, \ldots, x_n]$ the idéal generated by I.

Note that if k is not algebraically closed, the set $V(I)$ could be empty: for example, for $I = (x^2 + y^2 + 1) \subset \mathbb{R}[x, y]$. If $k = \mathbb{C}$ and $I = (f)$ with $f \in k[x]$ a non constant polynomial, the fundamental theorem of algebra says that $V(I)$ is not empty. In the case of polynomials in many variables, we have an analogous statement:

Theorem 1.1.4. [weak Nullstellensatz] *Let k be an algebraically closed field and let I be an ideal of $k[x_1, \ldots, x_n]$, $I \neq (1)$. The set $V(I)$ is nonempty.*

Proof. This theorem follows from a theorem on the structure of maximal ideals in $k[x_1, \ldots, x_n]$, that we give below, for the proof see the next section. In fact, the ideal I is contained in a maximal ideal $\mathfrak{m}$ (Krull's theorem), and we can write $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ by 1.1.5. As $V(\mathfrak{m})$ is nonempty, we see that $V(I)$ is nonempty as well. □

Theorem 1.1.5. *Let k be an algebraically closed field. Any maximal ideal $\mathfrak{m}$ in $k[x_1, \ldots, x_n]$ is of the form $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ with $a_1, \ldots, a_n \in k$.*

Definition 1.1.6. If X is a subset of k^n we denote

$$I(X) = \{f \in k[x_1, \ldots, x_n],\ f(x) = 0\, \forall x \in X\}$$

the ideal of X.

For example, if $X = \{0, 0\} \subset \mathbb{A}^2_k$, then $I(X)$ is the ideal of polynomials in $k[x, y]$ with zero constant term.

Note that $I(X)$ is indeed an ideal: if $f \in I(X)$ and $g \in k[x_1, \ldots, x_n]$, then the polynomial fg vanishes at every point of X.

Proposition 1.1.7. *1. Let I, J be the ideals of $k[x_1, \ldots, x_n]$.*

- *(a) $I \subset J \Rightarrow V(J) \subset V(I)$;*
- *(b) $V(I) \cap V(J) = V(I + J)$;*
- *(c) $V(I) \cup V(J) = V(I \cdot J) = V(I \cap J)$.*

2. If $X \subset Y$ are subsets of k^n, then $I(Y) \subset I(X)$.

3. If J is an ideal in $k[x_1, \ldots, x_n]$, then $J \subseteq I(V(J))$.

4. If $X \subset k^n$ is an algebraic variety, then $X = V(I(X))$.

Proof. We give a proof for *1(b)* et *1(c)*, the other properties follow immediately from the definitions.

1(b). Let $x \in V(I) \cap V(J)$. We then have $f(x) = 0$ and $g(x) = 0$ for all $f \in I$ and $g \in J$. We deduce $h(x) = 0$ for all $h \in I + J$. In the other direction, if $h(x) = 0$ for all $h \in I + J$, we have in particular that $f(x) = 0$ and $g(x) = 0$ for all $f \in I$ and $g \in J$, so that $x \in V(I) \cap V(J)$.

1(c). Let $x \in V(I) \cup V(J)$. We then have either $f(x) = 0$ for all $f \in I$, or $g(x) = 0$ for all $g \in J$. We deduce $h(x) = 0$ for all $h \in I \cdot J$ (resp. for all $h \in I \cap J$). In the other direction, assume $h(x) = 0$ for all $h \in I \cdot J$ (resp. for all $h \in I \cap J$). If $x \notin V(I)$, there exists $f \in V(I)$ such that $f(x) \neq 0$. Let $g \in J$. As $fg \in I \cdot J$ (resp. in $I \cap J$), we deduce $g(x) = 0$, so that $x \in V(J)$. □

The previous properties imply that the sets $V(I)$ are the closed sets of some topology, called **Zariski topology** on k^n. If $X \subset k^n$ is an affine algebraic variety, we call the induced topology on X **Zariski topology on** X as well.

Note that we do not necessarily have the equality $J = I(V(J))$. In fact, there could be two types of problems:

1. for $J = (x^2)$ an ideal in $k[x]$, we have $I(V(J)) = (x)$;
2. if k is not algebraically closed : for example, for $J = (x^2 + y^2)$ an ideal in $\mathbb{R}[x, y]$, we have $I(V(J)) = (x, y)$.

Hilbert theorem of zeros says that these two problems are essentially the only ones.

Recall the notion of a radical of an ideal:

Definition 1.1.8. If A is a (commutative) ring and $I \subset A$ is an ideal, the **radical of** I is

$$\sqrt{I} = \{a \in A \,|\, a^m \in I \text{ for some } m \geq 1\}.$$

One checks that $\sqrt{I}$ is also an ideal of A. The ideal I is **radical** if $I = \sqrt{I}$.

Example 1.1.9. For $J = (x^2)$ an ideal in $k[x]$, we have $\sqrt{J} = (x)$.

Theorem 1.1.10. [Nullstellensatz] *Let k be an algebraically closed field and let J be an ideal in $k[x_1, \ldots, x_n]$. Then $I(V(J)) = \sqrt{J}$.*

Proof. We deduce the theorem from its weak version. This argument is due to Artin and Tate. Let $f \in I(V(J))$, so that f vanishes at all common zeros of elements of J. Consider the ideal J' of $k[x_1, \ldots, x_{n+1}]$:

$$J' = (x_{n+1}f - 1, J).$$

By construction, $V(J') = \emptyset$. Using weak Nullstellensatz, $1 \in J'$, that is, we can write in the quotient ring $A = k[x_1, \ldots, x_{n+1}]/(x_{n+1}f - 1)$:

$$1 = \sum b_i a_i$$

with $b_i \in J, a_i \in A$, so that (writing by degrees of x_{n+1})

$$1 = c_0 + c_1 x_{n+1} + \ldots + c_m x_{n+1}^m$$

with $c_i \in J$. As $x_{n+1}f - 1 = 0$ in A, we deduce

$$f^m = c_0 f^m + c_1 f^{m-1} + \ldots + c_m,$$

that is, $f^m - c = 0$ with $c = c_0 f^m + c_1 f^{m-1} + \ldots + c_m \in J$. As the natural map $k[x_1, \ldots, x_n] \to A$ is injective, we deduce $f^m - c = 0$ in $k[x_1, \ldots, x_n]$, so that $f^m \in J$. □

Remark 1.1.11. Note that if $J = I(X)$, then $J = \sqrt{J}$: in fact, if $f^m \in J$, then $(f(x))^m = 0$ for all $x \in X$, so that $f(x) = 0$ for all $x \in X$, which implies that $f \in J$.

For the moment we introduced the objects of the category of affine algebraic varieties over k. One is then also interested to understand the morphisms between these objects.

Definition 1.1.12. Let X be an algebraic variety in k^n. A **polynomial function** on X is the restriction of a function in $k[x_1, \ldots, x_n]$ to X. If Y is another algebraic variety in k^m, the function $f : X \to Y$ is **polynomial** if every coordinate function is.

Note that a polynomial function $X \to Y$ is continuous for Zariski topology: if $Z = V(I) \cap Y \subset Y$ is closed, where I is an ideal in $k[y_1, \ldots, y_m]$ generated by $(h_1, \ldots h_r)$, then $f^{-1}(Z) = X \cap V(h_1 \circ f, \ldots h_r \circ f)$ is closed in X.

Proposition 1.1.13. *The algebra of polynomial functions on X is the algebra*

$$k[X] := k[x_1, \ldots, x_n]/I(X).$$

Proof. Let $f, g \in k[x_1, \ldots, x_n]$ be two polynomials inducing the same polynomial function on X. We then have $f - g = 0$ at all points of X, so that $f - g \in I(X)$. □

Let $f : X \to Y$ be a polynomial map between two affine varieties defined over a field k. We define the map $f^* : k[Y] \to k[X]$ by

$$f^*(\bar{P}) = \overline{P \circ f}$$

where $\bar{P}$ (resp. $\overline{P \circ f}$) is the class of P (resp. $P \circ f$) in $k[Y]$ (resp. $k[X]$). This map is well defined : if $P_1 - P_2 \in I(Y)$ then for all $x \in X$ we have $P_1(f(x)) = P_2(f(x))$ as $f(x) \in Y$.

Proposition 1.1.14. *Let X, Y be two affine varieties. Let $g : k[Y] \to k[X]$ be a morphism of algebras. There exists a polynomial map $f : X \to Y$ such that $g = f^*$.*

Proof. We write $k[X] = k[x_1, \ldots, x_n]/I(X)$ and $k[Y] = k[y_1, \ldots, y_m]/I(Y)$ by the previous proposition. Let G be the composition

$$k[y_1, \ldots, y_m] \to k[y_1, \ldots, y_m]/I(Y) \xrightarrow{g} k[x_1, \ldots, x_n]/I(X).$$

Let $f_i = G(y_i)$. Let $P_i \in k[x_1, \ldots, x_n]$ such that $f_i = \bar{P_i}$. Write $f = (P_1, \ldots, P_m)$. As $f^*(\bar{y_i}) = \bar{P_i} = g(\bar{y_i})$ by construction, it is enough to see that f has its values in Y.

Let $x = (a_1, \ldots, a_n) \in X$ and let $h \in I(Y)$. We have

$$h(f(x)) = h(P_1(a_1, \ldots, a_n), \ldots, P_m(a_1, \ldots a_n)).$$

For all $i = 1, \ldots, m$ we see that the value $P_i(a_1, \ldots, a_n)$ depends only on the values $\bar{P_i}$ of P_i in $k[X]$. As $\bar{P_i} = G(y_i)$ we get

$$\begin{aligned} h(f(x)) &= h(G(y_1), \ldots, G(y_n))(a_1, \ldots, a_n) = \\ &= [G \text{ is a homomorphism of algebras }] = Gh(y_1, \ldots y_m)(a_1, \ldots, a_n) = 0. \end{aligned}$$

so that $f(x) \in V(I(Y)) = Y$. □

Definition 1.1.15. Let X be an affine algebraic variety. We say that X is **irreductible** if

$$X = X_1 \cup X_2,\ X_1, X_2 \text{ closed in } X \Rightarrow X = X_1 \text{ or } X = X_2.$$

A variety X is irreductible if and only if $I(X)$ is a prime ideal (see the exercises). We deduce that the ring $k[X]$ is integral. Then we define **the field of functions** of X as the field of fractions $k(X)$ of the ring $k[X]$: the elements of $k(X)$ are the functions f/g with $f, g \in k[X]$ and $f/g = f_1/g_1$ if and only if $fg_1 = f_1 g$.

1.1.1 Finiteness properties

In this section we recall some properties of rings and modules.

Definition 1.1.16. Let A be a ring and B an A-algebra. We say that B is **of finite type** over A if B is generated, as an A-algebra, by a finite number of elements: $B \simeq A[x_1, \ldots, x_n]$ (where the elements $(x_i)_{1 \leq i \leq n}$ are not necessarily algebraically independent). We say that B is a finite A-algebra if B is of finite type as A-module, that is, B is generated by a finite number of elements as an A-module : $B \simeq Ax_1 + \ldots + Ax_n$.

Example 1.1.17. 1. If k is a field and $K = k(x)$ is an algebraic extension of k generated by x, then K is a k-module of finite type. In fact, if $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ is a minimal polynomial of x, then K is generated by $1, x, \ldots x^{n-1}$.

2. Let A be a ring. If B is an A-algebra of finite type (resp. a finite A-algebra) and C is a B-algebra of finite type (resp. finite), then C is an A-algebra of finite type (resp. finite).

Definition 1.1.18. Let A be a ring and let M be an A-module. We say that M is **noetherien** if any increasing sequence $M_1 \subseteq M_2 \subseteq \ldots M_n \subseteq \ldots$ of submodules of M is constant starting from some $n = n_0$. A ring A is **noetherian** if A is noetherian as an A-module, that is any increasing sequence $I_1 \subseteq I_2 \subseteq \ldots I_n \subseteq \ldots$ is constant starting from some $n = n_0$.

Proposition 1.1.19. *An A-module M is noetherian iff any submodule of M could be generated by a finite number of elements. In particular, a ring A is noetherian if and only if any ideal of A could be generated by a finite number of elements.*

Example 1.1.20. 1. Let M be an A-module. If M is noetherian, then any submodule of M is noetherian, any quotient of M is noetherian and any module of finite type over M is noetherian.

2. If A is noetherian, then the ring $A[x]$ is also noetherian, in particuliar, $k[x_1, \ldots, x_n]$ is noetherian. If B is an A-algebra of finite type, then B is a noetherian ring : in fact, B is a quotient of $A[x_1, \ldots x_n]$.

3. The ring $A = k[x_i]_{i\in\mathbb{N}}$ is not noetherian. The field of fractions K of A, being a field, is noethérien. This shows that a subring of a noetherian ring is not necessarily noetherian.

1.2 The structure of maximal ideals

Lemma 1.2.1. *Let $A \subseteq B \subseteq C$ be the inclusions of rings such that*

(i) A is a noetherian ring,

(ii) C is an A-algebra of finite type,

(iii) C is a B-module of finite type.

Then B is an A-algebra of finite type.

Proof. Let $x_1, \ldots, x_n$ be the elements of C generating C as an A-algebra. Let $y_1, \ldots, y_m \in C$ generating C as a B-module :

$$C = By_1 + \ldots + By_m.$$

We can then write, for all $1 \leq i, j \leq n$:

$$x_i = \sum_{t=1}^{m} b_{it} y_t$$

with $b_{it} \in B$ and

$$y_i \cdot y_j = \sum_{t=1}^{m} c_{ijt} y_t.$$

Let $B' \subset B$ be a subring generated over A by families (b_{it}) and (c_{ijt}). As B' is of finite type over A and A is a noetherian ring, we have that B' is noetherian. By construction, C is generated by $y_1, \dots y_m$ as a B'-module. We then have that C, viewed as a B'-module, is noetherien. As B is a submodule of C, we deduce that B is generated by a finite number of elements as a B'-module: $B = B'd_1 + \ldots + B'd_s$. We get that B is an A-algebra of finite type, generated by families (b_{it}) and (c_{ijt}) and (d_i). □

Proof of theorem 1.1.5. Let $K = k[x_1, \dots, x_n]/\mathfrak{m}$. The statement of the theorem is equivalent to

$$K = k[x_1, \dots, x_n]/\mathfrak{m} \simeq k.$$

In fact, it is enough to take a_i the image of x_i by the isomorphism above.

Next, as k is algebraically closed, it is enough to show that K is algebraic over k. Up to renumbering, we may assume that $x_1, \dots x_r \in K$ are algebraically independent over k and that $x_{r+1}, \dots x_n$ are algebraic over $k(x_1, \dots, x_r)$, that is K is a $k(x_1, \dots, x_r)$-module of finite type. If $r = 0$, there is nothing to prove. Assume that $r > 0$.

We apply proposition 1.2.1, to $B = k(x_1, \dots x_r)$, $C = K$ and $A = k$, B is a k-algebra of finite type. We write

$$B = k[z_1, \dots, z_s]$$

with

$$z_i = \frac{P_i(x_1, \dots x_r)}{Q_i(x_1, \dots x_r)}, P_i, Q_i \in k[x_1, \dots x_r].$$

Let $f \in k[x_1, \dots, x_r]$ be an irreducible polynomial. We have $\frac{1}{f} \in B$. As $B = k[z_1, \dots z_s]$, we can write $1/f$ as a polynomial in z_i, in particular, this implies that f divides at least one Q_i. But there is only a finite number of polynomials verifying this property. As k is algebraically closed, it is in particular infinite. We then have an infinite family $(x - a)_{a \in k}$ of irreducible polynomials over k, contradiction. □

1.3 Additional exercises 1

1. Show that the polynomial $f(x,y) = y^2 - x(x-1)(x+1) \in k[x,y]$ is irreducible over any field. Deduce that $X = V(f)$ is an irreducible variety. Draw a picture in the case $k = \mathbb{R}$.

2. (a) Let $X = V(y - x^2)$. Show that $k[X]$ is isomorphic to the polynomial ring in one variable.

   (b) Let $X = V(xy - 1)$. Show that $k[X]$ is not isomorphic to the polynomial ring in one variable.

3. Let k be a non algebraically closed field.

   (a) Show that there exists a polynomial $f \in k[x,y]$ such that $V(f) = (0,0)$. Deduce that for any $n > 0$ there exists a polynomial $F \in k[x_1, \ldots, x_n]$ such that $V(F) = (0, \ldots, 0)$.

   (b) If X is an affine variety over k, show that X could be defined by a single equation.

4. Let k be an algebraically closed field.

   (a) Let $f, g \in k[x,y]$ with f an irreducible polynomial and g not divisible by$f$.

      i. Show that there exists $u, v \in k[x,y]$ and $h \in k[x] \setminus \{0\}$ such that $uf + vg = h$.

      ii. Deduce that the curves $V(f)$ and $V(g)$ intersect only in a finite number of points.

   (b) Let I ne a prime ideal in $k[x,y]$. Show that either $I = (f)$ with f an irreducible polynomial, or I is maximal.

5. (**Algebraic groups**) Let k be a field.

   (a) Show that the determinant $det(x_{ij})_{1 \leq i \leq n, 1 \leq j \leq n}$ is an irreducible polynomial in n^2 variables.

   (b) Show that $GL_n(k)$ is open in $M_n(k) \simeq k^{n^2}$ for the Zariski topology.

   (c) Show that for all $0 \leq r \leq n$ the set M_r od matrices of rank at most r is irreducible closed subset of M_k^n.

Chapter 2

Projective varieties and plane curves

2.1 Projective varieties

Let k be a field. One can view the projective space $\mathbb{P}_k^n$ as the set of lines in k^{n+1} passing by 0. More precisely, let $\sim$ be an equivalence relation on k^{n+1} where we set

$$x \sim y \text{ if and only if } x = \lambda y, \lambda \in k.$$

Definition 2.1.1. The projective space $\mathbb{P}_k^n$ is defined as a quotient

$$\mathbb{P}_k^n = k^{n+1} - \{0\}/\sim .$$

For $(x_0, \dots x_n) \in k^{n+1} - \{0\}$ we denote $(x_0 : \dots : x_n)$ the corresponding point of $\mathbb{P}_k^n$.

Example 2.1.2. We view $\mathbb{P}_k^2$ as the set of triples $(X : Y : Z)$ where at least one coordinate is nonzero and we identify

$$(X : Y : Z) = (\lambda X : \lambda Y : \lambda Z),\ \lambda \in k^*.$$

If $f \in k[x_0, \dots, x_n]$ is a homogeneous polynomial of degree d, we have by definition $f(\lambda x_0, \dots, \lambda x_n) = \lambda^d f(x_0, \dots, x_n)$. Projective varieties are then defined as zero loci in $\mathbb{P}_k^n$ of homogeneous polynomials in $k[x_0, \dots, x_n]$.

Definition 2.1.3. An ideal I in $k[x_0, \dots, x_n]$ is **homogeneous** if $I = (f_1, \dots, f_m)$ where $f_i, 1 \leq i \leq m$ are homogeneous polynomials.

One easily checks that I is homogeneous if and only if for any $f \in I$ the homogeneous components of f are also in I.

Definition 2.1.4. For I a homogeneous ideal in $k[x_0, \dots, x_n]$ we set

$$V_p(I) = \{x = (x_0 : \dots : x_n) \in \mathbb{P}_k^n \mid f(x) = 0\, \forall f \in I\}$$

the **projective algebraic variety** defined by I.

Definition 2.1.5. For X a subset of $\mathbb{P}_k^n$ we define $I_p(X)$ a homogeneous ideal generated by the homogeneous polynomials $f \in k[x_0, \ldots, x_n]$ such that $f(x) = 0 \, \forall x \in X$, we call $I_p(X)$ **the ideal** of X.

Example 2.1.6.

1. **A hyperplane** H in $\mathbb{P}_k^n$ is defined as zero locus of a linear form in $x_0, \ldots, x_n$:
$$H = V_p(a_0 x_0 + \ldots + a_n x_n),$$
where the coefficients $a_i \in k$ are not all zero.

2. More generally, a **hypersurface** of degree d in $\mathbb{P}_k^n$ is defined as zero locus of a homogeneous polynomial of degree d in $x_0, \ldots, x_n$.

3. In $\mathbb{P}_k^2$ we have :
   - a **line** $L \subset \mathbb{P}_k^2$ given by an equation $aX + bY + cZ = 0$.
   - a **conic** $C \subset \mathbb{P}_k^2$ given by a homogeneous equation of degree 2.

4. If $V = V_p(I)$ is a projective variety in $\mathbb{P}_k^n$, we call the **cone** $C(V)$ of V the affine variety in $\mathbb{A}_k^{n+1}$ defined by $C(V) = V(I)$.

Similarly as in the affine case, we have the following properties:

Proposition 2.1.7.

1. *Let I, J be homogeneous ideals in $k[x_0, \ldots, x_n]$. Then $I \subset J \Rightarrow V_p(J) \subset V_p(I)$.*

2. *If $X \subset Y$ are the subsets of $\mathbb{P}_k^n$, then $I_p(Y) \subset I_p(X)$.*

3. *If $X \subset \mathbb{P}_k^n$ is an algebraic variety, then $X = V_p(I_p(X))$.*

4. *If J is a homogeneous ideal in $k[x_0, \ldots, x_n]$, then $J \subseteq I_p(V_p(J))$.*

5. *If k is infinite and $V = V(I)$ is a projective variety in $\mathbb{P}_k^n$, then $I_p(V) = I(C(V))$.*

Proof. We give a proof for the last property, the others are similar to the affine case. The inclusion $I_p(V) \subseteq I(C(V))$ is straightforward. Let $f \in I(C(V))$. Write $f = \sum f_d \in k[x_0, \ldots, x_n]$ where f_d are the homogeneous components of f. Because V is a projective variety, if $(x_0, \ldots, x_n) \in C(V)$, then for any $\lambda \in k$ one has $(\lambda x_0, \ldots, \lambda x_n) \in C(V)$, so that the polynomial
$$g(\lambda) = f(\lambda x_0, \ldots, \lambda x_n) = \sum \lambda^d f_d(x_0, \ldots, x_n)$$
vanishes at any $\lambda \in k$. As k is infinite, $f_d(x_0, \ldots, x_n) = 0$ for any d, i.e. the homogeneous components of f are in $I_p(V)$, so that $I(C(V)) \subseteq I_p(V)$. □

The sets $V_p(I)$ are the closed sets of a topology, called (as in the affine case) *Zariski* topology on $\mathbb{P}_k^n$. If $X \subset \mathbb{P}_k^n$ is a projective variety, one gets the induced

topology on X.

