N° d'ordre:13/2003-M/MT

Université des Sciences et de la Technologie

HOUARI Boumedienne

USTHB Alger

Faculté de Mathématiques

Thèse

présentée pour l'obtention du grade de :

Magister en Mathématiques

Spécialité : **Algèbre et Théorie des Nombres**

par

M^elle MOKHTARI Dejia

sujet

COURBES ELLIPTIQUES SUR LES CORPS DE NOMBRES ABELIENS DE DEGRE 5

Soutenue publiquement le 02/07/2003 devant le Jury composé de :

Mr M.HACHAICHI : Maître de Conférence à l'USTHB……..Président
Mr M.ZITOUNI : Professeur à l'USTHB……..Directeur de Thèse
Mr K.BETINA : Professeur à l'USTHB…….. Examinateur
Mr A. KESSI : Professeur à l'USTHB…… ……. Examinateur
Mr B.BENSBAA : Chargé de Cours à l'USTHB…… ……Examinateur
Mr R.BOUCHENNA : Chargé de Cours à l'USTHB…… .Examinateur

REMERCIMENTS

Je tiens à remercier :

Monsieur M .HECHAICHI, Maître de conférence à l'USTHB de l'honneur qu'il ma fait , de bien vouloir présider le jury de cette Thèse.

Messieurs :

K . BETINA , Professeur à l'USTHB

A. KESSI , Professeur à l'USTHB

B.BENSBAA , Chargé de cours à l'USTHB

R..BOUCHENNA , Chargé de cours à l'USTHB

de bien vouloir être membres du Jury

J'adresse ma gratitude et ma profonde reconnaissance à Monsieur M.ZITOUNI , Professeur à l'USTHB , qui a accepté de rapporter ma thèse et m'avoir suivi tout au long de ce travail.

S O M M A I R E

I N T R O D U C T I O N

La théorie des courbes elliptiques comporte des aspects géométriques, algébriques, analytiques et arithmétiques .

Lorsque les courbes elliptiques sont définies sur des corps de nombres de degré fini ,alors la théorie des nombres intervient par les entiers algébriques, les discriminants, les classes d'idéaux , la ramification , les valuations , l' analyse p-adique, les nombres premiers, les équations diophantiennes , les fonctions arithmétiques (Euler , Mobïus , Zêta…)de ces corps .

La place des courbes elliptiques dans le domaine des mathématiques pures a été indiquée par deux mathématiciens au moins .

« La théorie des courbes elliptiques (courbes de genre un) est riche et variée et elle fournit un bon exemple de liens entre la géométrie algébrique abstraite, l'analyse complexe et la théorie des nombres » , R. Harsthorne , « algebraic geometry ».

« La théorie des courbes elliptiques et des formes modulaires est un domaine dans lequel interviennent diverses branches des mathématiques : analyse complexe , géométrie algébrique, théorie des représentations , théorie des nombres » , N.Koblitz « Introduction to elliptic curves and modular forms » .

On commence par un premier chapitre contenant l'étude arithmétique des corps cycliques de degré 5 : Corps cyclotomiques, résolvantes de Lagrange , bases d'entiers , discriminants , corps unitaire et corps p primaires .

Le chapitre II est consacré à l'étude des courbes elliptiques : structures algébrique , transformation d'équations , loi de groupe abélien, isomorphismes ,

isogenies , automorphismes , réduction par une valuation non archimédienne discrète d'un corps de nombres .

Le chapitre III est réservé à l'étude des points d'ordre fini et au groupe de torsion du groupe de Mordell-Weil d'une courbe elliptique définie sur un corps de nombres en traitant des exemples de courbes elliptiques définies sur un corps de nombres cycliques de degré 5.

CHAPITRE I

CORPS DE NOMBRES CYCLIQUES DE DEGRE 5

Introduction

Un corps de nombres abélien K de degré [K : Q] = n admet un groupe de Galois $G_{K/Q}$ abélien d'ordre n . D'après la théorie des groupes abéliens finis , un groupe d'ordre premier est cyclique . Donc les groupes abéliens d'ordre 5 et les corps de nombres abéliens de degré 5 sont cycliques .

Pour construire ces corps de nombres, nous utilisons la théorie du corps de classes global ; d'autres théories interviendront (fonction arithmétique φ d'Euler , corps cyclotomiques , polynômes cyclotomiques , décomposition des idéaux ,...).

1- *Corps de classes global , discriminants , conducteurs*

Nous utilisons des résultats qui se trouvent dans plusieurs ouvrages de théorie des nombres .

Théorème 1 :

Tout corps de nombres abélien K , de degré n , est le corps de classes sur le corps Q des nombres rationnels, relativement à un ray- groupe d'idéaux J, du corps Q, de conducteur f . Le groupe de Galois $G_{K/Q}$ est isomorphe au groupe I(f)/J , où I(f) désigne le groupe des idéaux du corps Q premiers au conducteur f .

v

Théorème 2 :

La correspondance de Weber – Takagi établit une bijection entre le corps de classes K et le ray groupe J de conducteur f basée sur la décomposition complète d'idéaux premiers :

$$J \subset Q \longleftrightarrow K/Q$$

{ idéal premier P} $\longleftrightarrow$ *{P complètement décomposé }*

ν

Tout idéal premier contenu dans le ray- groupe J est complètement décomposé dans le corps de classes K ; réciproquement, tout idéal premier du corps Q complètement décomposé dans K est dans J.

Théorème 3 :

Le discriminant $dis_{K/Q}$ *du corps de classes K et le conducteur f du ray - groupe J associé admettent les mêmes diviseurs premiers.*

Preuve :C'est le théorème du conducteur - discriminant, il est dû à H. Hasse, cf [5]Théorème 7.3 ν

Théorème 4 :

Tout corps de nombres abélien K est inclus dans un corps cyclotomique .

Preuve : Ce théorème est dû à Kronecker . cf[9] corollaire 3 page 210 ν

Cette inclusion d'un corps de nombres abélien dans un corps cyclotomique permet de définir la notion de conducteur d'un corps abélien .

Définition 1 :

Dans l'ensemble $\{ C_l = l^{ème}$ *corps cyclotomique }des corps cyclotomiques qui contiennent un corps abélien K , le plus petit indice* l *est le conducteur du corps abélien K .*

Pour un corps de nombres abélien K de degré 5, de conducteur f, le groupe de Galois $G_{K/Q}$ est cyclique d'ordre 5 , isomorphe au groupe quotient :

$$I(f) / J \approx (Z/fZ)^*/J.$$

L'ordre du groupe multiplicatif $(Z/fZ)^*$ est déterminé avec la fonction φ d' Euler :

$\varphi(p) = p - 1$ et $\varphi(p^r) = (p-1)\, p^{r-1}$ pour tout nombre premier p impair;

$\varphi(2^r) = 2^{r-1}$, $\varphi(2n) = \varphi(n)$ pour tout entier impair n ;

$\varphi(a\, b) = \varphi(a)\, \varphi(b)$ pour toute paire {a,b } d'entiers premiers entre eux.

Le théorème 1 et la fonction φ impliquent la congruence :

$$\varphi(f) \equiv 0 \mod 5 \qquad (1)$$

Cette congruence admet une infinité de solutions :

a) $f = p$, premier , $p \equiv 1 \mod 5$, les solutions sont :

$p = 11,31,41,61,71,101,131,151,181,191,211,241,\ldots$

b) $f = 5^r$ pour $r \geq 2$ soit $f = 5^2, 5^3, 5^4, \ldots$

c) $f = n\, p\, 5^r$ pour $n \geq 1$

Les 15 plus petites valeurs du conducteur f sont :

$f = 11,22,25,31,33,41,44,50,55,61,62,66,71,75,77 \qquad (2)$

Il s'en suit qu'un corps cyclique K de degré 5 est un sous corps du $f^{ème}$ corps cyclotomique pour les solutions f trouvées .

Donnons quelques notions de la théorie des corps cyclotomiques .

2-Corps Cyclotomiques

Les résultats qui suivent se trouvent dans plusieurs ouvrages spécialisés (Washington , Lang , Artin ,…)

2.1) Structures arithmétiques

Définition 1:

Le $n^{ème}$ corps cyclotomique est l'extension algébrique du corps des nombres rationnels Q par l'adjonction d'une racine primitive $n^{ème}$ de 1 :

$$Q(z) \text{ avec } z = \exp(2\pi i / n) \qquad (3)$$

Le nombre de ces racines primitives est égal à $\varphi(n)$

La structure du corps $Q(z)$ est déterminée par le :

Théorème 5:

1) Le $n^{ème}$ corps cyclotomique est une extension abélienne du corps Q de degré $\varphi(n)$ pour tout entier $n > 1$.

2) Pour tout entier impair n, le $n^{ème}$ et le $2n^{ème}$ corps cyclotomiques coïncident

3) Le $n^{ème}$ corps cyclotomique est cyclique , de groupe de Galois isomorphe au groupe multiplicatif $(Z/nZ)^*$ pour tout entier $n = p$, $n = p^r$, p premier impair et $n = 4$.

4) Pour tout entier $n = p_1^{r_1} \dots p_s^{r_s}$ produit de puissances de nombres premiers distincts impairs $p_i^{r_i}$, le $n^{ème}$ corps cyclotomique est abélien de groupe de Galois isomorphe au groupe $\prod_{1 \le i \le s} (Z/p_i^{r_i})^*$

5) Le $2^{r\text{-}ème}$ corps cyclotomique est abélien pour $r \geq 3$.

Preuve : cf [5] ν

L'étude des sous corps du $n^{ème}$ corps cyclotomique est réalisée avec la correspondance de Galois entre les sous corps du $n^{ème}$ corps cyclotomique et les sous groupes du groupe de Galois du corps .

Soit $Q(z) = K$ le $p^{ème}$ corps cyclotomique , p premier , $z = \exp(2\pi i / p)$. Son groupe de Galois G et le groupe multiplicatif $(Z/pZ)^*$ sont isomorphes .

A tout générateur σ de G correspond un générateur g de $(Z/pZ)^*$. Il en résulte l'isomorphisme de groupes :

$$G = \{\sigma, \sigma^2, \ldots, \sigma^{p-1} = Id\} \overset{\sim}{\longrightarrow} (Z/pZ)^* = \{g, g^2, \ldots, g^{p-1} = 1\} \quad (4)$$

$$\sigma \longrightarrow g$$

On en deduit les Q- automorphismes du corps K :

$$\sigma(z) = z^g \quad et \ \sigma(z^r) = \sigma^r(z) = z^{g^r}, \ g^r \bmod p \quad (5)$$

Pour obtenir un sous corps L de degré un diviseur d de p-1 , nous considérons un sous groupe H d'indice d du groupe G :

$$H = \{\sigma^d, \sigma^{2d}, \ldots, \sigma^{d'd} = Id \text{ , avec } dd' = p-1\} \quad (6)$$

Posons : $\alpha = H(z) = \sigma^d(z) + \sigma^{2d}(z) + \ldots + z$ (7)

Alors , ce nombre α est dans le corps cyclotomique K ; ses conjugués sont de la forme

$$\sigma(\alpha) = \sum_{1 \le r \le d'} \sigma^{dr+1} \quad \text{et} \quad \sigma^x(\alpha), \text{ avec } x \bmod d \quad (8)$$

Cela implique que ce nombre α engendre un sous corps $L = Q(\alpha)$ de K Ce nombre α admet d conjugués : $\sigma(\alpha), \ldots \sigma^{d-1}(\alpha)$ et $\sigma^d(\alpha) = 1$.

Tout corps cyclotomique $Q(z)$ possède des sous corps particuliers :

Théorème 6 :

Soit le $n^{ème}$ corps cyclotomique $Q(z)$, pour $n \ge 5$.

1)$Q(z)$ contient un sous corps quadratique $Q([up]^{1/2})$ avec p diviseur de n, $u = +1$ pour $p \equiv 1 \bmod 4$, $u = -1$ pour $p \equiv 3 \bmod 4$.

2) Il contient un unique sous - corps réel maximal $Q(z + z^{-1})$; ce sous corps réel est de degré $\varphi(n)/2$. v

Exemple1

Le $7^{ème}$ corps cyclotomique contient le sous corps quadratique $Q([-7]^{1/2})$ ce sous corps est unique ;

Il contient un unique sous corps réel maximal : $Q(z + z^{-1}) = Q(\text{Cos}2\pi/7)$; ce sous corps est cubique .

Un générateur $[up]^{1/2}$ du sous corps quadratique du $p^{ème}$ corps cyclotomique $Q(z)$, p premier, est formé de la somme :

$$S = \sum_{1 \le a \prec p} (\frac{a}{b}) z^a, où \left(\frac{a}{b}\right) \text{ désigne le symbole de Legendre}$$

Exemple 2 :

Sous corps particuliers du $35^{éme}$ corps cyclotomique Q(z)

L'hypothèse $z^{35} = 1$ implique les 2 relations :

$(Z^5)^7 = 1$ et $(Z^7)^5 = 1$

Il en résulte que le $7^{éme}$ corps cyclotomique $Q(z^5)$ et le $5^{éme}$ corps cyclotomique $Q(z^7)$ sont des sous - corps de Q(z) .

On en déduit les 3 sous corps quadratiques de Q(z) :

$$Q(\sqrt{5}), \quad Q(\sqrt{-7}) \text{ et } Q(\sqrt{-35})$$

Le corps Q(z) admet un unique sous - corps réel maximal : Q(Cos $2\pi/35$) et deux sous corps réels Q(Cos $2\pi/5$) et Q(Cos $2\pi/7$)

L'intersection et le produit de 2 corps cyclotomiques sont déterminés par le :

Théorème 7 :

Soient 2 entiers m et n premiers entre eux et les corps cyclotomiques $Q(z_m)$ et $Q(z_n)$ où z_t désigne une racine primitive $t^{ème}$ de l'unité . Alors ,

1) L'intersection des 2 corps : $Q(z_m) \cap Q(z_n) = Q$;

2) Le produit des 2 corps : $Q(z_m)\, Q(z_n) = Q(z_{mn})$

Preuve : cf[6] corollaire du théorème 1 .2 page 257. ν

2.2- Polynômes cyclotomiques

Définition 2:

Le $n^{ème}$ polynôme cyclotomique est le polynôme minimal sur le corps des nombres rationnels Q d'une racine primitive d'ordre n de l'unité.

Le degré et la forme du $n^{ème}$ polynôme cyclotomique sont précisés par le :

Théorème 8 :

Soit le $n^{ème}$ polynôme cyclotomique $f_n(x)$; alors :

1)Ce polynôme est de degré $\varphi(n)$

2)C'est un polynôme de l'anneau Z[x]

3) $f_p(x) = (x^p - 1)/(x-1) = x^{p-1} + x^{p-2} + \ldots + x + 1$ pour p premier

4) $f_{p^r}(x) = f_p(x^{p^{r-1}})$ *pour tout entier* $r \ge 1$ *et pour p premier*

5) $f_{p^n}(x) = \dfrac{f_n(x^p)}{f_n(x)}$ *pour p premier ne divisant pas n*

6) $f_{2n}(x) = f_n(-x)$ *pour les entiers n impairs .*

Preuve : cf [9]

ν

Le calcul du polynôme $f_d(x)$ peut être fait avec le :

Théorème 9 :

Soit $f_n(x)$ *le* $n^{ème}$ *polynôme cyclotomique . Alors :*

1) $x^n - 1 = \prod_{d/n} f_d(x)$ *pour tous les diviseurs d de n ;*$1 \leq d \leq n$ *;*

2) $f_n(x) = \prod_{d/n} (x^{n/d} - 1)^{\mu(d)}$ *où* $1 \leq d \leq n$ *et* μ *est la fonction arithmétique de Möbius*

Preuve : Cf. [4] Lemme 9.44 page 81

ν

La fonction de Möbius satisfait les relations :

$\mu(1) = 1$, $\mu(n) = 0$ si n contient un facteur carré ;

$\mu(p_1 \ldots p_r) = (-1)^r$ pour r nombres premiers p_i ;

$\sum_{d/n} \mu(d) = 0$ pour $n > 1$

2.3- Décomposition des idéaux dans une extension cyclotomique K du corps Q

La décomposition des idéaux dans les corps cyclotomiques est précisée par les résultats suivants :

Dans la théorie des extensions galoisiennes de degré fini n du corps Q , les nombres premiers du corps Q ramifiés dans une extension K sont les diviseurs premiers du discriminant du corps K; tout diviseur premier p du discriminant se ramifie sous la forme :

$$pO_K = (P_1 \ldots .. P_g)^e$$

où e est l'indice de ramification de p , f est le degré résiduel de l'idéal premier P_i , la norme de P_i satisfait : $N(P_i) = p^f \equiv 1 \bmod n$ et la formule efg =degré du corps = n .

Les nombres premiers qui ne divisent pas le discriminant du corps sont décomposés en un produit d'idéaux premiers de degré f. Il en résulte que f est un diviseur du degré du corps .

Il existe plusieurs types de ramification des idéaux premiers p :

1) $pO_K = P^n$: ramification totale; le degré résiduel de l'idéal premier P est égal à 1.

2) $pO_K = P^d$ avec $d < n$: ramification ; le degré de l'idéal premier P est $f > 1$.

