Courbes elliptiques

objet du cours : une courbe elliptique E sur un corps $\mathbb{F}_q$ est une courbe lisse dans le plan projectif donnée par une équation (courte) de Weierstrass

$$y^2 = x^3 + ax + b \qquad a, b \in \mathbb{F}_q$$

Alors $E(\mathbb{F}_q) = \{(x,y) \in \mathbb{F}_q^2 \,/\, x, y \in E\}$ est un groupe fini commutatif de point neutre le point à l'infini O_E

1) rappels corps fini

A anneau commutatif, I idéal

I maximal $\iff A/I$ corps

I premier $\iff A/I$ intègre

Si A est intègre principal, $I = (f)$

si $I \neq 0$, I est premier $\iff I$ maximal $\iff f$ inéductible

exemple : $\mathbb{Z}$ principal

$I = (m)$ est premier ssi $m = p$ est un nombre premier.

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, p premier

multiplication, addition : division euclidienne

calcul d'inverse : Bezout

* Si k est un corps, $k[X]$ est principal

donc $k[X]/P(X)$ est un corps ssi P est inéductible sur k

on applique à $k = \mathbb{F}_p$

Si $P(X)$ sur $\mathbb{F}_p$ est inéductible de degré n

$\mathbb{F}_{p^n} = \mathbb{F}_p[X]/P(X)$ est un corps de cardinal p^n (car c'est un $\mathbb{F}_p$-ev de dimension n)

* addition, multiplication : division euclidienne par $P(X)$

* inverse : Bezout dans $\mathbb{F}_p[X]$

2 questions : 1) si Q irréductible de degré m, est-ce que $\mathbb{F}_p[X]/_{P(X)} \simeq \mathbb{F}_p[X]/_{Q(X)}$

2) est-ce qu'il existe toujours P irréductible de degré m sur $\mathbb{F}_p$

* let $\mathbb{F}$ be a finite field

then $\mathbb{Z} \to \mathbb{F}$, $n \mapsto n.1$ has kernel (p)

So $\mathbb{F}$ is an $\mathbb{F}_p$ vector space, of finite dimension m

If $\mathbb{F} \subset \overline{\mathbb{F}_p}$, $\mathbb{F} = \{ x \in \overline{\mathbb{F}_p} \mid x^{p^m} - x = 0 \}$

proof : if $x = 0$ in $\mathbb{F}$ $\quad x^{p^m} = x$

if $x \neq 0$ $\quad x^{p^m - 1} = 1$ so $x^{p^m} = x$

So $\mathbb{F}_{p^m}$, if it exists, is unique

conversely, $\mathbb{F} = \{ x \in \overline{\mathbb{F}_p},\ x^{p^m} - x = 0 \}$ is a subfield of $\overline{\mathbb{F}_p}$ of cardinal p^m

exercice : $(x+y)^p = x^p + y^p$ over $\mathbb{F}_p$

and $x^{p^m} - x$ has exactly p^m roots in $\overline{\mathbb{F}_p}$ since it is prime with p'

structure : let $\mathbb{F}_{p^m}$ be the finite field with p^m elements

then • $\mathbb{F}_{p^m}$ is an $\mathbb{F}_p$ vector space of dimension m

$$(\mathbb{F}_{p^m}, +) \simeq \mathbb{F}_p^m$$

• $(\mathbb{F}_{p^m} \setminus \{0\}, *) \simeq \mathbb{Z}/_{p^m - 1}$

abelian

proof : $\mathbb{F}_{p^m}^*$ is a finite group of the form

$$\mathbb{Z}/_{d_1\mathbb{Z}} \otimes \mathbb{Z}/_{d_2\mathbb{Z}} \otimes \dots \otimes \mathbb{Z}/_{d_r\mathbb{Z}} \qquad d_1 | d_2 | \dots | d_r$$

But $X^{d_1} - 1$ has at most d_1 roots over $\mathbb{F}_{p^m}$ since it is a field

so 2 has to be equal to 1 so $\mathbb{F}_p^* = \mathbb{Z}/_{d_1\mathbb{Z}}$ and $d - 1 = p - 1$

corolary: let $x \in \mathbb{F}_p^*$ be a generator (there are $\varphi(p^m-1)$ such generators) then $\mathbb{F}_p(x) = \mathbb{F}_{p^m}$
so the minimal polynomial of x is irreductible of degree m

