ANNALES DE L'INSTITUT FOURIER

GEORGES GRAS

# Sur les $\ell$-classes d'idéaux dans les extensions cycliques relatives de degré premier $\ell$

*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>

Ann. Inst. Fourier, Grenoble
**23**, 4 (1973), 1-44.

# 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 $M = \mathscr{H}(K)$, si et seulement si $|\mathscr{H}_1| = l$ (les quotients $\mathscr{H}_{i+1}/\mathscr{H}_i$ étant nécessairement d'ordre $l$ pour $i < n$).

Le théorème IV.1 nous donne :

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

et la condition $|\mathscr{H}_1| = l$ 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) $|\mathscr{H}(k)| = 1$, $t \geqslant 2$, $(E_k^+ : E_k^+ \cap NK^*) = l^{t-2}$,

(ii) $|\mathscr{H}(k)| = l$, $t \geqslant 1$, $(E_k^+ : E_k^+ \cap NK^*) = l^{t-1}$,

(iii) $|\mathscr{H}(k)| = l^2$ 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 $\mathscr{H}(K)$ est le $l$-groupe des classes de K, $N\mathscr{H}(K)$ est d'indice $l$ dans $\mathscr{H}(k)$ (théorie du corps de classes).

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

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

$$N\mathscr{H}(K) \cap \operatorname{Ker} j \neq \{1\},$$

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

$$|\mathscr{H}(K)^{\nu}| = |N\mathscr{H}(K)|).$$

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

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

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

$$= \frac{|\mathscr{H}_1|}{|\mathscr{H}^{\nu}|}\,\frac{|\mathscr{H}^{\nu}|}{|N\mathscr{H}|};$$

la suite exacte $1 \to \operatorname{Ker} j \cap N\mathscr{H} \to N\mathscr{H} \xrightarrow{j} \mathscr{H}^{\nu} \to 1$ donne

$$|\tilde{\mathscr{H}}/\mathscr{H}| = \frac{|\mathscr{H}_1|}{|\mathscr{H}^{\nu}|\,|\operatorname{Ker} j \cap N\mathscr{H}|} = \frac{|\hat{H}^0(H, \mathscr{H})|}{|\operatorname{Ker} j \cap N\mathscr{H}|},$$

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

## 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 $K = \mathbf{Q}(\sqrt{m})$ et $\hat{K} = \mathbf{Q}(\sqrt{-m})$ et réservons la notation $\hat{}$ pour toute quantité qui concerne le corps $\hat{K}$.

Soient $p_1, \ldots, p_{t^*}$ les nombres premiers ramifiés dans $K/\mathbf{Q}$ (ils se ramifient aussi dans $\hat{K}/\mathbf{Q}$). Si 2 ne divise pas $m$, il est nécessairement ramifié dans K ou dans $\hat{K}$ (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 :

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

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

$$\Lambda = \langle p_1, \ldots, p_{t^*} \rangle, \qquad \hat{\Lambda} = \langle p_1, \ldots, p_{t^*}, 2 \rangle \quad \text{ou vice versa,}$$

lorsque $m$ est impair;

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

Soient A et $\hat{A}$ les matrices (carrées) des systèmes linéaires associés aux groupes $\Lambda$ 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 K et $\hat{K}$ 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 $1 \leqslant i, j \leqslant t^*$ :

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

et $\delta_i = \dfrac{p_i - 1}{2}$ (les quantités $a_{ji}$, $\varepsilon_i$, $\eta_i$, $\eta_0$, $\delta_i$, ... 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 :

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

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) $\quad a_{ij} + a_{ji} = \delta_i \delta_j \quad \textit{pour} \quad i \neq j,$

(ii) $\quad \hat{a}_{ij} = a_{ij} \quad \textit{pour} \quad i \neq j,$

(iii) $\quad \hat{a}_{ii} = a_{ii} + \delta_i,$

(iv) $\quad \hat{\varepsilon}_i = \varepsilon_i + \delta_i,\ \hat{\eta}_i = \eta_i \quad \textit{et} \quad \hat{\eta}_0 = \eta_0.$

La première exprime la loi de réciprocité quadratique appliquée aux nombres $p_i$ et $p_j$ : $\left(\dfrac{p_i}{p_j}\right)\left(\dfrac{p_j}{p_i}\right) = (-1)^{\frac{p_i-1}{2}\frac{p_j-1}{2}}$ (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 :

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

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

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

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

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

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

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

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 $\delta_i$; 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

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

(ii) *Cas* $m < 0$. Dans ce cas, la somme $\delta_0$ 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 :

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

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

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

et

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

(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 :

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

or $A_1 {}^tM = \begin{pmatrix} {}^t\hat{B} & \delta_1 \\ & \vdots \\ & \delta_{t^*} \end{pmatrix}$ 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 :

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

(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 :

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

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

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

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 $m \equiv 1 \bmod 4$ si 2 ne divise pas $m$ et $\frac{m}{2} \equiv 1$ modulo 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 : $R_2 \leqslant \hat{R}_2 \leqslant R_2 + 1$ pour $m > 0$; $R_2 - 1 \leqslant \hat{R}_2 \leqslant R_2$ 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 $p_1, \ldots, p_t$ les nombres premiers ramifiés dans $K/\mathbf{Q}$ (dans $\hat{K}/\mathbf{Q}$, $p_1, \ldots, p_t$, $p$ se ramifient et ce sont les seuls). Si $\left(\frac{p_i}{p}\right) = 1$ pour tout $i$, $1 \leqslant i \leqslant t$, les 4-rangs $R_2$ et $\hat{R}_2$ de $\mathscr{H}(K)$ et $\mathscr{H}(\hat{K})$ vérifient :*

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

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

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

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

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

et

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

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 $p \equiv 1\,(4)$;
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 $i$,

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

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

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

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* $3$ *mod* $4$;

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

(i) $\mathscr{H}(K)$ *est cyclique,*

(ii) *si le symbole de Legendre* $\left(\frac{p}{q}\right)$ *est égal à* $-1$ *alors* $|\mathscr{H}(K)| = 2$,

(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* $|\mathscr{H}(K)| = 2^2$, *sinon* $|\mathscr{H}(K)|$ *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 $\Lambda$ associé à $\mathscr{H}_1$ 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 $\mathscr{H}(K) = \mathscr{H}_1$, d'où (ii). Supposons maintenant que $\left(\frac{p}{q}\right) = 1$ : le rang de A est nul. Pour déterminer un groupe d'idéaux $\mathscr{J}$ associé à $\mathscr{H}_2$ il faut résoudre les équations :

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

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

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

on constate sans peine que

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

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 $\mathscr{J} = \langle \mathfrak{p}, \mathfrak{q}, \mathfrak{A}, \mathfrak{A}^\sigma \rangle$ et que le

groupe $\Lambda$ 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 : « Algorithme 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) :

$$\begin{pmatrix} (-p, p)_p & (-p, 2)_p \\ (-p, p)_2 & (-p, 2)_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \text{ de rang nul.}$$

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

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

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

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

d'où la proposition.

