

ANNALES DE L'INSTITUT FOURIER

GEORGES GRAS

**Sur les ℓ -classes d'idéaux dans les extensions
cycliques relatives de degré premier ℓ**

Annales de l'institut Fourier, tome 23, n° 4 (1973), p. 1-44

http://www.numdam.org/item?id=AIF_1973__23_4_1_0

© Annales de l'institut Fourier, 1973, tous droits réservés.

L'accès aux archives de la revue « Annales de l'institut Fourier » (<http://annalif.ujf-grenoble.fr/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

SUR LES l -CLASSES D'IDÉAUX DANS LES EXTENSIONS CYCLIQUES RELATIVES DE DEGRÉ PREMIER l

par Georges GRAS.

CHAPITRE V (*)

QUELQUES APPLICATIONS DES RÉSULTATS PRÉCÉDENTS

A. Généralisation d'un théorème de Kisilewsky.

Les propositions IV.2 et IV.3 peuvent s'appliquer à $M = \mathcal{H}(K)$, si et seulement si $|\mathcal{H}_1| = l$ (les quotients $\mathcal{H}_{i+1}/\mathcal{H}_i$ étant nécessairement d'ordre l pour $i < n$).

Le théorème IV.1 nous donne :

$$|\mathcal{H}_1| = \frac{|\mathcal{H}(k)|l^{t-1}}{(E_k^+ : E_k^+ \cap NK^*)},$$

et la condition $|\mathcal{H}_1| = l$ se produit dans les trois cas suivants (compte tenu du théorème IV.3 appliqué à $\Lambda = E_k^+$ qui montre que $(E_k^+ : E_k^+ \cap NK^*)$ divise l^{t-1}):

- (i) $|\mathcal{H}(k)| = 1, t \geq 2, (E_k^+ : E_k^+ \cap NK^*) = l^{t-2},$
- (ii) $|\mathcal{H}(k)| = l, t \geq 1, (E_k^+ : E_k^+ \cap NK^*) = l^{t-1},$
- (iii) $|\mathcal{H}(k)| = l^2$ et $t = 0.$

(*) On rappelle que les chapitres précédents sont parus dans le tome 23 (fascicule 3) des Annales de l'Institut Fourier.

Si $k = \mathbf{Q}$ et l impair, il ne subsiste que le cas (i) avec $t = 2$. Avec le cas (iii), on retrouve un résultat ([22]) énoncé dans un cas très particulier.

B. Problème de O. Taussky.

Supposons K/k non ramifiée pour les idéaux; le théorème 94 de Hilbert [17] affirme qu'un idéal de k devient principal dans K/k (cf. remarque IV.1); si $\mathcal{H}(K)$ est le l -groupe des classes de K , $N\mathcal{H}(K)$ est d'indice l dans $\mathcal{H}(k)$ (théorie du corps de classes).

O. Taussky a donné la définition suivante [33]:

L'extension K/k est dite de type A si

$$N\mathcal{H}(K) \cap \text{Ker } j \neq \{1\},$$

sinon elle est dite de type B (dans le cas B on a donc

$$|\mathcal{H}(K)^\vee| = |N\mathcal{H}(K)|).$$

Si \mathcal{H} est un sous-H-module de $\mathcal{H}(K)$, on a

$$|\tilde{\mathcal{H}}/\mathcal{H}| = \frac{|\mathcal{H}(k)|}{|N\mathcal{H}|l}$$

(théorème IV.3), soit $|\tilde{\mathcal{H}}/\mathcal{H}| = \frac{|\mathcal{H}_1|}{|N\mathcal{H}|}$ (théorème IV.1)

$$= \frac{|\mathcal{H}_1|}{|\mathcal{H}^\vee|} \frac{|\mathcal{H}^\vee|}{|N\mathcal{H}|};$$

la suite exacte $1 \rightarrow \text{Ker } j \cap N\mathcal{H} \rightarrow N\mathcal{H} \xrightarrow{j} \mathcal{H}^\vee \rightarrow 1$ donne

$$|\tilde{\mathcal{H}}/\mathcal{H}| = \frac{|\mathcal{H}_1|}{|\mathcal{H}^\vee| |\text{Ker } j \cap N\mathcal{H}|} = \frac{|\hat{H}^0(\mathbf{H}, \mathcal{H})|}{|\text{Ker } j \cap N\mathcal{H}|},$$

en désignant par \hat{H}^i la cohomologie modifiée de Tate. Appliqué à $\mathcal{H} = \mathcal{H}(K)$ on retrouve un résultat de [22] (démontré dans le cas cyclique de degré quelconque): à savoir que la condition B équivaut à la condition: $|\hat{H}^0(\mathbf{H}, \mathcal{H}(K))| = 1$.

C. Résultats sur les corps quadratiques.

1. Comparaison des 4-rangs de $\mathbf{Q}(\sqrt{m})$ et de $\mathbf{Q}(\sqrt{-m})$ [8].

Soit m un entier sans facteurs carrés. Posons $\mathbf{K} = \mathbf{Q}(\sqrt{m})$ et $\hat{\mathbf{K}} = \mathbf{Q}(\sqrt{-m})$ et réservons la notation \wedge pour toute quantité qui concerne le corps $\hat{\mathbf{K}}$.

Soient p_1, \dots, p_{t^*} les nombres premiers ramifiés dans \mathbf{K}/\mathbf{Q} (ils se ramifient aussi dans $\hat{\mathbf{K}}/\mathbf{Q}$). Si 2 ne divise pas m , il est nécessairement ramifié dans \mathbf{K} ou dans $\hat{\mathbf{K}}$ (et dans l'un des deux seulement), sinon il est ramifié dans les deux corps.

D'après les corollaires IV.1 et IV.2, les ordres des groupes de classes invariantes sont respectivement :

$$|\mathcal{H}_1| = 2^{t-1} \quad \text{et} \quad |\hat{\mathcal{H}}_1| = 2^{\hat{t}-1};$$

les groupes \mathcal{H}_1 et $\hat{\mathcal{H}}_1$ étant engendrés par les classes des idéaux premiers ramifiés. Les groupes Λ et $\hat{\Lambda}$ associés sont donc :

$\Lambda = \langle p_1, \dots, p_{t^*} \rangle$, $\hat{\Lambda} = \langle p_1, \dots, p_{t^*}, 2 \rangle$ ou vice versa, lorsque m est impair;

$\Lambda = \hat{\Lambda} = \langle p_1, \dots, p_{t^*}, 2 \rangle$ lorsque 2 divise m .

Soient A et \hat{A} les matrices (carrées) des systèmes linéaires associés aux groupes Λ et $\hat{\Lambda}$ (cf. théorème IV.3).

Les propositions IV.1 et IV.2 et le corollaire IV.4 ramènent la comparaison des 4-rangs R_2 et \hat{R}_2 de \mathbf{K} et $\hat{\mathbf{K}}$ à la comparaison des rangs r et \hat{r} des matrices A et \hat{A} : en effet, on obtient immédiatement la relation :

$$R_2 - \hat{R}_2 = t - \hat{t} + \hat{r} - r.$$

Posons pour $1 \leq i, j \leq t^*$:

$$\begin{aligned} (m, p_i)_{p_j} &= (-1)^{a_{ji}}, & (-m, p_i)_{p_j} &= (-1)^{\hat{a}_{ji}}; \\ (m, p_i)_2 &= (-1)^{\varepsilon_i}, & (-m, p_i)_2 &= (-1)^{\hat{\varepsilon}_i}; \\ (m, 2)_{p_i} &= (-1)^{\eta_i}, & (-m, 2)_{p_i} &= (-1)^{\hat{\eta}_i}; \\ (m, 2)_2 &= (-1)^{\eta_0}, & (-m, 2)_2 &= (-1)^{\hat{\eta}_0} \end{aligned}$$

et $\delta_i = \frac{p_i - 1}{2}$ (les quantités a_{ji} , ε_i , η_i , η_0 , δ_i , ... étant définies modulo 2).

On pose enfin $m = 2d$ si 2 divise m , $m = d$ sinon et on peut supposer $d \equiv 1$ modulo 4 quitte à échanger les rôles de m et de $-m$ une fois pour toutes. La formule du produit appliquée à $(d, -1)$ conduit alors à :

$$(-1)^{\sum \delta_i} = \text{sgn}(d) \quad (\text{noté } (-1)^{\delta_0}).$$

De même, la formule du produit appliquée à $(m, 2)$ donne $\eta_0 + \sum_i \eta_i = 0$.

LEMME V.1. — *On a les relations :*

- (i) $a_{ij} + a_{ji} = \delta_i \delta_j$ pour $i \neq j$,
- (ii) $\hat{a}_{ij} = a_{ij}$ pour $i \neq j$,
- (iii) $\hat{a}_{ii} = a_{ii} + \delta_i$,
- (iv) $\hat{\varepsilon}_i = \varepsilon_i + \delta_i$, $\hat{\eta}_i = \eta_i$ et $\hat{\eta}_0 = \eta_0$.

La première exprime la loi de réciprocité quadratique appliquée aux nombres p_i et p_j : $\left(\frac{p_i}{p_j}\right)\left(\frac{p_j}{p_i}\right) = (-1)^{\frac{p_i-1}{2}\frac{p_j-1}{2}}$ (symboles de Legendre); les deux suivantes résultent du calcul du symbole $(-1, p_i)_{p_j}$: si $i \neq j$, $(-1, p_i)_{p_j} = 1$ et $(-1, p_i)_{p_i} = (-1)^{\delta_i}$. La dernière résulte des relations : $(-1, p_i)_2 = (-1)^{\delta_i}$ et $(-1, 2)_{p_i} = (-1, 2)_2 = 1$.

On pose :

$$B = \begin{pmatrix} a_{11} & \dots & a_{1t^*} \\ a_{t^*1} & \dots & a_{t^*t^*} \end{pmatrix}, \quad M = \begin{pmatrix} 1 & \delta_1 \\ \vdots & \vdots \\ 1 & \delta_{t^*} \\ & 1 \end{pmatrix},$$

$$\Delta = \begin{pmatrix} \delta_1 \delta_1 & \dots & \delta_1 \delta_{t^*} \\ \delta_{t^*} \delta_1 & \dots & \delta_{t^*} \delta_{t^*} \end{pmatrix},$$

$$D = \begin{pmatrix} \delta_1 & & 0 \\ & \ddots & \\ 0 & & \delta_{t^*} \end{pmatrix} \quad \hat{B} = B + D.$$

Le lemme précédent (assertion (i)) montre que :

$$\hat{B} = {}^tB + \Delta.$$

a) *Cas où 2 ne divise pas m.* (on rappelle que $m = d \equiv 1 \pmod{4}$). Le nombre 2 étant non ramifié dans K et ramifié dans \hat{K} on a :

$$A = B, \quad \hat{A} = \begin{pmatrix} \hat{B} & \eta_1 \\ & \vdots \\ & \eta_{t^*} \\ \delta_1 & \dots & \delta_{t^*} & \eta_0 \end{pmatrix}$$

et

$$M\hat{A} = \begin{pmatrix} {}^tB & \eta_1 + \delta_1 \eta_0 \\ & \vdots \\ & \eta_{t^*} + \delta_{t^*} \eta_0 \\ \delta_1 & \dots & \delta_{t^*} & \eta_0 \end{pmatrix}$$

(i) *Cas m > 0.* On a

$$(m, m)_{p_i} = (-1, m)_{p_i} (-m, m)_{p_i} = (-1)^{\delta_i}$$

car m est norme dans $\mathbf{Q}(\sqrt{-m})$; donc la somme des colonnes de B est formée des δ_i ; de plus les sommes $\sum_i \eta_i + \eta_0$ et $\delta_0 = \sum_i \delta_i$ sont nulles, par conséquent, la somme des lignes de $M\hat{A}$ est la ligne nulle et $\hat{r} = r$ ou $r + 1$, soit

$$-1 \leq R_2 - \hat{R}_2 \leq 0.$$

(ii) *Cas m < 0.* Dans ce cas, la somme δ_0 est égale à 1 et, la somme des lignes de B étant nulle ($\varepsilon_i = 0$), on peut, pour déterminer \hat{r} , remplacer la t^* -ème colonne de $M\hat{A}$ par la

colonne $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$; il en résulte immédiatement que $\hat{r} = r + 1$ ou $r + 2$ soit :

$$0 \leq R_2 - \hat{R}_2 \leq 1.$$

b) *Cas où 2 divise m.* On aura (compte tenu du lemme V.1) :

$$A = \begin{pmatrix} & B & \eta_1 \\ & & \vdots \\ \varepsilon_1 & \dots & \varepsilon_{t^*} & \eta_0 \end{pmatrix}$$

et

$$\hat{A} = \begin{pmatrix} & \hat{B} & \eta_1 \\ & & \vdots \\ \varepsilon_1 + \delta_1 & \dots & \varepsilon_{t^*} + \delta_{t^*} & \eta_{t^*} \\ & & & \eta_0 \end{pmatrix}$$

(i) *Cas* $m > 0$. La somme des colonnes de la matrice A est constituée des symboles $(m, m)_{p_i}$ et $(m, m)_2$.

On a $(m, m)_{p_i} = (-1)^{\delta_i}$ et $(m, m)_2 = 1$.

Compte tenu de ces relations et du fait que la somme des lignes de A est nulle, le rang r est égal au rang des matrices :

$$A_1 = \begin{pmatrix} B & \delta_1 \\ & \vdots \\ & \delta_{t^*} \end{pmatrix} \quad \text{et} \quad A_1^t M = \begin{pmatrix} B + \Delta & \delta_1 \\ & \vdots \\ & \delta_{t^*} \end{pmatrix};$$

or $A_1^t M = \begin{pmatrix} {}^t \hat{B} & \delta_1 \\ & \vdots \\ & \delta_{t^*} \end{pmatrix}$ et \hat{A} a même rang que \hat{B} (en effet la somme des lignes et la somme des colonnes de \hat{A} sont nulles). On aura, dans ce cas, $r = \hat{r}$ ou $r = \hat{r} + 1$ soit encore :

$$-1 \leq R_2 - \hat{R}_2 \leq 0.$$

(ii) *Cas* $m < 0$. On échange les rôles des matrices A et \hat{A} : la somme des colonnes de \hat{A} est constituée des symboles $(-m, -m)_{p_i}$ et $(-m, -m)_2$; or $(-m, -m)_{p_i} = (-1)^{\delta_i}$ et $(-m, -m)_2 = -1$; on vérifie que, de la même manière A a même rang que B et que \hat{A} a même rang que les matrices :

$$\hat{A}_1 = \begin{pmatrix} \hat{B} & \delta_1 \\ & \vdots \\ & \delta_{t^*} \end{pmatrix} \quad \text{et} \quad \hat{A}_1^t M = \begin{pmatrix} \hat{B} + \Delta & \delta_1 \\ & \vdots \\ & \delta_{t^*} \end{pmatrix}$$

soit $\hat{A}_1^t M = \begin{pmatrix} {}^t B & \delta_1 \\ & \vdots \\ & \delta_{t^*} \end{pmatrix}$; d'où la conclusion :

$$0 \leq R_2 - \hat{R}_2 \leq 1.$$

On peut alors énoncer le résultat (obtenu dans [8] par dénombrement d'extensions non ramifiées et, ici, comme

conséquence des lois de réciprocité quadratique) :

PROPOSITION V.1. — Soit m un entier sans facteurs carrés avec $m \equiv 1 \pmod 4$ si 2 ne divise pas m et $\frac{m}{2} \equiv 1 \pmod 4$ si 2 divise m . Les 4-rangs R_2 et \hat{R}_2 de $\mathbf{Q}(\sqrt{m})$ et de $\mathbf{Q}(\sqrt{-m})$ diffèrent d'une unité au plus. De façon plus précise : $R_2 \leq \hat{R}_2 \leq R_2 + 1$ pour $m > 0$; $R_2 - 1 \leq \hat{R}_2 \leq R_2$ pour $m < 0$.

