UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENE

Faculté des Sciences Mathématiques
Département d'Algèbre Et Théorie des Nombres

Thèse

Présentée pour obtenir le diplôme de
Docteur d'ETAT EN MATHEMATIQUES

par
Aïni Laoudi

Unités de corps de nombres, valeurs de fonctions algèbriques

Soutenue le 17 octobre à l'USTHB devant le jury composé de :

Président	Benali Benzaghou	Professeur, USTHB
Directrice de thèse	Odile Lecacheux	Maître de Conférences, Paris VI
Co-directeur	Kamel Betina	Professeur, USTHB
Examinateur	Abdelouahab Arouche	Maître de Conférences , USTHB
Examinateur	Abdallah Derbal	Maître de Conférences , ENS
Examinateur	Arezki Kessi	Professeur, USTHB
Examinateur	Alain Salinier	Maître de Conférences, U. Limoges

Remerciements

Je tiens à exprimer mes vifs remerciements à ma directrice de thèse Odile Lecacheux, pour m'avoir proposé ce sujet de thèse, pour son suivi continuel et pour ces conseils.
Je tiens à remercier mon co-directeur le professeur Kamel Betina pour sa disponibilité et son aide.
Je remercie le professeur Benali Benzaghou pour l'honneur qu'il me fait en présidant le jury de cette thèse.
Je remercie Alain Salinier, Maître de Conférences à l'université de Limoges, d'avoir bien voulu faire partie du jury.
Je remercie Arezki Kessi, professeur à l'USTHB, ainsi que Abdallah Derbal et Abdelouahab Arouche, respectivement Maître de Conférences à l'ENS et à l'USTHB, pour avoir accepté de faire partie du jury.
Je tiens à remercier l'équipe de théorie des nombres de Paris VI de m'avoir accueilli dans leur équipe où j'ai bénéficié de bonnes conditions de travail pour préparer cette thèse, grâce à une bourse Algéro-Française .
Je remercie Gilles Godefroy, directeur de l'institut de Mathématiques de Jussieu, pour sa diponibilité et ses conseils.
Je souhaite remercier tous les thésard pour leur soutien et la bonne ambiance sur le plateau 7C : Aïcha, cécile, fabien, françois, kenly, miguel, mostafa, olivier, saïda, titem.
C'est en lisant un brouillon de la thèse de François Brunault[**?**] que j'ai eu l'idée de certaines démonstrations dans les formules du calcul du régulateur. Je tiens à le remercier. Je remercie tonton Damou, Zola et sa famille pour leur soutien et leur disponibilité durant mon séjour à Paris.
Pour finir, je remercie mes parents, mes frères et ma soeur qui ont toujours été présents à mes côtés.

Table des matières

Remerciements **2**

1 Rappels. **9**
1.1 Courbes elliptiques 9
1.2 Courbes modulaires. 11
1.2.1 Sous-groupe de congruence. 11
1.2.2 Les courbes modulaires $X_1(N)$ et $X_0(N)$. 12
1.2.3 Calcul des pointes des courbes $X_0(N)$ et $X_1(N)$. 13
1.2.4 Action du groupe de Galois sur les pointes. 13
1.2.5 Revêtements modulaires et involutions. 14
1.3 Formes modulaires 15
1.3.1 Formes modulaires pour $SL_2(\mathbb{Z})$. 15
1.3.2 Formes modulaires pour les sous-groupes de congruence. 16
1.3.3 Exemples d'unités modulaires. 16

2 Surfaces elliptiques modulaires et corps cubiques cycliques. **18**
2.1 Surfaces elliptiques modulaires associées au groupe de congruence $\Gamma_0(9) \cap \Gamma_1(3)$. 20
2.1.1 Expression de a et α comme fonctions modulaires 21
2.2 Polynômes de Type Shanks 23
2.3 Surface elliptique modulaire associée au groupe $\Gamma_0(18) \cap \Gamma_1(6)$ et involution w_2 27
2.4 Unités modulaires. 28
2.5 Corps encore plus simples 31
2.6 Spécialisations. 31
2.6.1 Monogénéité 32
2.7 Formule analytique pour le régulateur. 34
2.7.1 Calcul de $\log|m|$. 34
2.7.2 Calcul du régulateur. 35
2.8 Calcul d'un équivalent du régulateur. 36
2.9 Involutions d'Atkin-Lehner. 38

2.9.1 Différentes courbes elliptiques 40

3 Arithmétique d'une famille de corps cubiques 41
3.1 Généralités et résultats 41
3.2 Ordre maximal d'une famille de corps cubiques. 44
3.3 Décomposition des nombres premiers facteurs de $n-1$ et du nombre premier 2. 49
3.4 Unités de K 51

4 Courbes elliptiques associés a une famille de corps cubiques 55
4.1 Famille de courbes elliptiques. 55
4.1.1 Réduction modulo p. 55
4.2 Homomorphismes liés à la famille de courbes elliptiques E_n . . . 60
4.2.1 Cas local 62
4.2.2 Caractérisation de $\mathrm{Im}\lambda_p$. 63

5 2-Rang du groupe des classes et rang de courbes elliptiques. 71
5.1 Groupe de classes au sens ordinaire (resp. au sens restreint). . . 73
5.2 Le 2-groupe de Selmer 75
5.3 Borne supérieure de Billing pour le rang d'une courbe elliptique. 77
5.4 Résultat de Washington. 81
5.5 Sous-groupe du 2-groupe de Selmer et 2-rang du groupe de classes 84
5.6 Exemples. 87
5.6.1 Construction d'exemples. 87
5.6.2 Exemples. 89

Bibliographie 94

Introduction

Dans l'étude des corps de nombres l'une des premières étapes est de déterminer le groupe des unités. Si le théorème de Dirichlet donne la structure de ce groupe, il reste toujours à le déterminer explicitement. Dans le cas des extensions quadratiques réelles, le problème est entièrement explicité par l'algorithmique des fractions continues. Même dans ce cas, un corps de petit discriminant peut avoir une unité fondamentale surprenante : citons l'exemple de $\mathbb{Q}(\sqrt{94})$ qui a une unité fondamentale égale à $-2143295+221064\sqrt{94}$. Il est donc intéressant d'avoir des familles de corps de nombres dépendant d'un paramétre dont il est facile de déterminer un sous-groupe d'unités d'indice fini.
Dans cette thèse nous nous intéresserons aux extensions cubiques cycliques K_n engendrées par une racine θ du polynôme

$$P_n(X) = X^3 - (n^3 - 2n^2 + 3n - 3)X^2 - n^2X - 1,$$

où $n \in \mathbb{Z}$.
• Dans la première partie de cette thèse, nous expliquerons l'origine de cette famille et étudierons quelques propriétés arithmétiques de cette famille de corps. Cette partie comporte trois chapitres :

1. Le premier chapitre est essentiellement un chapitre de rappels sur les courbes modulaires et les courbes elliptiques.
2. Le deuxième chapitre explicite la construction de 2 familles de corps cubiques cycliques à partir des surfaces elliptiques modulaires associées aux groupes de congruences $\Gamma_0(9) \cap \Gamma_1(3)$ et $\Gamma_0(18) \cap \Gamma_1(6)$.

   Le principe de cette construction modulaire est le suivant : à partir d'un revêtement de courbes modulaires $X_1(N) \longrightarrow X_0(N)$, lorsque la courbe de base est de genre 0, on construit par spécialisation d'un générateur n du corps des fonctions de la courbe $X_0(N)$, avec $n \in \mathbb{Z}$, une famille de corps de nombres engendrés par des unités, spécialisations d'unités modulaires de $X_1(N)$. Le revêtement étant cyclique, on peut dans certains cas trouver un sous groupe d'indice fini d'unités de ces corps de nombres. Le théorème de Manin-Drinfield se traduit par une propriété

sur le régulateur de ces unités que nous allons expliciter pour $N = 18$. La courbe $X_1(18)$ de genre 2, est la compactification de $Y_1(18)$, obtenue en ajoutant les 16 pointes qu'on peut représenter par les couples suivants :

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 7 \end{pmatrix}, \begin{pmatrix} 0 \\ 5 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \end{pmatrix}, \begin{pmatrix} 1 \\ 8 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 6 \end{pmatrix},$$
$$\begin{pmatrix} 5 \\ 6 \end{pmatrix}, \begin{pmatrix} 1 \\ 9 \end{pmatrix}, \begin{pmatrix} 4 \\ 9 \end{pmatrix}, \begin{pmatrix} 2 \\ 9 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 5 \\ 0 \end{pmatrix}, \begin{pmatrix} 7 \\ 0 \end{pmatrix}.$$

Les six premières pointes seront respectivement notées P_1, P_2, P_3, Q_1, Q_2, Q_3. L'action du groupe de Galois sur ces pointes, qu'on explicitera dans le paragraphe 1.2.4 du premier chapitre, montre qu'elles sont rationnelles. Soit i l'immersion de $X_1(18)$ dans la jacobienne $J_1(18)$ de $X_1(18)$:

$$\begin{array}{rcl} i & : & X_1(18) \to J_1(18) \\ X & \mapsto & [X - Q_1] \end{array}$$

alors d'après le théorème de Manin-Drinfield, l'image des pointes de $X_1(18)$ est contenu dans $J_1(18)_{Tor}$.

Soit $\wp(z;\tau)$ la fonction de Weierstrass. Posons

$$\begin{aligned} f_i(\tau) &= \wp(\frac{i}{9};\tau) - \wp(\frac{1}{2};\tau) \\ g_i(\tau) &= \wp'(\frac{i}{9};\tau), \end{aligned}$$

les fonctions f_i (resp. g_i) sont des formes modulaires de poids 2 (resp. 3) sur $\Gamma_1(18)$, et ont leurs diviseurs concentrés aux pointes. Posons $U_i = \frac{g_i}{2f_i}$, on obtient alors trois formes modulaires de poids 1. Si l'on pose $z = \frac{U_1}{U_4}$, et $z_1 = \frac{U_2}{U_4}$ alors z et z_1 sont deux fonctions modulaires qui ne s'annulent pas en dehors des pointes de $X_1(18)$ et dont on peut déterminer le diviseur en utilisant les q-développements de ces fonctions, $(q = exp(2i\pi\tau))$. Les diviseurs de z et z_1 sont respectivement $Q_1 + 2Q_2 - 3Q_3$ et $3Q_1 - Q_2 - 2Q_3$, et comme $X_1(18)$ est de genre 2, le diviseur de la fonction zz_1^2 est $7(Q_1 - Q_3)$ et $[Q_1 - Q_3]$ est d'ordre 7. En considérant le diviseur de z on en déduit que $[Q_1 - Q_3] + 2[Q_2 - Q_3] = 0$, ce qui montre que $[Q_3 - Q_1]$ est dans le même groupe que $[Q_2 - Q_1]$.

Le revêtement galoisien $X_1(18) \to X_0(18)$ et un bon choix de n nous permettent alors de construire la famille de corps cubiques définie par le polynôme P_n et un système d'unités. Nous donnons alors une formule analytique pour le régulateur des unités construites ainsi qu'un équivalent quand n tend vers l'infini, comme le montre le théorème et la proposition suivants :

Théorème 1. *Le régulateur R du système d'unités $\{z, z^\sigma\}$ est donné par la formule*

$$R = \left(\ln|z| - \zeta^6 \ln|z^\sigma|\right)\left(\ln|z| - \zeta^{12} \ln|z^{\sigma^2}|\right)$$

où

$$\ln|z| - \zeta^6 \ln|z^\sigma| = -\frac{3\zeta^2}{2\pi} \lim_{s\to 1} \sum_{(p,q)\neq(0,0)} \frac{\left(-\mu\zeta^3\chi(p) + \theta(p)\right)\Im(\tau)^s}{|p\tau + q|^{2s}}$$

avec $\mu = 5\zeta^3 - 1$, χ et θ deux caractères respectivement modulo 9 et 18 avec $\chi(2) = -\zeta^3$ et $\theta(5) = \zeta^6, \zeta = \exp(2i\pi/18)$; et z^σ, z^{σ^2} sont les conjugués de z.

Proposition 1. *Quand n tend vers $\pm\infty$, le régulateur R est équivalent à $7\ln^2|n|$.*

Si $9^{-c}(n^2+3)(n^2+3n-3)$, $c \in \{0,1\}$, $n \in \mathbb{Z}, n \neq 1, 2$, est sans facteurs carrés alors les racines de P_n engendrent le groupe des unités de K et on montre qu'il existe une infinité de tels corps.

3. Dans le chapitre 3, nous donnons quelques propriétés arithmétiques de ces corps et étudions quelques cas particuliers. On montre que l'anneau des entiers n'est jamais monogène.

• Dans la seconde partie, on étudie le lien entre les courbes elliptiques E_n données par l'équation : $y^2 = G_n(x)$ et le 2-rang du groupe des classes des corps cubiques K_n, où $G_n(x) = -x^3 P_n(-1/x)$. Cette partie comporte les deux derniers chapitres :

1. Dans le chapitre 4, on étudie les courbes elliptiques E_n et on définit des homomorphismes liés à la 2-descente.
2. Dans le chapitre 5, on définit un sous-groupe $S_2'(\mathbb{Q})$ du 2-groupe de Selmer $S_2(\mathbb{Q})$, et un sous-groupe H de $E_n(\mathbb{Q})$. On montre alors les deux résultats suivants.

   a) En adaptant une méthode classique de 2-descente (par exemple [**?**]), on montre une majoration du rang sur $\mathbb{Q}$ des courbes elliptiques E_n en fonction du nombre de facteurs premiers de $|n-1|$ et du 2-rang r_2 du groupe des classes de K_n, comme le montre la proposition suivante :

   Proposition 2. *Soient n un entier relatif pair tel que $(n^2+3)(n^2-3n+3)$ soit sans facteurs carrés, p un nombre premier qui divise $n-1$. Soit n_p le nombre de facteurs premiers de $n-1$, r_2 le 2-rang de $C_2(K)$. Alors le rang r de $E_n(\mathbb{Q})$ satisfait l'inégalité*

$$r \;\leq\; 1 + n_p + r_2.$$

Si de plus on pose $H = \cap_{p|n-1} H'_p \cap E_n(\mathbb{Q})$, *alors*

$$\mathrm{rg}_2(H/2E_n(\mathbb{Q})) \leq 1 + r_2.$$

b) En suivant un résultat de L.C.Washington [**?**] on montre, sous certaines conditions, portant sur n, que les suites

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \langle [0,1] \rangle & \longrightarrow & S'_2(\mathbb{Q}) & \xrightarrow{\nu} & C_2(K) & \longrightarrow & 1, \\ 1 & \longrightarrow & (E'_n(\mathbb{Q}) \cap H)/2E_n(\mathbb{Q}) & \xrightarrow{\mu} & C_2(K) & \longrightarrow & Ш'_2 & \longrightarrow & 1, \end{array}$$

$$\nu : [\alpha] \mapsto \overline{I_\alpha},$$

$$\mu : [(x,y)] \mapsto \overline{I_x},\ (x-\rho) = I_x^2,$$

sont des suites exactes, où $Ш'_2$ est le conoyau de l'application $f_1 : H/2E_n(\mathbb{Q}) \to S'_2(\mathbb{Q})$ et $E'_n(\mathbb{Q}) = 2E_n(\mathbb{R}) \cap E_n(\mathbb{Q})$. On montre alors qu'il existe une relation entre le 2-rang de $H/2E_n(\mathbb{Q})$, c'est-à-dire la dimension de $H/2E_n(\mathbb{Q})$ en tant que $\mathbb{F}_2$-espace vectoriel, et le 2-rang du groupe des classes de K_n. Dans le dernier paragraphe, on explicite quelques exemples, en particulier pour $n = 626$ on obtient une courbe de rang 7.

Remarque 1. *Si on considère* n *comme une indéterminée et si on étudie les surfaces d'équations* $H(x,y,n) = y^2 - G_n(x) = 0$ *et* $J(x,y,n) = y^2 - P_n(x) = 0$ *alors la première surface est une surface rationnelle tandis que la seconde est, après désingularisation une surface* K_3. *On constate que les calculs effectués sont trop lents pour la seconde famille. Tandis que pour la première, les calculs sont plus rapides et plus intéressants, ce qui justifie le choix d'étudier la première famille.*

Chapitre 1

Rappels.

1.1 Courbes elliptiques

Dans cette partie, on rappelle brièvement quelques concepts de base liés aux courbes elliptiques.
Soit k un corps, une *courbe elliptique sur* k est une courbe projective lisse de genre 1 avec un point à coordonnées dans k.

Proposition 3. *Étant donnée une courbe elliptique sur k, il existe un système de coordonnées homogènes X, Y, Z tel que la courbe elliptique soit donnée par l'équation*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1.1.1}$$

où $(a_1, a_2, a_3, a_4, a_6) \in k^5$.
Toute courbe donnée par l'équation **??** *est elliptique si et seulement si elle est lisse.*

Remarque 2. *La courbe elliptique donnée par l'équation* **??** *rencontre la droite d'équation $Z = 0$ en un point $O = [0 : 1 : 0]$ appelé le point à l'infini.*
On utilise les coordonnées non homogènes, en posant $x = X/Z$, $y = Y/Z$, la courbe affine est donnée par l'équation :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.1.2}$$

si la caractéristique de k est différente de 2, par un changement de variables, l'équation **??** *s'écrit :*

$$y^2 = f(x) = x^3 + ax^2 + bx + c, \tag{1.1.3}$$

Définition 1. *Soient une courbe elliptique donnée par l'équation* **??**, *et* Δ_f *le discriminant du polynôme* f. *Le* discriminant *noté* Δ *(resp. l'invariant modulaire* j*) de la courbe elliptique est défini :*

$$\Delta = 16.\Delta_f(\ \textit{resp. } j = (16(a^2 - 3b))^3/\Delta)$$

Proposition 4. *Soit une courbe donnée par l'équation* **??**.
Elle est lisse, donc elliptique si et seulement si son discriminant est non nul.

Soit $P = (x_0, y_0)$ un point satisfaisant l'équation

$$g(x, y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) = 0.$$

Supposons que P est un point singulier de la courbe $g(x, y) = 0$, alors

$$\partial g/\partial x(P) = \partial g/\partial y(P) = 0.$$

Alors le développement de Taylor de $g(x, y)$ au point P est de la forme :

$$g(x, y) - g(x_0, y_0) = [(y - y_0) - \alpha(x - x_0)][(y - y_0) - \beta(x - x_0)] - (x - x_0)^3,$$

où $\alpha, \beta \in \overline{k}$.

Définition 2. *En gardant les mêmes notations que précédemment, le point singulier* P *est un noeud si* $\alpha \neq \beta$. *Dans ce cas, les droites*

$$y - y_0 = \alpha(x - x_0)\ \textit{et}\ y - y_0 = \beta(x - x_0)$$

sont les tangentes en P. *Si* $\alpha = \beta$, *le point* P *est une pointe. Dans ce cas la tangente en* P *est donnée par*

$$y - y_0 = \alpha(x - x_0).$$

Loi de groupe :

Définition 3. *Soit* k *un corps,* E *une courbe elliptique sur* k. *L'ensemble des points projectifs qui appartiennent à* E *à coordonnées dans* k *est appelé l'ensemble* des points k-rationnels *de* E, *qu'on notera* $E(k)$.

L'intérêt de l'étude des courbes elliptiques vient du fait que $E(k)$ possède une structure de groupe, dont O est l'élément neutre pour l'addition, qui est défini de la manière suivante :

Définition 4. *Soient* P *et* Q *deux points quelconques de la courbe* E, *et* R *le point d'intersection de la courbe* E *et de la droite* PQ, *on définit la somme des deux points* P *et* Q, *noté* $P + Q$ *comme étant le point d'intersection de* E *et de la droite* RO.

La structure du groupe $E(k)$ est donnée par le théorème de Mordell-Weil.

Théorème 2. *(Mordell-Weil)*
Soit k un corps de nombres. Soit E une courbe elliptique sur k. Le groupe $E(k)$ est un groupe abélien de type fini.

Morphismes : Un morphisme entre deux courbes est une application rationnelle partout régulière.

Définition 5. *Soient E, E' des courbes elliptiques. Une isogénie entre E et E' est un morphisme non constant*

$$\phi : E \ \rightarrow \ E',$$

satisfaisant $\phi(O) = O'$. Les courbes E et E' sont dites isogènes, s'il existe une isogénie entre elles.

Les isogénies sont des morphismes pour les lois de groupes sur E et E'.

1.2 Courbes modulaires.

1.2.1 Sous-groupe de congruence.

On note $\mathcal{H}$ le demi-plan supérieur de $\mathbb{C}$, autrement dit $\mathcal{H} = \{z \in \mathbb{C}/\Im(z) > 0\}$. Soit $SL_2(\mathbb{R})$ le groupe des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients réels, telles que $ad - bc = 1$. Le groupe $SL_2(\mathbb{R})$ opère sur $\mathcal{H}$, de la manière suivante :

$$\begin{aligned} SL_2(\mathbb{R}) \times \mathcal{H} &\longrightarrow \mathcal{H} \\ (g, z) &\longmapsto g.z = \frac{az + b}{cz + d}. \quad (1) \end{aligned}$$

On s'intéresse dans ce chapitre à l'action de sous-groupe de $SL_2(\mathbb{Q})$. On étend l'action (1) restreinte à $SL_2(\mathbb{Q})$ en une action sur $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}) = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$.
Le noyau est $\pm Id$ et on déduit une action fidèle de $SL_2(\mathbb{Z})/\{\pm Id\}$ sur $\mathcal{H}$. On appelle groupe modulaire le groupe

$$PSL_2(\mathbb{Z}) = \Gamma(1) = SL_2(\mathbb{Z})/\{\pm 1\}.$$

Définition 6. *Soit N un entier positif. On appelle sous-groupe de congruence de niveau N un sous-groupe de $SL_2(\mathbb{Z})$ contenant le sous-groupe*

$$\Gamma(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) / b \ \equiv \ c \ \equiv \ 0 \mod N, a \ \equiv \ 1 \mod N\}.$$

Exemple: Les sous-groupes $\Gamma_1(N)$, $\Gamma_0(N)$ de $SL_2(\mathbb{Z})$ définis par

$$\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})/\ c \ \equiv \ 0 \mod N\}.$$

et

$$\Gamma_1(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})/c \ \equiv \ 0 \mod N \text{ et } a \ \equiv \ 1 \mod N\}$$

sont des sous groupes de congruences de niveau N, et on a $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$.

Proposition 5. *La suite*

$$1 \longrightarrow \Gamma(N) \longrightarrow SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/N\mathbb{Z}) \longrightarrow 1$$

est une suite exacte.

1.2.2 Les courbes modulaires $X_1(N)$ et $X_0(N)$.

Les sous-groupes de congruences opèrent sur $\mathcal{H}^*$ par l'action (1).

Définition 7. *Les orbites de $\mathcal{H}$ sous l'action de $\Gamma_0(N)$ (resp. $\Gamma_1(N)$) sont notées*

$$Y_0(N) = \Gamma_0(N) \setminus \mathcal{H}$$

$$Y_1(N) = \Gamma_1(N) \setminus \mathcal{H}.$$

Les orbites de $\mathcal{H}^*$ sous l'action de $\Gamma_0(N)$ (resp. $\Gamma_1(N)$) sont notées

$$X_0(N) = \Gamma_0(N) \setminus \mathcal{H}^*$$

$$X_1(N) = \Gamma_1(N) \setminus \mathcal{H}^*,$$

et appelées courbes modulaires. Le complémentaire de l'ouvert $Y_0(N)$ dans $X_0(N)$ (resp. $Y_1(N)$ dans $X_1(N)$) est un ensemble fini dont les éléments s'appellent les pointes (cusps). Les deux pointes $\Gamma_0(N).0$ (resp. $\Gamma_1(N).0$) et $\Gamma_0(N).\infty$ sont notées pointes 0 et ∞.

Les courbes modulaires $Y_0(N)$ et $Y_1(N)$ sont des surfaces de Riemann non compactes, qui admettent des compactifications naturelles $X_0(N)$ et $X_1(N)$ obtenues en rajoutant les pointes.

Proposition 6. *Il existe une correspondance bijective entre les orbites* $\Gamma_0(N)\tau$ *et les classes d'isomorphismes formées du couple* $(E_N, \langle\ P\ \rangle)$ *où* E *est une courbe elliptique et* P *est un point de* E_N *d'ordre* N.
On a un énoncé analogue en remplaçant $Y_0(N)$ *par* $Y_1(N)$ *et* C_N *par un point* P *d'ordre* N.

Remarque 3. *Comme pour les sous-groupes de congruence* $\Gamma_0(N)$ *et* $\Gamma_1(N)$, *on définit de la même façon la courbe modulaire associée à un sous-groupe de congruence* Γ *de* $SL_2(\mathbb{Z})$. *Le quotient* $Y_\Gamma = \Gamma \setminus \mathcal{H}$ *est une courbe modulaire qui possède une structure de surface de Riemann, en la compactifiant on obtient* $X_\Gamma = \Gamma \setminus \mathcal{H}^*$. *L'ensemble* $X_\Gamma - Y_\Gamma$ *est un ensemble fini, dont les éléments s'appellent les pointes.*
Soit c *une pointe de* X_Γ *alors il existe* $\gamma \in SL_2(\mathbb{Z})$ *tel que* $c = \gamma\infty$. *On appelle largeur de la pointe* c *le plus petit entier* h *tel que* $\gamma^{-1}\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}\gamma \in \Gamma$.

1.2.3 Calcul des pointes des courbes $X_0(N)$ et $X_1(N)$.

Dans [**?**], Ogg donne la méthode suivante pour le calcul des pointes des courbes $X_0(N)$ et $X_1(N)$.
Pointes de $X_1(N)$ **:** Pour chaque pointe, on choisit un représentant de la forme $\begin{pmatrix} x \\ y \end{pmatrix}$ tel que x est réduit modulo (y, N) et $(x, y, N) = 1$, ces pointes sont définies sur $\mathbb{Q}(\mu_{(y,N)})$ i.e le corps de définition des ces pointes est égal à $\mathbb{Q}(\mu_{(y,N)})$.

Pointes de $X_0(N)$ **:** Pour chaque pointe, on choisit un représentant de la forme $\begin{pmatrix} x \\ d \end{pmatrix}$ où d est un diviseur de N et x est réduit modulo $(d, N/d)$, ces pointes sont définies sur $\mathbb{Q}(\mu_{(y,\frac{N}{(y,N)})})$ i.e le corps de définition des ces pointes est égal à $\mathbb{Q}(\mu_{(y,\frac{N}{(y,N)})})$.

1.2.4 Action du groupe de Galois sur les pointes.

Soit $\sigma \in Gal(\overline{Q}/Q)$ et N un entier. On notera $\mu_{\sigma,N}$ l'entier modulo N tel que $\sigma(\xi_N) = \xi_N^{\mu_{\sigma,N}}$ où ξ_N est une racine Nème de l'unité. L'action de σ sur la pointe $\begin{pmatrix} x \\ y \end{pmatrix}$ est alors donnée par $\sigma.\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \mu_{\sigma,N}\ x \\ y \end{pmatrix}$.
On a alors la propriété suivante pour les pointes. Comme x peut-être choisi modulo d avec $d = (y, N)$. Donc $\begin{pmatrix} x \\ y \end{pmatrix}$ est rationnelle si et seulement si

$\phi(d) = 1$ c'est à dire $d = 1$ ou 2.

1.2.5 Revêtements modulaires et involutions.

Définition 8. *Soit $p : X \longrightarrow Y$ un revêtement. On appelle fibre de p en $y \in Y$ l'ensemble $p^{-1}(\{y\})$.*

Définition 9. *Soient X et B deux espaces topologiques connexes et localement connexes par arcs et $p : X \longrightarrow B$ un revêtement . On appelle B-automorphisme de p un homéomorphisme $f : X \longrightarrow X$ tel que $p \circ f = p$. Ces automorphismes forment un groupe $G(p)$, qu'on appelle le groupe de Galois du revêtement.*

Définition 10. *On dit que le revêtement $p : X \longrightarrow B$ est galoisien si $G(p)$ opère sur chaque fibre de p.*

Pour construire des revêtements, nous procéderons de la manière suivante : soient Γ' et Γ deux sous-groupes de congruences de $SL_2(\mathbb{Z})$, tels que Γ' soit normal dans Γ. Soit f le morphisme $X_{\Gamma'} \longrightarrow X_\Gamma$ déduit de l'identité sur $\mathcal{H}^*$ par passage au quotient. Tout élément g de Γ induit par passage au quotient de $\tau \longrightarrow g.\tau$ un automorphisme de $X_{\Gamma'}$. Le groupe de Galois du revêtement $X_{\Gamma'} \longrightarrow X_\Gamma$ est égal à $\Gamma/\{-1, 1\}\Gamma'$.
Soit N_1 et N_2 tels que $(N_1, N_2) = 1$ avec $N = N_1N_2$ et $N_1 > 1$. Si $g = \begin{pmatrix} aN_1 & b \\ cN & N_1d \end{pmatrix}$, avec $a, b, c, d \in \mathbb{Z}$ et le déterminant de la matrice g est égal à N_1. Alors g est dans le normalisateur de $\Gamma_0(N)$. On définit alors, par passage au quotient de la transformation $\tau \longrightarrow g\tau$ un automorphisme de $X_0(N)$, qu'on appelle involution d'Atkin-Lehner, qu'on note w_{N_1}.
L'élément $g_1 = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ est dans le normalisateur de $\Gamma_0(N)$ et $\Gamma_1(N)$, comme précédemment, par passage au quotient, on définit un automorphisme de $X_0(N)$ et $X_1(N)$, qu'on appelle involution de Fricke, notée w_N. Cette dernière transforme un point de $Y_0(N)$ correspondant à la classe du couple (E, C_N) en la classe du couple $(E/C_N, E[N]/C_N)$ où $E[N] = \{P, NP = 0\}$.
Nous construisons pour $n|N$ l'espace $X_0(N)/w_n = G/\mathcal{H}^*$ où $G = \Gamma_0(N) \cup w_n\Gamma_0(N)$. Ainsi $X_0(N)/w_n$ est une surface de Riemann et l'application $\phi : X_0(N) \longrightarrow X_0(N)/w_n$ est un revêtement de degré $[G : \Gamma_0(N)] = 2$.

Exemple:
• Si $\Gamma' = \Gamma_1(N)$ et $\Gamma = \Gamma_0(N)$, alors $\Gamma_0(N) \triangleright \Gamma_1(N)$ et le revêtement $X_1(N) \longrightarrow X_0(N)$ est de degré $\phi(N)/2$ et son groupe de Galois est isomorphe au groupe $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$. En particulier, si $N = 18$ alors le revêtement $X_1(18) \longrightarrow X_0(18)$ est de degré 3.

• Si $g = \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N)$, alors g est un automorphisme sur $X_1(N)$, qu'on appelle l'automorphisme diamant, qu'on note $\langle d \rangle$.

1.3 Formes modulaires

Soit f une fonction méromorphe sur $\mathcal{H}$ de période 1. Alors f admet un développement en série de Laurent i.e

$$f(q) = \sum_{n \in \mathbb{Z}} a_n q^n, \text{ où } q = e^{2\pi i z}.$$

On dira que f est méromorphe à l'infini s'il existe N tel que $a_n = 0$ pour $n \leq -N$, f est holomorphe à l'infini si $a_n = 0$ pour $n < 0$, et que f s'annule à l'infini si $a_n = 0$ pour $n \leq 0$.

1.3.1 Formes modulaires pour $SL_2(\mathbb{Z})$.

Définition 11. *Soit f une fonction méromorphe sur $\mathcal{H}$ et k un entier. Supposons que f vérifie les deux relations suivantes :*

1. $f(z) = (az+d)^{-k} f(\frac{az+b}{cz+d})$, *pour tout* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.
2. *f est méromorphe à l'infini.*

Alors f est appelée fonction modulaire de poids k pour $SL_2(\mathbb{Z})$.
Si $k = 0$, on dira que f est une fonction modulaire pour $SL_2(\mathbb{Z})$.

Remarque 4. *En particulier, pour* $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *et* $\gamma_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ *la condition (1) est équivalente aux deux relations*

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

ii) $f(-1/z) = (-z)^k f(z)$.

Définition 12. *On appelle forme modulaire de poids k pour $SL_2(\mathbb{Z})$, toute fonction modulaire de poids k pour $SL_2(\mathbb{Z})$, qui est holomorphe sur $\mathcal{H}$ et à l'infini. Si de plus elle s'annule à l'infini, on dit que c'est une forme parabolique (cusp form).*

Une forme modulaire de poids k est donc donnée par une série

$$f(q) = \sum_{n=0}^{+\infty} a_n q^n = \sum_{n=0}^{+\infty} a_n e^{2\pi n i z}.$$

Si $a_0 = 0$, la forme modulaire est une forme parabolique.
On va définir les fonctions modulaires, les formes modulaires et les formes paraboliques pour des sous-groupes de congruence de $SL_2(\mathbb{Z})$.

1.3.2 Formes modulaires pour les sous-groupes de congruence.

Soit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, soit f une fonction définie sur $\mathcal{H}^*$ à valeurs dans $\mathbb{C} \cup \{\infty\}$, et $k \in \mathbb{Z}$. On définit la notation $f_{|k}\gamma$:

$$f_{|k}\gamma(z) = (cz + d)^{-k} f(\gamma z).$$

Définition 13. *Soit f une fonction méromorphe sur $\mathcal{H}$, Γ' un sous-groupe de congruence de $SL_2(\mathbb{Z})$, et $k \in \mathbb{Z}$. On dit que f est une fonction modulaire de poids k pour Γ' si*
1)$f_{|k}\gamma = f$ pour tout $\gamma \in \Gamma'$
2)$f_{|k}\gamma_0$ est méromorphe aux pointes, pour tout $\gamma_0 \in SL_2(\mathbb{Z})$.

La condition (2) signifie la propriété suivante ; soit c une pointe de largeur h et soit $\gamma \in SL_2(\mathbb{Z})$ telle que $\gamma c = \infty$. Alors la condition $\gamma^{-1} c \gamma \in \Gamma'$ et la condition 1 entraînent que $f_{|k}\gamma$ est périodique de période h.

Définition 14. *On appelle forme modulaire de poids k pour Γ', toute fonction modulaire de poids k pour Γ' qui est holomorphe sur $\mathcal{H}$ et $f_{|k}\gamma_0$ est holomorphe aux pointes pour tout $\gamma_0 \in \Gamma$. La forme modulaire est une forme parabolique si $f_{|k}\gamma_0$ s'annule aux pointes pour tout $\gamma_0 \in \Gamma$.*

L'ensemble des fonctions modulaires sur Γ est un corps de fonction en une variable, i.e de degré de transcendance égal à 1 et de type fini.

1.3.3 Exemples d'unités modulaires.

Définition 15. *Soit F_N le corps de fonctions de $X(N)$. On appelle unités modulaires les fonctions modulaires de F_N qui possèdent des zéros et des pôles seulement en les pointes.*

Soit η la fonction de Dedekind définie par $\eta(\tau) = q^{\frac{1}{24}} \prod_{n \geq 1}(1 - q^n)$. Soit $d|N$, l'ordre de la fonction $\eta(d\tau)$ sur $X_0(N)$ en une pointe $\begin{pmatrix} a \\ c \end{pmatrix}$ est égal à $\dfrac{18(d,c)^2}{24dc(c,N/c)}$. Sous certaines conditions, le produit des fonctions $\eta(d\tau)$ permet de construire des fonctions modulaires sur $X_0(N)$, comme l'a montré Newman dans son théorème.