PROPOSITION V.5. — *Soit $p$ premier impair; alors $|\mathscr{H}(\mathbf{Q}(\sqrt{2p}))| = 2$ si et seulement si $p \not\equiv 1$ modulo 8. Lorsque $p \equiv 1$ modulo 8 alors $|\mathscr{H}(\mathbf{Q}(\sqrt{2p}))|$ 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 $\mathscr{J}_1 = \langle \mathfrak{p}_2, \mathfrak{p}_p \rangle$ 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 $\mathscr{H}_2 = \mathscr{H}_1$ 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 $|\mathscr{H}_2| = 2|\mathscr{H}_1| = 4$. 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

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

ce qui entraîne

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

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

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

dont la matrice associée est

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

$$= \begin{pmatrix} 1 & 1 & (-1)^{\frac{u^2-1}{8}} & (-1)^{\frac{x^2-1}{8}} \\ 1 & 1 & (-1)^{\frac{u^2-1}{8}} & (-1)^{\frac{x^2-1}{8}} \end{pmatrix}$$

grâce à la formule du produit; le fait que $u^2 \equiv 1$ (16) et $x^2 \equiv 1$ (16) est équivalent à $y \equiv 0$ (4) et $p \equiv 1 \bmod 16$, 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 $\alpha$ choisi est tel que $q(\alpha) \in \mathfrak{X}^*$. 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 $\mathscr{P}_0 = (1 - \zeta)$ 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 $v_{\mathfrak{L}_0}(\alpha) \equiv 0$ modulo $l$.

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

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

*est première à $\mathscr{P}_0$.*

*Démonstration.* — Si $l$ est ramifié, c'est que l'entier maximum $\lambda$ tel que l'on ait $\alpha \equiv \xi^l \bmod \mathscr{P}_0^\lambda$ dans $\mathbf{Q}'$ vérifie $\lambda < l$ (cf. proposition I.2); on a donc $\alpha = \xi^l + (1 - \zeta)^\lambda w_1$ avec de plus $\xi \equiv 1 \bmod \mathscr{P}_0$ et $w_1 \not\equiv 0 \bmod \mathscr{P}_0$;

$$\alpha = (1 + (1 - \zeta)A)^l + (1 - \zeta)^\lambda w_1,$$

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

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

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

$$1 + (1 - \zeta^g)^\lambda \wp'^s = (1 + (1 - \zeta)^\lambda \wp')^g u^l,$$
$$1 + (1 - \zeta^g)^\lambda \wp'^s \equiv (1 + (1 - \zeta)^\lambda \wp')^g \bmod \mathfrak{P}_0^{\lambda+1},$$

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

$$1 + (1 - \zeta^g)^\lambda \wp'^s \equiv 1 + g\wp'(1 - \zeta)^\lambda \quad - \quad ,$$
$$(1 - \zeta)^\lambda (1 + \zeta + \cdots + \zeta^{g-1})^\lambda \wp'^s \equiv g\wp'(1 - \zeta)^\lambda \quad - \quad ,$$
$$(1 + \zeta + \cdots + \zeta^{g-1})^\lambda \equiv g \bmod \mathfrak{P}_0$$

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

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

La proposition III.2 nous montre que :

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

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

Définition VI.1. — *Soit* $t \geqslant 1$ *et soit* $\mathbf{V}$ *le quotient de l'ensemble des t-uples* $(\nu_1, \ldots, \nu_t) \in \mathbf{F}_l^t$ *avec les* $\nu_i$ *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 $t$-uple $(\nu_1, \ldots, \nu_t) \in \mathbf{F}_l^t$ défini par $\nu_i \equiv \nu_{\mathfrak{X}_i}(\alpha)$ avec $\mathfrak{P}_i \in \mathfrak{D}$ (on rappelle que $\mathfrak{D}$ 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 $t$-uple $(\nu_1, \ldots, \nu_{t-1}, \nu_t) \in \mathbf{F}_l^t$ défini par $\nu_i \equiv \nu_{\mathfrak{X}_i}(\alpha)$ pour

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

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

On définit, de cette manière, une application de $\mathbf{P}(\mathfrak{X}^*)$ dans $\mathbf{V}$ qui dépend du choix de $\mathfrak{D}$ et, lorsque $l$ est ramifié du choix de la racine primitive $l^{\text{ième}}$ de l'unité $\zeta_0$.

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'occurence ce nombre est égal à $(l-1)^{t-1}$).

2. *Systèmes linéaires associés aux groupes* $\Lambda$.

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

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

HYPOTHÈSE VI.1. — *On a pour* $\bar{t} \leqslant t$ : $a_1 = p_1, \ldots, a_{\bar{t}} = p_{\bar{t}}$, *et les nombres* $a_{\bar{t}+1}, \ldots, a_n$ *ne sont divisibles par aucun des nombres premiers* $p_1, \ldots, p_t$ *ramifiés dans* $K/\mathbf{Q}$.

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

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

$$[a]_{\mathscr{P}} = (p, a)_{\mathscr{P}}, \ (p) = \mathscr{P} \cap \mathbf{Z}, \ \mathscr{P} \neq \mathscr{P}_0$$
$$[a]_{\mathscr{P}_0} = (\zeta_0, a)_{\mathscr{P}_0} \quad \textit{sinon.}$$

On a alors le lemme suivant :

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

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

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

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

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

d'où le lemme dans ce cas.

Si $p_i = p_t = l$ on a $(\alpha,\ a)_l = \zeta_0^{S_{\mathfrak{P}_0} q_{\mathfrak{P}_0}\left(\frac{\lambda_{\mathfrak{P}_0}(\alpha-1)(a-1)}{l(\zeta_0-1)}\right)}$ (Proposition III.3) et, de même, $(\zeta_0,\ a)_{\mathfrak{P}_0} = \zeta_0^{S_{\mathfrak{P}_0} q_{\mathfrak{P}_0}\left(\frac{\lambda_{\mathfrak{P}_0}(\zeta_0-1)(a-1)}{l(\zeta_0-1)}\right)}$; on a alors $\nu_t \equiv \dfrac{\alpha-1}{1-\zeta_0}$ et $n_{\mathfrak{P}_0} = 1$; 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

$$(a,\ \alpha)_{\mathfrak{P}_0} = \zeta_0^{\mu v_t}$$

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

Posons, pour simplifier l'écriture,

$$n_i = n_{\mathfrak{P}_i}, \qquad [a]_i = [a]_{\mathfrak{P}_i}, \qquad \mathfrak{P}_i \in \mathfrak{D} \qquad \text{et} \qquad (\alpha,\ a_i)_j = (\alpha,\ a_i)_{\mathfrak{P}_j}.$$

