THEORIE DES NOMBRES
BESANCON

Années 1981-1982
et 1982-1983

UNE REMARQUE SUR L'ANNEAU DES ENTIERS DU CORPS DES RACINES SEPTIEMES DE L'UNITE

Jean COUGNARD

UNE REMARQUE SUR L'ANNEAU DES ENTIERS DU CORPS DES RACINES SEPTIEMES DE L'UNITE

par Jean COUGNARD

Pour un entier premier p, on note ζ_p une racine primitive p-ième de l'unité, $\mathbb{Q}(\zeta_p)$ le p-ième corps cyclotomique et, si $p \equiv 1(3)$, k le sous-corps de $\mathbb{Q}(\zeta_p)$ tel que $[\mathbb{Q}(\zeta_p) : k] = 3$. En confrontant un travail précédent [C] avec la thèse de I. Brinkhuis, on constate que $\mathbb{Z}[\zeta_p]$ ne possède pas de base normale relativement à l'anneau Z_k des entiers de k, pourvu que $p \neq 7$. On montre ici qu'il en est de même pour $p = 7$.

On suppose les corps plongés dans $\mathbb{C}$ et on pose $\zeta = \zeta_7$. Le sous-corps réel maximal K de $\mathbb{Q}(\zeta)$ est $\mathbb{Q}\left(\cos\left(2\Pi/7\right)\right)$ et l'élément $\theta = 2 \cos \frac{2\Pi}{7}$ engendre une base normale de Z_K ; le corps k est $\mathbb{Q}(\sqrt{-7})$.

Le groupe de Galois G de $\mathbb{Q}(\zeta)/k$ est engendré par l'automorphisme σ tel que $\sigma(\zeta) = \zeta^2$; on note χ le caractère de G tel que $\chi(\sigma) = j$, les deux autres caractères de G sont $\bar{\chi}$ le conjugué de χ et le caractère trivial χ_o.

On rappelle que pour ψ caractère de degré un de G, la résolvante de Lagrange $\langle x, \psi \rangle = \sum_{g \in G} g(x)\, \psi(x^{-1})$. Pour $\psi \neq \chi_o$ les éléments $\langle x, \chi \rangle$ et $\langle x, \bar{\chi} \rangle$ appartiennent à $\mathbb{Q}(\zeta, j)$ et sont conjugués sur $\mathbb{Q}(\zeta)$.

Si $\mathbb{Z}[\zeta]$ possède une Z_k-base normale u, $\langle u, \chi_o \rangle = Tr_{\mathbb{Q}(\zeta)/k}(\zeta)$ est une unité de $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ que l'on peut choisir égale à +1 et l'ensemble des $\frac{\langle x, \chi \rangle}{\langle \theta, \chi \rangle}$ lorsque x parcourt $\mathbb{Z}[\zeta]$ est un idéal fractionnaire principal de $\mathbb{Q}(\sqrt{-7}, j)$ engendré par $\frac{\langle u, \chi \rangle}{\langle \theta, \chi \rangle}$; on sait par ailleurs que cet idéal est égal à $\mathfrak{P}^{-1}$ où $\mathfrak{P}$ l'idéal premier de $\mathbb{Q}(\sqrt{-7}, j)$ au dessus de 7 tel que $j \equiv 2(\mathfrak{P})$ [C].

On sait de plus que $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}, j]$ l'anneau des entiers est principal et enfin que $3x = \langle x,\chi_o\rangle + \langle x,\chi\rangle + \langle x,\bar{\chi}\rangle = \langle x,\chi_o\rangle + T_{\mathbb{Q}(\zeta,j)/\mathbb{Q}(\zeta)}(\langle x,\chi\rangle)$.

Il en résulte aisément :

<u>Proposition</u> :

<u>Le $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}][G]$-module $\mathbb{Z}[\zeta]$ est libre si et seulement si il existe un générateur a de $\mathfrak{P}^{-1}$ tel que $\frac{1}{3}\left(1+\mathrm{Tr}_{\mathbb{Q}(\zeta,j)/\mathbb{Q}(\zeta)}(a\langle\theta,\chi\rangle)\right)$ est un entier de $\mathbb{Q}(\zeta)$.</u>

On va donc maintenant déterminer un générateur de $\mathfrak{P}^{-1}$ et les unités de $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}, j]$.

