Remerciements

Nous tenons tout d'abord à remercier **Allah** le tout puissant et miséricordieux, qui nous a donné la force et la patience d'accomplir ce modeste travail.

En second lieu, nous tenons à remercier notre encadreur Mr: "**Youmbai Ahmed El Amine**", de son précieux conseil et son aide durant toute la période du travail.

Nos vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner notre travail et de l'enrichir par leurs propositions.

Nos remerciements s'étendent également à tous nos enseignants durant les années des études.

Nos familles et nos amis qui par leurs prières et leurs encouragements, on a pu surmonter tous les obstacles.

Enfin, nous tenons à remercier toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail.

****

Table des matières

Introduction générale

Les courbes elliptiques sont un sujet très à la mode en mathématiques. Elles sont à la base de la démonstration du grand théorème de Fermat par Andrew Wiles. Elle fut l'objet de plusieurs conjectures surtout sur son rang.

L'un des principal problème relié aux courbes elliptiques et le groupe de Tate-Shafarevich, un groupe plein de mistères "sa finitude" ou sont "cardinal". Dont les mathématiciens restent incapables de les résoudre.

Dans ce memoire nous allons le définir, pour cela nous avons passé par un chapitre de la théorie des courbes elliptiques. Le second chapitre traite la cohomologie des groupes finis, puis à partir de ces deux dérniers nous définissons le groupe de Tate-Shafarevich.

Ce groupe est conjecturé fini, mais nul ne la prouver, son cardinal à été calculer pour quelques courbes de façon trés difficile car les méthodes utilisés peuvent marcher pour une courbe et non pas pour une autre.

Chapitre 1

Courbe Elliptique

Nous allons consacré ce chapitre à une étude approfondie sur "Les courbes elliptiques", que nous allons commencer par la définition d'une "Courbe algébrique", et de passer ensuite aux invariants tel "Singularité d'un point", nous allons mentionner deux espaces "Espace affine et Espace projectif", et la relation entre eux, pour conclure nous avons donné la forme générale de l'équation de "Weierstrass" (ecrite sur chacun de ces deux espaces) et quelques équations équivalents.

1.1 Courbe Algébrique

Définition 1.1.1 *Toute courbe algébrique plane est définie par une équation algébrique* $f(x, y) = 0$, f *est un pôlynome de l'anneau* $K[x, y]$ *des polynômes sur un corps commutatif* K *global, local ou fini.*

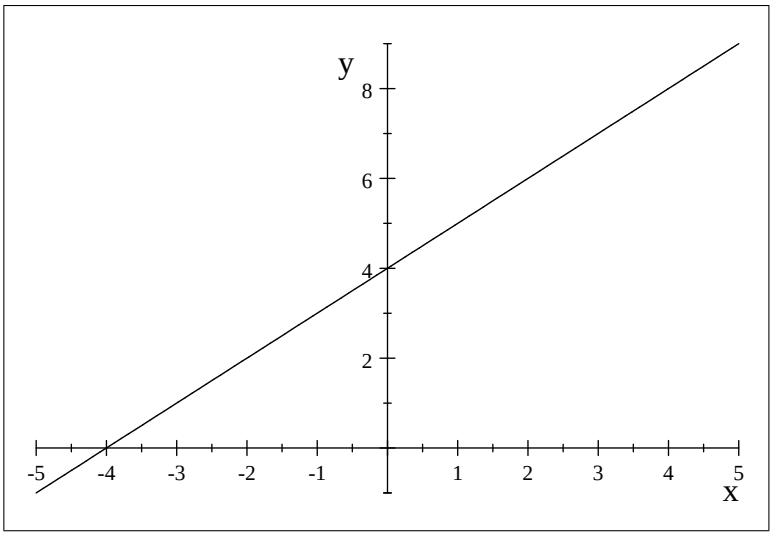
Définition 1.1.2 *Sous sa forme la plus génerale, une courbe algébrique sur un corps* K *est une variété de demension* 1 *sur* K. *Sébarée pour eviter des pathologies, en considérant les composantes irréductibles munies de la structure réduit en se ramène aux courbe projective réguliéres, ce qui est la situation la plus couramment abordée.*

En dehors des variétés algébrique de demension 0 qui se réduisent aux algèbres finies sur un corps, les courbes sont les premières variétés algébriques non triviales.

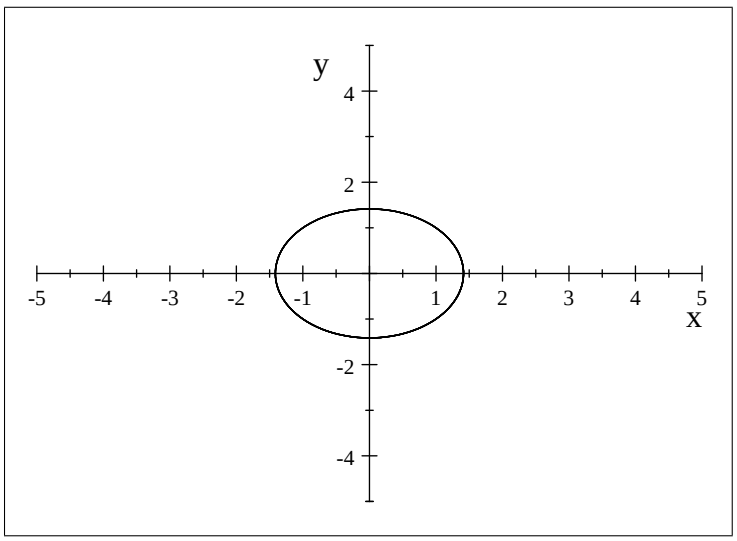
1. Une ensemble algébrique dans un espace affine $A^n(K)$ est l'ensemble des zéros d'une famille de polynôme $f_1, ..., f_d$ de l'anneau $K[X_1, ..., X_n]$.

2. Une variété affine est une partie irréductible et fermée d'un espace.

Exemple 1.1.1 *1.* $f = ax + by + c = 0$ *est l'équation d'une droite, par exemple:* $y = x + 4$



2. $f = (x-a)^2 + (y-b)^2 - r^2 = 0$ est l'équation d'un cercle, par exemple: $y^2 + x^2 = 2$



3. Pour $n = 3$ c'est l'équation d'une cubique.

1.2 Singularité d'un point

En mathématique, une singularité en générale d'un point, une valeur ou un cas dans lequel un certain objet mathematique n'est pas bien défini par exemple la fonction $x \mapsto \frac{1}{x}$ admet une singularité en $x = 0$

Un point d'une courbe est soit ordinaire soit singulier, la nature d'un point est précisée par la:

Définition 1: Soit C une courbe algèbrique, et un point $p\,(x, y)$ de C alors:

1. p est ordinaire si C admet en ce point une tangente unique, et cette tangente ne traverse pas la courbe C au voisinge de p.

2. p est un point d'un flexion si C admet en ce point une tangente unique qui traverse C au voisinage de p.

3. p est un point singulier(noeud), si C admet en ce point 2 tangentes distinctes.

4. p est un point singulier, point de rebrossement, si C admet en ce point 2 tangentes confondues.