Théorème 3. *(Newman) Soit la fonction* $F(\tau) = \prod_{0<d|N} \eta(d\tau)^{r_d}$*, tels que* $r_d \in \mathbb{Z}$*, satisfaisant les conditions suivantes :*
i) $\sum_{0<d|N} r_d = 0$,
ii) $\prod_{0<d|N} d^{r_d}$ *est un carré,*
iii) l'ordre de F *en chaque pointe est un entier.*
Alors F *est une unité modulaire sur* $X_0(N)$*.*

Soit $\tau = \dfrac{\omega_1}{\omega_2}$ et $\wp(z;\omega_1,\omega_2)$ la fonction de Weierstrass. Posons

$$\begin{aligned} f_{i,j}(\tau) &= \wp(\frac{i\omega_2}{N};\omega_1,\omega_2) - \wp(\frac{j\omega_2}{N};\omega_1,\omega_2) \\ g_i(\tau) &= \wp'(\frac{i\omega_2}{N};\omega_1,\omega_2), \end{aligned}$$

où $i \not\equiv j \mod N$. Les fonctions $f_{i,j}$ (resp. g_i) sont des formes modulaires de poids 2 (resp. 3) sur $\Gamma_1(N)$ et elles permettent de construire des fonctions modulaires sur $X_1(N)$ avec zéros et pôles uniquement aux pointes. En une pointe $\begin{pmatrix} x \\ y \end{pmatrix}$, $f_{i,j}$ a un zéro d'ordre

$$\frac{N}{2d}[B_2\{\frac{(i+j)y}{N}\} + B_2\{\frac{(i-j)y}{N}\} - 2B_2\{\frac{iy}{N}\} - 2B_2\{\frac{jy}{N}\}],$$

où $B_2(x) = x^2 - x + \frac{1}{6}$ est le polynôme de Bernoulli, $d = (N, y)$ et $\{x\}$ vérifie $\{x\} \equiv x \mod 1$ et $0 \leq x \leq 1$.
En une pointe $\begin{pmatrix} x \\ y \end{pmatrix}$, g_i a un zéro d'ordre $\frac{N}{2d}[B_2\{\frac{2iy}{N}\} - 4B_2\{\frac{iy}{N}\}]$. Le quotient de ces formes modulaires permettent de construire des unités modulaires.

Chapitre 2

Surfaces elliptiques modulaires et corps cubiques cycliques.

Si τ est un nombre quadratique imaginaire, on définit des unités elliptiques comme valeurs de fonctions modulaires en τ. Ces unités sont intéressantes pour l'étude des extensions abéliennes des corps quadratiques imaginaires $\mathbb{Q}(\tau)$.
Dans ce chapitre, nous construisons un analogue de ces unités elliptiques par spécialisation de fonctions modulaires dont le support du diviseur est formé de pointes d'une courbe modulaire. De telles fonctions sont des unités modulaires. Des constructions analogues ont été faites pour d'autres surfaces modulaires. Dans [**?**] L. Washington dit "it would be interesting to use the modular construction in an intrinsic way to study the arithmetic of these fields." La proposition 9 (ou le théorème 5) est un premier pas dans cette direction ; il serait ensuite intéressant de donner une formule d'indice comme pour les unités elliptiques. Plus précisément nous spécialisons en une valeur entière un générateur du corps des fonctions des courbes modulaires $X_0(9)$ et $X_1(18)$. Utilisant les revêtements, de degré 3 des courbes modulaires $X_1(9) \to X_0(9)$ et $X_1(18) \to X_0(18)$ nous construisons deux familles de corps cubiques cycliques et un système d'unités pour chaque famille. Ces constructions sont explicitées aux paragraphes 2.1 et 2.4. L'équation $F(X,m) = P_m(X) = 0$ où

$$P_m(X) = X^3 + \left(\left(m^2 - 2m + 4\right)(m+1) - 3\right)X^2 - (m-1)^2 X - 1,$$

est en fait une équation de la courbe modulaire $X_1(18)$ de genre 2.
Aux paragraphes 2.2 et 2.6 nous donnons quelques propriétés arithmétiques de ces corps et étudions quelques cas particuliers.
Enfin, dans le cas du revêtement $X_1(18) \to X_0(18)$ nous donnons une formule analytique pour le régulateur des unités construites ainsi qu'un équivalent quand m tend vers l'infini. Sans références modulaires cette famille de polynômes a été étudiée dans [**?**] et cet équivalent peut se retrouver de façon

élémentaire en utilisant les racines du polynôme P_m. La démonstration que nous donnons ici n'utilise pas l'équation de la courbe modulaire mais les propriétés des diviseurs des unités utilisées. Plus précisément l'ordre des zéros et des pôles en certaines pointes expliquent le facteur 7 obtenu au paragraphe 2.8.
On commence tout d'abord par des rappels sur les courbes et les surfaces elliptiques modulaires.
Si $\Gamma \subset PSL_2(\mathbb{Z})$ est un sous groupe de congruence sans torsion, le produit semi-direct de Γ par $\mathbb{Z}^2$, que l'on note $\widetilde{\Gamma} = \Gamma \rtimes \mathbb{Z}^2$, opère sur $\mathcal{H} \times \mathbb{C}$ par

$$\begin{aligned}&\widetilde{\Gamma} \times \mathcal{H} \times \mathbb{C} \longrightarrow \mathcal{H} \times \mathbb{C}\\ &(\gamma, p, q, \tau, z) \longmapsto (\gamma, p, q).(\tau, z) = \big(\gamma.\tau, (c\tau + d)^{-1}(z + p\tau + q)\big).\end{aligned}$$

On note E^0_Γ la surface quotient $\mathcal{H} \times \mathbb{C} \ \setminus \widetilde{\Gamma}$, et $Y_\Gamma = \Gamma \setminus \mathcal{H}$ la courbe quotient.

Définition 16. *On appelle fibration un homomorphisme surjectif entre variétés algébriques.*
1) Si les fibres non singulières sont des courbes elliptiques, la fibration est appelée fibration elliptique.
2) Si les fibres singulières sont de type I_c, où I_c est un polygone à c côtés formé de courbes rationnelles. Alors la fibration est appelée fibration semi-stable.

D'après [Ko], la fibration elliptique

$$\begin{aligned}&E^0_\Gamma \longrightarrow Y_\Gamma\\ &(\tau, z) \longmapsto \tau,\end{aligned}$$

se prolonge de manière unique en une fibration semi-stable

$$E_\Gamma \longrightarrow X_\Gamma,$$

La surface E_Γ obtenue est appelée surface elliptique modulaire associée au groupe modulaire Γ.

Définition 17. *On appelle surface elliptique semi-stable, une fibration $p : X \longrightarrow C$, où X est une surface compacte lisse, C est une courbe lisse de genre 0. Et tous les fibres singulières sont de type I_c, tels que I_c est un polygone à c côtés formé de courbes rationnelles.*

Si on considère les surfaces elliptiques semi-stables sur $\mathbb{P}^1$

$$f : X \longrightarrow \mathbb{P}^1$$

on montre qu'elles admettent au moins quatre fibres singulières et sont rationnelles. Dans [Be], Beauville a donné une liste (finie) de surfaces admettant exactement quatre fibres singulières et montré qu'elles correspondent aux surfaces elliptiques modulaires associées aux sous-groupes de $SL_2(\mathbb{Z})$ décrits dans le théorème suivant.

Théorème 4. *Soit $f : X \longrightarrow \mathbb{P}^1$ une famille semi-stable de courbes elliptiques admettant quatre fibres singulières. Alors f est isomorphe à la famille modulaire associée à l'un des six sous-groupes Γ ci dessous ;*

Γ	*equation*
$\Gamma(3)$	$X^3+Y^3+Z^3+tXYZ=0$
$\Gamma_1(4)\cap\Gamma(2)$	$X(X^2+Z^2+2ZY)+tZ(X^2-Y^2)=0$
$\Gamma_1(5)$	$X(X-Z)(Y-Z)+tZY(X-Y)=0$
$\Gamma_1(6)$	$(X+Y)(Y+Z)(Z+X)+tXYZ=0$
$\Gamma_0(8)\cap\Gamma_1(4)$	$(X+Y)(XY-Z^2)+tXYZ=0$
$\Gamma_0(9)\cap\Gamma_1(3)$	$X^2Y+Y^2Z+Z^2X+tXYZ=0$

2.1 Surfaces elliptiques modulaires associées au groupe de congruence $\Gamma_0(9)\cap\Gamma_1(3)$.

Dans notre cas, la surface elliptique modulaire associée au groupe de congruence $\Gamma_0(9)\cap\Gamma_1(3)$ a pour équation

$$x^2y+y^2z+z^2x+axyz=0,$$

on déduit alors l'équation de Weierstrass de cette surface

$$y^2+axy+y=x^3, \tag{2.1.1}$$

qu'on appelle forme normale de Deuring. On notera E_a la fibre générique d'invariant $j(a)=\frac{a^3(a^3-24)^3}{a^3-27}$ et de discriminant $\Delta=a^3-27$. Sauf exceptions on notera (x,y) les coordonnées d'un point de E_a pour l'équation de Weierstrass ci dessus. Explicitons les coordonnées d'un point A_9 d'ordre 9 de E_a tel que le couple $(E_a,<A_9>)$ corresponde à un point de la courbe modulaire $X_{\Gamma_0(9)\cap\Gamma_1(3)}$. Le point $A_3=(0,0)$ de la courbe E_a est d'ordre 3. Si $M=(x,y)\in E_a$ alors le point $3M$ a pour coordonnées (u,v) avec

$$u=\frac{(x^3-(a+3)x^2+ax+1)\,H(x)}{x^2(3x^3+a^2x^2+3ax+3)^2},$$

où $H(x)=x^6+(a+3)x^5+(a^2-a+9)x^4+(a+2)(a+1)x^3+(a^2+a+3)x^2+2ax+1$.

Si α est l'une des racines du polynôme

$$S_{a+3}(x) = x^3 - (a+3)x^2 + ax + 1.$$

les deux autres racines sont $\dfrac{\alpha-1}{\alpha}$ et $\dfrac{-1}{\alpha-1}$. Le générateur du groupe de Galois de l'extension $\mathbb{Q}(a)(\alpha)/\mathbb{Q}(a)$, que l'on note σ, est défini par $\sigma(\alpha) = \dfrac{\alpha-1}{\alpha}$. Soit $A_9 = (\alpha, -\alpha(\alpha-1))$ le point d'ordre 9 tel que $3A_9 = -A_3$. On a alors $\sigma(A_9) = 7A_9$ et $\sigma^2(A_9) = 4A_9$. Les ordonnées des points iA_9 avec $i = 1, 4, 7$ sont les racines du polynôme en y

$$y^3 + \left(a^2 + 3a + 6\right) y^2 + 3y - 1.$$

Nous regroupons dans un tableau les coordonnées des points iA_9

$$\begin{array}{cc} A_9 = (\alpha, -\alpha(\alpha-1)) & -A_9 = \left(\alpha, \frac{\alpha^2}{\alpha-1}\right) \\ 7A_9 = \left(\frac{\alpha-1}{\alpha}, \frac{\alpha-1}{\alpha^2}\right) & -7A_9 = \left(\frac{\alpha-1}{\alpha}, \frac{(\alpha-1)^2}{\alpha}\right) \\ 4A_9 = \left(\frac{-1}{\alpha-1}, \frac{-\alpha}{(\alpha-1)^2}\right) & -4A_9 = \left(-\frac{1}{\alpha-1}, -\frac{1}{\alpha(\alpha-1)}\right). \end{array}$$

Tous les points P vérifiant $3P = -A_3$, sont de la forme $iA_9 + sB_3$ où $3B_3 = 0$ et $B_3 \notin \{\pm A_3, 0\}$. Les abscisses de ses points sont racines du polynôme H, qui se factorise sur $\mathbb{Q}(a)(e^{2\pi i/3})$.

2.1.1 Expression de a et α comme fonctions modulaires

Proposition 7. *Les fonctions a et α sont des fonctions modulaires respectivement pour $\Gamma_1(3) \cap \Gamma_0(9)$ et $\Gamma_1(9)$ et l'on a*

$$\begin{aligned} a - 3 &= 3^3 \frac{\eta(9\tau)^3}{\eta(\tau)^3}, \\ \alpha &= -\frac{\mathfrak{k}\left(\frac{2}{9};\tau\right)\mathfrak{k}\left(\frac{4}{9},\tau\right)}{\mathfrak{k}^2\left(\frac{1}{9};\tau\right)}, \end{aligned}$$

où $\eta(\tau)$ est la fonction de Dedekind, $\mathfrak{k}(v;\tau)$ la forme de Klein.
La fonction α est une unité sur $\mathbb{Z}[a]$ racine du polynôme

$$X^3 - (a+3)X^2 + aX + 1.$$

Preuve
Posons $Y = y + \frac{ax+1}{2}$, l'équation de la courbe E_a devient $Y^2 = x^3 + \left(\frac{ax+1}{2}\right)^2$. Si $Y_{iA_9} = y_{iA_9} + \frac{ax_{iA_9}+1}{2}$, en calculant les polynômes minimaux de $x_{A_9} - x_{4A_9}$ et Y_{A_9}, on obtient alors les égalités suivantes :

$$(x_{A_9} - x_{4A_9})(x_{A_9} - x_{7A_9})(x_{7A_9} - x_{4A_9}) = a^2 + 3a + 9$$

$$Y_{A_9}Y_{4A_9}Y_{7A_9} = \frac{a^2+3a+9}{8},$$

il en résulte que

$$\frac{\Delta(a)(x_{A_9}-x_{4A_9})(x_{A_9}-x_{7A_9})(x_{7A_9}-x_{4A_9})}{(Y_{A_9}Y_{4A_9}Y_{7A_9})^2} = 8^2(a-3).$$

Il est facile de vérifier que

$$\frac{x_{4A_9}-x_{A_9}}{x_{4A_9}-x_{7A_9}} = \alpha.$$

Si $E_a(\mathbb{C}) = \mathbb{C}/(\omega_1\mathbb{Z}+\omega_2\mathbb{Z})$, les fonctions $a-3$ et α sont des fonctions du réseau $(\omega_1\mathbb{Z}+\omega_2\mathbb{Z})$ de poids 0. Posant $\tau = \frac{\omega_1}{\omega_2}$, on identifie $(E_a(\mathbb{C}), A_9)$ et $\left(\mathbb{C}/(\mathbb{Z}\tau+\mathbb{Z}), \frac{1}{9}\right)$; les fonctions $a-3$ et α sont des fonctions modulaires respectivement pour $\Gamma_0(9)\cap\Gamma_1(3)$ et $\Gamma_1(9)$. On exprime ces quotients au moyen des fonctions $\wp(v;\tau)$ de Weierstrass, on obtient alors

$$\frac{\Delta(a)(\wp(1/9;\tau)-\wp(4/9;\tau))(\wp(1/9;\tau)-\wp(7/9;\tau)(\wp(7/9;\tau)-\wp(4/9;\tau))}{(\wp'(1/9;\tau)\wp'(4/9;\tau)\wp'(7/9;\tau))^2} = a-3,$$

$$\frac{\wp(4/9;\tau)-\wp(1/9;\tau)}{\wp(4/9;\tau)-\wp(7/9;\tau)} = \alpha,$$

puis des fonctions $\mathfrak{k}(u;\tau)$ de Klein, en utilisant les relations

$$\wp(u;\tau)-\wp(v;\tau) = -\frac{\mathfrak{k}(u+v;\tau)\,\mathfrak{k}(u-v;\tau)}{\mathfrak{k}(u;\tau)^2\,\mathfrak{k}(v;\tau)^2}.$$

$$\wp'(u;\tau) = -\frac{\mathfrak{k}(2u;\tau)}{\mathfrak{k}^4(u;\tau)}.$$

$$\mathfrak{k}(u_2;\tau) = -\mathfrak{k}(u_2+1;\tau).$$

On obtient

$$\alpha = -\frac{\mathfrak{k}(5/9,\tau)\mathfrak{k}^2(7/9,\tau)}{\mathfrak{k}^2(1/9,\tau)(11/9,\tau)}$$

$$a-3 = \frac{\Delta(a)\mathfrak{k}(5/9;\tau)\mathfrak{k}(-3/9;\tau)\mathfrak{k}(-6/9;\tau)\mathfrak{k}(11/9;\tau)\mathfrak{k}(3/9;\tau)\mathfrak{k}^4(1/9;\tau)\mathfrak{k}^4(4/9;\tau)\mathfrak{k}^4(7/9;\tau)}{(\mathfrak{k}^2(2/9;\tau)\mathfrak{k}^2(8/9;\tau)\mathfrak{k}^2(14/9;\tau))^2}$$

Si $q_\tau = e^{2i\pi\tau}$ et $q_u = e^{2i\pi(u_1\tau+u_2)}$, on utilise les développements en produits infinis des fonctions $\mathfrak{k}(u,\tau)$

$$\mathfrak{k}(u_1\tau+u_2;\tau) = -2i\pi q_\tau^{1/2(u_1)(u_1-1)}e^{2i\pi u_2(u_1-1)/2}(1-q_u)\prod_{n=1}^{\infty}\frac{(1-q_\tau^n q_u)(1-q_\tau^n/q_u)}{(1-q_\tau^n)^2}.$$

On a alors

$$\mathfrak{k}\,(u_2;\tau) = -\mathfrak{k}\,(u_2+1;\tau)\,.$$

de plus, on a l'égalité suivante :

$$\begin{aligned}(1-e^{2i\pi/9})(1-e^{-4i\pi/9})(1-e^{8i\pi/9}) &= (1-e^{2i\pi/9})(1-e^{2i\pi/3}e^{2i\pi/9}) \\ &\quad (1-e^{4i\pi/3}e^{2i\pi/9}) \\ &= 1-e^{2i\pi/3}.\end{aligned}$$

En remplaçant dans $(*)$, on obtient

$$\begin{aligned}a-3 &= -(e^{2i\pi/3}-e^{-2i\pi/3})^3(e^{i\pi/9}-e^{-i\pi/9})^3\left(e^{2i\pi/9}-e^{-2i\pi/9}\right)^3 \\ &\quad (e^{4i\pi/9}-e^{-4i\pi/9})^3(\frac{\eta(9\tau)}{\eta(\tau)})^3 \\ &= (1-e^{4i\pi/3})^3(1-e^{2i\pi/3})^3(\frac{\eta(9\tau)}{\eta(\tau)})^3 \\ &= 3^3(\frac{\eta(9\tau)}{\eta(\tau)})^3.\end{aligned}$$

On obtient après simplification l'expression donnée dans la proposition.
La fonction modulaire α a un diviseur égal à -$\begin{pmatrix}0\\1\end{pmatrix}$+$\begin{pmatrix}0\\5\end{pmatrix}$, donc elle admet un pôle et un zero simple, on déduit alors que α engendre le corps de fonction de la courbe modulaire $X_1(9)$.
L'ordre de la fonction modulaire $a-3$ en chaque pointe est un entier. D'après le théorème **??** , on déduit que $a-3$ est une fonction modulaire sur $X_0(9)$, qui admet un zéro et un pôle simple. Donc la fonction $a-3$ engendre le corps de fonction de $X_0(9)$.

2.2 Polynômes de Type Shanks

Rappelons quelques propriétés des corps cubiques cycliques. Si κ est un générateur d'une extension L cubique cyclique d'un corps k, et σ un générateur du groupe de Galois alors $u_\kappa = \dfrac{\kappa-\kappa^\sigma}{\kappa-\kappa^{\sigma^2}}$ vérifie les propriétés suivantes : $t := tr_{L/k}(u_\kappa) = -tr_{L/k}(\dfrac{1}{u_\kappa})+3$; $N_{L/k}(u_\kappa) = 1$ et $u_\kappa^\sigma = \dfrac{u_\kappa-1}{u_\kappa}$, ceci montre que u_κ engendre l'extension L/k et a pour polynôme minimal

$S_t = X^3 - tX^2 + (t-3)X + 1$. On montre facilement que $\dfrac{u_\kappa - u_\kappa^\sigma}{u_\kappa - u_\kappa^{\sigma^2}}$ est un conjugué de u_κ. Nous appellerons un tel polynôme un polynôme de type Shanks(dans [**?**], Shanks a introduit ces polynômes dans le cas où $t \in \mathbb{Z}$ et a étudié les corps cubiques engendrés par l'une des racines de ces polynômes, et les a appelés "Simplest cubic fields"). L'extension cubique associée sera notée L_t. Appliquons cette propriété au groupe engendré par A_9 de la courbe E_a,

$$\alpha = \frac{x_{4A_9} - x_{A_9}}{x_{4A_9} - x_{7A_9}}, \quad \frac{\alpha - 1}{\alpha} = \frac{x_{A_9} - x_{4A_9}}{x_{A_9} - x_{7A_9}}.$$

Si $a \in \mathbb{Z}$, en utilisant la construction modulaire précédente, retrouvons la propriété de l'extension L_a donnée dans la proposition suivante. Remarquons tout d'abord que le point A_9 de E_a est défini sur L_a et que α et α^σ sont des unités de L_a. Aux deux valeurs a et $-a-3$ correspondent la même extension cubique. Par contre, à ces deux valeurs correspondent deux courbes elliptiques différentes E_a et E_{-a-3}. Les représentations ρ_a (respectivement ρ_{-a-3}) du groupe de Galois de $\bar{\mathbb{Q}}/\mathbb{Q}$ sur les points de 9-torsion de la courbe E_a (respectivement E_{-a-3}) sont réductibles et si $\rho_a = \begin{pmatrix} \chi & * \\ 0 & * \end{pmatrix}$ alors $\rho_{-a-3} = \begin{pmatrix} \chi^{-1} & * \\ 0 & * \end{pmatrix}$.

Théorème 5. *L'indice du groupe engendré par* ± 1 *et les racines du polynôme* S_{a+3} *dans le groupe des unités de* L_{a+3}*, est égal à* 3 *si seulement si* $a = -6$ *ou* 3*, ce qui correspond au sous corps réel de* $\mathbb{Q}(\zeta_9)$*.*

Preuve :

Posons $t = a+3$. Le groupe des unités U_{L_t} du corps L_t et le groupe U_1 engendré par ± 1, α et α^σ sont des $\mathbb{Z}[\zeta_3]$-modules libres de rang 1, l'opération étant définie par $\zeta_3 \epsilon = \epsilon^\sigma$ où $\epsilon \in U_{L_t}$ et $\zeta_3^3 = 1$. Comme $\mathbb{Z}[\zeta_3]$ est un anneau principal alors $U_1 = \alpha\mathbb{Z}[\zeta_3]$, et comme $\alpha \in \mathbb{Z}_K^*$ alors il existe $\theta \in \mathbb{Z}[\zeta_3]$ tel que $\alpha = \pm\theta\epsilon$ où $\epsilon \in \mathbb{Z}_K^*$. Le quotient U_{L_t}/U_1 est isomorphe comme $\mathbb{Z}[\zeta_3]$-module à $\mathbb{Z}[\zeta_3]/\theta\mathbb{Z}[\zeta_3]$, et on a $[U_{L_t} : U_1] = Norm_{\mathbb{Z}[\zeta_3]/\mathbb{Z}}(\theta)$.
Si l'indice est égal à 3 et comme $3 = (1-\zeta_3)(1-\zeta_3^2)$, il existe alors une unité η telle que $\alpha = (1-\zeta_3)\eta = \frac{-\eta}{\eta'}$, où $\eta' = \eta^\sigma$, $\eta'' = \eta^{\sigma^2}$. D'autre part, $\alpha^2\alpha^\sigma = \alpha(\alpha - 1) = -\eta^3$. Il en résulte que l'ordonnée y_{A_9} du point A_9 est un cube. En remplaçant dans **??**, on obtient l'équation suivante : $\eta^6 - a\alpha\eta^3 - \eta^3 = \alpha^3$, et en divisant par η^3, il vient

$$\eta^3 - a\alpha - 1 = (\frac{\alpha}{\eta})^3.$$

Posant le changement de variable $\omega = \frac{\alpha}{\eta}$, le point $S = (-\omega, \eta)$ est sur la courbe C_a définie par l'équation $u^3 + w^3 + 1 = auw$. Cette courbe elliptique C_a est

isogène à la courbe E_a par une isogénie ϕ qui est définie comme suit :

$$\phi : C_a \to E_a, (u, v) \mapsto (-uv, v^3),$$

le noyau de cette isogénie est le groupe engendré par le point A_3. Comme $\phi(S) = A_9$ alors $\phi^*(\phi(S)) = 3S = \phi^*(A_9)$; d'autre part, $\phi^*(3A_9) = -\phi^*(A_3) = O$. Il en résulte que le point S est d'ordre 9 sur la courbe $C_a(L_{a+3})$. Si $S = \phi^*(T)$ alors T est d'ordre 27 et on vérifie facilement que le point T engendre un groupe stable par le groupe de Galois de $\bar{\mathbb{Q}}/\mathbb{Q}$. Le couple $(E_a, < T >)$ correspond à un point de $X_0(27)(\mathbb{Q})$. La courbe modulaire $X_0(27)$ est de genre 1. Un modèle de cette courbe est donné par les fonctions modulaires x et y définies sur $X_0(27)$: $x = \dfrac{\eta^4(3\tau)}{\eta(9\tau)\eta^3(\tau)}$ et $y = 27\dfrac{\eta^3(9\tau)}{\eta^3(\tau)}$ qui vérifient l'équation

$$y^2 + 9y + 27 = x^3.$$

Cette courbe est de rang nul, donc les points rationnels sont les points de torsion sur $\mathbb{Q}$. Comme $(3, 0)$ et $(3, -9)$ sont les seuls points de torsion sur $\mathbb{Q}$, et $a - 3 = y$ alors $a = 3$ ou $a = -6$.
On peut aussi, par un calcul élémentaire directe, retrouver cette propriété : comme α est racine du polynôme $x^3 - (a + 3)x^2 + ax + 1$, on aura alors

$$\begin{aligned}\alpha^\sigma = \frac{\alpha - 1}{\alpha} = \frac{\eta'}{\eta''} &= -\eta\eta'^2 \\ = \frac{\frac{-\eta}{\eta'} - 1}{\frac{-\eta}{\eta'}} &= \frac{\eta + \eta'}{\eta},\end{aligned}$$

ce qui donne la relation suivante entre les η

$$-\eta^2\eta'^2 = \eta + \eta' = \frac{1}{\eta''^2}. \tag{2.2.1}$$

Soit $X^3 - sX^2 + bX + 1$ le polynôme minimal de η. Alors

$$tr_{L_t/\mathbb{Q}}(\eta^3) = s\ tr_{L_t/\mathbb{Q}}(\eta^2) - b\ tr_{L_t/\mathbb{Q}}(\eta) - 3 \tag{**}$$

comme $tr_{L_t/\mathbb{Q}}(\eta^3) = a^2 + 3a + 6$, $tr_{L_t/\mathbb{Q}}(\eta^2) = -s^2 + 2b$ et $tr_{L_t/\mathbb{Q}}(\eta) = s$, en remplaçant dans $**$, on déduit que

$$s^3 - 3bs - 3 = a^2 + 3a + 6. \tag{2.2.2}$$

En prenant les traces dans l'égalité **??**, on obtient $b = 0$, donc l'équation **??** devient $s^3 - 3 = a^2 + 3a + 6$. Il en résulte que le point de coordonnées (s, a)

appartient à la courbe elliptique $y^2 + 3y + 9 = x^3$ qui est une equation de la courbe modulaire $X_0(49)$, dont les points de torsion sont $(3, 3)$ et $(3, -6)$.
Le cas $a = 3$ correspond à une courbe E_a singulière. Pour $a = -6$, on a l'isogénie $E_{-6} \longrightarrow C_{-6}$, et la courbe C_{-6} est birationnellement équivalente à la courbe C'_{-6} d'équation $y^2 = x^3 - 108x^2 + 3888x - 349992$; d'autre part, il existe un isomorphisme ψ de E_0 dans C'_{-6} défini par $\psi(x, y) = (216x + 108, 36(x + 1))$; donc les courbes E_0 et C_{-6} sont isomorphes sur $\mathbb{Q}$. La courbe E_{-6} est à multiplication complexe par l'ordre de conducteur 3 du corps de discriminant -3 et la courbe E_0 d'invariant nul est à multiplication complexe par l'anneau des entiers de ce même corps. Si A_9^a désigne les points d'ordre 9 pour les courbes E_a alors $A_9^{-6} = \phi^*(A_9^0)$, ce qui prouve, en utilisant les calculs précédents, que le groupe des unités engendré par les racines de S_{-3} est d'indice 3 dans le groupe des unités engendré par les racines de S_0. On vérifie que les racines de S_0 engendrent le groupe des unités de $L_{-3} = L_0$.

Remarque 1 : On peut démontrer de la même façon que l'indice du groupe des unités engendré par ± 1 et les racines du polynôme S_{a+3} dans le groupe des unités de L_{a+3} n'est jamais égal à 7 sauf pour $a = 5$. Pour cela, on se sert d'une paramétrisation des corps L_{a+3} construite à partir du revêtement des courbes modulaires $X_1(7) \longrightarrow X_0(7)$. Si l'indice est égal à 7, alors l'unité α s'exprime en fonction de η et η'. D'autre part, α est solution du polynôme $x^3 - (n + 8)x^2 + (n + 5)x + 1$ qui est l'équation du revêtement précédent. En effet, si l'indice est égal à 7 et comme $7 = (1 - 2\zeta_3)(1 - 2\zeta_3^2)$ alors on a $\alpha = \dfrac{-\eta}{\eta'^2}$.
On obtient la relation entre les η :

$$(\eta\eta')^3 \ = \eta + \eta'^2 \ = -\frac{1}{\eta''^3} \ .$$

En passant aux traces, on a

$$tr_{K/\mathbb{Q}}(-\frac{1}{\eta''^3}) = tr_{K/\mathbb{Q}}(-\frac{1}{\eta^3}) = -s^2 + 2b + s,$$

Comme $\dfrac{-1}{\eta^3}$ a pour polynôme minimal :

$$X^3 - (b^3 + 3sb + 3)X^2 - (s^2 - 3sb - 3)X - 1,$$

alors $tr_{K/\mathbb{Q}}(-\dfrac{1}{\eta''^3}) = b^3 + 3bs + 3$, il en résulte l'équation suivante

$$s^2 + 3bs - s = -b^3 + 2b - 3,$$

en posant $X = -b$, $Y = s$, on obtient une autre équation de la courbe modulaire $X_0(49)$ qui est donnée par $Y^2 - 3XY - Y = X^3 - 2X - 3$, le point de coordonnées $(1, 2)$ est le seul point de torsion, donc $b = -1,\ s = 2$. La valeur de n se calcule en fonction de s et b

$$n + 8 = \ tr_{K/\mathbb{Q}}(\alpha) = tr_{K/\mathbb{Q}}(-\frac{\eta}{\eta'^2}) = 8,$$

ce qui donne $n = 0$, soit $a = 0$.

Remarque 5. *Si a est un entier l'application $C_a(\mathbb{Q}) \longrightarrow E_a(\mathbb{Q})$ est surjective. La démonstration fait appel à des techniques élémentaires d'arithmétiques.*

2.3 Surface elliptique modulaire associée au groupe $\Gamma_0(18) \cap \Gamma_1(6)$ et involution w_2 .

La courbe E_a aura un point d'ordre 2 rationnel sur $\mathbb{Q}(a)$ si le polynôme $P(X, a) = X^3 + (\frac{aX+1}{2})^2$ a une racine r dans $\mathbb{Q}(a)$. Considéré comme polynôme en a, il est de degré 2 de discriminant $D = -x^5$. Si $x = -t^2$ alors $a = \frac{1 \pm 2t^3}{t^2}$, en posant $m = 2t$, on obtient $a = \dfrac{4}{m^2} - m$. Le point d'ordre 2, que l'on note A_2, a pour coordonnées $(-m^2/4, -m^3/8)$, et celles du point A_6 d'ordre 6, $(2/m, 1)$. En exprimant, en fonction de m, l'invariant modulaire et le discriminant de la courbe elliptique, on obtient

$$\Delta(m) = \frac{-(m^3-1)(m^3+8)^2}{m^6}, \quad j(m) = \frac{(m^9 + 12m^6 + 48m^3 - 64)^3(m^3-4)^3}{m^{18}(m^3-1)(m^3+8)^2}.$$

En remplaçant a par $\dfrac{4}{m^2} - m$ dans l'équation **??**, on obtient :

$$m^2y^2 + (4 - m^3)xy + m^2y = m^2x^3.$$

Posant $y = \dfrac{y'}{m^6}, x = \dfrac{x'}{m^4}$, l'équation précédente se réécrit :

$$y'^2 + (4 - m^3)x'y' + m^6y' = x'^3$$

qui est l'équation de la surface modulaire associée au groupe $\Gamma_0(18) \cap \Gamma_1(6)$. On notera F_m la fibre générique, et posant $T = x' + \dfrac{m^6}{4}, Y = y' + \dfrac{(4 - m^3)x' + m^6}{2}$, on utilisera l'équation de F_m

$$Y^2 = T(T^2 - \frac{m^6 + 4m^3 - 8}{2}T + \frac{m^9(m^3+8)}{16}).$$

La courbe elliptique isogène, quotient de F_m par le sous-groupe engendré par le point d'ordre 2 de coordonnées $T = 0, Y = 0$, a pour équation

$$Y'^2 = T'\big(T'^2 + (m^6 + 4m^3 - 8)T' - 16(m^3 - 1)\big).$$

Et l'isogénie $i : F_m \longrightarrow F'_m$ est définie par

$$(T, Y) \longrightarrow \big(T' = \frac{Y^2}{T^2}, Y' = \frac{Y(T^2 - \frac{m(m^3+8)}{16})}{T^2}\big).$$

L'involution w_2 est définie sur $X_{\Gamma_0(9)\cap\Gamma_1(6)}$ et correspond à l'automorphisme

$$(F_m, A'_3, (0,0), < A'_9 >) \mapsto (F'_m, i(A'_3), i(0,0), < i(A'_9) >)),$$

où $A'_3 = (\frac{m^6}{4}, \frac{m^6}{2}), A'_9 = (T_{A_9}, Y_{A_9})$. De plus, on remarquera que l'image du point A_9 par cette isogénie est un point d'ordre 9 défini sur le même corps cubique. La courbe F'_m est isomorphe sur $\mathbb{Q}(a)$ à la courbe $E_{a|w_2}$, tel que $a|w_2 = m^2 + 2/m$, et l'isomorphisme ψ_1 de $E_{m^2+2/m}$ dans F'_m est défini par

$$\psi_1(x, y) = (4(m^2x + 1), 8m^3y + 4m^2(m^3 + 2)x + m^3)).$$

Comme $m^2 + 2/m = 4/(m/w_2)^2 - m/w_2$, et w_2 est définie sur $\mathbb{Q}(m)$ alors $m/w_2 = -2/m$. On retrouve ce résultat, en utilisant la représentation matricielle de $w_2 = \begin{pmatrix} -2 & -1 \\ 18 & 8 \end{pmatrix}$, et en exprimant m au moyen de la fonction η donnée dans le paragraphe suivant.

