§9. Les idéaux de l'anneau des entiers d'un corps quadratique et leur décomposition en produit d'idéaux premiers.

Définitions. On appelle produit de deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ d'un anneau A, l'idéal $\mathfrak{a}\mathfrak{b}$ formé par toutes les sommes de produits d'un nombre de $\mathfrak{a}$ par un nombre de $\mathfrak{b}$.

Si $\mathfrak{a} = (\alpha_1, \alpha_2, \dots, \alpha_r)$ et $\mathfrak{b} = (\beta_1, \beta_2, \dots, \beta_s)$

$$\mathfrak{a}\mathfrak{b} = (\alpha_1\beta_1, \dots, \alpha_1\beta_s, \dots, \alpha_r\beta_s)$$

En particulier, si $\mathfrak{a} = (\alpha)$ et $\mathfrak{b} = (\beta)$ sont [illegible]

La multiplication des idéaux est commutative, associative, l'idéal $(1) = A$ joue le rôle d'unité.

On désignera encore par $\mathfrak{a} + \mathfrak{b}$

$$\mathfrak{a} + \mathfrak{b} = (\alpha_1, \alpha_2, \dots, \alpha_r, \beta_1, \beta_2, \dots, \beta_s)$$ [illegible] sommes d'un nombre de $\mathfrak{a}$ et de [illegible]

C'est le plus petit idéal qui contient [illegible]

[illegible]

On dira que l'idéal $\mathfrak{c}$ *divise* $\mathfrak{a}$, s'il existe un idéal $\mathfrak{c}$ tel que $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.

Un idéal $\mathfrak{p} \neq (0)$ de A est dit *premier*, si l'anneau quotient $A/\mathfrak{p}$ est intègre, ou, ce qui revient au même, si le produit de deux nombres de A ne peut appartenir à $\mathfrak{p}$ sans qu'un de ces nombres appartienne à $\mathfrak{p}$.

Passons maintenant à l'étude des idéaux de l'anneau des entiers de $\mathbb{Q}(\sqrt{m})$, qu'on appellera aussi en abrégé *idéaux de* $\mathbb{Q}(\sqrt{m})$. Nous commencerons par le

Lemme. *Pour tout idéal* $\mathfrak{a}$ *de* $\mathbb{Q}(\sqrt{m})$, $\mathfrak{a} \neq 0$, *on peut trouver un autre idéal* $\mathfrak{m}$ *tel que* $\mathfrak{a}\mathfrak{m} =$ *idéal principal* $\neq 0$.

D'une manière plus précise, nous montrerons que si $\mathfrak{a}'$ est l'idéal conjugué de $\mathfrak{a}$ (formé par les conjugués des nombres de $\mathfrak{a}$), *le produit* $\mathfrak{a}\mathfrak{a}'$ *est un idéal engendré par un entier rationnel.*

Pour cela, remarquons d'abord que tout idéal peut être engendré par deux nombres. En effet,

un idéal $\mathfrak{a} \neq (0)$ de $Q(\sqrt{m})$ est un sous-module du module de tous les entiers de $Q(\sqrt{m})$, de rang 2, et possède donc une base formée de deux nombres qui évidemment engendrent l'idéal.

Soit alors $\mathfrak{a} = (\alpha, \beta)$, $\mathfrak{a}' = (\alpha', \beta')$. On a $\mathfrak{a}\mathfrak{a}' = (\alpha\alpha', \alpha\beta', \beta\alpha', \beta\beta')$. Si d est le p.g.c.d. des entiers rationnels $\alpha\alpha'$, $\alpha\beta' + \beta\alpha'$, $\beta\beta'$, on a $(d) = (\alpha\alpha', \alpha\beta' + \beta\alpha', \beta\beta')$.

On va montrer que $(d) = \mathfrak{a}\mathfrak{a}'$. Il est évident que $\mathfrak{a}\mathfrak{a}' \supset (d)$ et il suffira de prouver que $\alpha'\beta \in (d)$.

Pour cela, nous utiliserons le fait que si ρ est racine d'un polynôme $P(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$ à coefficients entiers rationnels, $a_0\rho$ est un entier algébrique, car $a_0\rho$ est racine de $Q(y) = a_0^{n-1} P\left(\frac{y}{a_0}\right) = y^n + \dots + a_0^{n-1} a_n$.

Appliquons cette remarque à $P(x) = \frac{(\alpha x - \beta)(\alpha' x - \beta')}{d} = \frac{\alpha\alpha'}{d} x^2 + \dots$.
C'est un polynôme à coefficients rationnels dont $\frac{\beta}{\alpha}$ est une racine. Par suite $\frac{\alpha\alpha'}{d} \frac{\beta}{\alpha} = \frac{\alpha'\beta}{d}$ est un entier, $d / \alpha'\beta$ et $\alpha'\beta \in (d)$. c.q.f.d.