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

$$\begin{cases} \prod_{i=1}^{n} [a_i]_j^{v_j x_i} \prod_{k=1}^{t} [a_j]_k^{-v_k x_j} = 1, \ 1 \leqslant j \leqslant \bar{t}, \\ \prod_{i=1}^{n} [a_i]_j^{x_i} = 1, \ \bar{t}+1 \leqslant j \leqslant t, \end{cases}$$

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

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

$$\prod_{i=1}^{\bar{t}} (\alpha,\ a_i)_j^{x_i} \prod_{i>\bar{t}} (\alpha,\ a_i)_j^{x_i} = 1;$$

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

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

$$\prod_{i=1}^{n} (\alpha, a_i)_j^{x_i} = \prod_{\substack{i=1 \\ i \neq j}}^{\bar{t}} (\alpha, a_i)_j^{x_i} (\alpha, a_j)_j^{x_j} \prod_{i > \bar{t}} (\alpha, a_i)_j^{x_i} = 1$$

$$= \prod_{\substack{i=1 \\ i \neq j}}^{\bar{t}} [a_i]_j^{-n_j v_j x_i} (\alpha, a_j)_j^{x_j} \prod_{i > \bar{t}} [a_i]_j^{-n_j v_j x_i} = 1$$

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

La formule du produit donne $\prod_{\mathfrak{X}} (\alpha, a_i)_{\mathfrak{X}} = 1$, ou encore $\prod_{\substack{\mathfrak{X} \\ \text{ramifié}}} (\alpha, a_j)_{\mathfrak{X}} = 1$, soit $\prod_{k=1}^{t} (\alpha, a_j)_k^{n_k} = 1$ ;

$$(\alpha, a_j)_j = \prod_{\substack{k=1 \\ k \neq j}}^{t} (\alpha, a_j)_k^{-n_k/n_j} = \prod_{\substack{k=1 \\ k \neq j}}^{t} [a_j]_k^{n_k^2 v_k/n_j}.$$

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 :

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

Il vient alors pour la j[ième] ligne du système $(j \leqslant \bar{t})$ :

$$\prod_{\substack{i=1 \\ i \neq j}}^{n} [a_i]_j^{-n_j v_j x_i} \prod_{\substack{k=1 \\ k \neq j}}^{t} [a_j]_k^{n_j v_k x_j} = 1,$$

soit

$$\prod_{\substack{i=1 \\ i \neq j}}^{n} [a_i]_j^{v_j x_i} \prod_{\substack{k=1 \\ k \neq j}}^{t} [a_j]_k^{-v_k x_j} = 1, \quad j \leqslant \bar{t}.$$

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

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

soit encore

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

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

*du système devient :*

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

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

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

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* $\Lambda$ *est*

$$\prod_{i=1}^{n} (m, a_i)_j^{x_i} = 1, \quad 1 \leqslant j \leqslant t$$

*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)

*où* $\qquad a' = \dfrac{a}{p^{v_p(a)}}, \qquad b' = \dfrac{b}{p^{v_p(b)}}, \qquad p \neq 2,$

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

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

*Remarque* VI.2. — Si $r_i$ désigne le rang du système linéaire associé à la détermination de $|\mathscr{H}_{i+1}/\mathscr{H}_i|$, la proposition IV.2 montre que $l^{R_1} = \prod_{i=0}^{l-2} |\mathscr{H}_{i+1}/\mathscr{H}_i| = \prod_{i=1}^{l-2} l^{t-1-r_i}$, 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* $\mathscr{H} = \mathscr{H}_1$.

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

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

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* $p_i = l$. *En outre, lorsque* $r = 0$ *relativement à* K/**Q**, *on a* $r = 0$ *relativement aux* $(l-1)^{t-1}$ *extensions ayant même discriminant que* K/**Q**.

*Démonstration.* — La dernière partie de la proposition est évidente car la nullité de $r$ ne dépend pas du système $\{\varphi_1, \ldots, \varphi_t\}$ 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* $\mathscr{H}_2$ *est le même pour les* $l - 1$ *extensions* K/**Q** *ramifiées en* $p_1$, $p_2$;

(ii) *si* $r$ *est égal à* 0 (*ce qui équivaut à la condition* $\mathscr{H}_2/\mathscr{H}_1 \neq \{1\}$) *soit* $p$ *un nombre premier décomposé dans* K/**Q** *tel que l'un des symboles* $[p]_{\mathfrak{P}_1}$, $[p]_{\mathfrak{P}_2}$ *soit différent de* 1; *alors* $\mathscr{H}$(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 :

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

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

$$\begin{cases} -a_{12}\wp_2 x_1 + a_{21}\wp_1 x_2 = 0 \\ a_{12}\wp_2 x_1 - a_{21}\wp_1 x_2 = 0 \end{cases}$$

dont le rang ne dépend pas des nombres $\wp_i$ 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 $\mathfrak{p}^q$ est d'ordre une puissance de $l$ dans $\mathcal{H}(K)$. Considérons $\mathcal{J} = \langle \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}^q, \mathfrak{p}^{q\sigma}, \ldots, \mathfrak{p}^{q\sigma^{t-1}} \rangle$ où $\mathfrak{p}_1$, $\mathfrak{p}_2$ désignent les deux idéaux premiers ramifiés dans $K/\mathbf{Q}$ 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

$$|\tilde{\mathcal{H}}/\mathcal{H}| = l^{t-1-r'} = l^{1-r'}$$

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 $\mathfrak{p}^q$; 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 $\lambda$ 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 :

$$\begin{pmatrix} \wp_2 + \wp_3 & 2\wp_1 & 2\wp_1 \\ 2\wp_2 & \wp_1 - \wp_3 & \wp_2 \\ 2\wp_3 & \wp_3 & \wp_1 - \wp_2 \end{pmatrix}$$

Pour $\wp_1 = 1, \wp_2 = \wp_3 = 2$ 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 $\{p_1, \ldots, p_t\}$ pour $t$ donné, de la manière suivante :

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

*Le graphe associé à* $\{p_1, \ldots, p_t\}$ *est constitué de* $t$ *sommets* $S_1, \ldots, S_t$ *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* $K/\mathbf{Q}$ *de discriminant donné.*

Lorsque $t$ augmente le nombre de systèmes possibles, relativement à $\mathscr{H} = \mathscr{H}_1$ (i.e. $\Lambda_1 = \langle p_1, \ldots, p_t \rangle$), est rapidement très grand (les $[p_i]_j$ pouvant prendre toutes valeurs) et l'étude du rang en fonction du $t$-uple $(\varrho_1, \ldots, \varrho_t)$ 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 $[p_i]_j = \zeta_0^{a_{ij}}$).

