THÉORIE DES NOMBRES. — *Quelques exemples d'anneaux euclidiens* [1].

Note (*) de **Hendrik W. Lenstra** Jr., transmise par M. Jacques Tits.

Dans cette Note nous donnons sept exemples de corps et de corps gauches, tous de degré 8 sur le corps des nombres rationnels, dont les ordres maximaux sont euclidiens pour la norme. La démonstration repose sur certaines propriétés du réseau Γ_8.

In this Note we give seven examples of fields and skew fields having degree eight over the rational numbers, the maximal orders of which are euclidean with respect to the norm. The proof depends on certain properties of the lattice Γ_8.

1. LEMME. — *Soit* V *un espace vectoriel de dimension* 8 *sur* $\mathbf{Q}$, *muni d'une forme quadratique définie positive* f. *Notons par* $(\ ,\ )$ *le produit scalaire associé à* f :

$$(x,\ y)=\frac{1}{2}(f(x+y)-f(x)-f(y)).$$

Supposons que E *soit un sous-groupe de* V, *libre sur* $\mathbf{Z}$ *de rang* 8, *tel que :*

(*a*) *pour tout* $x\in V$, *on ait* $x\in E$ *si et seulement si* $(x,\ y)\in\mathbf{Z}$ *pour tout* $y\in E$;

(*b*) $f(x)\in 2\mathbf{Z}$ *pour tout* $x\in E$.

Alors pour tout $x\in V$ *il existe* $y\in E$ *tel que* $f(x-y)\leqq 1$.

Démonstration. — Les conditions (*a*) et (*b*) entraînent que E est un *module quadratique pair* de rang 8 sur $\mathbf{Z}$, [*voir* (9), chap. V]. On sait qu'un tel module ne peut être défini positif que s'il est isomorphe au module quadratique Γ_8, [*cf.* (3), (5), (8) et (9)]. Donc il suffit de démontrer le lemme dans le cas $E=\Gamma_8$, $V=\Gamma_8\otimes\mathbf{Q}$. Ceci peut se faire soit par un calcul direct, basé sur une description explicite de Γ_8 [*voir* (9), chap. V, 1.4.3], soit de la manière suivante.

Notons W le groupe d'automorphismes de Γ_8. Dans (2) (chap. VI, 2.1 et 2.2, cor. à prop. 5) on trouve une description d'un ensemble $\overline{C}\subset V$ ayant la propriété que pour chaque $x\in V$ il existe $\sigma\in W$ et $y\in\Gamma_8$ tels que $\sigma(x-y)\in\overline{C}$. Comme il est facile de vérifier que $f(z)\leqq 1$ pour tout $z\in\overline{C}$ [utiliser (2), p. 268-270], on voit bien que pour tout $x\in V$ il existe $y\in\Gamma_8$ tel que $f(x-y)\leqq 1$.

2. Si L est un corps de nombres algébriques, la trace et la norme $L\to\mathbf{Q}$ sont notées Tr_L et N_L, respectivement.

Soit F un corps de nombres algébriques de degré 8 sur $\mathbf{Q}$ qui est une extension quadratique totalement imaginaire d'un corps totalement réel K. On suppose que l'extension F/K est non ramifiée en dehors de l'infini, et qu'il existe un élément totalement positif δ de K qui engendre la différente de K sur $\mathbf{Q}$. Évidemment, ces hypothèses impliquent que la différente de F sur $\mathbf{Q}$ est également engendrée par δ. Notons par $^-:F\to F$ l'automorphisme non trivial de F sur K. Alors il est immédiat que l'application $f:F\to\mathbf{Q}$ définie par

$$f(x)=Tr_F(x\bar{x}/\delta)$$

est une forme quadratique définie positive sur F, et que le produit scalaire associé est donné par

$$(x,\ y)=Tr_F(x\bar{y}/\delta).$$

Soit A l'anneau des entiers de F. Pour $x \in F$, on a $(x, y) \in \mathbf{Z}$ pour tout $y \in A$ si et seulement si $\mathrm{Tr}_F((x/\delta) . y) \in \mathbf{Z}$ pour tout $y \in \overline{A} = A$, si et seulement si x/δ appartient à la différente inverse de $F/\mathbf{Q}$, c'est-à-dire si $x \in A$. On voit donc que l'hypothèse (a) du lemme est vérifiée pour $V = F$, $E = A$. Pour démontrer (b), on observe que

$$f(x) = 2 . \mathrm{Tr}_K(x\bar{x}/\delta) \in 2\mathbf{Z} \qquad \text{pour} \quad x \in A,$$

puisque $x\bar{x}/\delta$ appartient à la différente inverse de $K/\mathbf{Q}$.