3) $pO_K = P_1^{n_1} P_2^{n_2}$ avec $n_1 f_1 + n_2 f_2 = n$: ramification ; les degrés des idéaux sont des entiers $f_i > 1$

Il existe plusieurs types de non ramification :

4) $pO_K = P_1 \dots P_n$ avec $\deg P_i = 1$, p est totalement décomposé ;

5) $pO_K = P_1 \dots P_g$ avec $\deg P_i = f > 1$ et $fg = n$; p est décomposé ;

6) $pO_K = P$ avec $\deg P = n$, p est inerte .

Théorème 10 :

Soit un entier composé $n = p^r n_0$ où p est un nombre premier qui ne divise pas n_0 , le $n^{ème}$ corps cyclotomique $Q(z) = K$ et l'anneau des entiers O_K du corps K ;, alors :
Le nombre premier p se ramifie sous la forme :

$$pO_K = (P_1 \dots P_g)^{\varphi(p^r)}$$

où les P_i sont des idéaux premiers de K , conjugués, de norme commune $N(P_i) = p^f \equiv 1 \bmod n_0$; f est égal à l'ordre de la classe résiduelle p mod n_0 et $fg = \varphi(n_0)$. ν

Dans le $p^{ème}$ corps cyclotomique $K = Q(z)$, le nombre premier p est totalement ramifié :

$$pO_K = P^{p-1}$$

où l'idéal premier P est du premier degré $N(P) = p$ et $P = (1 - z)O_K$

Preuve : cf[6] ; page 258-259
ν

Théorème 11 :

Soit le $n^{ème}$ corps cyclotomique $K = Q(z)$ et son anneau des entiers O_K. Alors tout nombre premier p qui ne divise pas n se décompose sous la forme :

$$p O_K = P_1 \dots P_g$$

où les P_i sont des idéaux premiers de K conjugués de degré f , $N(P_i) = p^f \equiv 1 \bmod n$ et $fg = \varphi(n)$. ν

Les nombres premiers p totalement décomposés sont les $p \equiv 1 \bmod n$

2.4- Bases d'entiers et discriminants de corps cyclotomiques

Commençons par l'évaluation des discriminants du $p^{ème}$ corps cyclotomique , p premier impair .

Théorème 12 :

Soit le $p^{ème}$ corps cyclotomique $K= Q(z)$ pour p premier impair et son anneau des entiers O_K. Alors :

1) L'ensemble $\{ 1,z,...z^{p-2}\}$ est une base des entiers du corps K

2) L'anneau O_K est un ZI - module libre de rang p-1.

3) Le discriminant du $p^{ème}$ corps cyclotomique vaut :

$$disc_{K/Q} = (-1)^{(p-1)/2}\ p^{p-2}$$

Preuve : cf[5] et cf[13] Chap.V

ν

Théorème 13 :

Soit un nombre premier impair p , le $p^{s-ème}$ corps cyclotomique $K = Q(z)$ et son anneau des entiers O_K . Alors :

1) L'ensemble des puissances $\{ 1,z ,z^2...z^{\varphi(p^S)-1}\}$ est une base des entiers du corps K ;

2) L'anneau O_K est un ZI – module libre de rang $\varphi(p^s) –1$;

3) Le discriminant du corps K vaut :

$$dis_{K/Q} = (-1)^{\varphi(p^S)/2}\ p^T \quad où \quad T = p^{s-1}(ps –s-1)$$

ν

Théorème 14 :

Soit un entier $m = p_1^{s_1} p_2^{s_2} ... p_t^{s_t}$ produit de puissances d'entiers premiers p_i , le $m^{ème}$ corps cyclotomique $K= Q(_m)$ et son anneau d'entiers O_K. Alors :

1) L'ensemble des puissances $\{1,z ,z^2...z^{\varphi(m)-1}\}$ est une base des entiers du corps K

2) L'anneau O_K est un Z- module libre de rang $\varphi(m) -1$.

3) Le discriminant du corps K vaut :

$$dis_{K/Q} = (-1)^{\frac{\varphi(m)}{2}} \frac{m^{\varphi(m)}}{\prod_{p/m} p^{\frac{\varphi(m)}{p-1}}} = \left[\frac{m\,(-1)^{1/2}}{\prod_{p/m} m p^{\frac{1}{p-1}}} \right]^{\varphi(m)} = \left[\frac{m(-1)^{1/2}}{\prod_{p/m} \sqrt{p}\, m^{p-1}} \right]^{\varphi(m)}$$

Les produits étant pris sur tous les diviseurs p premiers de m

Preuve des théorèmes 12 et 13 :cf[5] page525-526

ν

Exemples

1) $m = p = 11$, $dis_{K/Q} = -11^9$;

2) $m = p^s = 11^6$, $dis_{K/Q} = -11^T$; avec $T = 11^5 .59$;

3) $m = 5^8\ x11^4\ x13^7$, $dis_{K/Q} = 5^{\frac{31}{4}\varphi(m)} .\ 11^{\frac{39}{10}\varphi(m)} .\ 13^{\frac{83}{12}\varphi(m)}$

Corollaire :

Soit le $2^{s\text{-ème}}$ corps cyclotomique $K = Q(z)$ avec $s \geq 3$ et son anneau d'entiers O_K. Alors :

1)L'ensemble des puissances $\{1, z, z^2, \ldots, z^T\}$ avec $T = 2^{s-1} - 1$ est une base des entiers du corps K

2) L'anneau O_K est un Z- module libre de rang T ;

3) Le discriminant du corps K vaut :

$$dis_{K/Q} = 2^{T'} \text{ avec } T' = (s-1)\ 2^{s-1}$$

*P*reuve : par application du théorème 14

ν

Les formules des discriminants donnent les nombres premiers ramifiés et ceux qui ne le sont pas .

2.5- Classes d'idéaux

La détermination des classes d'idéaux d'un corps de nombres se traite avec des éléments de la théorie analytique des nombres :

la fonction Zêta de Dedekind du $n^{ème}$ corps cyclotomique :

$$\xi_K(s) = \prod_p \prod_{P/p} [(1 - N(P))^{-s}]^{-1}$$

où P parcourt l'ensemble des idéaux premiers de K qui divisent p,

le régulateur R_K , l' existence d'un idéal I de norme bornée :

$$N(I) \leq \left(\frac{2}{\pi}\right)^t |d_K|^{\frac{1}{2}}$$

Le nombre h_p de classes d'idéaux du $p^{ème}$ corps cyclotomique est de la forme :

$$h_p = \frac{\sqrt{p}}{2^{\frac{p-3}{2}} \pi^{\frac{p-1}{2}} R} L(1,\chi)$$

où L est la série de Dirichlet et χ le caractére modulaire de L

La borne de Minkowski pour les idéaux dans les corps de nombres F de degré n est :

$$B_F = \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|dis_{F/Q}|}$$

où t désigne le nombre de paires de conjugués complexes du corps F ($n = r + 2t$).

Il existe plusieurs résultats sur le nombre de classes du $n^{ème}$ corps cyclotomique .

Le $n^{ème}$ corps cyclotomique $K = Q(z_n)$, pour $3 \leq n \leq 10$ admet un nombre de classes égal à $h_K = 1$.

Preuve : cf[14]E. Weiss , proposition 7.7.1

Pour n impair , l'égalité des corps cyclotomiques $Q(z_n) = Q(z_{2n})$ implique les nombres de classes :

$$h_{Q(z_3)} = h_{Q(z_6)} \quad et \quad h_{Q(z_4)} = h_{Q(z_8)}$$

Pour étudier les autres corps cyclotomiques , n= 5, 7, 9 nous utilisons la borne de Minkowski :

$$B = \left(\frac{4}{\pi}\right)^{\frac{\varphi(n)}{2}} \frac{n!}{n^n} \sqrt{|dis_{F/Q}|}$$

Les calculs donnent B< 5 pour n=9

Pour l'idéal $2O_K$ dans $Q(z_9) = K$, la norme de cet idéal satisfait la congruence $2^f \equiv 1 \bmod 9$; elle admet la solution minimale $2^f = 64$.

Il en résulte la norme $N(2O_K) = 64 > 5$.

Il n'y a pas d'idéaux I dans la classe $2\,O_K$ dont la norme satisfasse le critére de Minkowski.

On en déduit $h_{Q(z_9)} = 1$

Théorème 15 :

Il y a exactement 29 corps cyclotomiques de nombres de classes h =1 ; ce sont les $n^{èmes}$ corps $K = Q(z_n)$ pour les 29 valeurs :

n=3,4,5,7,8,9,11,12,13,15,16,17,19,20,21,24,25,27,27,28,32,33,35,36,40,44,45,48,60,et 84.

Preuve : cf[11]Théorème page 248 ν

Les spécialistes décomposent le nombre h de classes d'idéaux du $n^{ème}$ corps cyclotomique $K = Q(z_n)$ en un produit : $h = h_0 h_1$ où h_0 est le nombre de classes du sous- corps réel maximal $K_0 = Q(\cos 2\pi /n)$. Ce facteur h_0 est lié aux groupes des unités U_K de K et U_{K0} du sous- corps réel maximal K_0 de K par le :

Théorème 16 :

Dans le $p^{ème}$ corps cyclotomique $K = Q(z_p)$, le facteur h_0 du nombre de classes est égal à l'indice $[U_K : U_{K0}]$ du groupe U_{K0} engendré par les unités $u = \sin(k\pi/p)/\sin(\pi/p)$ pour $k = 2,3,\ldots,(p-1)/2$, du corps K dans le groupe U des unités réelles positives du corps K

Preuve : Cf[13] chap V : méthodes analytiques § 5-3 p 406

ν

2.6-Unités du $n^{ème}$ corps cyclotomique

Dans la théorie des nombres , une unité d'un corps de nombres K est un entier u du corps de norme $N(u) = \pm 1$.Les unités du corps K forment un groupe multiplicatif U_K.

La structure de ce groupe est précisée par le :

Théorème 17 :

Dans un corps de nombres F de degré n , les unités forment un groupe multiplicatif U_F produit direct de r groupes monogènes infinis C_t et un groupe cyclique C_F :

$$U_F = C_F . C_1 . C_2 \ldots . C_r \text{ , où } r = r_1 + r_2 - 1 \text{ , } r_1 + 2r_2 = n$$

r_1 conjugués réels de F , r_2 paires de conjugués complexes de F.

Preuve : C'est le théorème des unités de Dirichlet - Hasse.

ν

Définition 3 :

a) Le rang du groupe des unités de F est égal à r.

b)Le système $\{u_1 , u_2 ,\ldots, u_r\}$ de générateurs des groupes cycliques C_t est

un système d'unités fondamentales de F.

c) Le groupe fini C_F est l'ensemble des racines de l'unité contenues dans le corps F .

Il en résulte que ce groupe est d'ordre pair .

Définition 4 :

Le régulateur d'un corps de nombres F de degré fini n est le déterminant :

$$R_F = det\ [\sigma_s\ (log|u_t|\ )\ ]$$

où $1 \le t \le r$; r: rang du groupe des unités de F , $1 \le s \le r$ et

σ_s : Q-automorphismes du corps.

Ce régulateur est un nombre positif lorsque $r \ge 1$, ; on convient de la valeur $R_F = 1$ pour $r = r_1 + r_2 - 1 = 0$.

Ces notions s'appliquent aux corps cyclotomiques.

Théorème 18 :

a) Le nombre d'unités indépendantes dans le $n^{ème}$ corps cyclotomique $K = Q(z_n)$ est égal à $(\varphi(n) - 3)/2$.

b) Le nombre des racines de l'unité est égal à n quand n est impair et à 2n quand n est pair.

Preuve :

Dans le corps K , $r_1 = 0$ et $2\ r_2 = \varphi(n)$; cela implique que le rang du groupe des unités est égal à $\frac{1}{2}\ \varphi(n) - 1$

La $2^{ème}$ partie vient de la relation entre corps cyclotomiques

$$Q(z_n) = Q(z_{2n}) \text{ lorsque n est impair}$$

Les racines de l'unité dans le corps $Q(z_n)$ sont les puissances :

$$z_n\ , z^2_n, \ldots, z^n_n = 1$$

Les racines de l'unité dans le corps $Q(z_{2n})$ sont les nombres :

$$\pm z_n, \pm z^2_n, \ldots, \pm 1$$

ν

Théorème 19 :

Soit le $n^{ème}$ corps cyclotomique $K = Q(z_n)$ .Alors :

1) Lorsque $n = p^s$ est une puissance d'un nombre premier p, les nombres

(1 - z_n^a) / (1- z_n) sont des unités du corps K pour 2≤ a≤ n-1

2) Lorsque n = $p_1^{s_1} p_2^{s_2} ... p_t^{s_t}$ avec t≥ 2 , les nombres 1 - z_n^a sont des unités pour 1 ≤ a ≤n-1

3) Lorsque n = p^s est une puissance d'un nombre premier p , tout système d'unités fondamentales du sous - corps réel maximal $k_0 = Q(z_n + z_{-n})$ est un système d'unités indépendantes du corps cyclotomique K = Q (z_n). ν

3- Corps cycliques de degré 5

Nous utilisons la méthode d'Albert Châtelet développée dans sa monographie sur les corps cubiques abéliens pour construire des corps cycliques de degré 5 ; elle est basée sur la théorie des résolvantes de Lagrange et des idéaux essentiels d'un corps de nombres abélien.

Ces corps sont classés en corps unitaires et corps non unitaires selon que leurs bases soient normales ou ordinaires .

Ces corps sont classés en corps primaires et non primaires selon le nombre de facteurs premiers de leurs discriminants .

3.1- Résolvantes de Lagrange dans les Corps cycliques de degré 5

Soit un corps de nombres K = $Q(\theta)$, cyclique de degré 5 , d'élément primitif θ entier , son anneau d'entiers O_K et son groupe de Galois :

$$G_{K/Q} = \{\sigma,\sigma^2,\ldots,\sigma^5 = Id_K \} \quad (1)$$

On lui associe le 5ème corps cyclotomique $Q(z)$ =C
la racine primitive z satisfait les 3 relations :

$$z^5 = 1 \quad , \quad 1+z+z^2+z^3+z^4 = 0 \quad \text{et} \quad \sigma(z) = z^2 \quad (2)$$

Le groupe de Galois de C est un groupe cyclique d'ordre 4 :

$$G_{C/Q} = \{\tau,\tau^2,\ldots,\tau^4 = Id_C \} \quad (3)$$

Le composé L = K(z) = $Q(z, \theta)$ est une extension abélienne du corps Q de degré 20 . (4)

Les Q – automorphismes σ^s et τ^t se prolongent à l'extension L par les Q- automorphismes :

$$\sigma_L = \sigma \quad \text{et} \quad \tau_L = \tau \quad (5)$$

Il en résulte que le groupe de Galois $G_{L/Q}$ est abélien d'ordre 20 :

$$G_{L/Q} = \{\sigma^s\tau^t, s \bmod 5 \text{ et } t \bmod 4 \} \quad (6)$$

Ce groupe opère sur le corps L par les formules :

$\theta = \theta_1$, $\sigma(\theta_1) = \theta_2$, $\sigma^u(\theta_1) = \theta_{u+1}$, $\sigma(z) = z$

$\tau(\theta_u) = \theta_u$, $\tau(z) = z^2$, $\tau^h(z) = z^t$; $t = 2^h$

avec u et u+1 mod 5, h mod 4 et 2^h mod4 ; (7)

Suivant A . Châtelet cf[1] , nous posons la :

Définition 1 :

Soit un corps cyclique K=Q(θ) de degré 5 , de groupe de Galois $G_{K/Q} = \{\sigma^s, s \text{ mod } 5\}$, *le* $5^{ème}$ *corps cyclotomique Q(z) , de groupe de Galois* $G_{Q(z)/Q} = \{\tau^h, h \text{ mod } 4\}$ *et le corps composé K(z).*

Alors les résolvantes de Lagrange d'un conjugué θ_u *de* θ *sont les 5 sommes finies :*

$$La(\theta_u, k) = \sum_{m=0}^{4} z^{km}\ \theta_{u+m} \quad avec \quad u,\ k,\ u+m \ mod\ 5$$

Exemples : Les résolvantes de Lagrange du nombre θ_1

$La(\theta_1, 0) = \theta_1 + \theta_2 + \theta_3 + \theta_4 + \theta_5 =$ trace de θ_u ;

$La(\theta_1, 1) = \theta_1 + z\theta_2 + z^2\theta_3 + z^3\theta_4 + z^4\theta_5$;

$La(\theta_1, 2) = \theta_1 + z^2\theta_2 + z^4\theta_3 + z\theta_4 + z^3\theta_5$;

$La(\theta_1, 3) = \theta_1 + z^3\theta_2 + z\theta_3 + z^4\theta_4 + z^2\theta_5$;

$La(\theta_1, 4) = \theta_1 + z^4\theta_2 + z^3\theta_3 + z^2\theta_4 + z\theta_5$;

Signalons que S . Lang et d'autres spécialistes nomment « sommes de Gauss » ces résolvantes de Lagrange.

