SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

NICOLE MOSER

Unités et nombre de classes d'une extension galoisienne diédrale de Q

Séminaire de théorie des nombres de Grenoble, tome 3 (1973-1974), exp. n° 4, p. 1-22

<http://www.numdam.org/item?id=STNG_1973-1974__3__A4_0>

Séminaire de Théorie des Nombres
15 novembre 1973 et 14 mars 1974
Grenoble

UNITES ET NOMBRE DE CLASSES D'UNE EXTENSION GALOISIENNE DIEDRALE DE $\mathbb{Q}$.

par Nicole MOSER

Soit G un groupe diédral d'ordre $2p$, p nombre premier impair. On se propose, en utilisant la classification des $\mathbb{Z}[G]$-modules donnée par M.P. Lee dans [13] et rappelée en [16] , d'étudier la structure de G-module des unités d'une extension diédrale $K/\mathbb{Q}$, et en particulier l'existence d'une unité de Minkowski. (Rappelons qu'une unité de Minkowski est telle que de l'ensemble de ses conjuguées, on puisse extraire un système d'unités fondamentales de K).

Cette étude met en évidence un indice a d'un sous-groupe d'unités, que l'on retrouve dans une formule liant le nombre de classes de K et ceux de ses sous-corps. L'utilisation simultanée de ces deux groupes de résultats permet de donner quelques exemples numériques lorsque $p = 3$.

I - GENERALITES.

1. Notations.

Pour tout corps de nombres Λ , nous poserons :

U_Λ : le groupe des unités de Λ .

V_Λ : le groupe des racines de l'unité contenues dans Λ .

E_Λ : le quotient U_Λ/V_Λ
h_Λ : le nombre de classes de Λ
D_Λ : le discriminant de $\Lambda/\mathbb{Q}$
R_Λ : le régulateur de Λ .

Nous réserverons la lettre K pour désigner une extension diédrale de $\mathbb{Q}$ de degré $2p$, p nombre premier impair, et la lettre G pour désigner un groupe diédral d'ordre $2p$. Le groupe G admet deux générateurs σ et τ , liés par les relations

$$\sigma^p = \tau^2 = 1$$
$$\tau\sigma = \sigma^{-1}\tau \quad .$$

Nous noterons k le sous-corps de K fixe par $H = \langle\sigma\rangle$, et L celui qui correspond à $g = \langle\tau\rangle$.

Enfin, nous désignerons par :

$\mathbb{Q}^{(p)}$: le p-ième corps cyclotomique
ζ : une racine primitive p-ième de l'unité
A : l'anneau des entiers de $\mathbb{Q}^{(p)}$
$\mathbb{Q}_o$: le sous-corps réel maximal de $\mathbb{Q}^{(p)}$
et A_o son anneau d'entiers.

2. Théorie de Galois pour le $\mathbb{Z}[G]$-module E_K .

PROPOSITION I.1. *Soit $K/\mathbb{Q}$ une extension diédrale de degré $2p$. Le sous-groupe de E_K fixe par τ (resp. σ) est E_L (resp. E_k) .*

Démonstration : Vérifions d'abord que tout élément de V_K est dans V_k . Soit ϵ un générateur de V_K , d'ordre m ; il existe un entier a tel que

$$\epsilon^\sigma = \epsilon^a \quad .$$

Comme $\sigma^p = 1$ et que $\tau\sigma\tau^{-1} = \sigma^{-1}$, on a les congruences modulo m :

$$a^p \equiv 1 \ (m)$$
$$a^2 \equiv 1 \ (m) \quad .$$

Donc a est congru à 1 modulo m , et ϵ appartient à k . Les racines de l'unité contenues dans K sont donc $+1$ et -1 , sauf si $k = \mathbb{Q}(i)$ ou $\mathbb{Q}(j)$.

Soit $\bar{\alpha}$ un élément de E_K fixe par τ : il est représenté par un élément α de U_K. Comme K est le composé des corps k et L, et que k est de la forme $\mathbb{Q}(\sqrt{m})$, où m est un entier sans facteur carré, α s'écrit :

$$\alpha = \sum_{\ell \in I} (a_\ell + b_\ell \sqrt{m}) c_\ell$$

où a_ℓ et b_ℓ sont des rationnels, et c_ℓ un élément de L.

$$\alpha^\tau = \sum_{\ell \in I} (a_\ell - b_\ell \sqrt{m}) c_\ell \quad .$$

Comme $\bar{\alpha}$ est fixe par τ, $\alpha^{\tau-1}$ est un élément de V_K. Distinguons alors les cas suivants :

1) $\alpha^{\tau-1} = 1$; alors $\alpha \in U_L$.

2) $\alpha^{\tau-1} = -1$.

Dans ce cas, $\sum_{\ell \in I} a_\ell c_\ell = 0$; l'élément $\lambda = \sum_{\ell \in I} b_\ell c_\ell$ appartient à L, et l'on a :

$$\alpha = \lambda \sqrt{m}$$
$$N_{K/L}\, \alpha = -\lambda^2 m \quad .$$

Si m est différent de -1, pour tout idéal premier $\mathfrak{p}$ de L qui divise m, on a :

$$0 = 2v_{\mathfrak{p}}(\lambda) + v_{\mathfrak{p}}(m) \quad .$$

Comme l'extension $L/\mathbb{Q}$ est de degré impair on peut choisir $\mathfrak{p}$ de sorte que $v_{\mathfrak{p}}(m)$ soit impaire, ce qui conduit à une contradiction.

Si $m = -1$, c'est-à-dire $k = \mathbb{Q}(i)$, $\beta = i\alpha$ appartient à U_L, donc $\bar{\beta} = \bar{\alpha}$ est un élément de E_L.

3) $\alpha^{\tau-1} = i$ ou $-i$.

On montre par un calcul analogue au précédent que

$$N_{K/L}\, \alpha = 2\lambda^2 \quad , \quad \lambda \in L \quad ,$$

donc ces cas sont à exclure.

4) $\alpha^{\tau-1} = j$ (resp j^2) .