Affine charts of $\mathbb{P}^n_k$. Let $\phi_i : \mathbb{A}^n_k \to \mathbb{P}^n_k$, $i = 0, \ldots, n$ be the morphism $(x_1, \ldots, x_n) \mapsto (x_1 : \ldots : x_{i-1} : 1 : x_i : \ldots x_n)$. It is clear that the space $\mathbb{P}^n_k$ is covered by the images of these maps ϕ_i. Let $U_i \subset \mathbb{P}^n_k$ be an open $\{x_i \neq 0\}$: it is a complement of the hyperplane $x_i = 0$. Let

$$\psi_i : U_i \to \mathbb{A}^k_n, (x_0 : \ldots : x_n) \mapsto (\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}.)$$

One immediately sees that ψ_i is an isomorphism, its inverse is the map ϕ_i. We call U_i the **affine charts** of $\mathbb{P}^n_k$.

In particular, we have the following affine charts for $\mathbb{P}^2_k$:

1. If $Z \neq 0$, we have $(X : Y : Z) = (\frac{X}{Z} : \frac{Y}{Z} : 1)$, so that we have an isomorphism ψ_Z between the open set $U_Z := \{Z \neq 0\}$ and $\mathbb{A}^2_k$
$$(X : Y : Z) \mapsto (\frac{X}{Z}, \frac{Y}{Z}),\ (x : y : 1) \leftarrow (x, y).$$
2. if $Y \neq 0$, one has $(X : Y : Z) = (\frac{X}{Y} : 1 : \frac{Z}{Y})$, so that we have an isomorphism ψ_Y between $U_Y := \{Y \neq 0\}$ and $\mathbb{A}^2_k$
$$(X : Y : Z) \mapsto (\frac{X}{Y} : 1 : \frac{Z}{Y}),\ (x : 1 : y) \leftarrow (x, y).$$
3. if $X \neq 0$, one has $(X : Y : Z) = (1 : \frac{Y}{X} : \frac{Z}{X})$, so that we have an isomorphism ψ_X between $U_X := \{X \neq 0\}$ and $\mathbb{A}^2_k$
$$(X : Y : Z) \mapsto (1 : \frac{Y}{X} : \frac{Z}{X}),\ (1 : x : y) \leftarrow (x, y).$$

Here is an example of changing the charts : $\psi_Y \circ \psi_Z^{-1} : (x, y) \mapsto (x : y : 1) \mapsto (\frac{x}{y}, \frac{1}{y})$ (if $y \neq 0$).

A homogeneous polynomial $f(x_0, \ldots, x_n)$ of degree d induces a polynomial map f_i on U_i given by $f_i(x_0, \ldots, x_{i-1}, 1, x_{i+1}, x_n)$. Conversely, if $f \in k[x_1, \ldots x_n]$ is a polynomial of degree d, we call the **homogenization** of f the homogeneous polynomial

$$f^*(x_0, \ldots, x_n) = x_0^d f(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}).$$

One can do a similar construction with x_i instead of x_0.

If I is a homogeneous ideal in $k[x_0, \ldots x_n]$, we are also interested to know if $V_p(I)$ is not empty. Of course, it does not hold for $I = (x_0, \ldots, x_n)$ or even if $I = (x_0^r, \ldots, x_n^r)$. A projective version of the Hilbert theorem of zeros claims that over an algebraically closed field these are the only such examples :

Theorem 2.1.8 (Homogeneous Nullstellensatz). *Let k be an algebraically closed field and let I be a homogeneous ideal in $k[x_0, \ldots, x_n]$.*

(i) $V_p(I) = \emptyset \Leftrightarrow \exists r > 0,\ (x_0, \ldots, x_n)^r \subset I$;

(ii) if $V_p(I) \neq \emptyset$, *then* $I_p(V_p(I)) = \sqrt{I}$.

Proof. (i) The implication $\Leftarrow$ is straightforward. Let us show the implication $\Rightarrow$. We have $V_p(I) = \emptyset \Leftrightarrow C(V) = \{(0, \ldots, 0) \in k^{n+1}\}$. Using the affine Nullstellensatz, this is equivalent to $\sqrt{I} = (x_1, \ldots, x_n)$, which implies that $\exists r > 0,\ (x_0, \ldots, x_n)^r \subset I$.

(ii) If $V_p(I) \neq \emptyset$, one has $I_p(V) = I(C(V)) = \sqrt{I}$ by 2.1.7 and by the affine Nullstellensatz theorem.

□

Examples of morphisms. Let $(f_0, \ldots f_m)$ be a family of homogeneous polynomials of degree d in n variables $x_0, \ldots, x_n$, with coefficients in a field k. If the polynomials f_i have no common zeros $(x_0, \ldots, x_n) \neq (0, \ldots, 0)$ (if k is algebraically closed, this means that the ideal $(x_0, \ldots, x_n)^r$ is contained in the the ideal generated by $f_1, \ldots, f_m$), so that one can define a map

$$F : \mathbb{P}^n_k \to \mathbb{P}^m_k, (x_0 : \ldots : x_n) \mapsto (f_0(x_0 : \ldots x_n), \ldots : f_m(x_0, \ldots x_n)).$$

More generally, let $X \subset \mathbb{P}^n_k$ and $Y \subset \mathbb{P}^m_k$ be two projective varieties. If $X \cap V(f_0, \ldots f_m) = \emptyset$ and if for all $x \in X$ we have $(f_0(x), \ldots, f_m(x)) \in Y$, then one can define a map

$$F : X \to Y, (x_0 : \ldots : x_n) \mapsto (f_0(x_0, \ldots x_n) : \ldots : f_m(x_0, \ldots x_n)).$$

Example 2.1.9.

1. A line in $\mathbb{P}^n_k$ is the image of a morphism $\mathbb{P}^1_k \to \mathbb{P}^n_k$ given by linear polynomials. As usual, there is a unique line passing through two given distinct points of $\mathbb{P}^n_k$.
2. Let $V \subset \mathbb{P}^2_k$ be a conic given by the equation $x^2 + y^2 - z^2 = 0$. We have a morphism $\mathbb{P}^1 \to V$, $(u : v) \mapsto (u^2 - v^2, 2uv, u^2 + v^2)$.
3. Let $k = \mathbb{F}_q$ be a finite field and let $V \subset \mathbb{P}^n_k$ be a projective variety. One defines the Frobenious map by $Fr : V \to V, (x_0 : \ldots : x_n) \mapsto (x_0^q : \ldots : x_n^q)$.

In this lectures we will be interested in affine and projective varieties, as well as in their products. A motivation to be interested in projective varieties (rather than in affine varieties) is the following result, which gives an exact number of points of intersection of two curves in the projective plane (for $\mathbb{A}^2_k$ the statement is no longer true as one can have for example two parallel lines).

Theorem 2.1.10 (Bézout's theorem)**.** *Let k be an algebraically closed field and let C_1, C_2 be two projective curves defined in $\mathbb{P}^2_k$ by homogeneous equations of degrees d_1 and d_2. The number of intersection points of C_1 and C_2 counted with multiplicities, is $d_1 d_2$.*

We will now give a proof of this theorem if C_1 is a line or a conic. These two cases are very important in order to define a group law on the points of an elliptic curve.

2.2 Some projective geometry

In this section k is an algebraically closed field. We start by two first cases of Bézout theorem.

Lemma 2.2.1. *Let $C \subset \mathbb{P}^2_k$ be a curve defined by a homogeneous polynomial of degree d and let $L \subset \mathbb{P}^2_k$ be a line not contained in C (as a component). Then the intersection $C \cap L$ consists of d points counted with multiplicities.*

Proof. Let $F(X, Y, Z) = 0$ be the homogenious equation of degree d defining the curve C and let $aX + bY + cZ = 0$ be the equation of the line L. Up to a permutation of the coordinates, one may assume that $a \neq 0$ and that the equation of the line is $X = -b'Y - c'Z$. The polynomial $f(Y, Z) = F(-b'Y - c'Z, Y, Z)$ is a nonzero homogeneous polynomial (as L is not contained in C) of degree d. As k is algebraically closed, one has a factorisation

$$f(Y, Z) = \alpha(Y - \alpha_i Z)^{m_i} \tag{2.1}$$

with $\sum m_i = d$. The points of intersection of L and C are given by the condition $f(Y, Z) = 0$, so that we have $\sum m_i = d$ of these points. □

Remark 2.2.2. Assume that k is not algebraically closed. If C, L and $d-1$ points of intersection of L and C are defined over k, then the proof above shows that $f(Y, Z)$ has a direct factor of degree $d - 1$ defined over k. We then get that the decomposition (2.1) exists over k and all d intersection points of L and C are defined over k.

Lemma 2.2.3. *Let $C \subset \mathbb{P}^2_k$ be a curve defined by a homogeneous polynomial of degree d and let $D \subset \mathbb{P}^2_k$ be a conic not contained in C. Then $C \cap D$ consists of $2d$ points counted with multiplicities.*

Proof. Let $F(X, Y, Z) = 0$ be a homogeneous equation of degree d defining the curve C. If the conic D is reducible, D is a union of two lines, so that the statement follows from the previous lemma. Up to a linear change of coordinates, one can assume that the conic is given by an equation $XY - Z^2 = 0$, i.e. that D is

the image of the morphism $\mathbb{P}^1 \to \mathbb{P}^2, (u : v) \mapsto (u^2 : v^2 : uv)$. The polynomial $f(u, v) = F(u^2, v^2, uv)$ is a nonzero homogeneous polynomial (as D is not contained in C) of degree $2d$. As k is algebraically closed, we have a factorization $f(Y, Z) = \alpha(Y - \alpha_i Z)^{m_i}$ with $\sum m_i = 2d$. The intersection points of D and C are given by the condition $f(u, v) = 0$, so that we have $\sum m_i = 2d$ of such points. □

In the next statements we will be interested to describe the plane curves passing by some given points. In general, the set of hypersurfaces of degree d in $\mathbb{P}_k^N$ gives also a projective space with coordinates corresponding to the coefficients. For example, a conic in $\mathbb{P}_k^2$ is given by a homogeneous equation $q(X, Y, Z) = \sum a_{ijs} X^i Y^j Z^s$ with $i + j + s = 2$, so that one has 6 coefficients. One associates to a conic the vector of its coefficients. The set of all the forms $q(X, Y, Z)$ is then a vector space of dimension 6. Two forms define the same conic if they differ by a multiplication by a scalar. The set of the conics is then a projective space $\mathbb{P}_k^5$.

Lemma 2.2.4. *Let $P_1, \ldots, P_5$ be distinct points in $\mathbb{P}_k^2$. There exists a conic in $\mathbb{P}_k^2$ containing these points. If no four of these points are on a line, the conic is unique.*

Proof. A conic C in $\mathbb{P}_k^2$ is given by a homogeneous equation $q(X, Y, Z) = \sum a_{ijs} X^i Y^j Z^s$ with $i+j+s = 2$. The k-vector space V of coefficients of conics is then of dimension 6. The condition that the conic C passes by a point gives a linear condition on this space. The coefficients of a conic passing by 5 points are then the solutions of a system of 5 linear equations in a space of dimension 6, so that there is always a conic passing by 5 points.

Assume that 3 points, say, P_1, P_2, P_3 are on a line. Let L be the line P_1P_2. The equation q of the conic C is then divisible by the equation of L and q vanishes at P_4 and P_5. As P_4 and P_5 are not on L, the conic C is a union of two lines $L \cup P_4P_5$.

Assume that no three points from $P_1, \ldots, P_5$ are on a line. Let P_6 be a point on the line $L = P_1P_2$, distinct from P_1 and P_2. Assume that the dimension of the k-vector space of the equations of conics passing by the points $P_1, \ldots, P_5$ is at least 2. Then there is a conic containing $P_1, \ldots, P_6$: in fact the condition that the conic passes through a given point is a linear condition. As the points P_1, P_2, P_6 are on a line, C is a union of L and another line, so that $P_3, \ldots, P_5$ are on a line, contradiction. □

Lemma 2.2.5. *Let $P_1, \ldots, P_8$ be distinct points of $\mathbb{P}_k^2$, no four of these points on a line, no seven on the same conic. Let V be a k-vector space of homogeneous polynomials of degree 3 vanishing at $P_1, \ldots, P_8$. Then* $\dim V = 2$.

Proof. The k-vector space W of coefficients of a cubic is of dimension 10, so that $\dim V \geq 10 - 8 = 2$. We have the following cases to consider :

1. Assume P_1, P_2, P_3 are on a line, let L be a corresponding line. Let P_9 be a point (distinct from P_1, P_2, P_3) on this line. The vector space of cubics

passing by these nine points is of dimension $\dim V - 1$. If a cubic C passes by $P_1, \ldots, P_9$, then the intersection of C and L contains at least 4 points, so that C is the union $L \cup Q$ for Q a conic. Using the hypothesis, Q contains $P_4, \ldots, P_8$. Using lemma 2.2.4, there exists just one such conique. We get $\dim V - 1 \leq 1$, and the result follows.

2. Assume that $P_1, P_2, \ldots, P_6$ are on a conic Q. Let P_9 be another point on this conic. We have again that any conic containing $P_1, \ldots P_9$ should contain Q, so that one gets $C = Q \cup L$. Using the hypothesis, $L = P_7P_8$. We obtain again $\dim V - 1 \leq 1$ and the claim follows.

3. General case : no three points among $P_1, \ldots, P_8$ are on a line, no six are on a conic. Let P_9, P_{10} be on a line $L = P_1P_2$ different from P_1 and P_2. Assume $\dim V > 2$. There is a cubic C passing by $P_1, \ldots, P_{10}$, so that this cubic contains the line L, so that it is a union of L and another conic. We get a contradiction with the hypothesis on $P_1, \ldots, P_8$.

□

Lemma 2.2.6. *Let C_1 and C_2 be two cubics in $\mathbb{P}^2_k$. Assume that C_1 is irreducible. Assume that we have 9 points $P_1, \ldots P_9$ of intersection of C_1 and C_2, such that the points $P_1, \ldots, P_8$ are distinct. If a cubic C contains the points $P_1, \ldots, P_8$, then it contains the point P_9.*

Proof. The cubic C_1 does not contain 4 points on a line: if not, using lemma 2.2.1, we would get that C_1 contains a line, which is not possible since C_1 is irreducible. Similarly, C_1 does not contain 7 points on a conic. The points $P_1, \ldots, P_8$ satisfy the hypothesis of lemma 2.2.5 and the vector space over k of homogeneous polynomials of degree 3 vanishing at $P_1, \ldots, P_8$ is of dimension 2. We deduce that it is generated by C_1 and C_2. Then the equation of the cubic C is a linear combination of the equations of C_1 and C_2, in particular, it vanishes at P. □

2.3 Additional exercises 2

1. Let k be an algebraically closed field and let $q(X, Y, Z)$ be a quadratic form over k in three variables. Let $Q = V_p(q) \subset \mathbb{P}^2_k$. Show that Q is either a union of two lines or Q is an irreducible conic which is defined by the equation $XY - Z^2$, up to a linear change of coordinates.

2. Let k be an infinite field, let $\Phi : \mathbb{P}^1_k \to \mathbb{P}^3_k$ be the morphism

$$\Phi(x, y) = (x^3, x^2y, xy^2, y^3)$$

and let X be the image of Φ.

(a) Show that $X = V(I)$ where $I = (XT - YZ, Y^2 - XZ, Z^2 - YT)$ in the homogeneous coordinates $(X : Y : Z : T)$ of $\mathbb{P}^3_k$.

(b) Show that $I(X) = I$ (show first that any homogeneous $f \in k[X, Y, X, T]$ could be written modulo I as $f = a(X, T) + b(X, T)Y + c(X, T)Z$).

(c) Show that I can not be defined by two generators.

(d) Show that X could be written as $X = V(Z^2 - YT, P)$ where P is a homogeneous polynomial of degree 3.

Chapter 3

Elliptic curves : first properties

3.1 Eliiptic curves and the group law

An image. Assume we have a pyramide with n bowls. If the pyramide falls down, could one arrange the bowls in a square?

Let x be the height of the pyramide. We are looking for the solutions of

$$y^2 = x(x+1)(2x+1)/6.$$

This equation defines an elliptic curve. One can show (this is not at all obvious!) that the only integral solutions are $(1,1)$ and $(24,70)$.

Let k be a field and $C \subset \mathbb{P}^2_k$ be a plane curve defined by a homogeneous equation $F(X,Y,Z) = 0$.

Definition 3.1.1. The curve C is **smooth** at a point $P \in C$ if

$$(\partial F/\partial X(P), \partial F/\partial Y(P), \partial F/\partial Z(P)) \neq (0,0,0).$$

If this is the case, the tangent line to C at P is the line

$$\frac{\partial F}{\partial X}(P)X + \frac{\partial F}{\partial Y}(P)Y + \frac{\partial F}{\partial Z}(P)Z = 0.$$

The curve C is **smooth** if it is smooth at all its points.

For the most general definition of an elliptic curve, one takes a smooth plane curve E defined by a homogeneous equation of degree 3 with $E(k) \neq \emptyset$. One can show, that one can define such curve by the following equation, called **the Wierstrass form** of E, the definition that we will use for this course.

Definition 3.1.2. An **elliptic curve** E is a plane curve defined by the equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \text{ with } 4a^3 + 27b^2 \neq 0. \tag{3.1}$$

We have $E(k) \neq \emptyset$: the point $O_E = (0:1:0)$ is in E. We call $\Delta = -(4a^3 + 27b^2)$ the **discriminant** of E.
Following the context, we also call **elliptic curve** an *affine* curve defined by the equation

$$y^2 = x^3 + ax + b, \tag{3.2}$$

with the same conditions for a and b: it is an open $\{Z \neq 0\}$ of the curve defined by the equation (3.1). The complement of this open contains only the point O_E. The conditions on a and b are justified by the following lemma:

Lemma 3.1.3. *(i) The plane curve C defined by the quation $Y^2Z = X^3 + aXZ^2 + bZ^3$ is smooth if and only if $\Delta = -(4a^3 + 27b^2) \neq 0$.*

(ii) Let e_1, e_2, e_3 be the roots od $f(x) = x^3 + ax + b$ in an algebraic closure $\bar{k}$ of k: $f(x) = (x - e_1)(x - e_2)(x - e_3)$. Then

$$\Delta = [(e_1 - e_2)(e_1 - e_3)(e_2 - e_3)]^2.$$

Proof. exercise. □

If P is a point of an elliptic curve E, we write $P = (X_P : Y_P : Z_P)$ in the projective coordinates (3.1) or $P = (x_P, y_P)$ in the affine coordinates (3.2), if $P \neq O_E$. The fundamental result in the theory of elliptic curves, which is also the base of the cryptographical applications, is that the points of an elliptic curve form an abelian group.

The group law: definition. Let E be an elliptic curve given by an affine equation (3.2). Let $P \neq Q \in E(k)$. Since E is defined by an equation of degree 3, the line $L = PQ$ intersects E in the third point R (see lemma 2.2.1 and the remark after the lemma), eventually $R = O_E$. We define $P + Q = -R$ where the point $-R$ is the point $(X_R : -Y_R : Z_R)$. If $P = Q$ we take for L the tangent line at P. We define also $P + O_E = O_E + P$, $O_E + O_E = O_E$.

Theorem 3.1.4. *The composition law on $E(k)$ as defined above is a group law. This law is commutative, the neutral element is O_E.*

Proof. The commutativity follows easily from the definition, also it is straightforward that O_E is the neutral element and that $-P$ is the inverse of a point P. The most difficult part is to establish the associativity, that we will do in the next section using some results from the projective geometry. □

There are also explicit formulas for the group law of an elliptic curve :

Proposition 3.1.5. *Let $P, Q \in E(k)$ be two points distinct from O_E.*

1. $-P = (x_P, -y_P)$;

2. *If $P = Q$ let $\lambda = (3x_P^2 + a)/2y_P$ and $\mu = y_P - \lambda x_P$. Then*

$$P + Q = (\lambda^2 - x_P - x_Q, -\lambda^3 + \lambda(x_P + x_Q) - \mu).$$

3. *If $P \neq Q$ let $\lambda = \frac{y_P - y_Q}{x_P - x_Q}$ and $\mu = y_P - \lambda x_P$. Then $\lambda = \frac{x_P^2 + x_P x_Q + x_Q^2 + a}{y_P + y_Q}$ and*

$$P + Q = (\lambda^2 - x_P - x_Q, -\lambda^3 + \lambda(x_P + x_Q) - \mu).$$

Proof. The formula for $-P$ follows from the definition. Let L be the line PQ if $P \neq Q$ and the tangent line to E at P, if $P = Q$. It follows from the definition of λ and μ that the line L is given by the equation $y = \lambda x + \mu$. Let R be the third point of intersection of the line L with the curve E. We have $P + Q = (x_R, -y_R)$. The x-coordinate of the point R is the solution of

$$0 = x^3 + ax + b - (\lambda x + \mu)^2 = x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)x + (b - \mu^2).$$

Since x_P and x_Q satisfy this equation, one deduces the expressions of the third solution as claimed. □

The following formulas are also useful:

Proposition 3.1.6. 1. $x_{P+Q} + x_{P-Q} = \frac{2(x_P + x_Q)(a + x_P x_Q) + 4b}{(x_P - x_Q)^2}$.

2. $x_{P+Q} x_{P-Q} = \frac{(x_P x_Q - a)^2 - 4b(x_P + x_Q)}{(x_P - x_Q)^2}$.

3. $x_{2P} = \frac{x_P^4 - 2ax_P^2 - 8bx_P + a^2}{4(x_P^3 + ax_P + b)}$.

Proof. One verifies the identities of the proposition using the explicit group law 3.1.5. □

3.2 The associativity of the group law

General case

We take $P, Q, R \in E(k)$ three distinct points. We set
L_1 is the line PQ, T is the third intersection point with E;
L_2 is the line TO_E, $T' = -T$ is the third intersection point with E;
L_3 is the line RT', U is the third intersection point with E;
M_1 is the line QR, S is the third intersection point with E;
M_2 is the line SO_E, $S' = -S$ is the third intersection point with E;
M_3 is the line PS', V is the third intersection point with E;
From this construction, $(P + Q) + R = -U$ et $P + (Q + R) = -V$ we want to show that $U = V$.