L'action des groupes de Galois des corps abéliens K, Q(z) et K(z) est déterminée par le :

Théorème 20 :

Soit les résolvantes de Lagrange $La(\theta_u, k)$ *d'un élément* θ_u *du corps K , les groupes de Galois :*

$G_{K/Q} = \{\sigma^s, s \text{ mod}5\}$, $G_{C/Q} = \{\tau^t, t \text{ mod}4\}$ *et* $G_{K(z)/Q} = \{\sigma^s\tau^t, s \text{ mod}5 \text{ et } t \text{ mod}4\}$. *Alors :*

1) Les résolvantes de Lagrange $La(\theta_u, k)$ *sont des nombres du corps composé K(z) .*

2) un nombre x du composé K(z) est rationnel si et seulement si il est invariant par σ *et* τ *:*

$$\sigma(x) = \tau(x) = x.$$

3) L'action du groupe $G_{K/Q}$ sur les résolvantes de Lagrange donne les conjugués :

$$\sigma^s (La(\theta_u, k)) = La(\theta_{u+s}, k) \text{ avec } u,\ u+s \text{ et } s \bmod 5 .$$

4) L'action du groupe $G_{C/Q}$ sur les résolvantes de Lagrange donne les conjugués :

$$\tau^t(La(\theta_u, k)) = La(\theta_u, 2^t k) \text{ avec } t \bmod 4 \text{ et } 2^t k \bmod 5$$

Preuve : Nous appliquons les définitions des résolvantes de Lagrange de θ_u et l'action des Q - automorphismes σ et τ sur le corps K(z).

ν

Examinons quelques combinaisons des 5 résolvantes de Lagrange $La(\theta_u, k)$

Théorème 21:

Soit un corps cyclique $K=Q(\theta_u)$ de degré 5 et les 5 résolvantes de Lagrange $La(\theta_u, k)$ d'un conjugué θ_u .

Alors :

1) Leur somme n'est pas un nombre rationnel :

$$La(\theta_u, 0) + La(\theta_u, 1) + La(\theta_u, 2) + \ldots + La(\theta_u, 4) = 5\,\theta_u ;$$

2) La puissance $5^{ème}$ d'une résolvante de Lagrange $La(\theta_u, k)$ est un nombre du $5^{ème}$ corps cyclotomique de la forme :

$$La(\theta_{u\equiv}, k)^5 = \lambda_k^5 \prod_{m=1}^{4} \alpha_{k,m}^{m^{-1}} \text{ avec } \lambda_k \in C \ , mm^{-1} \equiv 1 \bmod 5$$

et $\alpha_{k,m}$ est un entier du corps C de norme $\equiv 1 \bmod 5$

3) Le produit de 2 résolvantes de Lagrange conjuguées est un nombre réel positif :

$$La(\theta_u, k).\ La(\theta_u, 5-k) = \lambda_k \lambda_{5-k}\ p_1 \ldots p_r ;$$

où λ_k et λ_{5-k} sont des entiers du corps C et les p_i des nombres premiers $\equiv 1 \bmod 5$

Preuve :Cf.[2] Elle repose sur les propriétés des résolvantes de Lagrange.

ν

Exemple de nombres $La(\theta_u, k)^5$

$$La(\theta_u, k)^5 = \lambda_k^5\ \alpha_{k,1}^1\ \alpha_{k,2}^3\ \alpha_{k,3}^2\ \alpha_{k,4}^4$$

Une condition d'appartenance de 5 nombres conjugués $\Psi_1, \Psi_2, \ldots \Psi_5$ d'un corps $Q(\Psi)$ au corps abélien $Q(\theta) = K$ est précisée dans le :

Théorème 22 :

Soit deux corps cycliques de degré 5 , $Q(\theta_u)$ et $Q(\Psi_u)$. Alors la famille $\{\Psi_1, \ldots, \Psi_5\}$ des 5 conjugués de Ψ_u appartient au corps $Q(\theta_u)$ si et seulement si les résolvantes de Lagrange des θ_u et des Ψ_u satisfont :

$$\frac{La\,(\theta_u\ ,k)}{La(\Psi_u\ ,k')} = \lambda = \text{élément du corps } C \text{ pour certains entiers } k \text{ et } k'$$

Preuve : cf[2] et cf[17]

Introduisons des nombres $\beta_{i,j}$ du corps $Q(\theta, z)$ par la formule :

$$\beta_{i,j} = \frac{La\,(\theta_u\ ,i)\ La\,(\theta_u\ ,j-i)}{La\,(\theta_u\ ,j)} \text{ pour } u\ ,\ i, j \text{ et } j-i \bmod 5 \qquad (8)$$

Alors pour $j = 2i$, la formule devient :

$$\beta_{i,2i} = \frac{La\,(\theta_u\ ,i)^2}{La\,(\theta_u\ ,2i)} \qquad (9)$$

La valeur $La\,(\theta_u\ ,i)^5 = \lambda_j^5 \prod_{m=1}^{4} (\alpha_{mj})^{m^{-1}}$ implique

$$\beta_{i,j} = \frac{\lambda_j\,\lambda_{j-i}}{\lambda_j} \prod_{m=1}^{4} (\alpha_{mj})^{M} \quad \text{avec} \quad M = [\,m^{-1} + (mj\,(j-1))^{-1} - j\,(mi)^{-1}\,] \Big/ 5 \qquad (10)$$
$$mi \neq m\,j$$

Ces nombres $\beta_{i,j}$ servent à déterminer des polynômes cycliques de degré 5.

3. 2 - Idéaux essentiels dans un corps cyclique de degré 5

Définition 2:

Un idéal essentiel du $n^{ème}$ corps cyclotomique est un idéal principal J qui satisfait les 2 conditions :

(1) Les conjugués J_k de l'idéal J sont principaux ;

(2) Le produit d'idéaux $J_1^k J_k^{-1} = a_k^n$ est la puissance $n^{ème}$ d'un idéal a_k du $n^{ème}$ corps cyclotomique (cf[1] Albert Châtelet)

Le $5^{ème}$ corps cyclotomique *C* ayant un nombre de classes h = 1 , tous ses idéaux sont principaux ; la $1^{ére}$ condition est satisfaite .

La structure des idéaux essentiels du corps *C* est précisée par les résultats suivants :

Théorème 23 :

Tout idéal essentiel J du $5^{ème}$ corps cyclotomique se met sous la forme d'un produit d'idéaux a_m du premier degré :

$$J = \lambda^5 \prod_{m=1}^{4} a_m^{m^{-1}} \text{ , avec } mm^{-1} \equiv 1 \bmod 5 \text{ , } \lambda \text{ entier du corps } Q(z)$$

$N(a_m)=p_1p_2...p_n$ *et* p_i *: nombres premiers congrus à 1 mod 5*

ν

Les idéaux a_m étant principaux , ils sont de la forme $a_m = \alpha_m O_5$

Il en résulte le :

Corollaire 1 :

Tout idéal essentiel J du $5^{ème}$ corps cyclotomique C se met sous la forme :

$$J = \lambda^5 \prod_{m=1}^{4} \alpha_m^{m^{-1}} O_5 \text{ , avec } \alpha_m \text{ entiers du corps } C .$$

Ce corollaire implique que tout idéal essentiel J_k admet une base particulière formée de 4 entiers conjugués $\alpha_m^{m^{-1}}$; pour simplifier l'écriture, nous posons :

$$b_k = \prod_{m=1}^{4} \alpha_m^{m^{-1}}$$

ν

L'idéal essentiel $J_k = b_k O_5$ est un idéal essentiel canonique .

Nous obtenons une relation entre 2 idéaux essentiels conjugués :

Corollaire 2 :

Tout idéal essentiel J_k du $5^{ème}$ corps cyclotomique C admet une base $\lambda_k b_k$, non puissance $5^{ème}$ exacte , qui satisfait la relation :

$J_k J_{5-k} = (\lambda_k \lambda_{5-k})^5 b_k b_{5-k} = (a\, p_1 \ldots p_n)^5$, *avec* $a = \lambda_k \lambda_{5-k}$, $b_k = \prod_{m=1}^{4} \alpha_m^{m-1}$

et $N(\alpha_m) = p_1 \ldots p_n$, $p_i \equiv 1 \bmod 5$ *et premiers .*

Preuve : théorème 4 , le corollaire 1 et les propriétés de structure des idéaux essentiels du corps *C* .

ν

Les résolvantes de Lagrange d'un élément θ_u du corps $K = Q(\theta)$ et les idéaux essentiels du corps *C* sont *liés par des relations* .

A tout idéal essentiel $J_k = \lambda_k^5 b_k O_5$ nous associons un corps cyclique $Q(\theta)$ de degré 5 par la relation :

$$\lambda_k^5 b_k = La(\theta_u, k)^5$$

Les bases b_k des idéaux essentiels permettent de distinguer la classe des corps cycliques K pourvus d'une base normale d'entiers et la classe des corps cycliques K sans base normale d'entiers

Théorème 24:

Soit le $5^{ème}$ corps cyclotomique C , son anneau d'entiers O_5 , ses idéaux essentiels $J_k = \lambda_k^5 b_k O_5$. Alors :

1) Un idéal J_k correspond à un corps cyclique de degré 5 , $K = Q(\theta)$, de resolvantes de Lagrange satisfaisant la relation :
$La(\theta_u, k)^5 = \lambda_k^5 b_k$ avec b_k = base définie au corollaire 1 du théorème 4.

2) Lorsque $b_k \equiv \pm 1 \bmod 5$, alors le corps K admet une base normale d'entiers de trace ± 1 et de discriminant $dis_{K/Q} = (p_1 \ldots p_n)^4$ avec des nombres premiers $p_i \equiv 1 \bmod 5$

3) Lorsque $b_k \not\equiv \pm 1 \bmod 5$, alors le corps K n'admet pas de base normale d'entiers ; il admet une base ordinaire $(1, \theta_2, \theta_3, \theta_4, \theta_5)$ de discriminant
$dis_{K/Q} = (25\, p_1 \ldots p_n)^4$.

Preuve : cf.[2]. ν

Le discriminant d'un corps cyclique $K = Q(\theta)$ s'exprime au moyen des résolvantes de Lagrange de θ.

Cas d'un corps K pourvu d'une base normale d'entiers $(\theta_1, \theta_2 \ldots, \theta_5)$

$$\begin{vmatrix} \theta_1 & \theta_2 & \theta_3 & \theta_4 & \theta_5 \end{vmatrix}^2$$

$$dis_{K/Q} = \begin{matrix} \theta_2 & \theta_3 & \theta_4 & \theta_5 & \theta_1 \\ \theta_3 & \theta_4 & \theta_5 & \theta_1 & \theta_2 \\ \theta_4 & \theta_5 & \theta_1 & \theta_2 & \theta_3 \\ \theta_5 & \theta_1 & \theta_2 & \theta_3 & \theta_4 \end{matrix} = [\prod_{k=0}^{4} La(\theta_u, k)]^2 = (p_1 \ldots p_n)^4$$

Le conducteur d'un tel corps K vaut $Cond(K) = p_1 \ldots p_n$.

Cas d'un corps K sans base normale d'entiers ; alors $\{1, \theta_2, \theta_3, \theta_4, \theta_5\}$ est une base ordinaire d'entiers

$$dis_{K/Q} = \begin{vmatrix} 1 & \theta_2 & \theta_3 & \theta_4 & \theta_5 \\ 1 & \theta_3 & \theta_4 & \theta_5 & \theta_1 \\ 1 & \theta_4 & \theta_5 & \theta_1 & \theta_2 \\ 1 & \theta_5 & \theta_1 & \theta_2 & \theta_3 \\ 1 & \theta_1 & \theta_2 & \theta_3 & \theta_4 \end{vmatrix}^2 = [\prod_{k=0}^{4} La(\theta_u, k)]^2 = (25 p_1 \ldots p_n)^4$$

Alors le conducteur d'un tel corps vaut $Cond(K) = 25\, p_1 \ldots p_n$.

Définition 3 :

Un corps cyclique K de degré 5 qui admet une base normale d'entiers est un corps unitaire ; sinon , c'est un corps non unitaire .

Le passage d'une base d'entiers (θ_u) d'un corps K à une autre base d'entiers (Ψ_u) s'obtient au moyen d'une 5x5 matrice $M = (m_j)$ satisfaisant les 3 conditions :

1) $m_j \in Z$;
2) La diagonale de la matrice M est formée de termes m_1 ;
3) $\sum_{j=1}^{5} m_j = \pm 1$

$$M = \begin{pmatrix} m_1 & m_2 & m_3 & m_4 & m_5 \\ m_5 & m_1 & m_2 & m_3 & m_4 \\ m_4 & m_5 & m_1 & m_2 & m_3 \\ m_3 & m_4 & m_5 & m_1 & m_2 \\ m_2 & m_3 & m_4 & m_5 & m_1 \end{pmatrix} \quad \text{avec} \quad \det(M) \neq 0$$

Exemple : $m_1 = 2$, $m_2 = -1$, $m_3 = m_4 = 1$ et $m_5 = -2$

3-3-Monoïde des corps cycliques de degré 5 et corps primaires

Les éléments du monoïde E(5) sont les corps cycliques de discriminants contenant un seul facteur premier et les corps cycliques de discriminants

contenant plusieurs facteurs premiers . Il en résulte que les conducteurs de ces corps contiennent un seul facteur premier ou plusieurs facteurs premiers .

Définition 4 :

Un corps cyclique K de degré 5 est primaire lorsque son discriminant contient un seul facteur premier .

D'après ce qui précède , il n'y a qu'un seul corps cyclique , primaire , non unitaire , de degré 5 : c'est le corps de conducteur 25.

Il y a une infinité de corps cycliques , primaires , unitaires, de degré 5 ; ce sont les corps de conducteur p , $p \equiv 1 \mod 5$.

Pour définir une loi de composition sur l'ensemble E(5) , nous commençons par 2 corps primaires unitaires $K_1 = Q(\theta)$ et $K_2 = Q(\Psi)$, de conducteurs respectifs p_1 et p_2 , de groupes de Galois respectifs $\{\sigma_1,\ldots, \sigma_1^5=Id\}$ et $\{\sigma_2,\ldots, \sigma_2^5=Id\}$. Alors le corps composé $K_1K_2 = Q(\theta,\Psi)$ est une extension abélienne de degré 25 du corps Q ;

Ce corps de degré 25 contient plusieurs sous corps cycliques de degré 5 : les 2 corps primaires K_1 et K_2 et des corps composés $L_t = Q(\beta_t)$.

Par définition la composition s'exprime à l'aide des résolvantes de Lagrange :

$$La(\theta_1, k)\, La(\Psi_1, k') = La(\beta, k'')$$

Cette relation donne des nombres du corps $K_1 K_2$.

Par exemple , les résolvantes de Lagrange $La(\theta_1, 1)$, $La(\Psi_1, 1)$ et la relation :

$$La(\beta_1, 1) = La(\theta_1, 1)\, La(\Psi_1, 1)$$

donnent le nombre :

$$\beta_1 = \theta_1\Psi_1 + \theta_2\Psi_5 + \theta_3\Psi_4 + \theta_4\Psi_3 + \theta_5\Psi_2$$

Les résolvantes $La(\theta_1, 1)$, $La(\Psi_1, 2)$ et la relation: $La(\beta_2, 1) = La(\theta_1, 1) La(\Psi_1, 2)$ donnent le nombre :

$$\beta_2 = \theta_1\Psi_2 + \theta_2\Psi_5 + \theta_3\Psi_5 + \theta_4\Psi_2 + \theta_5\Psi_5$$

Chaque nombre β_t admet 5 conjugués distincts $\sigma_2^r(\beta_t)$ pour $r = 1,2,\ldots,5$.

Cela implique que β_t engendre un corps cyclique L_t de degré 5 et de groupe de Galois $G_{L_t/Q}$ isomorphe au groupe $\{\sigma_2^r , r = 1,2,\ldots,5\}$.

Les calculs donnent 4 nombres β_t qui admettent des familles de nombres conjugués $\{\sigma_2^r(\beta_t)\}$ distinctes.

Nous avons démontré le :

Théorème 22 :

Il existe 4 corps de nombres cycliques de degré 5 de même discriminant $(p_1 p_2)^4$ *, avec* $p_i \equiv 1 \mod 5$ *et premiers .*

ν

Définition 5 :

Soient 2 corps cycliques $K = Q(\theta)$ *et* $L=Q(\Psi)$ *, de degré 5 et de discriminants respectifs dis(K) et dis(L) premiers entre eux .*

Le composé des corps K et L relativement au groupe de Galois du corps est le corps $Q(\beta)$ *cyclique de degré 5 construit avec les résolvantes de Lagrange :*

$La(\theta_u, k)\ La(\Psi_u, k') = La(\beta_u, k'')$.

Nous désignons ce composé par $Q(\beta) = K \times L$.

Cette composition de corps s'étend à plusieurs éléments de l'ensemble E(5) des corps cycliques de degré 5.

Corollaire 1 :

Il existe 4 corps de nombres cycliques de degré 5 , de même discriminant $(25p)^4$ *pour* $p \equiv 1 \mod 5$.

ν

Corollaire 2 :

Le nombre de corps cycliques de degré 5 et de même discriminant : $(25^t p_1 \ldots p_n)^4$ *est égal à* 4^{n+t-1}, *pour* $p_i \equiv 1 \mod 5$ *et premiers ,* $n \geq 1$ *et* $t = 0$ *ou 1.*

Preuve : par récurrence sur le nombre n. cf[2]

ν

3-4- Quelques Polynômes cycliques minimaux de degré 5

Définition 6 :

Un polynôme cyclique de degré n de l'anneau Z[x] est un polynôme unitaire f(x) qui admet n racines θ_u *, permutables par un groupe cyclique G(n) de degré n.*

Il existe une méthode de calcul de ces polynômes basée sur les résolvantes de Lagrange , utilisée par A. Châtelet .

Une autre méthode utilisée par D. Shanks, fournit des polynômes cycliques à un paramètre, de terme constant ± 1 . D Shanks les a nommés « polynômes simplest » .

Exemple $f_3(x) = x^3 - tx^2 - (t+3)x - 1$ avec la condition $t^2 + 3t + 9 = N$, N est un nombre premier et $t \equiv 1 \bmod 3$, comme N = 13,19,37,79 , 97,…..