2. Corps quadratiques ayant un 4-rang donné [6].

PROPOSITION V.2. — Soit $m \in \mathbf{Z}$ un entier sans facteurs carrés, soit p un nombre premier congru à 1 modulo 4 et ne divisant pas m . On pose $K = \mathbf{Q}(\sqrt{m})$ et $\hat{K} = \mathbf{Q}(\sqrt{pm})$; on note p_1, \dots, p_t les nombres premiers ramifiés dans K/\mathbf{Q} (dans \hat{K}/\mathbf{Q} , p_1, \dots, p_t, p se ramifient et ce sont les seuls).

Si $\left(\frac{p_i}{p}\right) = 1$ pour tout $i, 1 \leq i \leq t$, les 4-rangs R_2 et \hat{R}_2 de $\mathcal{H}(K)$ et $\mathcal{H}(\hat{K})$ vérifient :

$$\hat{R}_2 = R_2 + 1.$$

Démonstration. — A K est associé $\Lambda = \langle p_1, \dots, p_t \rangle$ et à \hat{K} est associé $\hat{\Lambda} = \langle p_1, \dots, p_t, p \rangle$. Posons

$$(-1)^{\varepsilon_{ij}} = (p, p_j)_{p_i},$$

$(-1)^{\alpha_{ij}} = (m, p_j)_{p_i}$, $(-1)^{\eta_i} = (pm, p)_{p_i}$, $(-1)^{\delta_i} = (pm, p_i)_p$ et $(pm, p)_p = (-1)^{\eta_0}$; alors les matrices associées à Λ et $\hat{\Lambda}$ sont respectivement :

$$A = \begin{pmatrix} a_{11} & \dots & a_{1t} \\ a_{21} & \dots & a_{2t} \\ \dots & \dots & \dots \\ a_{t1} & \dots & a_{tt} \end{pmatrix}$$

et

$$\hat{A} = \begin{pmatrix} \varepsilon_{11} + a_{11} & \dots & \varepsilon_{1t} + a_{1t} & \eta_1 \\ \varepsilon_{21} + a_{21} & \dots & \varepsilon_{2t} + a_{2t} & \eta_2 \\ \dots & \dots & \dots & \dots \\ \varepsilon_{t1} + a_{t1} & \dots & \varepsilon_{tt} + a_{tt} & \eta_t \\ \delta_1 & \dots & \delta_t & \eta_0 \end{pmatrix}$$

Pour $i \neq j$, $(-1)^{\varepsilon_{ij}} = (p, p_j)_{p_i} = 1$, pour $p_i \neq 2$,

$$(-1)^{\varepsilon_{ii}} = \left(\frac{p}{p_i}\right) = (-1)^{\frac{p-1}{2} \frac{p_i-1}{2}} \left(\frac{p_i}{p}\right) = \left(\frac{p_i}{p}\right)$$

car $p \equiv 1 \pmod{4}$;

si

$$p_i = 2, (-1)^{\varepsilon_{ii}} = (p, 2)_2 = (-1)^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right) = \left(\frac{p_i}{p}\right).$$

Si $\left(\frac{p_i}{p}\right) = 1$ pour tout i on aura

$$\hat{A} = \begin{pmatrix} & & & \eta_1 \\ & A & & \vdots \\ & & & \eta_t \\ \delta_1 & \dots & \delta_t & \eta_0 \end{pmatrix};$$

or $(pm, p)_{p_i} = (p, p)_{p_i}(m, p)_{p_i} = \left(\frac{p_i}{p}\right) = 1$ pour tout i ,

$$(pm, p_i)_p = (p, p_i)_p(m, p_i)_p = \left(\frac{p_i}{p}\right) = 1 \text{ pour tout } i,$$

et enfin $(pm, p)_p = (p, p)_p(m, p)_p = (-1)^{\frac{p-1}{2}} \left(\frac{m}{p}\right) = 1$;

d'où $\hat{A} = \begin{pmatrix} & & 0 \\ & A & \vdots \\ 0 & \dots & 0 \end{pmatrix}$ et les rangs de A et \hat{A} sont égaux.

On aura donc pour $K: |\mathcal{H}_2/\mathcal{H}_1| = 2^{t-1-r}$ et pour

$$\hat{K}: |\hat{\mathcal{H}}_2/\hat{\mathcal{H}}_1| = 2^{\hat{t}-1-\hat{r}} = 2^{t-r},$$

d'où la relation $\hat{R}_2 = R_2 + 1$.

On peut donc construire une infinité de corps quadratiques ayant un 4-rang donné.

3. Autres exemples avec $l = 2$.

Dans ce paragraphe, nous allons montrer que certains résultats connus sur les corps quadratiques (et qui utilisent aussi les symboles locaux) découlent naturellement des méthodes exposées ici.

PROPOSITION V.3. (Hasse [15] et [16]). Soient p et $q \neq 2$ deux nombres premiers distincts tels que $pq \equiv 2$ ou $3 \pmod{4}$;

soit $K = \mathbf{Q}(\sqrt{-pq})$ et soit $\{1, \theta\}$ une \mathbf{Z} -base de A_K , alors :

- (i) $\mathcal{H}(K)$ est cyclique,
- (ii) si le symbole de Legendre $\left(\frac{p}{q}\right)$ est égal à -1 alors $|\mathcal{H}(K)| = 2$,
- (iii) si $\left(\frac{p}{q}\right) = 1$, il existe $x, y, z \in \mathbf{Z}$, $z > 0$, $(x, y, z) = 1$, tels que $pz^2 = N(x + y\theta)$; si $\left(\frac{z}{p}\right) = -1$ alors $|\mathcal{H}(K)| = 2^2$, sinon $|\mathcal{H}(K)|$ est divisible par 2^3 .

Démonstration. — Les nombres premiers ramifiés sont p et q (2 n'est ramifié que lorsque $p = 2$) et le groupe Λ associé à \mathcal{H}_1 est donc $\Lambda_1 = \langle p, q \rangle$; la matrice du système étant (en notation multiplicative) :

$$A = \begin{pmatrix} (-pq, p)_p & (-pq, q)_p \\ (-pq, p)_q & (-pq, q)_q \end{pmatrix} = \begin{pmatrix} \left(\frac{p}{q}\right) & \left(\frac{p}{q}\right) \\ \left(\frac{p}{q}\right) & \left(\frac{p}{q}\right) \end{pmatrix};$$

si $\left(\frac{p}{q}\right) = -1$ le rang de A est $r = 1$ et $\mathcal{H}(K) = \mathcal{H}_1$, d'où (ii). Supposons maintenant que $\left(\frac{p}{q}\right) = 1$: le rang de A est nul. Pour déterminer un groupe d'idéaux \mathcal{I} associé à \mathcal{H}_2 il faut résoudre les équations :

$$p = N\alpha \quad \text{et} \quad q = N\beta, \quad \alpha, \beta \in K^*;$$

en fait la relation $N(\sqrt{-pq}) = pq$ montre qu'il suffit d'une seule équation ($p = N\alpha$). On a donc

$$pz^2 = N(x + y\theta), \quad x, y, z \in \mathbf{Z}, \quad (x, y, z) = 1;$$

on constate sans peine que

$$(x + y\theta)A_K = \mathfrak{A}^2\mathfrak{p} \quad \text{avec} \quad \mathfrak{p}^2 = p\mathbf{Z}$$

et $\mathfrak{A}^{1+\sigma} = z\mathbf{Z}$; il existe \mathfrak{A}' tel que $\left(\frac{x + y\theta}{z}\right)A_K = \mathfrak{p}\mathfrak{A}'^{1-\sigma}$ soit $\mathfrak{A}'^{1-\sigma} = \frac{\mathfrak{A}^2}{zA_K} = \mathfrak{A}^{1-\sigma}$. On peut donc prendre $\mathfrak{A}' = \mathfrak{A}$ et $N\mathfrak{A} = z$. Il en résulte que $\mathcal{I} = \langle \mathfrak{p}, q, \mathfrak{A}, \mathfrak{A}^\sigma \rangle$ et que le

groupe Λ associé est $\Lambda = \langle p, q, z \rangle$; la matrice B correspondante est donc $B = \begin{pmatrix} 1 & 1 & \left(\frac{z}{p}\right) \\ 1 & 1 & \left(\frac{z}{p}\right) \end{pmatrix}$: si $\left(\frac{z}{p}\right) = -1$ le rang de B est 1 et $\mathcal{H}_2 = \mathcal{H}(K)$, si $\left(\frac{z}{p}\right) = +1$ le rang de B est nul et $|\mathcal{H}_2/\mathcal{H}_1| = |\mathcal{H}_3/\mathcal{H}_2| = 2$, d'où l'assertion (iii).

Remarque V.1. — Le procédé peut alors se continuer (cf. chapitre VI: « Algorithmes pour $l = 2$ », valable pour un corps quadratique quelconque).

PROPOSITION V.4. (Hasse [12]) — Soit p congru à 1 modulo 8; alors il existe x et y positifs tels que $p = 2x^2 - y^2$. Si on a $x \equiv 1$ modulo 4, $|\mathcal{H}(\mathbf{Q}(\sqrt{-p}))|$ est divisible par 8.

Démonstration. — On aura $\Lambda_1 = \langle p, 2 \rangle$ car 2 est ramifié dans $\mathbf{Q}(\sqrt{-p})/\mathbf{Q}$; la matrice associée sera (en notation multiplicative):

$$\begin{pmatrix} \left(\frac{-p, p}{p}\right) & \left(\frac{-p, 2}{p}\right) \\ \left(\frac{-p, p}{2}\right) & \left(\frac{-p, 2}{2}\right) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \text{ de rang nul.}$$

Comme $p = N(\sqrt{-p})$, il suffit de traduire le fait que 2 est norme: or p étant décomposé dans $\mathbf{Q}(\sqrt{2})$, qui est principal et dont l'unité fondamentale est de norme -1 , on peut écrire $-p = y^2 - 2x^2$, x, y positifs premiers à p . On a donc $2x^2 = y^2 + p$; ceci conduit à la relation

$$\left(\frac{y + \sqrt{-p}}{x}\right) A_{\mathbf{K}} = \mathfrak{p}_2^{\sigma-1}, \text{ avec } \mathfrak{p}_2^2 = (2)A_{\mathbf{K}} \text{ et } N\mathfrak{A} = (x).$$

On obtient alors $\Lambda_2 = \langle p, 2, x \rangle$ avec pour matrice associée:

$$\begin{pmatrix} 1 & 1 & \left(\frac{-p, x}{p}\right) \\ 1 & 1 & \left(\frac{-p, x}{2}\right) \end{pmatrix} = \begin{pmatrix} 1 & 1 & (-1)^{\frac{x-1}{2}} \\ 1 & 1 & (-1)^{\frac{x-1}{2}} \end{pmatrix},$$

d'où la proposition.

PROPOSITION V.5. — Soit p premier impair; alors $|\mathcal{H}(\mathbf{Q}(\sqrt{2p}))| = 2$ si et seulement si $p \not\equiv 1$ modulo 8. Lorsque $p \equiv 1$ modulo 8 alors $|\mathcal{H}(\mathbf{Q}(\sqrt{2p}))|$ est divisible par 8 si et seulement si $p \equiv 1$ mod 16 et dans l'écriture $p = x^2 + 2y^2$, y est divisible par 4 (sinon ce nombre est égal à 4).

Démonstration. — On aura $\mathcal{I}_1 = \langle \mathfrak{p}_2, \mathfrak{p}_p \rangle$ et $\Lambda_1 = \langle 2, p \rangle$ la matrice associée sera alors :

$$A_1 = \begin{pmatrix} (2p, 2)_2 & (2p, p)_2 \\ (2p, 2)_p & (2p, p)_p \end{pmatrix} = \begin{pmatrix} (-1)^{\frac{p^2-1}{8}} & (-1)^{\frac{p^2-1}{8} + \frac{p-1}{2}} \\ (-1)^{\frac{p^2-1}{8}} & (-1)^{\frac{p^2-1}{8} + \frac{p-1}{2}} \end{pmatrix}$$

on a alors $\mathcal{H}_2 = \mathcal{H}_1$ si et seulement si l'un des 4 symboles est différent de 1 donc si et seulement si $p \equiv 3, 5$ ou 7 modulo 8.

Supposons $p \equiv 1$ modulo 8, alors $A_1 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ et $|\mathcal{H}_2| = 2|\mathcal{H}_1| = 4$. Il en résulte aussi que p est décomposé dans les corps $\mathbf{Q}(\sqrt{-2})$ et $\mathbf{Q}(\sqrt{2})$ et qu'il existe des entiers u, v, x et y tels que

$$-p = u^2 - 2v^2 \quad \text{et} \quad p = x^2 + 2y^2$$

ce qui entraîne

$$(2v)^2 - 2p = 2u^2 \quad \text{et} \quad p^2 - 2py^2 = px^2$$

où l'on peut supposer $(p, y) = 1$ et $(u, v) = 1$.

On a $(2v + \sqrt{2p})A_K = \mathfrak{p}_2\mathfrak{A}^2$ où \mathfrak{A} est un idéal entier de norme u et, de même $(p + y\sqrt{2p})A_K = \mathfrak{p}_p\mathfrak{A}'^2$ avec \mathfrak{A}' entier de norme x . On a déjà vu que cela entraînait

$$\mathcal{I}_2 = \langle \mathfrak{p}_2, \mathfrak{p}_p, \mathfrak{A}, \mathfrak{A}', \mathfrak{A}^\sigma, \mathfrak{A}'^\sigma \rangle \quad \text{et} \quad \Lambda_2 = \langle 2, p, u, x \rangle$$

dont la matrice associée est

$$\begin{aligned} \begin{pmatrix} 1 & 1 & (2p, u)_2 & (2p, x)_2 \\ 1 & 1 & (2p, u)_p & (2p, x)_p \end{pmatrix} &= \begin{pmatrix} 1 & 1 & (-1)^{\frac{u^2-1}{8}} & (-1)^{\frac{x^2-1}{8}} \\ 1 & 1 & \left(\frac{u}{p}\right) & \left(\frac{x}{p}\right) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & (-1)^{\frac{u^2-1}{8}} & (-1)^{\frac{x^2-1}{8}} \\ 1 & 1 & (-1)^{\frac{u^2-1}{8}} & (-1)^{\frac{x^2-1}{8}} \end{pmatrix} \end{aligned}$$

grâce à la formule du produit; le fait que $u^2 \equiv 1 \pmod{16}$ et $x^2 \equiv 1 \pmod{16}$ est équivalent à $y \equiv 0 \pmod{4}$ et $p \equiv 1 \pmod{16}$, d'où la proposition.

Remarque V.2. — Les résultats précédents sont connus de P. Kaplan qui en a donné une démonstration directe à partir de l'étude des formes quadratiques (cf [20] et [21]).