2.4 Unités modulaires.

Comme (T_{A_9}, Y_{A_9}) sont les coordonnées de A_9 dans le modèle F_m, on note U_1 le quotient

$$U_1 = \frac{Y_{A_9}}{2T_{A_9}},$$

alors U_1 et α sont liés par la relation suivante

$$\begin{aligned} U_1 &= \frac{-(2\alpha^2m^2 + (m^3 - 2m^2 - 4)\alpha - m^2)}{4\alpha + m^2} \\ &= \frac{-(m^2 + 2)\alpha + m + 2}{2\alpha + m - 2}, \end{aligned}$$

de plus U_1 est racine du polynôme

$$Z^3 + (m^2+m+1)Z^2 + (m-1)(m^2+m+1)Z - (m^2+m+1).$$

Si $d = (m^2+m+1)(m^2-2m+4)$, ce polynôme a pour discriminant m^2d^2. On montre aussi que $U_1^3/(m^2+m+1)$ est une unité sur $\mathbb{Z}[m]$, racine du polynôme

$$X^3 + (d-3)X^2 + (3+d(m-1))X - 1.$$

Notons $U_4 = \dfrac{Y_{4A_9}}{2T_{4A_9}}$, et posons $z = U_1/U_4 = \frac{m\alpha-2}{m\alpha+(m^2-2m+2)}$, alors z est une unité sur $\mathbb{Z}[m]$, racine du polynôme

$$P_{m-1}(X) = X^3 + ((m^2-2m+4)(m+1)-3)X^2 - (m-1)^2X - 1.$$

Le calcul des conjugués de z se déduit de l'action du groupe de Galois sur α, on a

$$\begin{aligned} z^\sigma &= \frac{-(m^2-2m+2)\alpha - m^2 + m - 2}{2\alpha + m - 2} \\ &= \frac{(m-1)\,z - 1}{(m^2-m+1)\,z + 1}, \end{aligned}$$

$$\begin{aligned} z^{\sigma^2} &= \frac{m\alpha + m^2 - 2m + 2}{m\alpha - 2} \\ &= -\frac{z+1}{(m^2-m+1)z - m + 1}. \end{aligned}$$

On remarquera que $\dfrac{z^\sigma}{z} = \dfrac{U_1^3}{m^2+m+1}$.

Proposition 8. *Les fonctions m et z sont des fonctions modulaires respectivement pour $\Gamma_1(6)\cap\Gamma_0(18)$ et $\Gamma_1(18)$ et l'on a*

$$\begin{aligned} m &= \frac{\eta^3(\tau)\,\eta(6\tau)}{\eta^3(2\tau)\,\eta(3\tau)} \\ z &= -\frac{\mathfrak{k}\left(\frac{2}{9};\tau\right)\mathfrak{k}^2\left(\frac{4}{9};\tau\right)}{\mathfrak{k}^3\left(\frac{1}{9};\tau\right)}\frac{\mathfrak{k}^2\left(\frac{1}{18};\tau\right)}{\mathfrak{k}^2\left(\frac{7}{18};\tau\right)}. \end{aligned}$$

La fonction z est une unité sur $\mathbb{Z}[m]$ racine du polynôme

$$P_{m-1}(X) = X^3 + ((m^2-2m+4)(m+1)-3)X^2 - (m-1)^2X - 1.$$

Par une démonstration analogue à celle donnée pour α on montre que z est une fonction modulaire sur $X_1(18)$. De plus ses pôles et ses zéros sont contenus dans l'ensemble pointes de $X_1(18)$, c'est donc une unité modulaire.
Comme

$$\begin{aligned} z &= \frac{Y_{A_9}}{Y_{4A_9}} \frac{T_{4A_9}}{T_{A_9}} \\ &= \frac{Y_{A_9}}{Y_{4A_9}} \frac{x_{4A_9} - x_{A_2}}{x_{A_9} - x_{A_2}}, \end{aligned}$$

et en exprimant z à l'aide des fonctions $\mathfrak{k}$ de Klein, on obtient alors :

$$\begin{aligned} z &= -\frac{\mathfrak{k}\left(\frac{2}{9};\tau\right)\left(\mathfrak{k}\left(\frac{4}{9};\tau\right)\right)^2 \mathfrak{k}\left(\frac{17}{18};\tau\right)\mathfrak{k}\left(\frac{-1}{18};\tau\right)}{\left(\mathfrak{k}\left(\frac{1}{9};\tau\right)\right)^2 \mathfrak{k}\left(\frac{8}{9};\tau\right)\mathfrak{k}\left(\frac{11}{18};\tau\right)\mathfrak{k}\left(\frac{-7}{18};\tau\right)} \\ &= -\frac{\mathfrak{k}\left(\frac{2}{9};\tau\right)\mathfrak{k}^2\left(\frac{4}{9};\tau\right)}{\mathfrak{k}^3\left(\frac{1}{9};\tau\right)} \frac{\mathfrak{k}^2\left(\frac{1}{18};\tau\right)}{\mathfrak{k}^2\left(\frac{7}{18};\tau\right)}. \end{aligned}$$

En utilisant les développements en produits infinis en q_τ des fonctions de Klein, la valeur de cette unité à la pointe infinie est égale à $\frac{\sin(2\pi/9)\sin^2(4\pi/9)\sin^2(\pi/18)}{\sin^3(\pi/9)\sin^2(7\pi/18)}$, qui est une unité cyclotomique de trace -3. On en déduit alors que la fonction m prend la valeur 1 en la pointe infinie.
Soit A_6 le point $A_3 + A_2$. On note (T_{A_6}, Y_{A_6}) et (T_{A_3}, Y_{A_3}) les coordonnées de A_6 et A_3 sur F_m, en utilisant les développements en produits infinis, on obtient l'identité suivante :

$$\begin{aligned} \frac{T_{A_3}}{T_{A_3} - T_{A_6}} &= (\frac{-m}{2})^3 \\ &= \frac{\mathfrak{k}(5/6;\tau)\mathfrak{k}^3(1/6;\tau)}{\mathfrak{k}^3(1/2;\tau)\mathfrak{k}(-1/6;\tau)} \\ &= -\frac{\mathfrak{k}^3(1/6;\tau)}{\mathfrak{k}^3(1/2;\tau)} \\ &= -(\frac{\eta^3(\tau)\eta(6\tau)}{2\eta^3(2\tau)\eta(3\tau)})^3. \end{aligned}$$

Comme la fonction m prend la valeur 1 en la pointe infinie de $X_1(18)$, il en résulte que m est égale à $\frac{\eta^3(\tau)\eta(6\tau)}{\eta^3(2\tau)\eta(3\tau)}$. Le diviseur de m est égal à $P - Q$ où $P = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ et $Q = \begin{pmatrix} 1 \\ -2 \end{pmatrix}$.
D'après le théorème **??**, la fonction m est une fonction modulaire sur $X_0(18)$, il en résulte alors que c'est aussi une fonction modulaire sur $X_{\Gamma_0(18)\cap\Gamma_1(6)}$.

2.5 Corps encore plus simples

A partir des trois racines U_1, U_4, U_7 du polynôme $X^3+(m^2+m+1)X^2+(m-1)(m^2+m+1)X-m^2-m-1$. Construisons l'élément $u=\dfrac{U_1-U_4}{U_1-U_7}$ racine du polynôme de type Shanks

$$S_{-\frac{(m+2)(m-1)}{m}+3}(X)=X^3-(\frac{(m+2)(m-1)}{m}-3)X^2-\frac{(m+2)(m-1)}{m}X+1.$$

Si on pose $s=\dfrac{(m+2)(m-1)}{m}$ alors

$$\begin{aligned} s|w_2 &= \frac{(-2/m+2)(-2/m+1)}{-2/m} \\ &= \frac{(m+2)(m-1)}{m}, \end{aligned}$$

on déduit alors que s est invariant par l'involution w_2. Comme la fonction m admet un zéro et un pôle simple, on déduit alors que la fonction s admet sur $X_0(18)$ deux zéros et deux pôles. Il en résulte que s a un zéro et un pôle simple sur $X_0(18)/w_2$, donc s est un générateur du corps des fonctions de la courbe $X_0(18)/w_2$ et l'équation liant u, s

$$u^3+(s-3)u^2-su+1=0$$

est l'équation de la courbe $X_1(18)/w_2$. Une démonstration directe de la propriété : u est invariant par w_2 est donnée dans [4].

2.6 Spécialisations.

Si on donne à m des valeurs entières les racines du polynôme P_m définissent en général une extension cubique cyclique de $\mathbb{Q}$, qu'on notera L_m. Si $m=0$ le polynôme $P_0=(X-1)(X+1)^2$ et si $m\neq 0$ le polynôme est irréductible. Si $m=1$ ou $m=-2$ ($a=3$), on obtient le même corps L_m, sous corps réel du corps des racines 9èmes de l'unité, ce qui correspond au corps de définition des pointes $\begin{pmatrix}1\\9\end{pmatrix}, \begin{pmatrix}4\\9\end{pmatrix}, \begin{pmatrix}2\\9\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}5\\0\end{pmatrix}, \begin{pmatrix}7\\0\end{pmatrix}$ de $X_1(18)$. La valeur de la fonction modulaire z en ces pointes est une unité cyclotomique. Si $m=-1$ ou $m=2$, on obtient le même corps, le sous corps réel des racines 7èmes de l'unité, et les deux courbes E_{-1} et E_2 sont 2-isogènes.
Il existe exactement deux valeurs de m, $m=18$, et -19 pour lesquelles $m^2+m+1=u^3$, $u\in\mathbb{Z}$ et $\neq\pm 1$. Pour ces deux valeurs $u=7$. Les corps L_{18}

et L_{-19} correspondants ont pour discriminants respectivement 73^2 et $13^2.31^2$. Pour ces corps l'élément $U_1/7$ est unité, racine respectivement des polynômes $X^3+49X^2+119X-1$ et $X^3+49X^2-140X-1$. Un calcul fait avec pari/GP montre que $U_1/7$ et $U_1^\sigma/7$ engendrent le groupe des unités de norme 1 et $\langle z, z^\sigma\rangle$ est un sous-groupe d'indice 3 de ce groupe.
L'arithmétique des corps L_m a été étudiée dans [**?**]. On définit δ par $\delta = 0$ si $m \not\equiv 1 \bmod 3$, et $\delta = 1$ si $m \equiv 1 \bmod 3$ et on pose $D(m) = d/9^\delta = (m^2+m+1)(m^2-2m+4)/9^\delta$. Si on écrit $d = bc^3$ avec b sans facteurs cubiques, le discriminant de L_m est égal à $81^\delta \prod_{p|b,p\geq 5} p^2$ [**?**]. Si $D(m)$ est sans facteurs carrés, il est montré dans [**?**] que le groupe des unités de L_m est engendré par $-1, z, z^\sigma$. Dans le reste du paragraphe, nous nous restreindrons à ces cas. Le paragraphe suivant montre qu'il existe une infinité de corps L_m ($m \in \mathbb{Z}$) qui ne sont pas de type Shanks S_a avec $a \in \mathbb{Z}$.

2.6.1 Monogénéité

Proposition 9. *Si $m \neq -1$ et $D(m)$ est sans facteurs carrés, aucun générateur de l'extension L_m n'est racine d'un polynôme S_t avec $t \in \mathbb{Z}$. Pour ces corps l'anneau des entiers n'est pas monogéne c'est à dire n'est pas de la forme $\mathbb{Z}[v]$, $v \in L_m$. Enfin il existe une infinité de tels corps.*

Preuve : Soit $u \in L_m$ racine d'un polynôme S_t avec $t \in \mathbb{Z}$, alors u est une unité et donc un élément du groupe engendré par $\pm 1, z, z^\sigma$. Si $\mathfrak{P}$ est un idéal premier de L_m au dessus d'un premier p divisant m, alors en utilisant la congruence $P_m(X) \equiv (X-1)(X+1)^2 \bmod m$ on montre que z et z^σ sont congrus à $\pm 1 \bmod \mathfrak{P}$. Il en résulte que les traces des unités sont congrues à ± 3 et $\pm 1 \bmod p$. La relation $trace(u - \frac{1}{u}) = 3$ ne peut être vérifiée.
Si l'anneau des entiers est de la forme $\mathbb{Z}[v]$ alors $u_v = \frac{v-v^\sigma}{v-v^{\sigma^2}}$ est un entier racine d'un polynôme S_t, $t \in \mathbb{Z}$, ce qui montre la deuxième partie de la proposition.
Utilisons une méthode classique([**?**], p. 454) adaptée avec l'aide de J. Oesterlé, pour montrer qu'il existe une infinité d'entiers positifs m tels que $D(m)$ soit sans facteurs carrés.
Soit N un entier positif. Si $m = 6n+3$ avec $0 \leq n \leq N$ et que $(m^2+m+1)(m^2-2m+4)$ a des facteurs carrés alors m^2+m+1 et m^2-2m+4 sont premiers entre eux et m^2+m+1 ou m^2-2m+4 est multiple du carré d'un nombre premier p compris entre 7 et $6N$. Si $D(m)$ est divisible par un carré, alors en utilisant le lemme de Hensel $m^2+m+1 \equiv 0 \bmod p^2$ ou $m^2-2m+4 \equiv 0 \bmod p^2$, d'après le théorème chinois il existe exactement 4 valeurs m_i dans l'intervalle $[0, p^2-1]$ telles que $m \equiv m_i \bmod p^2$. Comme $m \equiv 3 \bmod 6$, on déduit alors qu'il existe m_i' tel que $m \equiv m_i' \bmod 6p^2$.

Notons $r_p(N)$ le nombre d'entiers m de la forme $6n+3$ tels que $D(m)$ soit multiple de p^2. On a donc

$$\begin{aligned} r_p(N) &= \sum_{n\leq N,\ D(6n+3)\ \equiv\ 0 \bmod p^2} 1 \\ &\leq \left(1+\left[\frac{N}{p^2}\right]\right) \sum_{D(m_i')\ \equiv\ 0 \bmod p^2,\ m_i'\in[0,6p^2-1]} 1, \end{aligned}$$

Comme il existe exactement 4 entiers $m_i' = 6n_i + 3$ dans $[0, 6p^2 - 1]$ tels que $D(m_i') \equiv 0 \bmod p^2$. On a donc $r_p(N) \leq 4\left(1+\left[\frac{N}{p^2}\right]\right) \leq 4\left(1+\frac{N}{p^2}\right)$. Le nombre d'entiers positifs $r(N)$ de la forme $6n+3$ avec $0 \leq n \leq N$ tels que $D(m)$ soit sans facteurs carrés sera égal à $N - \sum_{p\geq 7,\ p\ \equiv\ 1 \bmod 6} r_p(N)$. De plus on a la minoration

$$\begin{aligned} r(N) &\geq N - 4 \sum_{p\geq 7,\ p\ \equiv\ 1 \bmod 6} 1 - 4N \sum_{p\geq 7,\ p\ \equiv\ 1 \bmod 6} p^{-2} \\ &\geq N\left(1 - 4 \sum_{p\geq 7,\ p\ \equiv\ 1 \bmod 6} \frac{1}{p^2}\right) + o(N). \end{aligned}$$

Comme

$$\begin{aligned} 4 \sum_{p\geq 7,\ p\ \equiv\ 1 \bmod 6} \frac{1}{p^2} &\leq 2\sum_{n=1}^{\infty} \frac{1}{(6n-1)^2} + \frac{1}{(6n+1)^2} \\ &= 2(\frac{\pi^2}{6} - \frac{1}{4}\frac{\pi^2}{6} - \frac{1}{9}\frac{\pi^2}{8} - 1) \\ &\leq 0.2, \end{aligned}$$

il en résulte que $r(N) \geq 0.8N + o(N)$, d'où $r(N)$ tend vers l'infini si N tend vers l'infini.

Proposition 10. *Pour $m \neq \pm 1, \pm 2$, l'anneau des entiers du corps L_m n'est pas monogène.*

Preuve : Comme nous l'avons vu, la norme de U_1 est égal à $m^2 + m + 1$. On écrit $m^2 + m + 1 = 3^\delta b_1 c_1^3$ avec b_1 sans facteurs cubiques. Si $b_1 \neq \pm 1$, la décomposition de l'idéal principal (U_1/c_1) donne une relation, dans le groupe des classes d'idéaux, entre certains idéaux ramifiés divisant m^2+m+1. Notons $\mathfrak{P}_3$ un idéal au dessus de 3. Si l'anneau des entiers de L_m est monogène l'idéal $\mathfrak{P}_3 \prod_{\mathfrak{P} \text{ ramifié}} \mathfrak{P}$ est un idéal principal et on obtient ainsi la seule relation liant

tous les premiers ramifiés dans le groupe des classes d'idéaux [**?**]. Si les deux relations ainsi obtenues sont non triviales et différentes, alors l'anneau n'est pas monogène. L'étude des points rationnels des courbes elliptiques d'équations $Y^2+Y+1=X^3$ et $Y^2+Y+1=3X^3$ montre que les seuls entiers m tels que $m^2+m+1=3^\delta u^3$ avec $u\in\mathbb{Z}$, sont $m=\pm 1, 18, -19$. De même on montre que les seuls m tels que $m^2-2m+4=3^\delta.4^\alpha u^3$ avec $\alpha=0$ ou 1 sont $m=\pm 2, -36, 38$. Si $m\neq 1, 18, -19, \pm 2, -36, 38$ les deux relations sont différentes et l'anneau des entiers de L_m n'est pas monogène.
Si $m=-36$ et 38 un calcul avec pari/GP montre que le groupe des unités de norme positive est engendré par z et z^σ. Enfin pour $m=18, -19, -36,$ et 38, l'anneau des entiers de L_m n'est pas monogène. Pour cela on utilise un critère de [**?**] : si $s=Trace(\epsilon)$ et $t=Trace(1/\epsilon)$, avec $\epsilon, \epsilon^\sigma$ générateurs du groupe des unités de norme 1 alors $s+t\ \equiv\ 1 \bmod 2$ et $s+t+3\ \equiv\ 1 \bmod C$ où C est le conducteur du corps.

2.7 Formule analytique pour le régulateur.

2.7.1 Calcul de $\log|m|$.

Soit $\tau=x+iy$, tel que $y>0$. Considérons les fonctions $E_{u,0}(\tau,s)$ définies par les séries

$$E_{u,0}(\tau,s)=\sum_{(a,b)\neq(0,0)} e^{2i\pi au}\frac{y^s}{|a\tau+b|^{2s}},$$

avec $\Re(s)>1$. En choisissant $u=k/18$, on posera $\xi=e^{2i\pi/18}$, $E_{k/18,0}(\tau,s)=E_k(s)$ ce qui donne

$$E_k(s)=\sum_{(a,b)\neq(0,0)} \xi^{ka}\frac{y^s}{|a\tau+b|^{2s}}.$$

D'après la deuxième formule limite de Kronecker, les fonctions E_k se prolongent en des fonctions holomorphes et leurs valeurs en $s=1$ est égale à

$$-2\pi ln|2\pi\eta^2(\tau)\mathfrak{k}(k/18;\tau)|.$$

En utilisant l'expression de la fonction m en fonction des formes de Klein écrites dans le réseau $[1,\tau]$, on obtient :

$$(-\frac{m}{2})^3 \ = \ \frac{\mathfrak{k}\left(\frac{5}{6};\tau\right)\left(\mathfrak{k}\left(\frac{1}{6};\tau\right)\right)^3}{\mathfrak{k}\left(\frac{-1}{6};\tau\right)\mathfrak{k}\left(\frac{1}{2};\tau\right)^3},$$

donc en passant au logarithme, on a alors :

$$\begin{aligned} 3\log|m/2| &= -\frac{1}{2\pi}\lim_{s\to 1}(E_{15}(s)+3E_3(s)-E_{-3}(s)-3E_9(s)) \\ &= -\frac{1}{2\pi}\lim_{s\to 1}\sum_{(a,b)\neq(0,0)}(\xi^{15a}+3\xi^{3a}-\xi^{-3a}-3\xi^{-9a})\frac{y^s}{|a\tau+b|^2} \\ &= -\frac{9}{2\pi}\lim_{s\to 1}\sum_{(a,b)\neq(0,0)}(-1)^{a-1}\chi_1(a)\frac{y^s}{|a\tau+b|^{2s}}. \end{aligned}$$

où χ_1 est le caratère trivial modulo 9. On déduit alors

$$\log|m| = \frac{-3y}{2\pi}\lim_{s\to 1}\sum_{(a,b)\neq(0,0)}\frac{(-1)^{a-1}\chi_1(a)}{|a\tau+b|^{2s}} - \log 2.$$

2.7.2 Calcul du régulateur.

Le régulateur du système d'unités $\{z, z^\sigma\}$ s'exprime en fonction de $\tau = x+iy$, quotient de périodes de la courbe elliptique E_m.

Théorème 6. *Soient $\zeta = e^{2\pi i/18}$, $\mu = 5\zeta^3 - 1$, et les deux caractères χ et θ définis respectivement sur $(\mathbb{Z}/9\mathbb{Z})^*$ et $(\mathbb{Z}/18\mathbb{Z})^*$ par $\chi(2) = -\zeta^3$ et $\theta(5) = \zeta^6$. Le régulateur R du système d'unités $\{z, z^\sigma\}$ est donné par la formule suivante :*

$$R = (\ln|z| - \zeta^6\ \ln|z^\sigma|)(\ln|z| - \zeta^{12}\ \ln|z^{\sigma^2}|),$$

où

$$\ln|z| - \zeta^6\ \ln|z^\sigma| = \frac{-3\zeta^2}{2\pi}\lim_{s\to 1}\sum_{(a,b)\neq(0,0)} y^s\frac{\zeta^{15}\mu\chi(a)+4\theta(a)}{|a\tau+b|^{2s}}.$$

Preuve : En utilisant les expressions des fonctions z et z^σ en fonction des formes de Klein écrites dans le réseau $[1,\tau]$.

$$\begin{aligned} z &= \frac{\mathfrak{k}\left(\frac{2}{9};\tau\right)\left(\mathfrak{k}\left(\frac{4}{9};\tau\right)\right)^2\mathfrak{k}\left(\frac{17}{18};\tau\right)\mathfrak{k}\left(\frac{-1}{18};\tau\right)}{\left(\mathfrak{k}\left(\frac{1}{9};\tau\right)\right)^2\mathfrak{k}\left(\frac{8}{9};\tau\right)\mathfrak{k}\left(\frac{11}{18};\tau\right)\mathfrak{k}\left(\frac{-7}{18};\tau\right)} \\ z^\sigma &= \frac{\mathfrak{k}\left(\frac{8}{9};\tau\right)\mathfrak{k}\left(\frac{7}{9};\tau\right)\right)^2\mathfrak{k}\left(\frac{5}{18};\tau\right)\mathfrak{k}\left(\frac{23}{18};\tau\right)}{\left(\mathfrak{k}\left(\frac{4}{9};\tau\right)\right)^2\mathfrak{k}\left(\frac{5}{9};\tau\right)\mathfrak{k}\left(\frac{-1}{18};\tau\right)\mathfrak{k}\left(\frac{17}{18};\tau\right)}. \end{aligned}$$

On obtient alors

$$ln|z| = \frac{-1}{2\pi}\lim_{\substack{s\to 1\\(a,b)\neq(0,0)}}\sum(\zeta^{4a}+2\zeta^{8a}-2\zeta^{2a}-\zeta^{16a}+\zeta^{17a}+\zeta^{-a}-\zeta^{11a}-\zeta^{-7a})\frac{y^s}{|a\tau+b|^{2s}}.$$

$$ln|z^\sigma| = \frac{-1}{2\pi} \lim_{\substack{s\to 1 \\ (a,b)\neq(0,0)}} \sum (\zeta^{16a} + 2\zeta^{14a} - 2\zeta^{8a} - \zeta^{10a} + 2\zeta^{5a} - 2\zeta^{-a}) \frac{y^s}{|a\tau + b|^{2s}}.$$

On en déduit alors que :

$$ln|z| - \zeta^6\ ln|z^\sigma| =$$
$$\frac{-1}{2\pi} \lim_{\substack{s\to 1 \\ (a,b)\neq(0,0)}} \sum (\zeta^{4a} + \zeta^a + \zeta^{7a+6} + \zeta^{a+15} + \zeta^{-4a} + \zeta^{-a} + \zeta^{-7a+6} + \zeta^{-a+15}) \frac{y^s}{|a\tau + b|^{2s}}.$$

Le tableau suivant regroupe les différentes valeurs du coefficient t_i qui précède $\frac{y^s}{|a\tau+b|^{2s}}$ où $a = i$ ou $18 - i$:

$t_1 = -3\zeta^5$	$t_4 = 3\zeta^2(-4\zeta^3 + 5)$	$t_7 = -3/\zeta$
$t_2 = 3\zeta^2(5\zeta^3 - 1)$	$t_5 = 3\zeta^2$	$t_8 = 3\zeta^2(-\zeta^3 - 4)$
$t_3 = 0$	$t_6 = 0$	$t_9 = 0$

il en résulte la formule donnée dans le théorème.
on calcule de même $ln|z| - \zeta^{12} ln|z^\sigma|$. Comme précédemment, les valeurs du coefficient t'_i qui précède $\dfrac{y^s}{|a\tau + b|^{2s}}$ où $a = i$ ou $18 - i$:

$t'_1 = 3\zeta^4$	$t'_4 = 3\zeta(-\zeta^3 + 5)$	$t'_7 = -3\zeta$
$t'_2 = -3\zeta(4\zeta^3 + 1)$	$t'_5 = 3\zeta^{-2}$	$t'_8 = 3\zeta(5\zeta^3 - 4)$
$t'_3 = 0$	$t'_6 = 0$	$t'_9 = 0$

En multipliant les deux facteurs $ln|z| - \zeta^6\ ln|z^\sigma|$ et $ln|z| - \zeta^{12}\ ln|z^\sigma|$, on obtient :

$$\begin{aligned} &9(A_1^2 + A_5^2 + A_7^2) + 189(A_2^2 + A_4^2 + A_8^2) - 81(A_2A_1 + A_4A_7 + A_5A_8) \\ &+27(A_4A_1 + A_7A_8 + A_2A_5) + 54(A_1A_8 + A_2A_7 + A_4A_5) \\ &-9(A_1A_5 + A_1A_7 + A_5A_7) - 189(A_2A_4 + A_4A_8 + A_8A_2). \end{aligned}$$

où $A_i = \displaystyle\sum_{a \equiv i \bmod 18} \frac{y^s}{|a\tau + b|^{2s}}$.

2.8 Calcul d'un équivalent du régulateur.

Proposition 11. *Quand m est réel et tend vers $\pm\infty$, le régulateur R est équivalent à la quantité $7\log^2|m|$.*

Preuve :
La fonction modulaire m n'a qu'un seul pôle sur $X_0(18)$ en la pointe $\frac{-1}{2}$. Soit Δ_{18} un domaine fondamental pour le groupe $\Gamma_0(18)$ image, par un système de représentants comprenant la matrice $g = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$, de $SL_2(\mathbb{Z})$ modulo $\Gamma_0(18)$, du domaine fondamental de $SL_2(\mathbb{Z})$: $\Delta = \{u \in \mathcal{H} : |Re(u)| \leq 1/2,\ |u| \geq 1\}$. Si m est réel et tend vers $+\infty$, il existe un $\tau \in \Delta_{18}$ tel que $m = m(\tau)$ et τ tend vers $\frac{1}{2}$. En utilisant la proposition suivante

Proposition 12. *Soit E une courbe elliptique sur $\mathbb{R}$ et j son invariant modulaire. Alors il existe un unique τ dans l'ensemble*

$$\mathcal{C} = \{it : t \geq 1\} \cup \{e^{i\theta} : \pi/3 \leq \theta \leq \pi/2\} \cup \{1/2 + it : t \geq \sqrt{3}/2\}$$

tel que

$$j(\tau) = j(E).$$

Si $m \geq 4^{1/3}$ l'invariant modulaire de la courbe elliptique F_m est un nombre réel négatif, τ décrit la demi-droite $\{-\frac{1}{2} + iu; u \geq \frac{1}{2\sqrt{3}}\}$, c'est l'image par la matrice g de la demi-droite $\{\frac{1}{2} + it; t \geq \frac{\sqrt{3}}{2}\}$. On pose alors $\tau = g\tau'$ et $\tau' = \frac{1}{2} + it$, avec t qui tend vers $+\infty$. rappelons la propriété de $\mathfrak{k}(u;\tau)$

$$\mathfrak{k}(a_1\tau + a_2, \tau) = \mathfrak{k}(a_1\tau + a_2, [1,\tau]) = \frac{1}{-2\tau' + 1}\mathfrak{k}((a_1 - 2a_2)\tau' + a_2, [1,\tau']),$$

on obtient alors

$$|z| = |\frac{\mathfrak{k}(4\tau'/9 + 7/9;\tau')\mathfrak{k}^2(\tau'/9 + 4/9;\tau')\mathfrak{k}^2(\tau'/9 + 17/18;\tau')}{\mathfrak{k}^3(2\tau'/9 + 8/9;\tau')\mathfrak{k}^2(2\tau'/9 + 7/18;\tau')}|,$$

$$|z^\sigma| = |\frac{\mathfrak{k}(2\tau'/9 + 8/9;\tau')\mathfrak{k}^2(4\tau'/9 + 7/9;\tau')\mathfrak{k}^2(4\tau'/9 + 5/18;\tau')}{\mathfrak{k}^3(\tau'/9 + 4/9;\tau')\mathfrak{k}^2(\tau'/9 + 17/18;\tau')}|,$$

$$|\frac{-m}{2}|^3 = |\frac{\mathfrak{k}(\tau'/3 + 5/6;\tau')}{\mathfrak{k}^3(1/2;\tau')}|.$$

D'autre part, si m tend vers $+\infty$ le comportement de $\log|z|$ se déduit du lemme suivant

Lemme 1. *Soit Δ' le domaine fondamental de $SL_2(\mathbb{Z})$ et $\tau' \in \Delta'$. Soit $a = a_1\tau' + a_2$ tel que $0 \leq a_1 \leq 1/2$ et $0 \leq a_2 \leq 1$. Alors*

$$\log|\mathfrak{k}(a_1\tau' + a_2)| = \pi a_1(a_1 - 1)Im\tau' + \log|1 - e^{2\pi(a_1\tau + a_2)i}| + \psi(\tau'),$$

où ψ est une fonction bornée sur Δ'.

On obtient l'égalité suivante :

$$\log|z| \quad = \quad \frac{2\pi}{9}t + \nu(t),$$

où ν est une fonction bornée quand t tend vers $+\infty$.
De même,

$$\log|z^\sigma| = \frac{-2\pi}{3}t + \nu_1(t),$$
$$\log|m| = \frac{-2\pi}{9}t + \nu_2(t),$$

où les fonctions ν_1 et ν_2 sont des fonctions bornées quand t tend vers $+\infty$. On en déduit alors que R est équivalent à $7\log^2|m|$.

De même, si m est réel et tend vers $-\infty$, l'invariant modulaire de la courbe F_m est un nombre réel positif, τ décrit un arc de cercle centré au point $-1/4$ et d'extrémité $1/2$, image par la matrice g de la demi-droite $\{it; t \geq 1\}$. On pose alors $\tau = g\tau'$ et $\tau' = it$. De la même manière, on montre que

$$\log|z| \quad = \quad \frac{2\pi}{9}t + \nu(t),$$

et on déduit que le régulateur est équivalent à $7\log^2|m|$.

2.9 Involutions d'Atkin-Lehner.

Sur la courbe modulaire $X_0(9)$, il existe une involution qu'on notera w_9 dont la représentation matricielle est la suivante : $w_9 = \frac{1}{3}\begin{pmatrix} 0 & -1 \\ 9 & 0 \end{pmatrix}$. En utilisant l'expression de a en fonction des fonctions η, on en déduit que $a|w_9 - 3 = \frac{27}{a-3}$,

soit $a|w_9 = a' = 3\dfrac{a+6}{a-3}$. La courbe modulaire $X_0(18)$ admet trois involutions w_2 déja calculée, w_9 et $w_{18} = w_2 \circ w_9$. Comme m est un générateur du corps de fonction de $X_0(18)$, et w_9 est un automorphisme de $X_0(18)$ alors il existe γ dans $GL_2(\mathbb{C})$ tel que $m|w_9 = \gamma m$. En exprimant a en fonction de m et comme w_9 est défini sur $\mathbb{Q}(m)$, on obtient $m|w_9 = \dfrac{m+2}{m-1}$.
Soit E' la courbe elliptique, obtenue par quotient de E_a par le sous-groupe engendré par le point A_9 d'ordre 9. Pour trouver l'équation de la courbe E', rappelons la méthode de [De], étant donnée une courbe elliptique d'équation

$$y^2 = F(x) = x^3 + Ax + B,$$

où $(A, B) \in \mathbb{Q}$. Si les abscisses du noyau d'une isogénie cyclique engendrée par M, d'ordre impair, définie sur $\mathbb{Q}$, sont les racines d'un polynôme $h(x) \in \mathbb{Q}[x]$, alors l'isogénie est donnée par les relations

$$X = 9x - 2F'(\frac{h'}{h}) - 4F(\frac{h'}{h})' - 2p_1^{(h)},$$

$$Y = y\frac{dX}{dx},$$

où $p_i^{(h)}$ désigne la somme des racines (dans $\overline{K}$) à la puissance i du polynôme h. L'équation de la courbe isogène est la suivante :

$$Y^2 = X^3 + (A - 5(6p_2^{(h)} + 2Ap_0^{(h)}))X + B - 7(10p_3^{(h)} + 6Ap_1^{(h)} + 4Bp_0^{(h)}).$$

Pour la courbe elliptique E_a, on a $h(x) = xS_{a+3}(x)$ et l'équation de la courbe quotient est la suivante :

$$Y^2 = X^3 + \overline{A}X + \overline{B},$$

où

$$\overline{A} = -\frac{(a+6)(a^3 + 234a^2 + 756a + 2160)}{48},$$

$$\overline{B} = \frac{1}{864}a^6 - \frac{7}{12}a^5 - \frac{77}{4}a^4 - \frac{1139}{8}a^3 - \frac{1197}{2}a^2 - 1323a - \frac{6831}{4}.$$

de discriminant $(a^2+3a+9)(a-3)^9$. En posant $X' = X - \dfrac{(a+6)^2}{4}$, l'équation de la courbe devient

$$Y^2 = X'^3 - \frac{1}{108}(-9(a+6)X' + (a-3)^3)^2.$$

Contrairement à l'involution w_2 la courbe E' isogène à E_a n'est pas isomorphe sur $\mathbb{Q}(a)$ à la courbe $E_{a|w_9}$, mais est une tordue de $E_{a|w_9}$ par $\sqrt{-3}$.

Les points d'abscisses 0 sont définis sur $\mathbb{Q}(\sqrt{-3})$ et sont d'ordre 3. Les abscisses β des points N de 9-torsion tels que $3N = (0, *)$ sont racines du polynôme

$$S_{wa} : X^3 + (2a+3)(a-3)X^2 + \frac{1}{3}(a+6)(a-3)^3 - \frac{1}{27}(a-3)^6.$$

Les ordonnées sont dans le corps de degré 6 obtenu en rajoutant $\sqrt{-3}$. Si β est une racine de S_{wa}, on constate que le corps composé $\mathbb{Q}(a)(\alpha, \beta)$ contient le sous corps réel des racines 9èmes de l'unité i.e L_1 ou L_{-2}.

2.9.1 Différentes courbes elliptiques

Considérons la famille de courbes elliptiques d'équation :

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

en effectuant le changement de variables $x = -(m-1) - mz$, on obtient la famille de coubes elliptiques

$$y^2 = z^3 - \frac{(m-1)(m+2)}{m}z^2 - \frac{(m-1)^2 - 3}{m}z + 1.$$

En remplaçant le paramétre m par $m|w_9$, on construit une extension cubique engendrée par les racines du polynôme

$$z^3 - 9\frac{m}{(m+2)(m-1)}z^2 - 3\frac{m^2 - 2m - 2}{(m+2)(m-1)}z + 1$$

Par spécialisation ($m \in \mathbb{Z}$), il ne semble pas possible de construire un groupe d'unités d'indice fini et paramétrées.