Alors $\beta = j^2\alpha$ (resp $j\alpha$) appartient à U_L.

5) $\alpha^{\tau-1} = -j$ (resp $-j^2$) .

L'élément $\beta = j^2\alpha$ (resp $j\alpha$) vérifie

$$\beta^{\tau-1} = -1 ;$$

donc ce cas ne peut se présenter, d'après 2).

Pour démontrer la deuxième assertion de la proposition, choisissons maintenant un élément $\bar{\alpha}$ de E_L fixe par σ ; il est représenté dans U_L par un élément α tel que $\alpha^{\sigma-1}$ soit un élément ϵ de V_k , et l'on a :

$$\alpha^{(1+\sigma+\ldots+\sigma^{p-1})(\sigma-1)} = \epsilon^p = 1 .$$

Ceci implique $\epsilon = 1$, sauf peut-être si $k = \mathbb{Q}(j)$, et $p = 3$.

Supposons donc que $p = 3$ et $k = \mathbb{Q}(j)$, et soit α un élément de U_K tel que

$$\alpha^{\sigma} = \pm j\alpha \quad \text{ou} \quad \pm j^2\alpha .$$

C'est un élément primitif de $K/\mathbb{Q}(j)$.

$$N_{K/k}\,\alpha = \alpha^{1+\sigma+\sigma^2} = \alpha^3 .$$

Donc α^3 est une unité de $\mathbb{Q}(j)$; les seules unités de $\mathbb{Q}(j)$ sont les racines de l'unité. Si α^3 valait ± 1 , K serait identique à $\mathbb{Q}(j)$. Si α^3 valait $\pm j$ ou $\pm j^2$, K serait le corps cyclotomique $\mathbb{Q}^{(9)}$, qui est abélien sur $\mathbb{Q}$. Donc tous les éléments α de U_K vérifient :

$$\alpha^{\sigma} = \pm\alpha .$$

Comme $\alpha^{\sigma-1}$ est de norme 1 sur $\mathbb{Q}(j)$, le cas $\alpha^{\sigma-1} = -1$ est à exclure, et α est un élément de U_k . ∎

3. Sur les extensions galoisiennes totalement réelles de $\mathbb{Q}$.

Soit $\Lambda/\mathbb{Q}$ une extension galoisienne, totalement réelle, de degré n , de groupe de Galois Γ . Le théorème de Dirichlet sur les unités montre que E_Λ est un $\mathbb{Z}$-module libre de rang $n-1$. Posons $T = \sum_{s\in\Gamma} s$; le $\mathbb{Z}[\Gamma]$-module E_Λ , annulé par T , est en fait un $\mathbb{Z}[\Gamma]/T\mathbb{Z}[\Gamma]$-module, et la proposition suivante est immédiate :

PROPOSITION I.2. Les deux assertions suivantes sont équivalentes :

i) E_Λ est un module sur $\mathbb{Z}[\Gamma]$ monogène.

ii) E_Λ est $\mathbb{Z}[\Gamma]$-isomorphe à $R = \mathbb{Z}[\Gamma]/T\mathbb{Z}[\Gamma]$.

Considérons maintenant un sous-groupe γ de Γ , et pour tout Γ-module M , posons :

$$M^\gamma = \{a \in M \mid a^s = a \quad \text{pour tout} \quad s \in \gamma\}$$
$$T_\gamma = \sum_{s\in\gamma} s \quad .$$

PROPOSITION I.3. Si $R = \mathbb{Z}[\Gamma]/T\mathbb{Z}[\Gamma]$,

$$R^\gamma = T_\gamma R \quad .$$

Démonstration : (due à J.M. Fontaine). Considérons la suite exacte de γ-modules :

$$0 \to T\mathbb{Z}[\Gamma] \to \mathbb{Z}[\Gamma] \to R \to 0 \quad .$$

Il est clair que l'application $z \to zT$ est un isomorphisme de $\mathbb{Z}[\Gamma]$-modules de $\mathbb{Z}$ sur $T\mathbb{Z}[\Gamma]$. On en déduit la suite exacte courte :

$$0 \to \mathbb{Z} \to \mathbb{Z}[\Gamma] \to R \to 0 \ ,$$

et la suite exacte de cohomologie modifiée à la Tate :

$$\ldots \to \hat{H}^\circ(\gamma, \mathbb{Z}[\Gamma]) \to \hat{H}^\circ(\gamma, R) \to H^1(\gamma, \mathbb{Z}) \to \ldots \quad .$$

Or $\mathbb{Z}[\Gamma]$ est un $\mathbb{Z}[\gamma]$-module projectif, donc

$$\hat{H}^\circ(\gamma, \mathbb{Z}[\Gamma]) = 0 \ .$$

D'autre part, $H^1(\gamma, \mathbb{Z}) = \mathrm{Hom}(\gamma, \mathbb{Z}) = 0$. Donc $\hat{H}^\circ(\gamma, R) = 0$, et par définition des groupes de cohomologie modifiée, $R^\gamma = T_\gamma R$. ∎

Le corollaire suivant s'en déduit immédiatement.

COROLLAIRE. Soit Λ/Φ une extension galoisienne totalement réelle, admettant une unité de Minkowski η . Soit Λ' une extension intermédiaire, associée au sous-groupe γ de $\mathrm{Gal}(\Lambda/\Phi)$. Le sous-groupe de E_Λ fixe par γ est $E_{\Lambda'}$, et l'on a : $N_{\Lambda/\Lambda'} E_\Lambda = E_{\Lambda'}$; (en effet, $N_{\Lambda/\Lambda'} E_\Lambda \subset E_{\Lambda'}$) .

Si, de plus Λ'/Φ est galoisienne, Λ' admet $N_{\Lambda/\Lambda'}\eta$ comme unité de Minkowski.

II - $\mathbb{Z}[G]$-MODULE DES UNITES D'UNE EXTENSION DIEDRALE IMAGINAIRE.

