SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

J. J. PAYAN

Idéaux réduits d'un corps de nombres

Séminaire de théorie des nombres de Grenoble, tome 1 (1971-1972), p. 1-8

<http://www.numdam.org/item?id=STNG_1971-1972__1__1_0>

IDEAUX REDUITS D'UN CORPS DE NOMBRES

par J.J. PAYAN le 20.10.71 (1ère partie)

On trouvera dans ce qui suit une rédaction de remarques sur la notion d'idéal réduit introduitepar A. Châtelet et utilisée dans [1]. Ces remarques ont été suggérées par la lecture de certains travaux de G. Fardoux [2] et C. Paris [7]. Il s'agissait au départ d'esquisser une approche des problèmes suivants : K/Q étant une extension cyclique de degré premier p dont le discriminant est divisible par r_o nombres premiers, on sait d'après un résultat de H.W. Leopoldt [4] que le p-rang r du groupe des classes de K vérifie la double inégalité $r_o - 1 \leq r \leq (p-1)(r_o-1)$. Peut-on trouver des K avec $p = 3$ pour lesquels $r > r_o$? G. Gras et J. Martinet ont donné depuis une réponse affirmative à cette question [5] , le premier a même résolu ce problème pour p premier quelconque [3] . La seconde question posée était de savoir si, sachant que le nombre h_K de classes de K est norme d'un entier de $\mathbb{Q}(\sqrt{-3})$ (dans le cas $p = 3$) on peut trouver des cas pour lesquels $7/h_K$, $13/h_K$, $16/h_K$, $19/h_K$, $25/h_K$ (M.N. Montouchet ayant publié [6] les premiers exemples de K pour lesquels $4/h_K$). Des réponses positives ont été obtenues pour 7 et 13 en collaboration avec M.N. Gras et N. Moser.

I. IDEAUX REDUITS.

Soit $K/\mathbb{Q}$ une extension finie de degré n possédant r_1 conjugués réels et $2r_2$ conjugués non réels. On utilise classiquement ces conjugués pour plonger K dans $\mathbb{R}^n$ ce qui permet de considérer les idéaux fractionnaires non nuls de K comme des réseaux de $\mathbb{R}^n$. Si on désigne comme d'habitude par $\sigma_1, \sigma_2, \ldots, \sigma_{r_1+r_2}$ un ensemble de plongements non équivalents de K dans $\mathbb{C}$ on définit une application $\varphi : \alpha \in K \to \underset{1 \leq i \leq r_1+r_2}{\text{Max}} |\sigma_i(\alpha)|$ de K

dans $\mathbb{R}^+$ qui se prolonge par linéarité à $\mathbb{R}^n$.

Proposition I.1.

φ est une norme sur $\mathbb{R}^n$.

C'est bien clair.

Notons A l'anneau des entiers de K .

Définition 1.

Soit $\mathfrak{a}$ un idéal entier non nul de A , posons $\mathfrak{a} \cap \mathbb{Z} = a\mathbb{Z}$ avec $a > 0$. On dira que $\mathfrak{a}$ est réduit si pour tout α de $\mathfrak{a}^*$ on a $\varphi(a) = a \leq \varphi(\alpha)$.

Proposition I.2.

Toute classe d'idéaux contient au moins un idéal réduit.

Démonstration (adaptée de celle de [2]) :

$\mathfrak{a}$ étant représenté par un réseau, φ admet un minimum atteint sur $\mathfrak{a}^*$. Soit $\alpha_o \in \mathfrak{a}^*$ tel que $\varphi(\alpha_o) \leq \varphi(\alpha)$ pour tout α de $\mathfrak{a}^*$. Posons $\beta = \dfrac{N_{K/Q}(\alpha_o)}{\alpha_o}$, il est clair que $\beta \in A$ et $\beta\mathfrak{a} \sim \mathfrak{a}$, montrons que $\beta\mathfrak{a}$ est réduit. De $\varphi(\alpha_o) \leq \varphi(\alpha)$ résulte $\underset{1\leq i\leq r_1+r_2}{\text{Max}} \dfrac{|\sigma_i(\beta\alpha_o)|}{|\sigma_i(\beta)|} \leq \underset{1\leq i\leq r_1+r_2}{\text{Max}} \dfrac{|\sigma_i(\beta\alpha)|}{|\sigma_i(\beta)|}$ pour tout $\alpha \in \mathfrak{a}^*$ soit encore en tenant compte de $\beta\alpha_o \in \mathbb{Z}$