So every $\mathbb{F}_{p^m}$ is of the form $\mathbb{F}_{p^m} = \mathbb{F}_p[X]/P(X)$ with P irreductible of degree m

* field extension: if $\mathbb{F}_q \subset \mathbb{F}_{q'}$ with $q=p^m$, $q'=p^{m'}$ then $\mathbb{F}_{q'}$ is an $\mathbb{F}_q$-ev
so $(\mathbb{F}_{q'}, +) \simeq (\mathbb{F}_q, +)^d$ $\quad p^{m'} = p^{md}$

the converse is obvious since a root of $X^{p^m}-X$ is a root of $X^{p^{m'}}-X$

$\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \iff n \mid m$

we have, if $x \in \mathbb{F}_{q'}$, $x \in \mathbb{F}_q \iff x^q = x \iff \Pi_q(x) = x$

where $\Pi_q(x) = x^q$ is the q-Frobenius

2) How to compute multiplication

* $G = E(\mathbb{F}_p), +$

$P \mapsto mP = P+P+\dots+P$

* $G = \mathbb{F}_q^*$ $\quad$ m is going to be very large $\simeq 2^{256}$

$x \mapsto x^m$

fast multiplication: $m = \overline{b_k \dots b_0}^2$ in binary

$= \sum_{i=0}^{k} b_i 2^i$

$mP = \sum b_i 2^i P$

- right to left algorithm: compute all the multiples $2^i P$ by doubling each time $b_i = 1$ and add them

algo: $R=0$, $Q=P$, $i=0$

iterate: - if $b_i = 1$, $R = R+Q$
- $Q = 2Q$

total cost: k doubling, $\leq k$ additions $\Rightarrow O(\log m)$

- left to right algorithm : start at $i = k$, each time we double and we add P if $b_i = 1$

$\overline{10}^2$ $P \mapsto 2P$ double

$\overline{11}^2$ $P \to 2P$ double, $2P+P \hookrightarrow 3P$ add

$\overline{100\,111\,00}^2$

$P \to 2P \to 4P \to 8P+P \to \dots \to 156P$

- windowing : a window of size 2 = the same but 2 bits at a time
  = looking at n in base 4

1) we precompute $\overline{00}^2 \Rightarrow P=0$ $\overline{01}^2 \to P=P$ $\overline{10}^2 \to P=2P$ $\overline{11}^2 \to P=3P$

$\overline{10}\ \overline{01}\ \overline{11}\ \overline{00}$

- $2P$
- double double $\Rightarrow 8P$ and add $\overline{01}^2 \to P=P \Rightarrow 9P$
- double double $\Rightarrow 36P$ and add $\overline{11}^2 \to P=3P \Rightarrow 39P$
- double double $\Rightarrow 156P$

- sliding window : go to the right as long as there is not a 1 on the left of the window
  ↪ less computation

$\overline{10}\ 01\ 11\ 00$

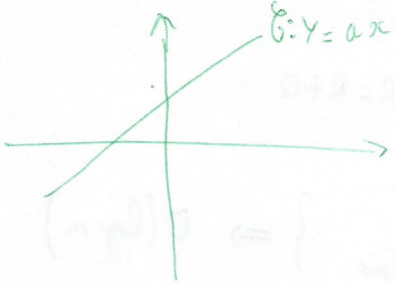
I Curve

An irreductible affine plane curve is given by an equation

$\mathcal{C}/_k$ $f(x,y) = 0$ where $f(x,y) \in k[X,Y]$ is irreductible

in $\mathbb{A}^2_k$

example : a line $y = ax+b$ is a curve



* A point P on the curve is $P=(x,y)$ such that $f(x,y)=0$

* $\mathcal{C}(\bar{k})$ = points of $\mathcal{C}$ in $\bar{k}$ $= \{P=(x,y),\ x,y \in \bar{k} \text{ and } f(x,y)=0\}$

example: the "circle" $x^2+y^2+1=0$ has no points in $\mathbb{R}$ but has points in $\mathbb{C}$

lemma: $\mathcal{C}$ is uniquely determined from $\mathcal{C}(\bar{k})$ (if it is reduced)