D'après le théorème de Dirichlet, sur les unités, E_K est un $\mathbb{Z}$-module de rang $p-1$, et E_k est un $\mathbb{Z}$-module de rang 0. Donc tout élément de E_K a pour norme 1 sur E_k, et le $\mathbb{Z}[G]$-module E_K est un module sur A. Utilisons la classification des modules sur l'algèbre d'un groupe diédral (cf. [15] et [16], th. III) pour énoncer :

PROPOSITION II.1. *E_K est $\mathbb{Z}[G]$-isomorphe à un idéal de A de la forme $(1-\zeta)^{\epsilon}\mathfrak{a}A$, où $\mathfrak{a}$ est un idéal de A_o, et où ϵ vaut 0 ou 1.*

DEFINITION II.1. Nous dirons que E_K est de *type α* s'il est $\mathbb{Z}[G]$-isomorphe à un idéal de la forme $\mathfrak{a}A$, et de *type β* dans l'autre cas.

Pour que E_K soit $\mathbb{Z}[G]$-monogène, il faut et il suffit que la classe dans A de l'idéal $\mathfrak{a}$ que lui associe la proposition II.1 soit la classe principale. En particulier :

PROPOSITION II.2. *Soit $K/\mathbb{Q}$ une extension diédrale imaginaire de degré $2p$. Si A_o est principal, K admet une unité de Minkowski.*

(On sait que A_o est principal pour tout nombre premier inférieur ou égal à 23).

Démonstration : Si A_o est principal, E_K est $\mathbb{Z}[G]$-monogène ; soit η un de ses générateurs. Pour le type α, η vérifie $\eta^{\tau} = \eta$, et pour le type β, $\eta^{\tau} = \eta^{-1}$; donc un représentant de η dans U_K est une unité de Minkowski de K. ∎

Parmi les sous $\mathbb{Z}[G]$-modules de E_K de $\mathbb{Z}$-rang $\frac{p-1}{2}$ figurent les modules $E_{L^{\sigma^r}}$. Deux corps L^{σ^r} et L^{σ^s} distincts, (r et s sont des éléments de $\mathbb{Z}/p\mathbb{Z}$), de degré premier sur $\mathbb{Q}$, ont une intersection

réduite à $\mathbb{Q}$; donc $E_{L^{\sigma r}} \cdot E_{L^{\sigma s}}$ est un sous $\mathbb{Z}[G]$-module d'indice fini dans E_K. Enonçons les résultats suivants, valables pour deux conjugués distincts quelconques de L , avec L et L^σ .

PROPOSITION II.3. Soit $K/\mathbb{Q}$ une extension diédrale imaginaire de degré $2p$. Posons $a = (E_K : E_L E_{L^\sigma})$. L'indice a vaut 1 si E_K est de type α , et p si E_K est de type β .

Démonstration : Les éléments 1 et ζ constituent une A_o-base de A . Si E_K est de type α , il est isomorphe à un idéal $\mathfrak{a}A$, donc encore à la somme directe $\mathfrak{a} \oplus \mathfrak{a}\zeta$. Compte tenu de la proposition I.1, l'image de E_K par cet isomorphisme est la partie de $\mathfrak{a}A$ fixe par τ ; c'est donc $\mathfrak{a}$. Par définition de l'action de σ sur A , l'image de E_{K^σ} est $\zeta\mathfrak{a}$, d'où l'égalité :

$$E_K = E_L . E_{L^\sigma} \quad .$$

Si E_K est de type β , il est isomorphe à $(1-\zeta)\mathfrak{a}A$, où $\mathfrak{a}$ est un idéal de A_o . Désignons par $\mathfrak{p}$ l'idéal premier de A_o au-dessus de p . Dans ce cas, la partie de $(1-\zeta)\mathfrak{a}A$ fixe par τ est $\mathfrak{p}\mathfrak{a}$, donc l'image de E_L est égale à $\mathfrak{p}\mathfrak{a}$, et celle de E_{L^σ} à $\zeta\mathfrak{p}\mathfrak{a}$. Le module $E_L . E_{L^\sigma}$ est isomorphe à $\mathfrak{p}\mathfrak{a}A$, et

$$(E_K : E_L E_{L^\sigma}) = ((1-\zeta)\mathfrak{a}A : \mathfrak{p}\mathfrak{a}A) = p \quad . \qquad \blacksquare$$

PROPOSITION II.4. Soit $K/\mathbb{Q}$ une extension diédrale imaginaire de degré $2p$. L'application norme $N_{K/L} : E_K \to E_L$ est surjective.

Démonstration : Le module $N_{K/L} E_K$ est $\mathbb{Z}[G]$-isomorphe à $\mathrm{Tr}_{\mathbb{Q}(p)/\mathbb{Q}_o} (1-\zeta)^\epsilon \mathfrak{a}A$. Comme l'extension $\mathbb{Q}(p)/\mathbb{Q}_o$ est modérément ramifiée, la trace de A sur A_o est surjective (cf. J. Martinet [13]), et

$$\mathrm{Tr}_{\mathbb{Q}(p)/\mathbb{Q}_o} (1-\zeta)^\epsilon \mathfrak{a}A = [(1-\zeta)^\epsilon \mathfrak{a}A] \cap A_o = \mathfrak{p}^\epsilon \mathfrak{a} \quad .$$

Donc $E_L = N_{K/L} E_K$. $\blacksquare$

Remarque : Si l'on se restreint aux unités totalement positives, on a $U_L^+ = N_{K/L} U_K^+$.

III - $\mathbb{Z}[G]$-MODULE DES UNITES D'UNE EXTENSION DIEDRALE REELLE.