Définition 1.2.1 *Une courbe algebrique plane C d'equation $f(x, y) = 0$ admet un point singulier s si elle satisfait:*

$$f(s) = 0, f'_x(s) = 0, f'_y(s) = 0$$

Exemple 1.2.1 *Courbe algebrique C d'équation:*

$$C : f(x, y) = y^3 + 3x^2 - 2xy \ \in R[x, y]$$

Dérivées partielle de f:

D'ordre 1: $f'_x = 6x - 2y$, $f'_y = 3y^2 - 2x$

D'ordre 2: $f''_{x^2} = 6$, $f''_{xy} = -2$, $f''_{y^2} = 6y$

Calculs: $f'_x(s) = f'_y(s) = 0$ implique $s = (0, 0)$, $f''_{x^2} = 6$

Donc le point s est un point singulier double, le nombre de points singuliers d'une courbe algebrique plane permet d'introduire un invariant: le genre de C.

Définition de genre: Soit une courbe algébrique plane de dégrée n qui possède s points singuliers.

Alors son genre est égal à l'entier positif ou nul égale à:

$g(C) = (n-1)(n-2)/2 - s$

Exemple 1.2.2 *Courbe C d'équation:*

$$f(x,y) = -x^3 + 3x + y^2 - 2y - 1 = 0$$

$$f'_x = -3x^2 + 3 \quad , f'_y = 2y - 2$$

Ce système admet les solutions $(1,1)$ et $(-1,1)$

$f(1,1) = f'_x(1,1) = f'_y(1,1) = 0$, alors le point $p = (1,1)$ est singulier.

$f(-1,1) = -4 \neq f'(-1,1) = f'_y(-1,1) = 0$, alors le point $p = (-1,1)$ est non singulier.

1.3 Espace Affine

Définition 1.3.1 *Un n-espace affine est l'ensemble des points de l'espace K^n:*

$$A^n = A^n(K) = \{a = (a_1, a_2, ...a_n); a_1, a_2, ...a_n \in K\}$$

C'est un espace de dimension n.

1. l'espace affine $A^2(\mathbb{R})$ est représenté par le plan réel O_{xy}, tout point p de cet espace a deux coordonnées $x; y$.

2. L'espace affine $A^1(\mathbb{C})$ est représenté par une droite; tout point p de cet espace a une coordonnée z qui est un nombre complexe.

3. L'espace affine $A^3(\mathbb{R})$ est représenté par l'espace $Oxyz$ à 3 dimensions; chaque point $p(x,y,z)$ a 3 coordonnées réelles.

Avec une relation d'équivalence sur un $(n+1)$-espace affine A^{n+1}, nous construisons un espace projectif P^n.

1.4 Espace Projectif

Définition 1.4.1 *Soit K un corps, le plan projectif $P^2(K)$ est l'ensemle des points*

$P=(a,b,c)\neq(0,0,0)\in K^3$ de sorte que deux points $P=(a,b,c)$ et $P'=(a',b',c')$ sont considérés comme étant des points équivalents s'il existe $t\in K^*$ tel que $(a,b,c)=t(a',b',c')$ les nombre a,b,c sont appelés les cordonnées homogènes du point P. Plus généralment, nous définissions le n-espace projectif $P^n(k)$ comme l'ensemble des classes d'équivalences des $(n+1)$-uples suivants

$$P^n(k)=\frac{\{(a_0,a_1,....,a_n)\in K^{n+1}/a_0,a_1...a_n \text{ non tous nuls}\}}{\sim}$$

où $(a_{0,}a_{1,}a_2,....,a_n)\sim\left(a'_{0,}a'_{1,}a'_2,....,a'_n\right)$ s'il existe $t\in K^*$

tel que $(a_{0,}a_{1,}a_2,....,a_n)=t\left(a'_{0,}a'_{1,}a'_2,....,a'_n\right)$. Si $n=2$, alors $P^2(\mathbb{R})$ est le plan projectif.

Définition 1.4.2 *Un $n-$espace projectif $P^n(K)$ est l'espace quotient d'un $(n+1)$-espace affine $A^{n+1}(K)$ par la relation d'équivalence T qui satisfait la condition:*

$$a=(a_1,...,a_{n+1})\,T\,(b_1,...,b_{n+1})=b$$

si seulement si: $a=\lambda.b$ pour $\lambda\neq0$ et $\lambda\in k$

Alors $P^n(K)=A^{n+1}/T$

Cette définition implique qu'un point P de l'espace projectif P^n admet $(n+1)$ coordonnées

$$P=(x_1,x_2,...,x_{n+1})\in P^n$$

Chaque point P est donc le représentant d'une classe:

$$cl(P)=\{(x_1,x_2,...,x_{n+1}),(\lambda x_1,\lambda x_2,...,\lambda x_{n+1}),(tx_1,tx_2,...,tx_{n+1}),...\}$$

Les coordonnées $x_1,x_2,...,x_{n+1}$ sont les coordonnées homogènes d'une point du plan projectif P^n.

Exemple 1.4.1 *Dans l'éspace (plan) projectif $P^2(\mathbb{R})$, il y a une infinité de classes :*

1. $Cl\,(1,1,1) = \{(2,2,2)\,,(-2,-2,-2)\,,(5,5,5)\,,.....\}$

2. $Cl\,(2,0,3) = \{(2,0,3)\,,(-2,0,-3)\,,(4,0,6)\,,.....\}$

3. $Cl\,(2,4,2) = \{(2,4,2)\,,(-2,-4,-2)\,,(4,8,4)\,,.....\}$

1.5 Le point à l'infini

Définition 1.5.1 *Dans le plane projectif l'intersection de deux droites parallèles a lieu en un point pour lequel $z = 0$. Un tel point est appelé point à l'infini. Pour plus de détails sur le point à l'infini voir* [4] *et* [2].

Il sera noté O, nous allons voir que ce point joue un rôle très important. En effet il appartient à toute les cubiques, de plus c'est un point non singulier.

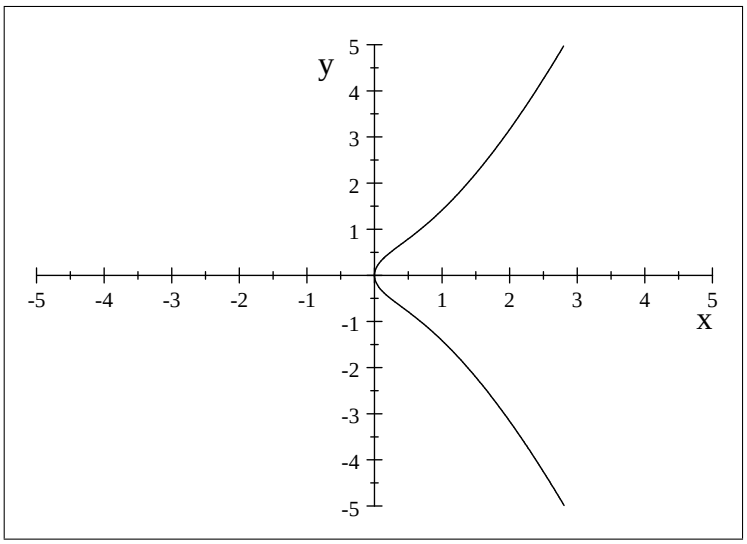
Désormé, nous avons le bagage nécéssaire pour définir une courbe élliptique.