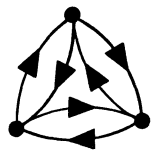
PROPOSITION VI.5. — *a) Si* $l = 3$ *et* $t = 2$ *alors :*

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

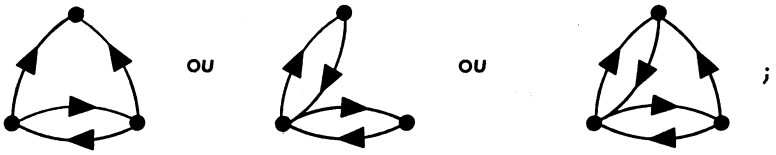
(ii) $R_1 = 1$ *pour les deux corps si le graphe associé est :*


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

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

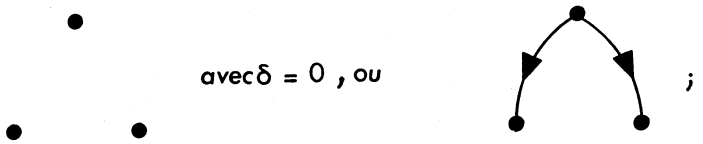


(ii) $R_1 = 3$ *pour les quatre corps si le graphe associé est:*



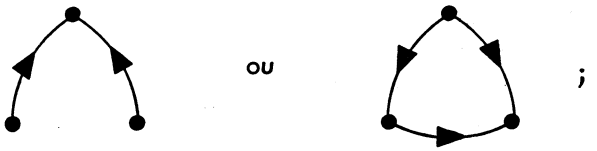

;

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



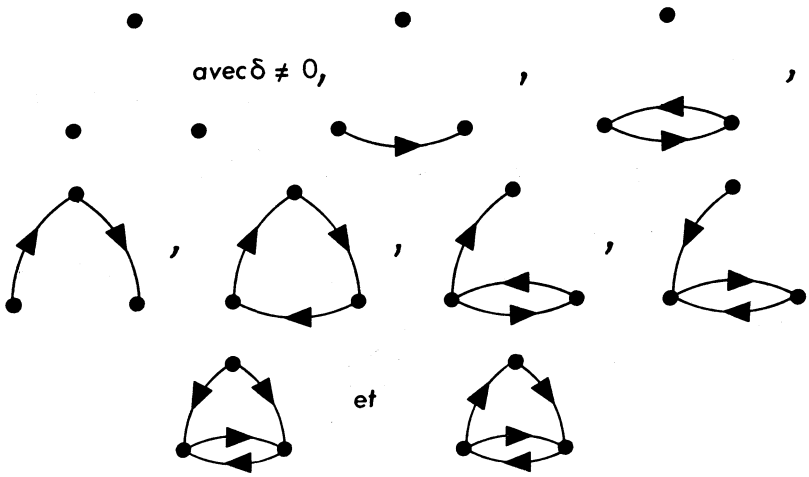

;

(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);

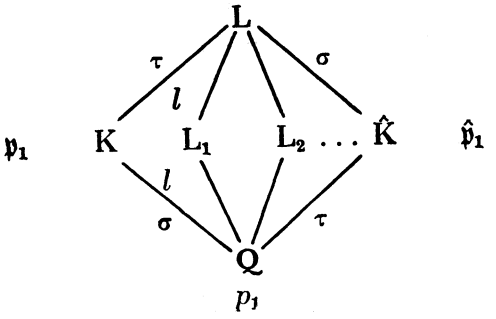
(v) : (7, 31, 67); (7, 31, 37); (7, 37, 181); (7, 13, 31); (7, 13, 73); (7, 73, 181), (7, 43, 181), (7, 13, 223); (7, 19, 181).

**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 $|\mathscr{H}_2| = l^2$ pour les $l - 1$ corps $K_i$ et les symboles $[p_1]_{p_2}$ 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* $|\mathscr{H}_3/\mathscr{H}_2| = l$. *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 $\sigma$ (resp. $\tau$) un générateur de $\mathrm{Gal}(L/\hat{K})$ (resp. $\mathrm{Gal}(L/K)$).

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 $\hat{\alpha}_i A_{\hat{K}} = \hat{\mathfrak{p}}_i \hat{\mathfrak{A}}_i^{\sigma-1} (i = 1, 2)$, $\hat{\alpha}_i \in \hat{K}$, et on doit démontrer que les $\hat{a}_i$ (normes des $\hat{\mathfrak{A}}_i$) sont aussi normes dans $\hat{K}/\mathbf{Q}$. 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 $[p_1]_{p_2} = 1$, 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) :

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

D'après les hypothèses faites $q_1 = N\mathfrak{q}_1$ est norme d'un élément de K, donc les symboles $[q_1]_{p_1}$ et $[q_1]_{p_2}$ sont égaux à 1 (c'est-à-dire que $q_1$ est totalement décomposé dans $L/\mathbf{Q}$).

LEMME 2. — *Le nombre* $\alpha$ *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 $\alpha A_K$ (sinon $\alpha$ est une unité en $\mathfrak{p}$ donc norme, car $L/K$ est non ramifiée); nécessairement $\mathfrak{p} = \mathfrak{q}_1$ (ou $\mathfrak{q}_1^{\sigma}$), or ceci est absurde car $q_1$ est totalement décomposé dans $L/\mathbf{Q}$.

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 $N_{L/\mathbf{Q}}\varphi = p_1$ donc $\varphi A_L = \mathfrak{P}\mathfrak{A}_1$ avec $N_{L/\mathbf{Q}}\mathfrak{A}_1 = \mathbf{Z}$; 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 $\hat{H}_0(\mathrm{Gal}(L/\mathbf{Q}), \mathscr{J}(L)) = \{1\}$ et $\mathfrak{A}_1 \in \mathscr{J}(L)^I$ où I est l'idéal d'augmentation de

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

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

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

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

Si $\hat{\mathfrak{q}}$ est inerte dans $L/\hat{K}$, $\hat{f} = l$ et $\hat{q}^{f\hat{f}} \in N(\hat{K})$. Si $\hat{q}$ est inerte ou ramifié dans $\hat{K}/\mathbf{Q}$ alors $\hat{\mathfrak{q}}^{\tau-1} = A_{\hat{k}}$. Supposons $\hat{q}$ totalement décomposé dans $L/\mathbf{Q}$. Alors $\hat{q}$ est décomposé dans $L_1$ et dans $L_2$, donc les symboles $[\hat{q}]_{p_1}$ et $[\hat{q}]_{p_2}$ valent 1 et $\hat{q}$ est norme dans $\hat{K}/\mathbf{Q}$.

