§7. Les entiers et les unités d'un corps quadratique.

On appelle <u>nombre algébrique</u> tout nombre α qui satisfait à une équation algébrique à coefficients entiers rationnels

$$P(x) \equiv a_0 x^n + a_1 x^{n-1} + \dots + a_n = 0 \quad .$$

Si de plus α satisfait à une telle équation où $a_0 = 1$, on dit que α est un <u>entier algébrique</u>.

Si $P(x)$ est irréductible, le degré n est appelé <u>degré du nombre algébrique</u>. Les nombres algébriques de degré 1 sont les nombres rationnels. Les nombres algébriques de degré 2 sont appelés <u>nombres quadratiques</u>.

Si m est un nombre rationnel qui n'est pas un carré, x et y deux nombres rationnels, alors $x + y\sqrt{m}$ est un nombre quadratique. L'ensemble de ces nombres, pour m fixe, forme un corps qu'on désigne par $Q(\sqrt{m})$, et qu'on appelle <u>corps quadratique</u>. Il est clair que ce corps ne change pas si l'on remplace m par $z^2 m$, où z est un nombre rationnel $\neq 0$. On peut par suite supposer que m est un entier $\neq 0$ et $\neq 1$

Si $\xi = x + y\sqrt{m}$, $\xi' = x - y\sqrt{m}$ est appelé le conjugué de ξ et $\xi\xi' = x^2 - my^2$ est la norme de ξ.

Cherchons les entiers de $\mathbb{Q}(\sqrt{m})$. Comme ξ satisfait à l'équation $X^2 - (\xi+\xi')X + \xi\xi' = 0$, il est entier si $\xi + \xi' = 2x$ et $\xi\xi' = x^2 - my^2$ sont entiers. Cela entraine que $m(2y)^2$ est entier, par suite $2y$ est aussi entier. En posant $t = 2x$ et $s = 2y$, on a $t^2 - ms^2 = 4(x^2 - my^2)$, donc $t^2 - ms^2 \equiv 0 \pmod 4$.

Si $m \equiv 2$ ou $3 \pmod 4$, cela entraine $t \equiv s \equiv 0 \pmod 2$ et x et y sont entiers. Les entiers de $\mathbb{Q}(\sqrt{m})$ sont alors les nombres de la forme $x + y\sqrt{m}$ avec $x, y \in \mathbb{Z}$

Si $m \equiv 1 \pmod 4$, cela entraine seulement que s et t sont de même parité. Les entiers de $\mathbb{Q}(\sqrt{m})$ sont alors les nombres de la forme $x + y\sqrt{m}$ où x et y sont ou bien des entiers, ou bien des entiers $+ \frac{1}{2}$; ou encore, ce qui revient au même, les nombres de la forme $x + y\frac{1+\sqrt{m}}{2}$, avec $x, y \in \mathbb{Z}$.

On vérifie immédiatement que la somme et le produit de deux entiers sont des entiers : les entiers de $\mathbb{Q}(\sqrt{m})$ forment un anneau. C'est aussi un module qui a une base formée par $[1, \sqrt{m}]$ ou $[1, \frac{1+\sqrt{m}}{2}]$ suivant le cas.

Un nombre algébrique α est appelé <u>une unité</u>, si α et $\frac{1}{\alpha}$ sont entiers. Les unités contenues dans le corps $Q(\sqrt{m})$ sont les éléments inversibles de l'anneau des entiers de ce corps, et forment un groupe multiplicatif. Cherchons à les déterminer.

Pour que l'entier ξ de $Q(\sqrt{m})$ soit une unité, il faut et il suffit que $N\xi = \xi\xi' = \pm 1$. Si $m \equiv 2$ ou $3 \pmod 4$, $\xi = x + y\sqrt{m}$, $N\xi = x^2 - my^2$ et l'on est ramené à la recherche des solutions en nombres entiers de l'équation

$$(1) \qquad x^2 - my^2 = \pm 1 .$$

Si $m \equiv 1 \pmod 4$, $\xi = \frac{u + v\sqrt{m}}{2}$ où u et v sont des entiers de même parité et l'on est ramené à la recherche des solutions en nombres entiers de l'équation

$$(2) \qquad u^2 - my^2 = \pm 4 ,$$

qui se ramène aussi à (1) si u et v sont pairs.

<u>Cas où m est négatif.</u> Le corps $Q(\sqrt{m})$ est alors appelé un corps imaginaire. Si $m < -3$, on voit qu'il n'y a pas d'autre unité que 1 et -1.

Pour $m=-1$, on trouve les 4 racines 4-ièmes de l'unité ± 1 et $\pm i$ et pour $m=-3$ les 6 racines 6-ièmes de l'unité ± 1 et $\frac{\pm 1 \pm \sqrt{-3}}{2}$.

Cas où m est positif. Le corps $\mathbb{Q}(\sqrt{m})$ est alors un corps quadratique réel.

Supposons que ξ soit une unité différente de 1 et -1. Alors $\xi\xi' = \pm 1$, et $-\xi$, ξ', $-\xi'$ sont comme ξ des unités. De ces 4 unités, deux sont positives et l'une est supérieure à 1. Supposons que c'est $\xi = a + b\sqrt{m}$. Comme $\xi' = a - b\sqrt{m}$, $-\xi = -a - b\sqrt{m}$ et $-\xi' = -a + b\sqrt{m}$, ξ étant la plus grande des quatre, on a $a > 0$ et $b > 0$. Comme a et b sont des entiers rationnels ou des moitiés d'entiers impairs, cela entraîne qu'il ne peut exister qu'un nombre fini d'unités > 1 et $< M$, M étant un nombre fixé arbitrairement. Par suite, s'il existe des unités $\neq \pm 1$, il y a une unité > 1 plus petite que toutes les autres. Elle est appelée unité fondamentale du corps $\mathbb{Q}(\sqrt{m})$.