* let $P \in \mathcal{C}(\bar{k})$, $\mathcal{C}$ is smooth at P if either:
  * $\frac{\partial f}{\partial x}(x_P, y_P) \neq 0$

  or

  * $\frac{\partial f}{\partial y}(x_P, y_P) \neq 0$

in this case, $\mathcal{C}$ has a tangent at P given by the equation

$$\frac{\partial f}{\partial x}(x_P, y_P)\,(x-x_P) + \frac{\partial f}{\partial y}(x_P, y_P)\,(y-y_P) = 0$$

* elliptic curve: in general, an elliptic curve is given by a smooth affine equation of the form:

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

if car. $k \neq 2,3$, we can always do a linear change of variables to get

(caractéristique)

$$y^2 = x^3 + ax + b \quad \leftarrow \text{a short Weierstrass affine equation}$$

proof: $y^2 = x^3 + ax + b$ is irreductible in $\bar{k}[x,y]$ since x^3+ax+b has no square root in $k[x]$ since it is of degree 3

⚠ A curve of the form $y^2 = x^3 + ax + b$ is an elliptic curve only if it is smooth

example: $y^2 = x^3$ is not smooth at $(0,0)$ so it is not an elliptic curve

Theorem: $E: y^2 = x^3 + ax + b$ (car $k \neq 2,3$) is smooth if and only if

$f(x) = x^3 + ax + b$ has no multiple roots over $\overline{k}$

$\Leftrightarrow$ $\Delta_f \neq 0$ (discriminant)

$\Leftrightarrow \Delta_E = -16(4a^3 + 27b^2) \neq 0$

$= -16\,\Delta_f$

example: if $f(x) = ax^2 + bx + c$, $\Delta_f = b^2 - 4ac$

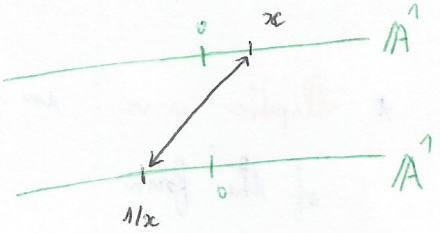
II projective line

$\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$

$= \mathbb{A}^1 \sqcup \mathbb{A}^1 / \sim$ where we glue the two $\mathbb{A}^1$ via the map

$\mathbb{A}^1 \setminus \{0\} \longrightarrow \mathbb{A}^1 \setminus \{0\}$

$x \longmapsto 1/x$



$\mathbb{P}^1(\overline{k}) = \{(x:y) \mid (x,y) \neq (0,0)\}$ where $(x:y)$ is the equivalence class of tuple (x,y) modulo the equivalence

$(x_1, y_1) = (x_2, y_2)$ if $\exists k \in \overline{k}^*$ such that $\begin{cases} x_2 = k\,x_1 \\ y_2 = k\,y_1 \end{cases}$

example: over $\mathbb{Q}$ $\quad (6:2) = (3:1) = (12:4) = \dots$

$(1:0) = (2:0) = (5:0) = \dots$

if $P \in \mathbb{P}^1(\overline{k})$, $P = (x,z)$ and $z \neq 0$ then $P = (\frac{x}{z}, 1)$

$\mathbb{A}^1 \longrightarrow \mathbb{P}^1$

$x \longmapsto (x:1)$ we get all the points except $\infty = (0:1)$

III Projective plane

$$\mathbb{P}^2(\bar{k}) = \{ (x:y:z) \in \bar{k}, \text{ where } (x,y,z) \neq (0,0,0) \} / \sim$$

modulo the equivalence relation $(x_1,y_1,z_1) \sim (x_2,y_2,z_2)$ if there exists $h \in \bar{k}^*$ such that $\begin{cases} x_2 = h x_1 \\ y_2 = h y_1 \\ z_2 = h z_1 \end{cases}$

$$\mathbb{P}^2(\bar{k}) = \mathbb{A}^3_{\setminus\{(0,0,0)\}} / \bar{k}^* = \text{set of lines in } \mathbb{A}^3 \text{ passing through } 0$$

$$\mathbb{A}^2 \longrightarrow \mathbb{P}^2$$
$$(x,y) \longmapsto (x:y:1)$$

$$\mathbb{P}^2 \setminus \mathbb{A}^2 = \{ (x:y:z) \text{ where } z \neq 0 \} = \{ (x:y:0) \text{ where } (x,y) \neq (0,0) \} = \mathbb{P}^1$$

$$\mathbb{P}^2 = \mathbb{A}^2 \sqcup \mathbb{P}^1$$
$$= \mathbb{A}^2 \sqcup \mathbb{A}^1 \sqcup \infty$$