Pour appliquer les résultats sur la classification des $\mathbb{Z}[G]$-modules, mettons en évidence l'ensemble E'_K des éléments de E_K de norme 1 sur E_k ; c'est un $\mathbb{Z}$-module de rang $2p-2$; il est donc isomorphe à $(1-\zeta)^{\varepsilon_1}\mathfrak{a}A \oplus (1-\zeta)^{\varepsilon_2}\mathfrak{b}A$, où $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux de A_o . Le quotient $E_K/E_{K'}$ est un $\mathbb{Z}$-module de rang 1 , sur lequel τ n'opère pas trivialement, donc c'est un $\mathbb{Z}[G]$-module isomorphe à S_2 . Tout $\mathbb{Z}[G]$-module est somme directe de $\mathbb{Z}[G]$-modules indécomposables ; d'après ([13] et [16], th. III), cinq cas sont possibles :

$\alpha)$ $E_K \simeq \mathfrak{a}A \oplus \mathfrak{b}A \oplus S_2$

$\beta)$ $E_K \simeq (1-\zeta)\mathfrak{a}A \oplus \mathfrak{b}A \oplus S_2$

$\gamma)$ $E_K \simeq (1-\zeta)\mathfrak{a}A \oplus (1-\zeta)\mathfrak{b}A \oplus S_2$

$\delta)$ $E_K \simeq \mathfrak{a}A \oplus (\mathfrak{b}A, S_2)$

$\varepsilon)$ $E_K \simeq (1-\zeta)\mathfrak{a}A \oplus (\mathfrak{b}A, S_2)$.

Ces cinq modules ne sont pas $\mathbb{Z}[G]$-isomorphes : en effet, le théorème de Krull-Schmidt est valable pour les $\mathbb{Z}_{(p)}[G]$-modules, et d'après ([13] et [16], § V), les localisés en p de ces modules ne sont pas $\mathbb{Z}_{(p)}[G]$-isomorphes.

PROPOSITION III.1. Posons $a = (E_K : E_L E_L{}^{\sigma} E_k)$, et $b = (E_k : N_{K/k}E_K)$. Les cinq cas ci-dessus sont caractérisés par :

$\alpha)$ $a = 1$, $b = p$

$\beta)$ $a = p$, $b = p$

$\gamma)$ $a = p^2$, $b = p$

$\delta)$ $a = p$, $b = 1$

$\varepsilon)$ $a = p^2$, $b = 1$.

Dans tous les cas, $N_{K/L}E_K = E_L$.

Démonstration : Posons $\mathfrak{p} = [(1-\zeta)A] \cap A_o$. L'image de E_L par le $\mathbb{Z}[G]$-isomorphisme de E_K sur l'un des modules définis ci-dessus est égale

à :

$$[(1-\zeta)^{\varepsilon_1}A \oplus (1-\zeta)^{\varepsilon_2}\mathfrak{b}A] \cap A_o = \mathfrak{p}^{\varepsilon_1}\mathfrak{a} \oplus \mathfrak{p}^{\varepsilon_2}\mathfrak{b} .$$

Donc le conjugué E_{L^σ} de E_L est $\mathbb{Z}[G]$-isomorphe à $\zeta\mathfrak{p}^{\varepsilon_1}\mathfrak{a} \oplus \zeta\mathfrak{p}^{\varepsilon_2}\mathfrak{b}$.

Dans les cas α , β et γ , le sous-groupe de E_K fixe par σ , E_k , est $\mathbb{Z}[G]$-isomorphe à S_2 ; donc $E_L E_{L^\sigma} E_k$ est $\mathbb{Z}[G]$-isomorphe à $\mathfrak{p}^{\varepsilon_1}\mathfrak{a}A \oplus \mathfrak{p}^{\varepsilon_2}\mathfrak{b}A \oplus S_2$, et

$$a = (E_K : E_L E_{L^\sigma} E_k) = p^{\varepsilon_1+\varepsilon_2} .$$

Dans les cas δ et ε , l'action de σ sur $(\mathfrak{b}A, S_2)$ est définie par la formule :

$$\sigma(x,y) = (\zeta x + yn_o, y)$$

avec $y \in S_2$, $x \in \mathfrak{b}A$, $n_o \in \mathfrak{b}A \setminus (1-\zeta)\mathfrak{b}A$. (cf. [13] et [16]). Les éléments (x,y) fixes par σ vérifient donc :

$$\zeta x + yn_o = x .$$

Comme n_o n'appartient pas à $(\zeta-1)\mathfrak{b}A$, il faut choisir y dans $S_2 \cap (\zeta-1)A = pS_2$, et E_k est isomorphe à pS_2 . Pour le calcul de l'indice a , il suffit de considérer la structure de $\mathbb{Z}$-module de E_K , et l'on obtient :

$$a = p^{1+\varepsilon_1} .$$

Pour le calcul de b , dans les cas α , β et γ , on remarque que $N_{K/k}E_k$ est isomorphe à pS_2 , et que $N_{K/k}E'_K = 1$. Donc $N_{K/k}E_K$, isomorphe à pS_2 , est égale à E_k^p . D'après la proposition I.3, le $\mathbb{Z}[G]$-module $R = \mathbb{Z}[G]/T\mathbb{Z}[G]$, où $T = \sum_{s\in G} s$, est du type δ ou ε ; dans ces deux cas, les normes se calculent de la même façon, donc $b = 1$.

Enfin, pour calculer $N_{K/L}E_K$, remarquons que :

$$(1+\tau)S_2 = 0$$

$$(1+\tau)(1-\zeta)^{\varepsilon}\mathfrak{a}A = \mathfrak{p}^{\varepsilon}\mathfrak{a} .$$

Si (x,y) appartient à $(\mathfrak{b}A,S_2)$, d'après [16],

$$\tau(x,y) = (\bar{x}+\frac{y}{\bar{\zeta}-1}(\bar{n}_o-\bar{\zeta}_{n_o}),-y) \ .$$

Comme l'extension $\mathbb{Q}^{(p)}/\mathbb{Q}_o$ est modérément ramifiée, on en déduit que :

$$(1+\tau)(\mathfrak{b}A,S_2) = \mathfrak{b} \ .$$

D'où : $$N_{K/L}E_K = E_L \quad . \blacksquare$$

Remarque : Comme dans le cas imaginaire, on peut remplacer L et L^σ par deux conjugués distincts quelconques de L .