Si ε est cette unité fondamentale, $\pm\varepsilon^k$ $(k \in \mathbb{Z})$ est encore une unité. Il n'y en a pas d'autre, car toute unité $\xi > 0$ étant comprise dans un intervalle $\varepsilon^k \leq \xi < \varepsilon^{k+1}$,

l'unité $\xi\varepsilon^{-k}$ satisfaisant à $1 \leq \xi\varepsilon^{-k} < \varepsilon$ est égale à 1 et $\xi = \varepsilon^k$.

Exemples. Dans $Q(\sqrt{2})$, $1+\sqrt{2}$ est l'unité fondamentale. Dans $Q(\sqrt{3})$, c'est $2+\sqrt{3}$ et dans $Q(\sqrt{5})$ c'est $\frac{1+\sqrt{5}}{2}$, ainsi qu'on le vérifie facilement.

Voici, pour quelques valeurs de m, l'unité fondamentale ε de $Q(\sqrt{m})$ et sa norme $N\varepsilon$.

m	2	3	5	6	7	10	11	19	31
ε	$1+\sqrt{2}$	$2+\sqrt{3}$	$\frac{1+\sqrt{5}}{2}$	$5+2\sqrt{6}$	$8+3\sqrt{7}$	$3+\sqrt{10}$	$10+3\sqrt{11}$	$170+39\sqrt{19}$	$1520+273\sqrt{31}$
$N\varepsilon$	-1	1	-1	1	1	-1	1	1	1

On peut trouver l'unité fondamentale en cherchant le plus petit entier rationnel positif y (resp. v) tel que $my^2 \pm 1$ (resp. $mv^2 \pm 4$) soit un carré parfait. Une autre méthode, meilleure lorsque m n'est pas très petit, est basée sur la théorie des fractions continues (voir §16).

C'est Lagrange qui a prouvé le premier que tout corps quadratique réel contient des unités $\neq \pm 1$. Il suffit de montrer que l'équation $x^2 - my^2 = 1$ a des solutions en entiers x, y avec $y \neq 0$. La démonstration suivante

est due à Dirichlet.

Montrons d'abord qu'il existe une infinité de couples d'entiers x, y satisfaisant à $|x^2 - my^2| < 1 + 2\sqrt{m}$

Soit n un entier positif. En donnant à t les $n+1$ valeurs $0, 1, 2, \ldots, n$ et désignant par $s = [t\sqrt{m}]$ la partie entière de $t\sqrt{m}$, on obtient $n+1$ nombres $-s + t\sqrt{m}$ tous ≥ 0 et < 1. Par suite, l'un au moins des n intervalles $\left[\frac{i-1}{n}, \frac{i}{n}\right[$ $(i = 1, 2, \ldots, n)$ contient deux de ces nombres (C'est le principe des tiroirs de Dirichlet : si n tiroirs contiennent plus de n objets, un tiroir au moins contient au moins deux objets). La différence $x + y\sqrt{m}$ de ces deux nombres satisfait alors à

$$0 < |x - y\sqrt{m}| < \frac{1}{n}$$

et l'on peut supposer $y > 0$, de sorte que $0 < y \leq n$. L'égalité est exclue car $\sqrt{m}$ est irrationnel. Cela entraîne

$$|x + y\sqrt{m}| \leq |x - y\sqrt{m}| + 2y\sqrt{m} < \frac{1}{n} + 2y\sqrt{m}$$

d'où

$$|x^2 - my^2| = |x - y\sqrt{m}|\,|x + y\sqrt{m}| < \frac{1}{n^2} + \frac{2y}{n}\sqrt{m} < 1 + 2\sqrt{m}$$

En prenant n de plus en plus grand, on fera tendre $x - y\sqrt{m}$ vers zéro et l'on a bien une infinité de solutions.

L'une des valeurs de $x^2 - my^2$, soit k, sera prise une infinité de fois, c'est-à-dire que l'équation $x^2 - my^2 = k$ aura une infinité de solutions, et il y aura certainement deux solutions distinctes x', y' et x'', y'' telles que $x' \equiv x''$ et $y' \equiv y'' \pmod{k}$. En posant

$$(x' - y'\sqrt{m})(x'' + y''\sqrt{m}) = x_1 + y_1\sqrt{m},$$

on a $x_1^2 - m y_1^2 = k^2$ et

$x_1 = x'x' - y'y''m \equiv x'^2 - my'^2 \equiv 0 \pmod{k}$,

$y_1 = x'y'' - x''y' \equiv 0 \pmod{k}$. Par suite,

$x = \frac{x_1}{k}$ et $y = \frac{y_1}{k}$ sont des entiers satisfaisant à $x^2 - my^2 = 0$ et $y \neq 0$.

Remarque On a prouvé d'abord qu'il existe une infinité d'entiers de $\mathbb{Q}(\sqrt{m})$ dont la norme est en valeur absolue inférieure à $1 + 2\sqrt{m}$, et ensuite que parmi ces entiers il y en a forcément deux dont le rapport est une unité, car on a en effet

$$\frac{x' - y'\sqrt{m}}{x'' - y''\sqrt{m}} = \frac{(x' - y'\sqrt{m})(x'' + y''\sqrt{m})}{k} = x + y\sqrt{m}.$$