$$|N_{K/Q}(\alpha_o)| \underset{1\leq i\leq r_1+r_2}{\text{Max}} \frac{1}{|\sigma_i(\beta)|} \leq \underset{1\leq i\leq r_1+r_2}{\text{Max}} \frac{|\sigma_i(\beta\alpha)|}{|\sigma_i(\beta)|}$$

Soit encore $|N_{K/Q}(\alpha_o)| \leq \underset{1\leq i\leq r_1+r_2}{\text{Max}} \left(\dfrac{\dfrac{1}{|\sigma_i(\beta)|}}{\underset{1\leq i\leq r_1+r_2}{\text{Max}} \dfrac{1}{|\sigma_i(\beta)|}} \cdot |\sigma_i(\beta\alpha)| \right) \leq \underset{1\leq i\leq r_1+r_2}{\text{Max}} |\sigma_i(\beta\alpha)|$

or $N_{K/Q}(\alpha_o) \in \beta\mathfrak{a} \cap \mathbb{Z}$ d'où le résultat.

Définition 2.

Nous dirons qu'un idéal entier $\mathfrak{a}$ de A est sans facteur rationnel si pour tout nombre premier naturel p on a $\mathfrak{a} \not\subset pA$.

Proposition I.3.

Il n'y a qu'un nombre fini d'idéaux réduits sans facteurs rationnels.

Démonstration :

Le théorème de Minkowski montre que $(\underset{\alpha\in\mathfrak{a}^*}{\text{Min}}\ \varphi(\alpha))^n \leq 2^n \frac{\sqrt{|\Delta(\mathfrak{a})|}}{V_\varphi}$ où $\Delta(\mathfrak{a})$ est le discriminant de $\mathfrak{a}$ et V_φ le volume de la boule unité. Si $\mathfrak{a}$ est réduit et $a\mathbb{Z} = \mathfrak{a} \cap \mathbb{Z}$ avec $a > 0$ on en déduit $a^n \leq (\frac{2}{\pi})^{r_2} \sqrt{|\Delta(A)|}\ N\mathfrak{a}$ où $N\mathfrak{a} = \text{Card } A/\mathfrak{a}$. Il est clair que $a^n = N_{K/Q}(a)$ est un multiple de $N\mathfrak{a}$, montrons que l'hypothèse $\mathfrak{a}$ sans facteur rationnel entraîne que tout diviseur premier p de $N\mathfrak{a}$ divise l'entier $\frac{a^n}{N\mathfrak{a}}$. Ecrivons $(p) = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_g^{e_g}$ la décomposition de (p) dans A et notons f_i le degré de $\mathfrak{p}_i$. Notons $\mathfrak{p}_1^{x_1} \ldots \mathfrak{p}_g^{x_g}$ la participation de p à $\mathfrak{a}$; la p-participation à $N\mathfrak{a}$ est donc $p^{f_1x_1+\ldots+f_gx_g}$. Il est clair en outre que la p-participation à a est le plus petit entier naturel supérieur ou égal à $\underset{1\leq i\leq g}{\text{Max}} \frac{x_i}{e_i}$. La participation de p à $\frac{a^n}{N\mathfrak{a}}$ est donc $p^{nx-(f_1x_1+\ldots+f_gx_g)}$ or $n = \sum_{i=1}^{g} e_i f_i$ d'où

$$nx - \sum_{i=1}^{g} f_i x_i = \sum_{i=1}^{g} e_i f_i (x - \frac{x_i}{e_i}) \ .$$

Comme $\mathfrak{a} \not\subset \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$, il existe au moins un indice i pour lequel $\frac{x_i}{e_i} < 1$ et $p/N\mathfrak{a}$ entraîne $x > 0$ donc $x - \frac{x_i}{e_i} > 0$ d'où le résultat. Il est clair en outre que

$$nx - \sum_{i=1}^{g} f_i x_i \geq (\underset{1\leq i\leq g}{\text{Min}}\ e_i f_i) \underset{1\leq i\leq g}{\text{Max}} (\frac{x_i}{e_i} - 1) \ .$$

On en déduit qu'un nombre fini de p peuvent diviser $N\mathfrak{a}$ et que leur p-participation est bornée, la finitude annoncée en résulte.