CHAPITRE VI

MÉTHODES EFFECTIVES. RÉSULTATS NUMÉRIQUES

A. Étude du cas $k = \mathbf{Q}$.

1. Construction des extensions cycliques de degré l de \mathbf{Q} .

Nous reprenons ici l'étude générale du chapitre III (paragraphe B) avec l premier impair.

A K/\mathbf{Q} est associée l'extension de Kummer K'/\mathbf{Q}' définie par $K' = \mathbf{Q}'(\sqrt[l]{\alpha})$ où le nombre α choisi est tel que $q(\alpha) \in \mathfrak{K}^*$. Les seules places qui peuvent se ramifier dans K'/\mathbf{Q}' sont :

les idéaux premiers totalement décomposés dans \mathbf{Q}'/\mathbf{Q} , l'idéal premier $\mathcal{P}_0 = (1 - \zeta)$ au-dessus de l dans \mathbf{Q}' .

D'après la proposition III.2 on aura $R = P_0 \cup P_2$ (cf. Définition I.2); en particulier on aura toujours $v_{\mathcal{P}_0}(\alpha) \equiv 0$ modulo l .

PROPOSITION VI.1. — *Choisissons α congru à 1 modulo \mathcal{P}_0 ; alors l est ramifié dans K'/\mathbf{Q}' (donc dans K/\mathbf{Q}) si et seulement si la quantité*

$$\varpi = \frac{\alpha - 1}{1 - \zeta}$$

est première à \mathcal{P}_0 .

Démonstration. — Si l est ramifié, c'est que l'entier maximum λ tel que l'on ait $\alpha \equiv \xi^\lambda \pmod{\mathcal{P}_0^\lambda}$ dans \mathbf{Q}' vérifie $\lambda < l$ (cf. proposition I.2); on a donc $\alpha = \xi^\lambda + (1 - \zeta)^\lambda \varpi_1$ avec de plus $\xi \equiv 1 \pmod{\mathcal{P}_0}$ et $\varpi_1 \not\equiv 0 \pmod{\mathcal{P}_0}$;

$$\alpha = (1 + (1 - \zeta)A)^\lambda + (1 - \zeta)^\lambda \varpi_1,$$

ce qui est de la forme $\alpha = 1 + (1 - \zeta)^\lambda \varpi'$ avec ϖ' premier à \mathcal{P}_0 .

Soit s un générateur de $G = \text{Gal}(\mathbf{Q}'/\mathbf{Q})$ et soit g un

entier tel que $\alpha^s = \alpha^g u^l$, $u \in \mathbf{Q}'$. On obtient :

$$\begin{aligned} 1 + (1 - \zeta^g)^{\lambda \omega'^s} &= (1 + (1 - \zeta)^{\lambda \omega'})^g u^l, \\ 1 + (1 - \zeta^g)^{\lambda \omega'^s} &\equiv (1 + (1 - \zeta)^{\lambda \omega'})^g \pmod{\mathcal{P}_0^{\lambda+1}}, \end{aligned}$$

car $u^l \equiv 1$ modulo $(1 - \zeta)^l$,

$$\begin{aligned} 1 + (1 - \zeta^g)^{\lambda \omega'^s} &\equiv 1 + g \omega' (1 - \zeta)^\lambda && - , \\ (1 - \zeta)^\lambda (1 + \zeta + \dots + \zeta^{g-1})^{\lambda \omega'^s} &\equiv g \omega' (1 - \zeta)^\lambda && - , \\ (1 + \zeta + \dots + \zeta^{g-1})^\lambda &\equiv g \pmod{\mathcal{P}_0} \end{aligned}$$

(on a, en effet, $\omega'^s \equiv \omega' \pmod{\mathcal{P}_0}$ car G opère trivialement sur $A_{\mathbf{Q}'}/\mathcal{P}_0$); finalement, $g^\lambda \equiv g \pmod{l}$ entraîne $\lambda = 1$ (car g est racine primitive modulo l et $1 \leq \lambda < l$) et $\omega' = \omega$;

La réciproque est immédiate car alors la congruence $\alpha \equiv \xi^l \pmod{\mathcal{P}_0}$ est manifestement insoluble.

La proposition III.2 nous montre que :

$$\overline{\alpha A_{\mathbf{Q}'}} = \prod_{\mathfrak{P} \in \mathcal{D}} \overline{\mathcal{P}^{e^* x_{\mathfrak{P}}}}, \quad x_{\mathfrak{P}} \in \mathbf{Z};$$

on est donc amené à introduire l'ensemble \mathbf{V} suivant :

DÉFINITION VI.1. — Soit $t \geq 1$ et soit \mathbf{V} le quotient de l'ensemble des t -uplets $(\nu_1, \dots, \nu_t) \in \mathbf{F}_l^t$ avec les ν_i tous non nuls, par la relation d'équivalence définissant l'espace projectif $\mathbf{P}(\mathbf{F}_l^t)$.

On peut alors associer à $q(\alpha)$ un point de \mathbf{V} de la manière suivante :

(i) si l est non ramifié dans K/\mathbf{Q} on associe le t -uplet $(\nu_1, \dots, \nu_t) \in \mathbf{F}_l^t$ défini par $\nu_i \equiv \nu_{\mathfrak{P}_i}(\alpha)$ avec $\mathfrak{P}_i \in \mathcal{D}$ (on rappelle que \mathcal{D} est un système d'idéaux premiers non conjugués deux à deux représentant les idéaux premiers totalement décomposés dans \mathbf{Q}'/\mathbf{Q}).

(ii) Si l est ramifié dans K/\mathbf{Q} on associe le t -uplet $(\nu_1, \dots, \nu_{t-1}, \nu_t) \in \mathbf{F}_l^t$ défini par $\nu_i \equiv \nu_{\mathfrak{P}_i}(\alpha)$ pour

$$1 \leq i \leq t-1, \mathfrak{P}_i \in \mathcal{D}$$

et $\nu_t \equiv \frac{\alpha - 1}{1 - \zeta_0}$ modulo \mathcal{P}_0 , $\zeta_0^l = 1$, $\zeta_0 \neq 1$.

On définit, de cette manière, une application de $\mathbf{P}(\mathfrak{X}^*)$ dans \mathbf{V} qui dépend du choix de \mathcal{D} et, lorsque l est ramifié du choix de la racine primitive $l^{\text{ième}}$ de l'unité ζ_0 .

PROPOSITION VI.2. — *L'application définie ci-dessus est bijective.*

Ce résultat provient, par exemple, du fait que l'on peut dénombrer l'ensemble des extensions cycliques de degré l ramifiées en t places données (en l'occurrence ce nombre est égal à $(l - 1)^{t-1}$).

2. *Systèmes linéaires associés aux groupes Λ .*

Soient p_1, \dots, p_t les nombres premiers ramifiés dans K/\mathbb{Q} ; si l est ramifié on posera $l = p_t$.

Soit Λ le groupe de nombres associé à un quotient $\tilde{\mathcal{H}}/\mathcal{H}$ (notations du théorème IV.3). Étant donnée une base de Λ/Λ' de la forme $q(a_1), \dots, q(a_n)$ on fera l'hypothèse suivante (peu restrictive en pratique) :

HYPOTHÈSE VI.1. — *On a pour $t \leq n$: $a_1 = p_1, \dots, a_t = p_t$, et les nombres a_{t+1}, \dots, a_n ne sont divisibles par aucun des nombres premiers p_1, \dots, p_t ramifiés dans K/\mathbb{Q} .*

Par exemple cette hypothèse sera vérifiée facilement si \mathcal{H} contient \mathcal{H}_1 .

DÉFINITION VI.2. — *Soit \mathcal{P} un idéal premier dans \mathbb{Q}' ; on note $n_{\mathcal{P}}$ le nombre de conjugués distincts de \mathcal{P} dans \mathbb{Q}'/\mathbb{Q} et on pose pour $a \in \mathbb{Q}$:*

$$\begin{aligned} [a]_{\mathcal{P}} &= (p, a)_{\mathcal{P}}, \quad (p) = \mathcal{P} \cap \mathbb{Z}, \quad \mathcal{P} \neq \mathcal{P}_0 \\ [a]_{\mathcal{P}_0} &= (\zeta_0, a)_{\mathcal{P}_0} \quad \text{sinon.} \end{aligned}$$

On a alors le lemme suivant :

LEMME VI.1. — *Soit $p = p_i$ et soit $a \in \mathbb{Q}$, a premier à p_i ; alors $(\alpha, a)_{p_i} = [a]_{\mathcal{P}_i}^{v_i n_{\mathcal{P}_i}}$.*

Si $p_i \neq l$ on a $(\alpha, a)_{p_i} = (\alpha, a)_{\mathcal{P}_i}$ et (Proposition II.2) :

$$(\alpha, a)_{\mathcal{P}_i} \equiv (\alpha^{v_{\mathcal{P}_i}(\alpha)} a^{-v_{\mathcal{P}_i}(\alpha)})^{\frac{p_i-1}{l}} \text{ modulo } \mathcal{P}_i \equiv (a^{-v_i})^{\frac{p_i-1}{l}} \text{ modulo } \mathcal{P}_i;$$

or $[a]_{\mathcal{P}_i} = (p_i, a)_{\mathcal{P}_i}$ et $n_{\mathcal{P}_i} = l - 1$;

$$(p_i, a)_{\mathcal{P}_i} \equiv (p_i^{v_{\mathcal{P}_i}(\alpha)} a^{-v_{\mathcal{P}_i}(p_i)})^{\frac{p_i-1}{l}} \text{ modulo } \mathcal{P}_i \equiv (a^{-1})^{\frac{p_i-1}{l}} \text{ modulo } \mathcal{P}_i,$$

d'où le lemme dans ce cas.

Si $p_i = p_t = l$ on a $(\alpha, a)_l = \zeta_0^{S_{\mathcal{F}_0} \mathcal{G}_{\mathcal{F}_0} \left(\frac{\lambda_{\mathcal{F}_0}(\alpha-1)(a-1)}{l(\zeta_0-1)} \right)}$ (Proposition III.3) et, de même, $(\zeta_0, a)_{\mathcal{F}_0} = \zeta_0^{S_{\mathcal{F}_0} \mathcal{G}_{\mathcal{F}_0} \left(\frac{\lambda_{\mathcal{F}_0}(\zeta_0-1)(a-1)}{l(\zeta_0-1)} \right)}$; on a alors $\nu_i \equiv \frac{\alpha-1}{1-\zeta_0}$ et $n_{\mathcal{F}_0} = 1$; le lemme en résulte alors immédiatement.

Remarque VI.1. — Les calculs effectifs du chapitre III, paragraphe C montrent que si l'on pose

$$a^{l-1} = 1 + \mu l,$$

alors

$$(a, \alpha)_{\mathcal{F}_0} = \zeta_0^{\mu \nu_i}$$

lorsque $l = p_t$ est ramifié (on a, en effet, $S_{\mathcal{F}_0} =$ identité, $\lambda_{\mathcal{F}_0} = 1$ d'après la proposition VI.1).

Posons, pour simplifier l'écriture,

$$n_i = n_{\mathcal{F}_i}, \quad [a]_i = [a]_{\mathcal{F}_i}, \quad \mathcal{P}_i \in \mathcal{D} \quad \text{et} \quad (\alpha, a)_j = (\alpha, a)_{\mathcal{F}_j}.$$

THÉORÈME VI.1. — Soit Λ un groupe de nombres associé au quotient $\tilde{\mathcal{H}}/\mathcal{H}$ et soit $q(a_1), \dots, q(a_n)$ une base de Λ/Λ' vérifiant l'hypothèse VI.1; le système linéaire $\prod_{i=1}^n (\alpha, a_i)_{j^i} = 1$, $1 \leq j \leq t$ s'écrit (pour l impair) :

$$\begin{cases} \prod_{i=1}^n [a_i]_{j^i}^{\nu_i} \prod_{k=1}^t [a_j]_{k^i}^{-\nu_i k^i} = 1, & 1 \leq j \leq \bar{t}, \\ \prod_{i=1}^n [a_i]_{j^i}^{\nu_i} = 1, & \bar{t} + 1 \leq j \leq t, \end{cases}$$

où l'on a posé $[a]_{\mathcal{F}} = (p, a)_{\mathcal{F}} (p\mathbf{Z} = \mathcal{P} \cap \mathbf{Z}, \mathcal{P} \neq \mathcal{P}_0)$ et $[a]_{\mathcal{F}_0} = (\zeta_0, a)_{\mathcal{F}_0}$.

Démonstration. — Le système $\prod_{i=1}^n (\alpha, a_i)_{j^i} = 1$ s'écrit

$$\prod_{i=1}^{\bar{t}} (\alpha, a_i)_{j^i}^{\nu_i} \prod_{i>\bar{t}} (\alpha, a_i)_{j^i}^{\nu_i} = 1;$$

pour $i > \bar{t}$, a_i est premier à tous les p_j , $j = 1, \dots, t$ donc

(Lemme VI.1) $(\alpha, a_i)_j = [a_i]_j^{-n_j p_j}$. On aura donc pour $j \leq \bar{t}$:

$$\begin{aligned} \prod_{i=1}^n (\alpha, a_i)_{j^i} &= \prod_{\substack{i=1 \\ i \neq j}}^{\bar{t}} (\alpha, a_i)_{j^i} (\alpha, a_j)_{j^j} \prod_{i > \bar{t}} (\alpha, a_i)_{j^i} = 1 \\ &= \prod_{\substack{i=1 \\ i \neq j}}^{\bar{t}} [a_i]_j^{-n_j v_j^i} (\alpha, a_j)_{j^j} \prod_{i > \bar{t}} [a_i]_j^{-n_j v_j^i} = 1 \end{aligned}$$

Calcul de $(\alpha, a_j)_j$ ($j \leq \bar{t}$):

La formule du produit donne $\prod_{\mathfrak{P}} (\alpha, a_i)_{\mathfrak{P}} = 1$, ou encore $\prod_{\mathfrak{P}} (\alpha, a_j)_{\mathfrak{P}} = 1$, soit $\prod_{k=1}^t (\alpha, a_j)_{k^k} = 1$;

ramifié

$$(\alpha, a_j)_j = \prod_{\substack{k=1 \\ k \neq j}}^t (\alpha, a_j)_{k^k}^{-n_k/n_j} = \prod_{\substack{k=1 \\ k \neq j}}^t [a_j]_{k^k}^{n_k v_k/n_j}$$

Or $n_i = 1$ ou $l - 1$; par conséquent, on aura $n_k^2 \equiv 1$ et $1/n_j \equiv n_j$ modulo l et:

$$(\alpha, a_j)_j = \prod_{\substack{k=1 \\ k \neq j}}^t [a_j]_{k^k}^{n_j v_k}$$

Il vient alors pour la $j^{\text{ième}}$ ligne du système ($j \leq \bar{t}$):

$$\begin{aligned} \prod_{\substack{i=1 \\ i \neq j}}^n [a_i]_j^{-n_j v_j^i} \prod_{\substack{k=1 \\ k \neq j}}^t [a_j]_{k^k}^{n_j v_k^i} &= 1, \\ \text{soit} \quad \prod_{\substack{i=1 \\ i \neq j}}^n [a_i]_{j^i}^{v_j^i} \prod_{\substack{k=1 \\ k \neq j}}^t [a_j]_{k^k}^{-v_k^i} &= 1, \quad j \leq \bar{t}. \end{aligned}$$