PROPOSITION III.2. *Le $\mathbb{Z}[G]$-module $R = \mathbb{Z}[G]/T\mathbb{Z}[G]$, où T désigne $\sum_{s\in G} s$, est de type δ .*

Démonstration : Dans R , tout élément fixe par τ (resp. $\sigma\tau$, resp. σ), est représenté par un élément de $\mathbb{Z}[G]$ de la forme $(1+\tau)\sum_{i=0}^{p-1} a_i\sigma^i$ (resp. $(1+\sigma\tau)\sum_{0}^{p-1} a_i\sigma^i$, resp. $(1+\sigma+\ldots+\sigma^{p-1})(a_o+b_o\tau)$) . Pour qu'un élément $\sum(a_i+b_i\tau)\sigma^i$ de R se décompose en somme de trois éléments fixes respectivement par σ , τ et $\sigma\tau$, il faut et il suffit qu'il s'écrive :

$$\sum_{i=0}^{p-1}(a_i+b_i\tau)\sigma^i = (1+\tau)\sum_i \alpha_i\sigma^i + (1+\sigma\tau)\sum_i \beta_i\sigma^i + (\gamma+\delta\tau)(1+\sigma+\ldots+\sigma^{p-1}) \ .$$

Par identification, on obtient la condition nécessaire et suffisante :

$$\sum_i a_i - \sum_i b_i = p(\gamma-\delta) \ .$$

Donc l'indice a correspondant à R vaut p . La proposition I.3 donne $b = 1$. $\blacksquare$

PROPOSITION III.3. *Si A_o est principal, et si E_K est de type δ , K admet une unité de Minkowski.*

Démonstration : D'après [13] et [16], si A_o est principal, tous les $\mathbb{Z}[G]$-modules de type δ sont isomorphes ; en particulier, ils sont $\mathbb{Z}[G]$-isomorphes à R . Lorsque A_o est principal, et que E_K est de type δ ,

K admet donc une unité de Minkowski, d'après le corollaire de la proposition I.3.

IV - REGULATEUR ET NOMBRE DE CLASSES D'UNE EXTENSION DIEDRALE.

Il existe une formule liant les régulateurs et les nombres de classes des corps K , L et k :

$$h_K = \frac{R_L^2 R_k}{R_K} h_L^2 h_k \ .$$

On peut l'obtenir directement en utilisant les résultats de R. Brauer ([4], Satz 3). Ou bien l'on peut partir de la formule analytique du nombre de classes (cf. [3]) et comparer les fonctions "zêta" des corps K , L et k , grâce au tableau de décomposition des idéaux premiers dans une extension diédrale, qui figure dans [14].

Pour comparer les régulateurs, il nous faut distinguer deux cas :

1) $K/\mathbb{Q}$ <u>totalement réelle</u>.

Désignons par $\{\varepsilon_1, \ldots, \varepsilon_{p-1}\}$ un système d'unités fondamentales de L , et par u une unité fondamentale de k . Notons R^* le régulateur du système d'unités

$$\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{p-1}, \varepsilon_1^{\sigma}, \ldots, \varepsilon_{p-1}^{\sigma}, u\} \ .$$

Si $a = (E_K : E_L E_{L^{\sigma}} E_k)$, par définition du régulateur du corps K , on a :

$$a R_K = R^* \ .$$

Le régulateur R^* est la valeur absolue d'un mineur quelconque d'ordre 2p-1 de la matrice suivante (cf. [3]) :

$$\begin{bmatrix}
\log|\varepsilon_1| & \log|\varepsilon_1^{\sigma}| & \dots & \log|\varepsilon_1^{\sigma^{p-1}}| & \log|\varepsilon_1^{\tau}| & \dots\dots & \log|\varepsilon_1^{\sigma^{p-1}\tau}| \\
\vdots & \vdots & & \vdots & \vdots & & \\
\log|\varepsilon_{p-1}| & \log|\varepsilon_{p-1}^{\sigma}| & \dots & \log|\varepsilon_{p-1}^{\sigma^{p-1}}| & \log|\varepsilon_{p-1}^{\tau}| & \dots\dots & \log|\varepsilon_{p-1}^{\sigma^{p-1}\tau}| \\
\log|\varepsilon_1^{\sigma}| & \log|\varepsilon_1^{\sigma^2}| & \dots & \log|\varepsilon_1| & \log|\varepsilon_1^{\tau\sigma}| & \dots\dots & \log|\varepsilon_1^{\sigma^{p-1}\tau\sigma}| \\
\vdots & \vdots & & \vdots & \vdots & & \vdots \\
\log|\varepsilon_{p-1}^{\sigma}| & \log|\varepsilon_{p-1}^{\sigma^2}| & \dots & \log|\varepsilon_{p-1}| & \log|\varepsilon_{p-1}^{\tau\sigma}| & \dots\dots & \log|\varepsilon_{p-1}^{\sigma^{p-1}\tau\sigma}| \\
\log|u| & \log|u^{\sigma}| & \dots & \log|u^{\sigma^{p-1}}| & \log|u^{\tau}| & \dots\dots & \log|u^{\sigma^{p-1}\tau}|
\end{bmatrix}$$

Remarquons que u est fixe par σ, tandis que les ε_i sont fixes par τ.

Notons E_i la colonne $\begin{pmatrix} \log|\varepsilon_1^{\sigma^i}| \\ \vdots \\ \log|\varepsilon_{p-1}^{\sigma^i}| \end{pmatrix}$.

En supprimant la p-ième colonne, on obtient :

$$R^* = \left| \det \begin{bmatrix}
E_o & E_1 & \dots & E_{p-2} & E_o & \dots & E_{p-1} \\
E_1 & E_2 & \dots & E_{p-1} & E_{p-1} & \dots & E_{p-2} \\
\log|u| & \log|u| & \dots & \log|u| & \log|u^{\tau}| & \dots & \log|u^{\tau}|
\end{bmatrix} \right|$$

Additionnons les colonnes d'indices congrus molulo p .

$$R^* = \left| \log|u^{\tau}| \det \begin{bmatrix}
E_o+E_1 & \dots & E_{p-2}+E_{p-1} & E_o & \dots & E_{p-1} \\
E_1+E_o & \dots & E_{p-1}+E_{p-2} & E_{p-1} & \dots & E_{p-2} \\
0 & \dots & 0 & 1 & \dots & 1
\end{bmatrix} \right|$$

D'où :

$$R^* = \left| \log|u| \det\left[E_o+E_1,\dots,E_{p-2}+E_{p-1}\right] \det \begin{bmatrix} E_{p-1}-E_o,\dots,E_{p-2}-E_{p-1} \\ 1 \quad \dots \quad 1 \end{bmatrix} \right|$$

Développons en remarquant que $|\log|u||$ est égal à R_k, que $\sum_{i=0}^{p-1} E_i = (0)$, et que $R_L = |\det[E_o,E_1,\dots,E_{p-2}]|$. Il vient $R^* = p^2 R_L^2 R_k = aR_K$.