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 $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ dans $K/\mathbf{Q}$ et que, d'après le théorème IV.1, il existe une relation :

$$\mathfrak{p}_1^{x_1^0} \ldots \mathfrak{p}_t^{x_t^0} = (\alpha)A_K, \tag{1}$$

$x_i^0$ non tous congrus à 0 modulo $l$, $(x_1^0, \ldots, x_t^0)$ 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) : $\prod_{i=1}^{t} (\alpha, p_i)_{p_j}^{x_i} = 1$, $1 \leqslant j \leqslant t$ (associé à $\Lambda_1 = \langle p_1, \ldots, p_t \rangle$), dont le rang est $r_1 \leqslant t - 1$, admet la solution $(x_1^0, \ldots, x_t^0)$. 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

$\eta \neq \pm 1$ (par exemple l'unité « cyclotomique ») on écrit

$$\eta = \psi^{(\sigma-1)^r}, \quad r \geqslant 1,$$

$r$ étant supposé maximum et $\psi A_K$ entier sans facteur rationnel; on vérifie sans difficulté que

$$\psi A_K = \prod_{i=1}^{t} \mathfrak{p}_i^{x_i^0}$$

est la relation non triviale cherchée (cf. [13] pour la recherche pratique de $\psi$).

Soit $\mathfrak{f}$ le conducteur du corps ($\mathfrak{f} = p_1 \ldots p_{t-1} l^2$ ou $p_1 \ldots p_t$ selon que $l$ est ramifié ou non); on pose $1^* = 2$ (resp. $1^* = 1$) si $l$ est ramifié (resp. non ramifié). Le cas

$$(x_1^0, \ldots, x_t^0) = (1, \ldots, 1, 1^*)$$

est particulièrement intéressant à cause du fait suivant (cf. [29]) :

Proposition VI.7. — *Si l'anneau des entiers de* K *est monogène* (*i.e.* $A_K = \mathbf{Z}[\theta]$, $\theta \in A_K$) *il est nécessaire que la relation* (1) *soit* :

$$\mathfrak{p}_1 \ldots \mathfrak{p}_{t-1} \mathfrak{p}_t^{1^*} = \alpha A_K.$$

*Démonstration.* — Si $A_K = \mathbf{Z}[\theta]$, le polynôme irréductible de $\theta$ a pour discriminant le discriminant du corps soit

$$N_{K/Q}\left(\prod_{i=1}^{l-1} (\theta - \theta^{\sigma^i})\right) = \mathfrak{f}^{l-1};$$

on a alors

$$\prod_{i=1}^{l-1} (\theta - \theta^{\sigma^i}) A_K = (\mathfrak{p}_1 \ldots \mathfrak{p}_{t-1} \mathfrak{p}_t^{1^*})^{l-1},$$

d'où la proposition.

Corollaire VI.4. — *Pour que* $A_K = \mathbf{Z}[\theta]$ *il est nécessaire que* (S) *admette la solution* $(1, \ldots, 1, 1^*)$.

Corollaire VI.5. — *Supposons* $t = 2$.

(i) *si le graphe associé à* $\{p_1, p_2\}$ *est* : • • *alors*

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

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

La matrice associée est :

$$A = \begin{pmatrix} -a_{12}\rho_2 & a_{21}\rho_1 \\ a_{12}\rho_2 & -a_{21}\rho_1 \end{pmatrix};$$

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

$$a_{12}\rho_2 = a_{21}\rho_1 . 1^*,$$

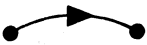
soit $\rho_2 = \dfrac{a_{21}}{a_{12}} \rho_1 . 1^*$, ce qui se produit pour un corps et un seul.

Dans le cas (ii) on a, par exemple, $a_{21} = 0$ et $a_{12} \neq 0$, soit $A = \begin{pmatrix} -a_{12}\rho_2 & 0 \\ a_{12}\rho_2 & 0 \end{pmatrix}$ 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).

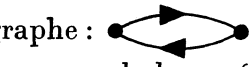
(i) $\{3,7\}$ (graphe : • •); un corps et un seul admet une base $\{1, \theta, \theta^2\}$ ($a = 3$, $b = 1$ pour ce corps, $a = 4$, $b = 2$ pour l'autre),

(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 ($\theta$ racine de $X^3 - 3.307\,X - 307.35$) pour le corps défini par $a = 19$, $b = 17$ on prend $\theta$ 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 $(1, \ldots, 1, 1^*)$ est solution, il n'y a pas nécessairement de base d'entiers $\{1, \theta, \ldots, \theta^{l-1}\}$; 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 3e degré, à savoir :

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

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

$\alpha$ 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 $p_1, \ldots, p_t$ les nombres premiers ramifiés dans $K = \mathbf{Q}(\sqrt{m})$. La détermination de $\mathscr{H}(K)$ se ramène à la détermination de deux suites croissantes $\mathscr{J}_i$ et $\Lambda_i$, $i \geqslant 1$, vérifiant les hypothèses des théorèmes IV.2 et IV.3.

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

Dans la pratique, il suffit de connaître

$$\Lambda_{i-1} = \langle p_1, \ldots, p_t, q_1, \ldots, q_n \rangle$$

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

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

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

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

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

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

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

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

*Remarque* VI.4. — Il est clair que les groupes $\mathscr{J}_i$ satisfont à la condition $\mathscr{J} \cap \mathscr{J}(\mathrm{K})^{\sigma-1} = \mathscr{J}^{\sigma-1}$. L'hypothèse $\mathscr{J}$ 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 $\mathscr{J}(\mathrm{K})^{\sigma-1} \cap \mathscr{J} = \mathscr{J}^{\sigma-1}$, 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 $\mathrm{K} = \mathbf{Q}(\sqrt{-146})$. On aura $\mathscr{J}_1 = \langle \mathfrak{p}_2, \mathfrak{p}_{73} \rangle$ et $\Lambda_1 = \langle 2, 73 \rangle$ dont la matrice associée est $A_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$; d'où $|\mathscr{H}_2/\mathscr{H}_1| = 2$.

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 :

$$\mathscr{J}_2 = \langle \mathfrak{p}_2, \mathfrak{p}_{73}, \mathfrak{p}_3^2, \mathfrak{p}_3^{2\sigma} \rangle \qquad \text{et} \qquad \Lambda_2 = \langle 2, 73, 3^2 \rangle$$

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

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 :

$$\mathscr{J}_3 = \langle \mathfrak{p}_2, \mathfrak{p}_{73}, \mathfrak{p}_3, \mathfrak{p}_3^{\sigma} \rangle \qquad \text{et} \qquad \Lambda_3 = \langle 2, 73, 3 \rangle ;$$

$A_3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$, car 3 est un carré modulo 73, et $|\mathscr{H}_4/\mathscr{H}_3| = 2$. On trouve alors $3.7^2 = 1^2 + 146.1^2$ soit :

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

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

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

est cyclique d'ordre 16.