Pour $j > \bar{t}$, l'hypothèse a_i premier avec p_j est vérifiée pour tout i et on obtient:

$$\prod_{i=1}^n (\alpha, a_i)_{j^i} = \prod_{i=1}^n [a_i]_j^{-n_j v_j^i} = 1$$

soit encore

$$\prod_{i=1}^n [a_i]_{j^i} = 1, \quad j > \bar{t}.$$

COROLLAIRE VI.1. — Lorsque \mathcal{K} contient \mathcal{K}_1 , on peut toujours supposer que $a_1 = p_1, \dots, a_t = p_t$ et l'expression

du système devient :

$$\prod_{i=1}^t [p_i]_j^{v_i x_i} [p_j]_i^{-v_i x_j} \prod_{i=t+1}^n [a_i]_j^{v_i x_i} = 1, \quad 1 \leq j \leq t.$$

COROLLAIRE VI.2. — Lorsque $\mathcal{H} = \mathcal{H}_1$ le groupe Λ est égal à $\Lambda_1 = \langle p_1, p_2, \dots, p_t \rangle$ et le système est alors :

$$\prod_{i=1}^t [p_i]_j^{v_i x_i} [p_j]_i^{-v_i x_j} = 1, \quad 1 \leq j \leq t.$$

THÉORÈME VI.2. — Lorsque l est égal à 2, il existe $m \in \mathbf{Z}$ tel que $K = \mathbf{Q}(\sqrt{m})$ et le système associé à Λ est

$$\prod_{i=1}^n (m, a_i)_{j_i}^{x_i} = 1, \quad 1 \leq j \leq t$$

avec les formules :

$$(a, b)_p = (-1)^{\frac{p-1}{2} v_p(a) v_p(b)} \left(\frac{b'}{p} \right)^{v_p(a)} \left(\frac{a'}{p} \right)^{v_p(b)}$$

(Symboles de Legendre)

$$\text{où} \quad a' = \frac{a}{p^{v_p(a)}}, \quad b' = \frac{b}{p^{v_p(b)}}, \quad p \neq 2,$$

$$(2, a)_2 = (-1)^{\frac{a^2-1}{8}} \quad \text{si } a \text{ est impair,}$$

$$(a, b)_2 = (-1)^{\frac{a-1}{2} \frac{b-1}{2}} \quad \text{si } a \text{ et } b \text{ sont impairs.}$$

Remarque VI.2. — Si r_i désigne le rang du système linéaire associé à la détermination de $|\mathcal{H}_{i+1}/\mathcal{H}_i|$, la proposition

IV.2 montre que $l^{R_1} = \prod_{i=0}^{l-2} |\mathcal{H}_{i+1}/\mathcal{H}_i| = \prod_{i=1}^{l-2} l^{t-1-r_i}$, soit :

$$R_1 = (l-1)(t-1) - \sum_{i=0}^{l-2} r_i$$

(cf. remarque de [28] p. 361 ainsi que [9]. Si l'hypothèse VI.1 n'est pas vérifiée, on ne peut pas donner une forme générale du système : on procède directement en utilisant, comme dans la démonstration du théorème VI.1, la formule du produit pour le calcul des symboles $(\alpha, p_i)_{p_i}$.

3. *Étude du cas* $\mathcal{H} = \mathcal{H}_1$.

La dimension du quotient $\mathcal{H}_2/\mathcal{H}_1$ est égale à $t - 1 - r$ où r est le rang du système

$$(S) : \prod_{i=1}^t [p_i]_j^{v_i x_i} [p_j]_i^{-v_i x_j} = 1, \quad 1 \leq j \leq t.$$

PROPOSITION VI.3. — *Le rang r du système (S) est égal à 0 si et seulement si p_i est congru à une puissance $l^{\text{ème}}$ modulo p_j pour tout $i, j, i \neq j$, en remplaçant cette condition par p_i congru à 1 modulo $l^2, i < t$, lorsque $p_t = l$. En outre, lorsque $r = 0$ relativement à K/\mathbb{Q} , on a $r = 0$ relativement aux $(l - 1)^{t-1}$ extensions ayant même discriminant que K/\mathbb{Q} .*

Démonstration. — La dernière partie de la proposition est évidente car la nullité de r ne dépend pas du système $\{v_1, \dots, v_t\}$ considéré.

On aura $r = 0$ si et seulement si $[p_i]_j = 1$ pour tout $i, j, i \neq j$; si $p_j \neq l$ on a

$$[p_i]_j = (p_j, p_i)_{\mathfrak{P}_j} \equiv (1/p_i)^{\frac{p_j-1}{l}} \text{ modulo } \mathfrak{P}_j,$$

d'où l'assertion; si $p_j = l$ alors

$$[p_i]_j = (\zeta_0, p_i)_{\mathfrak{P}_0} = \zeta_0^{\frac{p_i-1}{l}}.$$

PROPOSITION VI.4. — *Lorsque $t = 2$ on a les résultats suivants :*

(i) *l'ordre des groupes \mathcal{H}_2 est le même pour les $l - 1$ extensions K/\mathbb{Q} ramifiées en p_1, p_2 ;*

(ii) *si r est égal à 0 (ce qui équivaut à la condition $\mathcal{H}_2/\mathcal{H}_1 \neq \{1\}$) soit p un nombre premier décomposé dans K/\mathbb{Q} tel que l'un des symboles $[p]_{\mathfrak{P}_1}, [p]_{\mathfrak{P}_2}$ soit différent de 1; alors $\mathcal{H}(K)$ est le l -sous-groupe de Sylow du H -module engendré par la classe d'un idéal premier \mathfrak{p} au-dessus de p dans K .*

Démonstration. — Pour $t = 2$ le système (S) s'écrit :

$$\begin{cases} [p_2]_1^{v_1 x_1} [p_1]_2^{-v_2 x_1} = 1 \\ [p_1]_2^{v_2 x_1} [p_2]_1^{-v_1 x_2} = 1. \end{cases}$$

Posons $[p_i]_j = \zeta_0^{aj}$; on obtient alors en notation additive le système :

$$\begin{cases} -a_{12}\nu_2x_1 + a_{21}\nu_1x_2 = 0 \\ a_{12}\nu_2x_1 - a_{21}\nu_1x_2 = 0 \end{cases}$$

dont le rang ne dépend pas des nombres ν_i car ceux-ci sont non nuls par hypothèse.

D'où l'assertion (i).

Supposons maintenant $r = 0$. Il existe q premier à l tel que la classe de p^q est d'ordre une puissance de l dans $\mathcal{H}(K)$. Considérons $\mathcal{J} = \langle p_1, p_2, p^q, p^{q\sigma}, \dots, p^{q\sigma^{l-1}} \rangle$ où p_1, p_2 désignent les deux idéaux premiers ramifiés dans K/Q . Soit \mathcal{H} l'image de \mathcal{J} dans le groupe des classes de K ; on a en fait $\mathcal{H} \subset \mathcal{H}(K)$.

On vérifie que $\mathcal{J} \cap \mathcal{J}(K)^{\sigma^{-1}} = \mathcal{J}^{\sigma^{-1}}$; on peut alors appliquer les théorèmes IV.2 et IV.3 : on aura

$$|\tilde{\mathcal{H}}/\mathcal{H}| = l^{l-1-r'} = l^{1-r'}$$

où r' est le rang du système associé au groupe :

$$\Lambda = \langle p_1, p_2, p^q \rangle;$$

or l'hypothèse faite sur p entraîne $r' = 1$ soit $\tilde{\mathcal{H}} = \mathcal{H}$; il en résulte alors que $\mathcal{H}(K) = \mathcal{H}$. Soit h la classe de p^q ; elle est différente de 1 sinon on aurait $\mathcal{H}(K) = \mathcal{H}_1$ (ce qui est contraire à l'hypothèse); par conséquent, un générateur h_1 de \mathcal{H}_1 est de la forme $h^{(\sigma^{-1})^\lambda}$ pour λ convenable et $\mathcal{H}(K)$ est bien le H-module engendré par h .

Le résultat (i) devient faux en général lorsque t est strictement plus grand que 2 :

Exemple VI.1. — Soit $l = 3$; considérons les 4 corps cubiques de discriminant $(7.163.271)^2$; la matrice du système linéaire associé au groupe $\Lambda = \langle 7, 163, 271 \rangle$ est de la forme :

$$\begin{pmatrix} \nu_2 + \nu_3 & 2\nu_1 & 2\nu_1 \\ 2\nu_2 & \nu_1 - \nu_3 & \nu_2 \\ 2\nu_3 & \nu_3 & \nu_1 - \nu_2 \end{pmatrix}$$

Pour $\nu_1 = 1, \nu_2 = \nu_3 = 2$ la matrice du système est $\begin{pmatrix} 1 & 2 & 2 \\ 1 & 2 & 2 \\ 1 & 2 & 2 \end{pmatrix}$

et est de rang 1 et le corps correspondant à un 3-rang égal à 3; on vérifie que dans tous les autres cas la matrice obtenue est de rang 2; les trois autres corps ont donc un 3-rang égal à 2.

On peut donner une classification des ensembles $\{p_1, \dots, p_t\}$ pour t donné, de la manière suivante :

DÉFINITION VI.3. — *Graphe associé à l'ensemble $\{p_1, \dots, p_t\}$.*

Le graphe associé à $\{p_1, \dots, p_t\}$ est constitué de t sommets S_1, \dots, S_t et des arêtes orientées $S_i \curvearrowright S_j$, où (i, j) , $i \neq j$, parcourt l'ensemble des couples pour lesquels $[p_i]_j = 1$ (Définition VI.2). Ce graphe est donc associé à l'ensemble des $(l - 1)^{t-1}$ extensions K/\mathbb{Q} de discriminant donné.

Lorsque t augmente le nombre de systèmes possibles, relativement à $\mathcal{H} = \mathcal{H}_1$ (i.e. $\Lambda_1 = \langle p_1, \dots, p_t \rangle$), est rapidement très grand (les $[p_i]_j$ pouvant prendre toutes valeurs) et l'étude du rang en fonction du t -uplet (ν_1, \dots, ν_t) complexe; l'étude du graphe associé semble simplifier la situation : nous donnons les résultats pour $l = 3, t = 2$ et 3 (la démonstration n'étant qu'une vérification fastidieuse). Posons $\delta = a_{12}a_{23}a_{31} - a_{13}a_{32}a_{21}$ (on rappelle que $[p_i]_j = \zeta_0^{a_{ij}}$).

PROPOSITION VI.5. — *a) Si $l = 3$ et $t = 2$ alors :*

(i) $R_1 = 2$ pour les deux corps si le graphe associé est :

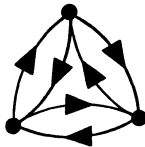


(ii) $R_1 = 1$ pour les deux corps si le graphe associé est :

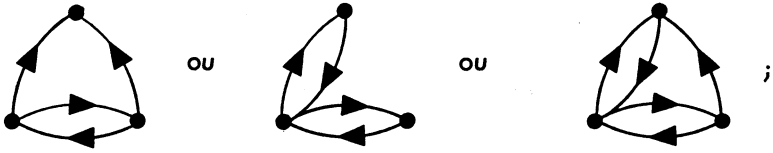


b) Si $l = 3$ et $t = 3$ alors :

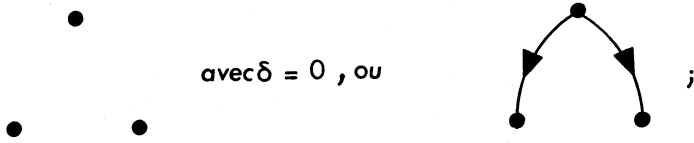
(i) $R_1 = 4$ pour les quatre corps si le graphe associé est :



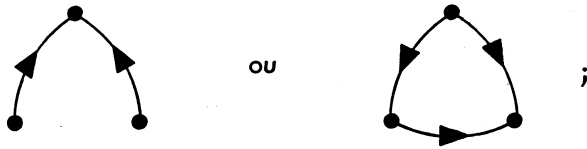
(ii) $R_1 = 3$ pour les quatre corps si le graphe associé est :



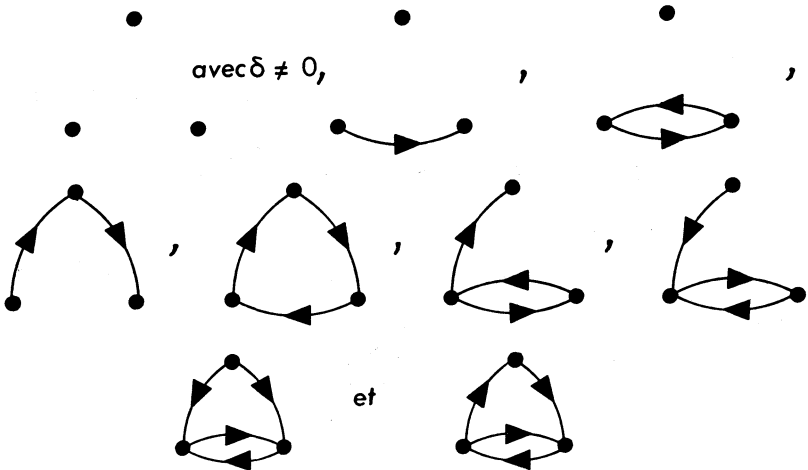
(iii) $R_1 = 3$ pour un corps et $R_1 = 2$ pour les trois autres si le graphe associé est :



(iv) $R_1 = 3$ pour deux corps et $R_1 = 2$ pour les deux autres si le graphe associé est



(v) $R_1 = 2$ pour les quatre corps dans les autres cas, i.e. pour les graphes suivants :



Remarque VI.3. — Pour $l = 3$ et $t = 3$ on peut donner un exemple des 17 situations possibles, à savoir (dans l'ordre des graphes ci-dessus) :

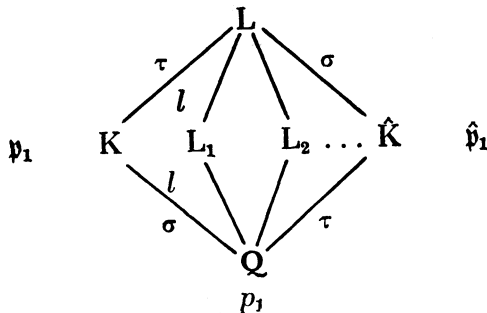
- (i) : (7, 181, 673);
- (ii) : (13, 103, 223); (7, 181, 463) et (7, 181, 223);
- (iii) : (7, 163, 271); (7, 13, 163);
- (iv) : (7, 13, 43); (7, 43, 97);
- (v) : (7, 31, 67); (7, 31, 37); (7, 37, 181); (7, 13, 31); (7, 13, 73); (7, 73, 181), (7, 43, 181), (7, 13, 223); (7, 19, 181).

4. *Étude du cas $t = 2$.*

Considérons le cas l impair et $t = 2$. Soient p_1, p_2 les nombres premiers ramifiés dans les $l - 1$ extensions K_i cycliques de degré l de \mathbf{Q} de discriminant commun. On suppose qu'il y a des classes exceptionnelles; donc, d'après les propositions VI.3 et VI.4 on a $|\mathcal{H}_2| = l^2$ pour les $l - 1$ corps K_i et les symboles $[p_1]_{p_1}$ et $[p_2]_{p_1}$ sont égaux à 1.