2) $K/\mathbb{Q}$ imaginaire.

Posons $q = \frac{p-1}{2}$, et soit $\{\varepsilon_1,\dots,\varepsilon_q\}$ un système d'unités fondamentales de L. Si l'on désigne par R^* le régulateur du système d'unités

$\{\varepsilon_1,\ldots,\varepsilon_q,\varepsilon_1^\sigma,\ldots,\varepsilon_q^\sigma\}$, et si l'on pose $a = (E_K : E_L E_{L^\sigma})$, on a l'égalité :

$$R^* = aR_K \ .$$

R^* est la valeur absolue d'un des mineurs d'ordre $p-1$ de la matrice :

$$\begin{bmatrix} \log|\varepsilon_1|^2 & \log|\varepsilon_1^\sigma|^2 \ \ldots\ldots & \log|\varepsilon_1^{\sigma^{p-1}}|^2 \\ \vdots & \vdots & \vdots \\ \log|\varepsilon_q|^2 & \log|\varepsilon_q^\sigma|^2 \ \ldots\ldots & \log|\varepsilon_q^{\sigma^{p-1}}|^2 \\ \log|\varepsilon_1^\sigma|^2 & \log|\varepsilon_1^{\sigma^2}|^2 \ \ldots\ldots & \log|\varepsilon_1|^2 \\ \vdots & \vdots & \vdots \\ \log|\varepsilon_q^\sigma|^2 & \log|\varepsilon_q^{\sigma^2}|^2 \ \ldots\ldots & \log|\varepsilon_q|^2 \end{bmatrix}$$

(En effet, τ est la restriction à K de la conjugaison complexe). Comme l'indice a ne dépend pas du couple de conjugués de L choisi, et que L admet un plongement réel, on peut supposer les ε_i réels. Les paires d'isomorphismes conjugués de L sont σ^i et $\tau\sigma^i = \sigma^{p-i}\tau$; de plus U_L est fixe par τ . Si l'on pose $E_i = \begin{pmatrix} \log|\varepsilon_1^{\sigma^i}| \\ \vdots \\ \log|\varepsilon_q^{\sigma^i}| \end{pmatrix}$ la matrice s'écrit :

$$\begin{bmatrix} 2E_o & 2E_1 \ \ldots\ 2E_q & 2E_q \ \ldots & 2E_1 \\ 2E_1 & 2E_2 \ \ldots\ 2E_o & \ldots\ldots & 2E_o \end{bmatrix}$$

Supprimons la q-ième colonne pour obtenir l'égalité :

$$R^* = \left| \det \begin{bmatrix} 2E_o \ \ldots\ 2E_{q-1} & 2E_q & \ldots\ 2E_1 \\ 2E_1 \ \ldots\ 2E_q & 2E_{q-1} & \ldots\ 2E_o \end{bmatrix} \right|$$

Des combinaisons de colonnes, puis de lignes, donnent :

$$R^* = |\det [\, 2E_o+2E_1,\ldots,2E_{q-1}+2E_q\,] \times \det [\, 2E_{q-1}-2E_q,\ldots,2E_o-2E_1\,]| \ .$$

Développons en remarquant que :

$$R_L = |\det [E_o, 2E_1,\ldots,2E_{q-1}]| \ ,$$

et que :

$$E_o+2E_1+\ldots+2E_q = 0 \ .$$

Il vient :

$$R^* = pR_L^2 = aR_K .$$

Dans ce cas, $R_k = 1$.

Rassemblons ces résultats dans l'énoncé suivant :

THEOREME IV.1. Soit $K/\mathbb{Q}$ une extension diédrale de degré $2p$, p nombre premier impair. Posons $a = (E_K : E_L E_{L\sigma} E_k)$. Alors :

$$h_K = a \frac{h_L^2 h_k}{p^r} ,$$

où r vaut 1 si K est imaginaire, et 2 si K est réelle.

Remarque : Ce résultat généralise celui donné par Ishida [9(12)], lorsque $p = 3$ et K imaginaire. D'autre part, Barrucand et Cohn [1] signalent cette formule comme conséquence des travaux de Hasse et C. Meyer [15], lorsque K est du type $\mathbb{Q}(j, \sqrt[3]{m})$.

V - RESULTATS NUMERIQUES, POUR $p = 3$.

1) $K/\mathbb{Q}$ imaginaire.

D'après le théorème IV.1., pour que a soit égal à 3 , il suffit que les nombres de classes h_k et h_L soient premiers à 3 . D'après les tables de [2] et de [3], cette condition est vérifiée pour les corps de décomposition des polynômes suivants :

α) $X^3 + X^2 + X - 1$

$D_L = -44$; $h_L = 1$; $D_k = -11$; $h_k = 1$.
Donc $h_K = 1$.

β) $X^3 + 3X - 1$

$D_L = -135$; $h_L = 1$; $D_k = -15$; $h_k = 2$.
Donc $h_K = 2$.

Pour illustrer le cas $a = 1$, utilisons le théorème 1 de Ishida [9]. Il s'énonce ainsi :

THEOREME. Soit $L = \mathbb{Q}(\eta)$ le corps cubique engendré par une racine η de l'équation :

$$X^3 + \ell X - 1 = 0 \qquad (\ell \in \mathbb{Z} \ , \ \ell \geq 2) \ .$$

Soit K le corps de décomposition de cette équation. Si $4\ell^3 + 27$ est sans facteur carré, ou si $\ell = 3m$ et $4m^3 + 1$ est sans facteur carré, η est l'unité fondamentale de L . Si de plus ℓ est pair, deux racines de l'équation constituent un système fondamental d'unités de K .