Chapitre 3

Arithmétique d'une famille de corps cubiques

Dans ce chapitre, on commence par rappeler quelques résultats sur les corps de nombres. Puis, on s'interesse à l'étude de quelques propriétés arithmétiques d'une famille de corps cubiques engendré par une racine du polynôme

$$P_n(X) = X^3 - (n^3 - 2n^2 + 3n - 3)X^2 - n^2X - 1.$$

Si on pose $m = n - 1$ et $m \in \mathbb{Z}$, en utilisant la construction modulaire décrite dans le chapitre 2, on construit cette famille de corps cubiques.
Si $n \in \mathbb{Z}$, une autre contruction de cette famille de corps de nombres est donnée dans [**?**] par L.C. Washington. Pour trouver cette famille, il considére les couples (a, b) tel que le discriminant du polynôme $X^3 - aX^2 - bX - 1$ soit un carré. Si l'extension $K/\mathbb{Q}$ est cubique cyclique et si σ engendre le groupe de Galois et si $x \in K$ et $x \notin \mathbb{Q}$ alors $1, x, \sigma(x)$ et $x\sigma(x)$ sont $\mathbb{Q}-$linéairement dépendants. Il existe donc $g \in Gl_2(\mathbb{Q})$ tel que $\sigma(x) = \frac{ax+b}{cx+d} = g.x$. De plus g est un élément d'ordre 3 de $PGl_2(\mathbb{Q})$. Washington détermine g telle que $X.(g.X)(g^2.X) = \frac{P(X)}{Q(X)}$ avec $P - Q \in \mathbb{Z}[\mathbb{X}]$ soit un polynôme unitaire.

3.1 Généralités et résultats

Soit k un corps de nombres. On désigne par $[k : \mathbb{Q}]$ son degré. L'anneau des entiers de k, que l'on note $\mathbb{Z}_k$, est un anneau de Dedekind. Le discriminant d'une base de $\mathbb{Z}_k$, est appelé le discriminant du corps, que l'on note D_k. On appelle signature du corps k le couple d'entiers (r_1, r_2) tel que $r_1+2r_2 = [k : \mathbb{Q}]$, où r_1 est le nombre de plongements réels et $2r_2$ est le nombre de plongements complexes. Le groupe des éléments inversibles de $\mathbb{Z}_k$ est appelé le groupe des unités de k, que l'on note U_k. D'après le théorème de Dirichlet, c'est un $\mathbb{Z}$-module de rang $r = r_1 + r_2 - 1$. Si $k/\mathbb{Q}$ est une extension galoisienne, on notera

par $Gal(k/\mathbb{Q})$ son groupe de Galois.
Soit α un entier de k, on définit l'indice de α, que l'on note $I(\alpha)$ par :

$$I(\alpha) = [\mathbb{Z}_k : \mathbb{Z}[\alpha]],$$

où $[\mathbb{Z}_k : \mathbb{Z}[\alpha]]$ est l'indice de $\mathbb{Z}[\alpha]$ dans $\mathbb{Z}_k$.
On appelle discriminant du système $(\alpha_1, \alpha_2, \cdots, \alpha_{n-1}) \in K$ le nombre (rationnel)

$$D(\alpha_1, \alpha_2, \cdots, \alpha_{n-1}) = \det(\sigma_i(\alpha_j))^2 = \det\left(Tr_{K/\mathbb{Q}}(\alpha_i\alpha_j)\right).$$

Soit G le polynôme irréductible unitaire de α de degré n. on appelle discriminant du polynôme $G(X)$ l'entier

$$D(G) = D(\alpha) = D(1, \alpha, \cdots, \alpha^{n-1}).$$

On déduit alors la relation qui lie le discriminant de α à son indice :

$$D(\alpha) = I(\alpha)^2 D_k. \tag{3.1.1}$$

Définition 18. *On appelle ordre de k un sous anneau de k, qui considéré comme $\mathbb{Z}$-module, est de type fini et de rang maximal $n = [k : \mathbb{Q}]$.*

Il est clair que l'anneau des entiers $\mathbb{Z}_k$ de k est un ordre. De plus, si $\alpha \in \mathcal{O}$ où $\mathcal{O}$ est un ordre de k, alors α est un entier algébrique de k, donc $\alpha \in \mathbb{Z}_k$. Ainsi pour tout ordre $\mathcal{O}$ de k, on a $\mathcal{O} \subseteq \mathbb{Z}_k$, donc $\mathbb{Z}_k$ est l'ordre maximal de k.

Définition 19. *Soient $\mathcal{O}$ un ordre d'un corps de nombres k, p un nombre premier.*
1) On dira que $\mathcal{O}$ est p-maximal si $[\mathbb{Z}_k : \mathcal{O}]$ n'est pas divisible par p.
2) On définit le p-radical I_p comme suit :

$$I_p = \{x \in \mathcal{O} / \exists m \geq 1, x^m \in p\mathcal{O}\}$$

Définition 20. *Soient $\mathcal{O}$ un ordre et $\{x_1, x_2, \cdots, x_n\}$ une base de O, considéré comme sous $\mathbb{Z}$-module du $\mathbb{Z}$-module libre $\mathbb{Z}_k$, le discriminant de $\mathcal{O}$, que l'on note $disc(\mathcal{O})$ est défini par :*

$$disc(\mathcal{O}) = D(x_1, x_2, \cdots, x_n)$$

où $D(x_1, x_2, \cdots, x_n)$ est le discriminant du système $\{x_1, x_2, \cdots, x_n\}$.

Théorème 7. *Soient $\mathcal{O}$ un ordre du corps de nombre k et p un nombre premier. Soit $\mathcal{O}' = \{x \in k / xI_p \subset I_p\}$, alors soit $\mathcal{O}' = \mathcal{O}$, dans ce cas $\mathcal{O}$ est p-maximal ou $\mathcal{O} \subset \mathcal{O}'$ tel que p divise $[\mathcal{O}' : \mathcal{O}]$ et $[\mathcal{O}' : \mathcal{O}]$ divise p^n.*

Théorème 8. *(critère de Dedekind) Soit θ un entier, $k = \mathbb{Q}(\theta)$ un corps de nombres ; $T \in \mathbb{Z}[X]$ le polynôme irréductible unitaire de θ, et soit p un nombre premier. Soit $\overline{T}(X) = \prod_1^k \overline{t_i}(X)^{e_i}$ la factorisation de $T(X)$ modulo p dans $\mathbb{F}_p[X]$, et $g(X) = \prod_1^k t_i(X)$ où $t_i \in \mathbb{Z}[X]$ sont des relèvements unitaires arbitraires de $\bar{t}_i$. Alors*
(1) le p-radical I_p de $\mathbb{Z}[\theta]$ en p est donné par :

$$I_p = p\mathbb{Z}[\theta] + g(\theta)\mathbb{Z}[\theta].$$

(2)Soit $h(x) \in \mathbb{Z}[X]$ le relèvement unitaire de $\frac{\overline{T}(X)}{\overline{g}(X)}$ et soit

$$f(X) = (g(X)h(X) - T(X))/p$$

alors $\mathbb{Z}[\theta]$ est p-maximal si et seulement si$(\overline{f}, \overline{g}, \overline{h}) = 1$ dans $\mathbb{F}_p[X]$.
*(3) Plus généralement, soit $\mathcal{O}'$ un ordre donné par le théorème **??** si $\mathcal{O} = \mathbb{Z}[\theta]$. Alors, si U est le relèvement unitaire de $\overline{T}/(\overline{f}, \overline{g}, \overline{h})$ de $\mathbb{Z}[X]$, nous avons*

$$\mathcal{O}' = \mathbb{Z}[\theta] + \frac{1}{p}U(\theta)\mathbb{Z}[\theta]$$

et si $m = deg(\overline{f}, \overline{g}, \overline{h})$ alors $[\mathcal{O}' : \mathbb{Z}[\theta]] = p^m$, ainsi $disc(\mathcal{O}') = disc(T)/p^{2m}$.

Définition 21. *Soit L le corps de décomposition du polynôme P dans $\mathbb{C}$. On appelle groupe de Galois de P, que l'on note $Gal(P)$, le groupe de Galois de L sur $\mathbb{Q}$.*

Proposition 13. *Soit θ un entier algébrique de degré 3, $k = \mathbb{Q}(\theta)$ une extension cubique . Alors l'extension $k/\mathbb{Q}$ est une extension cubique, cyclique si et seulement si le discriminant de P est un carré.*

Théorème 9. *Soit θ un entier, $k = \mathbb{Q}(\theta)$ un corps de nombres ; $T \in \mathbb{Z}[X]$ le polynôme irréductible unitaire de θ, et soit p un nombre premier qui ne divise pas f, où $f = [\mathbb{Z}_k : \mathbb{Z}[\theta]]$. Soit*

$$T(X) \equiv \prod_{1 \le i \le g} T_i^{e_i}(X) \mod p,$$

la décomposition de T en facteurs irréductibles dans $\mathbb{F}_p[X]$, où T_i sont unitaires. Alors la décomposition de l'idéal $p\mathbb{Z}_k$ en idéaux premiers, est comme suit :

$$p\mathbb{Z}_k = \prod_{1 \le i \le g} \mathfrak{p}_\mathfrak{i}^{e_i},$$

où

$$\mathfrak{p}_\mathfrak{i} = (p, T_i(\theta)) = p\mathbb{Z}_k + T_i(\theta)\mathbb{Z}_k.$$

D'autre part, le degré résiduel, que l'on note f_i, est égal au degré de T_i.

Proposition 14. *Soit θ un entier, $k = \mathbb{Q}(\theta)$ un corps de nombres ; $T \in \mathbb{Z}[X]$ le polynôme irréductible unitaire de θ. Soit p un nombre premier qui divise f. Soit*

$$T(X) \equiv \prod_{1 \leq i \leq g} \overline{T_i^{e_i}(X)} \quad mod\ p.$$

La décomposition de T en facteurs irréductibles dans $\mathbb{F}_p[X]$, où les T_i sont des relèvements unitaires arbitraires de $\overline{T_i}$ dans $\mathbb{Z}[X]$. Alors

$$p\mathbb{Z}_k = \prod_{1 \leq i \leq g} \mathfrak{a}_\mathfrak{i}.$$

où $\mathfrak{a}_\mathfrak{i} = (p, T_i^{e_i}(\theta)) = p\mathbb{Z}_k + T_i^{e_i}(\theta)\mathbb{Z}_k$, les idéaux $\mathfrak{a}_\mathfrak{i}$ ne sont pas nécessairement premiers mais sont premiers entre eux. D'autre part, si n_i est le degré de T_i alors $N(\mathfrak{a}_\mathfrak{i}) = p^{e_i n_i}$, $N(\mathfrak{a}_\mathfrak{i})$ désigne la norme de l'idéal $\mathfrak{a}_\mathfrak{i}$. Et tous les idéaux premiers divisant $\mathfrak{a}_\mathfrak{i}$ ont un degré résiduel divisible par n_i.

3.2 Ordre maximal d'une famille de corps cubiques.

Soit n un entier relatif, considérons la famille de polynômes cubiques,

$$P_n(x) = x^3 - (n^3 - 2n^2 + 3n - 3)x^2 - n^2x - 1.$$

Pour $n \neq 1$, $P_n(\pm 1) \neq 0$ alors ces polynômes sont irréductibles. Le discriminant de ces polynômes, noté $D(P_n)$, est égal :

$$D(P_n) = (n-1)^2(n^2+3)^2(n^2-3n+3)^2. \tag{3.2.1}$$

Soit θ une racine de $P_n(x)$. Soit $K_n = \mathbb{Q}(\theta)$, alors K_n est une extension cubique cyclique. En effet, le discriminant de P_n est un carré, d'après la proposition **??**, on déduit alors que K est une extension cubique cyclique.
Comme K est cubique alors $P_n(x)$ possède au moins une racine réelle, de plus K est cyclique alors toutes ses racines sont dans K, donc K est totalement réelle.
Notons θ_i, $1 \leq i \leq 3$, les racines du polynôme $P_n(x)$. Comme leur produit est positif, et $\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3 = -n^2$ alors le polynôme P_n possède une racine positive, qui sera noté $\theta = \theta_1$ et deux racines négatives qui seront notées θ_2, θ_3, qui vérifient les égalités suivantes :

$$\theta_2 = \frac{-(\theta_1+1)}{(n^2-n+1)\theta_1 + n}, \quad \theta_3 = \frac{-(n\theta_1+1)}{(n^2-n+1)\theta_1 + 1}.$$

On note alors σ l'unique générateur de $Gal(K_n/\mathbb{Q})$ vérifiant $\theta_2 = \sigma(\theta_1), \theta_3 = \sigma^2(\theta_1)$.
Dans [**?**] L.C. Washington détermine le discriminant du corps K_n et il montre le résultat suivant :

Théorème 10. *Si $(n^2+3)(n^2-3n+3) = bc^3$ où b est sans facteurs cubiques. Alors le discriminant D_K du corps K est égal à :*

$$D_K = 81^{\delta} \prod_{p|b, p\geq 5} p^2,$$

où $\delta = 0$ si $n \not\equiv 0 \ mod\ 3$ et $\delta = 1$ si $n \equiv 0 \ mod\ 3$.

Preuve :
Nous reprenons la démonstration de Washington en simplifiant certaines formules. Pour déterminer le discriminant nous cherchons les premiers ramifiés dans l'extension $K/\mathbb{Q}$.
• Si p premier $\neq 2, \neq 3$ divise le discriminant de P_n il divise un seul des trois facteurs $n-1$, n^2+3 et n^2-3n+3 du discriminant.
Le nombre premier 3 divise le discriminant si 3 divise $n-1$ ou $3|n$. Dans ce dernier cas $v_3(n^2-3n+3) = v_3(n^2+3) = 1$.
• Si $p = 2$ divise n^2+3 alors n est impair et ne divise pas n^2-3n+3. De plus on a $v_2(n^2+3) = 2$.
• Si $p \geq 3$ divise $n-1$ alors

$$P_n(X) = (X-1)(X+1)^2 \text{mod } n-1$$

Le polynôme P_n mod $n-1$ a au moins deux racines distinctes donc p n'est pas ramifié.
• Si $p \neq 3$ divise n^2-3n+3 posons $\theta = \frac{1}{u+1-n}$. Le polynôme minimal de u est H et on a

$$H(X) = X^3 + \left(n^2-3n+3\right)X^2 - n\left(n^2-3n+3\right)X - n^2+3n-3.$$

Il en résulte que $v_p(u) > 0$ et $3v_p(u) = v_p(u^3) = v_p(n^2-3n+3)$. Si $v_p(n^2-3n+3) \not\equiv 0 \bmod 3$ alors p est ramifié. Si $v_p(n^2-3n+3) = 3a$ alors le discriminant de l'entier $\frac{u}{p^a}$ n'est pas divisible par p et p n'est pas ramifié.
• Si $p \neq 3, 2$ divise n^2+3 on procède de même en posant $\theta = \frac{1}{1+u}$ et

$$H(X) = X^3 + \left(n^2+3\right)X^2 + n\left(n^2+3\right)X + (n-1)\left(n^2+3\right).$$

• Si n est impair et si $\theta = \frac{1}{1+u}$ alors $\frac{u}{2}$ est racine de

$$X^3 + \frac{(n^2+3)}{2}X^2 + n\frac{(n^2+3)}{4}X + \frac{(n^2+3)}{4}\frac{(n-1)}{2}$$

Modulo 2 ce polynôme a deux racines distinctes ou pas de racines. Il en résulte que 2 n'est pas ramifié. Ceci montre aussi que si $v_2(n-1) = 1$ l'idéal 2 est inerte et si $v_2(n-1) > 1$ l'idéal 2 est décomposé.
On notera que si $p \neq 3$ se ramifie alors il est totalement ramifié, donc p^2 divise le discriminant. Si 3 se ramifie alors 81 divise le discriminant. on a alors la forme voulue du discriminant. □
On définit γ par $\gamma = 1$ si n est impair (resp. $\gamma = 0$ si n est pair) et on pose $D(n) = (n^2+3)(n^2-3n+3)/4^\gamma$.
On se propose de retrouver en partie ce résultat, en construisant une base d'entiers du corps de nombres K_n. On commence tout d'abord, en utilisant le critère de Dedekind, par construire un ordre maximal à partir de l'ordre $\mathbb{Z}[\theta]$, comme le montre le lemme suivant :

Lemme 2. *Si $D(n)$ est sans facteurs carrés. Alors l'ordre $\mathbb{Z}[\theta, \theta_2]$ est p-maximal pour tout premier p qui divise $D(n)$.*

Preuve :
Si p divise $D(n)$ alors p divise (n^2+3) ou p divise (n^2-3n+3) , ce qui nous conduit à étudier deux cas :
a) Considérons le cas où p divise (n^2-3n+3), alors

$$P_n(x) \equiv (x+2-n)^3 \bmod p$$

ce qui donne :

$$P_n(x) - (x+2-n)^3 = pm_1(x+1)(x(n+1)+3-n)$$

où p ne divise pas m_1.
Si on pose $g(x) = x+2-n$, $h(x) = (x+2-n)^2$, $f(x) = \frac{P_n(x)-(x+2-n)^3}{p}$, alors $(\overline{f}, \overline{g}, \overline{h}) = (\overline{f}, \overline{g})$. Comme $(m_1, p) = (n-1, p) = 1$ et $f(n-2) = m_1(n-1)^3$, alors $n-2$ n'est pas racine de f modulo p, donc $(\overline{f}, \overline{g}) = 1$.
D'après le critère de Dedekind $\mathbb{Z}[\theta]$ est p-maximal pour p^2 ne divisant pas $D(n)$. Comme $\mathbb{Z}[\theta] \subseteq \mathbb{Z}[\theta, \theta_2] \subseteq \mathbb{Z}_K$ alors $\mathbb{Z}[\theta, \theta_2]$ est p-maximal pour p^2 ne divisant pas $D(n)$.

b) Si p est un nombre premier impair qui divise (n^2+3), alors

$$P_n(x) - (x-1)^3 = -pm_2x((n-2)x+1),$$

tel que p ne divise pas m_2. Posons $g_1(x) = x-1$, $h_1(x) = (x-1)^2$, $f_1(x) = \frac{P_n(x)-(x-1)^3}{p}$, alors $(\overline{f_1}, \overline{g_1}, \overline{h_1}) = (\overline{f_1}, \overline{g_1})$.
En utilisant les mêmes arguments que précédemment, on montre que 1 n'est pas racine de f_1 modulo p, donc $(\overline{f_1}, \overline{g_1}) = 1$. D'après le critère de Dedekind $\mathbb{Z}[\theta, \theta_2]$ est p-maximal pour p^2 ne divisant pas $D(n)$.

• si 2 divise n^2+3, alors n est impair et en utilisant le critère de Dedekind, on vérifie que 1 est racine du polynôme

$$f_1(x) = m_2x((n-2)x+1),$$

dans $\mathbb{Z}/2\mathbb{Z}$, donc l'ordre $\mathbb{Z}[\theta,\theta_2]$) n'est pas 2-maximal. □

Etudions quelques exemples dans le cas où $D(n)$ posséde des facteurs carrés.

Exemples:
1) Si $n=24$ alors $D(n)=3^2 13^2 193$, on montrera dans la proposition **??** que l'indice $\mathbb{Z}[\theta]$ dans $\mathbb{Z}[\theta,\theta_2]$ est égal à $n-1$, donc dans notre cas à 23. Puis en utilisant le critère de Dedekind, on va étudier si l'ordre $\mathbb{Z}[\theta,\theta_2]$ est p-maximal pour p nombre premier qui divise $D(n)$.
• Si $p=3$ alors

$$P_{24}(x)-(x-1)^3 = -3(4247x^2-576x-1),$$

en posant $g(x)=x-1$, $h(x)=(x-1)^2$ et $f(x)=\frac{P_{24}(x)-(x-1)^3}{3}$ alors $\overline{f}(x)=(x-1)(x+1)$ et $(\overline{f},\overline{g},\overline{h})=x-1$, donc $\mathbb{Z}[\theta,\theta_2]$ n'est pas 3-maximal.
soit $\mathcal{O}'$ un ordre donné par le théorème **??**. Si U est le relèvement unitaire de $\overline{P_{24}}/(\overline{f},\overline{g},\overline{h})$ de $\mathbb{Z}[X]$, alors $U(x)=h(x)$ et nous avons

$$\mathcal{O}' = \mathbb{Z}[\theta] + \frac{1}{3}(\theta-1)^2\mathbb{Z}[\theta],$$

tel que $[\mathcal{O}':\mathbb{Z}[\theta]]=3$ et $disc(\mathcal{O}')=23^2 13^2 193^2$.
• Si $p=13$ alors

$$P_{24}(x)-(x+4)^3 = 7.13(x+4)^2,$$

en posant $g(x)=x+4$, $h(x)=(x+4)^2$ et $f(x)=\frac{P_{24}(x)-(x+4)^3}{13}$ alors $f(x)=7(x+4)^2$ et $(\overline{f},\overline{g},\overline{h})=x+4$, donc $\mathbb{Z}[\theta,\theta_2]$ n'est pas 13-maximal.
On obtient alors

$$\mathcal{O}'_1 = \mathbb{Z}[\theta] + \frac{1}{13}(\theta+4)^2\mathbb{Z}[\theta],$$

tel que $[\mathcal{O}'_1:\mathbb{Z}[\theta]]=13$ et $disc(\mathcal{O}'_1)=23^2 3^2 193^2$.
• Si $p=193$ alors

$$P_{24}(x)-(x+192)^3 = 193(-69x^2-576x-36673),$$

en posant $g(x)=x+192$, $h(x)=(x+192)^2$ et $f(x)=\frac{P_{24}(x)-(x+192)^3}{193}$ alors $f(x)=-69x^2-576x-36673$ et $(\overline{f},\overline{g},\overline{h})=1$, donc $\mathbb{Z}[\theta,\theta_2]$ est 193-maximal.
2) Si $n=45$ alors $D(n)=3^2 13^2 631$, donc $3, 13$ et 631 sont les seuls diviseurs premiers de $D(n)$ et $[\mathbb{Z}[\theta,\theta_2]:\mathbb{Z}[\theta]]=44$.

• Si $p = 3$ alors

$$P_{45}(x) - (x+2)^3 = 3(-29071x^2 - 679x - 3),$$

en posant $g(x) = x + 2$, $h_1(x) = (x+2)^2$ et $f(x) = \frac{P_{45}(x)-(x+2)^3}{3}$ alors $\overline{f}_1(x) = 2(x+1)x$ et un simple calcul montre que $(\overline{f}, \overline{g}, \overline{h}) = 1$, donc $\mathbb{Z}[\theta, \theta_2]$ est 3-maximal.

• Si $p = 13$ alors

$$P_{45}(x) - (x+12)^3 = 13(-6711x^2 - 189x - 133),$$

en posant $g(x) = x + 12$, $h(x) = (x+12)^2$ et $f(x) = \frac{P_{24}(x)-(x+12)^3}{13}$ alors $f(x) = 10(x+12)^2$, $U(x) = h(x)$ et $(\overline{f}, \overline{g}, \overline{h}) = x + 12$, donc $\mathbb{Z}[\theta, \theta_2]$ n'est pas 13-maximal et nous avons

$$\mathcal{O}'_2 = \mathbb{Z}[\theta] + \frac{1}{13}(\theta+12)^2\mathbb{Z}[\theta],$$

tel que $[\mathcal{O}'_2 : \mathbb{Z}[\theta]] = 13$ et $disc(\mathcal{O}'_2) = 2^2 3^2 11^2 631^2$.
• Si $p = 631$ alors

$$P_{45}(x) - (x+588)^3 = 631(-141x^2 - 1647x - 322183),$$

en posant $g(x) = x + 588$, $h(x) = (x+588)^2$ et$f(x) = \frac{P_{45}(x)-(x+588)^3}{193}$ alors $\overline{f}(x) = 490x^2 + 246x + 258$ et $(\overline{f}, \overline{g}, \overline{h}) = 1$, donc $\mathbb{Z}[\theta, \theta_2]$ est 631-maximal.

3) Si $n = 37$, alors $D(n) = 7^3 13\ \ 97$, $[\mathbb{Z}[\theta, \theta_2] : \mathbb{Z}[\theta]] = 36$, et on montre que $\mathbb{Z}[\theta, \theta_2]$ est p-maximal pour $p = 13, 97$ mais n'est pas 7-maximal.

4) Si $n = 124$, alors $D(n) = 713^3 43\ \ 349$, $[\mathbb{Z}[\theta, \theta_2] : \mathbb{Z}[\theta]] = 123$ et on montre que $\mathbb{Z}[\theta, \theta_2]$ est p-maximal pour $p = 7, 43, 349$ mais n'est pas 13-maximal.

Proposition 15. *Si $D(n)$ est sans facteurs carrés. Alors $\{1, \theta, \theta_2\}$ est une base d'entiers de K. Le discriminant D_K du corps K est égale à :*

$$D_K = D(n)^2.$$

Preuve :
D'après le lemme **??**, les nombres premiers pour lesquels $Z[\theta, \theta_2]$ n'est pas p- maximal sont des diviseurs de $n - 1$ et comme $(n-1, (n^2+3)/4^\gamma) = (n-1, n^2 - 3n + 3) = 1$ où $\gamma = 1$ si n est impair (resp. $\gamma = 0$ si n est pair), alors le discriminant du corps K est divisible par $D(n)^2$. Donc $D_K = a^2 D(n)^2$, en remplaçant dans **??** on obtient :

$$D(P_n) = (n-1)^2 D(n)^2 = I(\theta)^2 D_K = I(\theta)^2 a^2 D(n)^2.$$

D'où

$$(n-1)^2 = I(\theta)^2 a^2$$

donc $I(\theta)$ divise $n-1$. Comme $\mathbb{Z}[\theta] \subseteq \mathbb{Z}[\theta, \theta_2] \subseteq \mathbb{Z}_K$ et

$$[\mathbb{Z}[\theta, \theta_2] : \mathbb{Z}[\theta]] = \begin{vmatrix} 1 & 0 & -(n^2-n+1) \\ 0 & 1 & (-n^2+n-2)(n-1) \\ 0 & 0 & n-1 \end{vmatrix} = n-1,$$

alors $n-1$ divise $I(\theta)$ donc $I(\theta) = n-1$, d'où

$$(n^2+3)^2(n^2-3n+3)^2 = D_K.$$

Comme $D(1, \theta, \theta_2) = D_K$, on déduit alors $\{1, \theta, \theta_2\}$ est une base d'entiers de K.

3.3 Décomposition des nombres premiers facteurs de $n-1$ et du nombre premier 2.

Soit $n \in \mathbb{Z}$, $n \neq 1$, et p un nombre premier qui divise $n-1$, nous supposerons que $D(n)$ est sans facteurs carrés. Dans la proposition suivante, on montre que l'idéal $p\mathbb{Z}_K$ est inerte ou décomposé dans l'extension cubique $K/\mathbb{Q}$.

Proposition 16. *1) Soit p un nombre premier impair qui divise $n-1$. Alors p est totalement décomposé dans $K/\mathbb{Q}$ et l'on a*

$$p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,$$

où on note $\mathfrak{p}_1 = p\mathbb{Z}_K + (\theta+1)\mathbb{Z}_K$, $\mathfrak{p}_2 = \mathfrak{p}_1^{\sigma}, \mathfrak{p}_3 = \mathfrak{p}_1^{\sigma^2}$ et $\mathfrak{p}_2\mathfrak{p}_3 = p\mathbb{Z}_K + (\theta-1)^2\mathbb{Z}_K$, où θ est une racine du polynôme $P_n(x)$.
2) • si n est pair alors le nombre premier 2 est inerte dans l'extension $K/\mathbb{Q}$.
• Si n est impair et si $v_2(n-1) = 1$ (resp. $v_2(n-1) > 1$) alors l'idéal 2 est inerte (resp. décomposé).

Preuve :
• La factorisation du polynôme $P_n(x)$ modulo $n-1$ est la suivante :

$$P_n(x) \equiv (x+1)(x-1)^2 \bmod (n-1).$$

D'après la proposition **??**, la décomposition de l'idéal $p\mathbb{Z}_K$ en produit d'idéaux premiers est la suivante

$$p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{b},$$

où $\mathfrak{p}_1 = p\mathbb{Z}_K + (\theta+1)\mathbb{Z}_K$, $\mathfrak{b} = p\mathbb{Z}_K + (\theta-1)^2\mathbb{Z}_K = \mathfrak{p}_1^{\sigma}\mathfrak{p}_1^{\sigma^2}$, et $N(\mathfrak{p}_1) = p$, $N(\mathfrak{b}) = p^2$. On déduit alors que l'idéal $p\mathbb{Z}_K$ se décompose dans $K/\mathbb{Q}$, donc

$$p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_1^{\sigma}\mathfrak{p}_1^{\sigma^2}.$$

• Si n est pair, la factorisation du polynome G_n modulo 2, est la suivante :

$$P_n(x) \equiv x^3 + x^2 + 1 \bmod 2.$$

D'après le théorème **??**, la décomposition de l'ideal $2\mathbb{Z}_K$ est la suivante :

$$2\mathbb{Z}_K = \mathfrak{p},$$

où $\mathfrak{p} = p\mathbb{Z}_K + (\theta^3+\theta^2+1)\mathbb{Z}_K$, et le degré résiduel f est égal à 3.
• Si n est impair alors on reprend la même preuve faite dans le théorème **??**.

Exemples: I. Soit $n = -23$, alors 2 et 3 sont les seuls diviseurs premiers de -24. D'après la proposition **??**, les idéaux $2\mathbb{Z}_K$ et $3\mathbb{Z}_K$ se décomposent totalement dans l'extension $K/\mathbb{Q}$ et l'on a :

$$3\mathbb{Z}_K = \mathfrak{q'}_1\mathfrak{q'}_2\mathfrak{q'}_3,$$

tels que $\mathfrak{q'}_1 = 3\mathbb{Z}_K + (\theta+1)\mathbb{Z}_K$, $\mathfrak{q'}_2 = \mathfrak{q'}_1^{\sigma}$, $\mathfrak{q'}_3 = \mathfrak{q'}_1^{\sigma^2}$,

$$2\mathbb{Z}_K = \mathfrak{p'}_1\mathfrak{p'}_2\mathfrak{p'}_3,$$

tels que $\mathfrak{p'}_1 = 2\mathbb{Z}_K + (\theta+1)\mathbb{Z}_K$, $\mathfrak{p'}_2 = \mathfrak{p'}_1^{\sigma}$, $\mathfrak{p'}_3 = \mathfrak{p'}_1^{\sigma^2}$.

II. Soit $n = 11$, alors 2 et 5 sont les seuls diviseurs premiers de 10, comme précédemment, l' idéal $2\mathbb{Z}_K$ est inerte et la décomposition de l'idéal $5\mathbb{Z}_K$ est la suivante :

$$5\mathbb{Z}_K = \mathfrak{b}_1\mathfrak{b}_2\mathfrak{b}_3,$$

avec $\mathfrak{b}_1 = 5\mathbb{Z}_k + (\theta+1)\mathbb{Z}_K, \mathfrak{b}_2 = \mathfrak{b}_1^{\sigma}, \mathfrak{b}_3 = \mathfrak{b}_1^{\sigma^2}$.
III. Soit $n = 22$ alors 3 et 7 sont les seuls diviseurs premiers de 21, les décompositions des idéaux $3\mathbb{Z}_K$ et $7\mathbb{Z}_K$ sont les suivantes :

$$3\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,$$

tels que $\mathfrak{p}_1 = 3\mathbb{Z}_K + (1+\theta)\mathbb{Z}_K, \mathfrak{p}_2 = \mathfrak{p}_1^{\sigma}, \mathfrak{p}_3 = \mathfrak{p}_1^{\sigma^2}$.

$$7\mathbb{Z}_K = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$$

avec $\mathfrak{q}_1 = 7\mathbb{Z}_K + (\theta+1)\mathbb{Z}_K$, $\mathfrak{q}_2 = \mathfrak{q}_1^{\sigma}$, $\mathfrak{q}_3 = \mathfrak{q}_1^{\sigma^2}$.

3.4 Unités de K

Dans ce paragraphe, on va s'intéresser au groupe des unités de K. Dans [**?**] L.C. Washington a montré, sous certaines conditions, que les racines du polynôme P_n sont des unités fondamentales, comme le montre le résultat suivant :

Théorème 11. *Soit $n \in \mathbb{Z}$, $n \neq 1, 2$. Si $9^{-c}(n^2+3)(n^2+3n-3)$, $c \in \{0,1\}$, est sans facteurs carrés alors les racines de P_n engendrent le groupe des unités de K.*

On se propose de montrer que ce résultat reste vrai dans le cas où 4 est le seul facteur carré qui divise $9^{-c}(n^2+3)(n^2+3n-3)$, comme le montre la proposition suivante.

Proposition 17. *Soit $n \in \mathbb{Z}$, $n \neq 1, 2$. Si $9^{-c}(n^2+3)(n^2+3n-3) = 4^{\gamma}b$, où $c, \gamma \in \{0,1\}$ et b est sans facteurs carrés, alors les racines de P_n engendrent le groupe des unités de K.*

Preuve :
Le régulateur R du corps K est lié au régulateur R_1 du système d'unités $\{\theta_1, \theta_2\}$ par l'égalité suivante : $R_1 = IR$ où I désigne l'indice du groupe engendré par $-1, \theta_1, \theta_2$ dans le groupe des unités du corps. Comme R vérifie l'inégalité suivante :

$$R \geq \frac{1}{16}\log^2(D_K/4)$$

alors I est majoré par

$$\frac{16R_1}{\log^2(D_K/4)}.$$

Si n tend vers l'infini alors R_1 est équivalent à $7\log^2 n$ et D_K est équivalent à n^8 si n est pair (resp. $n^8/16$ si n est impair), il en résulte que l'indice est majoré par $7/4$, d'où $I = 1$. Pour les petites valeurs de n tels que $n \neq 1, 2$, on montre que l'indice est majoré par 3, donc $I = 1$ ou 2.
Notons U le groupe des unités de K et U_1 le sous-groupe des unités engendré par $-1, \theta_1, \theta_2$. Comme $U/\{\pm 1\}$ et $U_1/\{\pm 1\}$ sont des $\mathbb{Z}[\zeta_3]$-modules alors

$$[U : U_1] = [U/\{\pm 1\} : U_1/\{\pm 1\}] = Norm_{\mathbb{Z}[\zeta_3]/\mathbb{Z}}(\alpha),$$

où $\alpha \in \mathbb{Z}[\zeta_3]$. D'autre part, 2 n'est pas une norme. Il en résulte alors que $I = 1$.
Pour $n = 2$, un calcul avec pari montre que l'indice est égal à 3.
Dans tout le reste du paragraphe, On se propose de donner certaines propriétés des unités de K.

Proposition 18. *Soient $e_0 = 1$, $e_1 = n-2$, $e_2 = 1-n$. Soit p un nombre premier qui divise $n^2 - 3n + 3$. Alors chaque unité ϵ de K est congrue à $\pm e_k$ modulo $\mathfrak{p}$, où $\mathfrak{p}$ est un idéal premier au dessus de l'idéal $p\mathbb{Z}_K$, $0 \leq k \leq 2$. Pour chaque conjugué ϵ' de ϵ, on a ϵ' est congru à ϵ modulo $\mathfrak{p}$.*

Preuve : La factorisation du polynôme $P_n(x)$ modulo p est la suivante :

$$P_n(x) \equiv (x - n + 2)^3 \bmod p,$$

comme $p\mathbb{Z}_K = \mathfrak{p}^3$, alors $\theta_i \equiv n-2 \bmod \mathfrak{p}$; de l'égalité $\theta_1\theta_2\theta_3 = 1$, il s'ensuit alors que $(2-n)^3 \equiv 1 \mod \mathfrak{p}$. Comme $\{\theta_1, \theta_2\}$ sont des unités fondamentales de K, alors d'après le théorème de Dirichlet, $\epsilon = \pm\theta_1^t\theta_2^s$. Donc $\epsilon \equiv \pm(n-2)^k \bmod \mathfrak{p}$, où $0 \leq k \leq 2$. Les restes de $(2-n)^k$ par $(n^2 - 3n + 3)$ sont les e_k. Comme $\theta_i \equiv \theta_j \equiv (2-n) \bmod \mathfrak{p}$, pour $1 \leq i, j \leq 3$ alors $\epsilon' \equiv \epsilon \bmod \mathfrak{p}$.