Désignons par Δ le discriminant de K sur $\mathbf{Q}$. Pour chaque $z \in F$, on a

$$N_F(z) = N_K(z\bar{z}) = N_K(\delta) . N_K(z\bar{z}/\delta) = \Delta . \prod_\sigma \sigma(z\bar{z}/\delta),$$

où σ parcourt l'ensemble des plongements $K \to \mathbf{R}$. Chacun des facteurs $\sigma(z\bar{z}/\delta)$ est un nombre réel positif ou nul, donc en appliquant l'inégalité entre la moyenne géométrique et la moyenne arithmétique on trouve que

$$0 \leqq N_F(z) \leqq \Delta . (\sum_\sigma \sigma(z\bar{z}/\delta)/4)^4 = \Delta . f(z)^4 . 8^{-4}.$$

Supposons maintenant que $\Delta < 8^4 = 4\,096$. Nous affirmons que l'anneau A est euclidien pour la norme N_F. Pour le démontrer, soient a, b deux éléments de A, avec $b \neq 0$. En appliquant le lemme à $x = ab^{-1}$ nous trouvons qu'il existe $y \in A$ tel que $f(ab^{-1} - y) \leqq 1$. Posons $z = ab^{-1} - y$ dans l'inégalité ci-dessus; il s'ensuit que

$$N_F(ab^{-1} - y) \leqq \Delta . 8^{-4} < 1.$$

Par conséquent, on a

$$a = yb + r,$$

avec $r = a - yb \in A$ et

$$N_F(r) = N_F(ab^{-1} - y) . N_F(b) < N_F(b),$$

ce qui achève la démonstration.

3. D'après les tables de Godwin ([4]) exactement treize corps biquadratiques totalement réels K vérifient la condition $\Delta < 4\,096$, à isomorphisme près. Un examen facile révèle que seulement quatre d'entre eux admettent une extension quadratique totalement imaginaire F qui est non ramifiée en dehors de l'infini. Ce sont

$$K = \mathbf{Q}(\zeta_{15} + \zeta_{15}^{-1}), \quad \Delta = 1\,125, \quad F = \mathbf{Q}(\zeta_{15}),$$
$$K = \mathbf{Q}(\zeta_{20} + \zeta_{20}^{-1}), \quad \Delta = 2\,000, \quad F = \mathbf{Q}(\zeta_{20}),$$
$$K = \mathbf{Q}(\zeta_{24} + \zeta_{24}^{-1}), \quad \Delta = 2\,304, \quad F = \mathbf{Q}(\zeta_{24}),$$
$$K = \mathbf{Q}(\sqrt{3}, \sqrt{5}), \quad \Delta = 3\,600, \quad F = \mathbf{Q}(\sqrt{-3}, \sqrt{-1}, \sqrt{5}),$$

où ζ_m désigne une racine primitive m-ième de l'unité. Comme générateur totalement positif de la différente sur $\mathbf{Q}$ on peut prendre, dans les cas respectifs :

$$\delta = 5 . (\zeta_5 - \zeta_5^{-1})^{-1} . (\zeta_3 - \zeta_3^{-1}) . (\zeta_3\zeta_5^{-1} + \zeta_5\zeta_3^{-1}),$$
$$\delta = 10 . (\zeta_5 - \zeta_5^{-1})^{-1} . \zeta_4 . (\zeta_4\zeta_5^{-1} + 1 + \zeta_5\zeta_4^{-1}),$$
$$\delta = 4 . (3 - \sqrt{6}),$$
$$\delta = 2 . \sqrt{3} . \sqrt{5} . \theta . (\sqrt{3} - \theta),$$

avec $\theta = (1 + \sqrt{5})/2$.