Remarque 1 :

Cette définition des idéaux réduits est moins restrictive que celle donnée par A. Châtelet [2] pour le cas des corps quadratiques imaginaires. L'idéal $(3, \sqrt{7}-1)$ de $\mathbb{Z}[\sqrt{7}]$ est réduit au sens ci-dessus sans l'être au sens d'A. Châtelet.

On pourrait alors penser que la détermination des idéaux réduits est un bon moyen de majoration du nombre de classes h_K de K. La propriété ci-dessous montre que cette détermination soulève des problèmes algorithmiques non triviaux.

Proposition I.4.

Soient $\mathfrak{a}$ un idéal entier de A admettant une $\mathbb{Z}$-base $\{\omega_1, \omega_2, \ldots, \omega_n\}$ et ψ la norme définie par

$$\psi(\alpha) = \operatorname{Max}_{1 \le i \le n} |\lambda_i| \quad \text{ou} \quad \alpha = \sum_{1 \le i \le n} \lambda_i \omega_i \quad \text{avec} \quad \lambda_i \in \mathbb{Z}.$$

Alors si K est totalement réel on a

$$\psi \le C\varphi \quad \text{où} \quad C = D_n \frac{[\operatorname{Max} \varphi(\omega_i)]^{n-1}}{\sqrt{|\Delta(\mathfrak{a})|}}$$

et où D_n désigne le maximum en valeur absolue des discriminants des matrices carrées d'ordre n à coefficients réels compris entre -1 et $+1$. (D'après Marc Duc-Jacquet $D_n = 2^n$ pour $n \ge 2$).

On est donc conduit à rechercher si on peut trouver des idéaux réduits plus simples. Plaçons-nous dans un cas particulier.

II. CAS DES EXTENSIONS CYCLIQUES DE DEGRE PREMIER ℓ.

Le cas $\ell = 2$ étant bien connu nous supposerons ℓ impair.

Définition 3.

Nous dirons qu'un idéal entier sans facteur rationnel est élémentaire s'il divise un nombre premier p.

Il en résulte que si (p) se décompose (resp se ramifie) dans K, un diviseur élémentaire de p est de la forme $\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_r$ (resp $\mathfrak{p}^r$) avec $r \leq \ell-1$.

Proposition II.1.

Tout idéal $\mathfrak{a}$ réduit sans facteurs rationnels est produit d'idéaux réduits élémentaires.

Démonstration :

Supposons $\mathfrak{a}$ réduit sans facteur rationnel et $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$ avec $\mathfrak{a}_1$, $\mathfrak{a}_2$ entiers et $(N\mathfrak{a}_1, N\mathfrak{a}_2) = 1$ notons a_1 et a_2 les entiers naturels définis par $a_1\mathbb{Z} = \mathfrak{a}_1 \cap \mathbb{Z}$ et $a_2\mathbb{Z} = \mathfrak{a}_2 \cap \mathbb{Z}$. Il est clair que $\mathfrak{a}_1\mathfrak{a}_2 \cap \mathbb{Z} = a_1a_2\mathbb{Z}$ et $a_1\mathfrak{a}_2 \subset \mathfrak{a}$: comme $\mathfrak{a}$ est réduit $a_1a_2 \leq \varphi(\alpha)$ pour tout α de $\mathfrak{a}^*$, donc a fortiori $a_1a_2 \leq \varphi(\alpha)$ pour tout α de $a_1\mathfrak{a}_2^*$, $a_1\mathfrak{a}_2^*$ est donc réduit et il en est de même pour $\mathfrak{a}_2$. Cela nous ramène au cas où $N\mathfrak{a}$ n'admet qu'un diviseur premier p. Si p est ramifié, l'hypothèse sans facteur rationnel entraîne $\mathfrak{a} = \mathfrak{p}^r$ avec $1 \leq r \leq \ell-1$ et $\mathfrak{a}$ est élémentaire. Si p est décomposé, écrivons $\mathfrak{a} = \mathfrak{p}_1^{x_1}\ldots\mathfrak{p}_r^{x_r}$ avec $r \leq \ell-1$ et $0 < x_r \leq x_{r-1} \leq \ldots \leq x_1$, et posons $\mathfrak{a}_1 = \mathfrak{p}_1^{x_1-x_2}$, $\mathfrak{a}_2 = (\mathfrak{p}_1\mathfrak{p}_2)^{x_2-x_3}$, ..., $\mathfrak{a}_r = (\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_r)^{x_r}$. On voit que $\mathfrak{a}_i \cap \mathbb{Z} = p^{n_i}\mathbb{Z}$ avec $n_i = x_i - x_{i+1}$ si $1 \leq i < r$ et $n_r = r$. Par ailleurs $\mathfrak{a} \cap \mathbb{Z} = p^{x_1}\mathbb{Z}$. Il est clair que