Proposition 19. *Soit p un nombre premier qui divise $n^2 + 3$ (resp. $n-1$). Notons par ϵ une unité de K. Alors ϵ est congrue à ± 1 mod $\mathfrak{p}$. Où $\mathfrak{p}$ est un ideal premier au dessus de l'idéal $p\mathbb{Z}_K$.*

Preuve :
1) Si p est un nombre premier qui divise $n^2 + 3$. Alors la factorisation du polynôme $P_n(x)$ modulo p est la suivante :

$$P_n(x) \equiv (x-1)^3 \bmod p.$$

Comme $p\mathbb{Z}_K = \mathfrak{p}^3$, alors $\theta_i \equiv 1 \bmod \mathfrak{p}$, avec $1 \leq i \leq 3$, d'après les théorèmes **??** et de Dirichlet $\epsilon \equiv \pm 1 \bmod \mathfrak{p}$.
2) Si p est un nombre premier qui divise $n-1$. Alors la factorisation du polynôme P_n modulo p est la suivante :

$$P_n(x) \equiv (x+1)^2(x-1) \bmod p.$$

Pour le reste de la preuve, on procède de la même façon que précédemment. Ce qui termine la preuve de la proposition.

Proposition 20. *Soit ϵ une unité de K. Alors la trace de ϵ est congru à ± 1 ou ± 3 modulo $n-1$.*

Preuve :
D'après le théorème **??**, les unités θ_1, θ_2 sont des unités fondamentales de K, et d'après le théorème de Dirichlet, une unité ϵ de K, s'écrit comme suit $\epsilon = \pm\theta_1^{m_1}\theta_2^{m_2}$. Donc il reste à montrer que $Tr_{K/\mathbb{Q}}(\theta_1^{m_1}\theta_2^{m_2}) \equiv 1$ ou $3 \bmod (n-1)$.
de l'égalité $P_n(\theta_i)/\theta_i = 0$, on montre par récurrence que :

$$\theta_i^{2\lambda k} \equiv -k\theta_i^{\lambda} + k\theta_i^{-\lambda} + 1 \mod (n-1),$$

$$\theta_i^{\lambda(2k+1)} \equiv \ -k\theta_i^{-\lambda} + (k+1)\theta_i^{\lambda} \mod (n-1),$$

où $k \in \mathbb{N}^*$, et $\lambda = \pm 1$ ce qui donne

$$Tr_{K/\mathbb{Q}}(\theta_i^{2\lambda k}) \equiv \ 3 \bmod (n-1),\ Tr_{K/\mathbb{Q}}(\theta_i^{\lambda(2k+1)}) \equiv \ -1 \bmod (n-1).$$

on montre alors que

$$Tr_{K/\mathbb{Q}}(\theta_1^{m_1}\theta_2^{m_2}) \equiv \begin{cases} 3 \mod (n-1) & \text{si } m_1,\ m_2 \text{ sont pairs,} \\ -1 \mod (n-1) & \textit{sinon.} \end{cases}$$

La proposition suivante donne une caractérisation des carrés de $\mathbb{Z}_K/4\mathbb{Z}_K$, dont on verra l'utilité dans le chapitre 5.

Proposition 21. *Si n est pair et $x \in K$ premier avec 2, alors il existe une unité ϵ de K tel que $x\epsilon$ soit un carré dans $\mathbb{Z}_K/4\mathbb{Z}_K$.*

Preuve :
On montre sans trop de difficultés que $\{1, \theta, w\}$ où $w = (-\theta^2+1)/(n-1)$ est une base d'entiers. Soit x un élément de K alors $x = a_0 + a_1\theta + a_2 w$. Notons par S l'ensemble des carrés non nuls de K modulo 4,

$$S = \{1, \theta^2, w^2, (\theta+w)^2, (w+1)^2, (\theta+1)^2, (1+\theta)^2 + w^2 + 2w(1+\theta)\}.$$

Soit $\theta' = \frac{-(\theta+1)}{(n^2-n+1)\theta+n}$ le conjugué de θ, alors $\theta'^{-1} = -w - (n^2-n+2)\theta - n$, et $\theta\theta'^{-1} = w + \theta$.
Notons par T l'ensemble des unités modulo les carrés.

$$T = \{\pm 1, \pm\theta, \pm\theta'^{-1}, \theta\theta'^{-1}\}.$$

On distinguera deux cas.
Premier cas
Si $n \equiv 0 \bmod 4$, la factorisation du polynôme $P_n(x)$ modulo 4 est la suivante :

$$P_n(x) \equiv x^3 + 3x^2 - 1 \bmod 4.$$

On en déduit les relations suivantes modulo 4 :
$\theta^3 = \theta^2 + 1$, $w = \theta^2 - 1$, $\theta^4 = \theta^2 + \theta + 1$, $\theta^2(\theta - 1) = 1$ et $\theta^{-1} = \theta^2 - \theta$.
L'ensemble S des carrés non nuls de K modulo 4,

$$S = \{1, \theta^2, -\theta^2 + \theta + 2, 2\theta^2 - \theta, \theta^2 + \theta + 1, \theta^2 + 2\theta + 1, \theta - 1\}.$$

L'ensemble T des unités modulo les carrés,

$$T = \{\pm 1, \pm\theta, \pm(-\theta^2 + 2\theta + 1), \pm(\theta^2 + \theta - 1)\}.$$

Considérons W l'ensemble des produits d'un élément de S par un élément de T. Par un simple calcul, on vérifie que ces produits sont différents.
En calculant les 56 classes résiduelles non nulles modulo 4, on retrouve les éléments de W.
Donc pour chaque élément x de W, il existe une unité ϵ de K tel que le produit $x\epsilon$ soit un élément de S.
Deuxième cas
Si $n \equiv 2 \bmod 4$, la factorisation du polynôme $P_n(x)$ modulo 4 est la suivante :

$$P_n(x) \equiv x^3 + x^2 - 1 \bmod 4.$$

En reprenant les même notations et le même raisonnement que précédemment, les ensembles S_1 et T_1 sont les suivants :

$$S_1 = \{1, \theta^2, 3\theta^2 + \theta, 2 + 3\theta + 2\theta^2, \theta + \theta^2 + 3, 1 + \theta, 1 + 2\theta + \theta^2\}.$$

$$T_1 = \{\pm 1, \pm\theta, \pm(-\theta^2 + \theta - 1), \pm(2\theta^2 - \theta - 1)\}.$$

On conclut alors que pour chaque élément x de W_1, où W_1 est défini de la même façon que W. Il existe une unité ϵ de K tel que le produit $x\epsilon$ soit un élément de S_1. Ce qui prouve la proposition.

Chapitre 4

Courbes elliptiques associés a une famille de corps cubiques

Dans ce chapitre, nous allons nous intéresser à l'étude de courbes elliptiques et les homomorphismes liés à la 2-descente.

4.1 Famille de courbes elliptiques.

Soient n un entier relatif différent de 1, et $G_n(x)$ le polynôme suivant :

$$G_n(x) = -x^3 P_n(-1/x) = x^3 - n^2x^2 + (n^3 - 2n^2 + 3n - 3)x + 1.$$

Notons ρ_1 la racine négative de $G_n(x)$. Alors $\rho_2 = \frac{-n\rho_1+n^2-n+1}{-\rho_1+1}$ et $\rho_3 = \frac{-\rho_1+n^2-n+1}{-\rho_1+n}$ sont les deux autres racines. Comme $\rho_i = -\frac{1}{\theta_i}$, alors les deux extensions
$L_n = \mathbb{Q}(\rho_i)$ et K_n coincident. Par la suite, par commodité d'écriture on utilisera K au lieu de K_n.
Pour $n \neq 1$, considérons les courbes elliptiques E_n définies sur $\mathbb{Q}$ par l'équation $y^2 = G_n(x)$. Les points de 2-torsion de E_n sont $(\rho_1, 0)$, $(\rho_2, 0)$, $(\rho_3, 0)$ et ne sont pas rationnels sur $\mathbb{Q}$ mais sont définis sur K. Le discriminant de E_n est égal à $16(n-1)^2\gamma^2$, où $\gamma = (n^2+3)(n^2-3n+3)$ est sans facteurs carrés ; et son invariant modulaire j est égal à $\dfrac{16^2\gamma^2}{(n-1)^2}$.

4.1.1 Réduction modulo p.

Considérons la courbe elliptique

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

Soit p un nombre premier, La courbe $\tilde{E}$ d'équation

$$\tilde{E} : y^2 = x^3 + \tilde{a}x^2 + \tilde{b}x + \tilde{c}$$

où $\tilde{a}$, $\tilde{b}$, $\tilde{c}$ sont les images de a, b, c dans $\mathbb{F}_p$, est appelé la réduction de E modulo p.
Soit R un anneau de valuation discréte, K son anneau de fraction et v la valuation associée. Soit E/K une courbe elliptique donnée par l'équation

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

Alors le changement de variables $x = u^2x', y = u^3y'$, où u est le dénominateur commun des a_i, nous donne une équation de Weierstrass à coefficients dans R. Notons Δ le discriminant de E. On dit que le modèle de la courbe E est minimale en la valuation discréte v, si $v(\Delta)$ est minimal parmi toutes les équations de Weierstrass à coefficients dans R.
On a le critère suivant pour déterminer si l'équation est minimale.

Proposition 22. *Soit $E/\mathbb{Q}$ une courbe elliptique donnée par une équation de Weierstrass. L'équation est minimale en p, $p \geq 5$, si et seulement si $v_p(\Delta) \leq 12$ ou $v_p(c_4) = v_p(b_2^2 - 24b_4) \leq 4$, où $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$.*

Remarque 6. *Quand $p = 2$ ou 3, l'algorithme de Tate détermine si l'équation est minimale en p.*

Exemple: Dans le cas des courbes elliptiques E_n, on a

$$\Delta = 16(n-1)^2\gamma^2,$$

$$c_4 = 16\gamma,$$

où $\gamma = (n^2+3)(n^2-3n+3)$.
Si p est un nombre premier impair, différent de 2 et 3, qui divise Δ alors $v_p(c_4) = 0$ ou 1. D'après la proposition **??**, on déduit que l'équation de la courbe elliptique E_n est minimale en p.
En utilisant l'algorithme de Tate, on montre que l'équation de la courbe elliptique E_n n'est pas minimale en 2. Si n est pair et en effectuant le changement de variable $x' = x+1, y' = y+x+1$, alors on obtient l'équation minimale en 2

$$y'^2 - 2x'y' = x'^3 - (4+n^2)x'^2 + (n^3 - 3n^2 + 3n)x' - (n^3 - 3n^2 + 3n - 3).$$

Si n est impair alors le changement de variable $x' = x+1, y' = y$, nous donne l'équation minimale en 2.
Comme précédemment, on utilise l'algorithme de Tate pour montrer que si 3 ne divise pas n, alors l'équation de la courbe elliptique E_n est minimale en 3. Si 3 divise n, alors le changement de variables $x = x' - 1, y = y'$, nous donne l'équation minimale en 3.

Définition 22. *a) Si $\tilde{E}$ est une courbe elliptique, on dit que E a une* bonne réduction en p.
b) Si $\tilde{E}$ admet un point double à tangentes distinctes dans $\mathbb{P}_2(\mathbb{F}_p)$, on dit que E a une réduction multiplicative en p.
c) Si $\tilde{E}$ admet une pointe, on dit que E a une réduction additive en p.

Remarque 7. *Dans les cas b) et c), on dit que E a une mauvaise réduction. Si E a une réduction multiplicative, alors la réduction est déployée (respectivement non déployée) si les pentes des droites tangentes au point double sont dans $\mathbb{F}_p$ (respectivement ne sont pas dans $\mathbb{F}_p$).*
Les nombres premiers de mauvaise réduction de E sont précisément ceux qui divisent le discriminant de E.

Il est facile de connaître le type de réduction d'une courbe elliptique à partir de son équation de Weierstrass minimale.

Proposition 23. *Soit E/K une courbe elliptique d'équation minimale :*

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

Soit Δ, c_4 les quantités définies dans la proposition précédente.
1) E a bonne réduction en p si et seulement si $v_p(\Delta) = 0$.
2) E a une réduction multiplicative en p si et seulement si $v_p(\Delta) > 0$ et $v_p(c_4) = 0$.
3) E a une réduction additive en p si et seulement si $v_p(\Delta) > 0$ et $v_p(c_4) > 0$.

En utilisant la proposition précédente, on va montrer que la courbe elliptique E_n a mauvaise réduction en les nombres premiers qui divisent $2(n-1)\gamma$, cette réduction est additive en les nombres premiers qui se ramifient dans K c'est-à-dire les nombres premiers qui divisent γ et en le nombre premier 2 ; elle est multiplicative en les nombres premiers qui divisent $(n-1)$, dans ce cas la réduction est déployée (resp. non déployée) si 2 est un carré (resp. n'est pas un carré) mod p.

Réduction additive :
On va distinguer trois cas :
1) si n est pair (resp. n est impair) alors $v_2(\Delta) = 4$ (resp. $v_2(\Delta) \leq 12$) et $v_2(c_4) \geq 2$, on déduit d'après la proposition **??** que la réduction est additive.
2) Si p est un nombre premier impair différent de 3, qui divise $n^2 - 3n + 3$. Alors le polynôme G_n s'écrit comme suit :

$$G_n(x) = (x - (n-1))^3 + (n^2 - 3n + 3)(-x^2 + (n-2)x + n).$$

En posant le changement de variable $X = x - (n-1)$, on obtient $G_n(X) = X^3 - (n^2 - 3n + 3)X^2 - n(n^2 - 3n + 3)X + (n^2 - 3n + 3)$. Donc $v_p(\Delta) > 0$ et $v_p(c_4) > 0$, pour p premier divisant $n^2 - 3n + 3$.
3) Si p est un nombre premier impair différent de 3, qui divise $n^2 + 3$ alors $G_n(x) = (x+1)^3 - (n^2+3)x^2 + (n-2)(n^2+3)x$. En posant le changement de variable $X = x + 1$, on obtient $G_n(X) = X^3 - (n^2+3)X^2 + n(n^2+3)X - (n-1)(n^2+3)$. On déduit alors que $v_p(c_4) > 0$, pour tout premier p divisant $n^2 + 3$.
Donc d'après la proposition **??** , la courbe E_n a une réduction additive en tout premier p qui divise $(n^2+3)(n^2-3n+3)$.

Réduction multiplicative.
Si p est un nombre premier impair facteur de $n-1$, alors $G_n(x) \equiv (x-1)^2(x+1) \bmod p$. Posons $u = x - 1$, l'équation de $\tilde{E}_n$ est la suivante :

$$y^2 \equiv u^2(u+2) \mod p$$

soit

$$y^2 - 2u^2 \equiv u^3 \mod p.$$

La courbe a donc une réduction multiplicative, la réduction est déployée (resp. non déployée) si 2 mod p est un carré (resp. si 2 mod p n'est pas un carré).

Définition 23. *Le conducteur d'une courbe elliptique $E/\mathbb{Q}$ est un entier positif N divisible précisément par les nombres premiers p de mauvaise réduction. Il est défini comme suit :*

$$N = \prod_p p^{f_p}, \text{ où}$$

$$f_p = \begin{cases} 0 & \text{si } E \text{ a bonne réduction en } p, \\ 1 & \text{si } E \text{ a réduction multiplicative en } p, \\ 2 + \delta_p & \text{si } E \text{ a réduction additive en } p, \end{cases}$$

et δ_p est un entier non négatif ($\delta_p = 0$ si $p \geq 5$ et δ_p est borné par 3 (resp. 6) pour $p = 2$ (resp. 3)).

La courbe $E/\mathbb{Q}$ est dite semi-stable en p si p^2 ne divise pas son conducteur N. Cela signifie que la courbe $E/\mathbb{Q}$ a, soit bonne réduction en p, dans le cas où p ne divise pas N, soit mauvaise réduction de type multiplicatif lorsque p divise exactement N. Si la courbe elliptique $E/\mathbb{Q}$ est semi-stable en tout nombre premier p i.e que N est sans facteur carré, alors la courbe $E/\mathbb{Q}$ est dite semi-stable.
Si $E/\mathbb{Q}$ est donnée par une équation de la forme $y^2 = f(x)$, où $f(x) \in \mathbb{Z}[x]$, alors les entiers f_p ($p \neq 2, 3$) sont déterminés en considérant le polynôme $f(x)$

sur le corps $\mathbb{F}_p$.
1. Si $f(x)$ a trois racines distinctes modulo p, alors E a bonne réduction et $f_p = 0$.
2. Si $f(x)$ a une racine double modulo p, alors E a réduction multiplicative en p et $f_p = 1$.
3. Si $f(x)$ a une racine triple. Il se pourrait que le modèle ne soit pas minimal et que la courbe soit en fait semi-stable en p. Si ce n'est pas le cas, alors E a réduction additive et $f_p = 2$.
Chaque point $P = (x_0, y_0) \in E(\mathbb{Q}_p)$ peut-être représenter par un point de coordonnées homogènes $(a : b : c)$ tels que $a, b, c \in \mathbb{Z}_p$ et $inf(v_p(a), v_p(b), v_p(c)) = 0$; on posera $x_0 = \frac{a}{c}$, $y_0 = \frac{b}{c}$. Le point réduit $\tilde{P} = (\tilde{x_0}, \tilde{y_0})$ où $\tilde{x_0} = \frac{\overline{a}}{\overline{c}}$ et $\tilde{y_0} = \frac{\overline{b}}{\overline{c}}$, tels que $\overline{a}, \overline{b}, \overline{c}$ sont les images de a, b, c dans $\mathbb{F}_p$, est dans $\tilde{E}(\mathbb{F}_p)$, ce qui définit une application $red : E(\mathbb{Q}_p) \to \tilde{E}(\mathbb{F}_p)$, défini par

$$red : P \mapsto \tilde{P}.$$

L'application $red : E(\mathbb{Q}_p) \to \tilde{E}(\mathbb{F}_p)$, est appelée application réduction.

Lemme 3. *L'application réduction est un homomorphisme de groupes.*

On va définir deux sous-ensembles de $E(Q_p)$ comme suit :

$$E^0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p)/\tilde{P} \text{ non singulier }\};$$
$$E^1(\mathbb{Q}_p) = \{P = (x, y) \in E(\mathbb{Q}_p)/\tilde{P} = \tilde{O}\}.$$

On remarquera que $E^1(\mathbb{Q}_p)$ est le noyau de la réduction.

Proposition 24. *Soit $\tilde{E}_{ns}(\mathbb{F}_p)$ l'ensemble des points non-singuliers de $\tilde{E}(\mathbb{F}_p)$, La suite de groupes abéliens*

$$1 \longrightarrow E^1(\mathbb{Q}_p) \longrightarrow E^0(\mathbb{Q}_p) \longrightarrow \tilde{E}_{ns}(\mathbb{F}_p) \longrightarrow 1$$

est exacte.

Proposition 25. *(Kodaira, Néron).*
Le groupe $E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p)$ est fini. Plus précisément, si E a une réduction multiplicative alors $E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p)$ est un groupe cyclique d'ordre $-v_p(j(E))$; sinon, $E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p)$ est d'ordre égal à 1, 2, 3 ou 4.

Dans le cas des courbes elliptiques E_n, on a montré que la courbe $\tilde{E_n}$ a un point multiple de coordonnées $(1, 0)$; donc

$$E_n^0(\mathbb{Q}_p) = \{P = (x, y) \in E_n(\mathbb{Q}_p)/x \not\equiv 1 \bmod p\}.$$

Remarque 8. *Soit* $(x, y) \in E_n^0(\mathbb{Q}_p)$ *alors* $v_p(x - \rho_i) \leq 0$, $2 \leq i \leq 3$.
En effet, si $(x, y) \in E_n^1(\mathbb{Q}_p)$ *alors* $x - \rho_i$ *ont des valuations négatives, donc égales.*
Si $(x, y) \notin E_n^1(\mathbb{Q}_p)$ *alors* $v_p(x - \rho_i) \geq 0$, *comme* $(x, y) \in E_n^0(\mathbb{Q}_p)$ *alors* $v_p(x-1) = 0$ *et* $v_p(1-\rho_2) > 0$. *Donc* $v_p(x-\rho_2) = inf(v_p(x-1), v_p(1-\rho_2)) = 0$.
D'autre part, $v_p(\rho_2 - \rho_3) = a > 0$ *et* $v_p(x - \rho_3) = inf(v_p(\rho_2 - \rho_3), v_p(x - \rho_2))$ *alors* $v_p(x - \rho_3) = 0$.

4.2 Homomorphismes liés à la famille de courbes elliptiques E_n

On énonce la proposition suivante pour un corps quelconque. La preuve sera faite pour $k = \mathbb{Q}$ et $f = G_n$, pour les autres cas voir [**?**].

Proposition 26. *Soit* k *un corps de caractéristique différente de* 2, E *une courbe elliptique définie sur* k *donnée par l'équation* $y^2 = f(x)$ *avec* f *un polynôme de degré* 3 *à coefficients dans* k. *Soit la* k*-algèbre* $A_k = k[T]/(f(T))$, *notons* A_k^* *le groupe multiplicatif de* A_k. *Alors*

1. *Si* E *n'a pas de points d'ordre* 2 *sur* k. *On définit l'application* $\lambda_k : E(k) \to A_k^*/A_k^{*2}$, *par*

$$\lambda_k : (x, y) \mapsto (x - T) \mod A_k^{*2},\ O \mapsto 1.$$

2. *Si* E *a un point d'ordre* 2, *alors* $f(x) = (x - \rho)g(x)$ *où* $g(x)$ *est un polynôme irréductible de degré 2 . On définit l'application* $\lambda_k : E(k) \to k \oplus k[T]/(g(T))$, *par*

$$\lambda_k : (x, y) \mapsto ((x - \rho) mod\ k^{*2}, (x - T) mod\ g(T)) \text{ si } x \neq \rho,\ O \mapsto 1,$$

$$(\rho, 0) \mapsto (f'(\rho)\ mod\ k^{*2}, (x - T) mod\ g(T)).$$

3. *Si* E *a trois points d'ordre* 2 $(\alpha_i, 0), 1 \leq i \leq 3$ *; on définit l'application* $\lambda_k : E(k) \to (k^*/k^{*2})^3$, *par*

$$\lambda_k : (x, y) \mapsto (x - \alpha_1, x - \alpha_2, x - \alpha_3) \mod (k^{*2})^3 si\ x \neq \alpha_i,$$

$$(\alpha_1, 0) \mapsto (f'(\alpha_1), \alpha_1 - \alpha_2, \alpha_1 - \alpha_3) \mod (k^{*2})^3,\ O \mapsto 1,$$

on définit de la même façon $(\alpha_i, 0)$, $2 \leq i \leq 3$.

Dans les trois cas, l'application λ_k *est un homomorphisme de groupes, de noyau égal à* $2E(k)$.

Preuve :
Si $k = \mathbb{Q}$, $A_k^* \backsimeq K^*$. Montrons alors que l'application $\lambda_{\mathbb{Q}} : E(\mathbb{Q}) \to K^*/K^{*2}$, définie par

$$\lambda_{\mathbb{Q}} : (x, y) \mapsto (x - \rho_1) \mod K^{*2},\ O \mapsto 1,$$

est un homomorphisme de groupes. Par commodité d'écriture, on utilisera la notation λ au lieu de $\lambda_{\mathbb{Q}}$.
Par définition de λ, $\lambda(R) = \lambda(-R) = (\lambda(R))^{-1}$. Soient $R_i = (a_i, b_i)$, $1 \leq i \leq 3$ des points de $E_n(\mathbb{Q})$ tels que $R_1 + R_2 + R_3 = 0$. Les points R_i appartiennent à la droite D d'équation

$$y = mx + l,$$

comme $G_n(x) - (mx + l)^2$ est un polynôme de degré 3 qui s'annule en a_i donc

$$y^2 - (mx + l)^2 = G_n(x) - (mx + l)^2 = (x - a_1)(x - a_2)(x - a_3) \tag{4.2.1}$$

En remplaçant x par ρ_1 dans **??** et multipliant par -1, on obtient

$$-G_n(\rho_1) + (m\rho_1 + l)^2 = (-\rho_1 + a_1)(-\rho_1 + a_2)(-\rho_1 + a_3), \tag{4.2.2}$$

l'équation **??** s'écrit aussi :

$$\lambda(R_1)\lambda(R_2)\lambda(R_3) = 1 \tag{4.2.3}$$

ce qui prouve que λ est un homomorphisme.
Il est évident que $\ker \lambda \supseteq 2E_n(\mathbb{Q})$.
Réciproquement, soit $R = (a, b) \in \ker \lambda$, alors $a - \rho_1 \in K^{*2}$; il existe donc $\alpha_i \in \mathbb{Q}$ avec $1 \leq i \leq 3$, tel que $a - \rho_1 = (\alpha_1 + \alpha_2\rho_1 + \alpha_3\rho_1^2)^2$.
Comme le polynôme minimal de ρ_1 est de degré 3, le coefficient α_3 de ρ_1^2 est non nul.
En effectuant la division euclidienne de $G_n(x)$ par le polynôme $q(x) = \alpha_1 + \alpha_2 x + \alpha_3 x^2$, on obtient :

$$G_n(x) = (\beta_1 + \beta_2 x)(\alpha_1 + \alpha_2 x + \alpha_3 x^2) + (r_1 x + r_2), \tag{4.2.4}$$

Remplaçant x par ρ_1 on a l'égalité

$$(\beta_1 + \beta_2\rho_1)(\alpha_1 + \alpha_2\rho_1 + \alpha_3\rho_1^2) = -(r_1 + r_2\rho_1), \tag{4.2.5}$$

où β_2 n'est pas nul car ρ_1 est de degré 3.
En divisant par β_2 et élevant au carré on obtient l'identité :

$$(\rho_1 + \beta_1/\beta_2)^2(\alpha_1 + \alpha_2\rho_1 + \alpha_3\rho_1^2)^2 = (r_1'\rho_1 + r_2')^2.$$

Le polynôme unitaire, de degré 3 $(x + \beta_1/\beta_2)^2(a - x) - (r_1'x + r_2')^2$ s'annule pour $x = \rho_i$; il est donc égal à $G_n(x)$.

La droite D_1 d'équation :

$$y = r_1'x + r_2'$$

rencontre la courbe E_n au point (a, b) et est tangente à la courbe au point rationnel d'abscisse $-\beta_1/\beta_2$. D'où $(a, b) \in 2E_n(\mathbb{Q})$. Ce qui termine la démonstration de la proposition.

4.2.1 Cas local

Soit p une place finie ou infinie de $\mathbb{Q}$, $\mathbb{Q}_p$ désignera le complété de $\mathbb{Q}$ en p. Ce sera le corps p-adique ou bien le corps des nombres réels $\mathbb{R}$. On désigne par $K_{\mathfrak{p}}$ le complété de K en l'idéal premier $\mathfrak{p}$ au dessus de p. On identifie K à un sous corps de $K_{\mathfrak{p}}$.
Si $k = \mathbb{Q}_p$ la $\mathbb{Q}_p$-algèbre $A_{\mathbb{Q}_p}$ sera notée :

$$A_{\mathbb{Q}_p} = K_p = \mathbb{Q}_p[X]/(G_n(X)).$$

Nous étudierons alors deux cas :
Premier cas :
Si G_n n'a pas de racines dans $\mathbb{Q}_p$ alors K_p est de degré 3 sur $\mathbb{Q}_p$. Dans ce cas, l'idéal $p\mathbb{Z}_K$ ne se décompose pas dans l'extension $K/\mathbb{Q}$. L'homomorphisme associé à $k = \mathbb{Q}_p$ sera noté et défini de la manière suivante :

$$\lambda_p : E_n(\mathbb{Q}_p) \to K_p^*/K_p^{*2}, (x, y) \mapsto (x - \rho_1) \mod K_p^{*2}.$$

Son noyau est égal à $2E_n(\mathbb{Q}_p)$.
Cet homomorphisme induit un homomorphisme injectif $\overline{\lambda_p}$: $E_n(\mathbb{Q}_p)/2E_n(\mathbb{Q}_p) \to K_p^*/K_p^{*2}$, $\overline{\lambda_p} : (x, y) \mod 2E_n(\mathbb{Q}_p) \mapsto (x - \rho_1) \mod K_p^{*2}$.
Deuxième cas :
Si G_n a trois racines dans $\mathbb{Q}_p$, qu'on notera ρ_i avec $1 \leq i \leq 3$, alors $p\mathbb{Z}_K$ se décompose et

$$K_p \backsimeq \mathbb{Q}_p[T]/(T - \rho_1) \times \mathbb{Q}_p[T]/(T - \rho_2) \times \mathbb{Q}_p[T]/(T - \rho_3),$$

comme $Q_p[T]/(T - \rho_i) \backsimeq K_{\mathfrak{p}_i} \backsimeq \mathbb{Q}_p$, pour $1 \leq i \leq 3$, alors $K_p \backsimeq \mathbb{Q}_p^3$.
On va tout d'abord étudier les racines du polynôme G_n dans $\mathbb{Q}_p$.
Si p est une place infinie, alors $\mathbb{Q}_p$ est le corps des nombres réels $\mathbb{R}$. Le produit des racines de G_n étant négatif, et comme $\rho_1\rho_2 + \rho_1\rho_3 + \rho_2\rho_3 = -n^2$ alors le polynôme G_n possède une racine négative qui sera notée ρ_1, et deux racines positives qui seront notées ρ_2 et ρ_3 .
Si p est une place finie divisant $n-1$, le discriminant de G_n n'est pas nul et est égal à $(n-1)^2(n^2+3)^2(n^2-3n+1)^2$ et $G_n(x) \equiv (x-1)^2(x+1) \mod p$. On

a donc une racine dans $\mathbb{Q}_p$ qui est congru à $-1 \mod p$ que l'on notera ρ_1 et deux autres racines ρ_2 et ρ_3 qui sont congrus à $1 \mod p$. Plus précisément, si $n-1 = p^a q$ avec $(p,q) = 1$, en calculant le développement de Hensel des racines ρ_2 et ρ_3, on notera ρ_2 la racine telle que $\rho_2 = 1 + a_1 p^a + \cdots + o(p^m)$, avec $a_1 \neq 0$ et pour $i \neq 1$, $0 \leq a_i \leq p-1$, et ρ_3 la racine telle que $\rho_3 = 1 + b_1 p^{2a} + \cdots + o(p^m)$ avec $0 \leq b_i \leq p-1$. On a alors $v_p(\rho_2 - \rho_3) = a = v_p(n-1)$.
Si p est une place finie ne divisant pas $n-1$, les trois racines du polynôme G_n sont distinctes modulo p.
Exemples: Soit le polynôme $G_{16}(x) = x^3 + 3629x^2 - 256x + 1$, ses racines dans $\mathbb{Q}_3$ sont égales à : $\rho_1 = 2 + 3^3 + 2.3^7 + 3^8 + o(3^9)$, $\rho_2 = 1 + 3 + 3^4 + 2.3^5 + 2.3^6 + 2.3^8 + o(3^9)$, et $\rho_3 = 1 + 3^2 + 3^4 + 3^6 + 3^7 + 3^8 + o(3^9)$.
Dans $\mathbb{Q}_5$, les racines sont les suivantes : $\rho_1 = 4 + 5 + 4.5^3 + 3.5^5 + 3.5^7 + 5^8 + o(5^{10})$, $\rho_2 = 1 + 3.5^2 + 5^3 + 5^4 + 3.5^5 + 4.5^7 + o(5^9)$, et $\rho_3 = 1 + 2.5 + 5^2 + 2.5^4 + 2.5^5 + 3.5^6 + 2.5^8 + o(5^9)$.

D'après la proposition **??**, on a l'homomorphisme local $\lambda_p : E_n(\mathbb{Q}_p) \to (\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2)^3$, défini par

$$(x,y) \mapsto (x-\rho_1, x-\rho_2, x-\rho_3) \mod (\mathbb{Q}_p^{*2})^3 \text{ si } x \neq \rho_i,$$

$$(\rho_1, 0) \mapsto (G_n'(\rho_1), \rho_1 - \rho_2, \rho_1 - \rho_3) \mod (\mathbb{Q}_p^{*2})^3,$$
$$(\rho_2, 0) \mapsto (\rho_2 - \rho_1, G_n'(\rho_2), \rho_2 - \rho_3) \mod (\mathbb{Q}_p^{*2})^3,$$
$$(\rho_3, 0) \mapsto (\rho_3 - \rho_1, \rho_3 - \rho_2, G_n'(\rho_3)) \mod (\mathbb{Q}_p^{*2})^3.$$

Remarque 9. *Dans les deux cas étudiés, on appellera l'homomorphisme $\lambda_p : E_n(\mathbb{Q}_p) \to K_p^*/K_p^{*2}$, l'homomorphisme local associé à p.*

4.2.2 Caractérisation de $\mathrm{Im}\lambda_p$.

Nous caractérisons les éléments de $\mathrm{Im}\lambda_\mathrm{p}$, en distinguant deux cas $p \nmid n-1$ et $p | n-1$.
Par la suite, pour $\alpha \in K^*$, α', α'' désigneront les conjugués de α ; $[\alpha]$ désigne la classe de α dans K^*/K^{*2} et $[\alpha]_p$ la classe de α dans K_p^*/K_p^{*2}.

Cas où $p \nmid n-1$.

Lemme 4. *Soit p un nombre premier qui ne divise pas $n-1$, $\mathfrak{p}$ un idéal premier au dessus de p. Soit $\alpha \in K^*$ tel que $[\alpha]_p \in Im\lambda_p$ alors α a une valuation $\mathfrak{p}$-adique paire.*

Preuve :
1) Si $p\mathbb{Z}_K$ ne se décompose pas dans $K/\mathbb{Q}$, alors $p\mathbb{Z}_K$ est inerte ou ramifié c'est-à-dire $p\mathbb{Z}_K = \mathfrak{p}$ ou $p\mathbb{Z}_K = \mathfrak{p}^3$ où $\mathfrak{p}$ est un idéal premier au dessus de p.