Let $C_1 = L_1 + M_2 + L_3$ and $C_2 = M_1 + L_2 + M_3$ be two cubics. We have $E \cap C_1 = \{P, Q, R, O_E, T, T', S, S', U\}$ and $E \cap C_2 = \{P, Q, R, O_E, T, T', S, S', V\}$. Assume that the points $P, Q, R, O_E, T, T', S, S', U$ are all distinct. Using lemma 2.2.6 for E and C_1, we then have $U = V$. We establish the remaining cases below, using the explicit group law.

Associativity of the group law : end of proof.

In the notation of the general case, we established the associativity if the points $P, Q, R, O_E, T, T', S, S'$ are all distinct. The remaining cases are :

1. At least one of the points $P, Q, R, T, T', S, S', U, V$ is the point O_E.

   (a) If $O_E \in \{P, Q, R\}$, we have $(P + Q) + R = P + (Q + R)$ using the definition of the sum with O_E.

   (b) Assume that no point from P, Q, R is the point O_E. Using the construction, $T = O_E$ iff $T' = O_E$. Assume this is the case. We then have $Q = -P$. We want to show that $R = (P + (-P)) + R = P + ((-P) + R)$, which is clear from the definition and the following argument using the symmetry with respect to the line $y = 0$. In fact, let D be the line passing by $-P$ and R and K be the thrd intersection point of D with E. We then have $-P + R = -K$. The line D' passing by P and $-K$ is symmetric to D. The third intersection point of D' eand E is then the point $-R$, so that $P + (-K) = R$, as claimed. The case $S = O_E$ is similar. Note that this case also implies that for two points W and W_1 of E we have

   $$W = W_1 \Leftrightarrow (-P) + W = (-P) + W_1.$$

   In fact, the implication $\Rightarrow$ is straightforward and fo the implication $\Leftarrow$ we observe that $P + ((-P) + W) = (P + (-P)) + W = W$, similarly for W_1.

   (c) Assume that $U = O_E$, i.e. that $R = -(P + Q)$. We want to show that

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

   The left side is O_E. We have

   $$O_E = P + (Q + (-(P + Q))) \Leftrightarrow -P = Q + (-(P + Q)) \Leftrightarrow -P + (-Q) = -(P + Q),$$

   which follows by a symmetry argument. The case $V = O_E$ is similar.

2. Assume that

   (*) $O_E \notin \{P, Q, R, T, T', S, S', U, V\}$ and no couple $(P, Q), (Q, R), (P + Q, R), (P, Q + R)$ contains two same points.

Let E^0 be the affine open $E \setminus \{O_E\}$ of the curve E and let A be the affine variety $E^0 \times E^0 \times E^0$. One checks that the variety A is irreducible, so that any open of A is irreducible as well. Let $A' \subset A$ be the open $\{P \neq Q, P \neq -Q, Q \neq R, Q \neq -R\}$. Using the explicit group law, for any $(P, Q, R) \in A'$, the coordinates of the points $P + Q$ and $Q + R$ are given by the formulas 3.1.5.3, in particular $x_{P+Q} = f(x_P, x_Q, y_P, y_Q)$ where $f = f_1/f_2$ is the rational fraction with non zero denominator, similarly for $y_{P+Q} = g_1/g_2$. The condition $P + Q = R$ is given by the polynomial conditions $f_1 - x_R f_2 = 0$, $g_1 - y_R g_2 = 0$. Similarly for the condition $P = Q + R$. We deduce that the locus of points $(P, Q, R) \in A'$ where the condition $(*)$ is satisfied is an open A'' of A'. By the the argument as above, for any $(P, Q, R) \in A''$, we express the coordinates of the points $P + Q, (P + Q) + R, Q + R, P + (Q + R)$ via the formulas 3.1.5.3, in particular, the locus of the points $(P, Q, R) \in A''$ such that $(P+Q)+R = P+(Q+R)$ is a closed set B of A''. But this closed set contains an open corresponding to the general case, where all the points $P, Q, R, T = -(P+Q), T' = (P+Q), S = -(Q+R), S' = (Q+R), O_E, U = -((P+Q)+R)$ are distincts. As A'' is irreducible, any open set is dense, so that $B = A''$ and we get that for all (P, Q, R) satisfying $(*)$ we have $(P+Q)+R = P+(Q+R)$.

3. The case where the points $P, Q, R, P + Q, Q + R$ are not all distinct and no point among $P, Q, R, T, T', S, S', U, V$ is O_E is left as an exercise.

Chapter 4

Elliptic curves over finite fields

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ with $q = p^n$ and p prime. The famous Hasse theorem allows to estimate the (finite) number of points $E(\mathbb{F}_q)$:

Theorem 4.0.1. [Hasse] *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Then*

$$|\#E(\mathbb{F}_q) - q - 1| < 2\sqrt{q}.$$

It is also known[1] that for any integer a prime to p and such that $|a| < 2\sqrt{q}$ there exists an elliptic curve E over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - a$.

We start by an approach coming from the analytic number theory, This method allows to establish the Hasse theorem in two particular cases : $q = p$ and E given by $y^2 = x^3 + D$ or $y^2 = x^3 - Dx$, where D is a nonzero integer.

4.1 Characters, Gauss and Jacobi sums.

Definition 4.1.1. A **multiplicative character** on $\mathbb{F}_p$ is a map $\chi : \mathbb{F}_p^* \to \mathbb{C}^*$ such that $\chi(ab) = \chi(a)\chi(b)$.

Proposition 4.1.2. *Let χ be a multiplicative character and let $a \in \mathbb{F}_p^*$. Then*

(i) $\chi(1) = 1$*;*

(ii) $\chi(a)^{p-1} = 1$*, i.e.* $\chi(a)$ *is a* $(p-1)$*-th root of unity;*

(iii) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Proof. (i) We use that $\chi(1) = \chi(1) \cdot \chi(1)$ and that $\chi(1) \neq 0$ by definition.

(ii) For $a \in \mathbb{F}_p^*$, we have $a^{p-1} = 1$. Hence $(\chi(a))^{p-1} = \chi(a^{p-1}) = \chi(1) = 1$ by (i).

(iii) We have $\chi(a)\overline{\chi(a^{-1})} = \chi(aa^{-1}) = 1$, so that $\chi(a^{-1}) = \chi(a)^{-1}$. By (ii), $|\chi(a)|^2 = \chi(a)\overline{\chi(a)} = 1$.

□

Exemples :

[1] this result uses more difficult techniques and can not be considered for this course.

1. the Legendre symbol (a/p) is a character;

2. the trivial character : $\epsilon(a) = 1$ for all $a \in \mathbb{F}_p^*$.

3. Recall that $\mathbb{F}_p^*$ is a cyclic group of order $p-1$. Let g be a generator of this group. In order to definie a multiplicative character on $\mathbb{F}_p$ it is enough to give its value at g. We define the character $\lambda : \mathbb{F}_p^* \to \mathbb{C}$ by $\lambda(g) = e^{2\pi i/(p-1)}$ (so that we have $\lambda(g^k) = e^{2\pi ik/(p-1)}$). We have $\lambda^{p-1} = 1 : \lambda(g)^{p-1} = \lambda(g^{p-1}) = \lambda(1) = 1$. In addition, if n is such that $\lambda^n = 1$, we have $\lambda(g)^n = \lambda(g^n) = e^{2\pi in/(p-1)} = 1$, so that we should have $p - 1 \,|\, n$.

4. One could extend the character χ to $\mathbb{F}_p$ by : $\chi(0) = 0$ if $\chi \neq \epsilon$ and $\chi(0) = 1$ if $\chi \neq \epsilon$.

The set of characters is a group: if χ, λ are two characters, we set $(\chi\lambda)(a) = \chi(a)\lambda(a)$ et $\chi^{-1}(a) = (\chi(a))^{-1}$.

Proposition 4.1.3. *The group of characters is a cyclic group of order $p-1$. If $a \in \mathbb{F}_p^*, a \neq 1$, then there exists a character χ such that $\chi(a) \neq 1$.*

Proof. Using the example 3 above, a character χ is determined by the value $\chi(g)$ and, by proposition 4.1.2, $\chi(g)$ is the $(p-1)$-th root of unity. We then have at most $p-1$ characters. Again using example 3, the characters $\epsilon, \lambda, \lambda^2, \ldots, \lambda^{p-1}$ are all distinct, so that we get exactly $p-1$ characters over $\mathbb{F}_p$ and the group of characters is cyclic. If $a \in \mathbb{F}_p^*, a \neq 1$, then $\lambda(a) \neq 1$. □

Proposition 4.1.4. *(i) For $\chi \neq \epsilon$ a multiplicative character we have $\sum_{a \in \mathbb{F}_p} \chi(a) = 0$.*

(ii) For $a \in \mathbb{F}_p^*, a \neq 1$ we have $\sum_\chi \chi(a) = 0$.

Proof. (i) Since $\chi \neq \epsilon$, there exists $b \in \mathbb{F}_p$ such that $\chi(b) \neq 1$. One checks that $\chi(b) \sum_{a \in \mathbb{F}_p} \chi(a) = \sum_{a \in \mathbb{F}_p} \chi(a)$, so that $\sum_{a \in \mathbb{F}_p} \chi(a) = 0$.

(ii) Using the previous proposition, there exists a character λ such that $\lambda(a) \neq 1$. We then get $\lambda(a) \sum_\chi \chi(a) = \sum_\chi \chi(a) = 0$.

□

The next two statements show how one can use the characters to solve the equations over $\mathbb{F}_p$.

Lemma 4.1.5. *Let $a \in \mathbb{F}_p^*$.*

1. *The equation $x^n = a$ has a solution iff $a^{p-1/d} = 1$ where $d = (n, p-1)$.*

2. *Assume that $n \,|\, p-1$. If the equation $x^n = a$ has no solution, there exists a caracter χ such that $\chi(a) \neq 1$ and $\chi^n = \epsilon$.*

Proof. 1. Follows from the fact that the group $\mathbb{F}_p^*$ is cyclic of order $(p-1)$.

2. Let g and λ be as in example 3 above. Let $n' = p - 1/n$. Let $\chi = \lambda^{n'}$. We then have $\chi^n = \epsilon$. Let us write $a = g^s$, we have that n does not divide s under the assumption that the equation $x^n = a$ has no solution. We deduce $\chi(a) = \chi(g)^s = e^{2\pi i(s/n)} \neq 1$.

□

Proposition 4.1.6. *Let $a \in \mathbb{F}_p^*$. Let n be an integer such that $n|p-1$. Let $N(x^n = a)$ be the number of solutions in $\mathbb{F}_p^*$ of the equation $x^n = a$. We have*

$$N(x^n = a) = \sum_{\chi, \chi^n = \epsilon} \chi(a).$$

Proof. 1. If $a = 0$ then $N(x^n = a) = 1$ and $\sum_{\chi,\chi^n=\epsilon} \chi(0) = 1$ as for any character $\chi \neq \epsilon, \chi(0) = 0$.

2. Assume that the equation $x^n = a$ has a solution : $a = b^n$. Note that, as the group of characters is cyclic, one has exactly n characters such that $\chi^n = \epsilon$. For such character χ we have $\chi(a) = \chi(b^n) = \chi(b)^n = \chi^n(b) = \epsilon(b) = 1$. We get $\sum_{\chi,\chi^n=\epsilon} \chi(a) = n = N(x^n = a)$.

3. Assume that the equation $x^n = a$ has no solution. Let χ as in the part 2 of the proposition above. We have $\chi(a) \sum_{\chi',\chi'^n=\epsilon} \chi'(a) = \sum_{\chi',\chi'^n=\epsilon} \chi'(a)$, so that $\sum_{\chi',\chi'^n=\epsilon} \chi'(a) = 0$ as $\chi(a) \neq 1$.

□

Definition 4.1.7. Let χ be a character of $\mathbb{F}_p$ and let $a \in \mathbb{F}_p$. Let $\zeta = e^{2\pi i/p}$. We define

$$g_a(\chi) = \sum_{t \in \mathbb{F}_p} \chi(t)\zeta^{at}$$

the Gauss sum of the character χ. One defines $g(\chi) = g_1(\chi)$.

Lemma 4.1.8. $g_a(\chi) = \begin{cases} \chi(a^{-1})g_1(\chi) & a \neq 0, \chi \neq \epsilon \\ 0 & a \neq 0, \chi = \epsilon \\ 0 & a = 0, \chi \neq \epsilon \\ p & a = 0, \chi = \epsilon. \end{cases}$

Proof. 1. Assume $a \neq 0, \chi \neq \epsilon$. Then $\chi(a)g_a(\chi) = \sum_{t \in \mathbb{F}_p} \chi(at)\zeta^{at} = g_1\chi$.

2. Assume $a \neq 0, \chi = \epsilon$. Then $g_a(\chi) = \sum_{t \in \mathbb{F}_p} \zeta^{at} = \frac{1-\zeta^{ap}}{1-\zeta^a} = 0$.

3. Assume $a = 0, \chi \neq \epsilon$. Then $g_a(\chi) = \sum_{t \in \mathbb{F}_p} \chi(t) = 0$ by proposition 4.1.4.

4. Assume $a = 0, \chi = \epsilon$. Then $g_a(\chi) = \sum_{t \in \mathbb{F}_p} 1 = p$.

□

Proposition 4.1.9. *If $\chi \neq \epsilon$, $|g(\chi)| = \sqrt{p}$.*

Proof. We write $S(\chi) = \sum_a g_a(\chi)\overline{g_a(\chi)}$. By the lemma above, for $a \neq 0$ one has

$$g_a(\chi)\overline{g_a(\chi)} = \chi(a^{-1})\chi(a)g(\chi)\overline{g(\chi)} = |g(\chi)|^2.$$

Since $g_0(\chi) = 0$ by the lemma above, one has $S(\chi) = (p-1)|g(\chi)|^2$. We also have

$$S(\chi) = \sum_a (\sum_u \sum_v \chi(u)\overline{\chi(v)})\zeta^{a(u-v)}.$$

But $\sum_t \zeta^{ct} = p$ if $c = 0$ and $\sum_t \zeta^{ct} = \frac{1-\zeta^{cp}}{1-\zeta^c} = 0$ if $c \neq 0$. We get

$$S(\chi) = \sum_u \sum_v \chi(u)\overline{\chi(v)}\delta(u,v)p = (p-1)p.$$

We then get $(p-1)|g(\chi)|^2 = (p-1)p$, and result follows.

□

Definition 4.1.10. Let χ and λ be two characters in $\mathbb{F}_p$. The Jacobi sum $J(\chi, \lambda)$ is defined by $J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$.

Proposition 4.1.11. *Let χ and λ be two characters in $\mathbb{F}_p$.*

(i) $J(\epsilon, \epsilon) = p$;

(ii) for $\chi \neq \epsilon$, one has $J(\epsilon, \chi) = 0$;

(iii) for $\chi \neq \epsilon$, one has $J(\chi, \chi^{-1}) = -\chi(-1)$;

(iv) if $\chi\lambda \neq \epsilon$ then $J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$;

(v) if $\chi\lambda \neq \epsilon$ then $|J(\chi, \lambda)| = \sqrt{p}$.

Proof. The statement (i) us straightforward, the statement (ii) follows from proposition 4.1.4, the statement (v) follows from (iv). Let us show (iii). We have

$$J(\chi, \chi^{-1}) = \sum_{a+b=1} \chi(a)\chi^{-1}(b) = \sum_{a+b=1, b\neq 0} \chi(a/b) = \sum_{a \neq 1} \chi(a/1-a) = [c = 1/1-a] = \sum_{c \neq -1} \chi(c) = [\text{par } 4.1.4] = -\chi(-1).$$

Let us show (iv). We have

$$g(\chi)g(\lambda) = (\sum_a \chi(a)\zeta^a)(\sum_b \lambda(b)\zeta^b) = \\ = \sum_{a,b} \chi(a)\lambda(b)\zeta^{a+b} = \sum_t (\sum_{a+b=t} \chi(a)\lambda(b))\zeta^t.$$

If $t = 0$, we get $\sum_a \chi(a)\lambda(-a) = \lambda(-1)\sum_a (\chi\lambda)(a) = 0$ par la proposition 4.1.4. If $t \neq 0$, we get $\sum_{a+b=t} \chi(a)\lambda(b) = \sum_{a'+b'=1} \chi(a't)\lambda(b't) = (\chi\lambda(t))J(\chi,\lambda)$. We then get $g(\chi)g(\lambda) = \sum_t (\chi\lambda(t))\zeta^t J(\chi,\lambda) = J(\chi,\lambda)g(\chi\lambda)$. □

4.2 Hasse theorem : particular cases

4.2.1 Case $E : y^2 = x^3 + D$

Let $p \geq 5$ be a prime and let E be an elliptic curve over $\mathbb{F}_p$ defined by a homogeneous equation $y^2z = x^3 + Dz^3$, $D \neq 0$. Let N_p be the set of points $E(\mathbb{F}_p)$. As E has a point at infinity, one has

$$N_p = 1 + N(y^2 = x^3 + D).$$

We have two cases to consider:

1. Assume $p \equiv 2(mod\ 3)$. Then $(p-1, 3) = 1$ and the map $x \mapsto x^3$ is an automorphism of $\mathbb{F}_p^*$. For a fixed $a = y^2$ the equation $x^3 = a^2 - D$ has a unique solution. We get $N(y^2 = x^3 + D) = p$ and $N_p = 1 + p$.

2. $p \equiv 1(mod\ 3)$. Let χ be a primitive multiplicative character of order 3 and ρ the multiplicative character of order 2 over $\mathbb{F}_p^*$. We have

$$N(y^2 = x^3 + D) = \sum_{a+b=D} N(y^2 = a)N(x^3 = -b) = [\text{par } 4.1.6] \\ = \sum_{a+b=D} (1 + \rho(a))(1 + \chi(-b) + \chi^2(-b)) = \\ = p + \sum_{a+b=D} \rho(a)\chi(b) + \sum_{a+b=D} \rho(a)\chi^2(b) = [a = Da', b = Db'] \\ = p + \rho\chi(D)J(\rho,\chi) + \overline{\rho\chi(D)J(\rho,\chi)}.$$

As $|J(\rho,\chi)| = \sqrt{p}$ by proposition 4.1.11, we deduce $|N_p - 1 - p| < 2\sqrt{p}$. □

4.2.2 Case $E : y^2 = x^3 - Dx$

Let E be an elliptic curve over $\mathbb{F}_p$, $p \geq 2$, defined by a homogeneous equation $y^2z = x^3 - Dxz^2$, with $D \neq 0$. Let N_p be the set of points $E(\mathbb{F}_p)$. As in the previous case, we have

$$N_p = 1 + N(y^2 = x^3 - Dx).$$

Lemma 4.2.1. *Let C be an affine curve $y^2 = x^3 - Dx$ and let C' be an affine curve $u^2 = v^4 + 4D$. Let*

$$T : \mathbb{A}^2 \to \mathbb{A}^2$$
$$u, v \mapsto \frac{u + v^2}{2}, \frac{v(u + v^2)}{2}$$

and let

$$S : \mathbb{A}^2 \to \mathbb{A}^2$$
$$x, y \mapsto 2x - \frac{y^2}{x^2}, \frac{y}{x}.$$

Then T maps C' to C and S maps $C \setminus \{0, 0\}$ to C'. In addition, the restriction $T \circ S | C \setminus \{0, 0\}$ is the identity on C' and the restriction of $S \circ T$ to C' is the identity on C.

Proof. Straightforward verification using definitions of the applications T and S. □

Let $N' = N(u^2 = v^4 + 4D)$. Using the lemma above, $N_p = 2 + N'$. We have two cases to consider:

1. Assume $p \equiv 3 (mod\ 4)$. Then -1 is not a square, i.e. any element $a \in \mathbb{F}_p$ could be written as $a = \pm b^2$. In particular, $a^2 = b^4$, i.e. any square is a 4^{th} power. Hence $N' = N(y^2 = v^4 + 4D) = N(u^2 = v^2 + 4D) = p - 1$ and $N_p = 2 + N' = 1 + p$.

2. $p \equiv 1 (mod\ 4)$. Let λ be multiplicative character of order 4 and $\rho = \lambda^2$. We have

$$N(u^2 = v^4 + 4D) = \sum_{a+b=4D} N(u^2 = a)N(v^4 = -b) = [\text{car } J(\rho, \rho) = -1] =$$
$$= p - 1 + \overline{\lambda(-4D)} J(\rho, \lambda) + \lambda(-4D)\overline{J(\rho, \lambda)}.$$

   As $|J(\rho, \lambda)| = \sqrt{p}$ by proposition 4.1.11, we deduce $|N_p - 1 - p| < 2\sqrt{p}$. □

4.3 Endomorphisms

In this section k is an algebraically closed field.

Definition 4.3.1. Let E be an elliptic curve defined over k. We define an **endomorphism** of E as a map $\alpha : E \to E$ given by rational functions and verifying

$$\alpha(P + Q) = \alpha(P) + \alpha(Q).$$

If E is given by affine equation (3.2), one can write

$$\alpha(x,y) = (R_1(x,y), R_2(x,y)).$$

In what follows, we will express α in a easier way and in particular definie α at the points where the denominator of R_1 or R_2 vanishes (in projective coordinates.)

Since $(x,y) \in E$, we may assume that the fractions R_1, R_2 do not have terms in y^2 and write

$$R_i(x) = \frac{p_1^i(x) + p_2^i(x)y}{q_1^i(x) + q_2^i(x)y} = \frac{(p_1^i(x) + p_2^i(x)y)(q_1^i(x) - q_2^i(x)y)}{(q_1^i(x))^2 - (q_2^i(x))^2(x^3 + ax + b)} = \frac{r_1^i(x) + r_2^i(x)y}{q^i(x)}$$

for some polynomials r_1^i, r_2^i, q^i.

Next, since α is an endomorphism, we have $\alpha(x,-y) = -\alpha(x,y)$ where $R_1(x,-y) = R_1(x,y)$ and $R_2(x,-y) = -R_2(x,y)$. We deduce that one can write

$$\alpha(x,y) = (\frac{p(x)}{q(x)}, \frac{s(x)y}{t(x)}) \tag{4.1}$$

with $p, q, r, t \in k[x]$ such that p, q have no common roots and s, t have no common roots.