$$p^{n_1}p^{n_2}\ldots p^{n_{i-1}}\mathfrak{a}_i p^{n_{i+1}}\ldots p^r \subset \mathfrak{a}$$

et

$$p^{n_1}p^{n_2}\ldots p^{n_{i-1}}\mathfrak{a}_i\, p^{n_{i+1}}\ldots p^r \cap \mathbb{Z} = p^{x_1}\mathbb{Z}$$

or $\mathfrak{a}$ est réduit ce qui montre que $\overline{\prod_{j\neq i} p^{n_j}\mathfrak{a}_i}$ est réduit et $\mathfrak{a}_i$ est donc réduit. Il reste à voir que si $(\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_i)^{n_i}$ est réduit, il en est de même pour $\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_i$. On remarque alors d'une part que

$$p^{n_i-1}\,\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_i \subset (\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_i)^{n_i}$$

et

$$p^{n_i-1}\,\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_i \cap \mathbb{Z} = (\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_i)^{n_i} \cap \mathbb{Z}$$

ce qui entraîne $p^{n_i-1}\,\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_i$ réduit d'où le résultat.

La notion de racine introduite par A. Châtelet [1] et C. Paris [7] se généralisant.

Définition 4.

Nous dirons qu'un idéal entier $\mathfrak{a}$ est de type 1 si $\mathfrak{a}\cap\mathbb{Z} = (N\mathfrak{a}).\mathbb{Z}$.

Remarque 2 :

Un idéal de type 1 est sans facteur rationnel et de plus n'est divisible ni par le carré d'un idéal ramifié ni par le produit de deux idéaux premiers distincts conjugués.

Définition 5.

Soit θ un entier primitif de K on dira qu'un nombre rationnel c est une racine de $\mathfrak{a}$ relativement à θ si $\theta - c \in \mathfrak{a}$.

Proposition II.2. (voir C. Paris [7])

Si $\mathfrak{a}$ est réduit et de type 1 il a deux racines au moins relativement à θ dans l'intervalle $]\theta_1, \theta_\ell[$ où θ_1 (resp θ_ℓ) désigne le conjugué minimum (resp maximum) de θ .

Démonstration :

Il suffit de remarquer que les racines de $\mathfrak{a}$ relativement à θ forment une progression arithmétique de raison $a = N\mathfrak{a}$. Notons c la plus grande racine inférieure à θ_1 . Puisque $\mathfrak{a}$ est réduit on a $a < \theta_\ell - c$ donc $a+c \in]\theta_1, \theta_\ell$ En outre $a+c-\theta_1 < a$ et $\mathfrak{a}$ réduit entraine $a < \theta_\ell - (a+c)$ d'où le résultat.

Propriété II.3.

Si $\{1, \theta, \ldots, \theta^{\ell-1}\}$ est une $\mathbb{Z}$-base de A , les progressions arithmétiques de racines de $\mathfrak{a}$ relatives à θ et à ses conjugués sont deux à deux distinctes si $\mathfrak{a}$ n'est pas produit d'idéaux premiers ramifiés.

Remarque 3 .