Soit α un représentant d'un élément $[\alpha]_p$ de K_p^*/K_p^{*2}, où $[\alpha]_p \in \mathrm{Im}\lambda_{\mathfrak{p}}$, alors il existe $\beta \in K_{\mathfrak{p}}^*$ et $(x,y) \in E_n(\mathbb{Q}_p)$ tel que $\alpha = (x-\rho_1)\beta^2$. Comme $K_p/\mathbb{Q}_p$ est cubique, et $x-\rho_1$, $x-\rho_2$, $x-\rho_3$ sont conjugués sur $\mathbb{Q}_p$, alors leurs valuations p-adique sont égales. D'autre part, le produit $(x-\rho_1)(x-\rho_2)(x-\rho_3)$ est un carré alors $v_p(x-\rho_i) \equiv 0 \mod 2$. Il en résulte que α a une valuation $\mathfrak{p}$-adique paire.
2) Si $p\mathbb{Z}_K$ se décompose dans $K/\mathbb{Q}$, alors $p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$. Soit $(\alpha, \alpha', \alpha'')$ un représentant d'un élément $[\alpha]_p$ de K_p^*/K_p^{*2}, où $[\alpha]_p \in \mathrm{Im}\lambda_{\mathfrak{p}}$. Alors il existe $\beta_i \in \mathbb{Q}_p^*$ et $(x,y) \in E_n(\mathbb{Q}_p)$ tels que $(\alpha, \alpha', \alpha'') = ((x-\rho_1)\beta_1^2, (x-\rho_2)\beta_2^2, (x-\rho_3)\beta_3^2)$. Posons $v_p(x-\rho_i) = m_i$, $1 \leq i \leq 3$. Comme le produit $(x-\rho_1)(x-\rho_2)(x-\rho_3)$ est un carré alors

$$m_1 + m_2 + m_3 \equiv 0 \mod 2. \tag{4.2.6}$$

Si $m_1 < 0$, comme $v_p(\rho_1) = 0 \neq m$ alors $v_p(x) = inf(v_p(x-\rho_1), v_p(\rho_1)) = m_1$. De plus, $v_p(\rho_2) = 0$ donc $v_p(x-\rho_2) = inf(v_p(x), v_p(\rho_2)) = m_1$, et de même $v_p(x-\rho_3) = m_1$. En remplaçant dans **??**, on déduit alors que m_1 est pair.
Si $m_1 > 0$, comme l'idéal $p\mathbb{Z}_K$ se décompose dans l'extension $K/\mathbb{Q}$ alors p ne divise pas le discriminant du corps, il en résulte que $v_p(\rho_i - \rho_j) = 0$ si $i \neq j$. On a alors $v_p(x-\rho_j) = inf(v_p(x-\rho_1), v_p(\rho_1 - \rho_j)) = 0$, $2 \leq j \leq 3$. On en déduit alors que $m_i \equiv 0 \mod 2$ pour $1 \leq i \leq 3$.

Remarque 10. *La condition " p ne divise pas $n-1$" est seulement essentielle pour la preuve du cas $m_1 > 0$.*

Proposition 27. *Supposons que $p \nmid n-1$ et p décomposé. Soit $\alpha \in K^*$, alors $[\alpha]_p$ est dans $\mathrm{Im}\lambda_p$ si et seulement si le produit $\alpha\alpha'\alpha''$ est un carré de $\mathbb{Q}_p^*$.*

Preuve : Soit $(\alpha, \alpha', \alpha'')$ un représentant de l'élément $[\alpha]_p$ de $Im\lambda_p$ alors il existe $\beta_i \in \mathbb{Q}_p^*$ et $(x,y) \in E_n(\mathbb{Q}_p)$ tels que $(\alpha, \alpha', \alpha'') = ((x-\rho_1)\beta_1^2, (x-\rho_2)\beta_2^2, (x-\rho_3)\beta_3^2)$, on déduit alors que le produit $\alpha\alpha'\alpha''$ est un carré de $\mathbb{Q}_p^*$. De plus, d'après le lemme **??**, $\alpha = p^{2m}u, \alpha' = p^{2m'}u'$ et $\alpha'' = p^{2m''}u''$, où $u, u', u'' \in \mathbb{Z}_p^*$ et $m, m', m'' \in \mathbb{Z}$.
Considérons l'application $\mu : \mathrm{Im}\lambda_p \to (\mathbb{Z}_p^*/\mathbb{Z}_p^{*2})^3$, définie par

$$(\alpha_1, \alpha_2, \alpha_3) \mod (\mathbb{Q}_p^{*2})^3 \mapsto (u_1, u_2, u_3) \mod (\mathbb{Z}_p^{*2})^3,$$

où $\alpha_i = p^{2m_i}u_i$, $m_i \in \mathbb{Z}, u_i \in \mathbb{Z}_p^*, 1 \leq i \leq 3$. L'application μ est un homomorphisme injectif, et le 2-rang de $\mathrm{Im}\lambda_p$ est égal à 2. En effet, les racines de G_n sont dans K et $K \hookrightarrow \mathbb{Q}_p$. Les points d'ordre 2 sont dans $E_n(\mathbb{Q}_p)$, ce qui entraîne que $(\mathbb{Z}/2\mathbb{Z})^2 \subset \mathrm{Im}\lambda_p$. Comme μ n'est pas surjectif alors $\mathrm{Im}\lambda_p \backsimeq (\mathbb{Z}/2\mathbb{Z})^2$. Comme $[\alpha]_p \in K_p^*/K_p^{*2}$ alors $\alpha = p^j u, \alpha' = p^{j_1}u', \alpha" = p^{j_2}u''$ ($j,\ j_1,\ j_2 \in \mathbb{Z}$ et $u, u', u'' \in \mathbb{Z}_p^*$). D'autre part, $\alpha\alpha'\alpha''$ est un carré de $\mathbb{Q}_p^*$, donc

$uu'u''$ est un carré de $\mathbb{Z}_p^*$, d'où $[\alpha]_p \in \mathrm{Im}\lambda_p$. Ce qui termine la démonstration de la proposition.

Cas où $p|n-1$**.**

Proposition 28. *Soit* $R=(x_R,y_R)$ *tel que* $R \in 2E_n(\mathbb{Q}_p)$*, si* $a=v_p(\rho_2-\rho_3)$ *est impair alors*

$$v_p(x_R-\rho_2)=v_p(x_R-\rho_3)<a,$$

si de plus la réduction est non déployée ou si $a=1$

$$2E_n(\mathbb{Q}_p) \subset E_n^0(\mathbb{Q}_p).$$

Preuve :
Soit $R=(x_R,y_R) \in 2E_n(\mathbb{Q}_p)$ alors $x_R-\rho_1$, $x_R-\rho_2$ et $x_R-\rho_3$ sont des carrés dans $\mathbb{Q}_p^*$ et leurs valuations sont paires.
Si $a<v_p(x_R-\rho_2)$ alors $v_p(x_R-\rho_3)=inf(a,v_p(x_R-\rho_2))=a$, contredit le fait que a est impair, on en déduit que :

$$v_p(x_R-\rho_2)=v_p(x_R-\rho_3)<a.$$

Si de plus, $a=1$ on en déduit que $v_p(x_R-\rho_2)=v_p(x_R-\rho_3)\leq 0$ et donc $R \in E_n^0(\mathbb{Q}_p)$.
Supposons la réduction non déployée, si $v_p(x_R-\rho_2)<0$, alors $R \in E_n^0(\mathbb{Q}_p)$. Si $v_p(x_R-\rho_2)>0$, comme $x_R-\rho_1=x_R-\rho_2+\rho_2-\rho_1$ et $v_p(\rho_2-\rho_1)=0$ donc $v_p(x_R-\rho_1)=0$ i.e $x_R-\rho_1 \equiv \rho_2-\rho_1 \mod p$, comme $x_R-\rho_1$ est un carré alors $\rho_2-\rho_1$ est un carré modulo p, ce qui contredit le fait que la réduction soit non déployée.

Proposition 29. *Soit* p *un nombre premier, différent de 2, tel que* $p|n-1$*. Soit l'application* $\lambda_p : E_n(\mathbb{Q}_p) \to (\mathbb{Q}_p^*/\mathbb{Q}_p^{*2})^3$*, défini par*

$$R=(x,y) \mapsto (x-\rho_1, x-\rho_2, x-\rho_3) \mod (\mathbb{Q}_p^{*2})^3$$

Si la réduction est déployée en p, alors $x-\rho_1$ *est un carré de* $\mathbb{Q}_p^*$*.*
Si la réduction n'est pas déployée en p et $(x,y) \in E_n^0(\mathbb{Q}_p)$*, alors* $x-\rho_1$ *est un carré de* $\mathbb{Q}_p^*$*.*

Preuve :
Soit $R=(x,y) \notin E_n^0(\mathbb{Q}_p)$ alors (x,y) se réduit sur le point $(1,0)$. Donc $x-\rho_1 \equiv \rho_2-\rho_1 \mod p$ et comme $\rho_2-\rho_1 \equiv 2 \mod p$ et 2 est un carré modulo p , on déduit alors que $x-\rho_1$ est un carré modulo p. C'est donc un carré de $\mathbb{Z}_p^*$ car $p \neq 2$.

Si $R \in E_n^0(\mathbb{Q}_p)$ et $R \notin E_n^1(\mathbb{Q}_p)$ alors $v_p(x-\rho_2) = v_p(x-\rho_3) = 0$ et $x-\rho_2 \equiv x-\rho_3 \mod p$, donc $(x-\rho_2)(x-\rho_3)$ est un carré dans $\mathbb{Q}_p^*$, comme le produit $(x-\rho_1)(x-\rho_2)(x-\rho_3)$ est aussi un carré, alors $x-\rho_1$ est un carré de $\mathbb{Q}_p^*$.
Si $R \in E_n^1(\mathbb{Q}_p)$ alors les valuations de $x-\rho_i$ sont négatives et $x-\rho_i = p^{-2n}e_i$ avec $1 \leq i \leq 3$ et $e_i \in \mathbb{Z}_p^*$. Comme $e_i \equiv e_j \mod p$ et $e_i^3 \equiv \eta^2 \mod p$ alors e_i est un carré.

Exemples:
1. Soit la courbe elliptique E_{-34}, donnée par l'équation $y^2 = x^3 - 1156x^2 - 41721x + 1$. Le point $P_1 = (-2204/64, 10115/64)$ est un point de la courbe, $P_1 \in E_{-34}^0(\mathbb{Q}_5)$ mais $P_1 \notin E_{-34}^0(\mathbb{Q}_7)$; d'autre part, le développement de Hensel en $p = 5$ jusqu'a l'ordre 9 de $-2204/64 - \rho_1$, est comme suit : $-2204/64 - \rho_1 = 5^2 + 2.5^4 + 5^5 - 3.5^6 - 5^7 + o(5^9)$, donc $-2204/64 - \rho_1 = 5^2.u$ tel que $u = 1 + 2.5^2 + 5^3 - 3.5^4 - 5^5 + o(5^7)$, et u est une unité de $\mathbb{Q}_5$ et $\overline{u}$ est un carré de $\mathbb{F}_5$.
Donc $-2204/64 - \rho_1$ est un carré de $\mathbb{Q}_5^*$. Comme 3 est un carré de $\mathbb{F}_5$, et $-2204/64 - \rho_2 = 3 - 5 + 4.5^2 + 5^3 + 5^4 + 2.5^5 + 5^7 + o(5^9)$, $-2204/64 - \rho_3 = 3 + 2.5 - 2.5^2 - 5^3 + 2.5^7 + o(5^9)$; donc ce sont des unités de $\mathbb{Q}_5^*$. On remarquera que $-2204/64 - \rho_2, -2204/64 - \rho_3$ sont aussi des carrés de $\mathbb{Q}_5^*$; ce qui n'est pas le cas toujours. Comme le montre l'exemple suivant.

2. Soit la courbe elliptique E_{10} d'équation : $y^2 = x^3 - 100x^2 + 827x + 1$, le point $P = (834/8, 2911/8)$ est un point de la courbe, et il appartient à $E_{10}^0(\mathbb{Q}_3)$. Le nombre $834/8 - \rho_1 = 1 - 2.3 + 2.3^4 + 2.3^5 - 2.3^6 + o(3^6)$ est bien un carré de $\mathbb{Q}_3^*$, par contre les nombres $834/8 - \rho_2 = -1 - 3^2 + 3^5 - 2.3^6 + o(3^6)$, et $834/8 - \rho_3 = -1 + 3^5 - 3^6 + o(3^6)$, ne sont pas des carrés de $\mathbb{Q}_3^*$.

Corollaire 30. *Soit $(x, y) \in E_n(\mathbb{Q})$. L'idéal principal $(x - \rho_1)$ a pour décomposition*

$$(x - \rho_1) = \mathfrak{a}\mathfrak{b}^2$$

où $\mathfrak{a} = \prod_{p|n-1}(\mathfrak{p}_2\mathfrak{p}_3)^{\gamma_p}$ et $\gamma_p \in \{0, 1\}$.

Preuve : La preuve se déduit du lemme **??** (resp. de la proposition **??**) quand $p \nmid n-1$ (resp. $p \mid n-1$ et E_n déployée ou E_n non déployée tel que $(x, y) \in E_n^0(\mathbb{Q}_p)$).
Si $(x, y) \notin E_n^0(\mathbb{Q}_p)$ et E_n non déployée alors $v_{\mathfrak{p}_1}(x - \rho_1) = 0$ et $v_{\mathfrak{p}_1}(x - \rho_2) > 0$. Comme le produit $(x - \rho_1)(x - \rho_2)(x - \rho_3)$ est un carré. Alors si $v_{\mathfrak{p}_1}(x - \rho_2)$ est impair, donc $v_{\mathfrak{p}_1}(x - \rho_3)$ est impair. Ce qui termine la preuve du corollaire.

Remarque 11. *Donnons des exemples de n et p tels que $\gamma_p = 1$.*

Exemples:
I. Considérons la courbe elliptique E_8 donnée par l'équation :

$$y^2 = x^3 - 64x^2 + 405x + 1.$$

Le point $(64, 161)$ est un point de la courbe E_8. La décomposition en ideaux premiers de l'ideal principal $(64 - \rho_1)$ est la suivante :

$$(64 - \rho_1) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{c}^2,$$

avec $\mathfrak{p}_2 = \mathfrak{p}_1^{\sigma}$, $\mathfrak{p}_3 = \mathfrak{p}_1^{\sigma^2}$, $\mathfrak{c} = 23\mathbb{Z}_K + (5 + \rho_1)\mathbb{Z}_K$, et $\mathfrak{p}_1 = 7\mathbb{Z}_K + (\rho_1 + 1)\mathbb{Z}_K$.
On déduit alors que les valuations $\mathfrak{p}_i$-adique, pour $2 \leq i \leq 3$, de $64 - \rho_1$ sont impaires.

II. Considérons la courbe elliptique E_{22} donnée par l'équation :

$$y^2 = x^3 - 484x^2 + 9743x + 1,$$

le point $(8980/8000, 813057/8000)$ est un point de la courbe. En utilisant le programme Pari, on a

$$(8980/8000 - \rho_1) = \mathfrak{n}^{-4}\mathfrak{m}^2\mathfrak{m}_1^{\sigma}(\mathfrak{m}_1^{\sigma^2})^3\ \mathfrak{m}_2^{-2}\mathfrak{m}_3^2,$$

avec $\mathfrak{n} = 2\mathbb{Z}_K$, $\mathfrak{m} = 3\mathbb{Z}_K + (\rho_1 + 1)\mathbb{Z}_K$, $\mathfrak{m}_1 = 7\mathbb{Z}_K + (\rho_1 + 1)\mathbb{Z}_K$, $\mathfrak{m}_2 = 5\mathbb{Z}_K$, $\mathfrak{m}_3 = 5531\mathbb{Z}_K + (2474 + \rho_1)\mathbb{Z}_K$.
On déduit alors que $v_{\mathfrak{m}}(8980/8000 - \rho_1) = 2$ et $v_{\mathfrak{m}_i}(8980/8000 - \rho_1) = 1$, pour $\mathfrak{m}_i = \mathfrak{m}^{\sigma^{i-1}}, 2 \leq i \leq 3$.

III. Considérons la courbe elliptique E_{26} donnée par l'équation :

$$y^2 = x^3 - 676x^2 + 16299x + 1.$$

Les points $(1, 125)$ et $(24, 125)$ sont des points de la courbe E_{26}. Les décompositions en ideaux premiers des ideaux principaux $(1 - \rho_1)$ et $(24 - \rho_1)$:

$$(1 - \rho_1) = \mathfrak{l}_2^4\mathfrak{l}_3^2,$$

tels que $\mathfrak{l}_2 = \mathfrak{l}_1^{\sigma}$, $\mathfrak{l}_3 = \mathfrak{l}_1^{\sigma^2}$, et $\mathfrak{l}_1 = 5\mathbb{Z}_K + (\rho_1 + 1)\mathbb{Z}_K$,
On déduit alors que $v_{\mathfrak{l}_2}(1 - \rho_1) = 4$, $v_{\mathfrak{l}_3}(1 - \rho_1) = 2$. Donc les valuations $\mathfrak{l}_i$-adiques de $1 - \rho_1$, $2 \leq\ i\ \leq\ 3$, sont paires.

Si $p|n - 1$, deux difficultés apparaissent :

1. la première est liée à la non parité de $v_p(x-\rho_1)$ montrée dans les exemples précédents.

2. La deuxième est liée au fait qu'on ne peut plus utiliser les points d'ordre 2 pour étudier $Im\lambda_p$.

La proposition suivante donne un équivalent de la proposition **??** avec des hypothéses sur n et en restreignant λ_p.
Soit

$$H_p = \{[\alpha]_p \in (\mathbb{Q}_p^*/\mathbb{Q}_p^{*2})^3 : \alpha \in K^*, v_p(\alpha) \equiv v_p(\alpha') \equiv v_p(\alpha'') \equiv 0 \bmod 2\}.$$

Posons $H'_p = \lambda_p^{-1}(H_p)$. Soit l'homomorphisme $\lambda'_p : H'_p \to (\mathbb{Q}_p^*/\mathbb{Q}_p^{*2})^3$.

Proposition 31. *Supposons que $n-1 = m^2$ (resp. $-m^2$) avec $m \in \mathbb{Z}$. Soit p un nombre premier et $p \mid m$.*
1) Si $p \equiv \pm 3$ mod 8, alors $[\alpha]_p$ est dans $\mathrm{Im}\lambda'_p$ si et seulement si le produit $\alpha\alpha'\alpha''$ est un carré de $\mathbb{Q}_p^*$ et $\alpha, \alpha', \alpha''$ ont des valuations p-adique paires.
2) Si $p \equiv -1$ mod 8, alors $[\alpha]_p$ est dans $\mathrm{Im}\lambda'_p$ si et seulement si α et $\alpha\alpha'\alpha''$ sont des carrés de $\mathbb{Q}_p^*$ et $\alpha, \alpha', \alpha''$ ont des valuations p-adique paires.

Dans la preuve de cette proposition, on utilisera le résultat suivant, qu'on expliquera dans le dernier paragraphe : si $n-1 = m^2$ (resp. $-m^2$) le point $(1, m^3)$ (resp. $(1-m^2, m^3)$) est un point de $E_n(\mathbb{Q})$.

Preuve : Soit $(\alpha, \alpha', \alpha'')$ un représentant de l'élément $[\alpha]_p$ de $\mathrm{Im}\lambda'_p$ alors il existe $\beta_i \in \mathbb{Q}_p^*$ et $(x, y) \in H'_p$ tels que $(\alpha, \alpha', \alpha'') = ((x-\rho_1)\beta_1^2, (x-\rho_2)\beta_2^2, (x-\rho_3)\beta_3^2)$ et les $x - \rho_i$, $1 \leq i \leq 3$, ont des valuations paires. On déduit alors que les valuations p-adique de α et ses conjugués sont paires.
Réciproquement, considérons l'application définie par

$$\mu' : \mathrm{Im}\lambda'_p \to (\mathbb{Z}_p^*/\mathbb{Z}_p^{*2})^3,$$

$$(\alpha_1, \alpha_2, \alpha_3) \mod (\mathbb{Q}_p^{*2})^3 \mapsto (u_1, u_2, u_3) \mod (\mathbb{Z}_p^{*2})^3$$

où $\alpha_i = p^{2m_i}u_i$, $m_i \in \mathbb{Z}$, $1 \leq i \leq 3$. L'application μ' est un homomorphisme injectif.
Étudions le 2-rang de $\mathrm{Im}\lambda'_{\mathrm{p}}$.
• Si $p \equiv \pm 3$ mod 8, alors 2 n'est pas un carré mod p et on va distinguer deux cas :
1) Si $p \equiv 1$ mod 4 alors -1 est un carré mod p et si $n-1 = m^2$ (resp. $-m^2$), comme $\rho_1 - \rho_i$, $2 \leq i \leq 3$, et $1-\rho_1$ sont congrus respectivement à -2 mod p et 2 mod p, alors $\rho_1 - \rho_i$, $2 \leq i \leq 3$, et $1-\rho_1$ ne sont pas des carrés dans $\mathbb{Q}_p^*$. On en déduit que les points $(\rho_1, 0)$ et $(1, m^3)$ (resp. $(\rho_1, 0)$ et $(1-m^2, m^3)$) ne sont pas dans $2E_n(\mathbb{Q}_p)$. D'autre part, les valuations p-adique de $\rho_1 - \rho_i$, $2 \leq i \leq 3$, et $1-\rho_j$, $1 \leq j \leq 3$ sont paires, donc les points $(\rho_1, 0)$ et $(1, m^3)$ (resp. $(\rho_1, 0)$ et $(1-m^2, m^3)$) sont dans H'_p. La première composante de $\lambda'_p(\rho_1, 0)$ est un

carré et celles de $\lambda'_p(1, m^3)$ et $\lambda'_p(1-m^2, m^3)$ sont égales à $1-\rho_1$ qui est congru à 2 mod p (non carré mod p). On en déduit que le 2-rang de $\mathrm{Im}\lambda'_{\mathrm{p}}$ est égal à 2.
2) Si $p \equiv 3 \bmod 4$ alors -1 n'est pas un carré mod p. Comme précédemment on montre que les points $(0,1)$ et $(1, m^3)$ (resp. $(0,1)$ et $(1-m^2, m^3)$) sont dans H'_p et ne sont pas dans $2E_n(\mathbb{Q}_p)$. Leurs images par λ'_p sont différentes, le 2-rang de $\mathrm{Im}\lambda'_p$ est égal à 2.
Comme $\alpha\alpha'\alpha''$ est un carré dans $\mathbb{Q}_p^*$, et $\alpha, \alpha', \alpha''$ ont des valuations paires alors $\alpha = p^{2j_1}u$, $\alpha' = p^{2j_2}u'$, $\alpha'' = p^{2j_3}u''$, $j_i \in \mathbb{Z}, 1 \leq i \leq 3$ et $uu'u''$ est dans $\mathbb{Z}_p^{*2}$. D'où $[\alpha]_p \in \mathrm{Im}\lambda'_p$.
• Si $p \equiv -1 \bmod 8$ alors 2 est un carré mod p. D'après la proposition **??**, on déduit que le 2-rang de $\mathrm{Im}\lambda'_p$ est strictement plus petit que 2. En reprenant les mêmes arguments utilisés dans 1), on montre alors que le point $(\rho_1, 0)$ est un point de H'_p qui n'est pas dans $2E_n(\mathbb{Q}_p)$, que la première composante de $\lambda'_p(\rho_1, 0)$ est un carré et que les deux autres composantes ne sont pas des carrés. Donc le 2-rang de $\mathrm{Im}\lambda'_p$ est égal à 1.
Comme α, $\alpha\alpha'\alpha''$ sont des carrés dans $\mathbb{Q}_p^*$, et $\alpha, \alpha', \alpha''$ ont des valuations paires alors $\alpha = p^{2j_1}u$, $\alpha' = p^{2j_2}u'$, $\alpha'' = p^{2j_3}u''$, $j_i \in \mathbb{Z}$, u et $uu'u''$ sont dans $\mathbb{Z}_p^{*2}$. D'où $[\alpha]_p \in \mathrm{Im}\lambda'_p$, ce qui montre la proposition.
Exemples: I. Considérons la courbe elliptique E_8 donnée par l'équation :

$$y^2 = x^3 - 64x^2 + 405x + 1.$$

Le point $(64, 161)$ est un point de la courbe E_8, donc le produit $(64-\rho_1)(64-\rho_2)(64-\rho_3)$ est un carré. D'autre part, la courbe E_8 a une réduction déployée en $p = 7$. Alors d'après la proposition **??**, $64-\rho_1$ est un carré de $\mathbb{Q}_7^*$, en effet, on a $64 - \rho_1 = 2 + 3.7 + 7^2 + o(7^2)$. D'autre part, par un simple calcul on obtient :

$$64 - \rho_2 = 7 - 3.7^2 + o(7^2),\ 64 - \rho_3 = 2.7 - 3.7^2 + o(7^2).$$

Donc $v_7(64 - \rho_i)$ est impair pour $2 \leq i \leq 3$. Ce qui implique que $[64 - \rho_1] \notin Im\lambda'_7$.

II. Considérons la courbe elliptique E_{26} donnée par l'équation :

$$y^2 = x^3 + 16299x^2 - 676x + 1.$$

Le point $(-24, 125)$ est un point de la courbe E_{26}. Par un simple calcul, on obtient :

$$-24 - \rho_1 = 2 + 2.5^2 + o(5^4),\ -24 - \rho_2 = 2.5^4 + o(5^4),$$

$$-24 - \rho_3 = 4.5^2 + 4.5^3 + 4.5^4 + o(5^4).$$

Donc $v_5(-24-\rho_i) \equiv 0 \bmod 2$. La courbe E_{26} a une réduction non déployée en 5, on déduit alors que $[-24-\rho_1] \in Im\lambda'_5$.

III. Considérons la courbe elliptique E_{-14} donnée par l'équation :

$$y^2 = x^3 - 196x^2 - 3181x + 1.$$

Le point $(459, 7345)$ est un point de la courbe E_{-14}. Par un simple calcul, on obtient :

$$459-\rho_1 = 4.5^2+5^3+o(5^4),\ 459-\rho_2 = 3-5+2.5^2+3.5^3+o(5^4),$$

$$459-\rho_3 = 3+5+2.5^2-2.5^4+o(5^4).$$

On déduit que $v_5(459-\rho_i) \equiv 0 \bmod 2, 1 \leq i \leq 3$. Comme $459-\rho_1$ et le produit $(459-\rho_1)(459-\rho_2)(459-\rho_3)$ sont des carrés dans $\mathbb{Q}_5^*$. Alors $[459-\rho_1]_5 \in \mathrm{Im}\lambda'_5$.

Chapitre 5

2-Rang du groupe des classes et rang de courbes elliptiques.

Soient k un corps de nombres, $C(k)$ le groupe des classes d'idéaux de k, et p un nombre premier. Depuis quelques années, plusieurs mathématiciens ont essayé de trouver des corps quadratiques avec un 3-rang assez élevé. Le problème correspondant dans le cas de degré 3, est de chercher des corps cubiques cycliques avec un 2-rang assez grand. Dans [**?**], L.C.Washington considère la famille de corps cubiques cycliques définis par les polynômes $P_a(x) = x^3 - (a+3)x^2 + ax + 1$, avec $a \in \mathbb{Z}$. Sous certaines conditions, le groupe des unités est explicitement déterminé. Il associe alors la famille de courbes elliptiques C_a sur $\mathbb{Q}$ d'équation $y^2 = P_a(x)$. Le corps de définition des points d'ordre 2 de C_a est le corps cubique défini par P_a. Il établit par une 2-descente une relation entre le 2-rang du groupe des classes des corps cubiques et le rang des courbes elliptiques. Par ailleurs, il choisit a tel que les réductions de la courbe C_a modulo les petits nombres premiers possèdent un grand nombre de points. Ces exemples donnent lieu à des courbes elliptiques de rang élevé, ce qui donne des corps cubiques avec un 2-rang assez grand. Les résultats de L.C.Washington ont été généralisés à d'autres corps cubiques par Kawachi et Nakano [**?**].
Dans ce chapitre, nous étudierons le lien entre les courbes elliptiques E_n données par l'équation : $y^2 = G_n(x)$ et le 2-rang du groupe des classes des corps cubiques K engendrés par une racine ρ du polynôme

$$G_n(x) = x^3 - n^2x^2 + (n^3 - 2n^2 + 3n - 3)x + 1.$$

On commencera tout d'abord par faire quelques rappels. Soit $\mathbb{Z}_k$ l'anneau des entiers du corps de nombres k. L'ensemble des places de k constitué des idéaux premiers de $\mathbb{Z}_k$ (places finies) et des places à l'infini ainsi définies : on considére les $[k : \mathbb{Q}]$ $\mathbb{Q}$-isomorphismes (ou plongements) distincts $\sigma : k \to \mathbb{C}$, de k dans

$\mathbb{C}$; parmi eux il y en a r qui sont réels et il y en a $2s$ qui sont complexes, tel que $r + 2s = [k : \mathbb{Q}]$.
Chaque fois que le plongement est réel, on lui associe une place à l'infini appelée place réelle. Pour chaque paire $\{\sigma, \tau\}$ de plongements complexes conjugués, on lui associe une seule place à l'infini appelée place complexe.

Définition 24. *Soit $\mathfrak{p}$ une place (finie ou infinie) de k. Le complété de k en $\mathfrak{p}$ sera noté $k_\mathfrak{p}$. Le* symbole de Hilbert local, *noté par $(x, y)_\mathfrak{p}$, est défini par*

$$(x, y)_\mathfrak{p} = \begin{cases} 1 & s'il\ existe\ \ (a, b)\ \in k_\mathfrak{p}^2\ tel\ que\ xa^2 + yb^2 = 1 \\ -1 & sinon \end{cases}$$

Définition 25. *Un élément de k est totalement positif s'il est positif en chaque plongement réel de k. L'ensemble des éléments totalements positifs sera noté k^+.*

Utilisons ces définitions pour les corps $k = K$. Comme K est une extension cubique totalement réelle de $\mathbb{Q}$, il y a trois places réelles, qu'on notera $\mathfrak{p}_\mathfrak{j}$, $1 \leq j \leq 3$, associées aux plongements réels η_j de K.
On définit l'application $\eta : K^* \to \{\pm 1\}^3$ par

$$\eta : x \mapsto ((-1, x)_{\mathfrak{p}_1}, (-1, x)_{\mathfrak{p}_2}, (-1, x)_{\mathfrak{p}_3})$$

Remarque 12. *Soient $\mathfrak{p}$ une place réelle de K, $\alpha \in K^*$. Alors α est totalement positif $\Leftrightarrow \quad \forall \ \mathfrak{p}, \quad (-1, \alpha)_\mathfrak{p} = 1$.*

Lemme 5. *L'application η est un homomorphisme, dont le noyau est égal à K^+. La suite*

$$1 \longrightarrow K^+ \longrightarrow K^* \xrightarrow{\eta} \{\pm 1\}^3 \longrightarrow 1$$

est exacte.

Preuve : La preuve se déduit de la remarque précédente.

On se propose de caractériser les unités totalement positives de K.

Lemme 6. *Toute unité de K totalement positive est un carré. Soit $\mathfrak{p}_\mathfrak{i}$ une place réelle de K, $1 \leq i \leq 3$. La restriction de η à U_K induit un isomorphisme $\overline{\eta} : U_K/U_K^2 \to \{\pm 1\}^3$, définie par*

$$\overline{\eta} : [u] \mapsto ((-1, u)_{\mathfrak{p}_1}, (-1, u)_{\mathfrak{p}_2}, (-1, u)_{\mathfrak{p}_3}).$$

Preuve :
Le groupe U_K des unités est isomorphe à $\{\pm 1\} \times \mathbb{Z}^2$. Les unités ρ_1, ρ_2 engendrent le groupe $U_K/\{\pm 1\}$.
Donc U_K/U_K^2 a pour représentant $\{\pm 1, \pm\rho_1, \pm\rho_2, \pm\rho_1\rho_2\}$. On constate que ces représentants (sauf 1) ne sont pas totalement positifs.
L'homomorphisme $\overline{\eta}$ a pour noyau U_K^+/U_K^2 et comme toute unité de K totalement positive est un carré alors les ordres des groupes U_K^+/U_K^2 et $\{\pm 1\}^3$ sont égaux, donc $\overline{\eta}$ est bijective.

Remarque 13. *Nous pouvons généraliser la première partie du lemme* **??** *à un corps cubique totalement réel, dont le groupe des unités est engendré par des unités de signes contraires.*

5.1 Groupe de classes au sens ordinaire (resp. au sens restreint).

Soit $I(k)$ le groupe des idéaux fractionnaires de k. Etant donnée deux idéaux I et J de $I(k)$, on définit la relation d'équivalence :

$$I \backsimeq J \;\Leftrightarrow\quad \exists\, \alpha \in K^* \text{ tel que } I = (\alpha)J$$

L'ensemble de ces classes d'équivalence forme un groupe appelé le groupe des classes d'idéaux de k, que l'on note $C(k)$, on montre que ce groupe est fini et son ordre est noté $h(k)$.
On définit une autre relation d'équivalence appelée relation d'équivalence au sens restreint :

$$I \backsim J \;\Leftrightarrow\; \exists\, \alpha \in K^* \text{ totalement positif tel que } I = (\alpha)J$$

L'ensemble des classes d'équivalences au sens restreint forme un groupe appelé le groupe des classes d'idéaux au sens restreint, qui sera noté $C^+(k)$, on montre que c'est un groupe fini et $h^+(k)$ désignera l'ordre de ce groupe.
Il est clair que si $I \backsim J$ alors $I \backsimeq J$, ce qui définit un homomorphisme surjectif

$$g : C^+(k) \to C(k).$$

Si $k = K$, on a la proposition suivante :

Proposition 32. *L'application $g : C_+(K) \to C(K)$ est un isomorphisme de groupes.*

Preuve :
La surjectivité se déduit par construction.
Si I est dans le noyau de g, i.e $I = (\alpha)$, il existe une unité ϵ telle que $\epsilon\alpha$ soit totalement positive car $\overline{\eta}$ est bijective. Ainsi $I = (\epsilon\alpha)$ et donc $I \backsim O$.
On se propose de faire quelques rappels sur la théorie du corps de classe.

Définition 26. *Soient k un corps, $C(k)$ le groupe des classes d'idéaux de k et A un sous-groupe de $C(k)$. Une extension L/k est le corps de classe de A si*
a) L est une extension abélienne fini de k ;
b) L/k est non ramifée en toutes les places.

Théorème 12. *Pour chaque sous-groupe F de $C(k)$, il existe un corps de classe. Le corps de classe est unique, et $C/F \backsimeq Gal(L/k)$.*

Définition 27. *Soit k un corps de nombres, on appelle corps de classe de Hilbert au sens ordinaire (resp. au sens restreint) de k, que l'on note k_H (resp. k_H^+), la plus grande extension abélienne de k totalement non ramifiée (resp. non ramifiée en les places finies).*

Théorème 13. *Soit k_H (resp. k_H^+) le corps de classe de Hilbert au sens ordinaire (resp. au sens restreint) de k. Et $C(k)$ le groupe des classes d'idéaux au sens ordinaire (resp. au sens restreint) de k. Alors*

$$Gal(k_H/k) \backsimeq C(k) \text{ (resp. } Gal(k_H^+/k) \backsimeq C^+(k)).$$

On déduit le corollaire suivant dans le cas où $k = K$.

Corollaire 33. *Toute extension quadratique de K non ramifiée en les places finies, est totalement non ramifiée.*

Preuve :
D'après le théorème **??**, on a $Gal(K_H/K) \backsimeq C(K)$ (resp. $Gal(K_H^+/K) \backsimeq C^+(K)$), il en résulte que toutes les extensions quadratiques de K totalement non ramifiées (resp. non ramifiées en les places finies) sont en bijection avec les sous-groupes de $C(K)$ (resp. $C^+(K)$) d'indice 2. D'après la proposition **??**, on conclut.

Théorème 14. *Soit $\mathfrak{p}$ un ideal premier de O_k ; on a $\mathfrak{p}O_{k_H} = \prod_{1\leq i\leq r} \mathfrak{p}_i$. Et l'ordre de $\overline{\mathfrak{p}}$ dans $C(k)$ est égal à n/r, où $n = [k_H : k]$.*

Corollaire 34. *Les idéaux premiers de O_k sont des ideaux principaux de k_H et ils se décomposent totalement dans k_H.*

Définition 28. *Soit $C(k)$ le groupe de classes de k, on appelle* 2-groupe des classes*, que l'on note $C_2(k)$, le sous groupe de $C(k)$*

$$C_2(k) = \{\overline{X} \in C(k) \ / \ \overline{X}^2 = 1\}$$

et on appelle 2-rang *de $C_2(k)$, que l'on note r_2, la dimension de $C_2(k)$ en tant que $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel.*

La parité du 2-rang de $C(K)$ est donné par le théorème suivant.