Definition 4.3.2. We define the **degree** of α as

$$deg\alpha = max\{deg\, p(x), deg\, q(x).\}$$

We say that α is **separable** if the derivative of the fraction $p(x)/q(x)$ is not identically zero.

We will now define α at the points where the denominators $q(x)$ or $t(x)$ vanish.

Since $\alpha(x,y) \in E$ we have

$$\frac{(x^3 + ax + b)s(x)^2}{t(x)^2} = \frac{p(x)^3 + ap(x)q(x)^2 + bq(x)^3}{q(x)^3}.$$

We have in particular the equality

$$(x^3 + ax + b)s(x)^2 q(x)^3 = (p(x)^3 + ap(x)q(x)^2 + bq(x)^3)t(x)^2$$

at any point x such that $q(x)t(x) \neq 0$. Since the set of roots of t and q is finite and k is algebraically closed, the equality above is true for any $x \in k$. Write

$$f(x) = x^3 + ax^2 + b = (x - e_1)(x - e_2)(x - e_3).$$

Let $S \subset \{e_1, e_2, e_3\}$ be the set of common roots of $t(x)$ and $x^3 + ax + b$. Since $t(x)$ and $s(x)$ have no common roots and the polynomial $x^3 + ax + b$ has only simple roots, we deduce that $q(x) = u(x)^2 \prod_S (x - e_i)$ and $t(x) = u(x)^3 \prod_S (x - e_i)^2$.

We could write α in the projective coordinates:

$$\alpha(x,y) = (p(x)u(x)\prod_S (x - e_i) : s(x)y : u(x)^3 \prod_S (x - e_i)^2). \tag{4.2}$$

If $q(x) \neq 0$ we have $u(x)^3 \prod_S (x - e_i)^2 \neq 0$, so that $\alpha(x, y)$ is well defined. If $q(x) = 0$, we set $\alpha(x, y) = O_E$. One could justify it as follows. If $q(x) = 0$, we have $s(x) \neq 0$. If $y \neq 0$, then $\alpha(x, y) = O_E$ using the formula above. If $y = 0$, we then have $x = e_i, i \in S$. Then we use $y^2 = \prod(x - e_i)$ to write

$$\alpha(x, y) = (p(x)u(x)y : s(x) \prod_{i \notin S} (x - e_i) : u(x)^3 y \prod_S (x - e_i)),$$

so that we see $\alpha(x, y) = O_E$.

The next two statements are very useful for the applications :

Proposition 4.3.3. *Let α be a nonzero endomorphism of an elliptic curve E. We then have*

(i) if α is separable, then $\deg \alpha$ is equal to the cardinal of $ker(\alpha)$;

(ii) if α is not separable, then $\deg \alpha > \#ker(\alpha)$;

Proof. We write α in the form (4.1). Let $r_1(x) = \frac{p(x)}{q(x)}$, $r_2(x) = \frac{s(x)}{t(x)}$.

(i) If α is separable, the function $r_1'(x)$ is not identically zero, in particular $p'q - pq'$ is not a zero polynomial. Let

$$S = \{x \in k, (p'q - pq')q(x) = 0.\}$$

Note that S is a finite set. Observe that the function $r_1(x)$ has an infinite number of values, in particular, there exists $P = (c, d) \in E(k)$ a point distinct from O_E such that

1. $c \neq 0, d \neq 0, c \notin r_1(S), (c, d) \in \alpha(E(k))$

2. $deg\,(p(x) - cq(x)) = deg\,(\alpha)$.

Let

$$S' = \{(x_0, y_0) \in E(k) \,|\, \alpha(x_0, y_0) = (c, d).\}$$

We will show that the set S' contains exactly $deg(\alpha)$ elements. In fact, if $(x_0, y_0) \in S'$, we have $\frac{p(x_0)}{q(x_0)} = c$ and $y_0 r_2(x_0) = d$. Since $(c, d) \neq O_E$ and $d \neq 0$, we have that $r_2(x_0) \neq 0$ is well defined and $y_0 = \frac{d}{r_2(x_0)}$. We then have that the cardinal of S' equals to the number of elements $x_0 \in k$ such that $p(x_0) = cq(x_0)$. Since $deg\,(p(x) - cq(x)) = deg\,(\alpha)$, it is enough to show that the polynomial $p(x) - cq(x)$ has simple roots. If not, there exists $x_1 \in k$ such that $p(x_1) = cq(x_1)$, $p'(x_1) = cq'(x_1)$, so x_1 is a root of polynomial $p'q - pq'$ (since $c \neq 0$), so that $c \in r_1(S)$, contradiction with the choice of c. We then have that $\#S' = \#ker(\alpha) = \deg \alpha$.

(ii) This case is similar to (i), the difference is that the polynomial $p(x) - cq(x)$ could have multiple roots, so that $\#ker(\alpha) < \deg \alpha$.

□

Proposition 4.3.4. *Let α be a nonzero endomorphism of an elliptic curve E. Then $\alpha : E \to E$ is a surjective map.*

Proof. The point $P = O_E$ is the image of O_E. Let $P = (c, d)$ be a point of E different from O_E. We are looking for (x, y) such that $\alpha(x, y) = (c, d)$. We write α in the form (4.1). Let $h(x) = p(x) - cq(x)$. We have two cases:

1. If $h(x)$ is not a constant polynomial, let x_0 be a root of h. If $q(x_0) = 0$, then $p(x_0) = 0$ and we get a contradiction with the fact that p and q have no common roots. We then have $q(x_0) \neq 0$. Let y_0 be a root of $x_0^3 + ax_0 + b$. Using (4.2), we get $\alpha(x_0, y_0) = (c, d')$ for $d' \in k$. Since (c, d') is a point of E, we have $d = \pm d'$, so that $(c, d) = \alpha(x_0, \pm y_0)$.

2. Assume that $h(x)$ is a constant polynomial. The fraction $\frac{p(x)}{q(x)}$ is not constant (in fact, $ker(\alpha)$ is finite by previous proposition, $E(k)$ is infinite, we then have a finite number of points with image by α a fixed point). We deduce that there is at most one element $c \in k$ such that $p(x) - cq(x)$ is a constant polynomial. By the previous case, we then have at most two points (c, d) and $(c, -d)$ not in the image of α (with $d^2 = c^3 + ac + b$). Let $(c_1, d_1) \in E(k)$ such that $(c_1, d_1) + (c, d) \neq (c, \pm d')$. We get that (c_1, d_1) and $(c_1, d_1) + (c, d)$ are in the image of α, so that (c, d) as well since α is an endomorphism.

□

Note that given an endomorphism $\alpha : E \to E$, it could be quite difficult to determine the degree of α, and also if α is separable. If $\alpha, \beta : E \to E$ are two endomorphisms, then one defines their sum by the formula $(\alpha + \beta)(P) = \alpha(P) + \beta(P)$. Since addition of points on an elliptic curve is given by rational fractions, we see that $\alpha + \beta$ is indeed an endomorphism of E. Similarly, one defines a linear combination of d'endomorphisms. We have the following formula to determine the degree (see exercises for the proof) :

Proposition 4.3.5. *Let α, β be two nonzero endomorphisms of an elliptic curve E. Let r, s be two integers. Then*

$$deg\, r\alpha + s\beta = r^2 deg\, \alpha + s^2 deg\, \beta + rs(deg\, \alpha + \beta - deg\, \alpha - deg\, \beta).$$

In the following examples we discuss some applications, admitting the facts on separability and the computations of the degree.

4.3.1 Frobenius endomorphism and Hasse theorem

Let k be an algebraic closure of a finite field $\mathbb{F}_q$ with $q = p^n$ elements. **The Frobenius morphism** ϕ_q on k is the map $x \mapsto x^q$. For $x, y \in k$ we have $(x+y)^q = x^q + y^q$, so that ϕ_q ia indeed a homomorphism (of additive groups). In addition, by construction, the field $\mathbb{F}_q$ is the field of decomposition of the polynomial $x^q - x$, so that

$$x \in \mathbb{F}_q \Leftrightarrow \phi_q(x) = x. \tag{4.3}$$

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over $\mathbb{F}_q$. Since $a^q = a$ and $b^q = b$, we have for all $P = (x, y) \in E(k)$,

$$y^{2q} = (x^3 + ax + b)^q = x^{3q} + ax^q + b, \text{ i.e. } (x^q, y^q) \in E(k).$$

Using the formulas of the explicit group law (Proposition 3.1.5), one can show that ϕ_q induces an endomorphism of E

$$\phi_q(x, y) = (x^q, y^q)$$

that we also call **Frobenius endomorphism**. Condition (4.3) gives

$$P \in E(\mathbb{F}_q) \Leftrightarrow \phi_q(P) = P.$$

We then see that

$$E(\mathbb{F}_q) = ker(\phi_q - 1). \tag{4.4}$$

By definition, the Frobenious endormorphism ϕ_q is not separable and $deg\, \phi_q = q$. More generally, let r, s be two nonzero integers. One can show that the endomorphism $r\phi_q - s$ est separable if and only if p does not divide s.

Using the results on the endomorphisms above, one can now give a proof of Hasse theorem.

Proof of theorem 4.0.1.

We have $E(\mathbb{F}_q) = ker(\phi_q - 1)$ by (4.4). Since the morphism $\phi_q - 1$ is separable, proposition 4.3.3 gives $deg(\phi_q - 1) = \#ker(\phi_q - 1)$ Let

$$a_q = q + 1 - \#E(\mathbb{F}_q) = q + 1 - deg(\phi_q - 1).$$

Let r, s be two integers with $(s, q) = 1$. We have that the endomorphism $r\phi_q - s$ is separable of degree (see proposition 4.3.5)

$$deg\, r\phi_q - s = r^2 q + s^2 + rs(deg\,(\phi_q - 1) - q - 1) = r^2 q + s^2 - rsa_q.$$

Since $deg\, r\phi_q - s \geq 0$ for all r, s, we have

$$q(\frac{r}{s})^2 - a_q \frac{r}{s} + 1 \geq 0.$$

But the rational numbers $\frac{r}{s}$ with $(s, q) = 1$ are dense in $\mathbb{R}$. We then have $qx^2 - a_q x + 1 \geq 0$ for all $x \in \mathbb{R}$. We get for the discriminant :

$$a_q^2 - 4q \leq 0,$$

so that $|a_q| \leq 2\sqrt{q}$, which finishes the proof of Hasse theorem. □

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{F}_q$. By investigating the properties of the Frobenius map, one manages to estimate the number of points $E(\mathbb{F}_{q^n})$ for any extension of $\mathbb{F}_q$. We have the following result (for the proof see exercise 6) :

Theorem 4.3.6. *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ and let $a_q = q + 1 - \#E(\mathbb{F}_q)$.*

1. *We have $\phi_q^2 - a_q\phi_q + q = 0$.*

2. *Let α, β be the roots of the polynomial $x^2 - a_q x + q$. Then α, β are conjugate complex numbers with absolute value $\sqrt{q}$. For any $n > 0$ one has*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).$$

3. *The zeta function of the curve E*

$$Z(E/\mathbb{F}_q, T) = exp(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n})\frac{T^n}{n}).$$

is a rational function $\frac{1-a_qT+qT^2}{(1-T)(1-qT)}$.

Complement. Let X be a projective variety defined over a finite field $\mathbb{F}_q$. As for plane curves, one can give a definition if the variety X is smooth. Similarly, there is a notion of dimension (for plane curves, the dimension is 1.) Assume that X est smooth, of dimension n. One defines the zeta function of X by

$$Z(X/\mathbb{F}_q, T) = exp(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n})\frac{T^n}{n}).$$

The **Weil conjecture** claims that the function above is a rational function : $Z(X/\mathbb{F}_q, T) \in \mathbb{Q}(T)$ verifying:

1. (functional equation) $Z(X/\mathbb{F}_q, 1/q^N T) = \pm q^{N\epsilon/2} T^\epsilon Z(X/\mathbb{F}_q, T)$ for some integer ϵ;

2. (Riemann hypothesis) $Z(X/\mathbb{F}_q, T) = \frac{P_1(T)...P_{2N-1}(T)}{P_0(T)P_2(T)...P_{2N}(T)}$ with $P_0(T) = 1 - T, P_{2N}(T) = 1 - q^N T$ et $P_i(T) = \prod_{j=1}^{b_i}(1 - \alpha_{ij}T)$, $0 < i < 2N$, with $|\alpha_{ij}| = q^{1/2}$.

These conjectures have been established by Deligne in the 1970^{th}.

4.3.2 Torsion points

Let E be an elliptic curves over a filed k (we still assume that the field k is algebraically closed). Let $n \geq 2$ be an integer. The multiplication by n gives an endomorphism $\cdot n : E \to E$. Similarly as for the multiplication by 2, one can give the explicit recursive formulas expressing $nP = (x_{nP}, y_{nP})$ in terms of $P = (x_P, y_P)$. More precisely, one has the following statement (see exercise 8):

Proposition 4.3.7. *(i) There exists polynomials ϕ_n, ψ_n, ω_n with $(\phi_n, \psi_n) = 1$ such that*

$$nP = (\frac{\phi_n(x)}{\psi_n(x)^2}, \frac{\omega_n(x,y)}{\psi_n(x)^3}).$$

(ii) The highest order term of $\phi_n(x)$ is x^{n^2}, the highest order term of $\psi_n(x)$ is $n^2 x^{n^2-1}$.

(iii) One has $nP = O_E \Leftrightarrow \psi_n(x) = 0$.

We then see that the degree of the endomorphism of multiplication by n on E is n^2 and that this morphism is separable if and only if n is prime to the characteristic of k. One defines **the group of points of n-torsion of E**:

$$E[n] = \{P \in E, nP = O_E\}.$$

It is a remarkable fact, that one can determine the group structure of $E[n]$ for any elliptic curve, independently of the (algebraically closed) field :

Theorem 4.3.8. *(i) If $(n, car.k) = 1$, then $E[n] = \mathbb{Z}/n \oplus \mathbb{Z}/n$.*

(ii) If $p = car.k \mid n$, then $E[n] = \mathbb{Z}/n' \oplus \mathbb{Z}/n'$ or $E[n] = \mathbb{Z}/n \oplus \mathbb{Z}/n'$, where $n = p^r n'$ and $(n', p) = 1$.

Proof. (i) Using the properties above and proposition 4.3.3, $E[n] = deg\,(\cdot n) = n^2$. The group $E[n]$ is a finite abelian group of order n^2. Using the structure theorem of the finite abelian groups, one gets

$$E[n] = \mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2 \oplus \ldots \oplus \mathbb{Z}/n_s$$

with $n_i | n_{i+1}, 1 \leq i \leq s-1$. Let l be a prime dividing n_1. Then l^s divides the order of $E[n]$. But $\#E[l] = l^2$. One gets $s = 2$ and

$$E[n] = \mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2, n_1 | n_2.$$

This group is also killed by n, so that $n_2 | n$. Since $\#E[n] = n^2 = n_1 n_2$, we deduce that $n_1 = n_2 = n$.

(ii) We will first determine the group structure of $E[p^s]$ for all $s > 0$. Since the multiplication by p map is not separable, $\#E[p] < p^2$. Any element of $E[p]$ is of order 1 or p, we then have that $\#E[p]$ is a power of p, so that it is 1 or

p. If $\#E[p] = 1$, then $\#E[p^s] = 1$ for all $s > 0$ (one uses that if $Q \in E[p^s]$, then $p^{s-1}Q \in E[p]$). Assume $\#E[p] = p$. Let $Q \in E[p^s]$. One then have $pQ \in E[p^{s-1}]$. By induction, $E[p^s]$ is cyclic of order p^s.

Let us write $n = p^r n'$. We then have $E[n] = E[n'] \oplus E[p^r]$. Since $E[n'] = \mathbb{Z}/n' \oplus \mathbb{Z}/n'$, $E[p^r] = 1$ or $\mathbb{Z}/p^r$ and $\mathbb{Z}/n' \oplus \mathbb{Z}/p^r \simeq \mathbb{Z}/n'p^r = \mathbb{Z}/n$, the result follows.

□

Similarly, one can show the structure theorem on points of an elliptic curve over a finite field :

Theorem 4.3.9. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. One has*

$$E(\mathbb{F}_q) = \mathbb{Z}/n \text{ or } \mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2$$

where $n \geq 1$ and $n_1, n_2 \geq 1$ are integers with $n_1 \mid n_2$.

The following statement is very useful for the study of elliptic curves :

Theorem 4.3.10. *Let k be an algebraically closed field and let n be an integer prime to the characteristic of k. Let E be an elliptic curve over k. There exists a pairing*

$$e_n : E[n] \times E[n] \to \mu_n$$

that we call **Weil pairing**, *such that*

1. *e_n is a bilinear:*

   $$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T),\ e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$$

   and non degenerate map :

   $$e_n(S, T) = 1\, \forall T \in E[n] \Rightarrow S = O_E,\ \text{and } e_n(S, T) = 1\, \forall S \in E[n] \Rightarrow T = O_E;$$

2. *$e_n(T, T) = 1$ and $e_n(T, S) = e_n(S, T)^{-1}\ \forall S, T \in E[n]$;*

3. *if $\sigma \in \operatorname{Aut} k$ fixes the coefficients a and b of the curve E, then $e_n(\sigma S, \sigma T) = \sigma(e_n(S, T))$;*

4. *if $\alpha : E \to E$ is an endomorphism, then*

   $$e_n(\alpha(S), \alpha(T)) = (e_n(S, T))^{deg\, \alpha}.$$

The proof of this statement needs more developed algebraic geometry tools.

Remarks.

1. If $S = (x, y) \in E(k)$ and if $\sigma \in \operatorname{Aut} k$, the point σS is defined by $\sigma S = (\sigma x, \sigma y)$.

2. Let E be an elliptic curve defined over a non algebraically closed field k and let $\bar{k}$ be an algebraic closure of k. We denote $E[n] = E(\bar{k})[n]$. We then get the Weil pairing on $E[n]$. If now $P, Q \in E(k)$, then for any $\sigma \in \mathrm{Aut}_k\, \bar{k}$ one has $\sigma P = P$ and $\sigma T = T$. Using the property 3 above, $e_n(S,T)$ is fixed by any such automorphism σ and in particular $e_n(S,T) \in k$.

Proposition 4.3.11. *Let k be an algebraically closed field, let n be an integer $(n, car.k) = 1$. Let E be an elliptic curve k. Let $\{T_1, T_2\}$ be the base of $E[n] = \mathbb{Z}/n \oplus \mathbb{Z}/n$. Then $e_n(T_1, T_2)$ is a primitive n^{th} root of unity*

Proof. exercise. □

Corollary 4.3.12. *Let E be an elliptic curve defined over $\mathbb{Q}$. We write $E[n]$ for the group of n-torsion points of E over an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Then $E[n] \nsubseteq E(\mathbb{Q})$ if $n \geq 3$.*

Proof. By theorem 4.3.10.3 and proposition 4.3.11 above, if $E[n] \subseteq E(\mathbb{Q})$, then $\mu_n \subset \mathbb{Q}$, which is not possible if $n \geq 3$. □

4.3.3 Automorphisms

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over an algebraically closed field k (we always assume that $car(k) \neq 2, 3$). One can show that any automorphism θ of E is given by the changing of variables $x = u^2x', y = u^3y'$ with $u \in k^*$ and $u^{-4}a = a$, $u^{-6}b = b$. Recall that the j-invariant of E is defined as

$$j = j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

We then have

1. if $j \neq 0, 1728$, the group of automorphisms $Aut(E)$ of E is the finite group $\mathbb{Z}/2 = (id, P \mapsto -P)$;
2. if $j = 1728$, $Aut(E) \simeq \mathbb{Z}/4$;
3. if $j = 0$, $Aut(E) \simeq \mathbb{Z}/6$.

4.4 Additional exercises 3

1. (a) Let α be an endomorphism of E.
   i. Show that α induces an endomorphism α_n of $E[n]$.
   ii. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ the matrix of α_n in the base $\{T_1, T_2\}$. Show that

$$deg\, \alpha \equiv det(\alpha_n) (\mathrm{mod}\ n)$$

   (one could express $\zeta^{deg\, \alpha}$ in terms of a, b, c, d.)

(b) Let α, β be two endomorphisms of E and r, s two integers.

i. Show that

$$det(r\alpha_n + s\beta_n) - r^2 det\alpha_n - s^2 det\beta_n = rs(det(\alpha_n + \beta_n) - det\alpha_n - det\beta_n)$$

(one can start by showing that $det(\alpha_n + \beta_n) - det\alpha_n - det\beta_n = Trace(\alpha_n \beta_n^*)$, where β_n^* is the adjoint matrix : if $\beta_n = \left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right)$, then $\beta_n^* = \left(\begin{smallmatrix} t & -y \\ -z & x \end{smallmatrix}\right)$).

ii. Deduce that

$$deg\, r\alpha + s\beta = r^2 deg\, \alpha + s^2 deg\, \beta + rs(deg\, (\alpha + \beta) - deg\, \alpha - deg\, \beta).$$

2. (a) Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, $q = p^r$, and let $a_q = q + 1 - \#E(\mathbb{F}_q)$. As before, we denote ϕ_q the Frobenius morphism on E and for any integer m prime to q one denote $(\phi_q)_m$ the endomorphism induced by ϕ_q on $E(\overline{\mathbb{F}}_q)[m]$. Show that

$$det(\phi_q)_m \equiv q \,(\text{mod } m) \text{ and } Trace(\phi_q)_m \equiv a_q \,(\text{mod } m)$$

(One could use that $\#Ker(\phi_q - 1) = deg\, (\phi_q - 1) = q + 1 - a_q$, see the proof of Hasse theorem)

(b) Deduce that the endomorphism $\phi_q^2 - a_q \phi_q + q$ is identically zero on $E(\overline{\mathbb{F}}_q)[m]$.

(c) Show that the kernel of the map $\phi_q^2 - a_q \phi_q + q$ is infinite; deduce that the polynomial $g(x) = x^2 - a_q x + q$ annihilates ϕ_q.

(d) Assume that b is an integer such that the polynomial $x^2 - bx + q$ annihilates ϕ_q. Deduce that $(a_q - b)$ annihilates $E(\overline{\mathbb{F}}_q)$ and finally that $a_q = b$.