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

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

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 :

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

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

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

On vérifie que $\left(\frac{3}{113}\right) = -1$, c'est-à-dire que $\mathscr{H}(K) = \mathscr{H}_3$ 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

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

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 $1 \leqslant i \leqslant t$.

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

Les résultats du chapitre III montrent que si $p_1, \ldots, p_{t'}$ sont les nombres premiers ramifiés dans $K/\mathbf{Q}$ et distincts de $l = 3$, un nombre $\alpha$ vérifiant $q(\alpha) \in \mathfrak{X}^*$ sera de la forme

$$\alpha = \beta D \qquad \text{avec} \qquad D = p_1 . p_2 \ldots p_{t'}$$

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

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

$$\alpha \equiv 1 \bmod \mathscr{P}_0 = (1-j)).$$

Si 3 est non ramifié il faut éventuellement multiplier $\beta$

par $j$ ou $j^2$ de telle manière que $\alpha$ vérifie :

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

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

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

Soit alors $\theta = \sqrt[3]{\alpha}$; on a $K' = \mathbf{Q}'(\theta)$ et on vérifie que $\mathrm{Tr}_{K'/K}(\theta)$ 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* $p_1, \ldots, p_t$, $p_i \equiv 1$ *mod* 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 :*

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

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

$$X^3 - 3DX - aD, \quad D = p_1 \ldots p_{t'} = \frac{a^2+3b^2}{4},$$

$b$ *non divisible par* 3, *lorsque* $p_t = 3$ *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 $\theta$ une racine de ce polynôme; le nombre

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

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 $\alpha A_K = \mathfrak{p}_{181}\mathfrak{p}_{17}\mathfrak{p}_{17}^{2\sigma}(\mathfrak{p}_{181}^3 = 181\mathbf{Z},\ N\mathfrak{p}_{17} = 17\mathbf{Z})$ et $\left(\frac{\alpha}{17}\right)A_K = \mathfrak{p}_{181}\mathfrak{p}_{17}^{\sigma(1-\sigma)}$. Par conséquent, le groupe $\mathscr{J}_2$ contiendra $\mathfrak{p}_{181}$, $\mathfrak{p}_7$ et $\mathfrak{p}_{17}$ et $\Lambda_2$ 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 $|\mathscr{H}_3/\mathscr{H}_2| = 1$ ($\mathscr{H}(K)$ est donc isomorphe à $(\mathbf{Z}/3\mathbf{Z})^2$).

(ii) Corps défini par le polynôme

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

On trouve un entier $\alpha$ dont le polynôme irréductible est :

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

on vérifie que $\alpha A_K = \mathfrak{p}_7\mathfrak{p}_2^2\mathfrak{p}_2^{7\sigma}\mathfrak{p}_3^3$ 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 $\theta$ est une racine de ce polynôme, les nombres $\alpha_1 = \dfrac{13.7 + \theta}{3}$ et $\alpha_2 = \dfrac{673 + 5\theta + 5\theta'}{3}$ 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 :

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

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

Écrivons maintenant que $3^3$ est norme :

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

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

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

et $\Lambda_3 = \langle 7, 673, 3 \rangle$; 3 n'étant pas reste cubique modulo 7 il en résulte $r_3 = 1$ et $|\mathscr{H}_4/\mathscr{H}_3| = 1$. On obtient que $|\mathscr{H}(K)| = 27$ et que $\mathscr{H}(K)$ 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 $K/\mathbf{Q}$ et le symbole $[3]_7$ est différent de 1 : $\mathscr{H}(K)$ est engendré par $h = \mathrm{Cl}(\mathfrak{p}_3)$ et on a la relation :

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

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 :

$$X^3 - 36.7X^2 - 3.7^2.4567X + 7.(73.4)^3$$

et

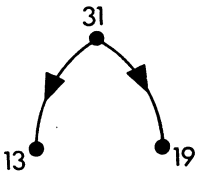
$$X^3 - 673X^2 - 673.3.53X + 673;$$

ce qui donne :

$$(\alpha_1)A_K = \mathfrak{p}_7\mathfrak{p}_{73}^3\mathfrak{p}_2^6 \qquad \text{et} \qquad (\alpha_2)A_K = \mathfrak{p}_{673}.$$

On a $\left(\frac{\alpha_1}{4.73}\right)A_K = \mathfrak{p}_7\mathfrak{p}_{73}^{(1-\sigma)(2+\sigma)}\mathfrak{p}_2^{2(1-\sigma)(2+\sigma)}$ et $(\alpha_2)A_K = \mathfrak{p}_{673}A_K^{1-\sigma}$, d'où : $\mathcal{J}_2 = \langle \mathfrak{p}_7, \mathfrak{p}_{673}, (\mathfrak{p}_2^2\mathfrak{p}_{73})^{2+\sigma}, \ldots \rangle$ et $\Lambda_2 = \langle 7, 673, 292^3 \rangle$; $r_2$ est nul et $|\mathscr{H}_3/\mathscr{H}_2| = 3$; alors $\mathcal{J}_3 = \langle \mathfrak{p}_7, \mathfrak{p}_{673}, \mathfrak{p}_2^2\mathfrak{p}_{73}, \ldots \rangle$ et $\Lambda_3 = \langle 7, 673, 292 \rangle$; on vérifie que 292 n'est pas reste cubique modulo 7, donc $r_3 = 1$ et $|\mathscr{H}(K)| = 27$ 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 $|\mathscr{H}(K)| = |\mathscr{H}_1| = 9$) et pour le dernier on aura $R_1 = 3$. On vérifie facilement que c'est pour le corps K défini par $a = 170$, $b = 8$ $\left(\frac{a^2 + 27b^2}{4} = 13.19.31,\ \text{cf. Proposition VI.8}\right)$ donc par le polynôme $X^3 - 13.19.31X - 8.13.19.31$; le triplet $(\nu_1, \nu_2, \nu_3)$ associé étant ici (1, 1, 1) relativement au choix des idéaux premiers au-dessus de 13, 19 et 31 :

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

(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 $\alpha_1$ et $\alpha_2$ de K tels que $N\alpha_1 = 31$ et $N\alpha_2 = 13.19$; on montre que

le polynôme irréductible de $\varphi = \dfrac{1\,439 - 16\theta - 18\theta'}{3}$ où $\theta$ 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 $\alpha_3$ 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

$$\mathfrak{p}_{31}\mathfrak{p}_{13}^2\mathfrak{p}_{19}^2 \sim 1$$

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 $\dfrac{\theta}{2} A_K = \mathfrak{p}_{13}\mathfrak{p}_{19}\mathfrak{p}_{31}\mathfrak{p}_2^{((1-\sigma)(2+\sigma)}$ et $N\mathfrak{p}_2^{2+\sigma} = 8$, d'où le groupe $\Lambda_2 = \langle 13, 19, 31, 8\rangle$ qui montre que

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

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 $|\mathscr{H}_4/\mathscr{H}_3| = 1$. La proposition IV.2 entraîne que $\mathscr{H}(K) \simeq (\mathbf{Z}/9\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z})^2$.

