§8. Corps quadratiques euclidiens. Factorisation. Entiers de Gauss.

Un corps quadratique k est dit <u>euclidien</u>, si, pour tout couple α, β d'entiers de k, on peut trouver deux autres entiers γ et δ tels que

$$\alpha = \beta\gamma + \delta \quad , \quad |N\delta| < |N\beta| .$$

On convient de dire que δ est <u>un reste de α modulo β</u>.

Dans un tel corps, il existe <u>un algorithme d'Euclide</u> : à partir de deux entiers α_0 et α_1, tels que $|N\alpha_1| < |N\alpha_0|$, on peut former une suite d'entiers α_k dans laquelle α_{k+1} est un reste de $\alpha_{k-1} \pmod{\alpha_k}$. Comme $|N\alpha_k|$ décroît, cette suite a un dernier terme non nul, et l'on vérifie que ce dernier terme engendre l'idéal (α, β).

<u>Théorème</u> <u>Dans l'anneau des entiers d'un corps euclidien, tout idéal est principal.</u>

Soit en effet $\mathfrak{a}$ un idéal $\neq (0)$ et β un nombre de $\mathfrak{a}$, $\neq 0$ et de norme minimum.

Si $\alpha \in \mathfrak{a}$, le reste de $\alpha \pmod{\beta}$ est nul, donc $\alpha \in (\beta)$ et $\mathfrak{a} = (\beta)$.

Corollaire Dans un corps euclidien, tout entier le laisse décomposer, d'une manière essentiellement unique, en un produit d'entiers irréductibles.

La condition pour qu'un corps soit euclidien revient à ceci : pour tout nombre ξ du corps, il existe un entier γ du corps, tel que $|N(\xi - \gamma)| < 1$.

En effet, si $|N\frac{\alpha}{\beta} - \gamma| < 1$, on a $\alpha = \beta\gamma + \delta$ avec δ entier et $|N\delta| < |N\beta|$.

Les corps quadratiques imaginaires sont $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$ et $\mathbb{Q}(\sqrt{-11})$, et il n'y en a pas d'autres. Cela est facile à vérifier, je ne reproduis pas la démonstration.

La détermination des corps quadratiques réels est plus difficile : $\mathbb{Q}(\sqrt{m})$ est euclidien pour $m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$. Ce sont les seuls corps quadratiques euclidiens.

On trouvera des renseignements là-dessus dans l'ouvrage : An introduction to the theory of numbers, de G.H. Hardy et E.M. Wright.

Considérons les entiers du corps $\mathbb{Q}(\sqrt{-1})$, ou entiers de Gauss, de la forme $a+bi$, et cherchons ceux qui sont irréductibles. Un entier irréductible peut être un nombre premier rationnel p, ou encore a p, c'est-à-dire égal à $\pm p$ ou $\pm ip$.

S'il ne l'est pas, $\pi = a+bi$ divise $\pi\overline{\pi} = (a+bi)(a-bi)$ ou $\pi\overline{\pi} = a^2+b^2$, et à cause de l'unicité de la décomposition en facteurs irréductibles, a^2+b^2 est nécessairement un nombre premier.

Comme $a^2+b^2 \not\equiv 3 \pmod 4$, un nombre premier $p \equiv 3 \pmod 4$ est irréductible.

Si $p \equiv 1 \pmod 4$, comme -1 est résidu quadratique $\pmod 4$, il existe un entier x tel que $p / x^2+1 = (x+i)(x-i)$. Comme p divise un produit sans diviser aucun des facteurs, p est réductible et il existe des entiers a et b tels que $p = a^2+b^2$.

Les deux facteurs irréductibles $\pi = a+bi$ et $\overline{\pi} = a-bi$ de p ne sont pas associés, car 2 ne divise pas la somme des nombres a et b est pair et l'autre impair.

Le nombre $2 = -i(1+i)^2$ est associé à un carré ; $2 = (1+i)(1-i)$, $1+i$ et $1-i$ sont associés.

Chercher les solutions de l'équation $x^2+y^2 = n$ en nombres entiers x et y revient à chercher les entiers de Gauss de norme n. Soit

$$n = 2^e p_1^{k_1} \cdots p_r^{k_r} q_1^{l_1} \cdots q_s^{l_s}$$

la décomposition de n en facteurs premiers, les p_i étant distincts et $\equiv 1 \pmod 4$, les q_j distincts et $\equiv 3 \pmod 4$. Si $p_j = \pi_j \overline{\pi_j}$, la décomposition de n en entiers de Gauss irréductibles s'écrit

$$n = (-i)^e (1+i)^{2e} \pi_1^{k_1} \overline{\pi}_1^{k_1} \cdots \pi_r^{k_r} \overline{\pi}_r^{k_r} q_1^{l_1} \cdots q_s^{l_s}.$$

On en déduit que, pour que n soit le produit de deux nombres conjugués, il faut et il suffit que les exposants l_j soient tous pairs. S'il en est ainsi, le nombre de solutions de l'équation $x^2+y^2 = n$ est

$$4(k_1+1)(k_2+1)\cdots(k_r+1).$$

Il existe des corps qui ne sont pas euclidiens et dans lesquels néanmoins tous les idéaux sont principaux. Par exemple $\mathbb{Q}(\sqrt{-19})$ comme on verra.

Mais il existe aussi des corps dans lesquels tous les idéaux ne sont pas principaux. Ainsi, dans $\mathbb{Q}(\sqrt{-5})$, les entiers sont $\xi = x + y\sqrt{-5}$ et $N\xi = \xi\bar{\xi} = x^2 + 5y^2$. Il n'existe pas d'entier de norme 2 ou 3, donc 2 et 3 sont indécomposables. Mais $6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5})$ montre qu'on a deux décompositions essentiellement différentes de 6. Le nombre $1+\sqrt{-5}$ est indécomposable (car s'il était le produit de deux entiers de norme < 6, leurs normes devraient être 2 et 3). L'idéal $(2, 1+\sqrt{-5})$ n'est pas principal, car il n'y a pas d'entier qui divise 2 et $1+\sqrt{-5}$ (sauf ± 1) et il n'est pas égal à (1) : on peut vérifier qu'il ne contient que des entiers rationnels pairs.