(e) Let α, β be the roots of the polynomial $g(x)$ and let $g_n(x)$ be the polynomial

$$g_n(x) = x^{2n} - (\alpha^n + \beta^n)x^n + q^n.$$

Show that $g(x)$ divides $g_n(x)$ for all n. Deduce that

$$(\phi_q^n)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n = 0.$$

(f) Deduce that $E(\mathbb{F}_{q^n})$ has cardinality $q^n + 1 - (\alpha^n + \beta^n)$.

(g) We define the sets function of the curve E by

$$Z(E/\mathbb{F}_q, T) = exp(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \frac{T^n}{n}).$$

Show that $Z(E/\mathbb{F}_q, T)$ is a rational function

$$\frac{1 - a_q T + qT^2}{(1 - T)(1 - qT)}.$$

3. Let E be an elliptic curve $y^2 = x^3+ax+b$ defined over a field k, $char(k) \neq 2, 3$. One defines the *division polynomials* $\psi_m(x, y)$ in a recursive way : $\psi_0 = 0$, $\phi_1 = 1$, $\psi_2 = 2y$
$\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2$
$\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3)$
$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$, $m \geq 2$
$\psi_{2m} = [\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)]/2y$, $m \geq 3$.

   (a) Show that ψ_n is a polynomial in x, y^2 if n is odd and that $y\psi_n$ is polynomial in x, y^2, if n is even.

   (b) One defines $\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$
   $\omega_m = [\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2]/4y$. Show that ϕ_n is a polynomial in x, y^2, that ω_n is a polynomial in x, y^2 if n is odd, and that $y\omega_n$ is a polynomial in x, y^2 if n is even.

   (c) By the previous question, on can define the polynomials $\phi_n(x)$ and $\psi_n^2(x)$ by replacing y^2 by $x^3 + ax + b$ in the polynomials $\phi_n(x, y)$ and $\psi_n^2(x, y)$. Show that $\phi_n(x)$ is the sum of x^{n^2} and the terms of lower degree, and that $\psi_n(x)^2$ is the sum of $n^2x^{n^2-1}$ and the terms of lower degree.

   (d) Show that for $P = (x, y)$ a point of E, one has

$$nP = \left(\frac{\phi_n(x)}{\psi_n(x)^2}, \frac{\omega_n(x, y)}{\psi_n(x)^3}\right)$$

   (e) Show that the polynomials $\phi_n(x)$ and $\psi_n(x)^2$ are relatively prime. Deduce the the multiplication by n map is of degree n^2.

Chapter 5

Elliptic curves algorithms

5.1 Factorisation

For N an integer we are interested in factorizing N into prime factors. This problem is still technically very difficult in practice (when N is large), which is fundamental for many modern cryptosystems. In this section we will discuss an approach that uses the elliptic curves : the algorithm **ECM** ("Elliptic Curve Method"), introduced by H. Lenstra in 1980^{th} and developped by R. Brent, P. Montgomery and others. This algorithm is the most efficient one, in terms of the size of the factors of N (and not N itself) : its running time is $exp(c\sqrt{log\, p(loglog\, p)})$, where p is the smallest factor of N. One of the latest examples is a factor with 74 digits : it is the following factor of $12^{284}+1$ found on October, 26, 2014 by B. Dodson :

26721194531973848954767772351114152203083577206813943149484875628623309473

5.1.1 Pollard's $p-1$ algorithm

To start with, we recall the $(p-1)$ Pollard's algorithm, the same ideas are also used for the ECM algorithm. Assume that N has a prime factor p such that

$$p-1 = q_1^{e_1} q_2^{e_2} \dots q_r^{e_r}.$$

If the factors q_i verify

$$q_i \leq B, 1 \leq i \leq r$$

we say that $p-1$ is B-**smooth**. The following algorithm allows to find a factor p if $p-1$ is B-smooth.

1. We take $2 \leq a < N$ and we set $x = a$.
2. For $i = 1, 2, \dots s$:
   (a) $x \to x^i \bmod N$ (here we compute $a^{i!} \bmod N$)
   (b) $d := (x-1, N)$

(c) if $1 < d < N$, we found a factor d of N

3. go back to the first step.

Let $s = max\, e_j q_j$. Then $q_j^{e_j}$ divides $s!$, that is $(p-1)|s!$. We then have $a^{s!} \equiv 1 \bmod p$. It is not very likely that $a^{s!} \equiv 1 \bmod N$, so that we hope to find a factor of N.

5.1.2 Algorithm ECM

Elliptic curves modulo N

Let E be an elliptic curve given by a homogeneous equation $Y^2Z = X^3 + aXZ^2 + bZ^3$ where the coefficients coefficients $a, b \in \mathbb{Z}/N$ and the determinant $\Delta(E)$ are invertibles. We define

$$E(\mathbb{Z}/N) = \{(X : Y : Z), X, Y, Z \in \mathbb{Z}/N, pgcd(N, X, Y, Z) = 1,\ Y^2Z = X^3 + aXZ^2 + bZ^3\}.$$

If N were prime, on could always find a sum $P+Q$ for two points $P, Q \in E(\mathbb{Z}/N)$ using the formulas of the explicit group law (Proposition 3.1.5). In these formulas we need to invert $x_P - x_Q$. If this is not possible, and if $x_P \neq x_Q$, we necessarily have that $(x_P - x_Q, N) > 1$ i.e. we found a factor of N. We then obtain the following algorithm. For more efficience, one often uses many curves at the same time.

The algorithm

1. We fix an integer m (often $10 < m < 20$) and an integer B (for example, of order 10^8).

2. We choose m random elliptic curves E_i modulo N :

$$E_i : Y^2Z = X^3 + a_iXZ^2 + b_iZ^3$$

and a point $P_i \in E_i$. In order to do this, we randomly choose a_i, $P_i = (x_{i,0}, y_{i,0})$ and we set $b_i = y_{i,0}^2 - x_{i,0}^3 - ax_{i,0}$.

3. For all i we successively compute $(B!)P_i$ on E_i. If one of the inversion operations is impossible, we found a factor of N.

4. If not, we change B or the curves E_i and we come back to the first step.

The inversion operation fails if $B!P_i = O$ in $E_i(\mathbb{F}_p)$ where p is a prime factor of N. It is the case if the order $\#E_i(\mathbb{F}_p)$ divides $B!$. But $\#E_i(\mathbb{F}_p)$ varies in the interval $]p+1-2\sqrt{p}, p+1+2\sqrt{p}[$, which is better than in the Pollard's method where $p-1$ is fixed. So that we expect that the algorithm is more efficient.

5.2 Schoof's algorithm

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. By the 4.0.1 theorem, the number $\#E(\mathbb{F}_q)$ satisfies the inequality

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

In this section we will describe an algorithm by Schoof, that allows to compute $\#E(\mathbb{F}_q)$ with the running time $O((log\, q)^c)$, for c some constant. Let

$$a_q = q + 1 - \#E(\mathbb{F}_q).$$

To determine a_q we will determine a_q modulo ℓ for many primes ℓ.

We take ℓ a prime. Let $P \in E(\overline{\mathbb{F}}_q)[\ell]$. Using the theorem 4.3.6, we have

$$a_q\phi_q(P) = \phi_q^2(P) + qP,$$

where ϕ_q is the Frobenius morphism. Since $\ell P = O_E$, we have

$$[a_q]_\ell\, \phi_q(P) = \phi_q^2(P) + [q]_\ell P, \tag{5.1}$$

where $[a_q]_\ell$ and $[q]_\ell$ are the rests modulo ℓ. In addition, the equality 5.1 determines $[a_q]_\ell$ in a unique way.

Using the proposition 4.3.7, we have $P \in E(\overline{\mathbb{F}}_q)[\ell] \Leftrightarrow \psi_\ell(P) = O_E$ for a polynomial ψ_ℓ defined in a recursive way. This polynomial is of degree $\frac{\ell^2-1}{2}$. In order to find the multiples of P, we need to work in the ring

$$R_\ell = \mathbb{F}_q[x, y]/(\psi_l(x), y^2 - x^3 - ax - b)$$

so that we never have powers of y^r for $r > 1$ and of x^r for $r > \frac{\ell^2-3}{2}$.

We can now describe Schoof's algorithm.

The algorithm

1. Let $A = 1$, $\ell = 3$.
2. if $A < 4\sqrt{q}$:
   (a) for $n = 0, \ldots \ell - 1$ one verifies the equality (in the ring R_ℓ) :
   $$(x^{q^2}, y^{q^2}) + [q]_\ell(x, y) = n(x^q, y^q)$$
   If the equality is satisied, we save $n_\ell = n$ and we go to the next step.
   (b) We change $A \to \ell A$, and we change ℓ by the next prime number.
3. We find a_q as a unique integer $|a_q| \leq 2q$ such that $a_q \equiv n_\ell$ pour tout ℓ.

Remark. At the last step of the algorithm we use the theorem on chinese rests in order to find a satisfying the conditions $a_q \equiv n_\ell$. Since $A = \prod \ell > 4\sqrt{q}$ and $a_q \in]-2\sqrt{q}, +2\sqrt{q}[$ by the Hasse theorem, such integer is unique.

5.3 Primality

The elliptic curves are also used in order to test (and prove) that some big integers (more than 20000 digits) are prime. One of the most recent records is the number

$$(2^{83339}+1)/3$$

which is prime and has 25088 digits. This algorithm runs in time $O((log\, N)^4)$.

We discuss here the primality test of Goldwasser-Kilian. We will need the following two statements.

Proposition 5.3.1. *Let N be an integer prime to 6 and let E be a curve with coefficients in $\mathbb{Z}/N$. Assume that there exists*

(i) an integer m and a prime q, $q|m$ and $q > (\sqrt[4]{N}+1)^2$;

(ii) a point $P \in E(\mathbb{Z}/N)$ such that $mP = O_E$ and $(m/q)P = (x : y : z)$ with z invertible in $\mathbb{Z}/N$.

Then N is prime.

Proof. Assume that N is not prime : we then have a prime factor l of N such that $l \leq \sqrt{N}$. We denote $\bar{E}$ the curve obtained by reducing the coefficients a, b of E modulo l. The reduction modulo l of the point P gives a point $\bar{P}$ of $\bar{E}$ of order divisible by q (using the condition (ii)). We then have $q \leq \#\bar{E}(\mathbb{F}_l) \leq (\sqrt{l}+1)^2$ by the Hasse theorem. But $l \leq \sqrt{N}$. We then obtain a contradiction with the condition (i). □

Proposition 5.3.2. *Let N be a prime, $(N, 6) = 1$ and let E be an elliptic curve given by the equation $Y^2Z = X^3 + aXZ^2 + bZ^3$ where the coefficients $a, b \in \mathbb{Z}/N$ and the derminant $\Delta(E)$ are invertible. Let $m = \#E(\mathbb{Z}/N)$. Assume there exists a prime number q such that $q|m$ and $q > (\sqrt[4]{N}+1)^2$. Then there exists a point $P \in E(\mathbb{Z}/N)$ such that $mP = O_E$ and $(m/q)P = (x : y : z)$ with z invertible in $\mathbb{Z}/N$.*

Proof. Assume that for any point P of $E(\mathbb{Z}/N)$ we have $(m/q)P = O_E$. Hence the order of $E(\mathbb{Z}/N)$ divides m/q. Using the theorem 4.3.9 we have $E(\mathbb{Z}/N) = \mathbb{Z}/d_1 \oplus \mathbb{Z}/d_2, d_1|d_2$, so that $d_2|(m/q)$. Since $m \leq d_2^2$, we get $m \leq (m/q)^2$. Since $m \leq (\sqrt{N}+1)^2$ by Hasse theorem, we get the contradiction with the hypothesis on q. □

As a consequence of the properties above, we get that if we find an elliptic curve E such that the order m of $E(\mathbb{Z}/N)$ has a big prime factor q (i.e. $q > (\sqrt[4]{N}+1)^2$), then N is prime iff there exists a point $P \in E(\mathbb{Z}/N)$ such that $mP = O_E$ and $(m/q)P = (x : y : z)$ with z invertible in $\mathbb{Z}/N$. For a given elliptic curve, one can use Schoof's algorithm to determine its order m. Then, in order to test if q is prime,

we do reiterate the procedure again. We then get the following algorithm.

The algorithm

1. We choose an elliptic curve E and we compute $m = \#E(\mathbb{Z}/N)$.
2. We devide m by the small prime numbers, that we denote m_0 the product and we are looking for $q = m/m_0$ verifying $q > (\sqrt[4]{N} + 1)^2$ and that passes the classical primality tests. If it is not the case, we go back to the first step.
3. We choose $x \in \mathbb{Z}/N$ such that $x^3 + ax + b$ is a square in $\mathbb{Z}/N$. So that we get a point P on a curve E. We check if $mP = 0_E$ and $(m/q)P = (x : y : z)$ with z invertible in $\mathbb{Z}/N$. If it is the case we know that N is prime if q is prime. We then go back to the first step with q at the place of N. If not, we change the point P and we continue.

5.4 Cryptography with elliptic curves

One generally considers the following context for the public keys cryptographical systems: two persons, Alice and Bob, want to exchange some messages in a secured way. Eva wants to read their messages, she has an access to a public transmission channel for the messages of Alice and Bob. In this system, one distinguishes three basic algorithms: keys exchange, the coding and the numerical signature. At the step of keys exchange, Alice and Bob produce a common key (known just by themselves), that they willl use later. The numerical signature allows Bob to check that the message he gets comes indeed from Alice. The methods we describe here could actually be used in any group, but we describe special aspects related to the elliptic curves.

5.4.1 Keys exchange: Diffie-Hellman's protocol

1. Public data: E an elliptic curve over a finite field $\mathbb{F}_q$ and a point $P \in E(\mathbb{F}_q)$ of a sufficiently big order.
2. Secret choice of Alice: an integer a.
3. Secret choice of Bob: an integer b.
4. Alice sends $P_a = aP$ to Bob.
5. Bob computes $P_b = bP$ and sends to Alice;
6. Alice computes $aP_b = abP$ and Bob computes $bP_a = abP$. The common key is some function of the point abP.

Definition 5.4.1. The **Diffie-Hellman** problem is the following question:

Given P, aP and bP in $E(\mathbb{F}_q)$, find abP.

This problem is (technically) very difficult to solve, which garantees the security of the Diffie-Hellman's protocol.

5.4.2 ElGamal cryptosystem

To receive a message from Alice, Bob takes an elliptic curve E over a finite fieldi $\mathbb{F}_q$ and a point $P \in E$. He chooses also a secret integer s and he computes $B = sP$. The public data is

$$E, P, B.$$

The secret Bob's key is the integer s.

To encode the message, Alice uses the following algorithm :

1. She represents her message as a point $M \in E(\mathbb{F}_q)$.
2. She chooses a random secret integer k and she computes $M_1 = kP$, $M_2 = M + kB$.
3. Alice sends the points M_1, M_2 to Bob.

To decode the message, Bob computes

$$M_2 - sM_1 = (M + kB) - s(kP) = M + k(sP) - skP = M.$$

5.4.3 Numerical signature

The numerical signature principle is somehow inverse to the coding : everybody could verify that the signature is correct, but only Alice could sign the document. We give here an algorithm that is used in the ECDSA standard.

In order to sign her document, Alice chooses an elliptic curve E over a finite field $\mathbb{F}_q$, such that $\#E(\mathbb{F}_q) = fr$, where r is a big prime number and f is an integer, in general, $f = 1, 2$ or 4. She chooses a point $P \in E$ of order r. She also chooses a secret integer s and she computes $Q = sP$. The data of

$$E, r, P, Q$$

is public.

In order to sign the message m (that one views as an integer this time), Alice chooses a random integer k and she computes $R = kP = (x, y)$ and $z = k^{-1}(m + sx) \bmod r$. Then Alice signes her document by

$$m, R, z.$$

In order to verify the signature, Bob does the following:

1. He computes $u_1 = z^{-1}m \bmod r$ and $u_2 = z^{-1}x \bmod r$.

2. He computes $V = u_1P + u_2Q$.

3. He decides that the signature is correct if $V = R$.

It is an exercice to check that $V = R$ if the document is signed by Alice.

5.5 Discret logarithm

Definition 5.5.1. Let G be a group. In the discret logarithm problem in G, for given $x, y \in G$ we are looking for an integer m such that $x^m = y$ (if it exists).

The fact that technically this problem is very difficult to resove for $G = E(\mathbb{F}_q)$ is the base of the security of the algoritms above. In general, if G is a group of order n, all known algorithms to resolve this problem have $O(\sqrt{N})$ running time (which is a lot!).

We briefly discuss two general algorithms for the discrete logarithm problem, as well as an algorithm, due to Menezes, Okamoto and Vanstone, that one could apply to some elliptic curves, it uses the Weil pairing.

5.5.1 Babystep-Giantstep

Let G be a group, $x, y \in G$ and let n be the order of x. Let N be the integer $N = \lceil \sqrt{n} \rceil$.

The algorithm

1. we save the following list of elements of G: $x, x^2, x^3, \ldots x^N$;

2. we set $z = (x^N)^{-1}$ and we save $yz, yz^2, yz^3, \ldots yz^N$.

3. we check for collisions: if $x^i = yz^j$, we found $y = x^{i+jN}$.

The problem with this algorithm is that one has to save the two lists. Pollard's method allows to solve this problem.

5.5.2 Pollard's ρ-method

Let G be a group, $x, y \in G$ and let n be the order of x. We search for m such that $x^m = y$. We will find the integers i, j, i_1, j_1 such that

$$x^i y^j = x^{i_1} y^{j_1}. \tag{5.2}$$

We will then have $x^{i-i_1} = y^{j_1-j}$, that allows us to find m if $j - j_1$ is prime to the order of x in G (we always can assume it up to restricting to the case when x has prime order).

Let $G = A \cup B \cup C$ be a partition, where A, B, C are of the same cardinal (up to few elements). Let $f : G \to G$ be the function

$$f(z) = \begin{cases} xz & z \in A \\ z^2 & z \in B \\ yz & z \in C. \end{cases}$$

Let $x_0 = x \in G$. For any $i > 1$ we define $x_i = f(x_{i-1})$. Let t be the biggest integer such that x_{t-1} appears only once in the sequence $(x_i)_{i \geq 0}$ and let l be the smallest integer such that $x_{t+l} = x_t$. Then, one can show that $t + l$ is of order $O(\sqrt{n})$ and that there exists $1 \leq i < t + l$ such that $x_{2i} = x_i$, so that we can find the collision 5.2.

5.5.3 The MOV attack

In the algorithm of Menezes, Okamoto and Vanstone one reduces to the discret logarithm problem in $E(\mathbb{F}_q)$ to the discrete logarithm problem in $\mathbb{F}_{q^d}$ for some d.

Definition 5.5.2. Let m be an integer. The **embedding degree** of m in the finite field $\mathbb{F}_q$ is the smallest integer d such that

$$q^d \equiv 1(\bmod m).$$

Remark. The condition above is equivalent to the condition $\mu_m \subset \mathbb{F}_{q^d}$.

Lemma 5.5.3. *Let E be an elliptic curve other a finite field $\mathbb{F}_q$ and let $m \geq 1$ be an integer prime to q and to $q - 1$. Let d be the embedding degree of m in $\mathbb{F}_q$. If $E(\mathbb{F}_q)$ contains a point of exact order m, then $E[m] \subset E(\mathbb{F}_{q^d})$.*

Proof. Let P be a point of exact order m and let $T \in E(\overline{\mathbb{F}}_q)[m]$ such that $\{P, T\}$ is a base of $E(\overline{\mathbb{F}}_q)[m] = \mathbb{Z}/m \oplus \mathbb{Z}/m$. Let ϕ_q be the Frobenius endomorphism. One has

$$\phi_q(P) = P, \phi_q(T) = uP + vT, u, v \in \mathbb{Z}/m.$$

Using the properties of the Weil pairing, we have

$$e_m(P, T)^q = e_m(\phi_q(P), \phi_q(T)) = e_m(P, P)^u e_m(P, T)^v = e_m(P, T)^v.$$

Since $e_m(P, T)$ is ℓ-th primitive root of unity (proposition 4.3.11), we deduce that $v \equiv q \,(\bmod\, m)$, i.e.

$$\phi_q(T) = uP + qT.$$

We then get

$$\phi_{q^d}(T) = u(1 + q + q^2 + \ldots + q^{d-1})P + q^d T.$$

By definition of d, one has $q^d \equiv 1 \,(\bmod\, m)$, so that $q^d T = T$ and $(1 + q + q^2 + \ldots + q^{d-1})P = O_E$. We deduce $\phi_{q^d}(T) = T$, so that $T \in E(\mathbb{F}_{q^d})$.

□

The algorithm
Let E be an elliptic curve over a finite field $\mathbb{F}_q$ and let m be an integer, $(m,q)=1$. Let P,Q be two points of order m and let d be the embedding degree of m in $\mathbb{F}_q$.

1. Let $T \in E(\overline{\mathbb{F}}_q)[m]$ such that P,T generate $E[m]$ (see 4.3.8). Using the Lemma above, $T \in E(\mathbb{F}_{q^d})$.

2. By proposition 4.3.11, $e_m(P,T)$ is m-th primitive root of unity. Using the definition of d, we get $e_m(P,T) \in \mathbb{F}_{q^d}$. There exists algorithms to compute the Weil pairing (in $E(\mathbb{F}_{q^d})$) : so that we find $e_m(Q,T)$. Since $e_m(P,T)$ is n-th primitive root of unity , we get

$$Q = rP \Leftrightarrow e_m(Q,T) = e_m(P,T)^r.$$

   So that the problem is reduced to the discrete logarithm problem in $\mathbb{F}_{q^d}$.

5.5.4 Supersingular curves

Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic $p \geq 5$. Recall (see theorem 4.3.8) that the group $E(\bar{\mathbb{F}}_p)[p]$ is either reduced to O_E, or $E(\bar{\mathbb{F}}_p)[p] \simeq \mathbb{Z}/p$.

Definition 5.5.4. We say that E is **supersingular** if $E(\bar{\mathbb{F}}_p)[p] = \{O_E\}$.

Proposition 5.5.5. *Let $a = q+1-\#E(\mathbb{F}_q)$. The following are equvalent :*

(i) E is supersingular;

(ii) $a \equiv 0 \ (mod\ p)$;

(iii) $\#E(\mathbb{F}_q) \equiv 1 \ (mod\ p)$.