PROPOSITION VI.6. — *Soit K l'un des corps K_i . On suppose que pour ce corps $|\mathcal{H}_3/\mathcal{H}_2| = l$. Alors il en est de même pour les $l - 2$ autres corps K_i distincts de K .*

Démonstration. — Soit \hat{K} l'un des $l - 2$ corps K_i distincts de K et soit L le composé de K et \hat{K} ; alors L contient les $l - 1$ corps K_i ainsi que le corps L_1 (resp. L_2) qui est l'extension cyclique de degré l de \mathbf{Q} dans laquelle p_1 (resp. p_2) est le seul nombre premier ramifié. Soit \mathfrak{p}_1 (resp. $\hat{\mathfrak{p}}_1$) l'idéal premier au-dessus de p_1 dans K (resp. \hat{K}).



On note enfin par σ (resp. τ) un générateur de $\text{Gal}(L/\hat{K})$ (resp. $\text{Gal}(L/K)$).

Dans ce cas, on a $\Lambda_1 = \hat{\Lambda}_1 = \langle p_1, p_2 \rangle$ et p_1 et p_2 sont normes dans K et \hat{K} (classes exceptionnelles dans les deux corps). On résout alors les équations $\hat{\alpha}_i A_{\hat{K}} = \hat{p}_i \hat{\mathfrak{A}}_i^{\sigma-1}$ ($i = 1, 2$), $\hat{\alpha}_i \in \hat{K}$, et on doit démontrer que les $\hat{\alpha}_i$ (normes des $\hat{\mathfrak{A}}_i$) sont aussi normes dans \hat{K}/\mathcal{Q} . Il suffit de le faire pour $i = 1$ par exemple.

LEMME 1. — (i) *Les extensions L/K et L/\hat{K} sont non ramifiées.*

(ii) \mathfrak{p}_1 (resp. $\hat{\mathfrak{p}}_1$) *est décomposé dans L/K (resp. L/\hat{K}).*

Le (i) est trivial et le (ii) résulte du fait que $[p_1]_{\mathfrak{p}_1} = 1$, donc que p_1 est décomposé dans L_2 .

Soit $\alpha \in K$ de norme p_1 , alors $\alpha A_K = \mathfrak{p}_1 \mathfrak{A}^{\sigma-1}$ et on peut supposer que \mathfrak{A} est un idéal premier de K (remarque IV.7) :

$$\alpha A_K = \mathfrak{p}_1 q_1^{\sigma-1}$$

D'après les hypothèses faites $q_1 = Nq_1$ est norme d'un élément de K , donc les symboles $[q_1]_{\mathfrak{p}_1}$ et $[q_1]_{\mathfrak{p}_2}$ sont égaux à 1 (c'est-à-dire que q_1 est totalement décomposé dans L/\mathcal{Q}).

LEMME 2. — *Le nombre α est norme dans L/K .*

Il suffit de le vérifier localement. Soit \mathfrak{p} un idéal premier dans K . Le cas \mathfrak{p} décomposé dans L/K étant trivial, on peut supposer \mathfrak{p} inerte dans L/K et figurant dans la décomposition de αA_K (sinon α est une unité en \mathfrak{p} donc norme, car L/K est non ramifiée); nécessairement $\mathfrak{p} = q_1$ (ou q_1^σ), or ceci est absurde car q_1 est totalement décomposé dans L/\mathcal{Q} .

On pose $\alpha = N_{L/K}\varphi$, $\varphi \in L$. Soit \mathfrak{P} un idéal premier au-dessus de \mathfrak{p}_1 dans L ; on a $N_{L/\mathcal{Q}}\varphi = p_1$ donc $\varphi A_L = \mathfrak{P}\mathfrak{A}_1$ avec $N_{L/\mathcal{Q}}\mathfrak{A}_1 = \mathbf{Z}$; il en résulte facilement que \mathfrak{A}_1 est de la forme $\mathfrak{A}_1 = \mathfrak{A}^{\sigma-1}\hat{\mathfrak{A}}^{\tau-1}$ (car $\hat{H}_0(\text{Gal}(L/\mathcal{Q}), \mathcal{J}(L)) = \{1\}$ et $\mathfrak{A}_1 \in \mathcal{J}(L)^I$ où I est l'idéal d'augmentation de

$$\mathbf{Z}[\text{Gal}(L/\mathcal{Q})]$$

(cf. [31] chap. VIII)), \mathfrak{A} et $\hat{\mathfrak{A}}$ idéaux de L . Soit $\hat{\mathfrak{S}}$ un idéal premier de L équivalent à $\hat{\mathfrak{A}}$: $\hat{\mathfrak{A}} = \hat{\mathfrak{S}}(\hat{\gamma})$, $\hat{\gamma} \in L$; on a

$$N_{L/\hat{K}}(\varphi \hat{\gamma}^{1-\tau} A_L) = \hat{p}_1(N_{L/\hat{K}} \hat{\mathfrak{S}})^{\tau-1}$$

soit $\hat{\alpha} A_{\hat{K}} = \hat{p}_1 \hat{\alpha}^{\hat{\gamma}^{\tau-1}}$ où $\hat{\alpha}^{\hat{\gamma}} = N_{L/\hat{K}} \hat{\mathfrak{S}}$ et où $\hat{\alpha} = N_{L/\hat{K}}(\varphi \hat{\gamma}^{1-\tau})$. La proposition sera démontrée si on montre que $\hat{\alpha}^{\hat{\gamma}^{\hat{f}}} = N_{\hat{K}/\mathbb{Q}} \hat{\alpha}^{\hat{\gamma}^{\hat{f}}}$ est norme d'un élément de \hat{K} (car $N_{\hat{K}/\mathbb{Q}}(\hat{\alpha}) = p_1$):

Si $\hat{\alpha}$ est inerte dans L/\hat{K} , $\hat{f} = l$ et $\hat{\alpha}^{\hat{\gamma}^{\hat{f}}} \in N(\hat{K})$. Si $\hat{\alpha}$ est inerte ou ramifié dans \hat{K}/\mathbb{Q} alors $\hat{\alpha}^{\tau-1} = A_{\hat{K}}$. Supposons $\hat{\alpha}$ totalement décomposé dans L/\mathbb{Q} . Alors $\hat{\alpha}$ est décomposé dans L_1 et dans L_2 , donc les symboles $[\hat{\alpha}]_{p_i}$ et $[\hat{\alpha}]_{p_i}$ valent 1 et $\hat{\alpha}$ est norme dans \hat{K}/\mathbb{Q} .

COROLLAIRE VI.3. — *Lorsque $l = 3$ (et $t = 2$) il y a deux corps K_i et l'un admet une classe d'ordre 9 si et seulement si l'autre a la même propriété.*

Voir à ce sujet la table 3 en annexe et aussi l'exemple VI.7.

5. *La relation de dépendance des classes invariantes ($l > 2$).*


On sait que les classes invariantes sont représentées par les idéaux premiers ramifiés p_1, \dots, p_t dans K/\mathbb{Q} et que, d'après le théorème IV.1, il existe une relation:

$$(1) \quad p_1^{x_1^0} \dots p_t^{x_t^0} = (\alpha) A_K,$$

x_i^0 non tous congrus à 0 modulo l , (x_1^0, \dots, x_t^0) unique à multiplication près par $\lambda \not\equiv 0$ modulo l .

On a donc $N\alpha = \prod_{i=1}^t p_i^{x_i^0}$ et par conséquent le système (S): $\prod_{i=1}^t (\alpha, p_i)_{p_j}^{x_i^0} = 1, 1 \leq j \leq t$ (associé à $\Lambda_1 = \langle p_1, \dots, p_t \rangle$), dont le rang est $r_1 \leq t - 1$, admet la solution (x_1^0, \dots, x_t^0) . En particulier, si $r_1 = t - 1$, le système donne la relation de dépendance en question. Si $r_1 < t - 1$, le système ci-dessus est insuffisant; il faut utiliser des méthodes plus directes par exemple comme celle de [13] qui illustre en fait le « théorème 92 » de Hilbert [17]: partant d'une unité quelconque

l'un au plus des corps associés peut admettre une base d'entiers $\{1, \theta, \dots, \theta^{l-1}\}$,

(ii) *si le graphe associé est*  *alors aucun des* $l - 1$ *corps n'admet une base* $\{1, \theta, \dots, \theta^{l-1}\}$.

La matrice associée est :

$$A = \begin{pmatrix} -a_{12}\nu_2 & a_{21}\nu_1 \\ a_{12}\nu_2 & -a_{21}\nu_1 \end{pmatrix};$$


dans le cas (i) on a $a_{12} \neq 0$ et $a_{21} \neq 0$; par conséquent $(1, 1^*)$ est solution si et seulement si

$$a_{12}\nu_2 = a_{21}\nu_1 \cdot 1^*,$$


soit $\nu_2 = \frac{a_{21}}{a_{12}} \nu_1 \cdot 1^*$, ce qui se produit pour un corps et un seul.


Dans le cas (ii) on a, par exemple, $a_{21} = 0$ et $a_{12} \neq 0$, soit $A = \begin{pmatrix} -a_{12}\nu_2 & 0 \\ a_{12}\nu_2 & 0 \end{pmatrix}$ et $(1, 1^*)$ ne peut être solution du système homogène associé.


Exemples ($l = 3$) (pour la définition de « a et b » se reporter à la proposition VI.8, partie B).


(i) $\{3, 7\}$ (graphe : ); un corps et un seul admet une base $\{1, \theta, \theta^2\}$ ($a = 3, b = 1$ pour ce corps, $a = 4, b = 2$ pour l'autre),

(ii) $\{3, 13\}$ (graphe : ); aucun corps n'admet de base $\{1, \theta, \theta^2\}$,

(iii) $\{3, 19\}$ (graphe : );

(iv) $\{3, 307\}$ (graphe : ); les deux corps admettent une base $\{1, \theta, \theta^2\}$: pour le corps défini par $a = 35, b = 1$ c'est évident (θ racine de $X^3 - 3.307 X - 307.35$) pour le corps défini par $a = 19, b = 17$ on prend θ racine du polynôme $X^3 - 7.3.307 X - 649.307$ (cf. [13]),

(v) $\{3, 73\}$ (graphe : ); l'un des corps est défini par $a = 17, b = 1$ (d'où une base $\{1, \theta, \theta^2\}$) et l'autre par $a = 10, b = 8$ (il est bien connu que lorsque a et b sont pairs, il n'y a pas de bases $\{1, \theta, \theta^2\}$),

(vi) $\{3, 271\}$ (graphe : ); pour un corps on a $a = 28, b = 10$ (donc pas de base $\{1, \theta, \theta^2\}$) et pour l'autre, $a = 1, b = 19$; le polynôme $X^3 - 3.271 X - 271$ montre que \mathfrak{p}_{271} est principal, donc il n'y a pas de base $\{1, \theta, \theta^2\}$.

Remarquons enfin que pour $t > 2$ une étude systématique conduirait à des énoncés plus compliqués mais du même type que celui du corollaire VI.5.

Lorsque $(1, \dots, 1, 1^*)$ est solution, il n'y a pas nécessairement de base d'entiers $\{1, \theta, \dots, \theta^{l-1}\}$; une condition nécessaire et suffisante permettant un test effectif pratique semble ne pas exister vu que dans [13] il est démontré un critère pour $l = 3$ portant sur des équations diophantiennes du 3^e degré, à savoir :

“(i) soit \mathfrak{f} un conducteur d'extension cubique cyclique de \mathbf{Q} ; si \mathfrak{f} est de la forme

$$\mathfrak{f} = \frac{\alpha^2 + 27}{4\gamma^3} \quad \text{ou} \quad \mathfrak{f} = \frac{27\alpha^2 + 1}{4\gamma^3},$$

α et $\gamma \in \mathbf{Z}$ premiers entre eux, il existe un corps $K(\alpha, \gamma, \mathfrak{f})$ de conducteur \mathfrak{f} admettant une base d'entiers $\{1, \theta, \theta^2\}$.

(ii) Toutes les extensions cubiques cycliques admettant une base d'entiers $\{1, \theta, \theta^2\}$ sont de la forme $K(\alpha, \gamma, \mathfrak{f})$ ”.

B. Algorithmes et illustrations.

1. Algorithme pour $l = 2$ (cf. [30] et [32]).

Soit m un entier sans facteurs carrés et soient p_1, \dots, p_t les nombres premiers ramifiés dans $K = \mathbf{Q}(\sqrt{m})$. La détermination de $\mathcal{H}(K)$ se ramène à la détermination de deux suites croissantes \mathcal{J}_i et $\Lambda_i, i \geq 1$, vérifiant les hypothèses des théorèmes IV.2 et IV.3.

On peut supposer que \mathcal{J}_i est engendré par des idéaux premiers de degré 1 pour tout i (cf. remarque IV.7).

Dans la pratique, il suffit de connaître

$$\Lambda_{t-1} = \langle p_1, \dots, p_t, q_1, \dots, q_n \rangle$$

car \mathcal{J}_{i-1} s'en déduit sans ambiguïté. Les nombres q_j se déterminent alors de la façon suivante :

LEMME VI.2. — Soit $\Lambda_{i-1} = \langle p_1, \dots, p_t, q_1, \dots, q_n \rangle$. Soit $\{1, \theta\}$ une \mathbf{Z} -base de A_K ($\theta = \sqrt{m}$ si $m \equiv 2$ ou $3 \pmod{4}$, $\theta = \frac{1 + \sqrt{m}}{2}$ sinon).

Pour a parcourant un ensemble de solutions indépendantes du système « $a \in \Lambda_{i-1} \cap NK^*$ », on résout l'équation :

$$az^2 = N(x + y\theta), \quad x, y, z \in \mathbf{Z}, \quad (z, x, y) = 1,$$

avec $z = 1$ ou z premier; Λ_i est alors obtenu par adjonction à Λ_{i-1} des solutions z qui sont des nombres premiers.

En effet, si $a = N(x + y\theta)$ (en supposant a sans facteurs carrés), $x, y \in \mathbf{Z}$, c'est qu'il existe un idéal $\mathfrak{A} \in \mathcal{J}_{i-1}$ de norme a qui est principal; l'idéal \mathfrak{A}' correspondant est par exemple A_K . S'il existe p_0 premier tel que

$$ap_0^2 = N(x + y\theta), \quad (p_0, x, y) = 1$$

c'est que $(x + y\theta)A_K$ est de la forme $\mathfrak{A}p_0^2$ avec $\mathfrak{A} \in \mathcal{J}$ et $N\mathfrak{A} = aZ$; d'où $\left(\frac{x + y\theta}{p_0}\right)A_K = \mathfrak{A}p_0^{1-\sigma}$ et en posant $\alpha = \frac{x + y\theta}{p_0}$ on obtient la solution $\mathfrak{A}' = \mathfrak{p}_0$, d'où le lemme.

Remarque VI.4. — Il est clair que les groupes \mathcal{J}_i satisfont à la condition $\mathcal{J} \cap \mathcal{J}(K)^{\sigma-1} = \mathcal{J}^{\sigma-1}$. L'hypothèse \mathcal{J} engendré par des idéaux premiers n'étant pas nécessaire pour un exemple traité « à la main » (il faut alors vérifier à chaque pas l'hypothèse $\mathcal{J}(K)^{\sigma-1} \cap \mathcal{J} = \mathcal{J}^{\sigma-1}$, elle est par contre indispensable pour un calcul systématique (sur ordinateur).