1.6 Courbe Elliptique

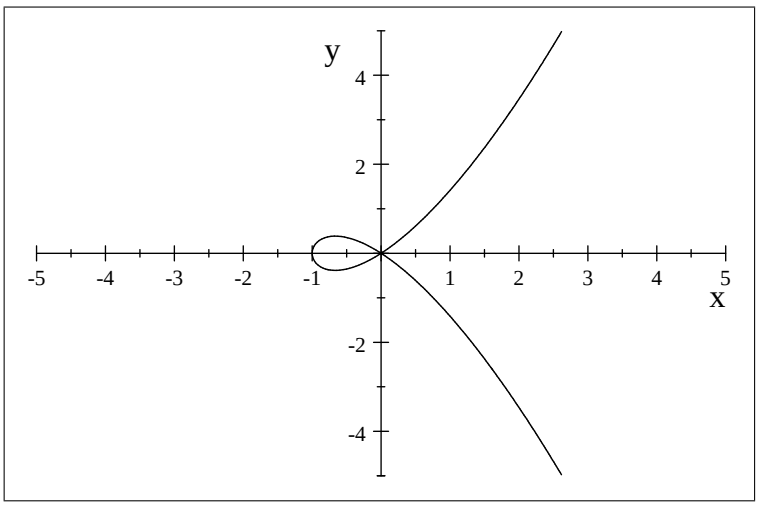
Définition 1.6.1 *Une courbe elliptique est une paire (E, O), où E est une cubique irreductible non singulière et $O \in E$. La courbe elliptique E est défini sur un corps K, si E est une courbe sur K et si $O \in E\,(K)$.*

Remarque 1.6.1 *K peut être un corps local, global ou fini.*

Exemple 1.6.1 *On prend $K = R$, on pose: $E_1 : y^2 = x^3 + x$*



et $E_2 : y^2 = x^3 + x^2$



les courbes E_1 et E_2 sont bien défini sur R puisque tous les coefficients sont réels, la courbe E_1 est lisse, en effet:

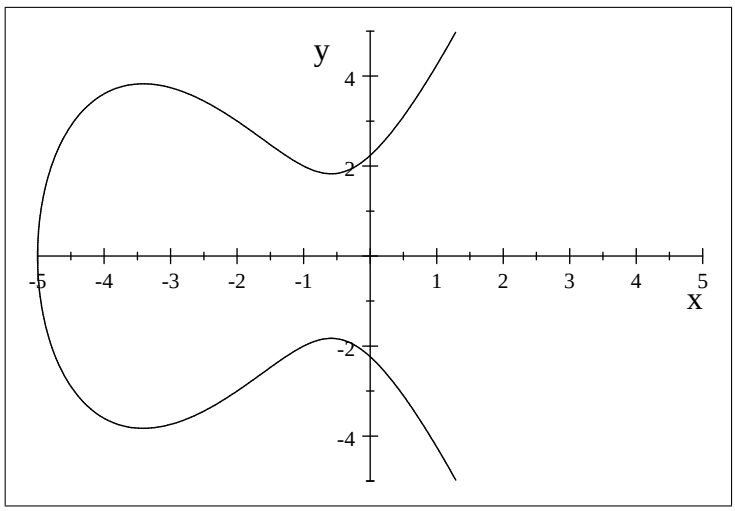
$$(\frac{\partial p}{\partial x}(x,y), \frac{\partial p}{\partial y}(x,y)) = (0,0) \Longleftrightarrow \left\{ \begin{array}{c} 3x^2+1=0 \\ 2y=0 \end{array} \right\} \Longleftrightarrow \left\{ \begin{array}{c} x = \frac{\pm i}{\sqrt{3}} \\ y = 0 \end{array} \right\}$$

or les points $\left(\frac{\pm i}{\sqrt{3}}, 0\right)$ne sont pas sur la courbe et E_1 est donc une courbe elliptique.

Pour E_2, le point $(0,0)$ est un point sur la courbe et on verifie aisément que:

$\frac{\partial p}{\partial x}(0,0) = \frac{\partial p}{\partial y}(0,0) = 0$ on dit alors que le point singulier alors la courbe E_2 n'est pas lisse et n'est pas une courbe elliptique.

Exemple 1.6.2 *Soit* $E(\mathbb{R})$ *définie par:* $E : y^2 = x^3 + 6x^2 + 6x + 5$



1.7 Equation de Weierstrass

Théorème 1.7.1 *Si* E *est une courbe elliptique définie sur un corps* K*, alors il existe une application :* $\phi\ E(K) \rightarrow P^2(k)$ *qui fournit un isomorphisme de* $E(K)$ *sur une courbe* $C\ (K)$ *donnée par l'équation de weierstrass (forme projective):*

$$C : F(x, y, z) = y^2z + a_1xyz + a_3xyz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 = 0$$

Où $a_1, ..., a_6 \in K$, et tel que $\phi(o) = (0, 1, 0)$. Le point $O = [0, 1, 0]$ est appelé point à l'infini.

Théorème 1.7.2 *Pour* $z \neq 0$*, on peut écrire* $x = \frac{x}{z^2}$, $y = \frac{y}{z}$ *et l'équation de weierstrass devient (forme affine):*

$$E : y^2 + a_1 + xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Si la caractéristique de K *est différente de* 2*, l'équation peut s'écrire:*

$$E : y^2 = x^3 + \grave{a}_2x^2 + \grave{a}_4x + \grave{a}_6$$

Si la caractéristique de K *est différente de* 2 *et de* 3*, l'équation peut s'écrire:*

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

1.8 Discriminant d'une cubique

Définition 1.8.1 *Le discriminant Δ de l'équation de weierstrass est la quantité*

$$\Delta = b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6$$

tel que:

$$b_2 = a_1^2 + 4a^2,\ b_4 = 2a_4 + a_1 a_3,\ b_6 = a_3^3 + 4a_6,\ b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$$

Corollaire 1.8.1 *Soit un courbe K de caractéristique p. Une courbe E définie sur K donnée par une équation de weierstrass prend alors une forme simplifiée*

Si $p \neq 2$, et $p \neq 3$:

$$y^2 = x^3 + a_4 x + a_6$$

Dans ce cas le discriminant

$$\Delta = -16\left(4a_4^3 + 27a_6^2\right)$$

Théorème 1.8.1 *Soit E une courbe donnée par une équation de weierstrass. Alors E est non singulière si et seulement si $\Delta \neq 0$*

Preuve. Montrons d'abord que le point à l'infini $O = (0, 1, 0)$ n'est jamais singulier.

Regardons E comme une courbe de $P^2(\Bbbk)$ donné par son équation

$$F(x, y, z) = y^2 z + a_1 xyz + a_3 yz^2 - x^3 - a_2 x^2 z - a_4 xz^2 - a_6 z^3 = 0$$

comme $\frac{\partial F}{\partial z}(0) = 1 \neq 0, O$ n'est pas un point singulier de E.