Proof. Let α, β be the roots of tha polynomial $x^2 - ax + q = 0$. Let $s_n = \alpha^n + \beta^n$. We have $s_0 = 2, s_1 = a$ and we check by induction:

$$s_{n+1} = as_n - qs_{n-1}.$$

Using the definition of a, we have $(ii) \Leftrightarrow (iii)$.

Assume (ii). We then have $s_n \equiv 0 \pmod p$, so that $\#E(\mathbb{F}_{q^n}) \equiv 1 \pmod p$ for any n (see theorem 4.3.6). So that we do not have a point of order p in the group $E(\mathbb{F}_{q^n})$, and we get (i).

Assume E is supersingular. Assume that $a \neq 0 \pmod p$. We have $s_{n+1} \equiv as_n \pmod p$ and

$$\#E(\mathbb{F}_q) = q^n + 1 - s_n \equiv 1 - a^n \pmod p.$$

For $n = p-1$ we then get that $p | \#E(\mathbb{F}_q)$ so that E is not supersingular. Contradiction. □

Corollary 5.5.6. *An elliptic curve E over $\mathbb{F}_p$ is supersingular iff $\#E(\mathbb{F}_p) = p+1$.*

Proof. By the Hasse theorem, $|a| \leq 2\sqrt{p}$. In the previous proposition we then have $a = 0 \Leftrightarrow a \equiv 0 \pmod{p} \Leftrightarrow \#E(\mathbb{F}_p) = p+1$. □

Corollary 5.5.7. *Assume that $p \equiv 2 \pmod 3$. Let $b \in \mathbb{F}_p$ non zero. The elliptic curve $y^2 = x^3 + b$ over $\mathbb{F}_p$ is supersingular.*

Proof. By the results in section 4.2.1, the condition (iii) in the proposition above is satisfied. □

There are very efficient algorithms for the arithmetic operations on a supersingular elliptic curve. Assume $a = 0$. We then have for any $P = (x, y) \in E(\bar{\mathbb{F}}_p)$:

$$q(x, y) = -\phi_q(x, y) = (x^{q^2}, -y^{q^2}).$$

Let m be an integer. In order to compute mP, we proceed as follows:

1. we decompose $m = m_0 + m_1 q + m_2 q^2 + \ldots + m_r q^r$ with $0 \leq m_i < q$;
2. we compute $m_i P = (x_i, y_i)$, and then $q^i m_i P = (x_i^{q^{2i}}, (-1)^i y_i^{q^{2i}})$, and finally we compute the sum of all these points.

On the other hand, the proposition above shows that the attack MOV could be applied to E, so that the discret algorithm problem for E could be reduced to the descret logarithm problem for $\mathbb{F}_{q^2}$, which is much more easy.

Proposition 5.5.8. *Let E be a supersingular elliptic curve over $\mathbb{F}_q$ and let $N > 0$ be an integer. Assume $a = q + 1 - \#E(\mathbb{F}_q) = 0$. If there exists a point $P \in E(\mathbb{F}_q)$ of order N, then $E(\bar{\mathbb{F}}_q)[N] \subset E(\mathbb{F}_{q^2})$.*

Proof. Let $Q \in E(\bar{\mathbb{F}}_q)[N]$. Since $\#E(\mathbb{F}_q) = q + 1$, we have $N | q + 1$. Since E is supersingular and $a = 0$, we have $\phi_q^2(S) = -qS = S$. Hence Q is fixed by ϕ_{q^2}, so that $Q \in E(\mathbb{F}_{q^2})$. □

Chapter 6

Elliptic curves over number fields

6.1 Generalities on the number fields

6.1.1 Some facts on the number fields and its ring of integers

Definition 6.1.1. A **number field** is a finite algebraic extension of the field of rational numbers $\mathbb{Q}$.

In this section we fix a number field K.

By the primitif element theorem one can write $K = \mathbb{Q}(\alpha)$ with $[K : \mathbb{Q}] = n = \deg P$, where P is the minimal polynomial of α. Assume that P has r_1 real roots $\alpha_1, \dots \alpha_{r_1}$ and r_2 pairs of complex roots $\alpha_{r_1+1}, \bar{\alpha}_{r_1+1}, \dots, \alpha_{r_1+r_2}, \bar{\alpha}_{r_1+r_2}$. We then have r_1 embeddings of K in $\mathbb{R}$ defined by $\sigma_i(\alpha) = \alpha_i$ and r_2 pairs of embeddings of K in $\mathbb{C}$: $\sigma_j(\alpha) = \alpha_{r_1+j}$ and $\bar{\sigma}_j(\alpha) = \bar{\alpha}_{r_1+j}$. We say that K has r_1 **real embeddings and** r_2 **pairs of complex embeddings.** We then define a canonical embedding

$$\tau_K : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$
$$\tau_K(x) = (\sigma_i(x))_{i=1,\dots,r_1+r_2}.$$

Definition 6.1.2. The ring of integers of K is the ring

$$\mathcal{O}_K = \{x \in K \text{ is a root of a unitary polynomial with integer coefficients}\}.$$

Examples.

1. If $K = \mathbb{Q}(\sqrt{d})$, where d has no square factors, then $\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod 4. \end{cases}$
2. More generally, if $[K : \mathbb{Q}] = n$, then one can find $e_1, \dots e_n \in \mathcal{O}_K$ such that

$$\mathcal{O}_K = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_n.$$

3. Assume that K has r_1 real embeddings and r_2 pairs of complex embeddings. If $\alpha \in \mathcal{O}_K$, then the polynomial $\chi_{\alpha,K} = \prod_{i=1}^{r_1}(x - \sigma_i(\alpha)) \prod_{j=1}^{r_2}(x - \sigma_{r_1+j}(\alpha))(x - \bar{\sigma}_{r_1+j}(\alpha))$ has integral coefficients: $\chi_{\alpha,K} \in \mathbb{Z}[x]$.

We have the following fundamental result:

Theorem 6.1.3. *The image $\tau_K(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.*

In other words, $D := \tau_K(\mathcal{O}_K)$ is a discret subgroup of $V = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ (i.e. for any real $r > 0$ the set $\{v \in D, |v| \leq r\}$ is finite) and generates V as an $\mathbb{R}$-vector space.

Definition 6.1.4. Let I, J be two ideals in $\mathcal{O}_K$. We say that I and J are **equivalent** if there exist $\alpha, \beta \in \mathcal{O}_K$ non zero, such that

$$\alpha I = \beta J.$$

Theorem 6.1.5. *Any ideal I of $\mathcal{O}_K$ is invertible: there exists $\alpha \in \mathcal{O}_K$ and an ideal $J \subset \mathcal{O}_K$ such that $IJ = \alpha\mathcal{O}_K$. The set of ideal classes is a group Cl_K. This group is finite.*

Theorem 6.1.6. *(i) Any nonzero prime ideal of $\mathcal{O}_K$ is maximal.*

(ii) Any ideal I of $\mathcal{O}_K$ could be decomposed in a unique way (up to a permutation) as a product of prime ideals.

Remark.

1. One shows that the ring $\mathcal{O}_K$ is a Dedekind ring: it is a noetherian integrally closed ring, such that any nonzero prime ideal is maximal.
2. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. The unicity of the decomposition in (ii) implies in particular that the inclusions $\mathfrak{p}^{m+1} \subset \mathfrak{p}^m$ are strict.

In particular, if p is a prime, one could write

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m}$$

with $\mathfrak{p}_i$, $i = 1, \dots, m$ distinct prime ideals and $e_i \geq 1$. The field $\mathcal{O}_K/\mathfrak{p}_i$ is a finite extension of the field $\mathbb{F}_p$, we set $f_{\mathfrak{p}_i} = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_p]$. In particuliar,

$$N\mathfrak{p}_i := card(\mathcal{O}_K/\mathfrak{p}_i) = p^{f_{\mathfrak{p}_i}}.$$

Recall that if $n = [K : \mathbb{Q}]$, then

$$n = \sum_{i=1}^{m} e_i f_{\mathfrak{p}_i}.$$

In fact, this follows from the identity

$$p^n = N(p\mathcal{O}_K) = N\mathfrak{p}_1^{e_1} \cdot \ldots \cdot N\mathfrak{p}_m^{e_m} = p^{\sum e_i f_{\mathfrak{p}_i}}.$$

Let I be an ideal of $\mathcal{O}_K$ and let $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$. Theorem 6.1.6 allows to define

$$\mathrm{ord}_{\mathfrak{p}}(I) = max\{n \geq 0 \,|\, I \subset \mathfrak{p}^n.\}$$

If $x \in \mathcal{O}_K$, one defines $\mathrm{ord}_{\mathfrak{p}}(x)$ as an oder at $\mathfrak{p}$ of the ideal (x) and one extends this notion to any $x \in K$.

6.1.2 Absolute values

Definition 6.1.7. Let K be a field. An **absolute value** v on K is a map

$$|\cdot|_v : K \to \mathbb{R}_+$$

such that

(i) $|x|_v = 0$ iff $x = 0$;

(ii) $|xy|_v = |x|_v|y|_v$ for any $x, y \in K$;

(iii) there exists a constant $C > 0$ such that $|x + y|_v \leq C \max\{|x|_v, |y|_v\}$ for any $x, y \in K$. If $C = 1$, we say that the absolute value is **ultrametric**.

Remark. One easily verifies that if $|\cdot|_v$ is an absolute value on a field F, then $|\cdot|_v^{\alpha}$ is also an absolute value on F for any $\alpha > 0$.

Finite places. For any prime ideal $\mathfrak{p}$ of the number field K one defines an absolute value on K by

$$|x|_{\mathfrak{p}} = N\mathfrak{p}^{-ord_{\mathfrak{p}}(x)}$$

We denote $\Sigma_{fini}(K)$ the set of these absolute values. One verifies that these absolute values are ultrametric.

Places of K. Assume that K has r_1 real embeddings and r_2 pairs of complex embeddings. For $\sigma_i : K \hookrightarrow \mathbb{R}$, $i = 1, \ldots r_1$, one defines an absolut value by

$$|x|_{\sigma_i} = |\sigma_i(x)|$$

and for $\sigma_j : K \hookrightarrow \mathbb{C}, j = 1, \dots r_2$ one defines an absolute value

$$|x|_{\sigma_j} = |\sigma_j(x)|^2.$$

We denote $\Sigma_\infty(K)$ the set of these $r_1 + r_2$ absolute values.

We set $\Sigma(K) = \Sigma_{fini}(K) \cup \Sigma_\infty(K)$ the set of **places** of K.

Theorem 6.1.8. [Product formula] *Let $x \in K^*$. Then we have*

$$\prod_{v \in \Sigma(K)} |x|_v = 1.$$

Proof. Assume first that $K = \mathbb{Q}$. We could then write $x = \pm p_1^{e_1} \dots p_r^{e_r}$ with p_i prime and $e_i \in \mathbb{Z} \setminus \{0\}, i = 1, \dots m$. We then have $|x|_{p_i} = p_i^{-e_i}$ for all finite places, for the place ∞ corresponding to the embedding $\mathbb{Q} \subset \mathbb{R}$, we have $|x|_\infty = |x| = p_1^{e_1} \dots p_r^{e_r}$. We then get

$$\prod_{v \in \Sigma(\mathbb{Q})} |x|_v = p_1^{-e_1} \cdot \dots \cdot p_r^{-e_r} p_1^{e_1} \dots p_r^{e_r} = 1.$$

In the general case let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Let us write

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m}.$$

Let $x \in K^*$ ans let $N_{K/\mathbb{Q}}(x) \in \mathbb{Q}$ be the norm of x. We then have

$$\prod_{\mathfrak{p}|p} |x|_\mathfrak{p} = |N_{K/\mathbb{Q}}(x)|_p. \tag{6.1}$$

In fact, one verifies that $N_{K/\mathbb{Q}}(x) = \pm N(x\mathcal{O}_K)$, so that

$$N_{K/\mathbb{Q}}(x) = \pm \prod_\mathfrak{p} N\mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x)} = \pm \prod p^{\sum_{\mathfrak{p}|p} f_\mathfrak{p} \mathrm{ord}_\mathfrak{p}(x)}.$$

We then deduce

$$|N_{K/\mathbb{Q}}(x)|_p = p^{-\sum_{\mathfrak{p}|p} f_\mathfrak{p} \mathrm{ord}_\mathfrak{p}(x)} = \prod_{\mathfrak{p}|p} N\mathfrak{p}^{-\mathrm{ord}_\mathfrak{p}(x)} = \prod_{\mathfrak{p}|p} |x|_\mathfrak{p},$$

and we get (6.1).

For the places at infinity we also have

$$\prod_{v \in \Sigma_\infty(K)} |x|_v = |N_{K/\mathbb{Q}}(x)|_\infty.$$

In fact, by the definition of the norm $N_{K/\mathbb{Q}}(x) = \prod_{i=1}^{r_1} \sigma_i(x) \prod_{j=1}^{r_2} \sigma_{i+j}(x)\bar{\sigma}_{i+j}(x)$, so that

$$|N_{K/\mathbb{Q}}(x)|_\infty = \prod_{v \in \Sigma_\infty(K)} |x|_v.$$

We then have:

$$\prod_{v\in\Sigma(K)} |x|_v = \prod_{w\in\Sigma(\mathbb{Q})} \prod_{v|w} |x|_v = \prod_{w\in\Sigma(\mathbb{Q})} N_{K/\mathbb{Q}}(x)_w = 1$$

by the first case when $K = \mathbb{Q}$.

□

6.2 Heights

6.2.1 Weil height on $\mathbb{P}^n(\overline{\mathbb{Q}})$

The notion of height is designed in order to 'measure' the size of points in a projective space or in a projective algebraic variety defined over a number field K.

Definition 6.2.1. Let K be a number field and let $P = (x_0 : \ldots : x_n)$ be a point of $\mathbb{P}^n_K$. One define the height of P relatively to the field K by the formula

$$H_K(P) = \prod_{v\in\Sigma(K)} \max(|x_0|_v, \ldots |x_n|_v).$$

Remark.

1. Using the product formula 6.1.8, this definition does not depend on a choice of projective homogeneous coordinates of the point P.
2. If $K = \mathbb{Q}$, one could find coordinates $P = (x_0 : \ldots : x_n)$ with x_i relatively prime integers. We then get $H_{\mathbb{Q}}(P) = \max(|x_0|, \ldots, |x_n|)$.

Lemma 6.2.2. *Let L/K be a finite extension of number fields of degree d. If $P \in \mathbb{P}^n(K)$, then*

$$H_L(P) = H_K(P)^d.$$

Proof. Left as an exercise. □

The lemma above allows to define the Weil height on $\mathbb{P}^n(\overline{\mathbb{Q}})$.

Definition 6.2.3. The **Weil height** on $\mathbb{P}^n(\overline{\mathbb{Q}})$ is a map

$$H : \mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{R}$$
$$P \in \mathbb{P}^n(K) \mapsto H_K(P)^{1/[K:\mathbb{Q}]}.$$

We set $h_K = logH_K$ and $h = logH$.

Definition 6.2.4. If K is a number field and $x \in K$, one defines

$$H(x) = H(1 : x).$$

Theorem 6.2.5. [Northcott, Kronecker] *Let $d \geq 1$, $C > 0$.*

(i) The set

$$\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}), [\mathbb{Q}(P) : \mathbb{Q}] \leq d, H(P) \leq C\}$$

is finite.

(ii) One has $H(P) > 1$, unless $P = (x_0 : \ldots : x_n)$ is such that for any i either x_i is a root of unity or $x_i = 0$.

Proof. (i) Let $P = (x_0 : \ldots : x_n)$. Up to a permutation one can assume $x_0 \neq 0$ and write $P = (1 : \alpha_1 \ldots : \alpha_n)$ avec $\alpha_i \in \overline{\mathbb{Q}}$. By definition

$$H(\alpha_i) \leq H(P) \text{ et } [\mathbb{Q}(\alpha_i) : \mathbb{Q}] \leq [\mathbb{Q}(P) : \mathbb{Q}].$$

We deduce that it is enough to show that the set

$$S = \{\alpha \in \overline{\mathbb{Q}}, [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d, H(\alpha) \leq C\}$$

is finite. By (ii) of the lemma below, the coefficients of the minimal polynomial are bounded for any $\alpha \in S$, which shows that the set S is finite.

(ii) We write $P = (1 : \alpha_1 \ldots : \alpha_n)$ as above. If $H(P) \leq 1$, then $|\alpha_i|_v \leq 1$ for any i and any v. This last condition is also satisfied by α_i^m for all $m > 0$. Using (i) we get that the set $\{(1 : \alpha_1^m \ldots : \alpha_n^m)\}$ is finite, so that α_i are the roots of unity.

□

Lemma 6.2.6. *(i) [Gauss Lemma] Let K be a number field and let $P, Q \in K[x]$. Let v be an absolute value corresponding the the prime ideal $\mathfrak{p}$ of K and let $||P||_v$ be the norm sup of the coefficients of P. Then $||PQ||_v = ||P||_v||Q||_v$.*

(ii) Let $\alpha \in \overline{\mathbb{Q}}$ and let $K = \mathbb{Q}(\alpha)$. Let $P \in \mathbb{Z}[x]$, $P(x) = a_0(x - \alpha_1) \ldots (x - \alpha_d)$ be the minimal polynomial of α. Then

$$H_K(\alpha) = |a_0| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}.$$

Proof. (i) Let $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ (see remark after the theorem 6.1.6 to insure that this set is nonempty). We have in particular $\text{ord}_{\mathfrak{p}}(\pi) = 1$. Up to multiplying the coefficients of P and Q by some power of π, we can assume that $||P||_v = ||Q||_v = 1$. In particular, the images $\bar{P}$ and $\bar{Q}$ of P and Q in the ring $\mathcal{O}/\mathfrak{p}[x]$ are nonzero. Since $\mathcal{O}/\mathfrak{p}[x]$ is an integral ring, we then deduce that $\bar{P}\bar{Q} = \overline{PQ}$ is nonzero which means that $||PQ||_v = 1$.

(ii) Let $L = \mathbb{Q}(\alpha_1, \dots, \alpha_d)$. By definition we have:

$$H_K(\alpha)^{[L:K]} = H_L(\alpha) = \prod_{w \in \Sigma_{fini}(L)} \max(1, |\alpha|_w) \prod_{w \in \Sigma_\infty(L)} \max(1, |\alpha|_w). \quad (6.2)$$

For the places at infinity we have:

$$\prod_{w \in \Sigma_\infty(L)} \max(1, |\alpha|_w) = \prod_{v \in \Sigma_\infty(K)} \max(1, |\alpha|_v)^{[L:K]} = (\prod_{i=1}^{d} \max(1, |\alpha_i|))^{[L:K]}. \quad (6.3)$$

Let $w \in \Sigma_{fini}(L)$. Using the Gauss lemma (i) for P we have

$$1 = ||P||_w = |a_0|_w \prod_{i=1}^{d} \max(1, |\alpha_i|_w).$$

In addition, by the product formula,

$$\prod_{w \in \Sigma_{fini}(L)} |a_0|_w = |a_0|^{-[L:\mathbb{Q}]}.$$

For the finite places we then have:

$$1 = \prod_{w \in \Sigma_{fini}(L)} |a_0|_w \prod_{i=1}^{d} \prod_{w \in \Sigma_{fini}(L)} \max(1, |\alpha_i|_w) = |a_0|^{-[L:\mathbb{Q}]} (\prod_{w \in \Sigma_{fini}(L)} \max(1, |\alpha|_w))^d. \quad (6.4)$$

We then deduce the result from (6.3), (6.4) and (6.2):

$$H_K(\alpha)^{[L:K]} = |a_0|^{[L:\mathbb{Q}]/d} (\prod_{i=1}^{d} \max(1, |\alpha_i|))^{[L:K]}.$$

□

Theorem 6.2.7. *Let $(P_0, \dots P_m), P_i \in \bar{\mathbb{Q}}[x_0, \dots x_n], i = 0, \dots m$ be a family of projective homogeneous polynomials of degree d. Let $Z = V_p(P_0, \dots P_m) \subset \mathbb{P}^n_{\overline{\mathbb{Q}}}$ and let $U = \mathbb{P}^n_{\overline{\mathbb{Q}}} \setminus Z$. Let $V \subset \mathbb{P}^n_{\overline{\mathbb{Q}}}$ be a projective variety such that $V \cap Z = \emptyset$. One defines*

$$\Phi : U(\overline{\mathbb{Q}}) \to \mathbb{P}^m_{\overline{\mathbb{Q}}}$$
$$x \mapsto (P_0(x) : \dots P_m(x)).$$

Then there are constants c_1, c_2, c_3 depending only on Φ and such that

(i) for any $x \in U(\overline{\mathbb{Q}})$ one has $H(\Phi(x)) \leq c_1 H(x)^d$;

(ii) for any $x \in V(\overline{\mathbb{Q}})$ one has $c_2 H(x)^d \leq H(\Phi(x)) \leq c_3 H(x)^d$;

Proof. (i) Let $x \in U(\overline{\mathbb{Q}})$. There exists K a number field such that $x \in U(K)$. We write $P_i(x) = \sum_{j=1}^{N} a_{ij} x^j$ where N is the number of monomials $x^j = x_0^{i_0} \dots x_n^{i_n}$ of degree d. Let $v \in \Sigma(K)$. By the triangular inequality for v, there exists a constant N_v such that

$$|y_1 + \ldots + y_N|_v \leq N_v \max(|y_1|_v, \ldots, |y_N|_v). \tag{6.5}$$

Note that one could take $N_v = 1$ for any finite place v. We then get

$$|P_i(x)|_v \leq N_v \max_j |a_{ij}|_v \max_i |x_i|_v^d. \tag{6.6}$$

Let $A_v = \max_{i,j} |a_{ij}|$. Note that $A_v = 1$ but for a finite number of places v. We get

$$H_K(\Phi(x)) = \prod_v \max_i |P_i(x)|_v \leq \prod_v N_v A_v \max_i |x_i|_v^d = (\prod_v N_v A_v) H_K(x)^d$$

so that $c_1 = (\prod_v N_v A_v)^{1/[K:\mathbb{Q}]}$ works.