*Remarque* VI.8. — L'exemple ci-dessus montre que l'on ne peut pas obtenir pour $t \geqslant 3$ un énoncé simple donnant la structure de $\mathscr{H}(K)$ (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 $\mathscr{H}_i$, $i > 3$, 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 $\theta$ 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 :

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

et

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

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 $\mathscr{J}_2$ sera donc égal à :

$$\mathscr{J}_2 = \langle \mathfrak{p}_{37}, \mathfrak{p}_{991}, \mathfrak{p}_5^{2(2+\sigma)}, \mathfrak{p}_5^{2+\sigma}\mathfrak{p}_{29}^{1+\sigma}, \ldots \rangle = \langle \mathfrak{p}_{37}, \mathfrak{p}_{991}, \mathfrak{p}_5^{2+\sigma}, \mathfrak{p}_{29}, \ldots \rangle$$

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

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

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

(ii) *Étude de* $\hat{K}$.

On vérifie que l'entier $\psi$, 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 $\theta$ et $\vartheta$ des racines des polynômes

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

et

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

on sait que l'on peut écrire :

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

à condition de définir la conjugaison $\sigma$ par l'expression

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

On considère enfin l'entier $\varphi$ défini par :

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

dont le polynôme irréductible est :

$$X^3 - 11.991X^2 + 2^5.3^2.5.13.991X - 991(2^2.7^2)^3;$$

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

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

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 $\varphi'$ tel que

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

On aura successivement :

$\mathscr{J}_1 = \langle \mathfrak{p}_{991} \rangle$, $\Lambda_1 = \langle 991 \rangle$,
$\mathscr{J}_2 = \langle \mathfrak{p}_{991}, \mathfrak{p}_2^{3(2+\sigma)}, \ldots \rangle$, $\Lambda_2 = \langle 991, 2^9 \rangle$,
$\mathscr{J}_3 = \langle \mathfrak{p}_{991}, \mathfrak{p}_2^{3(2+\sigma)}, \mathfrak{p}_2^{3(1+\sigma)} \rangle = \langle \mathfrak{p}_{991}, \mathfrak{p}_2^3, \ldots \rangle$, $\Lambda_3 = \langle 991, 2^3 \rangle$,
$\mathscr{J}_4 = \langle \mathfrak{p}_{991}, \mathfrak{p}_2^{2+\sigma}, \mathfrak{p}_2^3, \ldots \rangle$ qui est équivalent à
$\langle \mathfrak{p}_{991}, \mathfrak{p}_2^{2+\sigma}, \mathfrak{p}_7^3, \ldots \rangle$, $\Lambda_4 = \langle 991, 2^3, 7^3 \rangle$.

ceci afin de satisfaire à la condition :

$$\mathscr{J} \cap \mathscr{J}(\hat{K})^{\sigma-1} = \mathscr{J}^{\sigma-1};$$

$\mathscr{J}_5 = \langle \mathfrak{p}_{991}, \mathfrak{p}_2^{2+\sigma}, \mathfrak{p}_7^3, \mathfrak{p}_2^{1+\sigma}, \mathfrak{p}_7^{2+\sigma}, \ldots \rangle$ équivalent à
$\langle \mathfrak{p}_{991}, \mathfrak{p}_2, \ldots \rangle$ soit $\Lambda_5 = \langle 991, 2 \rangle$.

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

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

## TABLES NUMÉRIQUES

**1.** *Table* 1.

Table des corps cubiques définis par $p_1$ et $p_2 < 1\,000$ et pour lesquels $|\mathscr{H}_3| = 9$ (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 $|\mathscr{H}_3| = l^2$ ($p_1$ 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 $D = \dfrac{a^2 + 27b^2}{4} = p_1 \cdot p_2$. Pour $p_1$, puis de la même manière pour $p_2$, nous donnons les coefficients d'un polynôme irréductible d'un entier $\varphi_i$ tel que $|N\varphi_i| = p_i n$, $|\mathrm{Tr}\,(\varphi_i \varphi_i^{\sigma})| = p_i s$ et $|\mathrm{Tr}\,\varphi_i| = p_i t$. 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 $\mathscr{H}(K)$ s'en déduit dans presque tous les cas (la présence d'une $*$ indique que $\mathscr{H}(K)$ contient au moins un sous-groupe de la forme indiquée).

**4.** *Table* 4.

Exemples de corps cubiques tels que $\mathscr{H}(K) \simeq \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ (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