2) projective curve

A projective curve $\mathcal{C}/k$ in $\mathbb{P}^2_k$ is given by an irreductible equation

$$F(X,Y,Z) = 0 \quad \text{where } F(X,Y,Z) \in k[X,Y,Z] \text{ is homogeneous and irreductible}$$

F homogeneous = all the terms have the same total degree

if $f(x,y)$ is a polynomial of degree d in two variables, we can construct its homogeneisation $F(X,Y,Z) = Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right)$

example : the homogeneisation of $y^2 = x^3 + ax + b$ is $Y^2Z = X^3 + aXZ^2 + bZ^3$

note : when F is homogeneous,

$$F(hx, hy, hz) = h^d F(x,y,z)$$

so "$F(x,y,z)=0$" does not depend on the equivalence class of $(x:y:z)$

If $\mathcal{E} \in \mathbb{A}^2$ is an affine curve given by $f(x,y)=0$

let $F(X,Y,Z)$ be the homogeneisation of f. Then $\overline{\mathcal{E}} \subset \mathbb{P}^2$ the projective curve given by $F(X,Y,Z)=0$ is the projective closure of $\mathcal{E} \subset \mathbb{A}^2$ into $\mathbb{P}^2$

we call the points $\overline{\mathcal{E}}(\bar{k}) \setminus \mathcal{E}(\bar{k})$ the points at infinity

these are the points $\{(x:y:0)\}$ where $F(x,y,z)=0$

example : for $Y^2Z = X^3 + aXZ^2 + bZ^3$ the points at infinity are given by

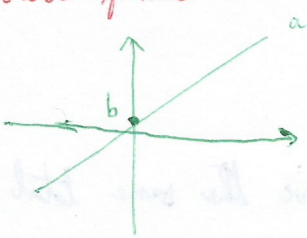
setting $Z=0 \Rightarrow X^3 = 0 \Rightarrow x=0$

$(0:y:0) = (0:1:0)$

definition : $O_E = (0:1:0)$ is the point at infinity of E

3) lines in the projective plane

a) $y = ax + b$

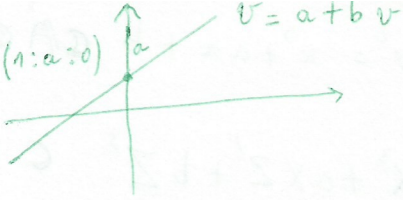


$Y = aX + bZ$

the point at infinity of this line is given by $Z=0 \Rightarrow Y = aX = (1:a:0)$

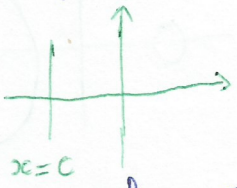
at this point, we can look at an affine equation by setting $v = \frac{Y}{X}$, $u = \frac{Z}{X}$

$\frac{Y}{X} = a + b\frac{Z}{X} \Rightarrow v = a + bu$



in the projective plane, lines always intersect at one point (a point at infinity if the lines are parallel)

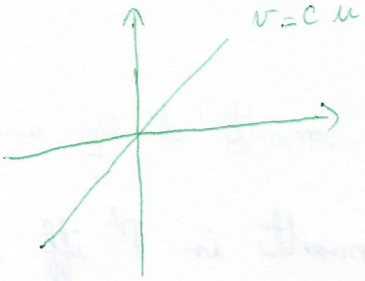
b) $x = c$



$X = cZ$ so when $Z=0$, $x=0$ so the only point is $(0:1:0)$

$\frac{X}{Y} = c\frac{Z}{Y} \Rightarrow v = cu$

$\frac{X}{Y}$ ~ v ; $\frac{Z}{Y}$ ~ u



4) smooth projective curves

Let $\mathcal{C} : F(X,Y,Z) = 0$ a projective curve, $P = (x_P : y_P : z_P) \in \mathcal{C}(\bar{k})$