Pour les autres points considérons la définition de la courbe E par son équation de weierstrass réduite:

$$E : f(x, y) = y^2 - x^3 - ax - b = 0$$

La courbe est singulière en un point $p_0 = (x_0, y_0) \in E$ si et seulement si:

$$\left\{ \begin{array}{c} \frac{\partial f}{\partial x}(x_0, y_0) = -3x_0^2 - a = 0 \\ \frac{\partial f}{\partial y}(x_0, y_0) = 2y_0 = 0 \end{array} \right\}$$

$$\left\{ \begin{array}{c} 3x_0^2 + a = 0 \\ 2y_0 = 0 \end{array} \right\}$$

$$\left\{ \begin{array}{c} x_0^2 = \frac{-a}{3} \\ y_0 = 0 \end{array} \right\}$$

Or p_0 est point de la courbe, par conséquent:

$$y_0^2 = 0 = x_0^3 + ax_0 + b = \frac{-a}{3}x_0 + ax_0 + b = \frac{2}{3}ax_0 + b$$

Il s'ensuit que

$$x_0^2 = \frac{9b^2}{4a^2} = \frac{-a}{3} soit \left(4a^3 + 27b^2\right) = 0$$

Alors $\Delta = -16\left(4a^3 + 27b^2\right) = 0$

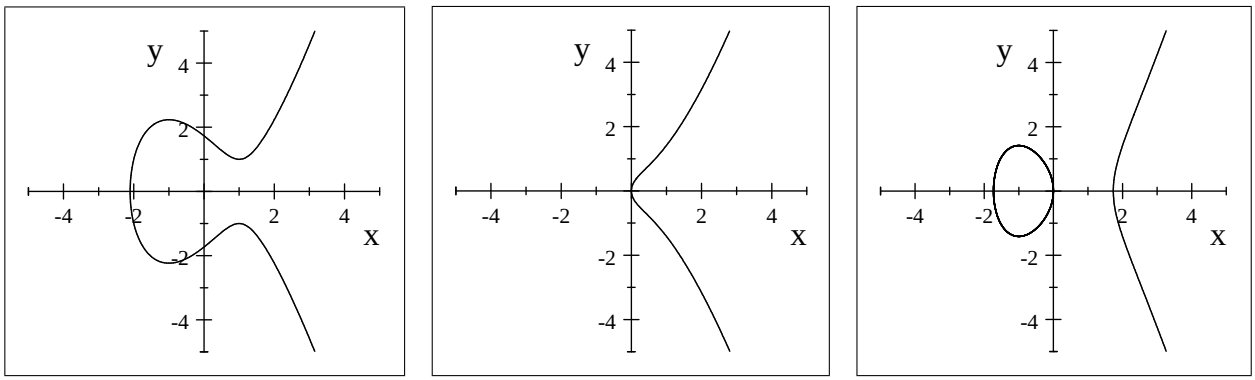
Finalement E est non singulière si et seulement si $\Delta \neq 0$ ■

Corollaire 1.8.2 *La cubique E est une courbe elliptique si et seulement si on a $\Delta \neq 0$*

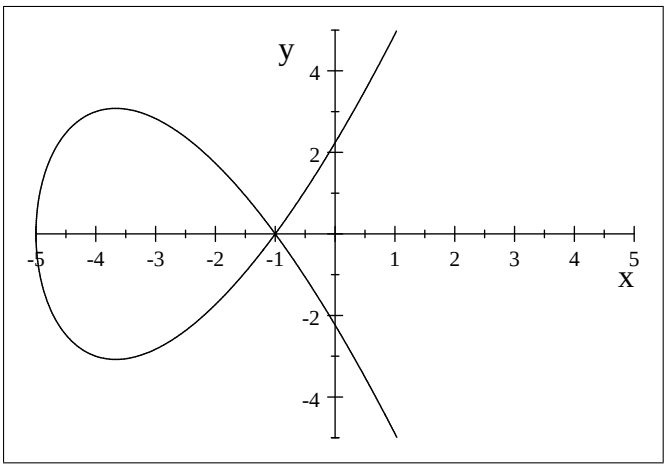
Exemple 1.8.1 *Les équations suivantes sont des courbes elliptiques*

$y^2 = x^3 - 3x + 3$ $\quad$ $\Delta = -2160$ $\quad$ $y^2 = x^3 + x$ $\quad$ $\Delta = -64$ $\quad$ $y^2 = x^3 - 3x$ $\quad$ $\Delta = 64$

:



Exemple 1.8.2 *Soit $E(\mathbb{R})$ définie par $E : y^2 = (x+1)^2(x+5)$. Ceci n'est pas une courbe elliptique car $\Delta = 0$*


y
4
2
-5
-4
-3
-2
-1
1
2
3
4
5
x
-2
-4

Chapitre 2

Cohomologie des groupes

Nous ne pouvons pas tirer une idée générale de l'objet de notre recherche et de l'objectif de" Groupe du Tate-Shafarevitch" sans recourir à la définition de "La cohomologie des groupes" où nous avons adopté dans ce chapitre, des définitions et des théories relatives à ce dernier, comme le corps des "nombres p-adiques" et la "réduction du Courbes elliptiques".

Pour définir le groupe de Tate-Shafarevitch, mais aussi pour démontrer la première partie du Théorème de Mordell, nous avons besoin d'étudier la cohomologie des groupes.

2.1 Cohomologie des groupes finis

Soit G un groupe fini. Un G-module est un groupe abélien M tel que G opère sur M : c'est-à-dire qu'il existe une application:

$$G \times M \to M$$

vérifiant :

$$(\sigma, m) \to \sigma m$$

1. $\sigma(m + m') = \sigma(m) + \sigma(m')$ pour tout $\sigma \in G$ et $m, m' \in M$
2. $(\sigma\tau)\, m = \sigma(\tau m)$ pour tout $\sigma, \tau \in G$ et $m \in M$
3. $1m = m$ pour tout $m \in M$

Soit un G-module. Nous définissons:

$$H^{\circ}(G,M) = M^{G} = \{m \in M \mid \sigma m = m, \forall \sigma \in G\}$$

Exemple 2.1.1 *Soit L une extension galoisienne de dégrée fini sur un corps K, G son groupe de Galois (le groupe de Galois d'une extension de corps L sur un corps K est le groupe des automorphismes de corps de L laissant K invariant.).*

Soit E une courbe elliptique sur K. L, L^{x} et $E(L)$ sont alors des G-modules; on a:

$$H^{\circ}(G,L) = K;\ H^{\circ}(G,L^{x}) = K^{x};\ H^{\circ}(G,E(L)) = E(K)$$

Un homomorphisme croisé est une application telle que:

$$f : G \to M\ tq\ f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$$

On vérifie immédiatement que:

$$f(1) = f(1,1) = f(1) + f(1)$$

et donc que

$$f(1) = 0$$

Si M est un G-module et si, on obtient un homomorphisme croisé en posant:

$$f(\sigma) = \sigma m - m$$

pour tout $\sigma \in G$

Un homomorphisme croisé défini de cette façon est dit principal.

La somme de deux homomorphisme croisés est un homomorphisme croisé et la somme de deux homomorphismes croisés principaux est aussi un homomorphisme croisé principal. On peut alors définir le quotient.

Nous définissons:

Si G opère trivialement sur M, i.e: $\sigma m = m$ pour tout $\sigma \in G$ et tout $m \in M$ alors un homomorphisme croisé est simplement un homomorphisme et tout homomorphisme croisé principal est réduit à 0. On a ainsi:

$$H^{1}(G;M) = Hom(G;M)$$

Proposition 2.1.1 *Soit L une extension galoisienne finie de K de groupe de Galois. Alors:*

$$H^1(G; L^x) = 0 \text{ (théorème 90 de Hilbert)}$$

Preuve. Soit $f : G \to L^x$ un homomorphisme croisé.