La construction de polynômes cycliques de degré premiers p avec les résolvantes de Lagrange est exposée dans (J.J Payan).

Un tel polynôme $f_p(x)$ est obtenu comme un déterminant d'une matrice pxp

Pour p = 5 , les polynômes cycliques de degré 5 sont obtenus par ordinateur .

Citons –en quelques uns :

$f_1(x) = x^5 - 110\,x^3 - 220\,x^2 + 1485\,x + 1276$;
$f_2(x) = x^5 - 310\,x^3 - 155\,x^2 + 20460\,x - 3751$;
$f_3(x) = x^5 - 410\,x^3 - 2255\,x^2 + 2460\,x + 17999$;
$f_4(x) = x^5 - 610\,x^3 - 4880\,x^2 + 5185\,x - 976$;
$f_5(x) = x^5 - 1010\,x^3 - 55555\,x^2 + 112110\,x + 398849$;
$f_6(x) = x^5 - x^4 - 60\,x^3 + 12\,x^2 + 784\,x - 128$;
$f_7(x) = x^5 - 1910\,x^3 - 8595\,x^2 + 594010\,x + 1596951$;
$f_8(x) = x^5 - 10\,x^3 - 5\,x^2 + 10\,x - 1$.

En conclusion de ce paragraphe , signalons que cet algorithme débute par la recherche de nombres a du Z-module des entiers Z[x] qui ont une norme égale à un nombre premier $p \equiv 1 \bmod 5$ .Nous cherchons aussi des nombres de norme égale à 25 ; c'est l'algorithme développé dans le PARI .

CHAPITRE II

THEORIE ALGEBRIQUE DES COURBES ELLIPTIQUES

1- Structures algébriques

Définition 1 :

Une courbe elliptique est une cubique plane E non singulière, irréductible, d' équation algébrique de la forme :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (1)$$

Définition 2 :

L'équation algébrique (1) est l'équation de Weierstrass de la courbe E

Dans l'équation (1) , les cinq coefficients a_i sont des éléments d'un corps commutatif K, les deux variables x et y sont racines de l'équation algébrique (1). Donc x et y sont des éléments d'une clôture algébrique K_{alg} du corps K.

Ce corps K est le corps de base de la courbe elliptique E .

Définition 3 :

Une courbe algébrique est singulière si elle admet un point singulier : un nœud où la courbe admet 2 tangentes distinctes ou un point de rebroussement où la courbe admet 2 tangentes confondues .

Les points singuliers d'une courbe plane d'équation projective:

$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - (x^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3) = 0$

sont déterminés par :

Théorème 1:

Soit une courbe algébrique plane C d'équation projective

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

Alors, les coordonnées des points singuliers de C sont solutions du système :

$F(X,Y,Z) = 0 ; F_x'(X,Y,Z) = 0, F_y'(X,Y,Z) = 0 , F_z'(X,Y,Z) = 0$

Preuve: avec la définition des points singuliers des courbes algébriques planes cf[28] chap.III § 1 page 50. v

Le groupe de Galois $G_{Kalg/K}$ de la clôture algébrique K_{alg} du corps K opère sur la courbe elliptique par les K-automorphismes σ:

$$\sigma(P) = [\sigma(x_p), \sigma(y_p)]$$

La nature du corps de base K influe sur les propriétés de la courbe elliptique E.

Lorsque K est un corps de nombres algébriques alors la théorie des nombres intervient sur la courbe elliptique par les entiers , les discriminants, les classes d'idéaux , la ramification , les valuations , l'analyse p-adique , les nombres premiers , les fonctions arithmétiques (d'Euler , Mobïus , Zêta …) de ce corps .

Lorsque K est le corps des nombres complexes IC , la théorie de ce corps intervient sur la courbe elliptique par l'analyse complexe (réseaux ,tores complexes, groupes de Lie , fonctions elliptiques , fonctions modulaires), et par la géométrie algébrique (variétés algébriques , variétés abéliennes , courbes algébriques projectives, diviseurs , schémas , cohomologie,..) .

Lorsque K est un corps fini IF_q avec $q = p^t$ éléments , alors la théorie de ces corps intervient sur la courbe elliptique (Théorème de Hasse , invariant de Hasse , courbes super- singulières, codage , cryptographie)

Lorsque K est un corps local ou un corps de fonctions , alors les théories de ces corps interviennent .

Ces influences du corps de base K sur la courbe elliptique impliquent plusieurs structures algébriques .

Ainsi une courbe elliptique possède :

une structure de variété abélienne de dimension un .
une structure de courbe algébrique projective non singulière de genre un .
une structure de schéma de dimension un.

2- Transformations linéaires des équations affines

Soit une courbe elliptique E d'équation affine :

$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ (1)

Le changement de variables linéaire :

$x = X$ et $y = ½ (Y - a_1 X - a_3)$

(en caractéristique de $K \neq 2$] transforme (1) en l'équation :

$E_1 : Y^2 = 4X^3 + b_2 X^2 + 2 b_4 X + b_6$ (2)

Les coefficients b_{2i} sont des polynômes « homogènes de degré 2 i » dans l'anneau $ZI [a_1, a_2, a_3, a_4, a_6]$

$b_2 = a_1^2 + 4a_2$; $b_4 = 2 a_4 + a_1 a_3$; $b_6 = 4 a_6 + a_3^2$ (3)

Le changement de variables linéaire pour caractéristique de $K \neq 2, 3$

$X = (x - 3 b_2)/36$ et $Y = y / 108$ (4)

transforme (2) en :

$E_2 : y^2 = x^3 - 27c_4 x - 54 c_6$ (5)

Les coefficients c_{2i} sont des polynômes « homogènes de degré 2i » dans l'anneau $ZI [b_2, b_4, b_6]$:

$c_4 = b^2_2 - 24b_4$; $c_6 = - b_2^3 + 36 b_2b_4 - 216 b_6$ (6)

Ces coefficients b_{2i} et c_{2i} permettent de définir des invariants d'une courbe elliptique E :

le discriminant, l'invariant modulaire , l' invariant différentiel , l' invariant de Hasse, le conducteur , le régulateur , la série L de Dirichlet , la fonction Zêta ….

Définitions 4:

a) Le discriminant d'une courbe elliptique E est le polynôme « homogène de degré 12 » de l'anneau $ZI [b_2, b_4, b_6, b_8]$

$$\Delta (E) = 9 b_2b_4 b_6 - 8 (b_4)^3 - 27(b_6)^2 - (b_2)^2b_8 \in ZI [b_2, b_4, b_6, b_8] \quad (7)$$

où l'on a posé :

$$4 b_8 = b_2 b_6 - (b_4)^2 \quad (8)$$

b) L'invariant modulaire d'une courbe elliptique E est l'élément :

$$j (E) = \boldsymbol{c_4}^3 \Big/ \Delta (E) = 1728 \ \boldsymbol{c_4}^3 \Big/ [\boldsymbol{c_4}^3 - \boldsymbol{c_6}^2] \quad (9)$$

c)L'invariant différentiel d'une courbe elliptique est :

$$w(E) = \frac{dx}{\quad} = \frac{dy}{\quad}$$

$2y + a_1x + a_3 \qquad 3x^2 + 2a_2x + a_4 - a_1 y$

D'autres formes d'équations de courbes elliptiques :

1) L'équation de Cassels : E : $y^2 = x^3 + A\,x + B$; $\Delta(E) = 4A^3 + 27B^2$

2) L'équation de Legendre : $E : y^2 = x(x-1)(x-\lambda)$; $\lambda \neq 0, 1$

3) L'équation de Tate : $y^2 + xy = x^3 + ax + b$

Théorème 2 :

Soit une cubique plane E définie sur un corps K d'équation :

E : $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$

de discriminant Δ *et de coefficient* c_4 *.Alors :*

1)La courbe E n'a pas de point singulier si et seulement si $\Delta \neq 0$.

2) La courbe E admet un nœud si et seulement si $\Delta = 0$ *et* $c_4 \neq 0$.

3)La courbe E admet un point de rebroussement si et seulement si $\Delta = c_4 = 0$.

Preuve : cf[28] chap.III § 1 proposition 1.4. ν

Exemples

1)E_1 : $y^2 = x^3 + x + 1$;

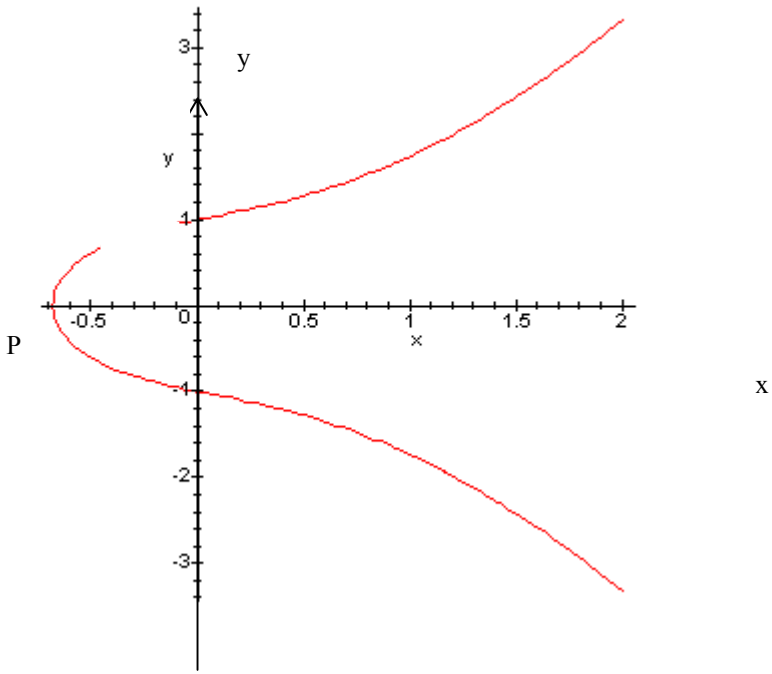
$b_2 = 0$; $b_4 = 6$; $b_6 = 4$; $\Delta(E) = -2^3.3^3.7$

Tableau des valeurs

x	-1	-0,5	0	1	2
y^2	-3	1,125	1	3	11
y	/	$\pm(0,375)^{1/2}$	± 1	$\pm\sqrt{3}$	$\pm\sqrt{11}$

Point d'intersection P de la courbe E_1 avec l'axe 0x :

x = -1/2

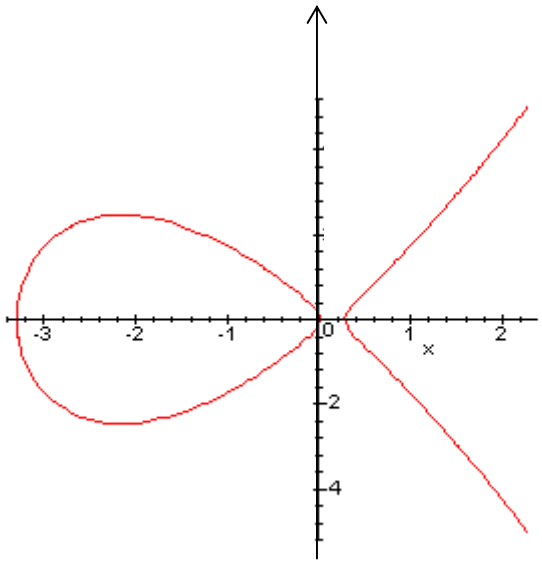


2)E_2 : $y^2 = x^3 + 3x^2 - x$;

$b_2 = 12$; $b_4 = -2$; $b_6 = 0$; $b_8 = -1$; $\Delta(E) = 208$

Tableau des valeurs

x	$-3/2-(\sqrt{13})/2$	-3	-2	-1	0	$-3/2+(\sqrt{13})/2$	1
y^2	0	3	6	3	0	0	3



y	0	$\pm\sqrt{3}$	$\pm\sqrt{6}$	$\pm\sqrt{3}$	0	0	$\pm\sqrt{3}$

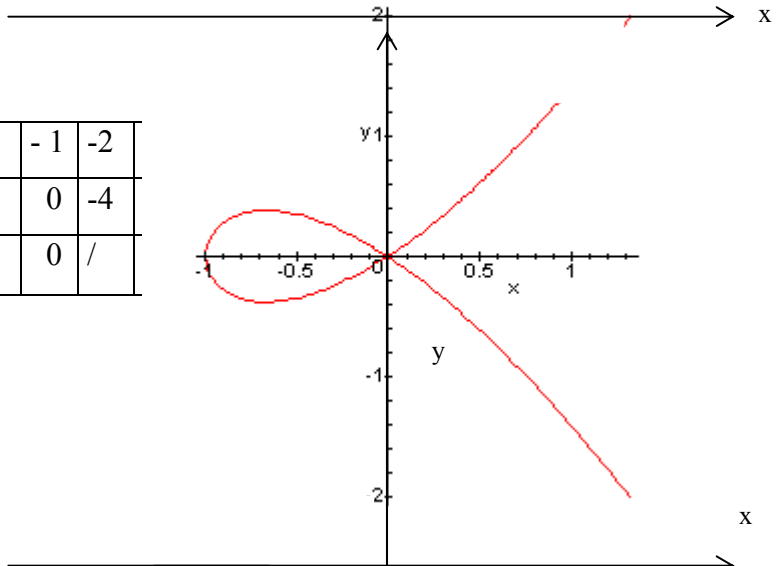
y

3)E_3 : $y^2 = x^3 + x^2$;

$\Delta(E) = 0$ et $c_4(E) = 16$, le point (0,0) est un nœud

Tableau des valeurs

x	0	- 1	-2
y^2	0	0	-4
y	0	0	/



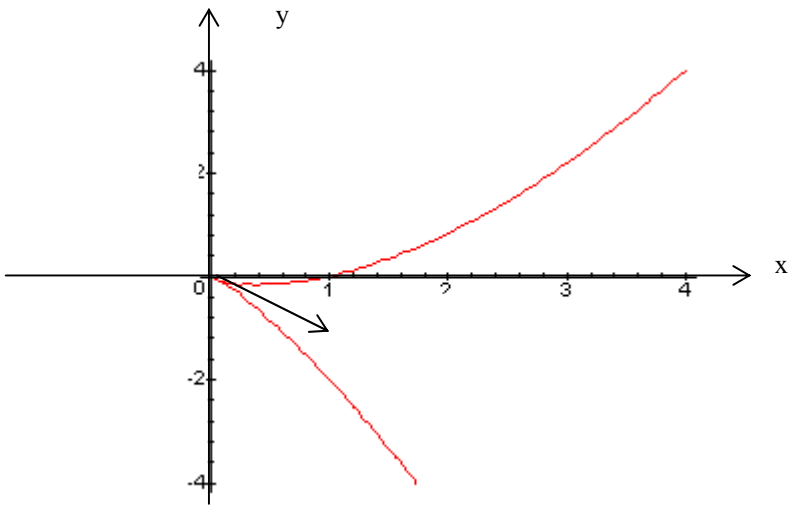
4) E_4 : $y^2+2xy = x^3 - x^2$

$\Delta(E)=0$ et $c_4(E)= 0$

Le point (0,0) est un point de rebroussement

Tableau des valeurs

x	0	1	2
y	0	0 et -2	$-2 \pm 2\sqrt{2}$



3- Groupe de Mordell-Weil E(K):

Soit une courbe elliptique E sur un corps K d'équation :

E : $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$;

Soit l'ensemble E(K) des points K – rationnels de la courbe E .

On adjoint à cet ensemble E(K) le point à l'infini de la courbe E :

$0_E = (\infty , \infty)$ dans le plan affine et (0,1,0) dans le plan projectif $P^2(K)$.

Ce point , unique par ses coordonnées projectives est déterminé par la direction de l'axe 0y.

La loi de groupe abélien sur l'ensemble E(K) est l'application :

$$T : E(K) \times E(K) \rightarrow E(K)$$

$$(P_1, P_2) \longrightarrow T(P_1,P_2) = P_1+P_2$$

L'image P_1+P_2 est déterminée par la règle géométrique :

« trois points colinéaires P_1, P_2 , P_3 d'une courbe elliptique E ont une somme nulle » :

$$P_1+P_2 +P_3= 0_E$$

Vérifions les 4 axiomes d'un groupe abélien :

Axiome de l'élément neutre :

C'est le point 0_E à l'infini qui joue le rôle d'élément neutre, dans la relation : $P+ 0_E = 0_E + P=P$, la sécante PO_E est parallèle à l'axe 0y par hypothèse sur le point O_E. (1)

Axiome du symétrique :

Dans la relation : $P_1+P_2 = P_2+P_1 = 0_E$ entre les 3 points , la sécante P_1P_2 est parallèle à l'axe 0y . (2)

Axiome de commutativité :

Les sécantes P_1P_2 et P_2P_1 sont confondues :

$(P_1+P_2) +P_3=(P_2+P_1) +P_3= 0_E$

Axiome d'associativité :

Il se vérifie par les calculs des coordonnées des points :

$(P_1 + P_2)+ P_3$ et $P_1 +(P_2 + P_3)$, pour des points $P_i \neq \pm P_j$.

Nous avons démontré le :

Théorème 3:

Soit une courbe elliptique E sur un corps K et le point à l'infini $0_E = (\infty,\infty) = (0,1,0)$ *. Alors , l'ensemble E(K) des points K rationnels de E , muni de l'application :* $(P_1,P_2) \longrightarrow P_1+P_2$ *basée sur « la règle géométrique de 3 points colinéaires » est un groupe abélien d'élément neutre* 0_E *.* v

Définition 5:

Le groupe E(K) des points K-rationnels d'une courbe elliptique E est le groupe de Mordell-Weil de la courbe .