α) $\ell = 2$; $4\ell^3 + 27 = 59$, donc $a = 1$.

D'où : $D_L = -59$; $h_L = 1$

$D_k = -59$; $h_k = 3$ et $h_K = 1$.

β) $\ell = 4$; $4\ell^3 + 27 = 283$, et $a = 1$.

Donc : $D_L = -283$; $h_L = 2$

$D_k = -283$; $h_k = 3$ et $h_K = 4$.

2) $K/\mathbb{Q}$ <u>réel</u>.

Nous allons illustrer les cas γ , δ et ϵ , grâce aux théorèmes suivants :

THEOREME A [5] : Soient K une extension cyclique de degré p premier impair d'un corps de nombres k , $h_{k,p}$ la p-participation au nombre de classes de k , et t le nombre d'idéaux premiers de k ramifiés dans K . Alors le p-groupe des classes ambiges est d'ordre :

$$\frac{h_{k,p} \times p^{t-1}}{(U_k : U_k \cap N_{K/k} K^*)} \ .$$

THEOREME B [12] : Soit K une extension cyclique de degré premier impair d'un corps de nombres k , ramifiée en une place finie au plus. Alors :

$$U_k = N_{K/k} U_K \ .$$

THEOREME C [11] : Si k est un corps de nombres dont le p-groupe des classes est cyclique d'ordre p, la p-tour des corps de classes de k est de longueur 1. Donc si K est le p-corps de classes de k, p ne divise pas h_K.

THEOREME D [10] : Soient k un corps de nombres, et K une extension galoisienne finie de k. S'il existe un idéal premier $\mathfrak{p}$ de k totalement ramifié dans K/k, le nombre de classes de K est divisible par le nombre de classes de k.

Cherchons d'abord des exemples des types γ et ε, pour lesquels $a = 9$ d'après la proposition III.1. D'après le théorème IV.1., pour que a soit égal à 9, il suffit que h_L et h_k soient premiers à 3. Ceci est réalisé dans les deux cas suivants :

1er cas : K est le corps de décomposition du polynôme $X^3 - X^2 - 3X + 1$. On a : $D_L = 148$; $D_k = 37$.

D'après les tables de [3], $h_L = h_k = 1$, et le théorème IV.1. donne :

$$a = 9 \quad \text{et} \quad h_K = 1 .$$

Calculons l'indice b : le discriminant de l'extension K/k est égal à 2^2 ; comme 2 est inerte dans $k/\mathbb{Q}$, il n'y a qu'un idéal ramifié dans l'extension K/k. Le théorème B permet de conclure que $b = 1$, donc le corps étudié est de type ε.

2e cas : K est le corps de décomposition du polynôme $X^3 - 6X + 2$. On a :

$$D_L = 756 \quad ; \quad D_k = 21 \quad ; \quad h_L = h_k = 1 .$$

D'après le théorème IV.1, $h_K = 1$ et $a = 9$. Calculons l'indice b : le discriminant de K/k vaut $2^2.3^2$; 3 est ramifié dans l'extension $k/\mathbb{Q}$, tandis que 2 est inerte, donc il y a deux idéaux ramifiés dans K/k. D'après le théorème A, le nombre de classes ambiges de K/k est égal à

$$\frac{3}{(U_k : U_k \cap N_{K/k}K^*)} .$$

Comme ce nombre divise h_K , il doit être égal à 1 , donc $b = 3$, et le corps étudié est de type γ .

3e cas : Remarquons d'abord que lorsque $h_k = 3$, et que $D_L = D_k$, l'extension K/k est non ramifiée. D'après le théorème B, b vaut 1 , et d'après le théorème C, 3 ne divise pas h_K . Dans ce cas se trouve le corps de décomposition du polynôme :

$$X^3 - X^2 - 9X + 12 .$$

$D_L = D_k = 1101$; $h_L = 1$; $h_k = 3$.

D'après la remarque précédente, et le théorème IV.1, $h_K = 1$, d'où $a = 3$. Donc ce corps est de type δ .

D'après la table ci-dessous, si l'on considère tous les corps L de discriminant inférieur à 1500 , les corps K correspondant sont de type γ , δ ou ε .

Table donnant le nombre de classes et le type de la clôture galoisienne des corps cubiques réels non galoisiens de discriminant < 1 500

Polynôme définissant L	D_L	D_k	h_L	h_k	nbre d'idéaux ramifiés dans K/k	a	b	h_L	Type	Nature de la justification
X^3-X^2-3X+1	$2^2.37$	37	1	1	1	9	1	1	ϵ	Th B + Th IV. 1.
X^3-4X-1	229	229	1	3	0	3	1	1	δ	Th B + Th C + Th IV. 1.
X^3-X^2-4X+3	257	257	1	3	0	3	1	1	δ	id.
X^3-X^2-4X+2	$2^2.79$	$2^2.79$	1	3	0	3	1	1	δ	Th B + Th C + Th IV. 1.
X^3-X^2-4X+1	321	321	1	3	0	3	1	1	δ	Th B + Th C + Th IV. 1.
X^3-X^2-5X-1	$2^2.101$	101	1	1	1	9	1	1	ϵ	Th B + Th IV. 1.
X^3-X^2-5X+4	469	469	1	3	0	3	1	1	δ	Th B + Th C + Th IV. 1.
X^3-5X-1	473	473	1	3	0	3	1	1	δ	id.
X^3-X^2-5X+3	$2^2.141$	141	1	1	1	9	1	1	ϵ	Th B + Th IV. 1.
X^3-X^2-6X-2	$2^2.142$	$2^2.142$	1	3	0	3	1	1	δ	Th B + Th C + Th IV. 1.
X^3-6X+3	$3^2.69$	69	1	1	1	9	1	1	ϵ	Th B + Th IV. 1.
X^3-7X+5	697	697	1	6	0	3	1	2	δ	Th B + Th C + Th IV. 1.
X^3-X^2-7X+8	733	733	1	3	0	3	1	1	δ	Th B + Th C + Th IV. 1.