Il faut trouver $\gamma \in L^x$ tel que$f(\sigma) = \frac{\sigma(\gamma)}{\gamma}$pour tout $\sigma \in G$.

les $f(\tau)$ sont non nuls car ils appartiennent à L^xet donc d'après le théorème de Dedekind d'indépendance linéaire des homomorphismes $[cf.\,[7]\,.p47] \sum_{\tau \in G} f(\tau)\,\tau \neq 0$

Donc il existe $\alpha \in L$ tel que $\beta = \sum_{\tau \in G} f(\tau)\,\tau(\alpha)$

or

$\sigma(\beta) = \sum_{\tau} \sigma(f(\tau))(\sigma\tau)(\alpha)$

$= \sum (f(\sigma))^{-1} f(\sigma\tau)(\sigma\tau)(\alpha)$

$= (f(\sigma))^{-1} \sum f(\tau)\,\tau(\alpha)$

$= (f(\alpha))^{-1}\beta$

D'où

$f(\sigma) = \frac{\beta}{\sigma(\beta)} = \frac{\sigma\left(\beta^{-1}\right)}{\beta^{-1}}$. ■

Proposition 2.1.2 *Pour toute suite exacte de G-modules*

$$0 \to M \xrightarrow{i} N \xrightarrow{j} P \to 0$$

on a la suite exacte canonique

$$0 \to H^0(G, M) \to H^0(G, N) \xrightarrow{j} H^0(G, P) \xrightarrow{\partial} H^1(G, M) \to H^1(G, N) \to H^1(G, P)$$

.

Il faut définir ∂.

Comme j est un homomorphisme de G-modules,

$$j \circ \sigma = \sigma \circ j$$

Soit

$$p \in P^g = H^0(G, P)$$

Alors $p = j(n)$ et $\sigma p = p$, pour tout $\sigma \in G$,

soit; d'où:

$$\sigma(n) - n \in \ker j = \operatorname{Im} i \text{ i.e } t\sigma(n) - n = i(m) \in M$$

Montrons que l'application

$$f : G \to M$$

est un homomorphisme croisé. En effet:

$$\sigma \circ \tau(n) - n = \sigma(\tau n - n) + \sigma(n) - n$$

On vérifie ensuite que si $p = j(n')$ définit l'homomorphisme croisé f, alors $f - f'$ est un homomorphisme croisé principal puisque

$$(f - f')(\sigma) = \sigma(n - n') - (n - n') = \sigma(i(m))$$

car

$$n - n' \in \ker j = \operatorname{Im} i$$

L'homomorphisme ∂ est ainsi bien défini. Le reste à démontrer est évident.

Si H est un sous groupe de G, on définit l'homomorphisme de restriction

$$\operatorname{Re} s : H^1(G, M) \to H^1(H, M)$$

qui fait correspondre à $f : G \to M$ sa restriction

$$f|_H : H \to H$$

Définition de Suite exacte: Dans le contexte de la théorie des groupes, soient $(G_i)_{i\in\mathbb{N}}$des groupes et $f_i : G_i \to G_{i+1}$ des morphismes de groupes. On dit que la suite:

$$G_0 \overset{f_0}{\to} G_1 \overset{f_1}{\to} ... \overset{f_{i-1}}{\to} G_i \overset{f_i}{\to} G_{i+1} \overset{f_{i+1}}{\to} ...$$

est exacte si pour tout entier naturel i on a $\operatorname{Im}(f_i) = Ker(f_{i+1})$.

Proposition 2.1.3 *Si G est d'ordre m, alors*

$$mH^1(G, M) = 0$$

La preuve utilise le résultat admit suivant: [4]

Si H est un sous groupe d'indice m de G, alors il existe un homomorphisme de corestriction cor:

$$H^i(H,M) \to H^i(G,M)$$

Tel que. cor $\mathrm{Re}\, s = m$

On prend ici $H = \{1\}$ et l'on utilise le fait que

$$H^1(\{1\},M) = 0$$

Si H est un sous groupe distingué de G est M un G-module, alors M^H est un G/H-module et tout homomorphisme croisé de G/H dans M^H se relève en un homomorphisme croisé de G dans M.

$$\begin{array}{ccc} G & \underset{\bar{f}}{\to} & M \\ P \downarrow & & \cup \\ G/H & \underset{f}{\to} & M^H \end{array}$$

On obtient ainsi l'homomorphisme d'inflation:

$$Inf : H^1\left(G/H,M^H\right) \to H^1(G,M)$$

la suite d'homomorphisme est exacte:

$$0 \to H^1\left(G/H,M^H\right) \overset{Inf}{\to} H^1(G,M) \overset{\mathrm{Re}\, s}{\to} H^1(H,M)$$

2.2 Nombre p-adique

En mathématiques, et plus particulièrement en théorie des nombre, si p est un nombre premier, un nombre p-adique est un objet qui peut se concevoir comme une suite de chiffres en base p, eventuellement infinie à gauche de la virgule (mais toujours finie à droite de la virgule) .

Avec une addition et une multiplication qui se calculent comme pour les nombres décimaux usuels, l'ensemble des nombres 2- adique forme un corps commutatif noté $\mathbb{Q}_2$, un nombre 2- adique est parfois appelé "diadique" mais ne doit pas être confondu avec une

fraction diadique, un nombre 3-adique est parfois appelé "triadique" chaque corps $\mathbb{Q}_p$ des nombres p-adiques est construit par complétion du corps $\mathbb{Q}$ des nombres rationnels lorsque celui-ci est muni d'une valeur absolue nommée valeur absolue p-adique.

Cette construction s'apparente à celle du corps $\mathbb{R}$ des nombres réels par complétion du corps des rationnels suivant la valeur absolue usuelle.

La principale motivation ayant donné naissance aux corps des nombres p-adique était de pouvoire utiliser les techniques des séries entières dans la théorie des nombres, mais leur utilité dépasse maintenant largement ce cadre.

De plus, la valeur absolue p-adique sur le corps $\mathbb{Q}_p$ est une valeur absolue non-archimédienne on obtient sur ce corps une analyse différente de l'analyse usuelle sur les réels, que l'on appelle analyse p-adique.

Courbes elliptique sur un corps.

Exemple 2.2.1

35 en tant que nombre 2-adique serait la suite $(1, 3, 3, 3, 3, 35, 35, 35, ...)$ explication:

$35 = 1 + (1.2^1) + (0.2^2) + (0.2^3) + (0.2^4) + (1.2^5) + (0.2^6) + ...$

La suite (a_n) s'obtient en faisant les sommes cumulées des x; 2^i(où $x_i \in \{0; 1\}$)

$a_1 = 1$

$a_2 = 1 + 2 = 3$

$a_3 = 1 + 2 + 0 = 3$

$a_4 = 1 + 2 + 0 + 0 = 3$

$a_5 = 1 + 2 + 0 + 0 + 0 = 3$

$a_6 = 1 + 2 + 0 + 0 + 0 + 2^5 = 35$, etc

On a bien pour tout $n \geq 1$:

$0 \leq a_n \leq 2^n$ et $a_n \equiv a_{n+1}$

$(\mathrm{mod}\, 2^n)$ puisque $a_{n+1} = a_n + x_{n+1}2^{n+1}$

2.3 Réduction de courbes elliptiques

La réduction d'une courbe elliptique peut être utilisée pour la détermination d'un sous groupe de m-torsion.

Cette réduction s'obtient avec une valuation du corps K de la courbe elliptique.