Proposition (unicité de la division).

Si $a_1 b = a_2 b$ et $b \neq (0)$, alors $a_1 = a_2$.

Démonstration. Soit $b b' = (b)$. L'hypothèse entraîne $a_1(b) = a_2(b)$ et l'on est ramené au cas où b est principal. Mais les nombres de a_1 sont les quotients par b des nombres de $a_2(b)$ et de même ceux de a_2 puisque $a_2(b) = a_1(b)$, donc $a_1 = a_2$.

Proposition (critère de divisibilité).

Pour que b divise a, il faut et il suffit que $b \supset a$.

Démonstration. Si $a = bc$, il est évident que $b \supset a$. Inversement, si $b \supset a$, on a $(b) = bb' \supset ab'$; l'idéal c formé des quotients par b des nombres de ab' satisfait à $ab' = (b)c = bb'c$ d'où, en divisant par b', $a = bc$.

Nous voyons ainsi que, pour les idéaux, "diviser" signifie "contenir". Aussi l'idéal $a + b$, plus petit idéal contenant a et b, est-il aussi la juste valeur appelé le p.g.c.d. de a et b. Si $a + b = (1)$ on dit que a et b sont premiers entre eux.

Le quotient $A/\mathfrak{a}$ de l'anneau A des entiers de $\mathbb{Q}(\sqrt{m})$ par un idéal $\mathfrak{a} \neq 0$ est fini. En effet, si $[1, \omega]$ est une base de A, comme $\mathfrak{a}$ contient un entier rationnel n, tout nombre de A est $\equiv \pmod{n}$ et par suite $\pmod{\mathfrak{a}}$ à l'un des n^2 nombres $x + y\omega$ $(x = 0, 1, \ldots, n-1 ; y = 0, 1, \ldots, n-1)$.

L'homomorphisme canonique de A sur $A/\mathfrak{a}$ établissant une bijection de l'ensemble des idéaux de A qui contiennent (c.a.d. divisent) $\mathfrak{a}$ et l'ensemble des idéaux de $A/\mathfrak{a}$, il en résulte que le nombre des idéaux qui divisent $\mathfrak{a}$ est fini.

Dans le cas d'un idéal premier $\mathfrak{p}$, l'anneau $A/\mathfrak{p}$ étant intègre et fini est un corps. Par suite $\mathfrak{p}$ n'a pas d'autres diviseurs que (1) et lui-même.

Lemme d'Euclide généralisé :

Si $m \mid \mathfrak{a}\mathfrak{b}$ et $\mathfrak{a} + m = (1)$, alors $m \mid \mathfrak{b}$

En effet, l'hypothèse entraîne $\mathfrak{b} = (\mathfrak{a} + m)\mathfrak{b} = \mathfrak{a}\mathfrak{b} + m\mathfrak{b} \subset m$ c.a.d. $m \mid \mathfrak{b}$.

En particulier, si $\mathfrak{p}$ est un idéal premier et $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$, alors $\mathfrak{p} \mid \mathfrak{a}$ ou $\mathfrak{p} \mid \mathfrak{b}$, puisque si $\mathfrak{p} \nmid \mathfrak{a}$ on a $\mathfrak{a} + \mathfrak{p} = (1)$, le seul idéal divisant $\mathfrak{p}$ autre que $\mathfrak{p}$ étant (1).

De ce qui précède, en raisonnant comme au §1 sur le théorème fondamental de l'arithmétique, on déduit le

Théorème. *Tout idéal d'un corps quadratique peut être décomposé, d'une manière unique, en un produit d'idéaux premiers.*

On écrira cette décomposition $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{a})}$, le produit étant étendu à tous les idéaux premiers $\mathfrak{p}$, et les exposants $n_{\mathfrak{p}}(\mathfrak{a})$ étant nuls sauf pour un nombre fini de $\mathfrak{p}$. Notons encore les formules

$$n_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) = n_{\mathfrak{p}}(\mathfrak{a}) + n_{\mathfrak{p}}(\mathfrak{b}), \quad n_{\mathfrak{p}}(\mathfrak{a}+\mathfrak{b}) = \inf\{n_{\mathfrak{p}}(\mathfrak{a}), n_{\mathfrak{p}}(\mathfrak{b})\}.$$

L'idéal $\mathfrak{a} \cap \mathfrak{b}$, intersection de $\mathfrak{a}$ et $\mathfrak{b}$, est le plus petit commun multiple de $\mathfrak{a}$ et $\mathfrak{b}$, et $n_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) = \sup\{n_{\mathfrak{p}}(\mathfrak{a}), n_{\mathfrak{p}}(\mathfrak{b})\}$.