Théorème 15. *Soit L/M une extension cyclique de degré n. Soit p un nombre premier tel que $p \nmid n$. Supposons que tous les corps F tels que $M \subset F \subset L$, satisfont $p \nmid h_F$, où h_F est le nombre de classes de F. Soit A le p-sous-groupe de Sylow du groupe des classes de L et f l'ordre de p mod n. Alors*

$$r_a(A) \ \equiv \ n_a \equiv \ 0 \ mod \ f,$$

pour tout a_i, où $A \ \backsimeq \ \oplus \ \mathbb{Z}/p^{a_i}\mathbb{Z}$, n_a est le nombre de i tel que $a_i = a$, r_a est le nombre de i tel que $a_i \geq a$. En particulier, si $p|h_L$ alors le p-rang de A est au moins égal à f et $p^f|h_L$.

Dans notre cas, $L = K$ et $M = \mathbb{Q}$ et $n = [K : \mathbb{Q}] = 3$. Soit $p \ \equiv \ 2 \bmod 3$, alors $f = 2$. Soit A le p-sous groupe de Sylow de $C(K)$. Comme il n'y a pas de sous-corps entre $\mathbb{Q}$ et K, toutes les conditions du théorème sont vérifiées, alors le p^a-rang de $C(K)$ est pair pour tout p. On déduit alors que le 2-rang, r_2, de $C(K)$ est toujour pair.

5.2 Le 2-groupe de Selmer

Nous rappelons que dans le chapitre précédent, on a défini un homomorphisme local associé à une place p, de la manière suivante :

$\lambda_p : E_n(\mathbb{Q}_p) \to K_p^*/K_p^{*2}$, $(x, y) \mapsto (x-\rho) \mod K_p^{*2}$, si p n'est pas décomposé;

et il est défini comme suit, quand p est décomposé,

$\lambda_p : E_n(\mathbb{Q}_p) \to (\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2)^3$, $(x, y) \mapsto (x-\rho_1, x-\rho_2, x-\rho_3) \mod (\mathbb{Q}_p^{*2})^3$ si $x \neq \rho_i$,

$$\begin{aligned}
(\rho_1, 0) &\mapsto (G_n'(\rho_1), \rho_1 - \rho_2, \rho_1 - \rho_3) \mod (\mathbb{Q}_p^{*2})^3, \\
(\rho_2, 0) &\mapsto (\rho_2 - \rho_1, G_n'(\rho_2), \rho_2 - \rho_3) \mod (\mathbb{Q}_p^{*2})^3, \\
(\rho_3, 0) &\mapsto (\rho_3 - \rho_1, \rho_3 - \rho_2, G_n'(\rho_3)) \mod (\mathbb{Q}_p^{*2})^3.
\end{aligned}$$

Définition 29. *Étant donnée une place p et $\alpha \in K^*$, on notera $[\alpha]_p$ la classe de α dans K_p^*/K_p^{*2}. Le* 2-groupe de Selmer*, noté par $S_2(\mathbb{Q})$, est défini par :*

$$S_2(\mathbb{Q}) = \{[\alpha] \in K^*/K^{*2} : \quad \forall \ \ p \ \ [\alpha]_p \in \text{Im } \lambda_p\}.$$

Soit U le sous-groupe de K^*/K^{*2},

$$U = \{[u] \in K^*/K^{*2} : [u]_p \in Im\lambda_p \ si \ p \nmid n-1$$
$$\text{ou si p est une place infini}, [u]_p \in Im\lambda'_p \ \text{ si } p|n-1\}.$$

Considérons le sous-groupe $S'_2(\mathbb{Q})$ de $S_2(\mathbb{Q})$ défini par :

$$S'_2(\mathbb{Q}) = \{[\alpha] \in S_2(\mathbb{Q}) : [\alpha] \in U\}.$$

Lemme 7. *Pour chaque élément $\alpha \in K^*$, tel que $[\alpha] \in S'_2(\mathbb{Q})$, il existe un idéal I_α tel que $(\alpha) = I_\alpha^2$. Si cet idéal est principal alors α ou $-\rho_1\alpha$ est un carré.*

Preuve :
Soit α un représentant d'un élément de $S'_2(\mathbb{Q})$, α' et α'' ses conjugués dans K. Alors $[\alpha] \in U$, donc $[\alpha]_p \in Im\lambda_p$ si $p \nmid n-1$ ou si p est une place infini, sinon$[\alpha]_p \in Im\lambda'_p$ si $p|n-1$. D'après le lemme **??** et la définition de $Im\lambda'_p$ la valuation p-adique de α est pair.
Décomposons l'idéal principal (α) en produit d'idéaux premiers,

$$(\alpha) = \prod_{1 \le i \le s} Q_i^{g_i}$$

avec $g_i = v_{Q_i}(\alpha) = 2b_i$.
L'égalité suivante défini I_α

$$(\alpha) = \prod_{1 \le i \le s} Q_i^{2b_i} = (\prod_{1 \le i \le s} Q_i^{b_i})^2 = I_\alpha^2.$$

Si I_α est principal, alors il existe une unité ϵ et un élément γ_1 de K^* tel que $I_\alpha = (\gamma_1)$ et $\alpha = \epsilon\gamma_1^2$.
Localement $[\alpha]_\infty \in \mathbb{R}$, il existe alors $(x, y) \in E_n(\mathbb{R})$ et $\alpha_i \in \mathbb{R}$ tels que $(\alpha, \alpha', \alpha'') = ((x-\rho_1)\alpha_1^2, (x-\rho_2)\alpha_2^2, (x-\rho_3)\alpha_3^2)$, et $(x-\rho_1)(x-\rho_2)(x-\rho_3)$ est un carré dans $\mathbb{R}$. D'autre part, ρ_1 est la racine négative du polynôme G_n et ρ_2, ρ_3 les racines positives telles que $\rho_2 \le \rho_3$ alors $x-\rho_1 > x-\rho_2 > x-\rho_3$, les signes de α, α', α'' sont : +, +, + ou +, -, -.
Dans le premier cas, l'unité ϵ est totalement positive, d'après le lemme **??**, ϵ est un carré. Ce qui implique que α est un carré.
Dans le second cas, $-\rho_1\epsilon$ est une unité totalement positive, d'après le

lemme **??**, $-\rho_1\epsilon$ est un carré. Donc $-\rho_1\alpha$ est un carré. Ce qui termine la démonstration de la proposition.

Exemples:
I. Considérons la courbe elliptique E_{22} d'équation $y^2 = x^3 - 484x^2 + 9743x + 1$. D'après le programme mwrank, les points $P_1 = (8520, 763819)$ et $P_2 = (8980/8000, 813057/8000)$ sont des points de la courbe E_{22}. Considérons $z = 8520 - \rho_1$, et $\eta = 8980/8000 - \rho_1$. D'après le programme Pari, la décomposition en idéaux premiers de l'idéal principal (z) est la suivante :

$$(z) = \mathfrak{p}_1^{\sigma}\mathfrak{p}_1^{\sigma^2}\mathfrak{a}^2\mathfrak{b}^2,$$

tels que $\mathfrak{p}_1 = 7\mathbb{Z}_K + (1+\rho_1)\mathbb{Z}_K$, $\mathfrak{a} = 19\mathbb{Z}_K + (-8+\rho_1)\mathbb{Z}_K$, $\mathfrak{b} = 5743\mathbb{Z}_K + (-2777+\rho_1)\mathbb{Z}_K$.
La décomposition en idéaux premiers de l'idéal principal (η) est la suivante :

$$(\eta) = \mathfrak{q}_1^{-4}\mathfrak{q}_2^2\mathfrak{q}_3^{-2}\ \mathfrak{p}_1^{\sigma}(\mathfrak{p}_1^{\sigma^2})^3\mathfrak{q}_4^2,$$

tels que $\mathfrak{q}_1 = 2\mathbb{Z}_K$, $\mathfrak{q}_2 = 3\mathbb{Z}_K + (1+\rho_1)\mathbb{Z}_K$, $\mathfrak{q}_3 = 5\mathbb{Z}_K$, $\mathfrak{q}_4 = 5531\mathbb{Z}_K + (2474+\rho_1)\mathbb{Z}_K$.
Donc $[z]$ et $[\eta]$ ne sont pas dans $S_2'(\mathbb{Q})$.

II. Soit la courbe elliptique E_{-8} d'équation $y^2 = x^3 - 64x^2 - 667x + 1$. Le point $(674/8, 2367/8)$ est un point de la courbe E_{-8}. Considérons $u = 674/8 - \rho_1$ alors la décomposition de l'idéal principal (u) en produit d'idéaux premiers est comme suit :

$$(u) = \mathfrak{q'}_1^2(\mathfrak{q'}_2^{\sigma})^2(\mathfrak{q'}_2^{\sigma^2})^2\mathfrak{q'}_4^2,$$

tels que $\mathfrak{q'}_1 = 2\mathbb{Z}_K$, $\mathfrak{q'}_2 = 3\mathbb{Z}_K + (\rho_1+1)\mathbb{Z}_K$, $\mathfrak{q'}_4 = 263\mathbb{Z}_K + (113+\rho_1)\mathbb{Z}_K$.
Donc les valuations p-adiques de u et ses conjugués sont paires, d'où $[u] \in U$ donc $[u] \in S_2'(\mathbb{Q})$.

5.3 Borne supérieure de Billing pour le rang d'une courbe elliptique.

Dans ce paragraphe, on énonce un résultat de Billing qui donne une majoration du rang d'une courbe elliptique sans points d'ordre 2 définis sur $\mathbb{Q}$. On se propose alors d'appliquer cette idée a notre famille de courbes elliptiques E_n. On commence tout d'abord par rappeller le résultat de Billings.

Soit E une courbe elliptique définie sur $\mathbb{Z}$:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in \mathbb{Z}.$$

On définit la 2-minimale b-forme, comme suit :

$$E' : y'^2 = x'^3 + 2^{2i-2}b_2x'^2 + 2^{4i-1}b_4x' + 2^{6i-2}b_6,\ a_i \in \mathbb{Z},$$

où $i \in \mathbb{Z}$ est choisi tel que E' soit défini sur $\mathbb{Z}$. Alors

$$x' = 2^{2i}x,\ y' = 2^{3i}(2y + a_1x + a_3),$$

définit un isomorphisme entre $E(\mathbb{Q})$ et $E'(\mathbb{Q})$. En particulier, les deux groupes ont le même rang.

Proposition 35. *Soit E une courbe elliptique définie sur $\mathbb{Z}$ et on suppose que ses points d'ordre 2 ne sont pas rationnels sur $\mathbb{Q}$. Soit E' la 2-minimale b-forme donnée par*

$$E' : y'^2 = x'^3 + ax'^2 + bx' + c = f(x'),$$

où $f(x')$ est irréductible sur $\mathbb{Q}$. Soit ϑ une racine de $f(x')$, $L = \mathbb{Q}(\vartheta)$, D_L le discriminant de L, $\mathcal{O}$ son anneau des entiers, I l'indice de $\mathbb{Z}[\vartheta]$ dans $\mathcal{O}$. Alors
(a) Le rang r de E vérifie l'inégalité

$$r \ \leq\ n_L + 2n_p + n_q + r_2,$$

où

$$n_L = \begin{cases} 1 & si\ D_L\ <\ 0, \\ 2 & si\ D_L\ >\ 0, \end{cases}$$

n_p est le nombre de nombres premiers p qui divise I et qui se décompose complètement dans $L/\mathbb{Q}$.
n_q est le nombre de nombres premiers q qui divise I et qui se factorise en idéaux premiers de la façon suivante $\mathfrak{p}\mathfrak{p}'$ ou $\mathfrak{p}^2\mathfrak{p}'$, $\mathfrak{p} \neq \mathfrak{p}'$.

Pour notre famille de courbes elliptiques, on a les résultats suivants.

Lemme 8. *Soit $x \in K$ premier avec 2.*
1) Il existe une unité ϵ de K tel que $x\epsilon$ est un carré dans $\mathbb{Z}_K/4\mathbb{Z}_K$.
2) Soit $T = \{c_0 + c_1\rho_1 + c_2\rho_2 : c_i \in \{0, \pm 1, 2\}\}$ un système de représentants des éléments de $\mathbb{Z}_K/4\mathbb{Z}_K$.
• *Si $n \equiv 0\ mod\ 4$, si $\beta \in T$ alors $\rho_3\beta^2 \equiv c_0 + c_1\rho_1 + c_2\rho_2\ mod\ 4$, avec $c_2 \not\equiv 0\ mod\ 4$.*
• *Si $n \equiv 2\ mod\ 4$, si $\beta \in T$ alors $\rho_2\beta^2 \equiv c_0 + c_1\rho_1 + c_2\rho_2\ mod\ 4$, avec $c_2 \not\equiv 0\ mod\ 4$.*

Proposition 36. *Soient n un entier relatif pair tel que $(n^2+3)(n^2-3n+3)$ soit sans facteurs carrés, p un nombre premier qui divise $n-1$. Soit n_p le nombre de facteurs premiers de $n-1$, r_2 le 2-rang de $C_2(K)$. Alors le rang r de $E_n(\mathbb{Q})$ satisfait l'inégalité*

$$r \ \leq \ 1 + n_p + r_2.$$

Si de plus on pose $H = \cap_{p|n-1} H'_p \cap E_n(\mathbb{Q})$, alors

$$\mathrm{rg}_2(H/2E_n(\mathbb{Q})) \leq 1 + r_2.$$

Preuve : D'après le théorème de Mordell-Weil, on a $E_n(\mathbb{Q}) \backsimeq T \oplus \mathbb{Z}^r$ où T est le groupe de torsion de $E_n(\mathbb{Q})$. Comme les points de 2-torsion ne sont pas rationnels sur $\mathbb{Q}$ alors $T/2T = 0$; donc $r = \mathrm{rg}_2(E_n(\mathbb{Q})/2E_n(\mathbb{Q}))$. D'après la proposition **??**, $Im\lambda_{\mathbb{Q}} \ \backsimeq \ E_n(\mathbb{Q})/2E_n(\mathbb{Q})$, il en résulte alors que $|Im\lambda_{\mathbb{Q}}| = 2^r$. Comme $(x,y) \in E_n(\mathbb{Q})$ alors $x = \dfrac{m}{e^2}, y = \dfrac{l}{e^3}$ où $m, l, e \in \mathbb{Z}$ et $(m,e) = (l,e) = 1$. Il en résulte que $l^2 \ \equiv \ m^3 + m(-n+1)e^4 + e^6 \bmod 4$. On déduit alors que l est toujours impair.
Si e est pair alors m et l sont impairs et en remplaçant dans l'équivalence précédente, on déduit la congruence suivante $l^2 \ \equiv \ m^3 \bmod 4$, il en résulte alors que $m - \rho_1 e^2 \ \equiv \ m \ \equiv \ 1 \bmod 4$. Si e est impair alors $m - \rho_1 e^2 \ \equiv \ c_0 - \rho_1 \bmod 4$ où $c_0 \in \{0, \pm 1, 2\}$. D'après le corollaire **??**, on a $(m - \rho_1 e^2) = \mathfrak{a}\mathfrak{b}^2$, avec $\mathfrak{a} = \prod_{p|n-1}(\mathfrak{p}_2\mathfrak{p}_3)^{\gamma_p}$ et $\gamma_p \in \{0,1\}$, donc

$$(m - \rho_2 e^2) = \mathfrak{a}'\mathfrak{b}'^2, (m - \rho_3 e^2) = \mathfrak{a}''\mathfrak{b}''^2$$

tels que les idéaux $\mathfrak{a}', \mathfrak{a}''$ (resp. $\mathfrak{b}', \mathfrak{b}''$) sont les conjugués de $\mathfrak{a}$ (resp. $\mathfrak{b}$) et $\mathfrak{a}.\mathfrak{a}'.\mathfrak{a}'' = (p)^{2\gamma_p}$. Donc

$$(m - \rho_1 e^2)(m - \rho_2 e^2)(m - \rho_3 e^2) = (p)^{2\gamma_p}(\mathfrak{b}.\mathfrak{b}'.\mathfrak{b}'')^2,$$

soit alors $(m - \rho_1 e^2) = (m - \rho_2 e^2)^{-1}(m - \rho_3 e^2)^{-1}(p)^{2\gamma_p}(\mathfrak{b}.\mathfrak{b}'.\mathfrak{b}'')^2$, on déduit que

$$(m - \rho_2 e^2)^{-1}(m - \rho_3 e^2)^{-1} = \mathfrak{a}(p)^{-2\gamma_p}(\mathfrak{b}'.\mathfrak{b}'')^{-2},$$

ce qui montre que l'inverse de la classe de $\mathfrak{a}$ dans le groupe des classes d'idéaux est un carré. Ainsi pour chaque $\mathfrak{a}$ choisissons $\mu_\mathfrak{a}$ et $\mathfrak{b}_\mathfrak{a}$ tels que

$$(\mu_\mathfrak{a}) = \mathfrak{a}\mathfrak{b}_\mathfrak{a}^2.$$

Le nombre de possibilités de l'idéal $\mathfrak{a}$ et donc de $\mu_\mathfrak{a}$ est au plus égal à 2^{n_p}. Donc

$$(m - \rho_1 e^2) = (\mu_\mathfrak{a})(\mathfrak{b}\mathfrak{b}_\mathfrak{a}^{-1})^2,$$

ce qui entraîne que $\mathfrak{b}\mathfrak{b}_{\mathfrak{a}}^{-1} \in C_2(K)$. Soit $J_1, J_2, \cdots, J_{r_2}$ des idéaux dont les classes forment une base de $C_2(K)$ en tant que $\mathbb{F}_2$-espace vectoriel, tels que $J_i^2 = (\xi_i)$ où $\xi_i \in \mathbb{Z}_K$ alors

$$(\mathfrak{b}\mathfrak{b}_{\mathfrak{a}}^{-1})^2 = (\alpha^2 \xi_1^{\nu_1} \cdots \xi_{r_2}^{\nu_{r_2}}),$$

où $\alpha \in K^*$ et $\nu_i \in \{0, 1\}$. Donc

$$m - \rho_1 e^2 = u\alpha^2\gamma \qquad (1)$$

où $u \in \mathbb{Z}_K^*$ et $\gamma = \mu_{\mathfrak{a}} \xi_1^{\nu_1} \cdots \xi_{r_2}^{\nu_{r_2}}$. En reprenant le raisonnement fait dans la deuxième partie du lemme **??**, on montre que $\mu_{\mathfrak{a}} > 0$ pour tout $\mathfrak{a}$. En remplaçant ξ_i par $-\xi_i$ si c'est nécessaire, on peut choisir tous les ξ_i positifs donc $u > 0$. Comme le groupe des unités positives est de rang égal à 2. Il en résulte alors que le nombre de $m - \rho_1 e^2 \bmod K^{*2}$ est au plus égal à 2^f où $f = 2 + n_p + r_2$.
Comme $(m - \rho_1 e^2, 2) = 1$ alors $v_2(\gamma) \equiv 0 \bmod 2$, on déduit alors que $(\gamma, 2) = 1$. D'après le lemme **??**, il existe une unité ϵ_1 tel que $\epsilon_1\gamma \equiv \beta^2 \bmod 4$. Si $\epsilon_1 > 0$ (resp. $\epsilon_1 < 0$) alors $m - \rho_1 e^2 = u\epsilon_1^2(\frac{\alpha}{\epsilon_1})^2\gamma \equiv u\epsilon_1(\frac{\alpha}{\epsilon_1})^2\beta^2 \bmod 4$(resp. $m - \rho_1 e^2 \equiv -u\epsilon_2(\frac{\alpha}{\epsilon_2})^2\beta^2 \bmod 4$, où $\epsilon_2 = -\epsilon_1$), comme le groupe des unités positives est engendré par les unités ρ_2 et ρ_3, alors $u\epsilon_i = \rho_2^{s_i}\rho_3^{t_i}$ où $s_i, t_i \in \mathbb{Z}$, $2 \leq i \leq 3$. Donc $m - \rho_1 e^2 \equiv \rho_2^{s_1}\rho_3^{t_1}\beta_1^2 \bmod 4$ (resp. $m - \rho_1 e^2 \equiv -\rho_2^{s_2}\rho_3^{t_2}\beta_1^2 \bmod 4$).
Si $n \equiv 0 \bmod 4$ (resp. $n \equiv 2 \bmod 4$) alors

$$\rho_3\beta_1^2 \equiv c_0 + c_1\rho_1 + c_2\rho_2 \bmod 4$$

$$(\text{resp. } \rho_2\beta^2 \equiv c_0 + c_1\rho_1 + c_2\rho_2 \bmod 4.)$$

où $c_2 \not\equiv 0 \bmod 4$. On déduit alors qu'il existe des unités positives qui ne vérifient pas l'égalité (1), ce qui prouve que $r \leq 1 + n_p + r_2$, ce qui termine la démonstration de la première partie de la proposition.
Considérons la restriction λ_1 de l'application $\lambda_{\mathbb{Q}}$ au sous groupe H, $\lambda_1 : H \to K^*/K^{*2}$. Alors $Im\lambda_1 \backsimeq H/2E_n(\mathbb{Q})$. Comme $(x, y) \in H$ alors $(x - \rho_1) = \mathfrak{b}^2$. En reprenant le raisonnement fait précédemment, on déduit que le nombre de $(x - \rho_1)K^{*2}$ est au plus égal à 2^{1+r_2}. Ce qui termine la preuve de la proposition.

Exemples:
I. Soit la courbe elliptique E_{-120} d'équation

$$y^2 = x^3 - 14400x^2 - 1757163x + 1.$$

Les points $(0,1),(-120,-1331)$ sont des points de la courbe E_{-120}, d'après le programme mwrank de Cremona, le rang de la courbe est égal à 3.
La décomposition en idéaux premiers de l'idéal principal $(-120-\rho_1)$ est la suivante :

$$(-120-\rho_1)=\mathfrak{m}_2^4\mathfrak{m}_3^2,$$

avec $\mathfrak{m}_2=\mathfrak{m}_1^\sigma, \mathfrak{m}_3=\mathfrak{m}_1^{\sigma^2}$ et $\mathfrak{m}_1=11\mathbb{Z}_K+(\rho_1+1)\mathbb{Z}_K$. Donc les points $(0,1),(-120,-1331)$ sont dans H et ils sont indépendants modulo $2E_{-120}(\mathbb{Q})$. Donc $\mathrm{rg}_2(H/2E_{-120}(\mathbb{Q}))\geq 2$ et d'après la proposition **??**, on obtient $2\leq \mathrm{rg}_2(H/2E_{-120}(\mathbb{Q}))\leq 3$.

II. Considérons la courbe elliptique E_{-14} donnée par l'équation :

$$y^2=x^3-196x^2-3181x+1.$$

D'après le programme mwrank de Cremona [**?**], les points $Q_1=(459,7345)$, $Q_2=(0,1), Q_3=(3661,215475)$, forment une base d'un sous-groupe d'indice fini du groupe de Mordell-Weil. Les décompositions des idéaux principaux $(459-\rho_1),(3661-\rho_1)$ sont les suivantes :

$$(459-\rho_1)=\mathfrak{r}_1^2\mathfrak{r}_2^2\mathfrak{r}_3^2,$$

tels que $\mathfrak{r}_1=5\mathbb{Z}_K+(1+\rho_1)\mathbb{Z}_K, \mathfrak{r}_2=13\mathbb{Z}_K+(-4+\rho_1)\mathbb{Z}_K, \mathfrak{r}_3=113\mathbb{Z}_K+(-7+\rho_1)\mathbb{Z}_K$,

$$(3661-\rho_1)=\mathfrak{r}_1^\sigma(\mathfrak{r}_1^{\sigma^2})^3\mathfrak{r}_4^\sigma\mathfrak{r}_4^{\sigma^2}\mathfrak{r}_5^2\mathfrak{r}_6^2,$$

avec $\mathfrak{r}_4=3\mathbb{Z}_K+(1+\rho_1)\mathbb{Z}_K$, $\mathfrak{r}_5=13\mathbb{Z}_K+(\rho_1+5)\mathbb{Z}_K$, $\mathfrak{r}_6=17\mathbb{Z}_K+(\rho_1-6)\mathbb{Z}_K$. Les points Q_1,Q_2 sont dans H et on montre que leurs classes forment une base de $H/2E_{-14}(\mathbb{Q})$, donc $rg_2(H/2E_{-14}(\mathbb{Q}))=2$. Comme r_2 est pair, on déduit d'après la proposition **??** que $r_2\geq 2$. D'après le programme pari [**?**], on trouve que $r_2=2$.

5.4 Résultat de Washington.

Soit a un entier positif tel que $\delta=a^2+3a+9$ soit sans facteur carré. Le corps cubique L_a, défini par le polynôme irréductible sur $\mathbb{Q}$,

$$S_{a+3}(x)=x^3-(a+3)x^2+ax+1$$

a été introduit par Shanks [**?**] et appelé "Corps cubiques simples". Ces corps ont été beaucoup étudiés car leur régulateur est explicite et petit. Ainsi leur nombre de classes a tendance à être particulièrement grand.

L.C.Washington [**?**] a introduit la famille de courbes elliptiques C_a définies sur $\mathbb{Q}$ par les équations

$$C_a : y^2 = S_{a+3}(x),$$

et il montre qu'il existe une relation entre le 2-rang du groupe des classes des corps cubiques simples et le rang de cette famille de courbes elliptiques. Il démontre le résultat suivant :

Théorème 16. *Le rang* $\mathrm{rg}(C_a(\mathbb{Q}))$ *de la courbe elliptique* $C_a(\mathbb{Q})$ *est au plus égal à* $1 + r_2$. *En fait la suite suivante est exacte :*

$$1 \longrightarrow C_a^0(\mathbb{Q})/2C_a(\mathbb{Q}) \longrightarrow C_2 \longrightarrow Ш_2 \longrightarrow 1,$$

où $C_a^0(\mathbb{Q}) = 2C_a(\mathbb{R}) \cap C_a(\mathbb{Q})$, $Ш_2$ *est la* 2*-torsion du groupe de Tate-Shafarevich et* C_2 *le* 2*-groupe des classes des corps définis par les polynômes* $S_{a+3}(x)$.

Dans ce paragraphe, sous certaines hypothèses, la proposition suivante donne un équivalent du théorème **??**. Dans la preuve de cette proposition, on a repris la même idée que Washington [**?**] pour les cas 1, 2 et 3. Mais le cas 4 ne s'est pas présenté pour sa famille de courbes elliptiques et corps cubiques.

Proposition 37. *Si* $n - 1 = m^2$ *(resp.* $-m^2$*), soit* p *un nombre premier qui divise* $n - 1$, *tel que* $p \equiv \pm 3 \bmod 8$ *ou* $p \equiv -1 \bmod 8$. *Alors La suite*

$$1 \longrightarrow \langle [(0,1)] \rangle \longrightarrow S_2'(\mathbb{Q}) \xrightarrow{\nu} C_2(K) \longrightarrow 1, \qquad (5.4.1)$$

$$\nu : [\alpha] \mapsto \overline{I_\alpha},$$

$$\mu : [(x,y)] \mapsto \overline{I_x},\ (x - \rho) = I_x^2,$$

est une suite exacte.

D'après le lemme **??**, pour chaque $[\alpha] \in S_2'(\mathbb{Q})$ il existe un idéal I_α tel que $I_\alpha^2 = (\alpha)$, donc $\overline{I_\alpha} \in C_2(K)$.
Il est évident que ν est un homomorphisme. Pour montrer que ν est un homomorphisme surjectif. On va tout d'abord, montrer le résultat suivant :

Lemme 9. *Soient* $\overline{I_\alpha}$ *un idéal de* $C_2(K)$, $\alpha \in K^*$ *tel que* $(\alpha) = I_\alpha^2$. *L'extension* $K(\sqrt{\alpha})/K$ *est non ramifiée en toutes les places de* K.

Pour la démonstration de ce lemme, on a besoin du lemme suivant dont la preuve se trouve dans [**?**].

Lemme 10. *Soit* k *un corps de nombres dans lequel 2 est inerte et* $\alpha \in k$ *relativement premier avec 2. Alors* $k(\sqrt{\alpha})/k$ *est non ramifiée en 2 si et seulement si* α *est un carré modulo 4.*
Cette extension est non ramifiée en les nombres premiers finis de k *si et seulement si l'idéal (fractionnaire)* (α) *est le carré d'un idéal de* k.
Si k *est totalement réel, alors l'extension est non ramifiée en les places à l'infini si et seulement si* α *est totalement positif.*

D'après la proposition **??**, si n est pair le nombre premier 2 est inerte dans l'extension $K/\mathbb{Q}$. Dans tout le reste du chapitre, on va supposer que n est pair.

Preuve du lemme ??

D'après le lemme **??**, L'extension $K(\sqrt{\alpha})/K$ est non ramifiée en les places finies et infinies de K, sauf peut-être en 2 .

D'après le lemme **??**, il existe une unité ϵ telle que l'extension $K(\sqrt{\epsilon\alpha})/K$ soit non ramifiée en 2.

Comme l'idéal $(\epsilon\alpha) = (\alpha) = I_\alpha^2$ alors $K(\sqrt{\epsilon\alpha})/K$ est non ramifiée en les places finies.

D'après le corollaire **??**, l'extension quadratique $K(\sqrt{\epsilon\alpha})/K$ non ramifiée en les places finies est non ramifiée en les places infinies, d'où $\epsilon\alpha$ est totalement positif, comme α est totalement positif, alors ϵ est totalement positif, d'après le lemme **??** ϵ est un carré.

On déduit alors que $K(\sqrt{\alpha})/K$ est non ramifiée en les places finies et infinies. Ce qui termine la preuve du lemme.

Preuve de la proposition ??

Montrons que ν est surjective. Soit $\overline{I_\alpha} \in C_2(K)$, il existe $\alpha \in K^*$ tel que $(\alpha) = I_\alpha^2$.

Nous allons montrer que $[\alpha]_p \in Im\lambda_p$ si $p \nmid n-1$, ou $[\alpha]_p \in Im\lambda'_p$ si $p|n-1$.

1) Si p est inerte dans K. Comme $K(\sqrt{\alpha})/K$ est une extension quadratique, donc c'est une extension abélienne finie de K, on a montré qu'elle est non ramifiée alors $K(\sqrt{\alpha})/K$ est le corps de classe d'un sous groupe A de $C(K)$. Par la théorie du corps de classe l'idéal principal $p\mathbb{Z}_{K(\sqrt{\alpha})}$ se décompose complètement dans $K(\sqrt{\alpha})$, $p\mathbb{Z}_{K(\sqrt{\alpha})} = \mathfrak{q}_1\mathfrak{q}_2$ où $\mathfrak{q}_i$ sont les idéaux premiers au dessus de p.

Notons par $K(\sqrt{\alpha})_{\mathfrak{q}_i}$ le complété de $K(\sqrt{\alpha})$ en l'idéal premier $\mathfrak{q}_i$, alors $K(\sqrt{\alpha})_{\mathfrak{q}_i}$ est une extension de $K_{\mathfrak{q}_i}$ de degré $[K(\sqrt{\alpha})_{\mathfrak{q}_i} : K_{\mathfrak{q}_i}] = e_{\mathfrak{q}_i} f_{\mathfrak{q}_i}$, comme $e_{\mathfrak{q}_i} = f_{\mathfrak{q}_i} = 1$ pour tout $1 \leq i \leq 2$ alors $K(\sqrt{\alpha})_{\mathfrak{q}_i} = K_{\mathfrak{q}_i}$ donc $\sqrt{\alpha} \in K^*_{\mathfrak{q}_i}$, soit $\alpha \in K^{*2}_{\mathfrak{q}_i}$ donc $[\alpha]_p \in Im\lambda_p$.

2) Si $p\mathbb{Z}_K$ se ramifie dans l'extension $K/\mathbb{Q}$, alors $p\mathbb{Z}_K = \mathfrak{q}^3$ où $\mathfrak{q}$ est un idéal premier au dessus de p. Donc l'ordre de la classe de $\mathfrak{q}$ est égal à 1 ou 3. Soit K_H le corps de classe de Hilbert de K, considérons la suite de corps

$$K \to K(\sqrt{\beta}) \to K_H.$$

Soit $\mathfrak{q}$ un idéal premier de K, d'après le théorème **??**, l'ordre de la classe de $\mathfrak{q}$ noté $ord(\overline{\mathfrak{q}})$ est égal à son degré résiduel f dans K_H.

Si $\mathfrak{q}$ reste premier dans $K(\sqrt{\alpha})$ alors 2 divise f. Donc $\mathfrak{q}$ ne peut être d'ordre 3 dans $C(K)$, alors $\mathfrak{q}$ est un idéal principal qui se décompose complètement dans l'extension non ramifiée $K(\sqrt{\alpha})/K$, et en reprenant les mêmes arguments que dans le cas 1), on déduit alors que $[\alpha]_p \in Im\lambda_p$.

Si $\mathfrak{q}$ n'est pas premier dans $K(\sqrt{\alpha})$ alors $\mathfrak{q} = \mathfrak{q}_1^2$ ou $\mathfrak{q} = \mathfrak{q}'_1\mathfrak{q}'_2$ mais comme $K(\sqrt{\alpha})/K$ est non ramifiée en tout idéal premier, donc le premier cas est à exclure. Alors l'idéal $\mathfrak{q}$ se décompose complètement dans l'extension $K(\sqrt{\alpha})/K$, en reprenant le même raisonnement fait dans le cas 1), on déduit que $[\alpha]_p \in Im\lambda_p$.
3) Si $p\mathbb{Z}_K$ se décompose et p ne divise pas $n-1$. Soit I_α un idéal tel que $(\alpha) = I_\alpha^2$. Comme $(\alpha\alpha'\alpha'') = (N_{K/\mathbb{Q}}(I_\alpha))^2$, il existe une unité ϵ tel que $\alpha\alpha'\alpha'' = \epsilon n^2$, comme α est totalement positif, alors ϵ est une unité totalement positive, d'après le lemme **??**, ϵ est un carré donc $\alpha\alpha'\alpha''$ est un carré ; comme $\alpha\alpha'\alpha'' = p^{2m}u_1u_2u_3$ donc $u_1u_2u_3$ est un carré de $\mathbb{Z}_p^*$. D'après la proposition **??**, $[\alpha]_p \in Im\lambda_p$.
4) Supposons que $p\mathbb{Z}_K$ se décompose dans $K/\mathbb{Q}$ et p divise $n-1$. Alors on distingue deux cas :
a) Si $p \equiv \pm 3 \bmod 8$, alors on reprend le raisonnement fait précédemment et d'après la proposition **??**, on déduit que $[\alpha]_p \in Im\lambda'_p$.
b) Si $p \equiv -1 \bmod 8$, $I_\alpha^2 = (\alpha)$ avec $\alpha = p^{2m}u$ où $u \in \mathbb{Z}_p^*$. Si $u \notin \mathbb{Z}_p^{*2}$, comme $\rho_1 \equiv -1 \bmod p$ alors $\rho_1 u \equiv -u \bmod p$, donc $-u$ est un carré mod p. Il en résulte que $\rho_1\rho_2\alpha$ est un carré mod p. La norme de $\rho_1\rho_2\alpha$ est un carré alors d'après la proposition **??**, $[\rho_1\rho_2\alpha]_p \in \mathrm{Im}\lambda'_{\mathrm{p}}$ et de plus $(\rho_1\rho_2\alpha) = (\alpha) = I_\alpha^2$.
D'après le lemme **??**, $ker\ \nu = \{1, -\rho_1\}K^{*2}/K^{*2} \backsimeq \langle\ [(0,1)]\rangle$. Ce qui termine la démonstration de la proposition.