La théorie des valuations se trouve dans les ouvrages de Théorie des Nombres comme:

"Algebraic Numbers and Algebraic Functions" par Artin

"Algebraic Numbers" par Lang

"Algebraic Number Theory" par Weiss

"Number Theory" par Hasse

Définition 2.3.1 *Une valuation sur un corps K est une fonction à valeurs réelles positives $v : K \to \mathbb{R}^+$ qui satisfait les axiomes:*

(Val1) si $v(x) \geq 0, v(x) = 0$ est seulement si $x = 0$

(Val2) $v(xy) = v(x)v(x)$ pour tous éléments x et y du corps K.

(Val3) $v(x + y) \leq c \max \{v(x), v(y)\}$ pour $c = 1$ ou $c = 2$.

La valuation v est triviale lorsqu'elle prend les valeurs:

$v(0) = 0$ et $v(x) = 1$ pour $x \neq 0$.

Les valuations sont classifiées selon la valeur de la constante c:

Pour, la valuation est non archimédienne.

Pour, la valuation est archimédienne.

Sur un corps K de caractéristique, toutes les valuations non triviales sont non archimédiennes.

2.3.1 Valuation exponentielle

Soit une valuation v. Par l'axiome $v(xy) = v(x)\, v(y)$, elle est multiplicative. Cette valuation implique la fonction $\varphi : K \to \mathbb{R} \cup \infty$ de valeur $\varphi(x) = -\log v(x)$, c'est la valuation exponentielle; elle satisfait les 3 axiomes $\varphi(x) = \infty$ si est seulement si $x = 0$

$$\varphi(xy) = \varphi(x) + \varphi(y)$$

et

$$\varphi(x+y) \geq \min\{\varphi(x), \varphi(y)\}$$

Cette valuation φ est additive.

Exemple 2.3.1 ***de valuation non archimédienne:*** $c = 2$

Valuation p-adique v_p du corps, p premier:
Elle prend les valeurs $v_p(1) = 1, v_p(p) = \frac{1}{p}$ et $v_p(q) = 1$ pour tout nombre premier $q \neq p$.
Soit un nombre rationnel $x = a.p^r$, avec a premier à p. Alors $v_p(x) = \frac{1}{p^r}$.
Cette valuation satisfait les axiomes des valuations non archimédiennes.

Exemple 2.3.2 ***de valuation archimédiènne:*** $c = 0$

La valeur absolue sur Q:
Ainsi $|+3| = |-3| = 3$; $|101.8| = 101.8$
Cette notion de valuation est utilisée pour réduire les courbes elliptiques.

Définition 2.3.2 *Soit une courbe elliptique E, son corps de base K et une valuation v de K.*

La réduction modulo v est l'application:

$$k \to \widetilde{k}$$

$$a \to \widetilde{a} = v(a)$$

Elle s'applique aux points $P = (x_p, y_p)$ du groupe $E(K)$ par l'application:

$$E(K) \to \widetilde{E}\left(\widetilde{K}\right)$$
$$P(x,y) \to \widetilde{P}(v(x), v(y))$$

La réduction d'un point P est le point réduit $\tilde{P}$; la réduction de la courbe elliptique $E(K)$ est la courbe réduite $\tilde{E}\left(\tilde{K}\right)$. Cette réduction modulo v détermine deux sous ensembles du groupe $E(K)$:

$$E_0(K) = \left\{ P \in E(K) ; \tilde{P} \text{ non singulier} \right\}$$

$$E_1(K) = \left\{ P \in E(K) ; \tilde{P} = 0_E \right\}$$

Exemple 2.3.3 ***de réduction***

Soit la courbe elliptique E d'équation de Weierstrass:

$$E : y^2 - 10x + 6y = x^3 + 12x^2 - 14x + 11 \in \mathbb{Q}[x, y]$$

Appliquons la valuation p-adique, pour:

$$\tilde{E} : y^2 + 2xy = x^3 + x + 2 \in F_3[x, y]$$

Nous obtenons l'équation de la courbe réduite.

Il y a plusieurs types de réductions suivant la valeur du discriminant de la courbe réduite.

Selon Silverman les réductions sont classées par la:

Définition 2.3.3 *Soit une courbe elliptique E et sa courbe réduite $\tilde{E}$ modulo une valuation v du corps K*

1. E a une bonne réduction sur K si la courbe réduite $\tilde{E}$ est elliptique.
2. E a une réduction multiplicative si $\tilde{E}$ a un nœud.
3. E a une réduction additive si $\tilde{E}$ a un point de rebroussement. Dans les 2 cas où $\Delta\left(\tilde{E}\right) = 0$ la réduction est mauvaise.
4. La réduction est stable si elle est bonne,

La réduction est semi stable si elle est multiplicative,

La réduction est instable si elle est additive.

Lorsque la valuation v est non archimédienne et discrète, nous considérons les 4 ensembles: l'anneau des v-entiers $A_v = \{x \in K, v(x) \geq 0\}$, l'idéal v-premier $M_v = \{x \in K, v(x) > 0\}$, le groupe des v-unités $U_v = \{x \in K, v(x) = 0\}$ et le corps résiduel A_v/M_v

Les réductions sont classifiées par la:

Proposition 2.3.1 *Soit une courbe elliptique E, une valuation v sur le corps K, les invariants $\Delta(E)$ et $c_4(E)$de la courbe elliptique.*

1. E a une bonne réduction en v si et seulement si $v(\Delta(E)) = 0$; alors $\Delta(E)$est une unité de $\tilde{K}$.

2. E a une réduction multiplicative si et seulement si $v(\Delta(E)) > 0$ et $v(c_4) = 0$. Dans ce cas la partie $\tilde{E}_{ns}$ non singulière de la courbe réduite $\tilde{E}$ est isomorphe au groupe multiplicatif
$$\tilde{E}_{ns}\left(\tilde{K}\right) \simeq \tilde{K}^*$$

3. E a une réduction additive en v si est seulement si $v(\Delta(E)) > 0$ et $v(c_4) > 0$. Dans ce cas la partie non singulière $\tilde{E}_{ns}$ de la courbe réduite $\tilde{E}$ est isomorphe au groupe additive
$$\tilde{E}_n\left(\tilde{K}\right) \simeq \tilde{K}^+$$

Cette réduction possède plusieurs propriétés intéressantes.

Proposition 2.3.2 *Soit une valuation non archimédienne discrète v et un entier m de valuation $v(m) = 0$. Soit une courbe elliptique E qui a bonne réduction en v. Alors l'application réduction:*
$$E(K)[m] \to \tilde{E}\left(\tilde{K}\right)$$
est injective.

Le groupe de Galois d'une clôture algébrique de K et un sous groupe de m-torsion sont liés par l'application bilinéaire de Kummer:

Définition 2.3.4 *L'application bilinéaire de Kummer est l'application:*

$$\lambda : E(K) \times G(K_{a\lg}/K) \to E(K)[m]$$

de valeur $\lambda(P, \sigma) = \sigma(R) - R$ avec $P = mR$.

1. L'application de Kummer est bilinéaire;

2. Son noyau à gauche est le sous groupe $mE(K)$;

3. Son noyau à droite est le groupe de Galois:

$$G(K_{a\lg}/L) \text{ où } L = K\left(m^{-1}E(K)\right) = \text{composé de tous les corps } K(R) \text{ lorsque } mR \in E(K).$$

4. L est une extension abélienne d'exposant m:

tout élément de L est d'ordre divisant m.