On peut enfin se poser la question suivante : soit K/Q cyclique de degré premier impair ℓ , toute classe d'idéaux contient-elle un idéal réduit de type 1 ? Ou encore -compte tenu de la proposition II.1- toute classe contient-

elle un produit d'idéaux premiers réduits ? Après en avoir discuté avec F. Châtelet il semble que la réponse soit négative. En effet, si elle était positive et si $2\ell+1$ était un nombre premier p le sous-corps réel maximal $\mathbb{Q}_o^{(p)}$ du corps cyclotomique $\mathbb{Q}^{(p)}$ serait principal. Cela se voit en remarquant que si ζ est une racine primitive p-ième de 1, $\{1, \theta, \theta^2, \ldots, \theta^{\ell-1}\}$ où $\theta = \zeta + \zeta^{-1}$ est une base d'entiers de $\mathbb{Q}_o^{(p)}$, comme $\theta_\ell - \theta_1 < 4$ les propriétés II.2 et II.3 montrent qu'il n'y a pas d'idéal réduit autre que l'idéal unité.

Si $A = \mathbb{Z}[\theta]$ et si $\mathfrak{a}$ est un idéal entier on obtient facilement à l'aide des racines de ses diviseurs de type 1 une $\mathbb{Z}$-base de $\mathfrak{a}$.

En effet soit $\mathfrak{a}$ un idéal entier sans facteur rationnel ; il s'écrit $\mathfrak{a} = \mathfrak{a}_1^{i_1}\mathfrak{a}_2^{i_2}\ldots\mathfrak{a}_r^{i_r}$ où $r \leq \ell-1$ et où les $\mathfrak{a}_i$ sont de type 1 et vérifient $N\mathfrak{a}_{i+1}$ divise $N\mathfrak{a}_i$ et $\mathfrak{a}_i^{i_i}$ et $\mathfrak{a}_j^{i_j}$ n'ont en commun que des facteurs ramifiés si $i \neq j$. On pose $a_i\mathbb{Z} = \mathfrak{a}_i^{i_i} \cap \mathbb{Z}$ et on note c_i une racine de $\mathfrak{a}_i^{i_i}$ (relativement à θ).

Proposition II.4. (G. Fardoux)

$\{a_1, (\theta-c_1)a_2, (\theta-c_1)(\theta-c_2)a_3, \ldots, (\theta-c_1)(\theta-c_2)\ldots(\theta-c_{r-1})a_r, \theta(\theta-c_1)\ldots(\theta-c_r), \ldots, \theta^{\ell-1-r}(\theta-c_1)\ldots(\theta-c_r)\}$ est une $\mathbb{Z}$-base de $\mathfrak{a} = \mathfrak{a}_1^{i_1}\ldots\mathfrak{a}_r^{i_r}$ défini ci-dessus.

Démonstration :

Il suffit de vérifier, ce qui est presque immédiat, que le discriminant du système ci-dessus, formé d'éléments de $\mathfrak{a}$, est égal à $(N\mathfrak{a})^2\Delta(A)$ l'égalité des $\mathbb{Z}$-modules considérés en résulte puisqu'ils sont emboîtés.

BIBLIOGRAPHIE

[1] - A. CHATELET - "L'arithmétique des corps quadratiques".
L'enseignement mathématique - Genève 1962.

[2] - G. FARDOUX - "Idéaux de polynômes et nombre de classes de corps de nombres algébriques".
Thèse - Université de Besançon - 1970.

[3] - G. GRAS - "Etude du ℓ-rang d'une extension cyclique de degré ℓ .
(à paraître).

[4] - H.W. LEOPOLDT - "Zur Geschlechtertheorie in abelschen Zahlkörpern".
Math. Naehr. 9 - 1953 - pp.351 à 362.

[5] - J. MARTINET - "A propos de classes d'idéaux".
Sem. Th. Nombres - Bordeaux nov.1971.

[6] - M.N. MONTOUCHET - "Sur le nombre de classes du sous-corps cubique cyclique de $\mathbb{Q}^{(p)}$, $p \equiv 1 \bmod 3$ ".
Proceedings of the Japan Academy, vol XLVII-7-1971.

[7] - C. PARIS - "Construction du groupe des classes d'idéaux dans un corps cubique abélien".
Journées arithmétiques - Besançon 1965.