(ii) Let $V = V(Q_1, \ldots, Q_r)$. Since $V \cap Z = \emptyset$, by porjective Nullstellensatz, there exists $M > 0$ and polynomials A_{ij} and B_{ij} such that

$$x_j^M = \sum A_{ij} P_i + \sum B_{ij} Q_i.$$

Note that one can assume that the polynomials A_{ij} are homogeneous of degree $M - d$. Up to replacing K by a fintie extension, one could also assume that the polynomials in the equality above have their coefficients in K. We then have, for any $x = (x_0, \dots x_n) \in V$:

$$|x_j|_v^M = |\sum A_{ij} P_i|_v \leq (m+1)_v \max_i |A_{ij}(x)|_v \max_i |P_i(x)|_v,$$

where $(m+1)_v$ are constants defined as in (6.5). We apply the inequalities 6.6 to the homogeneous polynomials A_{ij} of degree $M - d$, so that one could write

$$|x_j|_v^M \leq A'_v \max_i |x|_v^{M-d} \max_i |P_i(x)|_v$$

for some constants A'_v such that $A'_v = 1$ but in a finite number of places. We deduce

$$\max_j |x_j|_v^d \leq A'_v \max_i |P_i(x)|_v,$$

and we get the result by taking the product over v.

□

Remark. In the theorem above one could write $h(\Phi(x)) = dh(x) + \mathcal{O}(1)$.

6.2.2 Weil height on an elliptic curve

Let $E \subset \mathbb{P}^2_{\overline{\mathbb{Q}}}$ be an elliptic curve defined by

$$Y^2Z = X^3 + aXZ^2 + bZ^3. \tag{6.7}$$

For $P \in E(\overline{\mathbb{Q}})$ one defines

$$h(P) = \begin{cases} h(x_P), & P \neq 0_E \\ 0, & P = 0_E. \end{cases}$$

Theorem 6.2.8. *There exists a constant c_1 such that for any $P \in E(\overline{\mathbb{Q}})$ one has*

$$-c_1 \leq h(2P) - 4h(P) \leq c_1.$$

Proof. The statement is immediate if $P = 0$ or a 2-torsion point. Assume $x_{2P} \neq 0$. By lemma 6.2.10 below, the polynomials $P_0(T, X) = 4T(X^3 + aXT^2 + bT^3)$ and $P_1(T, X) = X^4 - 2aX^2T^2 - 8bXT^3 + a^2T^4$ have no common roots in $\mathbb{P}^1$. We apply theorem 6.2.7(i) to $\Phi : \mathbb{P}^1 \to \mathbb{P}^1$, $\Phi = (P_0 : P_1)$. Since $\Phi(1 : x_P) = (1 : x_{2P})$, we deduce

$$h(2P) = h(1 : x_P) = h(\Phi(1, x_P)) = 4h(P) + \mathcal{O}(1).$$

□

Theorem 6.2.9. *(i) $h(P) = h(-P)$;*

(ii) $h(P + Q) + h(P - Q) = 2h(P) + 2h(Q) + \mathcal{O}(1)$.

Proof. Assertion (i) is immediate. We show (ii). We may assume $Q \neq \pm P$. By 3.1.6, we have:

$$x_{P+Q} + x_{P-Q} = \frac{2(x_P + x_Q)(a + x_Px_Q) + 4b}{(x_P + x_Q)^2 - 4x_Px_Q}$$
$$x_{P+Q}x_{P-Q} = \frac{(x_Px_Q - a)^2 - 4b(x_P + x_Q)}{(x_P + x_Q)^2 - 4x_Px_Q}.$$

By theorem 6.2.7(ii) and lemma 6.2.10 we deduce that for the map

$$\Phi(T, U, V) : \mathbb{P}^2 \to \mathbb{P}^2$$
$$(T : U : V) \mapsto (U^2 - 4TV : 2U(aT + V) + 4bT^2 : (aT - V)^2 - 4bTU)$$

one has

$$h(\Phi(x)) = 2h(x) + \mathcal{O}(1).$$

Let

$$\psi : (E \setminus 0_E)^2 \to \mathbb{P}^2$$
$$(P, Q) \mapsto (1 : x_P + x_Q, x_Px_Q)$$

and $\mu(P,Q) = (P+Q, P-Q)$. We then have $\psi \circ \mu = \Phi \circ \psi$ and by lemma 6.2.11 below

$$h(\psi(P,Q)) = h(x_P) + h(x_Q) + \mathcal{O}(1).$$

We deduce

$$\begin{aligned} h(P+Q) + h(P-Q) &= h(1 : x_{P+Q} + x_{P-Q} : x_{P+Q}x_{P-Q}) + \mathcal{O}(1) = \\ &= h(\psi \circ \mu(P,Q)) + \mathcal{O}(1) = H(\Phi \circ \psi(P,Q)) + \mathcal{O}(1) = \\ &= 2h(\psi(P,Q)) + \mathcal{O}(1) = 2h(P) + 2h(Q) + \mathcal{O}(1). \end{aligned}$$

□

Lemma 6.2.10. *Let k be a field. Let $a, b \in k^*$ with $4a^3 + 27b^2 \neq 0$.*

(i) The polynomials x^3+ax+b et $x^4+2ax^2-8bx+a^2$ in $k[x]$ are relatively prime.

(ii) The homogeneous polynomial $U^2-4TV, 2U(aT+V)+4bT^2, (aT-V)^2-4bTU$ have no commun roots $\mathbb{P}^2_k$.

Proof. The statement (i) follows from :

$$\begin{aligned} (3x^2+4a)(x^4-2ax^2-8bx+a^2) - (3x^3-5ax-27b)(x^3+ax+b) = \\ = 4a^3 + 27b^2. \quad (6.8) \end{aligned}$$

The statement (ii) is trivial if $T = 0$. Assume $T \neq 0$ ans denote $u = U/2T$ and $v = V/T$. One has $u^2 - v = 2u(a+v) + 4b = 0$ et $(v-a)^2 - 8bu = 0$, so that $u^4 - 2au^2 - 8bu + a^2 = u^3 + au + b$, contradiction with (6.8). □

Lemma 6.2.11. *Let $\alpha, \beta \in \overline{\mathbb{Q}}$. Then*

$$1/2H(\alpha)H(\beta) \leq H(1 : \alpha+\beta : \alpha\beta) \leq 2H(\alpha)H(\beta).$$

Proof. Let K be a number field such that $\alpha, \beta \in K$. The statement follows from:

$$\max\{1, |\alpha+\beta|_v, |\alpha\beta|_v\} = \max\{1, |\alpha|_v\}\max\{1, |\beta|_v\}, v \in \Sigma_{fini}(K);$$

$$\begin{aligned} 1/2\max\{1, |\alpha|_v\}\max\{1, |\beta|_v\} \leq \max\{1, |\alpha+\beta|_v, |\alpha\beta|_v\} \leq \\ \leq 2\max\{1, |\alpha|_v\}\max\{1, |\beta|_v\}, v \in \Sigma_\infty(K). \end{aligned}$$

□

6.2.3 Néron-Tate height on an elliptic curve

The goal of this section is to define a height function for the points of an elliptic curve E which is a quadratic form.

Lemma 6.2.12. *Let S be a set. Assume that we have functions $h : S \to \mathbb{R}$ and $g : S \to S$ such that there are constants $d > 1$ and $c > 0$ such that*

$$|h(g(x)) - dh(x)| < c \text{ for any } x \in S.$$

Then for any $x \in S$ the sequence $x_n = \frac{h(g^n(x))}{d^n}$ converges in $\mathbb{R}$. If $\hat{h}(x)$ is the limit of the sequence (x_n), then

$$|h(x) - \hat{h}(x)| \leq c/(d-1)$$
$$\hat{h}(g(x)) = d\hat{h}(x).$$

Proof. Let us show that the sequence (x_n) is a Cauchy sequence. We write the inequality $|h(g(x)) - dh(x)| < c$ for $x = g^{k-1}(x)$:

$$-\frac{c}{d^k} \leq \frac{h(g^k(x))}{d^k} - \frac{h(g^{k-1}(x))}{d^{k-1}} \leq \frac{c}{d^k}.$$

We take a sum between $n+1$ and $n+m$ and we get

$$-\frac{c}{d^n(d-1)} \leq \frac{h(g^{n+m}(x))}{d^{n+m}} - \frac{h(g^n(x))}{d^n} \leq \frac{c}{d^n(d-1)}.$$

The sequence (x_n) is then a Cauchy sequence, we set $\hat{h}(x)$ its limit. Passing to the limit in the inequalities above, we get

$$-\frac{c}{d^n(d-1)} \leq \hat{h}(x) - \frac{h(g^n(x))}{d^n} \leq \frac{c}{d^n(d-1)},$$

so that $|h(x) - \hat{h}(x)| \leq c/(d-1)$. In addition,

$$\hat{h}(g(x)) = \lim_{n\to\infty} h(g^{n+1}(x))/d^n = d \lim_{n\to\infty} h(g^{n+1}(x))/d^{n+1} = d\hat{h}(x).$$

□

Let E be an elliptic curve defined over a number field K. By theorem 6.2.8, if we set $S = E(K)$, h the Weil height on E and g the multiplication by 2 on $E(K)$, then the conditions of the previous lemma are satisfied (with $d = 4$). We can then define :

Definition 6.2.13. The **Néron-Tate** height on E is defined by

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(x_{2^n P})}{4^n}.$$

Theorem 6.2.14. *(i)* $\hat{h}(P+Q)+\hat{h}(P-Q)=2\hat{h}(P)+2\hat{h}(Q)$;

(ii) $\hat{h}(P)=0$ *iff* P *is a torsion point.*

Proof. We get the statement (i) passing to the limit on n in inequalities

$$-c/4^n \leq \frac{h(2^n(P+Q))}{4^n}+\frac{h(2^n(P-Q))}{4^n}-\frac{h(2^nP)}{4^n}-\frac{h(2^nQ)}{4^n} \leq c/4^n$$

in the theorem 6.2.9.

If $mP=0$, then $0=\hat{h}(mP)=m^2\hat{h}(P)$, so that $\hat{h}(P)=0$. Inversely, if $\hat{h}(P)=0$, then $\hat{h}(mP)=0$ for all m. But the set $\{mP, m\in\mathbb{Z}\}$ is finite, so that P is torsion. □

Corollary 6.2.15. *Let E be an elliptic curve defined over a number field K. Then the torsion subgroup $E(K)_{tors}$ of $E(K)$ is a finite group.*

Proof. The statement follows from the previous theorem and the fact that we have only a finite number of points of bounded height. □

6.3 Mordell-Weil theorem

The goal of this section is to give a proof of the following famous theorem:

Theorem 6.3.1. [Mordell-Weil] *Let E be an elliptic curve over a number field K. The group $E(K)$ is an abelian group of finite type.*

In particular $E(K)=E(K)_{tors}\oplus\mathbb{Z}^r$ where the group of torsion points $E(K)_{tors}$ of E is finite and r is by definition the **rank** of E.

The proof is in two steps:

1. Let E/K be an elliptic curve defined by the equation $y^2=x^3+ax+b$ such that the polynomial $P_3(x)=x^3+ax+b$ has three roots in K. A decent argument and the existence of the quadratic height function $\hat{h}$ on $E(K)$ show that theorem 6.3.1 is a consequence of its "weak" version: le group $E(K)/2E(K)$ is finite.

2. In order to show the weak Mordell-Weil theorem we construct a homomorphism $E(K)\to(K^*/K^{*2})^3$ with kernel $2E(K)$ and finite image. This last property uses in particulr the Dirichlet theorem on units in the ring of integers of a number field (see below).

6.3.1 Descent

Proposition 6.3.2. *Let G be an abelian group and let $q : G \to \mathbb{R}$ be a quadratic form. Assume*

(i) the quotient $G/2G$ is finite;

(ii) for any $c \in \mathbb{R}$, the set $\{x \in G, q(x) \leq c\}$ is finite.

Then the group G is an abelian group of finite type : if S is the set of representatives for each class of $G/2G$ and if $c = max_{x \in S} q(x)$, then the set $\{x \in G\, q(x) \leq c\}$ generates G.

Proof. Note first that for any $x \in G$ one has $q(x) \geq 0$. In fact, if it was not the case, we would have $q(mx) = m^2 q(x) < 0$ for any integer $m > 0$, contradiction with *(ii)*. So that we could define

$$|x| = \sqrt{q(x)}.$$

Since q is a quadratic form, we have $|mx| = m|x|$ for any $m > 0$ and $|x+y| \leq |x|+|y|$.

Let c as in the statement and let $x \in G$ with $q(x) > c$. One could write $x = y_1 + 2x_1$ for $x_1 \in G$ and y_1 in the set of representatives of $G/2G$, in particular $|y_1| \leq \sqrt{c}$. We have

$$|x_1| = \frac{1}{2}|x_0 - y_1| \leq \frac{1}{2}|x_0| + |y_1| \leq \frac{1}{2}(|x_0| + \sqrt{c}) < |x_0|.$$

We then construct inductively the sequence (x_n) with $x_0 = x$ and $x_n = y_{n+1} + 2x_{n+1}$ and $|x_{n+1}| < |x_n|$. By the finiteness condition (ii), there exists n_0 such that $|x_{n_0|} < \sqrt{c}$. We then get that x is a combination of y_i, $i \leq n_0$ and and x_{n_0}, which are in the finite set S. □

"Weak" version implies theorem 6.3.1. Let E/K an elliptic curve defined by an equation $y^2 = x^3 + ax + b$. Let L/K be a finite extension such that L contains the decomposition field of the polynomial $P(x) = x^3 + ax + b$. We have an inclusion $E(K) \subset E(L)$, hence, if $E(L)$ is an abelian group of finite type, then $E(K)$ is lso of finite type. Up to replacing K by L, we may then assume that E is given by the equation (6.9).

The "weak" version gives the finiteness of the group $E(K)/2E(K)$. But we also have the Néron-Tate height $\hat{h} : E(K) \to \mathbb{R}$ which is a quadratic form and verifies the condition that for any $c \in \mathbb{R}$, the set $\{x \in E(K), \hat{h}(x) \leq c\}$ is finite. By proposition 6.3.2, the group $E(K)$ is an abelian group of finite typei. □

6.3.2 Dirichlet units theoerm

In order to establish the Mordell-Weil theorem we will need to use some additional properties of units in $\mathcal{O}_K$.

Definition 6.3.3. Let S be a finite set of prime ideals in $\mathcal{O}_K$. The ring of S-**algebraic integers** of K is the ring

$$\mathcal{O}_{K,S} = \{x \in K, \, \mathrm{ord}_{\mathfrak{p}}(x) \geq 0 \, \forall \mathfrak{p} \notin S\}.$$

We denote $\mathcal{O}_{K,S}^*$ the set of S-**units**. Note that if S is empty, then $\mathcal{O}_{K,S}^* = \mathcal{O}_K^*$.

Assume that K has r_1 real embeddings and r_2 pairs of conjugated complex embeddings. We consider a map

$$\Phi_{K,S} : \mathcal{O}_{K,S}^* \to \mathbb{R}^{r_1+r_2+|S|}$$
$$\Phi_{K,S}(x) = \prod_{i=1,\ldots,r_1+r_2} \log \sigma_i(x) \cdot \prod_{v \in S} \log |x|_v.$$

Lemma 6.3.4. *The image $\Phi_{K,S}(\mathcal{O}_{K,S}^*)$ is a discret subgroup of $\mathbb{R}^{r_1+r_2+|S|}$.*

Proof. Since Φ is a homomorphism, the image $I = \Phi_{K,S}(\mathcal{O}_{K,S}^*)$ is a subgroup of $V = \mathbb{R}^{r_1+r_2+|S|}$. Il is enough to show that there exists a neighborhood T of $0 \in V$ such that $T \cap I$ is finite. Let

$$T = \{x = (x_1, \ldots x_{r_1+r_2+|S|}) \in V, \, |x_i| < 1, i \leq r_1+r_2, |x_j| < \log N\mathfrak{p}, j \text{ corresponding to} \mathfrak{p} \in S.\}$$

Let $x = \Phi_{K,S}(\alpha) \in T \cap I$. The condition $|x_j| < \log N\mathfrak{p}$ for j corresponding to a prime $\mathfrak{p}$ implies that $|\mathrm{ord}_{\mathfrak{p}}(\alpha)| < 1$, so that $|\mathrm{ord}_{\mathfrak{p}}(\alpha)| = 0$. Hence, $\alpha \in \mathcal{O}_K^*$. In addition, $|\sigma_i(\alpha)|$ are bounded for all $i = 1, \ldots r_1 + r_2$. The finiteness of $T \cap I$ then follows from the lemma below. □

Lemma 6.3.5. *Let K be a number field havig r_1 real embeddings $\sigma_1, \ldots \sigma_{r_1}$ and r_2 pairs of conjugate complex embeddings $\sigma_{r_1+1}, \bar{\sigma}_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \bar{\sigma}_{r_1+r_2}$. Let $a_1, i = 1 \ldots, r_1 + r_2$ be strictly positive real numbers. Let*

$$U = \{\alpha \in \mathcal{O}_K, |\sigma_i(\alpha)| \leq a_i \, \forall \, i\}.$$

Then

(i) the set U is finite;

(ii) if $(a_1, \ldots, a_n) = (1, \ldots, 1)$, then any $\alpha \in U$ is a root of unity.

Proof. Let $\alpha \in U$ and let

$$\chi_{\alpha,K}(x) = \prod_{i=1}^{r_1}(x - \sigma_i(\alpha)) \prod_{j=1}^{r_2}(x - \sigma_{r_1+j}(\alpha))(x - \bar{\sigma}_{r_1+j}(\alpha)).$$

We have $\chi_{\alpha,K} \in \mathbb{Z}[x]$.We have $\chi_{\alpha,K}(\alpha) = 0$. SInce $|\sigma_i(\alpha)| \leq a_i \, \forall \, i$, the coefficients of $\chi_{\alpha,K}$ are bounded. We have only a finite number of such polynomials, so that we get the finiteness of U. If $(a_1, \ldots, a_n) = (1, \ldots, 1)$, then the condition $\alpha \in U$ implies that $\alpha^m \in U$ for any $m > 0$. SInce U is finite, we deduce that α is a root of unity. □

Theorem 6.3.6. [Dirichlet-Chevalley-Hasse] *Let K be a number field with r_1 real embeddings and r_2 pairs of conjugated complex embeddings. Let S be a finite set of prime ideals in $\mathcal{O}_K$, we denote $|S|$ its cardinaity (S could be empty). Then:*

(i) the group of S-units $\mathcal{O}_{K,S}^*$ is a groupe of finite type;

(ii) the rank of the group $\mathcal{O}_{K,S}^*$ equals to $r_1 + r_2 - 1 + |S|$.

Proof. We estalish here the part (i) of the theorem, it is enough for the applications to elliptic curves .

By lemma 6.3.5, $I := \Phi_{K,S}(\mathcal{O}_{K,S}^*)$ is a discrete subgroup of $\mathbb{R}^{r_1+r_2+|S|}$. By lemma below, there exist elements $v_1, \dots v_m \in I$ such that

(i) $v_i = \Phi_{K,S}(u_i)$, with $u_i \in \mathcal{O}_{K,S}^*$;

(ii) for any element $u \in \mathcal{O}_{K,S}^*$ we have $u = e \prod_i u_i^{r_i}$ with $r_i \in \mathbb{Z}$ and $e \in \ker \Phi_{K,S}$.

An element $e \in \ker \Phi_{K,S}$ verifies

(*) $\mathrm{ord}_{\mathfrak{p}}(e) = 0$ for any $\mathfrak{p} \in S$, in particular, $e \in \mathcal{O}_K$;

(**) $|\sigma_i(e)| = 1$ for any i.

In particular, conditions of lemma 6.3.5(ii) are satisfied, we then get that e is a root of unity and the set of such e is finite. We deduce from (ii) above that the group $\mathcal{O}_{K,S}^*$ is a group of finite type.

□

Lemma 6.3.7. *Let V be an $\mathbb{R}$-vector space of finite dimension. Let $I \subset V$ be a discret subgroup. Then there exist $\mathbb{R}$-linearly independent vectors $v_1, \dots, v_m \in V$ such that*

$$I = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_m.$$

Proof. Consider $w_1, \dots, w_n$ the maximal set of element of I, independent over $\mathbb{R}$. Hence $I' = \mathbb{Z}w_1 + \dots + \mathbb{Z}w_n \subset I$ and any element $a \in I$ could be written as $a = r_1w_1 + \dots + r_nw_n$ with $r_i \in \mathbb{R}$. Let

$$T = \{\sum \lambda_i w_i, 0 \leq \lambda_i \leq 1.\}$$

Since I is discret, $T \cap I$ is finite: $T \cap I = \{a_1, \dots, a_s\}$. From the argument above, we deduce that any $a \in I$ could be written as $a = a_i + a'$ with $a' \in I'$. In particular, I' is a subgroup of finite index in I, i.e. $dI \subset I'$ for some integer d. We then get that $I \subset \frac{1}{d}I'$ and $\frac{1}{d}I'$ is a free $\mathbb{Z}$-module of rank n. Hence I is a free $\mathbb{Z}$-module of finite rank $n \leq m$: let $v_1, \dots v_m$ be the generators of I. Since $w_1, \dots, w_n$ are independant over $\mathbb{R}$ and $\sum_{i=1}^n \mathbb{R}w_i \subset \sum_{j=1}^r \mathbb{R}v_j$, we deduce that $n = m$ and that $v_1, \dots, v_m$ are $\mathbb{R}$-linearly independent. □

6.3.3 Weak Mordell-Weil theorem

Let E be an elliptic curve over a number field K defined by an equation

$$y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \tag{6.9}$$

Let $P_i = (\alpha_i, 0)$. We define a map $\phi = (\phi_1, \phi_2, \phi_3) : E(K) \to (K^*/K^{*2})^3$ by

$$\phi_i(P) = \begin{cases} x_P - \alpha_i & P \neq P_i, 0_E \\ (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}), & P = P_i \\ 1 & P = 0_E \end{cases}$$

where we write $P = (x_P, y_P)$ the coordinates of the point P; the indices $i - 1$ and $i + 1$ are modulo 3.