Preuve. Proposition 1-2 et 1-5 du chapitre VIII « Silverman ». ■

Illustrons cette théorie par quelques exemples:

Exemple 2.3.4 *Courbe elliptique d'équation de Weierstrass:*

$$E_1 : y^2 = x^3 + 3x^2 + 22x - 24$$

Calculs des invariants:

$$\Delta(E_1) = 1000000 = 2^6 \times 5^6$$

$$c_4(E_1) = 1200 = 2^4 \times 3 \times 5^2$$

Réduction de la courbe E_1 modulo la valuation v_5:

$$v_5(\Delta(E_1)) = 6 > 0$$

$$v_5(c_4(E_1)) = 2 > 0$$

D'après la proposition 6, il en résulte que la courbe elliptique E_1 a une réduction additive modulo la valuation v_5.

Exemple 2.3.5 *Courbe elliptique d'équation de Weierstrass:*

$$E_2 : y^2 = x^3 + 6x^2 - x - 6$$

Calculs des invariants:

$$\Delta(E_2) = 78400 = 2^4 \times 5^2 \times 7^2$$

$$c_4(E_2) = 624 = 2^4 \times 3 \times 13$$

Réduction de la courbe E_2 modulo la valuation v_5

$$v_5(\Delta(E_2)) = 2 > 0$$

$$v_5(c_4(E_2)) = 0$$

On en déduit que la courbe E_2 a une réduction multiplicative modulo la valuation v_5.
Réduction de la courbe E_2 modulo la valuation v_{13}:

$$v_{13}(\Delta(E_2)) = 0$$

On en déduit que la courbe E_2 a une bonne réduction modulo la valuation v_{13}.

Chapitre 3

Groupe de Tate-Shafarevitch

La conclusion de notre recherche sera sous le titre "Groupe de Tate-Shafarevitch" et que nous avons ouvert à travers les chapitres 1 et 2, qui est considéré comme une question principale tournait autour de notre étude, qui a été partiellement renforcé représenté dans la clé "Finitude de groupe de Selmer" attaché avec une preuve de sa propre, ajouter les lemmes connexes.

Pour définir ce groupe on admettra le lemme suivant:

Lemme 3.0.1 *Soit K un corps algébriquement clos et E une courbe elliptique sur K. Alors la multiplication par n dans $E(K)$ est surjective.*

D'après le lemma on a la suite exacte

$$0 \to E_n\left(\bar{\mathbb{Q}}\right) \to E\left(\bar{\mathbb{Q}}\right) \xrightarrow{n} E\left(\bar{\mathbb{Q}}\right) \to E\left(\bar{\mathbb{Q}}\right) \to 0$$

où $E_n\left(\bar{\mathbb{Q}}\right)$ désigne le groupe de points de n-torsion.
On en déduit grâce à la proposition ( ) la suite de cohomologie:

$$0 \to E_n(\mathbb{Q}) \to E(\mathbb{Q}) \to E(\mathbb{Q}) \to H^1(\mathbb{Q}, E_n) \to H^1(\mathbb{Q}, E) \xrightarrow{n} H^1(\mathbb{Q}, E)$$

Et par suite, la suite exacte:

$$0 \to E(\mathbb{Q}) \diagup nE(\mathbb{Q}) \to H^1(\mathbb{Q}, E_n) \to h^1(\mathbb{Q}, E)_n \to 0$$

où

$$H^1(\mathbb{Q}, E)_n = \ker\left(H^1(\mathbb{Q}, E) \xrightarrow{n} H^1(\mathbb{Q}, E)\right)$$

Remarque 3.0.1 *Si $H^1(\mathbb{Q}, E)$ était fini, on obtiendrait la finitude de $E(\mathbb{Q})/nE(\mathbb{Q})$ mais cela et faux.*

En considérant la courbe elliptique sur $\mathbb{Q}_p$, on obtient alors le diagramme

$$\begin{array}{ccccccccc} 0 & \to & E(\mathbb{Q})/nE(\mathbb{Q}) & \to & H^1(\mathbb{Q}, E_n) & \to & H^1(\mathbb{Q}, E)_n & \to 0 \\ & & \downarrow & & \downarrow & & \downarrow & \\ 0 & \to & E(\mathbb{Q}_p)/nE(\mathbb{Q}_p) & \to & H^1(\mathbb{Q}_P, E_n) & \to & H^1(\mathbb{Q}_P, E) & \to 0 \end{array}$$

L'idée est de remplacer $H^1(\mathbb{Q}, E_n)$ par un sous groupe moins gros contenant l'image de $E(\mathbb{Q})/nE(\mathbb{Q})$, pour lequel on sache prouver la finitude.

On remarque que si $\gamma \in H^1(\mathbb{Q}, E_n)$ provient d'un élément de $E(\mathbb{Q})$, alors pour tout p, son image $\gamma_p \in H^1(\mathbb{Q}_p, E_n)$ sera l'image d'un élément de $E(\mathbb{Q}_p)$.

Définition 3.0.5 *On définit le groupe de Selmer $S^n(E/\mathbb{Q})$ par:*

$$\begin{aligned} S^n(E/\mathbb{Q}) &= \left\{\gamma \in H^1(\mathbb{Q}, E_n)/\gamma \text{ provienne de } E(\mathbb{Q}_p)\right\} \\ &= \ker\left(H^1(\mathbb{Q}, E_n) \to \prod_p H^1(\mathbb{Q}_p, E_n)\right) \end{aligned}$$

De même, en définit le groupe de Tate-Shafarevitch $TS(E/\mathbb{Q})$ par:

$$TS(E/\mathbb{Q}) = \ker\left(H^1(\mathbb{Q}, E) \to \prod_p H^1(\mathbb{Q}_p, E)\right)$$

Lemme 3.0.2 *Pour montrer le lien entre ces deux groupes, on utilise le lemme suivant. Pour tout couple d'homomorphismes de groupes abéliens*

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

On a la suite exacte:

$$0 \to \ker\alpha \to (\beta \circ \alpha) \xrightarrow{\alpha} \ker(\beta) \to co\ker(\alpha) \to co\ker(\beta \circ \alpha) \to co\ker(\beta) \to 0$$

où $co\ker(\alpha) = B/\operatorname{Im}(\alpha)$

Appliquant ce lemme a la suite d'homomorphismes

$$H^1(\mathbb{Q}, E_n) \xrightarrow{\alpha} H^1(\mathbb{Q}, E)_n \xrightarrow{\beta} \prod_p H^1(\mathbb{Q}_p, E)_n$$

On obtient la suite exacte fondamentale

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to S^{(n)}(E/\mathbb{Q}) \to TS(E/\mathbb{Q})_n \to 0$$

Par suite

$$S^{(n)}(E/\mathbb{Q})\ fini \Longrightarrow E(\mathbb{Q})/nE(\mathbb{Q})\ fini$$

3.1 Finitude de groupe de Selmer

Lemme 3.1.1 *Soit E une courbe elliptique sur $\mathbb{Q}_p$ ayant bonne réduction et n un entier naturel non divisible par p. Soit $P \in E(\mathbb{Q}_p)$, alors:*

$$P = nQ \qquad P \text{ et } Q \in E(\mathbb{Q}_p) \Longleftrightarrow \bar{P} = n\bar{Q} \qquad \bar{P} \text{ et } \bar{Q} \in E(F_p)$$

Preuve. ($\Longrightarrow$) est immédiate.