Soit une courbe elliptique E d'équation affine :

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \qquad (1)$$

Déterminons les coordonnées des points $-P$ et P_1+P_2

Calcul des coordonnées du symétrique $-P$ *d'un point P (fig. 1):*

Le point (-P) satisfait la relation $P + (-P) = 0_E$.

Le point (-P) est le 2ème point d'intersection de la courbe E par la paralléle à 0y passant par P .

L'équation de cette parallèle est l'équation (1) où $x = x_p$ et y est l'inconnue.

Les calculs donnent les coordonnées du symétrique -P de P :

$$-P = -(x , y) = (x , -y - a_1 x - a_3) \qquad (2)$$

Calcul des coordonnées du point somme $P_1 + P_2$ *pour* $P_1 \neq \pm P_2$*:(fig2) :*

Soit les points $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$

La somme est déterminée par la règle géométrique :

$$P_1 + P_2 + P_3 = 0_E$$

Cela implique $P_1 + P_2 = -P_3 = M$

Les coordonnées du point P_3 sont calculées avec l'équation de la sécante P_1P_2 :

$y = \lambda (x - x_1) + y_1$ et $\lambda = (y_1 - y_2)/(x_1 - x_2)$

Cette sécante P_1P_2 coupe la courbe en trois points simples P_1, P_2 et P_3

Les abscisses de ces 3 points sont les zéros de l'équation :

$$[\lambda (x - x_1) + y_1]^2 + (a_1 x + a_3)[\lambda (x - x_1) + y_1] = x^3 + a_2 x^2 + a_4 x + a_6$$

La somme de ces zéros est égale :

$$x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2$$

Les calculs donnent les coordonnées de la somme $P_1 + P_2 = -P_3 = M$:

$$\begin{cases} x_M = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_M = -\lambda^3 - 2a_1\lambda^2 + \lambda(a_2 + 2x_1 + x_2 - a_1^2) + a_1a_2 - a_3 - y_1 + a_1(x_1 + x_2) \end{cases} \quad (3)$$

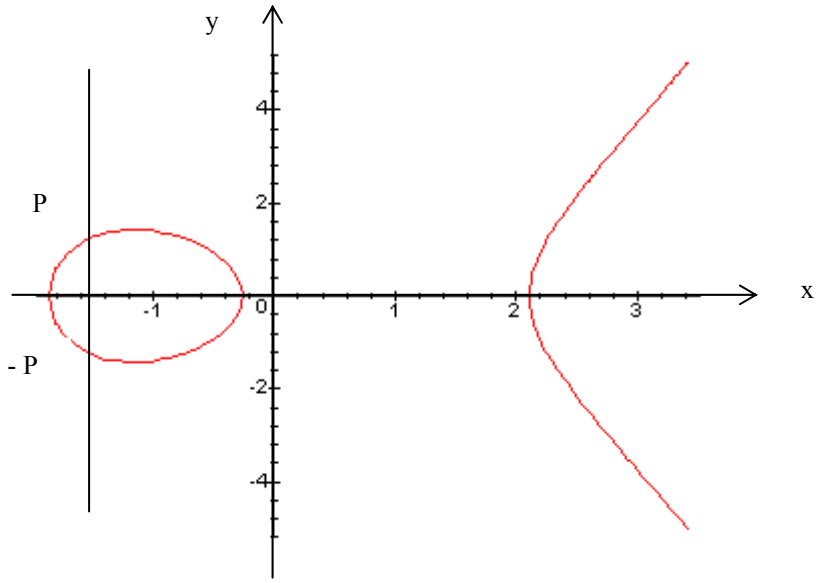


Figure 1 : Symétrique d'un point

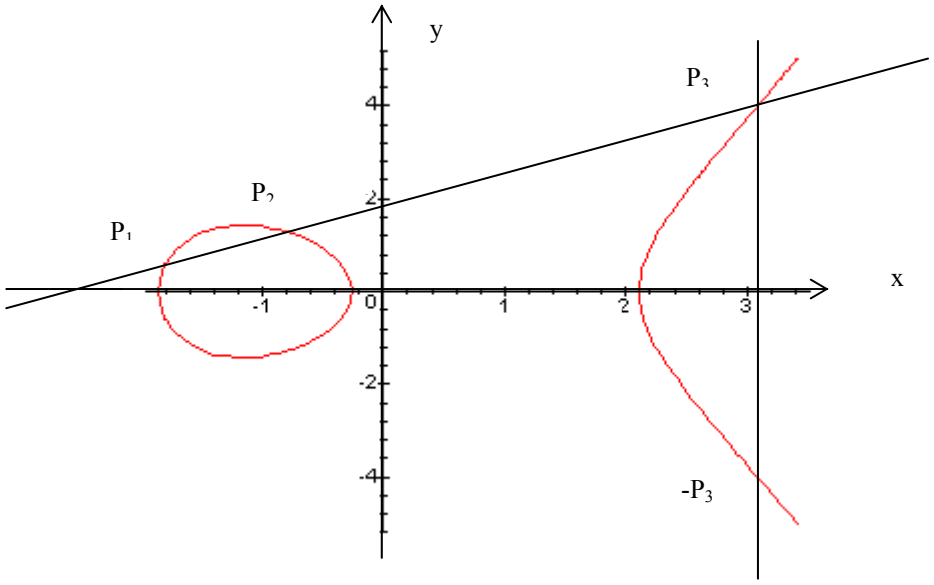


Figure 2 : Somme de deux points

4- Homomorphismes de courbes elliptiques

Ces homomorphismes sont de 4 types : isomorphismes , endomorphismes , automorphismes , isogénies.

4.1-Isomorphismes de courbes elliptiques :

Soient deux courbes elliptiques sur un corps K d'équations respectives :

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

$E' : y^2 + a'_1 xy + a'_3 y = x^3 + a'_2 x^2 + a'_4 x + a'_6$

Définition 6 :

Un isomorphisme de courbes elliptiques est une application de groupes de Mordell-Weil :

$$f : E(K) \longrightarrow E'(K)$$

qui satisfait :

$$f(P + Q) = f(P) + f(Q) \quad et \quad f(0_E) = f(0_{E'})$$

L'isomorphisme de E dans E′ est défini par le changement de variables (1)

$$\begin{aligned} x &= u^2 x' + r \\ y &= u^3 y' + u^2 x' s + t \end{aligned} \qquad (1)$$

avec u , r, s, t dans K et $u \neq 0$

Les calculs donnent des relations entre les coefficients et les invariants de E et E′:

Relations entre les coefficients a_i et a'_i :

$$\begin{aligned} u a'_1 &= a_1 + 2s \\ u^2 a'_2 &= a_2 - s a_1 + 3r - s^2 \\ u^3 a'_3 &= a_3 + r a_1 + 2t \\ u^4 a'_4 &= a_4 - s a_3 - r s a_1 + 2 r a_2 - t a_1 + 3r^2 - 2ts \\ u^6 a'_6 &= a_6 + r a_4 + r^2 a_2 - t a_3 - r t a_1 + r^3 - t^2 \end{aligned} \qquad (2)$$

Relations entre les coefficients b_i et b'_i :

$$\begin{aligned} u b'_2 &= b_1 + 12r \\ u^4 b'_4 &= b_4 + 2b_2 + 6r^2 \\ u^6 b'_6 &= b_6 + 2r b_4 + r^2 b_2 + 4r^3 \\ u^8 b'_8 &= b_8 + 3 r b_6 + 3r^2 b_4 + r^3 b_2 + 3r^4 \end{aligned} \qquad (3)$$

Relations entre les coefficients c_i et c'_i :

$$\begin{aligned} u^4 c'_4 &= c_4 \\ u^6 c'_6 &= c_6 \end{aligned} \qquad (4)$$

Relations entre les invariants :

$$u^{12} \Delta(E') = \Delta(E) \quad , \quad j(E') = j(E) \text{ et } u^{-1} w' = w \qquad (5)$$

(5) implique le :

***Théorème 4**:*

Deux courbes elliptiques E et E′ sur un corps algébriquement clos K sont isomorphes si et seulement si elles ont des invariants modulaires égaux j(E) = j(E′).

Preuve de « E et E′ isomorphes » implique *j(E) = j(E′)* :

Soit 2 courbes elliptiques E et E' isomorphes ;

Alors les coordonnées d'un point du groupe de Mordell-Weil E(K) sont liées à celles du point de E' isomorphe par les formules d'isomorphismes :

$$(x,y) \longrightarrow (u^2 x + r\ ,\ u^3 y + u^2 x s + t)$$

En particulier , ces relations (5) impliquent :

$$j(E) = j(E')$$

Preuve de « *j(E) = j(E') »* implique « E et E′ isomorphes » :

L'invariant modulaire j(E) d'une courbe elliptique E peut prendre des valeurs $j(E) = 0$, $j(E) = 1728$, $j(E) = t \neq 0, 1728$ sur un corps K de caractéristique $caracK \neq 2,3$.

Le discriminant de E satisfait la condition $\Delta(E) \neq 0$

Examinons les 3 cas possibles pour j(E)

Prenons une équation de la courbe elliptique E sous la forme :

$$E : y^2 = x^3 + c_4 x + c_6 \qquad (1)$$

Alors $j(E) = 1728\, c_4^3 / (c_4^3 - c_6^2)$ avec $c_4^3 - c_6^2 \neq 0$ (2)

1ère cas : l 'hypothèse $j(E) = 0$ implique $c_4 = 0$ et $c_6 \neq 0$

Il en résulte l'équation :

$$E : y^2 = x^3 + c_6$$

La relation entre les coefficients c_6 et c'_6:

$$u^6 = c_6 / c'_6$$

implique les formules d'isomorphisme :

$$(x,y) \longrightarrow (u^2 x\ ,\ u^3 y) \text{ avec } u = [c_6 / c'_6]^{1/6}$$

et l'équation :

$$E' : y^2 = x^3 + u^{-6} c_6 x$$

2ème cas :l 'hypothèse $j(E) = 1728$ implique $c_4 \neq 0$ et $c_6 = 0$

Il en résulte l'équation :

$$E : y^2 = x^3 + c_4 x$$

La relation entre les coefficients c_4 et c'_4 :

$u^4 = c_4 / c'_4$

implique les formules d'isomorphisme

$$(x,y) \longrightarrow (u^2x , u^3y) \text{ avec } u = [c_4 / c'_4]^{1/4}$$

et l'équation :

$E' : y^2 = x^3 + u^{-4} c_4 x$

$3^{ème}$ cas :l'hypothèse $j(E) = t \neq 0, 1728$ implique la relation :

$$(1728 c^3_4)/ (c^3_4 - c^2_6) = t \text{ avec } t \neq 0,1728, c_4 \neq 0 \text{ et } c_6 \neq 0 \quad (3)$$

cette relation se met sous la forme :

$$1728 c^3_4 = t (c^3_4 - c^2_6) \quad (4)$$

soit $tc^2_6 = c^3_4 (t - 1728)$ (5)

L'équation (5) admet la solution :

$$c_4 = t / (t - 1728) , c_6 = \pm t / (t - 1728) \quad (6)$$

il en résulte l'équation :

$E : y^2 = x^3 + [t / (t - 1728)] (x \pm 1)$

Les relations

$$u^4 c'_4 = c_6 \text{ et } u^6 c'_6 = c_6$$

impliquent les formules d'isomorphisme

$$(x,y) \longrightarrow (u^2x , u^3y) \text{ avec } u = [c_4 / c'_4]^{1/4} = [c_6 / c'_6]^{1/6}$$

et l'équation :

$E' : y^2 = x^3 + [t / (t - 1728)] (x u^{-4} \pm u^{-6})$

v

4.2- Endomorphismes d'une courbe elliptique :

Un endomorphisme d'une courbe elliptique E est un homomorphisme du groupe E(K) de Mordell-Weil dans lui même.

La description de l'anneau End(E) a été complètement déterminée par M. Deuring cf[27] page 96

Théorème 5:

Soit une courbe elliptique E sur un corps K. Alors l'anneau des endomorphismes End(E) de E est isomorphe soit à l'anneau ZI des entiers rationnels , soit à un ordre d'un corps quadratique imaginaire , soit à l'ordre de l'algèbre des quaternions .

Preuve :C'est le théorème de Deuring cf[28] page 100. v

Les 2 premiers cas interviennent pour des corps de caractéristique 0.

Le $3^{ème}$ cas intervient pour des corps de caractéristique $p>0$.

Définitions 7:

1) Soit un corps quadratique imaginaire K , son anneau A_K des entiers et un entier naturel s . Un ordre de l'anneau A_K est un sous anneau contenant ZI : ZI+ s A_K ; l'entier naturel s est le conducteur de cet ordre .

2) L'algèbre des quaternions sur le corps Q est l'ensemble :

$$A = Q + Q\alpha + Q\beta + Q\alpha\beta$$

où les générateurs α et β satisfont :

$$\alpha^2 \in Q \ , \beta^2 \in Q, \quad \alpha^2<0 \ , \ \beta^2<0 \ \text{ et } \ \beta\alpha = -\alpha\beta$$

3) Les courbes elliptiques dont l'anneau End(E) des endomorphismes contient ZI, sont des courbes elliptiques à multiplication complexe .

4.3- Automorphismes d'une courbe elliptique :

Les automorphismes d'une courbe elliptique sont précisés par le :

Théorème 6:

Soit une courbe elliptique E sur un corps K .Alors le groupe Aut (E) des automorphismes de E est un groupe d'ordre un diviseur de 24 :

1) Aut(E) est d'ordre 2 si j(E) $\neq$ 0, 1728

2) Aut(E) est d'ordre 4 si j(E) = 1728 et caractéristique de K différente de 2, 3

3) Aut(E) est d'ordre 6 si j(E) = 0 et caractéristique de K différente de 2, 3

4) Aut(E) est d'ordre 12 si j(E) = 0 =1728 et caractéristique de K égale à =3

5) Aut(E) est d'ordre 24 si j(E) = 0 = J(E) =1728 et caractéristique de K égale à 2

Preuve de (1):

Soit une courbe elliptique E sur un corps K , d'invariant modulaire j(E) $\neq$ *0, 1728* (1)

Nous prenons une équation de E de la forme

$$y^2 = x^3 + a_4 x + a_6 \qquad (2)$$

Son invariant modulaire vaut :

$$j(E) = 4 \cdot 1728 \cdot a_4^3 / (4 a_4^3 + 27 a_6^2) \qquad (3)$$

Nous prenons un automorphisme du groupe E(K) de la forme :

$$x = u^2 x' \ ; \ y = u^3 y' \qquad (4)$$

Les formules (1) et (3) impliquent :

$$a_4 \neq 0 \ \text{ et } \ a_6 \neq 0 \qquad (5)$$

Les relations entre les coefficients isomorphes sont :

$u^4 a_4 = a_4$ et $u^6 a_6 = a_6$ (6)

Il en résulte la valeur de u :

$u^2=1$ et $u = \pm 1$

Il y a donc 2 automorphismes de E :

$(x = x' , y = y')$ et $(x = x' , y = - y')$

Preuve de (2) :

Soit une courbe elliptique E, d'invariant modulaire $j(E) = 1728$ sur un corps K de caractéristique $\neq 2,3$. *(7)*

La formule (3) de l'invariant modulaire j(E) et (7) impliquent

$a_4 \neq 0$ et $a_6 = 0$ (8)

Les formules (6) impliquent :

$u^4 a_4 = a_4$

Il en résulte $u^4 =1$ et 4 valeurs de u : $u= \pm 1, \pm i$;ce sont les racines $4^{ème}$ de 1

Il en résulte 4 automorphismes :

$(x = x' , y = y')$, $(x = x' , y = - y')$, $(x = - x' , y = - i y')$ et $(x = - x' , y = i y')$

Preuve de (3) :

Soit une courbe elliptique E, d'invariant modulaire $j(E) = 0$ sur un corps K de caractéristique $\neq 2,3$ (9)

La formule (3) de l'invariant modulaire j(E) et (9) impliquent

$a_4 = 0$ et $a_6 \neq 0$ (10)

Les formules (6) implique :

$u^6 a_6 = a_6$

Il en résulte $u^6=1$ et 6 valeurs de u égales aux racines $6^{ème}$ de 1 :

$u_1= + 1$, $u_2= -1$, $u_3= + ½+i\sqrt{3}/2$, $u_4= + ½ - i\sqrt{3}/2$, $u_5= - ½ + i\sqrt{3}/2$,

$u_6= - ½ - i\sqrt{3}/2$

Il en résulte 6 automorphismes :

$(x = x' , y = y')$, $(x = x' , y = - y')$, $(x = u_3^2 x' , y = u_3{}^3 y')$,

$(x = u_4^2 x' , y = u_4{}^3 y')$ $(x = u^2_5 x' , y = u^3_5 y')$ et $(x = u^2_6 x' , y = u^3_6 y')$

Preuve de (4) :

Soit une courbe elliptique E, d'invariant modulaire $j(E) = 0$ sur un corps K de caractéristique égale à 3 *(11)*

Nous prenons un automorphisme de la courbe de la forme :

$x = u^2\ x' + r\ ;\ y = u^3 y'$

Les relations entre les coefficients isomorphes sont :

$u^4\ a_4 = a_4$ et $u^6\ a_6 = a_6 + r a_4 + r^3$ *(12)*

Les automorphismes sont déterminés par les couples (u,r)

chaque couple (u,r) est solution du système :

$u^4 = 1$ et $r^3 + r a_4 + a_6 (1 - u^2) = 0$ (13)

Sur une clôture algébrique de K , u engendre un sous groupe C_4 d'ordre 4 et r engendre un sous groupe C_3 d'ordre 3 .