$\mathcal{C}$ is smooth at P if either :

* $\frac{\partial F}{\partial X}(x_P, y_P, z_P) \neq 0$
* $\frac{\partial F}{\partial Y}(x_P, y_P, z_P) \neq 0$
* $\frac{\partial F}{\partial Z}(x_P, y_P, z_P) \neq 0$

in this case, the equation of the projective tangent line is given by

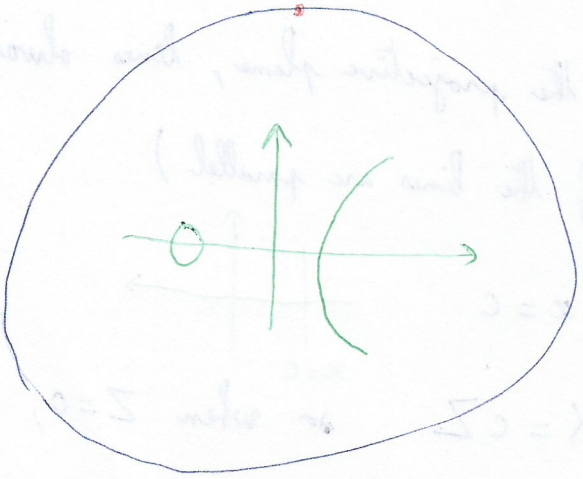
$$\frac{\partial F}{\partial X}(x_P, y_P, z_P)\, X + \frac{\partial F}{\partial Y}(x_P, y_P, z_P)\, Y + \frac{\partial F}{\partial Z}(x_P, y_P, z_P)\, Z = 0$$

exercise : show that if L is the affine tangent line of $\mathcal{C}$, $\bar{L}$ is the projective tangent line of $\bar{\mathcal{C}}$

example : $E: y^2 = x^3 + ax + b \subset \mathbb{A}^2$

$\bar{E}: Y^2Z = X^3 + aXZ^2 + bZ^3 \subset \mathbb{P}^2$

$O_E = (0:1:0)$



and $P = O_E = (0:1:0)$

$$\begin{cases} \frac{\partial F}{\partial X}(O_E) = 0 \\ \frac{\partial F}{\partial Y}(O_E) = 0 \\ \frac{\partial F}{\partial Z}(O_E) = Y^2 = 1 \end{cases}$$

so E is always smooth at O_E and the tangent line is $Z = 0$

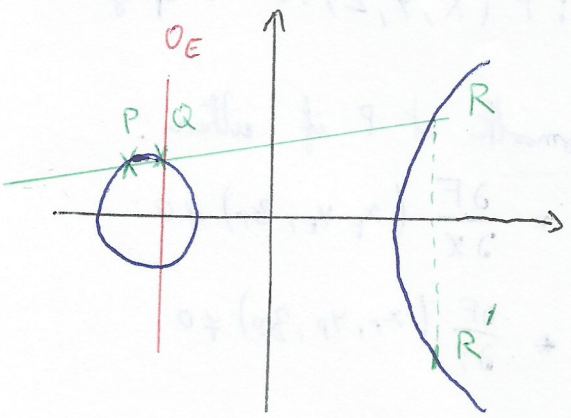
corollaire : E is smooth in $\mathbb{P}^2$ iff it is smooth in $\mathbb{A}^2$ (since O_E is always smooth)

$\iff \Delta_E = -16(4a^2 + 27b^2) \neq 0$

IV. Overview of the addition law

$E: y^2 = x^3 + \underset{a}{\cancel{\ }}x + b$

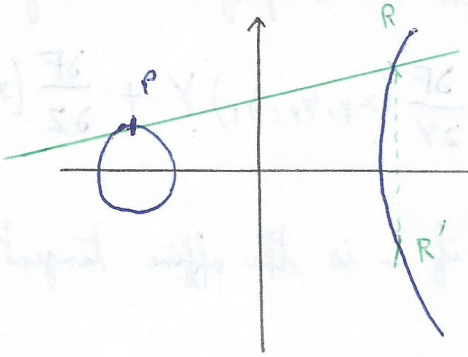
$\bar{E} \subset \mathbb{P}^2$



definition : $P + Q = R'$

* how about $P + P$?

$P + P = R'$



← tangent line of E at P it always exists since E is smooth