<u>Générateur de $\mathfrak{P}$</u> : Dans $\mathbb{Z}[j]$ on a $(2+\sqrt{-3})(2-\sqrt{-3}) = 7$ et $j-2 = j(2+\sqrt{-3})$ donc $\mathfrak{P}\cap\mathbb{Z}[j] = (2+\sqrt{-3})$.

Un générateur v de $\mathfrak{P}$ a pour norme et pour trace, dans $\mathbb{Q}(\sqrt{-7},j)/\mathbb{Q}(j)$, un générateur de $(2+\sqrt{-3})$; il s'en suit que v est racine d'une des équations du second degré ainsi obtenue. Une étude rapide conduit à choisir $u = \frac{2+\sqrt{-3}+\sqrt{-7}}{2}$.

Par conséquent, $\mathfrak{P}^{-1}$ est engendré par $u^{-1} = \frac{7-2\sqrt{-7}+\sqrt{21}}{2\times 7}$.

<u>Unités de $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}, j]$</u> : Le théorème de Dirichlet montre que ce groupe est de rang un, comme celui du sous-anneau $\mathbb{Z}[\frac{1+\sqrt{21}}{2}]$. Dans ce dernier l'unité fondamentale est $\frac{5+\sqrt{21}}{2}$, l'unité ε cherchée est donc soit $\frac{5+\sqrt{21}}{2}$, soit $\sqrt{\frac{5+\sqrt{21}}{2}}$ soit $\sqrt{-\frac{5+\sqrt{21}}{2}}$. On montre aisément que $\mathbb{Q}\left(\sqrt{-\frac{5+\sqrt{21}}{2}}\right) = \mathbb{Q}(\sqrt{-7}, j)$.

L'unité fondamentale de $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}, j]$ est donc $\sqrt{-\frac{5+\sqrt{21}}{2}}$ dont on constate qu'elle est égale à $\frac{\sqrt{-7}-\sqrt{-3}}{2}$.

Dans la proposition précédente il faut donc choisir

$a = (-j)^r \left(\frac{\sqrt{-7}-\sqrt{-3}}{2}\right)^n \left(\frac{7-2\sqrt{-7}+\sqrt{21}}{2\times 7}\right)$.

Puisque $(\sqrt{-3})$ est le seul idéal premier au dessus de 3 dans $\mathbb{Q}(\zeta, j)$, il suffit pour montrer qu'il n'y a pas de base normale que

$1+\mathrm{Tr}_{\mathbb{Q}(\zeta,j)/\mathbb{Q}(\zeta)}(a\langle\theta,\chi\rangle) \not\equiv 0\ (\sqrt{-3})$.

Comme $j \equiv 1\ (\sqrt{-3})$ on en déduit que $\langle\theta,\chi\rangle \equiv -1 \quad (\sqrt{-3})$

donc

$$1+\mathrm{Tr}_{\mathbb{Q}(\zeta,j)/\mathbb{Q}(\zeta)}(a\langle\theta,\chi\rangle) \equiv 1+(-1)^{n+r}(\sqrt{-7})^n(1+\sqrt{-7}) \quad (\sqrt{-3}).$$

Si $n = 2t$ ceci est congru à $1+(-1)^{r+t}\,(1+\sqrt{-7})$.

Si $n = 2t+1$ ceci est congru à

$$1+(-1)^{r+1}\,(-7)^t\,\sqrt{-7}\,(1+\sqrt{-7}) \equiv 1+(-1)^{r+t+1}\,(\sqrt{-7}-1)$$
$$\equiv 1+(-1)^{r+t}\,(1-\sqrt{-7}) \qquad (\sqrt{-3}).$$

On obtient donc soit $2+\sqrt{-7}$, soit $\sqrt{-7}$, soit leurs conjugués. Aucun de ces nombres n'est congru à zéro modulo $\sqrt{-3}$.

Il n'y a donc pas de base normale pour $\mathbb{Z}[\zeta]$ relativement à $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$.

On peut donc conclure que si $p \equiv 1\ (3)$, $\mathbb{Z}[\zeta]$ ne possède pas de base normale sur l'anneau Z_k des entiers du sous-corps cubique relatif.

REFERENCES

[B] J. BRINKHUIS :
Embedding problems and Galois modules. Thèse, Leyde, 1981.

[C] J. COUGNARD :
Quelques extensions modérément ramifiées sans base normale.

Jean COUGNARD
E.R.A. CNRS 070654
Laboratoire de Mathématiques
Faculté des Sciences
25030 BESANCON CEDEX