5. Un exemple explicite

déterminer explicitement une telle famille: on sait en effet (voir par exemple [10], p. 70) que toute classe d'idéaux de A contient un idéal entier $\mathfrak{a}$ tel que

$$N\mathfrak{a} \leqq M_K = \left(\frac{4}{\pi}\right)^{r2} \cdot \frac{n!}{n^n} \sqrt{|\Delta|},$$

Δ désignant le discriminant de K. On voit donc qu'on peut prendre pour D l'ensemble des idéaux premiers $\mathfrak{p}$ de A tels que $N\mathfrak{p} \leq M_K$. Bien entendu, l'ensemble D ainsi construit est en général « beaucoup trop grand »: mais il est clair que la détermination d'un D « minimal » équivaut pratiquement à la détermination de la structure du groupe des classes de A, ce qui est une autre affaire.

5. Un exemple explicite

Montrons pour terminer, sur un exemple numérique simple, que les méthodes précédentes mènent à des résultats tout à fait explicites. Nous considérons le corps quadratique imaginaire $K = \mathbf{Q}(\sqrt{-23})$, pour lequel $n = 2$, $r_1 = 0$, $r_2 = 1$, $a = 1$, $r = 0$, $W = \{1, -1\}$. Posons:

$$\alpha = \frac{-1+\sqrt{-23}}{2};$$

le polynôme minimal de α sur $\mathbf{Q}$ est $X^2 + X + 6$, et on a $A = \mathbf{Z}[\alpha]$, Δ (le discriminant) $= -23$. De là

$$\left(\frac{4}{\pi}\right)^{r2} \cdot \frac{n!}{n^n} \sqrt{|\Delta|} = \frac{2\sqrt{23}}{\pi} \leq 4,$$

et le groupe des classes de A est engendré par les classes des facteurs premiers de 2 et de 3 dans A. Mais (pour $p = 2,3$) on a

$$A/pA = \mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] \simeq \mathbf{Z}[X]/(p, X^2+X+6)$$

d'où, puisque $6 \equiv 0 \pmod{p}$,

$$A/pA \simeq \mathbf{Z}[X]/(p, X^2+X) \simeq \mathbf{F}_p[X]/(X(X+1))$$

et finalement $A/pA \simeq \mathbf{F}_p \times \mathbf{F}_p$. Ainsi, 2 et 3 sont décomposés dans A, et le calcul ci-dessus montre plus précisément qu'on peut écrire

$$(2) = \mathfrak{p}\bar{\mathfrak{p}}, \quad (3) = \mathfrak{q}\bar{\mathfrak{q}},$$

avec

$$\mathfrak{p} = (2, \alpha), \quad \bar{\mathfrak{p}} = (2, \alpha+1),$$

et

$$\mathfrak{q} = (3, \alpha), \quad \bar{\mathfrak{q}} = (3, \alpha+1).$$

On vérifie sans peine que $\mathfrak{p}\mathfrak{q} = (\alpha)$, $\mathfrak{p}\mathfrak{q} = (\alpha+1)$ et $\mathfrak{p}^3 = (\alpha+2)$. En revanche, $\mathfrak{p}^2$ n'est pas principal: car $N\mathfrak{p}^2 = 4$, mais $\mathfrak{p}^2 \neq (2)$, alors que 2 et -2 sont les seuls entiers de K ayant pour norme 4.

Il résulte de tout ceci que $\bar{\mathfrak{p}} \sim \mathfrak{p}^{-1}$, $\bar{\mathfrak{q}} \sim \mathfrak{q}^{-1}$, $\mathfrak{q} \sim \bar{\mathfrak{q}}^{-1} \sim \mathfrak{p}$, $\mathfrak{p}^3 \sim (1)$, mais qu'*on n'a pas* $\mathfrak{p}^2 \sim (1)$ (*ni* a fortiori $\mathfrak{p} \sim (1)$): le groupe des classes de A est donc cyclique d'ordre 3, engendré par la classe de $\mathfrak{p} = (2, \alpha)$.

Soit maintenant $\mathfrak{p}_\infty$ l'unique place archimédienne de K et posons

$$D = \{\mathfrak{p}\}, \quad S = \{\mathfrak{p}_\infty, \mathfrak{p}\}.$$

Alors, avec les notations du §1, on a $d = 1$, $s = 2$, $\mathfrak{p}_1 = \mathfrak{p}$, $n_1 = 3$, $x_1 = t = \alpha + 2$. Et on peut affirmer:

L'anneau A_S est formé des éléments de K du type $(x+y\alpha) / (\alpha+2)^m$ ($m \geq 0$; $x, y \in \mathbf{Z}$); A_S est un anneau principal: $h_S = 1$; enfin, le groupe U_S est formé des éléments du type $\pm (\alpha+2)^m$ ($m \in \mathbf{Z}$) (le fait que $\alpha + 2$ soit une « unité fondamentale » pour A_S tient à ce que $N(\alpha+2) = 8$ et que ni 2 ni 4 ne sont normes de S-unités de K).

BIBLIOGRAPHIE

[1] Chevalley, La théorie du corps de classes. *Ann. of Math.* (1940), 41, pp. 394-418.

[2] Artin-Whaples, Axiomatic characterization of fields by the product formula for valuations. *Bull. Am. Math. Soc.* (1945), 51, pp. 469-492.

[3] Artin, *Theory of algebraic numbers.* Göttingen (1959).

[4] Artin-Tate, *Class field theory.* Harvard (1960).

[5] Weiss, *Algebraic number theory.* McGraw-Hill (1963).

[6] Lang, *Algebraic numbers.* Addison-Wesley (1964).

[7] Borevich-Shafarevich, *Number theory.* Academic Press (1966).

[8] Cassels-Fröhlich, *Algebraic number theory.* Academic Press (1967).

[9] Weil, *Basic number theory.* Springer (1967).

[10] Samuel, *Théorie algébrique des nombres.* Hermann (1967).

Faculté des Sciences de Grenoble
Institut de Mathématiques pures

(Reçu le 30 julliet 1990)