($\Longleftarrow$) on utilise la filtration p-adique défini en cohomologie (Appendice B)

$$E(\mathbb{Q}_p) \supset E^1(\mathbb{Q}_p) \supset ... \supset E^n(\mathbb{Q}_p) \supset E^{n+1}(\mathbb{Q}_p) \supset ...$$

D'où on déduit

$$E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p) \simeq E(F_p) \qquad E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p) \simeq E(F_p)$$

L'hypothèse entraîne alors l'existence de $Q_0 \in E(\mathbb{Q}_p)$, tel que

$$P - nQ_0 \in E^1(\mathbb{Q}_p)$$

Mais $E^1(\mathbb{Q}_p)/E^2(\mathbb{Q}_p) \simeq E(F_p)$ et p ne divise pas n donc la multiplication par n est un isomorphisme dans $E^1(\mathbb{Q}_p)/E^2(\mathbb{Q}_p)$. D'où l'existence de $\mathbb{Q}_1 \in E^1(\mathbb{Q}_p)$ tel que

$$P - nQ_0 - nQ_1 \in E^2(\mathbb{Q}_p)$$

Suivant la procédure, on définit une suite $Q_0, Q_1, ... \in E(\mathbb{Q}_p)$ avec $Q_i \in E^i(\mathbb{Q}_p)$

Comme

$$\underset{n\geq 1}{\cap} E^n(\mathbb{Q}_p) = \{0\}$$

on déduit que $\lim_{n\to\infty} Q_i = 0$, ce qui entraîne la convergence de la série $\sum_i Q_I$, pour la topologie ultramétrique vers un point Q de $E(\mathbb{Q}_p)$ puisque $E(\mathbb{Q}_p)$ est compact. Finalement, comme

$$P - \sum_{i=0}^{m} Q_i \in E^{m+1}(\mathbb{Q}_p)$$

il vient

$$P = nQ$$

. ■

.

Lemme 3.1.2 *Pour tout extension finie k de F_p il existe une extension K de $\mathbb{Q}_p$ vérifiant:*
(1) $[K : \mathbb{Q}_p] = [K : F_p]$
(2) *la clôture intégrale de R de $\mathbb{Z}_p$ dans K est un anneau intégre principal ayant un unique idéal premier (p)(ou encore un unique élément premier à éléments associés prés) tel que*

$$R/_P R = k$$

Le corps K est l'extension non ramifiée de $\mathbb{Q}_p$ de corps résiduel k.

Conclusion 3.1.1 *Tout élément α de K s'écrie de façon unique $\alpha = up^m, u \in R^x$ inversible . par suite l'homomrphisme de valuation:*

$$\nu_p : \mathbb{Q}^x \to \mathbb{Z}$$

S'étend en un homomorphisme de valuation de $K^x \to \mathbb{Z}$.

La filtration de $E(\mathbb{Q}_P)$ s'étend alors en une filtartion de $E(K)$ et l'on a:

$$E(K)/E^1(K) \simeq \bar{E}(k). \qquad E^n(K)/E^{n+1}(K) \simeq k$$

Par suite le lemme 4 est valable pour K ou lieu de $\mathbb{Q}_p$.

Lemme 3.1.3 *Soit E une courbe elliptique ayant bonne réduction en P et n un entier naturel non divisible par P. Soit $P \in E(\mathbb{Q}_p)$. Alors il existe une extension non ramifiée de $\mathbb{Q}_p$ telle que $P \in nE(K)$.*

Preuve. On a $\bar{P} = n\bar{Q}$ dans où K est une extension finie de F_p; d'oú $P = nQ$ dans $E(K)$ extension non ramifiée de $\mathbb{Q}_p$ d'aprés le lemme précédant. ■

Proposition 3.1.1 *Soit E une courbe elliptique sur $\mathbb{Q}$ est T l'ensemble des nombres premiers divisant $2n\Delta$ où Δ est le discriminant de E. Pour tout $\gamma \in S^{(n)}$ et tout $P \notin T$, il existe une extension finie non ramifiée K de $\mathbb{Q}_p$ telle que γ s'envoie sur 0 dans $H^1(K, E_n)$.*

Preuve. Par la définition du groupe de Selmer, on sais qu'il existe $P \in E(\mathbb{Q}_p)$ envoyer a $\gamma_p \in H^1(\mathbb{Q}_P, E_n)$. Puisque p ne divise pas $2n\Delta$, E est de bonne réduction en p, et donc il y a une extension non ramifiée K de $\mathbb{Q}_p$ telle que $P \in nE(K)$.

Le diagramme suivant montre que γ s'envoie au 0 dans $H^1(\mathbb{Q}_P, E_n)$:

$$\begin{array}{ccccc} E(\mathbb{Q}) & \xrightarrow{n} & E(\mathbb{Q}) & \rightarrow & H^1(\mathbb{Q}, E_n) \\ \downarrow & & \downarrow & & \downarrow \\ E(\mathbb{Q}_p) & \xrightarrow{n} & E(\mathbb{Q}_P) & \rightarrow & H^1(\mathbb{Q}_P, E_n) \\ \downarrow & & \downarrow & & \downarrow \\ E(K) & \xrightarrow{n} & E(k) & \rightarrow & H^1(K, E_n) \end{array}$$

■

3.2 Preuve de la finitude du groupe de Selmer

Nous montrons que $S^{(2)}(E/\mathbb{Q})$ est fini dans le cas où les points d'ordre 2 dans E sont rationnels.

C'est-à-dire E est de la forme:

$$E : Y^2Z = (X - \alpha Z)(X - \beta Z)(X - \gamma Z), \alpha, \beta, \gamma \in \mathbb{Q}$$

Cela implique que:

$$E_2\left(\mathbb{Q}^{a1}\right) = E_2(\mathbb{Q}) \approx (\mathbb{Z}/2\mathbb{Z})^2 = (\mu_2)^2$$

Le groupe de Galois $Gal\left(\bar{\mathbb{Q}}/\mathbb{Q}\right)$ agis trivialement sur $E_2\left(\mathbb{Q}\right)$; d'où

$$H^1\ \left(\mathbb{Q}, E_2\right)\ \approx H^1\left(\mathbb{Q}, \mu_2\right) \approx \left(\mathbb{Q}^x/\mathbb{Q}^x\right)^2$$

3.3 perspectives

Etudier d'avantage le groupe de Tate Shafarevich fera un bon sujet de master, nous souhaitons calculer le cardinal de ce dérnier pour une courbe ou une famille donnée on calculant les composantes connexes.

Bibliographie

[1] **Abderrahman Nitaj,** Introduction aux courbes elliptiques, Rabat, 29 oct 2008, Université de Caen, France.

[2] **Daniel perrin,** Géométrie algébrique. Une introducton. CNRS EDITIONS.

[3] **Husemoller Dale**, Elliptic curves, Second Edition (Springer, GTM 111).

[4] **J.Silverman,** Arithmetic of elliptic curves, 106 GTM, springer verlage .

[5] **J.S.Milne**, Math 679, University of Michigan

[6] **Marc Joye,** Introduction élémentaire à la théorie des courbes elliptiques.

[7] **Pierre Samuel**, Théorie Algébrique des nombres. Hermann, 1967 - 131 pages.

[8] **Van Der Waerden,** Algebra Volume 1 et 2, seventh edition, Springer-Verlag Berlin, 1966.