Remarque VI.5. — L'algorithme ci-dessus est valable pour l quelconque sans changement (sauf en ce qui concerne l'expression de la norme).

Exemple VI.2. — Soit $K = \mathbf{Q}(\sqrt{-146})$. On aura $\mathcal{J}_1 = \langle \mathfrak{p}_2, \mathfrak{p}_{73} \rangle$ et $\Lambda_1 = \langle 2, 73 \rangle$ dont la matrice associée est $A_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$; d'où $|\mathcal{H}_2/\mathcal{H}_1| = 2$.

Comme $\mathfrak{p}_2\mathfrak{p}_{73}$ est principal il suffit de résoudre l'équation $2z^2 = x^2 + 146y^2$ dont une solution est $x = 4$, $y = 1$ et $z = 9$; on a :

$$\mathcal{I}_2 = \langle \mathfrak{p}_2, \mathfrak{p}_{73}, \mathfrak{p}_3^2, \mathfrak{p}_3^{2\sigma} \rangle \quad \text{et} \quad \Lambda_2 = \langle 2, 73, 3^2 \rangle$$

et évidemment $A_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$; ainsi $|\mathcal{H}_3/\mathcal{H}_2| = 2$.

On écrit $9 = N(3) = N(\mathfrak{p}_3^2)$ qui conduit à $(3) = \mathfrak{p}_3^2\mathfrak{A}'^{\sigma-1}$ avec $\mathfrak{A}' = \mathfrak{p}_3$, d'où :

$$\mathcal{I}_3 = \langle \mathfrak{p}_2, \mathfrak{p}_{73}, \mathfrak{p}_3, \mathfrak{p}_3^\sigma \rangle \quad \text{et} \quad \Lambda_3 = \langle 2, 73, 3 \rangle;$$

$A_3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$, car 3 est un carré modulo 73, et $|\mathcal{H}_4/\mathcal{H}_3| = 2$. On trouve alors $3 \cdot 7^2 = 1^2 + 146 \cdot 1^2$ soit :

$$\mathcal{I}_4 = \langle \mathfrak{p}_2, \mathfrak{p}_{73}, \mathfrak{p}_3, \mathfrak{p}_3^\sigma, \mathfrak{p}_7, \mathfrak{p}_7^\sigma \rangle \quad \text{et} \quad \Lambda_4 = \langle 2, 73, 3, 7 \rangle.$$

Cette fois $\left(\frac{7}{73}\right) = -1$ ainsi A_4 est de rang 1 et

$$\mathcal{H}_5 = \mathcal{H}_4 = \mathcal{H}(K) \quad \text{et} \quad \mathcal{H}(K)$$

est cyclique d'ordre 16.

Exemple VI.3. — Soit $K = \mathbf{Q}(\sqrt{226})$. On aura

$$\mathcal{I}_1 = \langle \mathfrak{p}_2, \mathfrak{p}_{113} \rangle \quad \text{et} \quad \Lambda_1 = \langle 2, 113 \rangle;$$

on vérifie que $A_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$; -1 étant norme et $N(\sqrt{226})$ étant égal à -226 il suffit de résoudre l'équation :

$$2z^2 = x^2 - 226y^2;$$

on trouve $(z, x, y) = (9, 7, 1)$ soit :

$$\mathcal{I}_2 = \langle \mathfrak{p}_2, \mathfrak{p}_{113}, \mathfrak{p}_3^2, \mathfrak{p}_3^{2\sigma} \rangle, \quad \Lambda_2 = \langle 2, 113, 3^2 \rangle,$$

$A_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, finalement :

$$\mathcal{I}_3 = \langle \mathfrak{p}_2, \mathfrak{p}_{113}, \mathfrak{p}_3, \mathfrak{p}_3^\sigma \rangle \quad \text{et} \quad \Lambda_3 = \langle 2, 113, 3 \rangle.$$

On vérifie que $\left(\frac{3}{113}\right) = -1$, c'est-à-dire que $\mathcal{H}(K) = \mathcal{H}_3$ est cyclique d'ordre 8.

Remarque VI.6. — Il existe d'autres algorithmes pour la détermination des 2-classes d'idéaux d'un corps quadratique (sans calcul préalable du nombre de classes du corps) : principalement celui de Shanks [32]. Celui que nous venons de définir donne, sans calculs supplémentaires, la structure du 2-groupe des classes (on peut considérer que c'est pratiquement celui de Shanks (qui est issu de la théorie des formes quadratiques) transposé dans le langage des classes d'idéaux).

2. Étude du cas $l = 3$.

La remarque VI.2 montre que le 3-rang d'une extension cubique cyclique de \mathbf{Q} est :

$$R_1 = 2(t - 1) - r_1,$$

où r_1 est le rang du système linéaire attaché au groupe

$$\Lambda_1 = \langle p_1, \dots, p_t \rangle.$$

Nous donnons en annexe les tables des corps cubiques cycliques pour lesquels $R_1 = 2(t - 1)$, avec $t = 2, 3$, et 4, $p_i < 10\,000$ pour $1 \leq i \leq t$.

Rappelons la construction des extensions cubiques cycliques de \mathbf{Q} de discriminant donné :

Les résultats du chapitre III montrent que si p_1, \dots, p_t sont les nombres premiers ramifiés dans K/\mathbf{Q} et distincts de $l = 3$, un nombre α vérifiant $q(\alpha) \in \mathfrak{K}^*$ sera de la forme

$$\alpha = \beta D \quad \text{avec} \quad D = p_1 \cdot p_2 \dots p_t,$$

où β est, dans $\mathbf{Q}' = \mathbf{Q}(j)$, un entier de norme D .

On peut écrire $\beta = \frac{a' + b' \sqrt{-3}}{2}$ (a', b' entiers de même parité) avec $a' \equiv -1 \pmod{3}$ (afin d'avoir

$$\alpha \equiv 1 \pmod{\mathfrak{P}_0 = (1 - j)}.$$

Si 3 est non ramifié il faut éventuellement multiplier β

par j ou j^2 de telle manière que α vérifie :

$$\alpha \equiv 1 \pmod{(1-j)^3} \quad (\text{Proposition VI.4}).$$

Dans ce cas, on a $\beta \equiv 1 \pmod{3}$ soit $\beta = \frac{a + 3b\sqrt{-3}}{2}$ et $D = \frac{a^2 + 27b^2}{4}$.

Si 3 est ramifié, on aura au contraire $\beta = \frac{a + b\sqrt{-3}}{2}$ avec $a \equiv -1 \pmod{3}$ et $b \not\equiv 0 \pmod{3}$ et $D = \frac{a^2 + 3b^2}{4}$.

Soit alors $\theta = \sqrt[3]{\alpha}$; on a $K' = \mathbf{Q}'(\theta)$ et on vérifie que $\text{Tr}_{K'/K}(\theta)$ est un élément primitif dans l'extension K/\mathbf{Q} . Son polynôme irréductible est alors [10] :

$$X^3 - 3DX - aD.$$

Résumons la situation dans la proposition suivante :

PROPOSITION VI.8. — Soient $p_1, \dots, p_t, p_i \equiv 1 \pmod{3}$ si $p_i \neq 3$; les 2^{t-1} extensions cubiques cycliques de \mathbf{Q} admettant les p_i comme nombres premiers ramifiés, sont définies par les polynômes suivants :

$$X^3 - 3DX - aD, \quad D = p_1 \dots p_t = \frac{a^2 + 27b^2}{4}$$

si 3 est non ramifié dans l'extension (ou encore $X^3 - DX - bD$);

$$X^3 - 3DX - aD, \quad D = p_1 \dots p_t = \frac{a^2 + 3b^2}{4},$$

b non divisible par 3, lorsque $p_i = 3$ est ramifié.

Remarque VI.7. — Le cas $l = 5$ peut se traiter d'une manière analogue en ce qui concerne la recherche d'un polynôme (cf. [10], p. 182).

Exemple VI.4. — Corps cubiques de discriminant $(7.181)^2$.

(i) Corps défini par le polynôme : $X^3 - 3.7.181X - 71.7.181$. Soit θ une racine de ce polynôme; le nombre

$$\alpha = 181 + \theta + 5\theta^2$$

est de norme 181.17^3 et son polynôme irréductible est :

$$X^3 - 3.181X^2 + 181.6.17X - 181.17^3;$$

il en résulte $\alpha A_K = \mathfrak{p}_{181}\mathfrak{p}_{17}\mathfrak{p}_{17}^{2\sigma}(\mathfrak{p}_{181}^3 = 181Z, N\mathfrak{p}_{17} = 17Z)$ et $\left(\frac{\alpha}{17}\right) A_K = \mathfrak{p}_{181}\mathfrak{p}_{17}^{\sigma(1-\sigma)}$. Par conséquent, le groupe \mathcal{J}_2 contiendra $\mathfrak{p}_{181}, \mathfrak{p}_7$ et \mathfrak{p}_{17} et Λ_2 contiendra 181, 7 et 17; or 17 n'est pas reste cubique modulo 7 et ceci suffit pour pouvoir affirmer que $r_2 = 1$ et donc que $|\mathcal{H}_3/\mathcal{H}_2| = 1$ ($\mathcal{H}(K)$ est donc isomorphe à $(Z/3Z)^2$).

(ii) Corps défini par le polynôme

$$X^3 - 3.7.181X - 64.7.181.$$

On trouve un entier α dont le polynôme irréductible est :

$$X^3 - 49X^2 - 308.7X + 7.(24)^3;$$

on vérifie que $\alpha A_K = \mathfrak{p}_7\mathfrak{p}_2^2\mathfrak{p}_3^{7\sigma}$ et par un raisonnement analogue au précédent on montre que $r_2 = 1$.

Exemple VI.5. — Corps cubiques de discriminant $(7.673)^2$.

(i) Corps défini par le polynôme $X^3 - 37.673X - 113.7.673$.

Si θ est une racine de ce polynôme, les nombres $\alpha_1 = \frac{13.7 + \theta}{3}$ et $\alpha_2 = \frac{673 + 5\theta + 5\theta'}{3}$ sont des entiers dont les polynômes irréductibles sont respectivement :

$$X^3 - 13.7X^2 + 170.7X - 7$$

et

$$X^3 - 673X^2 + 66.673X - 3^3.673.$$

On a $\alpha_1 A_K = \mathfrak{p}_7$ et $\alpha_2 A_K = \mathfrak{p}_{673}\mathfrak{p}_3^3$ et les idéaux $\alpha_1 A_K$ et $\left(\frac{\alpha_2}{3}\right) A_K$ sont de la forme :

$$\alpha_1 A_K = \mathfrak{p}_7 A_K^{\sigma-1}, \quad \frac{\alpha_2}{3} A_K = \mathfrak{p}_{673}(\mathfrak{p}_3^{2+\sigma})^{1-\sigma}$$

On peut donc écrire $\mathcal{J}_2 = \langle \mathfrak{p}_7, \mathfrak{p}_{673}, \mathfrak{p}_3^{2+\sigma}, \mathfrak{p}_3^{\sigma(2+\sigma)}, \mathfrak{p}_3^{\sigma^2(2+\sigma)} \rangle$ et $\Lambda_2 = \langle 7, 673, 3^3 \rangle$; le rang r_2 est alors nul et $|\mathcal{H}_3/\mathcal{H}_2| = 3$.

Écrivons maintenant que 3^3 est norme :

$$3^3\mathbf{Z} = \mathbf{N}(3) = \mathbf{N}(\mathfrak{p}_3^{2+\sigma})$$

soit $3A_{\mathbf{K}} = \mathfrak{p}_3^{2+\sigma}\mathfrak{p}_3^{(\sigma+1)(\sigma-1)}$; d'où

$$\mathcal{I}_3 = \langle \mathfrak{p}_7, \mathfrak{p}_{673}, \mathfrak{p}_3^{\sigma+2}, \dots, \mathfrak{p}_3^{\sigma+1}, \dots \rangle = \langle \mathfrak{p}_7, \mathfrak{p}_{673}, \mathfrak{p}_3, \mathfrak{p}_3^\sigma, \mathfrak{p}_3^{\sigma^2} \rangle$$

et $\Lambda_3 = \langle 7, 673, 3 \rangle$; 3 n'étant pas reste cubique modulo 7 il en résulte $r_3 = 1$ et $|\mathcal{H}_4/\mathcal{H}_3| = 1$. On obtient que $|\mathcal{H}(\mathbf{K})| = 27$ et que $\mathcal{H}(\mathbf{K})$ est isomorphe à $(\mathbf{Z}/9\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z})$ (cf. corollaire IV.3).

Utilisons l'assertion (ii) de la proposition VI.4; le nombre premier 3 est décomposé dans \mathbf{K}/\mathbf{Q} et le symbole $[3]_7$ est différent de 1: $\mathcal{H}(\mathbf{K})$ est engendré par $h = \text{Cl}(\mathfrak{p}_3)$ et on a la relation :

$$h^3 = \text{Cl}(\mathfrak{p}_{673})^2, \quad \text{avec} \quad \text{Cl}(\mathfrak{p}_{673}) \neq 1$$

puisque \mathfrak{p}_7 est principal.

(ii) Corps défini par le polynôme

$$X^3 - 3.7.673X - 76.7.673.$$

Considérons les nombres :

$$\alpha_1 = 12.7 + 8\theta + 3\theta' \quad \text{et} \quad \alpha_2 = \frac{673 + 6\theta + 2\theta'}{3}$$

dont les polynômes irréductibles sont :

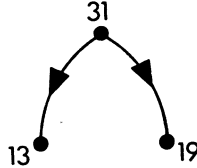
$$\begin{aligned} & X^3 - 36.7X^2 - 3.7^2.4567X + 7.(73.4)^3 \\ \text{et} & X^3 - 673X^2 - 673.3.53X + 673; \end{aligned}$$

ce qui donne :

$$(\alpha_1)A_{\mathbf{K}} = \mathfrak{p}_7\mathfrak{p}_{73}^3\mathfrak{p}_2^6 \quad \text{et} \quad (\alpha_2)A_{\mathbf{K}} = \mathfrak{p}_{673}.$$

On a $\left(\frac{\alpha_1}{4.73}\right)A_{\mathbf{K}} = \mathfrak{p}_7\mathfrak{p}_{73}^{(1-\sigma)(2+\sigma)}\mathfrak{p}_2^{2(1-\sigma)(2+\sigma)}$ et $(\alpha_2)A_{\mathbf{K}} = \mathfrak{p}_{673}A_{\mathbf{K}}^{1-\sigma}$, d'où: $\mathcal{I}_2 = \langle \mathfrak{p}_7, \mathfrak{p}_{673}, (\mathfrak{p}_2^2\mathfrak{p}_{73})^{2+\sigma}, \dots \rangle$ et $\Lambda_2 = \langle 7, 673, 292^3 \rangle$; r_2 est nul et $|\mathcal{H}_3/\mathcal{H}_2| = 3$; alors $\mathcal{I}_3 = \langle \mathfrak{p}_7, \mathfrak{p}_{673}, \mathfrak{p}_2^2\mathfrak{p}_{73}, \dots \rangle$ et $\Lambda_3 = \langle 7, 673, 292 \rangle$; on vérifie que 292 n'est pas reste cubique modulo 7, donc $r_3 = 1$ et $|\mathcal{H}(\mathbf{K})| = 27$ comme dans le cas (i) (la structure étant la même).