Le groupe Aut (E) est isomorphe au groupe produit $C_4 \times C_3$ d'ordre 12.

Preuve (5) :

Soit une courbe elliptique E, d'invariant modulaire j(E) = *0* sur un corps K de *caractéristique égale à 2* *(14)*

Nous prenons l'équation de la courbe sous la forme :

$y^2 + a_3 x = x^3 + a_4 x + a_6$ (15)

L'équation (15) est préservée par l'automorphisme

$x = u^2\ x' + s^2\ ;\ y = u^3 y' + u^2 s x' + t$ (16)

Les relations entre les coefficients impliquent :

$$u^3\ a'_3 = a_3$$
$$u^4\ a'_4 = a_4 + s\ a_3 + s_4 \quad (17)$$
$$u^6\ a'_6 = a_6 + s^2\ a_4 + t\ a_3 + s^6 + t^2$$

Le groupe Aut (E) de la courbe E est déterminé par les triplets (u,s,t) dans une clôture algébrique de K :

$u^3 = 1,\quad s^4 + s\ a_3 + a_4 (1-u) = 0$ et $t^2 + t a_3 + s^2 a_4 + s^6 = 0$ (18)

u engendre un groupe cyclique C_3 d'ordre 3 ; s engendre un groupe cyclique C_4 d'ordre 4 et t engendre un groupe cyclique C_2 d'ordre2 ; l'équation en t implique que le groupe C_4 est « twisté » par le groupe C_2 , ces 2 groupes donnent le groupe Q_8 des quaternions ; il en résulte que le groupe Aut(E) est un groupe d'ordre 24. v

4.4- Isogénies de courbes elliptiques

Ces morphismes particuliers sont précisés par la :

Définition8 :

Soient deux courbes elliptiques E et E′ sur un corps K d'éléments neutres respectifs 0_E et $0_{E'}$.

Une isogénie de E sur E' est un morphisme $\varphi : E(K) \longrightarrow E'(K)$ qui satisfait les 3 propriétés :

(1) $\varphi(E) \neq 0_{E'}$

(2)Le noyau de l'isogénie φ est un sous groupe fini du groupe de Mordell-Weil E(K)

(3) $\varphi(P_1 + P_2) = \varphi(P_1) + \varphi(P_2)$

Toute isogénie possède des invariants spécifiques : un degré et une isogénie duale.

Définition 9:

Le degré d'une isogénie φ est égal à l'ordre du sous groupe noyau de φ : $\deg\varphi = card(\ker\varphi)$

Exemple :

Soit une courbe elliptique E .La multiplication par un entier rationnel m est une isogénie de degré m^2 si m est premier à la caractéristique du corps K

$$m_E : E(K) \longrightarrow E(K)$$
$$P \longrightarrow m_E P = mP$$

(Corollaire 6.4 .page 89 cf[28])

Le symbole mP désigne les sommes :

$$\begin{cases} mP = P + P + \ldots + P \text{ , m fois P si } m > 0 \\ mP = (-P) + (-P) + \ldots + (-P) \text{ , (- m) fois (- P) si } m < 0 \\ 0P = 0_E \text{ si } m = 0 \end{cases}$$

Définition 10:

Chaque isogénie $\varphi : E(K) \longrightarrow E'(K)$ est associée à une application

$\varphi' : E'(K) \longrightarrow E(K)$ définie par les composées :

$\varphi o\varphi' : E'(K) \longrightarrow E'(K)$ avec $\varphi o\varphi' = Id_{E'(K)}$
$\varphi' o\varphi : E(K) \longrightarrow E(K)$ avec $\varphi' o\varphi = Id_{E(K)}$

Alors φ' est l'isogénie *duale de φ*

Théorème 7:

Soit une isogénie $\varphi : E(K) \longrightarrow E'(K)$. Alors

1) L'isogénie duale φ' *de l'isogénie* φ *est unique.*

2) L'isogénie φ *et son isogénie duale* φ' *ont même degré.*

v

Les formules d'une isogénie de courbes elliptiques font intervenir des fractions rationnelles des formules des coordonnées des points $P_1 + P_2$ et $2P$

Exemple : (Velu , CRAS Paris , série A273 (1971) p.239)

Equation d'une isogénie $\varphi : E(K) \longrightarrow E'(K)$

$$(x , y) \longrightarrow (X,Y)$$

Alors les coordonnées X et Y sont définies par les formules :

$$X = x + \sum_{p \in S} \left(\frac{t_p}{x - x_p} + \frac{u_p}{(x - x_p)^2} \right)$$

$$Y = y - \sum_{p \in S} \left(\frac{u_p (2y + a_1 x + a_3)}{(x - x_p)^3} + \frac{t_p (a_1(x - x_p) + y - y_p)}{(x - x_p)^2} + \frac{a_1 u_p - g_1 g_2}{(x - x_p)^2} \right)$$

où $g_1 = 3 x_p^2 + 2a_2 x_p + a_4 - a_1 y_p$

$g_2 = 6 - 2y_p - a_4 x_p - a_3$

$g(x,y) = x^3 + a_2 x^2 + a_4 x - y^2 - a_1 x y - a_3 y$;

$t_p = 2g_1 - a_1 g_2 = 6x^2_p + b_2 x_p + b_4$;

$u_p = 4x^3_p + b_2 x^2_p + 2 b_4 x_p + b_6$;

$S = F_2 \cup R$, ou $F_2 = \{$ points d'ordre 2 de E $\}$, R = partie de E (K) telle que $R \cap -R = \varnothing$ et $R \cup -R = E(K) - F_2$ ($-R = \{ -P ; P \in R \}$).

5- Réductions d'une courbe elliptique .

Pour obtenir des informations sur une courbe elliptique E sur un corps K , ″on réduit″ le corps K à un corps ″ local ″possédant un seul idéal premier ; alors les coefficients a_i et les variables x et y de la courbe E sont ″réduits″ modulo cet idéal premier ; c'est l'opération de réduction d'une courbe elliptique.

Les réductions d'une courbe elliptique E sur un corps K s'obtiennent avec les valuations de ce corps .

La théorie des valuations peut être consultée dans les ouvrages de théorie des nombres (Hasse , Weiss, Iyanaga , Artin ,…)

Nous en exposons les éléments dont nous avons bésoin .

5.1- Valuations archimédiennes et non archimédiennes

Valuation d'un corps

Définition 11:

Une valuation d'un corps K est une fonction réelle positive

$$\varphi : K \longrightarrow IR^{+}$$

qui satisfait les 3 propriétés :

(val1) $\varphi(a) = 0$ *équivaut à* $a = 0$ *et* $\varphi(a) \geq 0$ *pour tout élément a du corps K*

(val2) $\varphi(ab) = \varphi(a)\,\varphi(b)$ *pour tous les éléments a et b du corps K*

(val3) Il existe une constante réelle $c > 0$ *telle que :*

$\varphi(a) \leq 1$ *implique* $\varphi(1+a) \leq c$ *pour tout élément a de K*

Exemples :

1)Soit un corps K ; soit l' application $\varphi :$ K $\longrightarrow$ IR^{+} de valeurs

$\varphi(0)=0$ *et* $\varphi(a) = 1$ pour $a \neq 0$

Alors φ *est* la valuation triviale du corps K

2) Soit K = IR = corps des nombres réels et $\varphi(a) = \max\{a , -a\}$

Alors φ *est* la valeur absolue ordinaire des nombres réels .

Le 3ème axiome est satisfait pour c=2

3) Soit K = C = corps des nombres complexes et $\varphi(a)=(x^2 + y^2)^{1/2}$ pour $a = x + iy$

Le 3ème axiome est satisfait pour c=2

L'axiome (val2) implique qu'une valuation φ est un homomorphisme du groupe multiplicatif K^{*} dans le groupe multiplicatif des nombres réels positifs.

L'axiome (val3) de la définition peut être remplacé par l'inégalité triangulaire :

(val3′) $\varphi(a + b) \leq c \max\{\varphi(a), \varphi(b)\}$ *pour tous les éléments a et b du corps K*

Théorème 8:

Soit φ $K \longrightarrow R^{+}$, *une valuation d'un corps K*

Alors : φ *détermine sur ce corps K une topologie* T_{φ} *de HAUSDORFF*

Preuve : cf [14] E.Weiss : Algebraic number théory

ν

Un système de voisinages d'un élément a de K est l'ensemble :

$U(a,\varepsilon) = \{ b \in K ; \varphi(a - b) < \varepsilon\}$ pour une famille de nombres réels ε positifs

Dans l'ensemble V_K des valuations de K , on définit une relation d'équivalence par la :

Définition 12 :

Deux valuations φ_1 et φ_2 *d'un corps K sont équivalentes lorsqu'elles déterminent la même topologie sur le corps K*

Théorème 9:

Soit une valuation v_1 *d'un corps K .Alors , toute valuation* v_2 *équivalente à* v_1 *est de la forme* $v_2 = v_1^c$ *pour une constante* $c>0$.

v

Il en résulte la structure des classes d'équivalences dans l'ensemble V_K des valuations d'un corps K .

Diviseurs premiers d'un corps :

Les valuations équivalentes permettent de définir les diviseurs premiers d'un corps K

Définition 13 :

Chaque classe d'équivalence dans l'ensemble des valuations d'un corps K est un diviseur premier de K pour la valuation φ ,ce diviseur est différent d'un diviseur premier de K pour son arithmétique .

Dans l'ensemble V_K des valuations d'un corps K , on ne considère que les valuations non équivalentes qui sont des représentants des diviseurs premiers du corps K pour une valuation φ .

Dans l'ensemble V_K, les valuations sont réparties en 2 classes suivant la valeur du nombre c dans l'axiome (val 3).

Définition 14 :

Une valuation φ *d'un corps K est archimédienne si elle satisfait la relation :*

$\varphi(a) \leq 1$ *implique* $\varphi(a+1) \leq 2$.

Une valuation φ *d'un corps K est non archimédienne si elle satisfait la relation :*

$\varphi(a) \leq 1$ *implique* $\varphi(a+1) \leq 1$.

Exemples :

1) La valuation triviale sur un ensemble E est non archimédienne
2) Les valeurs absolues sur les corps IR et IC sont des valuations archimédiennes.

Théorème 10:

Soit une valuation non archimédienne φ d'un corps K .Alors elle satisfait les 2 propriétés :

1) $\varphi(a + b) \leq max \{\varphi(a), \varphi(b)\}$

2) L'ensemble $\{ \varphi(n.1) : n \in Z \}$ *est borné*

Preuve : cf [14] E.Weiss : Algebraic number théory

v

Chaque valuation non archimédienne φ d'un corps K détermine des sous ensembles dans ce corps K : anneau, idéal , groupe , corps résiduel de φ.

Définition 15 :

Soit une valuation non archimédienne φ d'un corps K

a) L'anneau de la valuation φ est l'ensemble :

$A_\varphi = \{ a \in K ; \varphi(a) \leq 1\}$ *=anneau des* φ*-entiers de K*

b) L'idéal maximal de φ est l'ensemble :

$M_\varphi = \{ a \in K ; \varphi(a) < 1\}$

c) Le groupe des unités de K est l'ensemble :

$U_\varphi = \{ a \in K ; \varphi(a) = 1\}$ *= groupe des* φ*-unités de K*

d) Le corps des classes résiduelles en φ du corps K est le corps quotient :

$k = A_\varphi / M_\varphi$

e) Une uniformisante de la valuation φ est un générateur π de l'idéal M_φ

Une valuation archimédienne ne possède pas ces sous ensembles .

Théorème 11:

1) Les seuls corps complets pour une valuation archimédienne sont le corps IR des nombres réels et le corps IC des nombres complexes.
2) Les corps de caractéristique $p > 0$ ne possèdent que des valuations non archimédiennes .

Preuve : cf Algebraic Numbers and algebraic functions « Artin » ; chap.I_v

Pour calculer les valuations de sommes d'éléments d'un corps et de polynômes d'un anneau de polynômes, on dispose de théorèmes d'approximation.

Théorème 12 :

Soit n valuations inéquivalentes $\varphi_1, \varphi_2, \ldots, \varphi_n$ d'un corps K . Alors il y a un élément a de K qui satisfait les inégalités :

$\varphi_1(a) > 1$ *et* $\varphi_t(a) < 1$ *pour* $t = 2,3,\ldots,n.$

v

Corollaire :

Soit n valuations φ_t d'un corps K et n éléments a_t de K .Alors :

A tout nombre réel $\varepsilon > 0$ correspond un élément a de K qui satisfait les inégalités :

$\varphi_t(a - a_t) < \varepsilon$ *pour* $t = 2,3,\ldots, n.$ v

Théorème 13:

Soit une valuation non archimédienne φ d'un corps K et n éléments $a_1, \ldots a_n$, qui satisfait la condition :

$\varphi(a_1) \geq \varphi(a_t)$ *pour* $t = 2,\ldots n$

Alors φ satisfait la relation :

$\varphi(a_1 + a_2 + \ldots + a_n) = \varphi(a_1)$

Preuve : avec les axiomes d'une valuation non archimédienne. v

5.2- Valuations non archimédiennes discrètes (VNAD)

Une valuation additive $\varphi : K \longrightarrow IR \cup \{\infty\}$ est discrète lorsque son groupe de valuation $\varphi(K^*)$ est discret dans le corps IR des nombres réels ; un anneau de valuation discrète est un anneau principal A qui possède un seul idéal premier ; il en résulte que tout élément a de l'anneau A est de la forme $a = \pi^r u$, où π est un générateur de l'idéal premier , r un entier naturel et u une unité .

Un anneau local est un anneau qui possède un unique idéal maximal.

Exemples de valuations non archimédiennes(VNAD) .

1) Valuation du corps Q des nombres rationnels

Tout nombre premier p donne la valuation p -adique :

$v_p : Q \longrightarrow IR^+$, de valeur

$v_p(p) = 1/p$ et $v_p(q) = 1$ pour tout nombre premier $q \neq p$

La valuation p-adique discrète : $v_p(p^r) = r$ et $v_p(q) = 0$ pour tout nombre premier $q \neq p$

2) Valuations d'un corps de nombres algébriques $K = Q(\theta)$

A tout idéal premier P_K du corps K est associée une valuation p-adique v_p de valeur $v_p(P_K) = 1/N(P_K)$, où $N(P_K)$ désigne la norme de l'idéal P_K.

5.3- V***aluations additives :***

L'axiome (2) des valuations d'un corps implique que ces valuations sont multiplicatives .

Toute valuation φ multiplicative non archimédienne donne une valuation additive

$\lambda : K \longrightarrow IR$ par l'application logarithme

Définition 16:

Soit une valuation non archimédienne $\varphi : K \longrightarrow IR^+$ multiplicative ;
La valuation additive associée est la valuation exponentielle
$\lambda : K \longrightarrow IR$ de valeur $\lambda(a) = - \log |\varphi(a)|$, où $|x|$ désigne la valeur absolue de x. Alors $\lambda(0) = +\infty$.

5.4 - Bonne et mauvaise réduction :

L'ensemble V_K des valuations non équivalentes d'un corps K est une partition $V_K = V_0 \cup V_\infty$, où V_0 est le sous ensemble des valuations non archimédiennes discrètes (VNAD) et V_∞ l'ensemble des valuations archimédiennes.

Les VNAD permettent de définir la notion d'équation minimale de Weierstrass et la notion de réduction modulo une VNAD d'une courbe elliptique.

Définition 17:

Soit une courbe elliptique E sur un corps K muni d'une VNAD φ :

$$E : \quad y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad , \qquad (1)$$

Cette équation (1) est minimale en φ si les coefficients a_i sont φ-entiers et si la valuation $\varphi(\Delta(E))$ du discriminant $\Delta(E)$ est minimale .

Il en résulte un critère de minimalité de l'équation de Weierstrass de E en φ ;ce critère est basé sur les coefficients a_i ,$c_4(E)$, $c_6(E)$et *sur l'invariant discriminant $\Delta(E)$*

(a) les cinq coefficients a_i sont φ-entiers et $\varphi(\Delta(E))<12$;

ou (b) les cinq coefficients a_i sont φ-entiers et $\varphi(c_4(E))<4$;

ou (c) les cinq coefficients a_i sont φ-entiers et $\varphi(c_6(E))<6$.

Définition 18 :

Une équation de Weierstrass minimale globale pour une courbe elliptique E sur K est une équation de Weierstrass

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

où les cinq coefficients a_i *sont* φ *- entiers et le discriminant* $\Delta(E)$ *minimal se factorise sous la forme :*

$$\Delta(E) = \prod_{\varphi \in V_K} p_v^{ord(\Delta_\varphi)}$$

Pour toute VNAD φ *du corps K , la réduction en* φ *est l'application :*

$\varphi : K \longrightarrow k$ *(*k =corps résiduel de φ*)*

avec $\varphi(a_i) = \tilde{a}_i$, φ(x) = x , φ(y) = y et k =corps résiduel de φ

La courbe réduite en φ a pour équation :

$\tilde{E}$: $y^2 + \tilde{a}_1 xy + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6$

Définitions 19:

1) La réduction en φ *est bonne si la courbe réduite* $\tilde{E}$ *est une courbe elliptique sur le corps résiduel k*

2) La réduction est multiplicative si $\tilde{E}$ *admet un nœud, elle est multiplicative décomposée si les équations des tangentes à* $\tilde{E}$ *au nœud sont à coefficients dans le corps résiduel k.*

3)La réduction est additive si $\tilde{E}$ *admet un point de rebroussement*

4)Une bonne réduction est une réduction stable.