CONCLUSION. — *L'anneau des entiers de chacun des corps* $\mathbf{Q}(\zeta_{15})$, $\mathbf{Q}(\zeta_{20})$, $\mathbf{Q}(\zeta_{24})$, $\mathbf{Q}(\sqrt{-3}, \sqrt{-1}, \sqrt{5})$ *est euclidien pour la norme.*

Le corps $\mathbf{Q}(\sqrt{-3}, \sqrt{-1}, \sqrt{5})$, de discriminant 12.960.000, est le seul qui ne figure pas dans [7], Table 11. Pour les deux corps $\mathbf{Q}(\zeta_{15})$, $\mathbf{Q}(\zeta_{20})$ une autre démonstration est donnée dans [6].

4. D'une manière analogue on obtient des exemples d'anneaux euclidiens non commutatifs. Soit K un des corps $\mathbf{Q}(\sqrt{5})$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{13})$, et soit D l'algèbre de quaternions $(-1, -1/K)$. Alors D est l'unique corps gauche de quaternions sur K qui est non ramifié aux places finies. Notons $\mathrm{Nrd} : D \to K$ la norme réduite, et posons $N = N_K \circ \mathrm{Nrd}$. Pour $x \in D$, nous définissons

$$f(x) = 2 \cdot \mathrm{Tr}_K(\mathrm{Nrd}(x)/\delta),$$

où

$$\delta = (5+\sqrt{5})/2 \quad \text{si} \quad K = \mathbf{Q}(\sqrt{5}),$$
$$\delta = 4+2\sqrt{2} \quad \text{si} \quad K = \mathbf{Q}(\sqrt{2}),$$
$$\delta = (13+3\sqrt{13})/2 \quad \text{si} \quad K = \mathbf{Q}(\sqrt{13}).$$

En procédant comme dans le paragraphe 2 et en observant que le discriminant de K sur $\mathbf{Q}$ est inférieur à 16 on trouve que pour chaque ordre maximal R de D, et pour chaque $a, b \in R$, $b \neq 0$, il existe $q, q', r, r' \in R$ tels que

$$a = qb + r = bq' + r',$$
$$N(r) < N(b), \qquad N(r') < N(b).$$

On exprime ceci en disant que R est euclidien pour la norme.

CONCLUSION. — *Soit*

$$D = \left(\frac{-1, -1}{\mathbf{Q}(\sqrt{5})}\right), \left(\frac{-1, -1}{\mathbf{Q}(\sqrt{2})}\right) \quad \textit{ou} \quad \left(\frac{-1, -1}{\mathbf{Q}(\sqrt{13})}\right).$$

Alors chaque ordre maximal de D *est euclidien pour la norme.*

(*) Séance du 20 février 1978.

(1) Cette recherche a été aidée par l'Organisation néerlandaise pour le Développement de la Recherche scientifique (Z.W.O.).

(2) N. BOURBAKI, *Groupes et algèbres de Lie*, chap. IV, V, VI, Hermann, Paris, 1968.
(3) D. ESTES et G. PALL, *Illinois J. Math.*, 14, 1970, p. 159-163.
(4) H. J. GODWIN, *J. London Math. Soc.*, 31, 1956, p. 478-485.
(5) M. KNESER, *Archiv Math. (Basel)*, 8, 1957, p. 241-250.
(6) H. W. LENSTRA, Jr, *J. London Math. Soc.*, 10, 1975, p. 457-465.
(7) H. W. LENSTRA, Jr, *Invent. Math.*, 38, 1977, p. 237-254.
(8) L. J. MORDELL, *J. Math. pures et appl.*, 17, 1938, p. 41-46.
(9) J.-P. SERRE, *Cours d'arithmétique*, Presses Universitaires de France, Paris, 1970.

Institut des Hautes Études scientifiques,
35, *route de Chartres*, 91440 *Bures-sur-Yvette.*