Exemple VI.6. — Considérons les 4 corps cubiques de discriminant $(13.19.31)^2$; le graphe associé (Définition VI.3) est le suivant :



donc d'après la proposition VI.5, pour 3 des corps on aura $R_1 = 2$ (c'est-à-dire que $|\mathcal{H}(K)| = |\mathcal{H}_1| = 9$) et pour le dernier on aura $R_1 = 3$. On vérifie facilement que c'est pour le corps K défini par $a = 170$, $b = 8$ $\left(\frac{a^2 + 27b^2}{4} = 13.19.31$, cf. Proposition VI.8) donc par le polynôme $X^3 - 13.19.31X - 8.13.19.31$; le triplet (ν_1, ν_2, ν_3) associé étant ici $(1, 1, 1)$ relativement au choix des idéaux premiers au-dessus de 13, 19 et 31 :

$$\mathcal{P}_{13} = (3 - j^2), \quad \mathcal{P}_{19} = (3 - 2j^2) \quad \text{et} \quad \mathcal{P}_{31} = (5 - j^2)$$

(cf. Définition VI.1) et pour

$$\beta = \frac{-170 + 24\sqrt{-3}}{2} = -73 + 24j = j(3 - j^2)(3 - 2j^2)(5 - j^2),$$

on trouve immédiatement $(\alpha = 13.19.31\beta)$:

$$\begin{array}{lll} (\alpha, 13)_{13} = j, & (\alpha, 13)_{19} = j, & (\alpha, 13)_{31} = j, \\ (\alpha, 19)_{13} = j^2, & (\alpha, 19)_{19} = j^2, & (\alpha, 19)_{31} = j^2, \\ (\alpha, 31)_{13} = 1, & (\alpha, 31)_{19} = 1, & (\alpha, 31)_{31} = 1, \\ (\alpha, 2)_{13} = j, & (\alpha, 2)_{19} = j^2, & (\alpha, 2)_{31} = 1; \end{array}$$

La matrice associée au groupe $\Lambda_1 = \langle 13, 19, 31 \rangle$ est donc

$$\begin{pmatrix} 1 & 2 & 0 \\ 1 & 2 & 0 \\ 1 & 2 & 0 \end{pmatrix}$$

de rang 1, comme prévu; on doit donc chercher α_1 et α_2 de K tels que $N\alpha_1 = 31$ et $N\alpha_2 = 13.19$; on montre que

le polynôme irréductible de $\varphi = \frac{1\,439 - 16\theta - 18\theta'}{3}$ où θ est une racine de $X^3 - 3DX - 170D$ ($D = 13.19.31$), est : $X^3 - 1\,439X^2 - 55\,041X - 1$ et qu'un entier α_3 tel que $\alpha_3^{\sigma-1} = \varphi$ (théorème 90 de Hilbert : $\alpha = 1 + \varphi + \varphi\varphi'$) est de norme $13^2.19^2.31$; on a donc la relation

$$p_{31}p_{13}^2p_{19}^2 \sim 1$$

et il suffit de considérer la solution $N\theta = 8.13.19.31$ obtenue à partir du polynôme $X^3 - DX - 8D$ (proposition VI.8) qui conduit à $\frac{\theta}{2} A_K = p_{13}p_{19}p_{31}p_2^{(1-\sigma)(2+\sigma)}$ et $Np_2^{2+\sigma} = 8$, d'où le groupe $\Lambda_2 = \langle 13, 19, 31, 8 \rangle$ qui montre que

$$|\mathcal{H}_3/\mathcal{H}_2| = 3.$$

Au stade suivant on aura évidemment $\Lambda_3 = \langle 13, 19, 31, 2 \rangle$, la matrice associée étant :

$$\begin{pmatrix} 1 & 2 & 0 & 1 \\ 1 & 2 & 0 & 2 \\ 1 & 2 & 0 & 0 \end{pmatrix};$$

son rang est 2, d'où $|\mathcal{H}_4/\mathcal{H}_3| = 1$. La proposition IV.2 entraîne que $\mathcal{H}(K) \simeq (\mathbf{Z}/9\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z})^2$.

Remarque VI.8. — L'exemple ci-dessus montre que l'on ne peut pas obtenir pour $t \geq 3$ un énoncé simple donnant la structure de $\mathcal{H}(K)$ (contrairement au cas $t = 2$, cf. corollaire IV.3); toutes les situations « intermédiaires » semblent être possibles.

Nous allons terminer par un exemple qui montre que la proposition VI.6 n'est pas généralisable en ce qui concerne la comparaison des groupes \mathcal{H}_i , $i > 3$, des corps ayant même discriminant (et avec $t = 2$):

Exemple VI.7. — On considère les deux corps cubiques de discriminant $(37.991)^2 = (36\,667)^2$. On vérifie facilement qu'il y a des classes exceptionnelles ($R_1 = 2$).

Soit K le corps défini par $a = 295$, $b = 47$ et soit \hat{K} le corps défini par $a = 376$, $b = 14$.

(i) *Étude de K.*

Si θ est une racine de $X^3 - 3DX - aD$, $D = 37.991$, on vérifie que :

$$\alpha_1 = \frac{1}{3} (37.8 + 6\theta + \theta^\sigma)$$

et
$$\alpha_2 = \frac{1}{3} (991.7 + 17\theta + 15\theta^\sigma)$$

ont respectivement pour polynômes irréductibles :

et
$$X^3 - 37.8X^2 - 37.13.727X - 37.5^6$$

$$X^3 - 991.7X^2 + 991.2^6.7.29X - 991(5.29)^3.$$

Il en résulte que $\alpha_1 A_K = \mathfrak{p}_{37} \mathfrak{p}_5^6$ et $\alpha_2 A_K = \mathfrak{p}_5^3 \mathfrak{p}_{29}^{2+\sigma}$; le groupe \mathcal{I}_2 sera donc égal à :

$$\mathcal{I}_2 = \langle \mathfrak{p}_{37}, \mathfrak{p}_{991}, \mathfrak{p}_5^{2(2+\sigma)}, \mathfrak{p}_5^{2+\sigma} \mathfrak{p}_{29}^{1+\sigma}, \dots \rangle = \langle \mathfrak{p}_{37}, \mathfrak{p}_{991}, \mathfrak{p}_5^{2+\sigma}, \mathfrak{p}_{29}, \dots \rangle$$

soit $\Lambda_2 = \langle 37, 991, 5^3, 29 \rangle$; 29 étant reste cubique modulo 37 et 991 il en résulte que $|\mathcal{H}_3/\mathcal{H}_2| = 3$.

Au stade suivant \mathcal{I}_3 contiendra \mathfrak{p}_5 et 5 n'étant pas reste cubique modulo 37 on aura $\mathcal{H}_4 = \mathcal{H}_3$ d'où

$$\mathcal{H}(K) \simeq \mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}.$$

(ii) *Étude de \hat{K} .*

On vérifie que l'entier ψ , de polynôme irréductible $X^3 + DX^2 + 13DX - D$, est un entier de \hat{K} ; il en résulte que $\mathfrak{p}_{37} \mathfrak{p}_{991}$ est principal, ce qui permet d'écrire :

$$\Lambda_1 = \langle \mathfrak{p}_{991} \rangle.$$

Soient θ et ϑ des racines des polynômes

et
$$X^3 - 3DX - aD \quad (a = 376)$$

$$X^3 - DX - bD \quad (b = 14),$$

on sait que l'on peut écrire :

$$\theta = \vartheta - \vartheta^\sigma$$

à condition de définir la conjugaison σ par l'expression

$$\vartheta^\sigma = -\frac{3}{a} \vartheta^2 + \frac{9b-a}{2a} \vartheta + \frac{2D}{a}.$$

On considère enfin l'entier φ défini par :

$$\varphi = \frac{1}{3} (11.991 + 42\theta + \theta^{\sigma^2})$$

dont le polynôme irréductible est :

$$X^3 - 11.991X^2 + 2^5 \cdot 3^2 \cdot 5 \cdot 13.991X - 991(2^2 \cdot 7^2)^3;$$

si on définit \mathfrak{p}_2 et \mathfrak{p}_7 par la relation

$$\mathfrak{p}A_K = \mathfrak{p}_2\mathfrak{p}_7,$$

on vérifie sans difficulté que :

$$\varphi A_K = \mathfrak{p}_{991}\mathfrak{p}_2^{3(\sigma+\sigma^2)}\mathfrak{p}_7^6,$$

et par conséquent, il existe un nombre φ' tel que

$$\varphi' A_K = \mathfrak{p}_{991}\mathfrak{p}_2^{3(\sigma+\sigma^2)-6} \quad \left(\text{on prend } \varphi' = \frac{\varphi}{9^6} \right).$$

On aura successivement :

$$\begin{aligned} \mathcal{I}_1 &= \langle \mathfrak{p}_{991} \rangle, & \Lambda_1 &= \langle 991 \rangle, \\ \mathcal{I}_2 &= \langle \mathfrak{p}_{991}, \mathfrak{p}_2^{3(2+\sigma)}, \dots \rangle, & \Lambda_2 &= \langle 991, 2^9 \rangle, \\ \mathcal{I}_3 &= \langle \mathfrak{p}_{991}, \mathfrak{p}_2^{3(2+\sigma)}, \mathfrak{p}_2^{3(1+\sigma)} \rangle = \langle \mathfrak{p}_{991}, \mathfrak{p}_2^3, \dots \rangle, & \Lambda_3 &= \langle 991, 2^3 \rangle, \\ \mathcal{I}_4 &= \langle \mathfrak{p}_{991}, \mathfrak{p}_2^{2+\sigma}, \mathfrak{p}_2^3, \dots \rangle \text{ qui est équivalent à} \\ & \langle \mathfrak{p}_{991}, \mathfrak{p}_2^{2+\sigma}, \mathfrak{p}_7^3, \dots \rangle, & \Lambda_4 &= \langle 991, 2^3, 7^3 \rangle. \end{aligned}$$

ceci afin de satisfaire à la condition :

$$\begin{aligned} \mathcal{I} \cap \mathcal{I}(\hat{K})^{\sigma-1} &= \mathcal{I}^{\sigma-1}; \\ \mathcal{I}_5 &= \langle \mathfrak{p}_{991}, \mathfrak{p}_2^{2+\sigma}, \mathfrak{p}_7^3, \mathfrak{p}_2^{1+\sigma}, \mathfrak{p}_7^{2+\sigma}, \dots \rangle \text{ équivalent à} \\ & \langle \mathfrak{p}_{991}, \mathfrak{p}_2, \dots \rangle \quad \text{soit} \quad \Lambda_5 = \langle 991, 2 \rangle. \end{aligned}$$

Or 2 n'est pas reste cubique modulo 37 donc $|\mathcal{H}_6/\mathcal{H}_5| = 1$ ce qui fait que la structure de $\mathcal{H}(\hat{K})$ est donnée par :

$$\mathcal{H}(\hat{K}) \simeq \mathbf{Z}/27\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z}.$$

TABLES NUMÉRIQUES

1. Table 1.

Table des corps cubiques définis par p_1 et $p_2 < 1\,000$ et pour lesquels $|\mathcal{H}_3| = 9$ (le 3-rang est donc maximum (= 2) et ceci a lieu pour les deux corps de même discriminant).

2. *Tables 2.*

Tables des corps de degré $l = 5$ et 7 pour lesquels $|\mathcal{H}_3| = l^2(p_1 \text{ et } p_2 < 1\,000)$.

3. *Table 3.*

Exemples de couples (p_1, p_2) figurant dans la table 1 précédente pour lesquels l'un des corps cubiques possède une classe d'ordre 9 (donc les deux d'après la proposition VI.6).

Nous définissons les corps par l'intermédiaire de a et b tels que $D = \frac{a^2 + 27b^2}{4} = p_1 \cdot p_2$. Pour p_1 , puis de la même manière pour p_2 , nous donnons les coefficients d'un polynôme irréductible d'un entier φ_i tel que $|N\varphi_i| = p_i n$, $|\text{Tr}(\varphi_i \varphi_i^\sigma)| = p_i s$ et $|\text{Tr} \varphi_i| = p_i t$. Les idéaux \mathfrak{A}_i sont définis par l'égalité

$$(\varphi_i)A_K = \mathfrak{p}_i \mathfrak{A}_i^{1-\sigma};$$

la conclusion sur la structure de $\mathcal{H}(K)$ s'en déduit dans presque tous les cas (la présence d'une * indique que $\mathcal{H}(K)$ contient au moins un sous-groupe de la forme indiquée).

4. *Table 4.*

Exemples de corps cubiques tels que $\mathcal{H}(K) \simeq \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ (pour $t = 2$).

5. *Table 5.*

Table des corps cubiques définis par p_1, p_2 et $p_3 < 1\,000$ et pour lesquels le 3-rang du groupe des classes est maximum (i.e. $R_1 = 4$). Ceci a alors lieu pour les 4 corps de même discriminant.

Signalons au passage que pour $p_i < 1\,000$, il existe un unique quadruplet : (3, 577, 757, 991), pour lequel les huit corps cubiques associés ont un 3-rang égal à 6.