5)Une réduction multiplicative est une réduction semi stable.

6)Une réduction additive est une réduction instable.

7)*Une mauvaise réduction est soit multiplicative , soit additive .*

Il existe des bonnes réductions qui sont potentielles

Définition 20 :

Soit une courbe elliptique E sur un corps K muni d'une valuation discrète φ *, E admet une bonne réduction potentielle modulo* φ *s'il existe une extension finie K′ de K telle que E admet une bonne réduction sur K′*

Thèorème 14:

Soit une courbe elliptique E sur un corps K muni d'une valuation discrète φ. *alors E admet une réduction potentielle si et seulement si son invariant modulaire j est dans l'anneau des entiers* A_φ .

Preuve : cf[28] proposition 5.4 page 181 ν

Les invariants $\Delta(E)$ et $c_4(E)$ permettent de déterminer la nature de la réduction en une VNAD φ.

Théorème 15:

Soit une courbe elliptique E sur un corps K , les invariants $\Delta(E)$ et $c_4(E)$ *de E et une VNAD* φ *de K .Alors :*

1)La réduction de E en φ *est bonne si et seulement si* $\varphi(\Delta(E)) = 0$;

2) La réduction est multiplicative si et seulement si $\varphi(\Delta(E)) > 0$ *et* $\varphi(c_4(E)) = 0$

3) *La réduction est additive si et seulement si* $\varphi(\Delta(E)) > 0$ *et* $\varphi(c_4(E)) > 0$

Preuve : cf [28] chap.VII proposition 5.1 ν

Les termes « multiplicative » et « additive » proviennent du :

Corollaire :

Soit les hypothèses du théorème ci-dessus . Alors :

1) Lorsque E a une réduction multiplicative en φ *, la partie non singulière* $\tilde{E}_0(k)$ *de la courbe réduite est un groupe multiplicatif isomorphe au sous groupe multiplicatif* k^x *du corps résiduel .*

2) Lorsque E a une réduction additive en φ *,* $\tilde{E}_0(k)$ *est un groupe additif isomorphe au sous groupe additif* k^+ *du corps résiduel .*

Preuve :

1) La définition de la réduction multiplicative de la courbe E en φ *implique l'invariant* $\Delta(E) = 0$ *et le coefficient* $c_4(E) \neq 0$ (1)

(1) implique la courbe reduite $\tilde{E}$ admet un nœud donc deux tangentes distinctes d'équations:

$$y = \alpha_1 x + \beta_1 \quad \text{et} \quad y = \alpha_2 x + \beta_2$$

L'application : $(x,y) \longrightarrow y - \alpha_1 x + \beta_1$

$$y - \alpha_2 x + \beta_2$$

est un isomorphisme du groupe $\tilde{E}_0(k)$ dans le groupe multiplicatif k^x

2)La réduction additive de la courbe E en φ *implique l'invariant* $\Delta(E) = 0$ *et le coefficient* $c_4(E) = 0$ donc la courbe reduite $\tilde{E}$ admet un point de rebroussement $P(x_r, y_r)$ donc deux tangentes confondues d'équation :

$$y = \alpha x + \beta$$

L'application : $(x,y) \longrightarrow \dfrac{y - x_r}{y - \alpha x + \beta}$

est un isomorphisme du groupe $\tilde{E}_0(k)$ dans le groupe additif k^+

v

Exemple : fig.3

Soit la Courbe elliptique E sur Q d'équation :

$y^2 = x^3 + 3x^2 + 1$; $a_1 = a_3 = 0$, $a_2 = 3$, $a_4 = 0$ et $a_6 = 1$

$b_2 = 2^2 . 3$, $b_4 = 0$, $b_6 = 2^2$ et $b_8 = 2^2 .3$

Les calculs donnent les valeurs des invariants : $\Delta(E) = -2^4 . 3^3 .5$ et $c_4(E) = 2^4 . 3^2$

On applique le théorème de réduction :

La courbe E a une bonne réduction en tout nombre premier p qui ne divise pas $\Delta(E)$ soit $p \neq 2, 3$ et 5 ;

Pour $p = 5$, la valuation p-adique φ *implique :*

$\varphi(\Delta(E)) > 0$ et $\varphi(c_4(E)) = 0$: réduction multiplicative en φ ;

Pour $p = 2,3$, la valuation p-adique φ *implique :*

$\varphi(\Delta(E)) > 0$ et $\varphi(c_4(E)) > 0$: réduction additive en φ.

Le point d'intersection P de la courbe avec l'axe 0x a pour abscisse :

$$x = -1/2(12 + 4\sqrt{5})^{1/3} - 2/(12 + 4\sqrt{3})^{1/3} - 1$$

Tableau des valeurs

X	-4	-3	-2	-1	0	1	2
y^2	-15	1	5	3	1	5	21
Y	/	± 1	$\pm\sqrt{5}$	$\pm\sqrt{3}$	± 1	$\pm\sqrt{5}$	$\pm\sqrt{21}$

Pour p =7 , la courbe E admet une bonne réduction modulo 7 donc la courbe réduite $\tilde{E}$ est une courbe non singulière admettant un nombre fini de points :

$$\tilde{E}(IF_7) = \{0_E, (0,1), (0,6), (4,6), (2,6), (4,6)\}$$

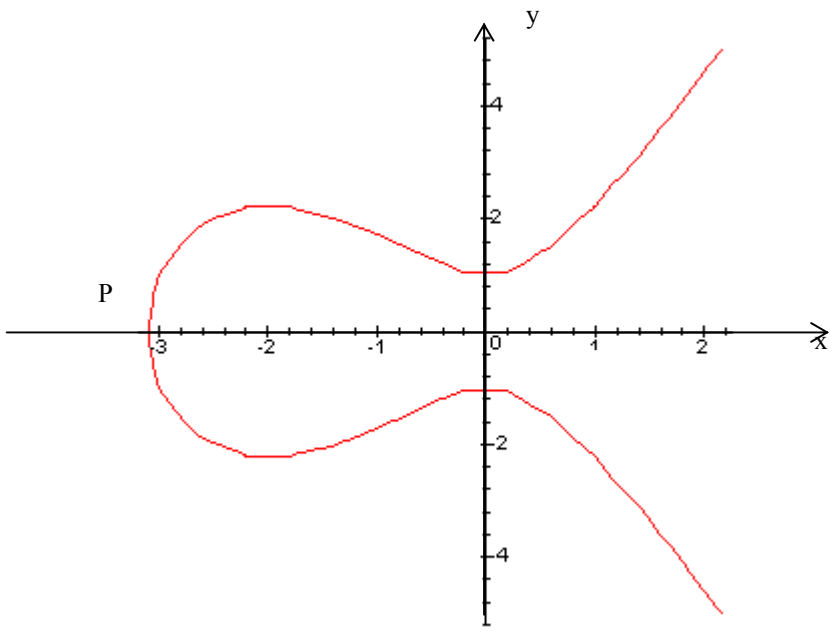


Figure 3

CHAPITRE III

POINTS D'ORDRE FINI SUR UNE COURBE ELLIPTIQUE

1- Sous groupe de torsion

Soit une courbe elliptique E , sur un corps K ; d'équation :

$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$; (1)

Son groupe de Mordell-Weil, E(K) , a une structure de groupe abélien de type fini et de rang $r(E) = r \geq 0$. (2)

Pour tout entier rationnel m , le groupe E(K) possède un sous groupe de m-torsion , E(K)[m].

Le groupe abélien E(K) contient un groupe de torsion T(E):

$$T(E) = \bigcup_{m \geq 0} E(K)[m]$$

Théorème1 :

Le groupe de Mordell-Weil E(K) d'une courbe elliptique E , sur un corps K , est isomorphe au produit de groupes :

$$E(K) \approx T(E) \oplus ZI^r$$

où ZI^r désigne r copies du groupe additif *ZI*

Preuve :

C'est le théorème de Mordell-Weil ; La preuve est divisée en 2 parties : une partie formée d'une descente infinie et une partie basée sur le groupe quotient E(K)/ mE(K). v

Cette structure rappelle la structure du groupe des unités d'un corps de nombres algébriques :

Théorème 2 (Théorème de Dirichlet) :

Soit un corps de nombres algébriques L , de degré n= s + 2t , avec s conjugués réels et 2t conjugués complexes . Alors l'ensemble U(L) des unités de L *est un groupe abélien isomorphe à un produit de groupes :*

$$U(L) \approx Z(L) \times ZI^r$$

où Z(L) est le groupe des racines de l'unité contenues dans L et r = s + t -1 est le rang de U(L). v

Il en résulte que le calcul du groupe Z(L) et du rang r = s + t -1 ne comporte aucune difficulté . Il n'en est pas de même du calcul du groupe T(E) de torsion de E et du rang r(E) = r d'une courbe elliptique .

2- Coordonnées des points mP pour m≥ 0

Dans le chapitre II page 32 , nous avons déterminé les coordonnées du symétrique - P d'un point P et les coordonnées de la somme $P_1 + P_2$ de 2 points avec la loi géométrique "trois points colinéaires de E ont une somme nulle " Les calculs donnent les résultats :

Le symétrique de P =(x,y) est le point - P de coordonnées ;

$$-P= -(x,y) = (x , - y - a_1 x - a_3) \qquad (1)$$

La somme $P_1 + P_2$, pour des points $P_i = (x_i ,y_i)$ et $P_1 \neq \pm P_2$ est le point

$P_1 + P_2 = M =(x_M ,y_M)$ de coordonnées

$x_M = t^2 + a_1 t - a_2 - x_1 - x_2$;

et $y_M = -t^3 - 2a_1 t^2 + (a_2 - a^2_1 + 2x_1 + x_2) t + a_1 a_2 - a_3 + a_2 (x_1 + x_2) - y_1$; (2)

$$t = \frac{y_1 - y_2}{x_1 - x_2}$$

La somme P + P = 2P est le point M = 2P = (x_M ,y_M) de coordonnées

$$x_M = y'^2_P + a_1 y'_P - a_2 - 2x_P ;$$

$$y_M = -y'^3_P - 2a_1 y'^2_P + (a_2 - a_1^2 + 3x_P) y'_P + a_1 a_2 - a_3 + 2a_1 x_p - y_P \qquad (3)$$

où $y' = (3x^2 + 2a_2 x + a_4 - a_1 y) \,/\, (2y + a_1 x + a_3)$

Les coordonnées d'un point mP , pour m≥ 3 peuvent être obtenues par le:

T***héorème 3 :***

Soit une courbe elliptique E d'équation :

E : $y^2 = x^3 + ax + b$ *avec* $4a^3 + 27b^2 \neq 0$

Pour tout entier m≥ 3 , les coordonnées d'un point mP sont de la forme :

$$mP = \left(\frac{A_m}{D_m^2} , \frac{B_m}{D_m^3} \right) \qquad (4)$$

où les numérateurs et les dénominateurs satisfont les relations :

$D_{-1}= - 1; D_0=0; D_1=1; D_2= 2y , D_3= 3x^4 + 6 a x^2 + 12bx - a^2$ et

$D_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5 a^2 x^2 - 4abx - 8b^2 - a^3)$;

et les formules de récurrences :

$$D_{2m}=D_m\,(D_{m+2}D_{m-1}-D^2_{m-2}\,D^2_{m+1})$$
$$D_{2m+1}=D_{m+2}\,D_{m+2}D^3_m-D_{m-1}\,D^3_{m+1}) \qquad (5)$$
$$A_m=x\,D^2_m-D_{m-1}\,D_{m+1}$$
$$4y\,B_m=D_{m+2}D^2_{m-1}-D_{m-2}\,D^2_{m+1}$$

Preuve:

On utilise une récurrence sur m.

Ce résultat se trouve dans cf [19] sous la forme d'un lemme page 214. ν

Par définition , un point P d'ordre m satisfait la relation :

$$mP = (\infty,\infty) \qquad (6)$$

Il en résulte la condition $D_m=0$; donc , théoriquement , le théorème précédent et (6) , permettent de déterminer les points de m-torsion en résolvant l'équation $D_m=0$ dans le corps de base K de E .

Dans le corps Q des nombres rationnels , $D_m=0$ est une équation diophantienne ; c'est pourquoi on commence par le groupe de torsion T(E) sur le corps Q.

Théorème4:

Soit une courbe elliptique E sur un corps de caractéristique nulle , avec un corps résiduel k de caractéristique $p > 0$, associé à une valuation φ de K et une uniformisante π de φ . Soit un point P de E(K) d'ordre $m \geq 2$.

1) Lorsque m n'est pas une puissance d'un nombre premier p , les coordonnées x et y de P sont φ-entiers .

2) Lorsque $m = p^t$, les coordonnées x et y satisfont :

$$\pi^{2r}x \text{ et } \pi^{3r}y \text{ sont } \varphi\text{-entiers et } r = \frac{\varphi(p)}{p^t - p^{t-1}} \text{ est la partie entière}$$

Preuve : cf[28] Théorème 3.4 ν

3 - Groupe de torsion $T_Q(E)$:

La structure de ce groupe a été conjecturé par OGG puis démontrée par Mazur.

Théorème 5:

Le groupe de torsion $T_Q(E)$ d'une courbe elliptique E sur le corps Q des nombres rationnels est isomorphe à l'un des 15 groupes abéliens suivants :

ZI / nZI *pour* $1 \leq n \leq 10$ *et* $n = 12$

$ZI / 2ZI \oplus ZI/2dZI$ *pour* $d = 1,2,3,4$

Preuve:

Dans "Invent.math 22 .44-49 Springer Verlag 1973", B.Mazur et J.Tate ont montré qu'il n'existe pas de courbes elliptiques sur Q de point de torsion d'ordre 13 .

Dans "C.R Acad SC.Paris , t.274 (1972): a été montré qu'il n'existe pas de courbes elliptiques sur Q de point de torsion d'ordre 15.

Selon [26] il faut montrer qu'il n'existe pas de courbes elliptiques E sur Q de point d'ordre $N = 11$ et $N \geq 17$.

Pour y parvenir , on suppose qu'il existe un point d'ordre $N=11$ et $N \geq 17$, il faut utiliser la bonne réduction potentielle en $p = 3$, la structure de variété abélienne de E , les fibres de Néron sur IF_3, les tables de Tate des algorithmes de calcul des fibres singulières de Pinceaux de courbes elliptiques .

Alors on obtient une contradiction .

ν

L'ordre du groupe de torsion d'une courbe elliptique sur le corps des nombres rationnels Q est au plus égal à 16.

4- Groupes de torsion $T_K(E)$ sur un corps de nombres algébriques K

Plusieurs travaux ont été menés pour déterminer les groupes de torsion $T_K(E)$ sur un corps de nombres K de degré 2,3,4 .

Citons Kamieny , Kenku , Momose , pour les courbes elliptiques sur un corps quadratique, Müller ,Ströher , Williams et Zimmer pour les courbes elliptiques sur un corps cubique pure , Kishi pour des courbes elliptiques sur un corps quartique cyclique imaginaire .

La contribution de Kubert [25]est importante pour l'étude de groupes de torsion T(E) sur un corps K de degré ≥ 2 .

Selon Kubert , le corps E(p) des points de p-division d'une courbe elliptique E sur un corps K est un $G_{Kalg/K}$ - module . L'image G_p du groupe $G_{Kalg/K}$ dans le

groupe linéaire GL(2, ZI / p ZI) ≈ Aut (E(p)) agit de façon naturelle sur les sous groupes cycliques du corps E(p).

Théorème 6:

Soit 3 points P_1 , P_2 et P_3 de coordonnées $P_i = (x_i , y_i)$ de p- torsion d'une courbe elliptique E sur un corps de nombres K d'invariant modulaire j(E) et une valuation discrète φ sur le corps K..

Soit l'élément $$u = \frac{x_1 - x_3}{x_1 - x_2}$$

Alors , si φ(j) ≥ 0 , φ(u)= φ(1-u)=0

Preuve : Kubert [25]. ν

Corollaire :

Soit les hypothèses du théorème précédent ;

Si φ(j)< 0 alors φ(u) = r/p et φ(1-u)= s/p pour certains r et s dans ZI. ν

Théorème 7:

Le groupe de torsion $T_K(E)$ d'une courbe elliptique E sur un corps K de degré n≥2 est fini.

Preuve:

Le groupe de torsion $T_K(E)$ est un sous groupe d'un groupe de type fini E(K), donc $T_K(E)$ est de type fini, la théorie des groupes de torsion implique que tout groupe de torsion de type fini est fini. ν

Théorème 8:

Soit une courbe elliptique E , sur un corps K , quadratique imaginaire , de groupe de torsion $T_K(E)$.

1) Pour p =2,3,5, il existe une constante C(p) satisfaisant :

il existe un point P de E de p^l -torsion , pour $l < C(p)$.

2) Tout point de $T_K(E)$ est d'ordre < C(p)

Preuve: Dans Kubert [26] ν

Dans [23] , sont déterminés les groupes de torsion $T_L(E)$ de courbes elliptiques sur un corps L , quartique , cyclique , imaginaire . Des renseignements sont obtenus

sur le groupe $T_L(E)$ avec des réductions modulo un nombre p premier , le degré résiduel f_p et l'indice de ramification e_p d 'un idéal 1^{er} P au dessus de p dans l'extension L du corps *Q*.