$X^3 - 6X + 2$	$6^2 . 21$	21	1	1	2	9	3	1	γ	Th A + Th IV. 1.
$X^3 - X^2 - 6X + 1$	761	761	1	3	0	3	1	1	δ	Th B + Th C + Th IV. 1.
$X^3 - X^2 - 6X + 5$	785	785	1	6	0	3	1	2	δ	Th B + Th C + Th IV. 1.
$X^3 - X^2 - 7X - 3$	$2^2 . 197$	197	1	1	1	9	1	1	ε	Th B + Th IV. 1.
$X^3 - 6X - 1$	$3^2 . 93$	93	1	1	1	9	1	1	ε	id.
$X^3 - X^2 - 8X + 10$	$2^2 . 223$	$2^2 . 223$	1	3	0	3	1	1	δ	Th B + Th C + Th IV. 1.
$X^3 - X^2 - 6X + 4$	$2^2 . 229$	229	1	3	1	9	1	3	ε	Th B + Th D + Th IV. 1.
$X^3 - 7X - 4$	$2^2 . 235$	$2^2 . 235$	1	6	0	3	1	2	δ	Th B + Th C + Th IV. 1.
$X^3 - X^2 - 6X + 1$	985	985	1	6	0	3	1	2	δ	Th B + Th C + Th IV. 1.
$X^3 - X^2 - 6X + 3$	993	993	1	3	0	3	1	1	δ	id.
$X^3 - X^2 - 6X + 2$	$2^2 . 254$	$2^2 . 254$	1	3	0	3	1	1	δ	Th B + Th C + Th IV. 1.
$X^3 - 8X - 6$	$2^2 . 269$	269	1	1	1	9	1	1	ε	id.
$X^3 - X^2 - 9X + 12$	1101	1101	1	3	0	3	1	1	δ	Th B + Th C + Th IV. 1.
$X^3 - 7X - 3$	1129	1129	1	9	0	9	1	9	ε	Th B + (1)
$X^3 - X^2 - 9X + 6$	1229	1229	1	3	0	3	1	1	δ	Th B + Th C + Th IV. 1.
$X^3 - X^2 - 8X + 9$	1257	1257	1	3	0	3	1	1	δ	id.
$X^3 - 11X + 2$	$2^2 . 326$	$2^2 . 326$	1	3	0	3	1	1	δ	Th B + Th C + Th IV. 1.

$X^3 - 7X + 1$	1345	1345	1	6	0	3	1	2	δ	Th B + Th C + Th IV. 1.
$X^3 - 8X + 5$	1373	1373	1	3	0	3	1	1	δ	id.
$X^3 - X^2 - 10X + 14$	$2^2.346$	$2^2.346$	1	6	0	3	1	2	δ	Th B + Th C + Th IV. 1.
$X^3 - 11X + 12$	$2^2.359$	$2^2.359$	1	3	0	3	1	1	δ	id.
$X^3 - X^2 - 10X - 7$	1489	1489	1	3	0	3	1	1	δ	Th B + Th C + Th IV. 1.

(1) D'après le théorème IV. 1., $h_K = a$, et la valeur commune est 3 ou 9. D'après la généralisation d'un théorème de Kisilevsky donnée par G. Gras [[6], prop. IV. 3], h_K est supérieur ou égal à 9.

BIBLIOGRAPHIE

[1] BARRUCAND P. et COHN H. - Remarks on principal factors in a relativ cubic field. J Number Theory t3 (1971).

[2] BILLEVIČ K.K. - Sur les unités d'un corps algébrique de degré 3 ou 4 (russe). Mat. Sbornik N.S. t40 (1956).

[3] BOREVIČ Z.I. et SCHAFAREVIČ I.R. - Number theory. Academic Press (1966).

[4] BRAUER R. - Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoischen Körpers. Math. Nachr. 4 (1951) 158-174.

[5] CHEVALLEY C. - Sur la théorie du corps de classes dans les corps finis et les corps locaux. Fac. of Sc. Tokyo, Sect. I, t21 (1933).

[6] GRAS G. - Sur les ℓ-classes d'idéaux dans les extensions cycliques relatives de degré premier ℓ . Ann. Inst. Fourier, tXXIII (1973) p. 1-48.

[7] GRAS G. et M.N. - Nombre de classes des corps $\mathbb{Q}(\sqrt{m})$. Univ. Grenoble (1972).

[8] HASSE H. - Die Einheitengruppe in einem total-reellen zyklischen kubischen Zählkörper und in zugehörigen bikubischen Normalkörper. Miscellanca Academica Berolinensia, vol. I, pp. 1-24, Akademie Verlag Berlin (1950).

[9] ISHIDA M. - Fundamental units of certain algebraic number fields. (Abh. Math. Semi. Univ. Hamburg, t 39 (1973)).

[10] IWASAWA - A note on class numbers of algebraic number fields. (Abh. Math. Sem. Hamburg, t 20 (1956)).

[11] KISILEVSKY H. - Some results related to Hilbert's theorem 94. J of Number theory , t 2 (1970).

[12] KURODA S.N. - Über die Klassenzahl eines relativ zyklischen Zahlkörpers von Primzahlgrade. Proc. Japan Academy, t 40 (1964).

[13] LEE M.P. - Integral representations of dihedral groups of order 2p . TRANS. AMS 110 (1964).

[14] MARTINET J. - Sur l'arithmétique des extensions galoisiennes à groupe de Galois dièdral d'ordre 2p .
Ann. Inst. Fourier, t 19 (1969), pp. 1-80.

[15] MEYER C. - Die Berechnung der Klassenzahl abelscher Zahlkörper über quadratischen Zahlkörpern.
Berlin, Akad., Verlag (1957).

[16] MOSER N. - Représentations entières des groupes dièdraux.
Sém. Th. Nb. Grenoble (1974).

-o-o-o-