5.5 Sous-groupe du 2-groupe de Selmer et 2-rang du groupe de classes

On a défini l'homomorphisme λ de la manière suivante :

$$\lambda : E_n(\mathbb{Q}) \to K^*/K^{*2}, \quad \lambda : (x,y) \mapsto [x - \rho_1].$$

Montrons que $Im\lambda \subset S_2(\mathbb{Q})$, en effet si $[\alpha] \in Im\lambda$ alors il existe $(x,y) \in E_n(\mathbb{Q})$ tel que $[\alpha] = [x - \rho_1]$, alors $[\alpha]_p = [x - \rho_1]_p \in Im\lambda_p$ pour tout p, ce qui termine la démonstration.
Donc l'homomorphisme λ induit un homomorphisme injectif $f : E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \to S_2(\mathbb{Q})$. On obtient alors la suite exacte suivante :

$$1 \longrightarrow E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \longrightarrow S_2(\mathbb{Q}) \longrightarrow Ш_2 \longrightarrow 1,$$

où $Ш_2$ est le conoyau de l'application f et que l'on appelle la 2-torsion du sous-groupe du groupe de Tate-Shafarevich. Cette suite est appelé la suite exacte fondamentale.

On a défini dans le chapitre 4, le sous-groupe

$$H_p = \{[\alpha]_p \in (\mathbb{Q}_p^*/\mathbb{Q}_p^{*2})^3 : \alpha \in K^*, v_p(\alpha) \equiv v_p(\alpha') \equiv v_p(\alpha'') \equiv 0 \bmod 2\}.$$

et on a posé $H'_p = \lambda_p^{-1}(H_p)$, où $\lambda_p : E_n(\mathbb{Q}_p) \to (\mathbb{Q}_p^*/\mathbb{Q}_p^{*2})^3$.
Considérons la restriction λ_1 de l'application λ au sous-groupe $H = \cap_{p|n-1} H'_p(\mathbb{Q}_p) \cap E_n(\mathbb{Q})$,

$$\lambda_1 : H \to K^*/K^{*2}.$$

On montre facilement que $ker\lambda_1 = H \cap 2E_n(\mathbb{Q})$ et comme $2E_n(\mathbb{Q}) \subset H$ alors $ker\lambda_1 = 2E_n(\mathbb{Q})$.
Montrons que $Im\lambda_1 \subseteq S'_2(\mathbb{Q})$. Soit $[\alpha] \in Im\lambda_1$ alors il existe $(x, y) \in H$, $\beta_1 \in K^*$ tel que $\alpha = (x - \rho_1)\beta_1^2$. Comme $[\alpha]_p = [x - \rho_1]_p$, alors $[\alpha] \in U$ donc $[\alpha] \in S'_2(\mathbb{Q})$.
Donc λ_1 induit un homomorphisme injectif

$$f_1 : H/2E_n(\mathbb{Q}) \to S'_2(\mathbb{Q}).$$

Et on obtient alors la suite exacte suivante :

$$1 \longrightarrow H/2E_n(\mathbb{Q}) \longrightarrow S'_2(\mathbb{Q}) \longrightarrow Ш'_2 \longrightarrow 1,$$

où $Ш'_2$ est le conoyau de f_1.
On a défini l'homomorphisme λ_k de la manière suivante :

$$\lambda_k : E(k) \to A_k^*/A_k^{*2}$$
$$(x, y) \mapsto [x - \rho_1]$$

Si $k = \mathbb{R}$, l'algèbre A_k^* est isomorphe à $\mathbb{R} \oplus \mathbb{C}$ (resp. $\mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$) si le discriminant Δ de la courbe elliptique E est négatif (resp. positif).
Le 2-rang de l'image de $\lambda_{\mathbb{R}}$ est donnée par la proposition suivante :

Proposition 38. *[?].*
Soient l'homomorphisme $\lambda_{\mathbb{R}} : E(\mathbb{R}) \to (\mathbb{R}^*/\mathbb{R}^{*2})^3$ et Δ le discriminant de la courbe elliptique E, si $\Delta > 0$ alors le 2-rang de $Im\lambda_{\mathbb{R}}$ est égal à 1.

Soit l'injection naturelle $i_\infty : E(\mathbb{Q}) \to E(\mathbb{R}), \quad P \mapsto P$.

Corollaire 39. *Le groupe quotient $E(\mathbb{R})/2E(\mathbb{R})$ est engendré par l'image du point $(0, 1)$ par l'application i_∞.*

Preuve
La preuve découle de la proposition **??** et du fait que $i_\infty(0, 1) \notin 2E(\mathbb{R})$.
Considérons l'application composée suivante :

$$\begin{array}{ccccc} E_n(\mathbb{Q}) & \xrightarrow{i_\infty} & E_n(\mathbb{R}) & \xrightarrow{s} & E_n(\mathbb{R})/2E_n(\mathbb{R}) \\ P & \longrightarrow & i_\infty(P) & \longrightarrow & s(i_\infty(P)) = [i_\infty(P)] \end{array}$$

Nous définissons le sous ensemble de $E_n(\mathbb{Q})$

$$E'_n(\mathbb{Q}) = \ker s \circ i_\infty = \{P \in E_n(\mathbb{Q})/i_\infty(P) \in 2E_n(\mathbb{R})\} = 2E_n(\mathbb{R}) \cap E_n(\mathbb{Q}).$$

En d'autres termes, $E'_n(\mathbb{Q})$ est le sous groupe de $E_n(\mathbb{Q})$ dont les points sont dans la composante connexe du point à l'infini de la courbe réelle $E_n(\mathbb{R})$. Notons par $E'_n(\mathbb{Q})$ la composante connexe du point à l'infini de la courbe réelle $E_n(\mathbb{R})$.

Lemme 11. *Soient n un entier relatif, p un nombre premier tel que p divise $n-1$, et $H = \cap_{p|n-1} H'_p \cap E_n(\mathbb{Q})$ alors*

$$H/2E_n(\mathbb{Q}) = \ \langle (0,1) \ \rangle \oplus (E'_n(\mathbb{Q}) \cap H)/2E_n(\mathbb{Q}).$$

Preuve.
Soient $[S] \in H/2E_n(\mathbb{Q})$ et $P = (0,1)$ alors si $S \notin E'_n(\mathbb{Q}) \cap H$, donc S appartient à la partie compacte de $E_n(\mathbb{R})$, la droite SP coupe $E'_n(\mathbb{R}) \cap H$ en P_1 et $S + P + P_1 = 0$, soit $S = -P - P_1$, $-P_1 \in E'_n(\mathbb{Q}) \cap H$.

Proposition 40. *Soient n un entier relatif pair tel que $(n^2+3)(n^2-3n+3)$ soit sans facteurs carrés, $H = \cap_{p|n-1} H_p \cap E_n(\mathbb{Q})$. Soit r_2 le 2-rang du groupe des classes de K et $\mathrm{rg}_2(H/2E_n(\mathbb{Q}))$ la dimension de $H/2E_n(\mathbb{Q})$ en tant que $\mathbb{F}_2$-espace vectoriel. Sous les hypothèses de la proposition* **??**, *la suite*

$$1 \longrightarrow (E'_n(\mathbb{Q}) \cap H)/2E_n(\mathbb{Q}) \xrightarrow{\mu} C_2(K) \longrightarrow Ш'_2 \longrightarrow 1,$$

$$\mu : [(x,y)] \mapsto \overline{I_x}, \ (x - \rho_1) = I_x^2,$$

est exacte. De plus,

$$\mathrm{rg}_2(H/2E_n(\mathbb{Q})) \leq 1 + r_2.$$

Preuve
Considérons le diagramme commutatif suivant, dont les deux lignes sont exactes.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \langle\ [(0,1)]\rangle & \xrightarrow{\nu_1} & S'_2(\mathbb{Q}) & \xrightarrow{\nu} & C_2(K) & \longrightarrow & 1 \\ \downarrow & & \sigma\downarrow & & \downarrow & & \downarrow\tau & & \\ 1 & \longrightarrow & H/2E_n(\mathbb{Q}) & \longrightarrow & S'_2(\mathbb{Q}) & \longrightarrow & Ш'_2 & \longrightarrow & 1, \end{array}$$

où σ est l'injection canonique, τ est la surjection naturelle.

D'après le lemme du serpent $\ker \tau \backsimeq (E'_n(\mathbb{Q}) \cap H)/2E_n(\mathbb{Q})$. On obtient la suite exacte :

$$1 \to (E'_n(\mathbb{Q}) \cap H)/2E_n(\mathbb{Q}) \to C_2(K) \to Ш'_2 \to 1.$$

D'après le lemme **??**,

$$\mathrm{rg}_2(H/2E_n(\mathbb{Q})) = 1 + \mathrm{rg}_2((E'_n(\mathbb{Q}) \cap H)/2E_n(\mathbb{Q})).$$

Comme la suite

$$1 \to (E'_n(\mathbb{Q}) \cap H)/2E_n(\mathbb{Q})) \to C_2(K) \to Ш'_2 \to 1,$$

est une suite exacte, il s'ensuit alors que :

$$\mathrm{rg}_2(H/2E_n(\mathbb{Q})) \leq 1 + r_2,$$

ce qui termine la démonstration de la proposition.

5.6 Exemples.

5.6.1 Construction d'exemples.

Les résultats du paragraphe précédent montrent que si on cherche des corps cubiques K de 2-rang élevé, on peut essayer de construire des courbes elliptiques ($y^2 = G_n(x)$) de rang grand. Pour cela, il est habituel de partir d'une courbe sur $\mathbb{Q}(T)$ de rang non nul et de spécialiser. Nous avons cherché pour la famille de Washington à élever le rang et obtenons une relation entre les deux familles expliquée ci-dessous.
Soit $S_{a+3}(x) = x^3 - (a+3)x^2 + ax + 1$, avec $a \in \mathbb{Q}$, on considère la courbe elliptique $y^2 = S_{a+3}(x)$. Les points rationnels d'ordonnée 1 sont rationnels si $S_{a+3}(x) - 1 = x(x^2 - (a+3)x + a)$ a trois racines rationnels c'est à dire si $(a+3)^2 - 4a$ est un carré dans $\mathbb{Q}$. En paramétrant la conique $(a+3)^2 - 4a = b^2$, on trouve que $a = (k+1)(k-2)/k$. En remplaçant la valeur de a obtenu dans le polynôme $S_{a+3}(x)$, et en posant le changement de variable $x = (u-1)/k$, on obtient $S_{a+3}(x) = Q_1(x)$ avec

$$k^3 Q_1(u) = G_{k+1}(u) = u^3 - (k+1)^2 u^2 + (k^3 + k^2 + 2k - 1)u + 1.$$

Comme $a = k - 2/k - 1$ reste invariant par la transformation $k \mapsto -2/k$; et en effectuant le changement de variable $x = -k(t-1)/2$. On obtient alors $S_{a+3}(x) = R_1(t)$ avec

$$\frac{-2^3}{k^3} R_1(t) = R(t) = t^3 - (\frac{k-2}{k})^2 t^2 - (\frac{k^3 + 4k^2 - 4k + 8}{k^3})t + 1.$$

Ce polynôme $R(t)$ est obtenu en remplaçant k par $-2/k$ dans le polynôme $G_{k+1}(t)$. Les courbes elliptiques

$$y^2 = G_{k+1}(u) \text{ et } z^2 = R(t)$$

sont tordues par $\sqrt{-2}$. Les abscisses de leurs points de 2-torsion sont liés par la relation $r_{G_{k+1}} - 1 = -2k^2(x_R - 1)$.
La courbe $y^2 = S_{a+3}(x)$ admet trois points rationnels

$$x = 0, y = 1 \text{ et } x = k + 1, y = 1 \text{ et } x = -2/k + 1, y = 1$$

dont la somme est nulle.

Proposition 41. *Soit k un entier tel que $k = n - 1 = m^2$ (resp. $-m^2$). Le rang des courbes elliptiques $E_n(\mathbb{Q})$, sauf pour un nombre fini de courbes, est supérieur ou égal à 3 (resp. 2). Les points $(0, 1), (1, m^3), (-1 + m^2, m^3)$ (resp. $(0, 1), (1 - m^2, m^3)$) sont des points rationnels de $E_n(\mathbb{Q})$ indépendants.*

Preuve : Donc si $k = m^2$ (resp. $k = -m^2$) les points

$$u = 1, y = m^3 \text{ et } u = -1 + m^2, y = m^3 \text{ et } u = 1 + m^2 + m^4, y = m^3$$

(resp. $(1 - m^2, m^3)$) sont sur la courbe $y^2 = G_{k+1}(u)$.
En spécialisant pour $m = 3$ les points $(0, 1)$, $(1, m^3)$, $(-1 + m^2, m^3)$ (resp. $(0, 1), (1 - m^2, m^3)$) sont indépendants. Donc si k est un carré (resp. $k = -m^2$) et sauf peut-être pour un nombre fini de courbes le rang est supérieur ou égal à 3 (resp. à 2).

A. Dujella [**?**] a utilisé la méthode suivante pour construire l'exemple de la courbe E_{626} de rang égal à 7, en spécialisant à partir des familles E_{m^2+1} et E_{-m^2+1}. Pour l un entier fixé, E une courbe elliptique et $a_p = p + 1 - |E(\mathbb{F}_p)|$, on définit

$$\begin{aligned} S_1(l) &= S_1(l, E) = \sum_{p \le l,\ p \text{ premier}} \frac{-a_p + 2}{p + 1 - a_p} \log(p), \\ S_2(l) &= S_2(l, E) = \sum_{p \le l,\ p \text{ premier}} \frac{-a_p + 2}{p + 1 - a_p}, \\ S_3(l) &= S_3(l, E) = \sum_{p \le l,\ p \text{ premier}} -a_p \log(p). \end{aligned}$$

Il est alors expérimentalement connu [**?**] et [**?**], qu'on peut espérer obtenir des courbes de grand rang si $S_{i=1,2,3}(N)$ est grand. Dans [**?**], des arguments étayent

le fait que c'est la conjecture de Birch et Swinnerton-Dyer qui fonde cette idée. Le rang est alors minoré par construction effective de points indépendants, utilisant les programmes mwrank de Cremona [**?**] et ratpoints de Stoll. La même méthode a été utilisée par O.Lecacheux [**?**] et A.Dujella [**?**] pour construire des courbes elliptiques de rang élevé.

5.6.2 Exemples.

La proposition suivante, donne une caractérisation des points qui sont dans $2E_n(\mathbb{Q})$. La preuve est faite dans l'article de Washington [10].

Proposition 42. *Soient E la courbe elliptique d'équation $y^2 = f(x)$, où $f(x)$ est un polynôme cubique, qui possède des racines distinctes. Soient $(d, e) \in E(\mathbb{Q})$ et*

$$f(x + d) = ax^3 + bx^2 + cx + e^2$$

avec $a, b, c \in \mathbb{Q}$. Alors $(d, e) \in 2E(\mathbb{Q})$ si et seulement si

$$q(x) = x^4 - 2bx^2 - 8aex + b^2 - 4ac$$

a des racines rationnelles.

• Dans tous les exemples traités par la suite, en utilisant le programme mwrank et après simplification, on obtient une base d'un sous-groupe d'indice fini du groupe de Mordell-Weil. Le programme pari nous donne les décompositions des idéaux principaux en facteurs d'idéaux premiers, et le 2-rang r_2 du groupe des classes de K. Ce programme utilise l'algorithme sous-exponentielle du nombre de classes et du régulateur, introduit par Hafner et McCurley [**?**] pour calculer le nombre de classes des corps quadratiques imaginaires. Ces idées ont été généralisées par Buchmann [**?**]. Par la suite Cohen, Diaz Y Diaz et Olivier [**?**] ont amélioré cet algorithme. Pour pouvoir décrire cet algorithme, il est essentiel de connaitre un système de générateurs du groupe de classes d'idéaux d'un corps de nombres K de degré n. Un tel système de générateurs est donné par le théorème de Minkowski mais la croissance de la constante de Minkowski est exponentielle en n. Si l'on accepte la validité de la Conjecture de Riemann Généralisée (GRH), on peut obtenir de meilleurs bornes pour les générateurs du groupe de classes de K :

Théorème 17. *Bach[**?**]*
Dans tout corps de nombres K, le groupe des classes d'idéaux est engendré par les idéaux de norme plus petite ou égale à B, avec $B = c(\log |D(K)|)^2$. On peut choisir $c = 6$ pour les corps quadratiques et $c = 12$ pour les corps de degré $n > 2$.

Puis déterminer les relations entre ces idéaux.

I. Considérons la courbe elliptique E_{-8} donnée par l'équation :

$$y^2 = x^3 - 64x^2 - 667x + 1.$$

On est dans le cas $n-1 = -3^2$, donc d'après la proposition **??**, les points $P_1 = (-8, 27), P_2 = (0, 1)$ sont indépendants. D'autre part, le programme mwrank de Cremona, nous dit que le rang de la courbe est égal à 3 et que les points P_1, P_2 et $P_3 = (22473/256, -1446661/4096)$ forment une base d'un sous-groupe d'indice fini du groupe de Mordell-Weil. En utilisant le programme Pari, les décompositions des idéaux principaux $(-8 - \rho_1)$ et $(22473/256 - \rho_1)$ sont les suivantes :

$$(-8 - \rho_1) = (\mathfrak{q}_1^{\sigma})^2 (\mathfrak{q}_1^{\sigma^2})^4,$$

tels que $\mathfrak{q}_1 = 3\mathbb{Z}_K + (\rho_1 + 1)\mathbb{Z}_K$.

$$(22473/256 - \rho_1) = \mathfrak{q'}_1^2 \mathfrak{q'}_2^2 \mathfrak{q'}_3^2,$$

avec $\mathfrak{q'}_1 = 2\mathbb{Z}_K, \mathfrak{q'}_2 = 761\mathbb{Z}_K + (153 + \rho_1)\mathbb{Z}_K, \mathfrak{q'}_3 = 1901\mathbb{Z}_K + (484 + \rho_1)\mathbb{Z}_K$. Donc les points P_1, P_3 sont dans $H \cap E'_{-8}(\mathbb{Q}_3)$ et d'après la proposition **??**, ils ne sont pas dans $2E_{-8}(\mathbb{Q})$ et on montre que leurs classes forment une base de $H/2E_{-8}$. On déduit alors que $\mathrm{rg}_2(H/2E_{-8}(\mathbb{Q})) = 3$. Comme r_2 est pair, d'après la proposition **??**, il en résulte que $r_2 \geq 2$. D'après le programme pari, on obtient $r_2 = 2$.

II. Considérons la courbe elliptique E_{10} donnée par l'équation :

$$y^2 = x^3 - 100x^2 + 827x + 1.$$

D'après la proposition **??**, les points $G = (0, 1), G_1 = (1, 27), G_2 = (8, 27)$ sont indépendants, et le programme mwrank de Cremona, nous dit que le rang de la courbe est égal à 3. Alors les points G, G_1, G_2 forment une base d'un sous-groupe d'indice fini du groupe de Mordell-Weil. En utilisant le programme pari, les décompositions des idéaux principaux $(1 - \rho_1), (8 - \rho_1)$ sont les suivantes :

$$(1 - \rho_1) = \mathfrak{b}_1^2 (\mathfrak{b}_1^{\sigma^2})^4,$$

où $\mathfrak{b}_1 = 3\mathbb{Z}_K + (\rho_1 + 1)\mathbb{Z}_K$,

$$(8 - \rho_1) = \mathfrak{b}_1^6.$$

Donc les points G, G_1, G_2 sont dans H, de plus ils sont indépendants modulo $2E_{10}(\mathbb{Q})$. Comme précédemment, on déduit que $\mathrm{rg}_2(H/2E_{10}(\mathbb{Q})) = 3$ et on trouve que $r_2 \geq 2$ et r_2 calculé par pari est égal à 2.

III. Considérons la courbe elliptique E_{50} donnée par l'équation :

$$y^2 = x^3 - 2500x^2 + 120147x + 1.$$

D'après le programme de Cremona, les points

$$D = (2451, 343),\ D_1 = (5265, 277991),\ D_2 = (2855/125, 150619/125),$$

$$D_3 = (120835, 41567239)$$

forment une base d'un sous-groupe d'indice fini du groupe de Mordell-Weil. D'après la proposition **??**, les points $D' = (0, 1), D'_1 = (1, 343), D'_2 = (48, 343)$ sont indépendants et en calculant le déterminant de la matrice des hauteurs des points D', D'_1, D'_2, D_1, on trouve qu'il est égal au déterminant de la matrice des hauteurs des points D, D_1, D_2, D_3. Donc les points D', D'_1, D'_2, D_1 forment une base d'un sous-groupe d'indice fini du groupe de Mordell-Weil. Les idéaux $(1 - \rho_1),\ (5265 - \rho_1),\ (48 - \rho_1)$ ont pour décompositions :

$$(1 - \rho_1) = (\mathfrak{h}_1^{\sigma})^2(\mathfrak{h}_1^{\sigma^2})^4,$$

avec $\mathfrak{h}_1 = 7\mathbb{Z}_K + (\rho_1 + 1)\mathbb{Z}_K$.

$$(5265 - \rho_1) = \mathfrak{h}_1^{\sigma}\mathfrak{h}_1^{\sigma^2}\mathfrak{h}'^2_2\mathfrak{h}'^2_3,$$

avec $\mathfrak{h}'_2 = 151\mathbb{Z}_K + (20 + \rho_1)\mathbb{Z}_K,\ \mathfrak{h}'_3 = 263\mathbb{Z}_K + (-5 + \rho_1)\mathbb{Z}_K,$

$$(48 - \rho_1) = \mathfrak{h}_1^6.$$

Les points D', D'_1, D'_2 sont des points de H qui sont indépendants modulo $2E_{50}(\mathbb{Q})$. D'autre part, la courbe E_{50} a une réduction non déployée en 7, alors d'après la proposition **??**, on obtient $\mathrm{rg}_2(H/2E_{50}(\mathbb{Q})) = 3$.

IV. Considérons la courbe elliptique E_{626} donnée par l'équation :

$$y^2 = x^3 - 391876x^2 + 244532499x + 1.$$

Les points

$$(0, 1), (1, 15625), (391251, 15625), (349, 194045), (133, 159979),$$

$$(63153799/49, 418730031875/343), (177607161/64, 2193522042995/512)$$

sont des points indépendants de E_{626}. Ils forment une base d'un sous-groupe d'indice fini de $E_{626}(\mathbb{Q})$.
Les décompositions en idéaux premiers des idéaux principaux $(1 -$

$\rho_1), (391251 - \rho_1), (349 - \rho_1), (133 - \rho_1), (236656201/576 - \rho_1)$ sont les suivantes :

$$(1 - \rho_1) = (\mathfrak{g}_1^{\sigma})^8 (\mathfrak{g}_1^{\sigma^2})^4,$$

$$(391251 - \rho_1) = (\mathfrak{g}_1^{\sigma})^4 (\mathfrak{g}_1^{\sigma^2})^8,$$

$$(349 - \rho_1) = \mathfrak{g}_1^2 \mathfrak{g}_4^4,$$

où $\mathfrak{g}_1 = 5\mathbb{Z}_K + (\rho_1 + 1)\mathbb{Z}_K$, $\mathfrak{g}_4 = 197\mathbb{Z}_K + (\rho_1 + 45)\mathbb{Z}_K$,

$$(133 - \rho_1) = \mathfrak{g}_5^2,$$

où $\mathfrak{g}_5 = 159979\mathbb{Z}_K + (\rho_1 + 159846)\mathbb{Z}_K$,

$$(177607161/64 - \rho_1) = \mathfrak{g}_1^2 \mathfrak{g}_6^{-6} \mathfrak{g}_7^2,$$

$\mathfrak{g}_6 = 2\mathbb{Z}_K, \mathfrak{g}_7 = 438704408599\mathbb{Z}_K + (\rho_1 - 116533633646)\mathbb{Z}_K$,

$$(63153799/49 - \rho_1) = (\mathfrak{g}_1^{\sigma})^4 (\mathfrak{g}_1^{\sigma^2})^4 \mathfrak{g}_8^{-2} \mathfrak{g}_9^2,$$

avec $\mathfrak{g}_8 = 7\mathbb{Z}_K, \mathfrak{g}_9 = 669968051\mathbb{Z}_K + (\rho_1 + 149112138)\mathbb{Z}_K$. Donc les 7 points sont dans H, et ils sont indépendants modulo $2E_{626}(\mathbb{Q})$. Comme le rang de la courbe est égal à 7, on déduit alors que $\mathrm{rg}_2(H/2E_{626}(\mathbb{Q})) = 7$. Il en résulte que $r_2 \geq 6$. Comme dans les exemples $1, 2$, r_2 calculé par pari est égal à 6.

Remarque 14. *Quand* $\mathrm{rg}_2(H/2E_n(\mathbb{Q}))$ *est égal au rang de la courbe elliptique* E_n*, alors on obtient dans ce cas une minoration de* r_2 *; comme on l'a vu dans les exemples* $1, 2$ *et* 4*.*

On résume dans le tableau suivant les résultats obtenus par les méthodes utilisées dans le chapitre 4, pour $-100 \leq n \leq 100$; s désigne la borne supérieure donnée dans la proposition **??**.

n	r	r_2	$rg_2(H_1/2E_n(\mathbb{Q}))$	s
-92	$1 \leq\leq 2$	0	1	3
-88	2	0	1	2
-70	2	0	1	2
-68	2	2	≤ 3	5
-58	3	2	3	5
-56	$1 \leq\leq 3$	2	≤ 3	5
-52	$1 \leq\leq 3$	2	≤ 3	4
-50	2	2	2	5
-46	2	0	1	2
-38	$1 \leq\leq 3$	2	≤ 3	5
-34	2	0	1	3
-32	3	2	2	5
-22	4	2	3	4
-20	2	2	2	5
-16	2	0	1	2
-14	3	2	2	5
-8	3	2	3	4
8	$2 \leq\leq 4$	2	2	4
10	3	2	3	5
22	2	0	1	3
26	3	2	2	5
44	3	2	3	5
50	4	2	3	4
52	2	2	2	5
80	2	0	1	2
88	$1 \leq\leq 3$	2	≤ 3	5
92	2	0	1	3
94	2	0	1	3
98	$2 \leq\leq 4$	0	1	2
100	$1 \leq\leq 3$	2	≤ 3	5

Remarque 15. • *Pour $n = -68$, d'après le programme mwrank de Cremona le rang r de la courbe est égal à 2, donc $rg_2(H_1/2E_n(\mathbb{Q})) \leq 2$. Ce qui donne une meilleure borne que la proposition* **??**.

• *Pour $n = 98$, le programme mwrank de Cremona donne seulement un encadrement de r : $2 \leq r \leq 4$, et d'après la proposition* **??**, $r \leq 1 + n_p + r_2$ *donc $r = 2$.*

Bibliographie

[1] Bach, E. *Explicit bounds for primality testing and related problems*. Math. Comp 55, 355-380 (1990).

[2] Beauville, A. *Les familles stables de courbes elliptiques sur* $\mathbb{P}^1$ *admettant quatre fibres singulières*. C. R. Acad. Sc. Paris 294, 657-660 (1982)

[3] Billing, G. *Beiträge zur arithmetischen Theorie der ebenen Kubischen Kurven vom Geschlecht eins*. Nova Acta Regiae Soc. Sci. Upsaliensis (4) 11, no.1 165 (1938).

[4] Brumer, A. Kramer, K. *The rank of elliptic curves*. Duke Math. J. 44, no.4 715-743 (1977).

[5] Brunault, F. *Etude en* $s = 2$ *de la fonction L d'une courbe elliptique*. Thèse de doctorat, Université Paris 7 Denis Diderot, Décembre 2005.

[6] Buchmann, J. *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*. Séminaire de Théorie des Nombres, Paris, 27-41 (1988-89).

[7] Campbell, G. *Finding Elliptic Curves and Families of Elliptic Curves over* $\mathbb{Q}$ *of Large Rank*, Dissertation, Rutgers, (1999).

[8] Cremona, J. *Algorithms for Modular Elliptic Curves*, Cambridge University. Press, (1997).

[9] Cohen, H. *A course in Computational Algebraic Number Theory*, volume 138 of Graduate Texts in Mathematics. Springer-Verlag, (1991).

[10] Dewaghe, L. *Isogénie entre courbes elliptiques*. Util. Math. 55, 123-127 (1999).

[11] Dujella, A. *High rank elliptic curves with prescribed torsion*, http ://www. math. hr/ duje/tors/tors. html, November 2001.

[12] Dujella, A. *An example of elliptic curve over* $\mathbb{Q}$ *with rank equal to* 15, Proc. Japan Acad. Ser. A Math. Sci. 78, 109-111 (2002).

[13] Hafner, J. McCurley, K. *A rigorous subexponential algorithm for computation of class groups*. J. Amer. Math. Soc. 2, 837-850 (1989).

[14] Gaàl, I. Phost, M. Power integral bases in a parametric family of totally real quintics, Math. Comput. 66, 1689-1696 (1997).

[15] Gras, M.N. *Sur les corps cubiques cycliques dont l'anneau des entiers est monogéne*. C. R. Acad. Sci. Paris Sér. A 278, 59-62 (1974).

[16] Gross, B. *Heegner points and modular curve of prime level*. Journ. Math. Soc. Japan, 32, 347-362 (1987).

[17] Hellegouarch,Y. *Points d'ordre fini sur les courbes elliptiques*. A 273, 540-543 (1971).

[18] Ireland, K. Rosen, M. *A Classical Introduction to Modern Number Theory*.

[19] Kawachi, M. Nakano, S. *The 2-Class groups of cubic fields and* 2*-descents on elliptic curves*. Tôhoku Math. J. 44, 557-565 (1992).

[20] Laoudi, A. 2*-rang du groupe des classes et courbes elliptiques*. Glasnik Matematicki.Vol 41(61), 31-49 (2006).

[21] Laoudi, A. Lecacheux, O. *Surfaces elliptiques modulaires et corps cubiques cycliques*. Annales des Sciences Mathématiques du Québec, à paraitre .

[22] Lecacheux, O. *Units in number fields and elliptic curves*. Gouvêa, Fernando Q. (ed.) et al. Advances in number theory. (Kingston, ON, 1991). Oxford Univ. Press, New York 293-301 (1993).

[23] Lecacheux, O. *Rang de courbes elliptiques avec groupe de torsion non trivial*, J. Theor. Nombres Bordeaux 15 , 231-247 (2003).

[24] Mazur, B., *Rational points on abelian varieties with values in towers of number fields,* Invent. Math. 18, 183-266 (1972).

[25] Mestre, J.F. *Courbes elliptiques et formules explicites*. Séminaire Théorie des Nombres, Paris, 179-187 (1981-82).

[26] Mestre, J.F. *Construction de courbes elliptiques sur* $\mathbb{Q}$ *de rang* ≥ 12. C. R. Acad. Sci. Paris Ser. I 295, 643-644 (1982).

[27] Nagao, K. *An example of elliptic curve over* $\mathbb{Q}$ *with rank* ≥ 20. Proc. Japan Acad. Ser. A Math. Sci. 69, 291-293 (1993).

[28] Narkiewicz, W. *Elementary and analytic theory of algebraic numbers*. 2nd ed., Springer-verlag ; PWN-Polish Scientific Publishers. (1990).

[29] Ogg, A.P. *Rationnal points on certain elliptic modular curves* . In analytic number theory (Proc. Sympos. Pure Math, Vol XXIV, St. Louis Univ, St. Louis, Mo, 1972), pages 221-231. Amer. Math. Soc, Providence, R.I, 1973.

[30] PARI/GP, version 2.1.5, Bordeaux, 2004, url http ://pari.math.u-bordeaux.fr/.

[31] Shanks, D. *Simplest cubic fields*. Math.Comp, 28, 1137-1152, (1974).

[32] Silverman, J.H. *The Arithmetic of elliptic curves* . Springer-verlag New York, 1986.

[33] Silverman, J.H. *Advanced topics in the arithmetic of elliptic curves*. Springer-verlag New York, 1994.

[34] Uchida, K. *Class numbers of cubic fields* . J. Math. Soc. Japan, v. 26, 447-453 (1974).

[35] Washington, L.C. *A family of cubic fields and zeros of* 3*-adic L-functions*. J. Number Theory 63, no.2, 408-417 (1997).

[36] Washington, L.C. *Class numbers of the simplest cubic fields*. Math. Comp. 48, no.177, 371-384 (1987).

[37] Washington, L.C. *Introduction to cyclotomic fields*. Springer- Verlag, New York-Heidelberg-Berlin, (1982).

[38] Washington, L.C. *A family of cyclic quartic fields arising from modular curves.* Math. Comp. 57, no. 196, 763-775 (1991).

Résumé

Dans cette thèse nous nous intéresserons aux extensions cubiques cycliques K_n engendrées par θ_n, racine du polynôme

$$P_n(X) = X^3 - (n^3 - 2n^2 + 3n - 3)X^2 - n^2X - 1,$$

où $n \in \mathbb{Z}$. Dans la première partie de cette thèse, nous expliquerons l'origine de cette famille. À partir du revêtement des courbes modulaires $X_1(18) \longrightarrow X_0(18)$, on construit ces corps par spécialisation d'un générateur n du corps des fonctions de la courbe $X_0(18)$ avec $n \in \mathbb{Z}$. On montre que si n décrit une partie infinie de $\mathbb{Z}$, certaines unités modulaires de $X_1(18)$ se spécialisent en un système générateur du groupe des unités de K_n. Le théorème de Manin-Drinfield se traduit par une propriété sur le régulateur de ces corps de nombres. On étudie l'arithmétique de ces corps et on montre que l'anneau des entiers n'est jamais monogène. Dans la seconde partie, on étudie le lien entre les courbes elliptiques E_n données par l'équation : $y^2 = G_n(x)$ et le 2-rang du groupe des classes des corps cubiques K_n, où $G_n(x) = -x^3P_n(-1/x)$. On obtient alors les résultats suivants : En adaptant une méthode classique de 2-descente, on montre, sous certaines conditions portant sur n, une majoration du rang des courbes elliptiques E_n en fonction du nombre de facteurs premiers de $|n-1|$ et du 2-rang r_2 du groupe des classes de K_n. On montre d'autre part, qu'il existe un sous-groupe H de $E_n(\mathbb{Q})$ et une suite exacte qui donnent une relation entre le 2-rang de $H/2E_n(\mathbb{Q})$ et le 2-rang du groupe des classes des corps cubiques K_n.

Summary

In this thesis, we study cyclic cubic extensions K_n generated by a root θ of the following polynomial $P_n(X) = X^3 - (n^3 - 2n^2 + 3n - 3)X^2 - n^2X - 1$, where n in $\mathbb{Z}$. In first part, we explain the origin of this family. Starting from a covering of modulars curves $X_1(18) \longrightarrow X_0(18)$, we build extensions by specializing a n-generator of the function field of the curve $X_0(18)$ with n in $\mathbb{Z}$. We show that as n varies in an infinite subset of $\mathbb{Z}$, some modular units specialize in a generating system of the units group of K_n. The Manin-Drinfield theorem then translates in a property of the regulator of these fields. We study their arithemtic and we show that the ring of integer is never generated by a single element. In the second part, we study the link between elliptic curves E_n given by the equation : $y^2 = G_n(x)$, where $G_n(x) = -x^3P_n(-1/x)$, and the 2-rank of the class group of the cubic fields K_n. We obtain the following results : A computation adapted from a classical 2-descent method gives, under some conditions on n, a bound on the rank of E_n in terms of the number of prime divisors of $|n-1|$ and of the 2-rank r_2 of the class group of cubic fields K_n. Besides, we show that there exists a subgroup H of $E_n(\mathbb{Q})$ and an exact sequence giving relations between the 2-rank of $H/2E_n(\mathbb{Q})$, and the 2-rank of the class group of cubic fields K_n.