Théorème 9:

Soit un corps de nombres L , quartique , cyclique , imaginaire et une courbe elliptique E sur L . Soit le groupe de torsion $T_L(E)$ et une valuation additive normalisée φ_p en 2, 3 . On suppose que E n'a pas de réduction multiplicative mod p et $f_2 < 4$ ou $f_3 < 4$.

Alors l'ordre du groupe $T_L(E)$ est un diviseur de l'un des entiers 11,13,21,30,56,80 et 576.

Preuve: Dans Kishi [23] ν

Dans [23] , l'auteur détermine des groupes de torsion d'ordres égaux à chaque entier de la liste ci-dessus.

Corollaire:

Soit les hypothéses du théorème n° 9 .

Alors le groupe de torsion $T_L(E)$ est isomorphe à l'un des 10 groupes abéliens suivants :

ZI / 11ZI ;, ZI / 13ZI ; ZI / 3ZI ⊕ ZI / 7ZI ; ZI / 5ZI ⊕ ZI / 6ZI;, ZI / 8ZI ⊕ ZI / 7ZI;
ZI / 12ZI ⊕ ZI / 4ZI ⊕ ZI / 7ZI; ZI / 5ZI ⊕ ZI / 16ZI ; ZI / 2ZI ⊕ ZI / 5ZI ⊕ ZI / 8ZI
ZI / 9ZI ⊕ ZI / 64ZI ;ZI / 2ZI ⊕ ZI / 9ZI ⊕ ZI / 32ZI.

Preuve: Dans Kishi [23] ν

Le groupe de torsion $T_K(E)$ d'une courbe elliptique E sur un corps de nombres K peut être étudié sur un corps local K_φ *muni d'une valuation φ ,d'un corps* résiduel k , d'une uniformisante π .La valuation φ opère sur le groupe E(K) de Mordell-Weil par réduction .

Théorème 10 :

Soit une courbe elliptique E sur un corps local K , la courbe réduite $\tilde{E}$ *modulo la valuation* φ *de K , le corps résiduel k .Soit un entier m premier à la caractéristique de k et le groupe de m-torsion E(K)[m] .*

Alors si la courbe réduite $\tilde{E}(k)$ est non singuliére , l'application :

$$E(K)[m] \longrightarrow \tilde{E}(k)$$

est injective .

Preuve:

Les sous groupes $E_0(K) = \{ P \in E(K) ; P \text{ non singulier} \}$ et $E_1(K) = \{ P \in E(K) ; P = \tilde{o} \}$

Forment une suite exacte :

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow \tilde{E}_{ns}(k) \longrightarrow 0$$

lorsque la courbe réduite $\tilde{E}$ n'est pas singulière , il en résulte les égalités :

$$E_0(K) = E(K) \text{ et } \tilde{E}_{ns}(k) = \tilde{E}(k)$$

v

5 - Courbes elliptiques sur un corps cyclique de degré 5

Pour déterminer une valuation d'un corps K , cyclique , de degré 5 , il faut connaître la décomposition d'un nombre rationnel premier p dans l'extension K du corps *Q*.

Théorème 11 :

Soit une extension séparable N =M(θ*) sur un corps M de degré n, d'élément primitif* θ entier , de polynôme minimal $f_\theta(x) = f(x)$. Si la famille de puissances $\{ 1, \theta, \ldots \theta^{n-1} \}$ *est une base d'entiers de N sur M , alors f(x) se factorise modulo un nombre* 1^{er} *p sous la forme :*

$$f(x) \equiv f_1(x)^{e_1} . f_2(x)^{e_2} \ldots f_g(x)^{e_g} \quad \text{modulo } p$$

où les $f_i(x)$ *sont des polynômes irréductibles modulo p et de degré* h_i .

Alors l'idéal pN se factorise sous la forme :

$$pN = \prod_{1 \le i \le g} \mathfrak{p}_i^{e_i}$$

où les p_i sont des idéaux 1^{er} du corps N , de degré h_i engendrés par le nombre premier p et le nombre $f_i(\theta)$.

Preuve : Théorème de Dedekind ν

Dans la suite nous traitons 2 exemples :

Exemple 1:

Le polynôme $f(x) = x^5 - x^3 - x^2 + x + 1$ est cyclique de degré 5 . Il admet 5 racines irrationnelles $\theta = \theta_1, \theta_2, \theta_3, \theta_4$, et θ_5 , permutables par un groupe cyclique d'ordre 5.

Ces cinq nombres θ engendrent un corps cyclique $K = Q(\theta)$ de degré 5.

Par ordinateur nous avons obtenu des valeurs approchées :

$\theta = \theta_1 = - 0,69287163,$
$\theta_2 = -0,6993110190 - 0,8112684045\ i$, $\theta_3 = -0,6993110190 + 0,8112684045\ i$;
$\theta_4 = 1,045746834 - 0,4055878029\ i$; $\theta_5 = \theta_4 = 1,045746834 + 0,4055878029\ i$

Factorisons le polynôme $f(x)$ modulo un nombre premier p.

Pour $p = 2$, la réduction modulo 2 donne :

$$f(x) \equiv g(x) \mod 2;\ g(x) = x^5 + x^3 + x^2 + x + 1$$

les 2 relations :

$$g(0) \equiv 1 \mod 2 \text{ et } g(1) \equiv 1 \mod 2 \qquad (1)$$

impliquent que $g(x)$ n'a pas de facteurs linéaire mod 2.

Cherchons un facteur de degré 2 :

$$g(x) = x^5 + x^3 + x^2 + x + 1 \equiv (x^2 + ax + b)(x^3 + cx^2 + dx + e) \mod 2 \qquad (2)$$

(2) implique les 5 congruences :

$$a + c \equiv 0 \mod 2\ ;\ d + ac + b \equiv 1 \mod 2\ ;\ e + ad + bc \equiv 1 \mod 2$$

$$ae + bd \equiv 1 \mod 2\ ;\ be \equiv 1 \mod 2 \qquad (3)$$

le système (3) n'a pas de solution modulo 2 (4)

Il en résulte que le polynôme $g(x)$ est irréductible .

Par le théorème de Dédekind , $p = 2$ engendre dans le corps $K = Q(\theta)$ un idéal :

$$2K = \mathfrak{p}_2 \qquad (5)$$

où $\mathfrak{p}_2$ est un idéal premier de norme $N(\mathfrak{p}_2) = 2^5$; donc $\mathfrak{p}_2$ est de degré 5.

Considérons la courbe elliptique E , définie sur le corps $K = Q(\theta)$ de degré 5

$E : y^2 = x^3 + x^2 - \theta x$ (6)

L'équation de Weierstrass de la courbe E a pour coefficients :

$a_1 = a_3 = a_6 = 0$; $a_2 = 1$, $a_4 = -\theta$. (7)

Calculons les invariants de la courbe elliptique :

$b_2 = 4$; $b_4 = -2\theta$; $b_6 = 0$ et $b_8 = -\theta^2$, $c_4(E) = 16(1 + 3\theta)$ (8)

Le discriminant est égal à :

$$\Delta(E) = 16\,\theta^2 (4\theta + 1) \quad (9)$$

L'invariant modulaire est égal à :

$$j(E) = 256\,\frac{(1 + 3\theta)^3}{(1 + 4\theta)} \quad (10)$$

Dans le groupe de Mordell Weil E(K) de la courbe E , un point de 2 -torsion a pour coordonnées les solutions du système des 2 équations :

$y^2 = x^3 + x^2 - \theta x$ et $y = 0$ (11)

l'équation $x^3 + x^2 - \theta x = 0$ admet 3 solutions :

$x = 0$, $x = -1/2\ (1 \pm \sqrt{1 + 4\theta^2})$ (12)

Le nombre $\sqrt{1 + 4\theta^2}$ n'est pas rationnel sur le corps $K = Q(\theta)$.

Il en résulte un seul point de 2-torsion :

(0,0) dans E(K). (13)

Exemple 2:

Soit le polynôme $f(x) = x^5 - 10x^3 - 5x^2 + 10x - 1$. (1)

obtenu par l'algorithme de Payan .

C'est donc un polynôme cyclique de degré 5 qui admet 5 racines irrationnelles $\theta = \theta_1, \theta_2, \theta_3, \theta_4$, et θ_5 , permutables par un groupe cyclique d'ordre 5:

$$\sigma(\theta_u) = \theta_{u+1} \quad \text{avec } u \text{ et } u + 1 \bmod 5 \quad (2)$$

Le corps de décomposition de ce polynôme est l'extension :

$$Q(\theta_1) = Q(\theta_2) = \ldots = Q(\theta_5) = L \quad (3)$$

Des valeurs approchées sont obtenues par ordinateur :

$\theta = \theta_1 = -2{,}52959008$, $\theta_2 = -1{,}56240369$, $\theta_3 = 0{,}10693961$, $\theta_4 = 0{,}72597754$, $\theta_5 = 3{,}25907738$.

La réduction modulo 2 de f(x) modulo p donne le polynôme g(x) :

$f(x) \equiv g(x) = x^5 + x^2 + 1 \mod 2$ (4)

Les valeurs $g(0) = g(1) = 1$ impliquent que le polynôme $g(x)$ est irréductible mod 2 (5)

Par le théorème de Dedekind, le nombre premier $p = 2$ engendre un idéal 1^{er} de degré 5:

$$2L = \mathfrak{p}_2 \text{ , idéal } 1^{er} \text{ de L de norme } N\mathfrak{p}_2 = 2^5 \text{ ,} \qquad (6)$$

La réduction modulo 5 de f(x) donne le polynôme g(x) :

$$f(x) \equiv g(x) = x^5 + 4 \mod 5 \qquad (7)$$

Les valeurs $g(1) = 5$; $g(2) = 1$, $g(3) = 2$, $g(-1) = 3$ mod 5 implique le facteur linéaire : $x - 1 = x + 4$:

$$g(x) \equiv (x+4)(x^4 + ax^3 + bx^2 + cx + d) \equiv (x+4)\, g(x) \mod 5 \qquad (8)$$

Les calculs donnent le facteur g_0 de g

$$g_0(x) = x^4 + x^3 + x^2 + x + 1 \qquad (9)$$

La valeur $g_0(1) = 5$ implique la factorisation :

$$g_0(1) = (x+4)(x^3 + 2x^2 + 3x + 4) \qquad (10)$$

Dans la formule (10) le polynôme $x^3 + 2x^2 + 3x + 4$ se factorise sous la forme

$$x^3 + 2x^2 + 3x + 4 \equiv (x+4)(x^2 + 3x + 1) \qquad (11)$$

$$\equiv (x+4)^3 \qquad (12)$$

Les formules (8), (10) et (12) impliquent la factorisation :

$$f(x) \equiv g(x) \equiv (x+4)^5 \mod 5 \qquad (13)$$

Par le théorème de Dedekind, le nombre premier 5 engendre dans l'extension L un idéal :

$$5\,L = \mathfrak{p}_5^5 \qquad (14)$$

puissance $5^{ème}$ d'un idéal 1^{re} $\mathfrak{p}_5$ de degré 1 engendré par 5 et $\theta + 4$

Considérons la courbe elliptique E sur ce corps cyclique L :

$$E : y^2 = x^3 + \theta x + 1 \qquad (15)$$

Les coefficients a_1 de l'équation de Weierstrass de E sont égaux à :

$$a_1 = a_3 = a_2 = 0 \; ; \quad a_4 = \theta \text{ et } a_6 = 1 \qquad (16)$$

Il en résulte les coefficients b_{2i} et c_4

$$b_2 = 0 \; ; \; b_4 = 2\theta \; ; \; b_6 = 4 \text{ et } b_8 = \theta^2 \text{ et } c_4 = -48\,\theta \qquad (17)$$

Le discriminant de la courbe E est égal à :

$$\Delta(E) = -16\,(4\theta^3 + 27) \qquad (18)$$

L'invariant modulaire de E est égal à :

$$j(E) = 6912 \quad \frac{\theta^3}{(4\theta^3 + 27)} \qquad (19)$$

Pour appliquer le théorème 9, on prend la valuation 5-adique sur le corps L , associée à l'idéal 1er $\mathfrak{p}_5$ de l'anneau A_L.

La courbe elliptique réduite modulo $\mathfrak{p}_5$ a pour équation :

$\tilde{E}$: $y^2 = x^3 + \theta x + 1$ (20)

Pour tout entier m 1er à 5 , le théorème 9 implique l'injection :

$$E(L)[m] \longrightarrow \tilde{E}[IF_5(4 + \theta)] \qquad (21)$$

Par le calcul on trouve un point P de coordonnées :

$P = ((4 + \theta)^2 = x , y = \theta^3 + 4\theta^2 + 4\theta + 4)$.

Plus particulièrement , les points P d'ordre m de la courbe elliptique E satisfont les équations :

Pour m =2:

$y^2 = x^3 + \theta x + 1$ et $y = 0$; soit $x^3 + \theta x + 1 = 0$. (22)

Pour m =3 :

$y^2 = x^3 + \theta x + 1$ et $3x^4 + 6\theta x^2 + 12x - \theta^2 = 0$ (23)

Pour m =4

$y^2 = x^3 + \theta x + 1$ et $y(x^6 + 5x^4\theta + 20x^3 - 5x^2\theta^2 - 4x\theta - \theta^3 - 8) = 0$ (24)

Ces trois systèmes peuvent être résolus par des méthodes d'ordinateur .

REFERENCES SUR LES CORPS DE NOMBRES

[1] Albert Châtelet : Arithmétique des corps cubiques , Annales de l'ENS (1946)

[2] Rachid Bouchenna : Arithmétique des corps abéliens de degré 7 , Thèse de Magister , Alger (1987).

[3] Claude Chevalley : Sur la théorie du corps de classes dans les corps finis et les corps locaux , thèse d'état , Paris (1933).

[4] H.Cohn : Invitation to algebraic numbers and class fields with appendices by Olga Tansskey , Springer Verlag (1978).

[5] H. Hasse : Number théory , Springer Verlag (1980).

[6] S . Iyanaga : the théory of numbers , North Holland Pub . comp. (1975).

[7] S.Iyanaga et T. Tamagawa : la théorie du corps de classes sur le corps Q des nombres rationnels , journal math.Soc Japan 3 (1951) p.220-227.

[8] Serge Lang : Cyclotomic Fiels I et II , GTM.59 et 69

[9] Serge Lang : Algebraic Number Théory

[10] Jacques Martinet : discriminants and permutation groups , monographie , Bordeaux (1986).

[11] Masley and Montgoméry : Cyclotomic fields with unique factorisation , jour. Reine Angew., band 286/287 (1976) p 248-256.

[12] Jean Jacques Payan : contribution à l'étude des corps abéliens de degré premier, thèse d'état , Annales Institut Fourier , Grenoble (1965) , p :133-199.

[13] I.Borevitch et R.Shafarevitch : Théorie des nombres , Gauthier Villard (1967)

[14] L.C Washington : Introduction to cyclotomic fields GTM 83 ; Springer Verlag (1982).

[15] Edvin Weiss : Algebraic number théory , Mc Graww – Hill Book company , inc , New-York.

[16] Hans J.Zassenhauss : the théory of groups , Chelsea Publishing company , New-York (1956)

[17] Mohamed ZITOUNI :Arithmétique des extensions cycliques de degré 4 du corps des rationnels , Thèse d'état Besançon (1972).

REFERENCES SUR LES COURBES ELLIPTIQUES

[18] B.J.Birch and H.P.F Swinnerton -Dyer ; Notes on Elliptic Curves , I Jour.Reine Angew .Math 212(1963)p :7-25.

[19]J.W.Cassels : Diophantine Equations With spécial références to Elliptic curves, the J.London Math .Soc41 (1965/66) p : 193-261.

[20] J.E.Cremona : Algorithms for modular Elliptic curves Combridge University (1997).

[21]R.Hartshorne : Algebraic géometry , Springer Verlag (1977)

[22] M.A Kenku :Certain torsion points on elliptic curves defined over quadratic fields , J.London Math .Soc19 (1979) p : 233-240.

[23] T.Kishi : On torsion subgroups of elliptic curves with integral J- invariant over imaginary quartic cyclique fields ,Tokyo Math 20 (1997) p : 315-327

[24]N.Koblitz : Introduction to Elliptic curves and modular forms GTM 97(1984).

[25] D.Kubert : Universal Bounds on the torsion of elliptic curves Pro.London Math .So33 (1976) p : 193-237.

[26]B.Mazur : Rationnel isogénie of prime degré Inv. Math 44 (1978) p : 129-162.

[27]Goro Shimura : Introduction to the arithmetic théory of automorphic functions , the Math .Soc of Japan n°11 (1971).

[28] J.H.Silverman : the arithmetic of elliptic curves .GTM 106 , Spring .Verlag (1986)

[29] J.H.Silverman : Advanced topics in the elliptic curves .GTM 151 , S.V (1994).

[30]John Tate : The arithmetic of elliptic curves, Inv .Math 23(1974) p179-206.

[31] G.Fung , H.Ströner , H Williams et G.Zimmer : Torsion groups of elliptics curves with integral J- Invariant over pure cubic fields J.of number theory 36(1990)p.12-45

[32]Modéle minimaux des varietés abeliennes sur les corps locaux et les corps globaux Publi. IHES 21 (1964).