TABLE 1

3, 73	619	283	619	643	829	883	643	829
271	829	337	631	733	283, 313	379, 409	823	859
307	883	349	661	199, 211	349	463	853	919
523	37, 103	409	769	313	499	541	997	643, 859
577	421	433	151, 211	397	619	601	523, 547	883
613	433	631	283	661	691	691	661	661, 727
757	487	673	331	733	307, 313	733	673	853
919	739	757	367	859	421	877	709	877
991	991	769	409	211, 307	499	937	739	673, 757
7, 181	43, 193	823	433	367	523	397, 523	757	769
223	409	859	547	223, 277	739	613	541, 739	787
337	457	877	607	283	919	631	757	997
421	613	97, 313	691	439	313, 349	907	853	691, 757
463	643	337	727	661	463	919	547, 619	823
673	61, 163	433	877	787	577	409, 523	571, 607	859
769	241	463	157, 337	859	607	571	661	907
811	277	601	373	919	331, 409	421, 499	709	937
853	313	997	379	229, 283	547	691	757	709, 727
883	487	103, 409	439	457	727	829	787	751
13, 103	613	439	487	241, 271	877	433, 571	859	727, 823
229	877	823	601	379	937	631	577, 619	919
421	907	919	727	457	337, 499	739	757	733, 859
499	67, 193	991	787	751	811	751	811	991
619	283	109, 199	877	787	349, 661	787	991	739, 967
853	349	373	883	829	709	439, 727	601, 811	751, 811
859	643	709	991	859	877	733	823	967
19, 151	661	997	163, 313	877	967	457, 673	607, 643	757, 907
277	937	127, 349	349	271, 487	367, 439	829	823	991
373	997	421	379	571	733	877	937	811, 919
487	73, 103	619	757	661	739	997	613, 643	823, 919
577	241	643	823	769	937	463, 547	811	877, 967
691	313	673	181, 331	823	373, 457	643	829	997
733	439	757	397	919	577	733	907	907, 919
31, 163	709	139, 199	673	967	613	487, 499	619, 643	919, 991
271	883	277	823	277, 397	769	499, 523	751	967, 991
349	79, 97	373	859	541	787	577	631, 661	997
373	157	601	193, 409	757				

TABLES 2

 $l = 5$

5, 251	991	941	751	631
601	41, 191	191, 941	941	601, 761
11, 241	571	211, 251	271, 571	641, 661
661	61, 761	811	991	701, 911
31, 191	131, 331	241, 701	331, 751	821, 881
211	571	251, 331	401, 421	941, 991

 $l = 7$

127, 449	197, 211	883	449, 827	673, 757
743	337, 673	379, 827	617, 953	757, 911

TABLE 3

$P_1 \cdot P_2$	a	b	n	s	t	\mathfrak{M}_1	n	s	t	\mathfrak{M}_2	$\%(\mathbb{K})$
7.673	413	15	1	2.5.17	13	(1)	3^3	2.83	1	$p_3^{2+\sigma}$	(9, 3)
7.769	76	22	$2^6 \cdot 7 \cdot 3^3$	3.7.4567	$2^2 \cdot 3^2$	$(p_2^2 p_3^2)^{2+\sigma}$	1	3.53	3	(1)	(9, 3)
37.991	92	22	2^6	677	$2^2 \cdot 5$	$p_2^{2(2+\sigma)}$	$2^6 \cdot 3 \cdot 13$	$2^2 \cdot 3^2 \cdot 31$	4	p_2^{2+31}	(9, 3)
67.643	43	27	3^3	2.41.19	17	$p_3^{2+\sigma}$	1	2	1	(1)	(9, 3)
73.241	376	14	$2^6 \cdot 13^3$	$2^2 \cdot 13 \cdot 3^4$	23	$p_2^2 p_3^{13}$	$2^6 \cdot 7^6$	$2^6 \cdot 3^2 \cdot 5 \cdot 13$	11	$p_2^{2+\sigma} p_3^{2(2+\sigma)}$	(27, 9)
79.349	295	47	5^6	43.727	2^3	$p_2^{2(2+\sigma)}$	$5^3 \cdot 29^3$	267.29	7	$p_2^{2+\sigma} p_3^9$	(9, 3)
79.409	343	45	$3^3 \cdot 5^3 \cdot 29^3$	$2^4 \cdot 3 \cdot 2029$	5	$p_3(p_2^2 p_3^9)^{2+\sigma}$	1733	$3^2 \cdot 19 \cdot 137$	$2^2 \cdot 3$	$p_2^{2+\sigma}$	(9, 3)
79.631	143	75	19^3	$2^8 \cdot 43 \cdot 3^2$	3.5	p_2^{10}	$5^3 \cdot 13^3$	$2^6 \cdot 3^3$	3	$(p_2^2 p_3^3)^{2+\sigma}$	(9, 3)
79.757	262	8	2^3	17	2	$p_2^{2+\sigma}$	1	17	1	(1)	(9, 3)
79.837	143	43	17^3	72.17	2.7	p_2^{17}	178	72.17	7	p_2^{17}	(9, 3)*
79.931	173	27	3^6	$3^4 \cdot 29$	41	$p_2^{2+\sigma}$	83^3	$3^2 \cdot 653$	$2^2 \cdot 3$	$p_2^{2+\sigma}$	(9, 3)
79.949	65	41	11^3	1201	2^2	$p_2^{2+\sigma}$	5^6	$3 \cdot 5^4$	2^2	$p_2^{2+\sigma}$	(9, 3)
79.973	328	40	$2^9 \cdot 5^6$	$2^3 \cdot 3541$	3.11	$p_2^{2(2+\sigma)}$	$2^{12} \cdot 19^3$	$2^8 \cdot 3 \cdot 5 \cdot 17 \cdot 31$	17	$p_2^{2+\sigma} p_3^{2+\sigma}$	(9, 3)*
79.991	331	27	$7^3 \cdot 23^3$	$2^3 \cdot 23 \cdot 23$	31	$p_2^{2(2+\sigma)}$	$7^3 \cdot 23^3$	12659	11	$p_2^{2+\sigma} p_3^{2+\sigma}$	(9, 3)*
79.999	196	58	2^{12}	$2^8 \cdot 37$	5	$p_2^{2+\sigma}$	2^{18}	$2^2 \cdot 5 \cdot 17$	1	$p_2^{2+\sigma}$	(9, 3)
79.999	433	21	7^6	$2^2 \cdot 5^2 \cdot 229$	1	$p_2^{2+\sigma}$	2^{18}	$2^2 \cdot 7^2 \cdot 13$	7	$p_2^{2+\sigma}$	(9, 3)
79.999	298	64	$2^9 \cdot 59^3$	$2 \cdot 59 \cdot 661$	3.5	$p_2^{2+\sigma} p_3^9$	$2^6 \cdot 19^3$	$2^4 \cdot 5^2 \cdot 37$	3^2	$p_2^{2+\sigma} p_3^{19}$	(9, 3)*
79.999	368	62	$2^6 \cdot 23^3$	$2^2 \cdot 23 \cdot 11 \cdot 37$	5	p_2^{2+23}	416	8069	1	$p_2^{2+\sigma}$	(9, 3)
79.999	125	91	61^3	$2^2 \cdot 3 \cdot 5^2 \cdot 11$	3^3	$p_2^{2+\sigma}$	$5^6 \cdot 13^3$	$3 \cdot 5^4 \cdot 19$	$2^2 \cdot 3$	$p_2^{2+\sigma} p_3^{13}$	(9, 3)*
79.999	142	64	1	3.139	1	(1)	2^6	$2^4 \cdot 5$	1	$p_2^{2+\sigma}$	(9, 3)
79.999	47	69	3^3	2.23	3	$p_2^{2+\sigma}$	$3^3 \cdot 29^3$	$2^2 \cdot 3 \cdot 29$	7	$p_2^3 p_3^9$	(9, 3)*
79.999	404	14	13^3	499	7	$p_2^{2+\sigma}$	$7^3 \cdot 31^3$	$11 \cdot 31 \cdot 67$	3.5	$p_2^{21} \cdot p_3^{2+\sigma}$	(9, 3)*
79.999	353	33	107^3	$2^3 \cdot 7 \cdot 13$	7	p_2^{13}	13^3	$2^3 \cdot 13$	1	p_2^{13}	(9, 3)*
79.999	245	59	5^3	$3^2 \cdot 7 \cdot 173$	$2^2 \cdot 3$	p_2^{107}	89^3	$2 \cdot 3 \cdot 11 \cdot 19 \cdot 53$	$3^2 \cdot 5$	p_2^{107}	(9, 3)
79.999	244	74	$2^8 \cdot 23^3$	$2 \cdot 4987$	17	$p_2^{2+\sigma}$	76	$3 \cdot 793$	2^3	$p_2^{2+\sigma}$	(9, 3)
79.999	55	87	$3^3 \cdot 5^6$	$2^5 \cdot 19 \cdot 23$	19	$p_2^{2+\sigma} p_3^{23}$	$2^6 \cdot 23^3$	$2^5 \cdot 13 \cdot 23$	13	$p_2^{2+\sigma} p_3^{23}$	(9, 3)*
79.999	343	73	$7^3 \cdot 23^3$	$13 \cdot 4157$	3.13	$p_2^{2+\sigma} p_3^{23}$	$7^3 \cdot 23^3$	61	1	$p_2^{2+\sigma} p_3^{23}$	(9, 3)*
79.999	305	79	67^3	$11^2 \cdot 23$	5	p_2^{67}	5^3	$2^2 \cdot 5 \cdot 67 \cdot 73$	3^3	p_2^{67}	(9, 3)*

TABLE 4

 $p_1 \leq 151, p_2 < 1\ 000.$

3, 73	13, 103	619	487	433	757
271	229	829	613	673	139, 199
307	421	883	877	769	601
523	499	37, 103	907	823	619
577	619	421	67, 193	859	631
613	853	433	283	877	661
757	19, 151	487	349	97, 313	769
919	277	739	661	433	151, 211
991	373	43, 193	937	463	283
7, 181	487	409	997	103, 439	331
223	577	457	73, 103	919	367
337	691	613	313	991	409
421	733	643	439	109, 199	547
463	31, 163	61, 163	709	373	607
811	271	241	883	997	691
853	349	277	79, 97	127, 349	727
883	373	313	283	421	877
			337	643	

TABLE 5

3 271 919	61 163 313	139 373 769	283 313 349
3 307 523	61 241 877	139 631 661	307 421 499
3 307 919	67 193 643	151 211 367	307 499 523
3 523 757	67 283 349	151 283 691	307 523 739
3 577 757	73 103 439	151 331 409	349 661 877
3 577 991	79 97 337	151 331 547	349 877 967
3 757 991	79 97 433	151 331 727	367 439 733
3 919 991	79 157 337	151 331 877	379 463 733
7 181 673	79 157 877	157 373 787	379 691 937
7 337 811	79 283 349	157 373 883	397 613 907
7 673 769	79 349 877	157 379 601	397 631 919
13 421 499	79 433 631	157 379 877	397 907 919
13 499 853	79 631 859	157 439 727	433 571 787
19 151 691	79 673 757	163 313 349	457 673 997
19 373 577	79 673 769	199 733 859	457 877 997
31 163 349	97 313 463	241 379 877	523 673 757
31 373 883	103 823 919	241 457 829	577 757 991
37 103 991	103 919 991	241 457 877	691 757 907
37 433 739	127 619 643	271 571 661	727 823 919
43 193 409	127 673 757	271 823 919	877 967 997
43 613 643	139 199 661	277 541 757	

BIBLIOGRAPHIE

- [1] E. ARTIN, Algebraic Numbers and algebraic Functions, *Lectures notes by I. Adamson, Gordon and Breach, New York, 1967.*
- [2] E. ARTIN and J. TATE, Class Field Theory, *Benjamin, New York, 1967.*
- [3] H. BAUER, Die 2-Klassenzahlen spezieller quadratischer Zahlkörper, *J.f.d.r.u.a. Math.*, 252 (1972).
- [4] H. BAUER, Über die kubischen Klassenkörper zyklischer kubischer Zahlkörper, *Dissertation, Karlsruhe Universität (1970).*
- [5] L. BOUVIER et J. J. PAYAN, Construction de certaines extensions de degré p , *Séminaire de théorie des nombres de Grenoble (1972).*
- [6] L. BOUVIER, Table des 2-rang, 4-rang et 8-rang du 2-groupe des classes d'idéaux au sens restreint de $\mathbb{Q}(\sqrt{m})\dots$, *L'Ens. Math.* II^e série, t. XVIII, 1, 1972, 37-45.
- [7] C. CHEVALLEY, Sur la théorie du corps de classes dans les corps finis et les corps locaux, *Jour. of the Fac. of Sc., Tokyo*, Vol. II, Part 9 (1933).
- [8] P. DAMEY et J. J. PAYAN, Existence et construction des extensions galoisiennes et non abéliennes de degré 8 d'un corps de caractéristique différente de 2, *J.f.d.r.u.a. Math.*, B. 244 (1970).
- [9] A. FRÖHLICH, The generalization of a theorem of L. Rédei's, *Quart. Jour. of math. Oxford* (2), 5 (1954), 13-140.
- [10] G. GRAS, Extensions abéliennes non ramifiées de degré premier d'un corps quadratique, *Bull. Soc. Math. France*, 100 (1972).
- [11] G. GRAS, Sur le l -groupe des classes des extensions cycliques de degré premier l , Note *C.R.A.S.*, t. 274 (1972), 1145-1148.
- [12] G. GRAS, Étude du l -groupe des classes des extensions cycliques de degré l , *Sém. Delange-Pisot-Poitou*, 13^e année, 1971-1972, n^o 20.
- [13] M. N. GRAS, Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de \mathbb{Q} ; bases d'entiers (à paraître).
- [14] H. HASSE, Über die Klassenzahl des Körpers $\mathbb{P}(\sqrt{-p})$ mit einer Primzahl $p \equiv 1 \pmod{2^3}$, *Aequationes math.* 3 (1969).
- [15] H. HASSE, Über die Klassenzahl des Körpers $\mathbb{P}(\sqrt{-2p})$ mit einer Primzahl $p \neq 2$, *J. of Number theory.*, 1 (1969), 231-234.
- [16] H. HASSE, Über die Teilbarkeit durch 2^3 der Klassenzahl imaginärquadratischer Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, *J.f.d.r.u.a. Math.*, 241 (1970).
- [17] D. HILBERT, Théorie des corps de nombres algébriques, trad. T. Got et A. Levy, *Hermann*, 1913.
- [18] E. INABA, Über die Struktur der l -klassengruppe zyklischer Zahlkörper von Primzahlgrad l , *J. Fac. Sci. Univ. Tokyo, Sect. I* 4 (1940), 61-115.
- [19] K. IWASAWA, A note on the group of units of an algebraic Number Field, *J. Math. Pures et App.*, 35 (1956), 189-192.

- [20] P. KAPLAN, Divisibilité par 8 du nombre de classes des corps quadratiques réels dont le 2-sous-groupe des classes est cyclique, Note *C.R.A.S.*, t. 275, 887-890.
- [21] P. KAPLAN, Divisibilité par 8 du nombre de classes des corps quadratiques dont le 2-sous-groupe des classes est cyclique et réciprocity biquadratique, à paraître au *J. Math. Soc. of Japan*.
- [22] H. KISILEVSKY, Some results related to Hilbert's Theorem 94, *J. of Number theory*, 2 (1970), 199-206.
- [23] S. KOBAYASHI, On the l -dimension of the ideal class group of Kummer extensions of a certain type, *J. Fac. Sci. Univ. Tokyo*, Sect. IA, Vol. 18 N° 2, 399-404.
- [24] S. KOBAYASHI, On the 3-rank of the ideal class group of certain pure cubic fields (à paraître).
- [25] T. KUBOTA, Über den bizyklischen biquadratischen Zahlkörper. *Nagoya Math. J.*, 10-12 (1956), 65-85.
- [26] S. N. KURODA, On the Class Number of Imaginary quadratic Number Fields, *Proceedings of Japan Academy*, 8, 1965.
- [27] S. LANG, Algebraic Number Theory, *Addison-Wesley Pub. comp.*, New York 1970.
- [28] H. W. LEOPOLDT, Zur Geschlechtertheorie in abelschen Zahlkörpern, *Math. Nachr.*, 9 (1953), 351-362.
- [29] J. J. PAYAN, Sur les classes ambiges et les ordres monogènes d'une extension cyclique de degré premier impair sur \mathbf{Q} ou sur un corps quadratique imaginaire, à paraître à *Arkiv för matematik*.
- [30] L. REDEI und H. H. REICHARDT, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, *J.f.d.r.u.a. Math.*, 170 (1933).
- [31] J. P. SERRE, Corps locaux, *Act. Sc. et ind.*, Paris 1962.
- [32] D. SHANKS, Gauss's Ternary form reduction and the 2-Sylow subgroup, *Math. of computation*, 25 (1971), 837-853.
- [33] O. TAUSKY, A remark concerning Hilbert's Theorem 94, *J.f.d.r.u.a. Math.*, 239/240 (1970), 435-438.

Thèse, Univers. Scient. et Médicale
de Grenoble, Novembre 1972,
acceptée par C. CHABAUTY

Georges GRAS,
Institut de Mathématiques Pures,
Université de Grenoble,
B. P. 116, 38402 Saint-Martin-d'Hères.