| $p_1 \cdot p_2$ | $a$ | $b$ | $n$ | $s$ | $t$ | $\mathfrak{A}_1$ | $n$ | $s$ | $t$ | $\mathfrak{A}_2$ | $\mathcal{H}(\mathrm{K})$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 7.673 | 113 | 15 | 1 | 2.5.17 | 13 | $(1)$ | $3^3$ | 2.83 | 1 | $p_3^{2+\sigma}$ | (9, 3) |
| | 76 | 22 | $2^6.73^3$ | 3.7.4567 | $2^2.3^2$ | $(p_2^2p_{73})^{2+\sigma}$ | 1 | 3.53 | 1 | $(1)$ | (9, 3) |
| 7.769 | 92 | 22 | $2^6$ | 677 | $2^2.5$ | $p_2^{2(2+\tau)}$ | $2^6 31^3$ | $2^2.3^2.31$ | 3 | $p_2^2p_{31}$ | (9, 3) |
| | 43 | 27 | $3^3$ | 2.11.19 | 17 | $p_3^{2+\sigma}$ | 1 | 2 | 1 | $(1)$ | (9, 3) |
| 37.991 | 376 | 14 | $2^6.13^3$ | $2^2.13.3^4$ | 23 | $p_2^2p_{13}$ | $2^6.7^6$ | $2^5.3^2.5.13$ | 11 | $p_2^{2+\sigma}p_7^{2(2+\sigma)}$ | (27, 9) |
| | 295 | 47 | $5^6$ | 13.727 | $2^3$ | $p_5^{2(2+\sigma)}$ | $5^3.29^3$ | $2^6 7.29$ | 7 | $p_5^{2+\sigma}p_{29}$ | (9, 3) |
| 67.643 | 343 | 45 | $3^3.5^3.29^3$ | $2^4.3.2029$ | 5 | $p_3(p_5p_{29})^{2+\sigma}$ | $173^3$ | $3^2.19.137$ | $2^2.3$ | $p_{173}^{2+\sigma}$ | (9, 3) |
| | 143 | 75 | $19^3$ | $2^3.43.3^2$ | 3.5 | $p_{19}^{2+\sigma}$ | $5^3.13^3$ | $2^6.3^3$ | 3 | $(p_5p_{13})^{2+\sigma}$ | (9, 3) |
| 73.241 | 262 | 8 | $2^3$ | 17 | 2 | $p_2^{2+\sigma}$ | 1 | 17 | 1 | $(1)$ | (9, 3) |
| | 143 | 43 | $17^3$ | $7^2.17$ | 2.7 | $p_{17}$ | $17^3$ | $7^2.17$ | 7 | $p_{17}$ | (9, 3)* |
| 79.157 | 173 | 27 | $3^6$ | $3^4.29$ | 11 | $p_3^{2+\sigma}$ | $83^3$ | $3^2.653$ | $2^2.3$ | $p_{83}^{2+\sigma}$ | (9, 3) |
| | 65 | 41 | $11^3$ | 1201 | $2^2$ | $p_{11}^{2+\sigma}$ | $5^6$ | $3.5^4$ | $2^2$ | $p_5^{2+\sigma}$ | (9, 3) |
| 79.349 | 328 | 10 | $2^9.5^6$ | $2^3.3541$ | 3.11 | $p_2^3p_5^{2(2+\sigma)}$ | $2^{12}.19^3$ | $2^3.3.5.17.31$ | $3^3$ | $p_2^{5+\sigma}p_{19}^{2+\sigma}$ | (9, 3) |
| | 301 | 27 | $7^3.23^3$ | 2.3.7.23.71 | $3^2.11$ | $p_7p_{23}$ | $7^3.23^3$ | 12659 | 17 | $p_7^{2+\sigma}p_{23}^{2+\sigma}$ | (9, 3)* |
| 79.409 | 331 | 27 | $223^3$ | 23.223 | 31 | $p_{223}$ | $89^3$ | $2^2.5.401$ | 11 | $p_{89}^{2+\sigma}$ | (9, 3)* |
| | 196 | 58 | $2^{12}$ | $2^3.37$ | 5 | $p_2^{5+\sigma}$ | $2^{18}$ | $2^3.5.17$ | 1 | $p_2^{2+3\sigma}$ | (9, 3) |
| 79.631 | 433 | 21 | $7^6$ | $2^2.5^2.229$ | 1 | $p_7^{2(2+\sigma)}$ | $23^3$ | $2.7^2.13$ | 7 | $p_{23}^{2+\sigma}$ | (9, 3) |
| | 298 | 64 | $2^9.59^3$ | 2.59.661 | 3.5 | $p_2^{5+2\sigma}p_{59}$ | $2^6.19^3$ | $2^4.5^2.37$ | $3^2$ | $p_2^{2+\sigma}p_{19}^{2+\sigma}$ | (9, 3)* |
| 79.757 | 368 | 62 | $2^6.23^3$ | $2^2.23.11.37$ | 5 | $p_2^2p_{23}$ | $11^6$ | 8069 | 1 | $p_{11}^{2(2+\sigma)}$ | (9, 3) |
| | 125 | 91 | $61^3$ | $2^2.3.5^2.11$ | $3^3$ | $p_{61}^{2+\sigma}$ | $5^6.13^3$ | $3.5^4.19$ | $2^2.3$ | $p_5^{2+\sigma}p_{13}^{2+\sigma}$ | (9, 3)* |
| 97.337 | 142 | 64 | 1 | 3.139 | 1 | $(1)$ | $2^6$ | $2^4.5$ | 1 | $p_2^{2+\sigma}$ | (9, 3) |
| | 47 | 69 | $3^3$ | 2.23 | 3 | $p_3^{2+\sigma}$ | $3^3.29^3$ | $2^2.3.29$ | 7 | $p_3p_{29}$ | (9, 3) |
| 103.409 | 404 | 14 | $13^3$ | 499 | 7 | $p_{13}^{2+\sigma}$ | $7^3.31^3$ | 11.31.67 | 3.5 | $p_{31} \cdot p_7^{2+\sigma}$ | (9, 3)* |
| | 1 | 79 | $13^3$ | $2^3.7.13$ | 7 | $p_{13}$ | $13^3$ | $2^3.13$ | 1 | $p_{13}$ | (9, 3)* |
| 139.277 | 353 | 33 | $107^3$ | $3^2.7.173$ | $2^3.3$ | $p_{107}^{2+\sigma}$ | $89^3$ | 2.3.11.19.53 | $3^2.5$ | $p_{89}^{2+\sigma}$ | (9, 3) |
| | 245 | 59 | $5^3$ | 2.4987 | 17 | $p_5^{2+\sigma}$ | $7^6$ | 3.733 | $2^3$ | $p_7^{2(2+\sigma)}$ | (9, 3) |
| 139.373 | 244 | 74 | $2^6.23^3$ | $2^5.19.23$ | 19 | $p_2^{2+\sigma}p_{23}$ | $2^6.23^3$ | $2^5.13.23$ | 13 | $p_2^{2+\sigma}p_{23}$ | (9, 3)* |
| | 55 | 87 | $3^3.5^6$ | $5^3.7$ | $2^2$ | $p_3^{2+\sigma}p_5^{2+\sigma}$ | $5^6$ | 61 | 1 | $p_5^{2(2+\sigma)}$ | (9, 3) |
| 151.433 | 343 | 73 | $7^3.23^3$ | 13.4157 | 3.13 | $p_7^{2+\sigma}p_{23}^{2+\sigma}$ | $7^3.67^3$ | $2^2.5.67.73$ | $3^3$ | $p_7^{2+\sigma}p_{67}$ | (9, 3)* |
| | 305 | 79 | $67^3$ | $11^2.23$ | 5 | $p_{67}^{2+\sigma}$ | $5^3$ | 661 | 1 | $p_5^{2+\sigma}$ | (9, 3) |

TABLE 4

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

| | | | | | |
|---|---|---|---|---|---|
| 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 $Q(\sqrt{m})$..., *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 $\mathbf{Q}$; bases d'entiers (à paraître).

[14] H. HASSE, Über die Klassenzahl des Körpers $P(\sqrt{-p})$ mit einer Primzahl $p \equiv 1 \bmod 2^3$, *Aequationes math.* 3 (1969).

[15] H. HASSE, Über die Klassenzahl des Körpers $P(\sqrt{-2p})$ 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 imaginär-quadratischer 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 réciprocité 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 mathematik.*

[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. TAUSSKY, 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.