Proposition 6.3.8. *The map ϕ is a homomorphism.*

Proof. By definition, for any point $P \in E(K)$, we have

$$\phi(P) = \phi(-P) = \phi(P)^{-1} \tag{6.10}$$

in $(K^*/K^{*2})^3$. Let $P, Q \in E(K)$ and let $R = -(P + Q)$, i.e.

$$P + Q + R = 0_E.$$

We then have $\phi(P + Q) = \phi(R)$ and we want to show that

$$\phi_i(P)\phi_i(Q)\phi_i(R) = 1, i = 1, 2, 3. \tag{6.11}$$

Let $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. Let $y = \lambda x + \mu$ the equation of the line L intersecting E in P, Q, R, so that the equation

$$f(x) - (\lambda x + \mu)^2 = 0$$

has three roots x_P, x_Q, x_R. We have the following cases to consider:

1. P, Q, R are all distinct from P_i and from 0_E. Consider

   $$g(x) := f(x + \alpha_i) - (\lambda x + \lambda\alpha_i + \mu)^2 = 0,$$

   then $g(x)$has three roots $x_P - \alpha_i, x_Q - \alpha_i, x_R - \alpha_i$. Since $f(\alpha_i) = 0$, the constant coefficient of the polynomial $g(x)$ is $(\lambda\alpha_i + \mu)^2$. We then have

   $$(x_P - \alpha_i)(x_Q - \alpha_i)(x_R - \alpha_i) = (\lambda\alpha_i + \mu)^2,$$

   and we get (6.11) in this case.

2. One point among P, Q, R is the point 0_E. By (6.10), one could assume that $R = 0_E$. One then gets (6.11) using (6.10) again.

3. One point among P, Q, R is the point P_i. One can assume $i = 1$ in order to simplify the notations. Using (6.10), one could assume $R = P_1$. We then argue as in the first case: the equation of the line L is $y = \lambda(x - \alpha_1)$ and the equation
$$f(x) = \lambda^2(x - \alpha_1)^2$$
has three roots: x_P, x_Q et α_1, i.e. the equation
$$(x - \alpha_2)(x - \alpha_3) = \lambda^2(x - \alpha_1)$$
has two roots x_P et x_Q. Let $x = x' + \alpha_1$. We then have that the equation
$$(x' + (\alpha_1 - \alpha_2))(x' + (\alpha_1 - \alpha_3)) = \lambda^2(x')^2$$
has two roots $\phi_1(P)$ and $\phi_1(Q)$, so that $\phi_1(P)\phi_1(Q) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3) = \phi_1(R)$, which implies (6.11).

□

Proposition 6.3.9. *The kernel of the map ϕ is $2E(K)$.*

Proof. By the previous proposition $\phi(2P) = \phi(P + P) = (\phi(P))^2 = 1$, so that $2E(K) \subset \ker\phi$. It is enough to establish the inclusion $\ker\phi \subset 2E(K)$. Let $P \in \ker\phi$. We can then find $z_i \in K^*$, $i = 1, 2, 3$ such that
$$x_P - \alpha_i = z_i^2. \tag{6.12}$$
Let u, v, w such that
$$u + v\alpha_i + w\alpha_i^2 = z_i$$
(in fact, u, v, w are solution of the Vandermonde linear system.) The equations (6.12) give the following conditions :
$$\begin{cases} u^2 - 2vwb - x_P = 0 \\ 2uv - 2vwa - bw^2 + 1 = 0 \\ v^2 + 2uw - aw^2 = 0, \end{cases}$$
so that $v^3 + vw^2a + bw^3 - w = 0$. Note that $w \neq 0$ (if not, $v = 0$ and we get a contradiction $1 = 0$ from the second equation). We then have
$$(v/w)^3 + a(v/w) + b = (1/w)^2.$$
We deduce that $Q = (v/w, 1/w)$ is a point of $E(K)$. One verifies that $P = 2Q$:
$$\begin{aligned} x_{2Q} = \frac{(v/w)^4 - 2a(v/w)^2 - 8b(v/w) + a^2}{4((v/w)^3 + a(v/w) + b)} = \\ = \frac{v^4 - 2av^2w^2 - 8bvw^3 + a^2w^4}{4w^2} = \\ = \frac{(aw^2 - 2uw)^2}{4w^2} + \frac{1}{4}(-2av^2 - 8bvw + aw^2) = \\ = u^2 - 2vwb - \frac{a}{2}(v^2 - aw^2 + 2uw) = x. \end{aligned} \tag{6.13}$$

□

Proposition 6.3.10. *The image $\phi(E(K))$ of the map ϕ dans $(K^*/K^{*2})^3$ is finite.*

Proof. By theorem 6.1.5, the group of classes $Cl(\mathcal{O}_K)$ is finite. One could then find a finite set S of places of K such that $\mathcal{O}_{K,S}$ is a principal ring. Up to enlarging S, one could assume in addition that $\Delta_E = -(4a^3 + 27b^3)$ is in $\mathcal{O}_{K,S}^*$. We have

$$\Delta_E = ((\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3))^2,$$

so that $\alpha_i - \alpha_j \in \mathcal{O}_{K,S}^*$. Let $P \in E(K)$. We write $x_P = u/v$ and $y_P = w/t$ with $u, v, w, t \in \mathcal{O}_{K,S}$ and

$$(u, v) = (w, t) = 1 \text{ in } \mathcal{O}_{K,S}. \tag{6.14}$$

We have

$$w^2v^3 = t^2(u - v\alpha_1)(u - v\alpha_2)(u - v\alpha_3).$$

Using conditions (6.14), we deduce that $v^3 = t^2$, up to a multiplicatin of v and t by units. One could then write $v = s^2$ and $t = s^3$, so that

$$P = (u/s^2, w/s^3),\ w^2 = (u - \alpha_1 s^2)(u - \alpha_2 s^2)(u - \alpha_3 s^2).$$

Any common divisor of $(u-\alpha_1 s^2)$ and $(u-\alpha_2 s^2)$ divides $(\alpha_1-\alpha_2)s^2$ and $(\alpha_1-\alpha_2)u$, so that it divides $(\alpha_1-\alpha_2) \in \mathcal{O}_{K,S}^*$. We then deduce that $(u-\alpha_1 s^2)$, $(u-\alpha_2 s^2)$ and $(u - \alpha_3 s^2)$ are relatively prime between them, so that

$$x_P - \alpha_i = \frac{u - \alpha_i s^2}{s^2} = \gamma_i r_i^2, \gamma_i \in \mathcal{O}_{K,S}^*.$$

Hence, $\phi(P) = (\gamma_1, \gamma_2, \gamma_3)$. The Dirichlet-Chevalley-Hasse theorem 6.3.6 implies that the group $O_{K,S}^*/(O_{K,S}^*)^2$ is finite. We deduce that $\phi(E(K))$ is finite. □

Theorem 6.3.11. [Weak Mordell-Weil] *Let E be an elliptic curve defined by equation (6.9). The group $E(K)/2E(K)$ is finite.*

Proof. By proposition 6.3.9, $E(K)/2E(K) \simeq \phi(E(K))$. This last group is finite by proposition 6.3.10. □

6.3.4 Computing the group $E(\mathbb{Q})$.

Let E be an elliptic curve over $K = \mathbb{Q}$ defined by an equation

$$y^2 = x^3 + ax + b = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

The proof of the weak Mordell-Weil theorem give in fact a method to detemine the group $E(\mathbb{Q})/2E(\mathbb{Q})$: we see that $Im\,\phi \subset \{(\gamma_1, \gamma_2, \gamma_3) \in (\mathcal{O}_{K,S}^*/(\mathcal{O}_{K,S}^{*2}))^3, \gamma_1\gamma_2\gamma_3 = 1\}$ where $S = \{p \text{ prime}, p|\Delta_E\}$. To determine the group $E(\mathbb{Q})_{tors}$ one could use the following result:

Theorem 6.3.12 (Lutz-Nagell)**.** *Let E be an elliptic curve $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. Let $P \in E(\mathbb{Q})$ be a torsion point. Then $x_P, y_P \in \mathbb{Z}$ and either $y_P = 0$ or $y_P^2 | 4a^3 + 27b^2$.*

Chapter 7

Elliptic curves over $\mathbb{C}$

In this chapter we briefly discuss elliptic curves defined over the field $\mathbb{C}$. In this case we can use in addition some analytic methods.

7.1 Elliptic functions

Let $\omega_1, \omega_2 \in \mathbb{C}$ be linearly independent over $\mathbb{R}$. Let $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subset \mathbb{C}$ be the corresponding lattice. The **fundamental domain** of Λ is the set

$$\prod = \{t_1\omega_1 + t_2\omega_2, 0 \leq t_1, t_2 < 1\}.$$

We have a bijection

$$\prod \xrightarrow{\sim} \mathbb{C}/\Lambda \tag{7.1}$$

so that we can identify $\prod$ with $\mathbb{C}/\Lambda$.

Definition 7.1.1. A **Λ-elliptic function** is a meromorphic function on $\mathbb{C}$ such that

$$f(z+w) = f(z)\, \forall w \in \Lambda, z \in \mathbb{C}.$$

These functions appear in the study of elliptic integrals

$$\int_\infty^x \frac{\mathrm{dt}}{\sqrt{t(t-1)(t-\lambda)}}.$$

Often we do not specify the lattice Λ and we say «an elliptic function». One could see an elliptic function f as a function on the quotient $\mathbb{C}/\Lambda$, using the isomorphism (7.1) above.

The set of all Λ-elliptic functions form a field that we denote $\mathcal{M}(\Lambda)$.

Recall that for any meromorphic function f and for any $z \in \mathbb{C}$, one defines the order $ord_z f$ and the residu $res_z f$. If f is elliptic, we have that $ord_z f$ and $res_z f$ depend only on the class of z in $\mathbb{C}/\Lambda$. We have the following properties.

Proposition 7.1.2. *Let f be an elliptic function.*

1. *If f has no poles, then f is constant;*

2. $\sum_{z\in\mathbb{C}/\Lambda} res_z f = 0$;

3. $\sum_{z\in\mathbb{C}/\Lambda} ord_z f = 0$;

4. $\sum_{z\in\mathbb{C}/\Lambda} ord_z f \cdot z \in \Lambda$.

5. *if f has only one pole z_0, then z_0 is not a simple pole.*

The constant functions are obviously elliptic. One defines

$$\rho(z) = \frac{1}{z^2} + \sum_{w\in\Lambda\setminus\{0\}} (\frac{1}{(z-w)^2} - \frac{1}{w^2})$$

the **Weierstrass function**.

Proposition 7.1.3. *1. the function ρ and its derivstive ρ' are elliptic;*

2. *the field $\mathcal{M}(\Lambda)$ of elliptic functions is generated by ρ and ρ':*

$$\mathcal{M}(\Lambda) = \mathbb{C}(\rho, \rho');$$

3. *we have*

$$\rho'(z)^2 = 4\rho(z)^3 - 60G_4\rho(z) - 140G_6 \tag{7.2}$$

where $G_{2k} = G_{2k}(\Lambda) = \sum_{w\in\Lambda\setminus\{0\}} \frac{1}{w^{2k}}, k \geq 2$;

4. *for*

$$g_2 = 60G_4 \text{ and } g_3 = 140G_6 \tag{7.3}$$

we have $g_2^3 - 27g_3^2 \neq 0$.

One also verifies the addition formulas for the Weierstrass function:

$$\rho(z_1 + z_2) = -\rho(z_1) - \rho(z_2) + \frac{1}{4}(\frac{\rho'(z_1) - \rho'(z_2)}{\rho(z_1) - \rho(z_2)})^2 \tag{7.4}$$

$$\rho(2z) = -2\rho(z) + \frac{1}{4}(\frac{\rho''(z)}{\rho'(z)})^2. \tag{7.5}$$

7.2 Properties of elliptic curves over $\mathbb{C}$

7.2.1 The group of points

Proposition 7.2.1. *Let E be a complex elliptic curve defined by the equation*

$$Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$$

where g_2 and g_3 are defined in (7.3). We then have a biholomorphic map

$$\Psi : \mathbb{C}/\Lambda \to E,\ z \mapsto [\rho(z) : \rho'(z) : 1]$$

which is a group isomorphism.

Proof. Consider first the surjectivity. Let $(x, y) \in E$. We then have that the function $h(z) = \rho(z) - x$ has a double pole at 0. Hence h has also a zero z_0 in $\prod$. We deduce from 7.2 that $\rho'(z_0)$ or $\rho'(-z_0)$ is y. Hence, either z_0, or $-z_0$ works.

For the injectivity assume that $\rho(z_1) = \rho(z_2)$ and that $\rho'(z_1) = \rho'(z_2)$. The goal is to show that $z_1 - z_2 \in \Lambda$. We distinguish the following cases :

1. If z_1 is the pole of ρ, then z_2 is also a pole, so that $z_1 - z_2 \in \Lambda$.

2. Assume that z_1 is not a pole of ρ. Note that for ω_1, ω_2 and $\omega_3 = \omega_1 + \omega_2$ we have $\rho'(\omega_i/2) = \rho'(-\omega_i/2) = -\rho'(\omega_i/2)$ (the first equality is a consequence of the fact that ρ' is elliptic). We then have that ρ' has three zeros $\omega_i/2$ in $\prod$. Since ρ' has only one pole of order 3 in $\prod$, we get that ρ' has no other zeros in $\prod$.

   If now $z_1 \neq \omega_i/2$ we introduce $h(z) = \rho(z) - \rho(z_1)$. Then $h(z) = 0$ for $z = z_1, z_2$ or $-z_1$. Since h has only one double pole in $\prod$, we deduce that $z_2 = -z_1$. Hence $y = \rho'(z_2) = \rho'(-z_1) = -y$ so that $\rho'(z_1) = 0$ which is not possible from the above argument.

3. If $z_1 = \omega_i/2$, we find $\rho'(z_1) = 0$, i.e. z_1 is a double root of h. But h has only two zeros (and $h(z_2) = 0$), so that $z_1 = z_2$.

In order to show that Ψ is a group homomorphism, we use the addition formulas for the Weierstrass function, we leave it as an exercise. □

Remark 7.2.2. 1. Let $a, b \in \mathbb{C}$ such that $a^3 - 27b^2 \neq 0$. The uniformization theorem says that there is a unique lattice $\Lambda \subset \mathbb{C}$ such that $g_2(\Lambda) = a$, $g_3(\Lambda) = b$. Up to a linear change of coordinates, any complex elliptic curve is given by an equation $y^2 = 4x^3 - g_2x - g_3$ with $g_2^3 - 27g_3^2 \neq 0$. We can always identify a complex elliptic curve with the quotient $\mathbb{C}/\Lambda$ for some lattice Λ. We call such a quotient a **complex torus**.

2. As a direct consequence of the proposition 7.2.1, we get the structure of the subgroup $E[n]$ of the n-torsion points, for a curve E defined over the field $\mathbb{C}$. In fcat, the kernel of the multiplication by n on $\mathbb{C}/\Lambda$ could be identified to $\{z \in \mathbb{C}, nz \in \Lambda\}/\Lambda = (\mathbb{Z}/n)^2$.

We also have another interpretation of the group of points of a complex elliptic curve, as a groupe of divisors.

Definition 7.2.3. A **divisor** D on $\mathbb{C}/\Lambda$ is a finite formal sum

$$D = \sum n_i z_i,\ z_i \in \mathbb{C}/\Lambda.$$

We define the **degree** of D by $deg(D) = \sum n_i$. A **principal** divisor is the divisor D of type

$$D = \sum_{z \in \mathbb{C}/\Lambda} (ord_z f) z$$

where f is an elliptic function.

The set of all divisors on $\mathbb{C}/\Lambda$ is an abelian group. We denote $Div(\mathbb{C}/\Lambda)$ this group, $Div^0(\mathbb{C}/\Lambda)$ is the subgroup of divisors of degree zero and $Div^p(\mathbb{C}/\Lambda)$ is the subgroup of principle divisors. By proposition 7.1.2.3 above, we have $Div^p(\mathbb{C}/\Lambda) \subset Div^0(\mathbb{C}/\Lambda)$.

Theorem 7.2.4 (Abel-Jacobi)**.** *The map*

$$Div(\mathbb{C}/\Lambda) \to \mathbb{C}/\Lambda,\ \sum n_i z_i \mapsto \sum n_i \cdot z_i$$

induces a group isomorphism

$$\phi : Div^0(\mathbb{C}/\Lambda)/Div^p(\mathbb{C}/\Lambda) \xrightarrow{\sim} \mathbb{C}/L.$$

Proof. (sketch) By proposition 7.1.2, the map ϕ is well defined. By the définition, it is a group homomorphism. Since $\phi(z - 0) = z$ for any $z \in \mathbb{C}/\Lambda$, the map ϕ is surjective. For the injectivity, if D is a divisor such that $\phi(D) = 0$, one explicitely constructs a function f such that $D = div(f)$. □

Corollary 7.2.5. *Let E be a complex elliptic curve $Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$ where g_2 and g_3 are defined in (7.3). We then have a group isomorphism*

$$Div^0(\mathbb{C}/\Lambda)/Div^p(\mathbb{C}/\Lambda) \to E.$$

Proof. We get an isomorphism as above by composition of the map ϕ and the map from proposition 7.2.1. □

7.2.2 The endomorphisms

Let E be a complex elliptic curve. By remark 7.2.2, one can identify it with the torus $\mathbb{C}/\Lambda$. On the other hand, for $u \in \mathbb{C}^*$, the multiplication by u induices an isomorphism between $\mathbb{C}/\Lambda$ and $\mathbb{C}/u\Lambda$. Up to multiplying by an element $u \in \mathbb{C}$ we can always assume that $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$ with τ in the Poincaré plan $\mathcal{H}$ (i.e. $Im\tau > 0$.)

Proposition 7.2.6. *Two complex tori $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau)$ and $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau')$ are isomorphic if and only if there is a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$ such that $\tau' = \frac{a\tau+b}{c\tau+d}$.*

Proof. Let $\phi : \mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau') \to \mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau)$ be a homomorphism. Note that ϕ is induced by a multiplication by an element $\alpha \in \mathbb{C}$ such that $\alpha(\mathbb{Z} \oplus \mathbb{Z}\tau') \subset \mathbb{Z} \oplus \mathbb{Z}\tau$. We then have $\alpha = c\tau + d$ and $\alpha\tau' = a\tau + b$ with $a, b, c, d \in \mathbb{Z}$. Hence $\tau' = \frac{a\tau+b}{c\tau+d}$. Since ϕ is an isomorphism, we have that the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is invertible, since $Im(\tau') = det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) Im(\tau)/|c\tau + d|^2$ we get $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$. □

Corollary 7.2.7. *Let $E = \mathbb{C}/\Lambda$ be an elliptic curve, where $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$. Then*

$$End(E) = \begin{cases} \mathbb{Z}, & [\mathbb{Q}(\tau) : \mathbb{Q}] > 2 \\ \mathbb{Z} + \mathbb{Z}A\tau, & [\mathbb{Q}(\tau) : \mathbb{Q}] = 2. \end{cases}$$

In the second case, the integer A is the coefficient of the minimal polynomial $A\tau^2 + B\tau + C$ of τ. We then say that E has **complex multiplication**.

Proof. We have $End(E) = \{\alpha \in \mathbb{C}, \mid \alpha\Lambda \subset \Lambda\}$. Using previous proposition we have that $\alpha = c\tau + d$ corresponds to the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$ such that $\tau = \frac{a\tau+b}{c\tau+d}$. We then get $c\tau^2 + (d-a)\tau - b = 0$. If $[\mathbb{Q}(\tau) : \mathbb{Q}] > 2$, we get $c = b = 0, a = d$, i.e. the multiplication by d. If $[\mathbb{Q}(\tau) : \mathbb{Q}] > 2$ and $A\tau^2 + B\tau + C$ is the minimal polynomial of τ, we find in addition $c = mA, d - a = mB, -b = mC$, so that $\alpha = mA\tau + d$. □

7.3 Complement : Fermat's Last Theorem

To finish this course we will explain the role of the elliptic curves in the proof of the Fermat's last theorem.

Let E be an elliptic curve defined over $\mathbb{Q}$. By a linear change of variables, one can assume that E is given by an equation

$$y^2 = x^3 + Ax + B, \ A, B \in \mathbb{Z}. \tag{7.6}$$

For any prime p, one has a curve

$$E_p : y^2 = x^3 + A_p x + B_p$$

where $A_p \in \mathbb{Z}/p$ (resp. B_p) is the reduction of A (resp. of B) modulo p. If $p \not| \Delta_E$, the curve E_p is an elliptic curve over $\mathbb{F}_p$. We say that E has **an additive reduction** at p if $A_p = B_p = 0$. If this happens for no prime p, we say that E has a

semi-stable reduction.

For any prime p and for any $r > 0$ one defines $a_{p^r} = p^r + 1 - \#E_p(\mathbb{F}_{p^r})$ if E_p is smooth. If it is not the case, one defines $a_{p^r} \in \{-1, 1, 0\}$ according to its type of reduction. If $n = \prod p_i^{r_i}$ is an integer, one defines $a_n = \prod a_{p_i^{r_i}}$. To an elliptic curve E one associates the series:

$$f_E(\tau) = \sum_{n=1}^{\infty} a_n q^n, q = e^{2\pi i \tau},$$

convergent for any $\tau \in \mathcal{H}$.

Theorem 7.3.1 (**Wiles, Breuil, Conrad, Diamond, Taylor**). **(Taniyama-Shimura-Weil Conjecture)**
Let E be the elliptic curve (7.6). The the curve E is modular : there exists an integer N such that for any $\tau \in \mathcal{H}$ one has

1. $f_E(\frac{a\tau+b}{c\tau+d}) = (c\tau+d)^2 f_E(\tau)$, $\forall \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, *with* $\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z}), c \equiv 0 \,(mod\ N)\}$;
2. $f_E(-\frac{1}{N\tau}) = \pm N\tau^2 f_E(\tau)$.

In 1994, A. Wiles established this conjecture for E semi-stable.

Let now

$$x^n + y^n = z^n, n \geq 3.$$

Assume that this equation has a nontrivial solution (a, b, c) with $a, b, c \in \mathbb{Z}$. It is enough to consider the case $n = \ell$ an odd prime. In 1986, Frey introduced an elliptic curve associated to such a solution

$$E_{\text{Frey}} : y^2 = x(x - a^\ell)(x + b^\ell).$$

Theorem 7.3.2 (Ribert, 1986)**.** *The curve E_{Frey} is not modular.*

This theorem and the theorem of A.Wiles imply that a solution (a, b, c) of the Fermat equation cannot exist.