§ 9. Les idéaux de l'anneau des entiers d'un corps quadratique et bien décomposables en deux idéaux.

Définitions. On appelle produit de deux idéaux \( \alpha \) et \( \beta \) d'un anneau \( A \), l'idéal additif formé par toutes les sommes de produits de \( \alpha \) par un nombre de \( \beta \).

\[ \alpha \beta = (\alpha_1 \beta_1, \alpha_2 \beta_2, \ldots, \alpha_n \beta_n) \]

En particulier, si \( \alpha = \langle A \rangle \) et \( \beta = \langle B \rangle \) sont les idéaux associés, l'idéal \( (\alpha \beta) = \langle AB \rangle \) sera l'idéal directe.

On désignera encore par \( \alpha + \beta \)

\[ \alpha + \beta = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_n + \beta_n) \]

tous les nombres d'un nombre de \( \alpha \) et de \( \beta \) additifs.

C'est le plus petit idéal qui contient \( \alpha \) et \( \beta \).

\[ \langle \alpha \beta \rangle = \langle \alpha + \beta \rangle \]
On dira que l'ideal \( \mathfrak{a} \) dérivé de \( \mathfrak{a} \), s'il existe, un ideal \( \mathfrak{a} \) tel que \( \mathfrak{a} = \mathfrak{a} \mathfrak{c} \).

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

Passons maintenant à l'étude de l'ideaux de l'anneau des entiers de \( \mathcal{O}(\sqrt{m}) \), qu'on appelle aussi les algèbre de \( \mathcal{O}(\sqrt{m}) \) : Nous commençons par le lemme. Pour tout ideal \( \mathfrak{a} \) de \( \mathcal{O}(\sqrt{m}) \), \( \mathfrak{a} \neq \mathfrak{0} \), on peut trouver un autre ideal \( \mathfrak{m} \) tel que \( \mathfrak{a} \mathfrak{m} = \text{ideal principal } \neq \mathfrak{0} \).

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

Pour cela, remarque d'abord que tout ideal peut être engendré par deux nombres. En effet,
un idéal \( \alpha \neq (0) \) de \( \mathbb{Q}((v)) \) est un sous-module du module de tous les entiers de \( \mathbb{Q}((v)) \), de rang 2, et possède donc une base formée de deux nombres qui évidemment engendrent l'idéal.

Soit alors \( \alpha = (\alpha, \beta) \), \( \alpha' = (\alpha', \beta) \). On a \( \alpha \cap \alpha' = (\alpha \alpha', \alpha' \beta, \beta \alpha', \beta' \beta) \). 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 \( (d) = \alpha \alpha' \). Il est évident que \( \alpha \alpha' \supset (d) \) et il suffira de prouver que \( \alpha' \beta \in (d) \).

Pour cela, nous utiliserons le fait que si \( p \) est une racine d'un polynôme \( P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \) à coefficients entiers rationnels, \( a_n \) est un entier algbrique, car \( a_n \) est racine de \( Q(y) = y^n + \ldots + a_0 \).

Appliquons cette remarque à \( P(x) = \frac{(\alpha x - \beta)(\alpha' x - \beta')}{d^2} = \frac{\alpha \alpha' x^2}{d^2} + \ldots \).

C'est un polynôme à coefficients rationnels dont \( \frac{\beta}{\alpha} \) est une racine. Par suite \( \frac{\alpha \alpha'}{d^2} \frac{\beta}{\alpha} = \frac{\alpha' \beta}{d^2} \) est un entier,

\( d/\alpha' \beta \) et \( \alpha' \beta \in (d) \). c.q.f.d.
Proposition (unité de la division).

Soit \( \alpha_1 \beta = \alpha_2 \beta' \) et \( \beta \neq (0) \), alors \( \alpha_1 = \alpha_2 \).

Démonstration. Soit \( \beta \beta' = (\beta) \). L'hypothèse entraîne \( \alpha_1(\beta) = \alpha_2(\beta') \) et l'on est ramené au cas où \( \beta \) est principal. Mais les nombres de \( \alpha_2 \) sont les quidets par \( \beta \) des nombres de \( \alpha_2(\beta) \) et de même ceux de \( \alpha_2 \) (puisque \( \alpha_2(\beta) = \alpha_1(\beta) \)), donc \( \alpha_1 = \alpha_2 \).

Proposition (carré de divisibilité).

Pour que \( \beta \) divise \( \alpha_2 \), il faut et il suffit que \( \beta \mid \alpha_2 \).

Démonstration. Si \( \alpha_2 = \beta \beta' \), il est évident que \( \beta \mid \alpha_2 \).

Inversement, si \( \beta \mid \alpha_2 \), on a \( \alpha_2(\beta) = \beta \beta' \alpha_2 \); l'idéal \( \beta \) formé des quidets par \( \beta \) des nombres de \( \alpha_2 \) satisfait à \( \alpha_2 \beta = (\beta) \alpha_2 = \beta \beta' \), d'où, en divisant \( \beta \beta' \), \( \alpha_2 = \beta \alpha_2 \).

Nous savons ainsi que, dans les idéaux, "diviser" signifie "contenir". Ainsi l'idéal \( \alpha + \beta \), plus petit idéal contenant \( \alpha \) et \( \beta \), est-il antérieur \( \alpha \) et \( \beta \), appelé le p.g.c.d. de \( \alpha + \beta \). Si \( \alpha + \beta = (1) \) on dit que \( \alpha \) et \( \beta \) sont premiers entre eux.
Le quotient $\mathbb{A}/\alpha$ de l'anneau $\mathbb{A}$ des entiers de $\mathbb{Q}(\sqrt{m})$ par un idéal $\alpha \neq 0$ est fini. En effet, si $[1, \omega]$ est une base de $\mathbb{A}$, comme $\alpha$ contient un entier rationnel $n$, tout nombre de $\mathbb{A}$ est $\equiv (mod n)$ et $\equiv (mod \alpha)$ à l'un des $n^2$ nombres $x + y \omega$ ($x = 0, 1, \ldots, n-1; y = 0, 1, \ldots, n-1$).

L'isomorphisme canonique de $\mathbb{A}$ sur $\mathbb{A}/\alpha$ établit une bijection de l'ensemble des idéaux de $\mathbb{A}$ qui contiennent $\alpha$ et $\mathbb{A}/\alpha$. Il en résulte que le nombre des idéaux qui contiennent $\alpha$ est fini.

Dans le cas d'un idéal premier $\mathfrak{p}$, l'anneau $\mathbb{A}/\mathfrak{p}$ est 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 $m/\alpha \mathfrak{b}$ et $\alpha + m = (1)$, alors $m/\mathfrak{b}$.

En effet, l'idéal intègre $\mathfrak{b} = (\alpha + m)\mathfrak{b} = \alpha \mathfrak{b} + m \mathfrak{b} \subseteq m\mathfrak{b}$, c.a.d. $m/\mathfrak{b}$. 


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

De ce qui précède, en raisonnant comme au §23 du 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'ideaux premiers.

On trouve cette décomposition $\mathfrak{a} = \prod \mathfrak{p}^{\eta_{\mathfrak{p}}(\mathfrak{a})}$, le produit étant étendu à tous les idéaux premiers $\mathfrak{p}$, et les exposants $\eta_{\mathfrak{p}}(\mathfrak{a})$ étant tous pairs ou un nombre fini de $\mathfrak{p}$. Notons encore les formules

$$
\eta_{\mathfrak{p}}(\mathfrak{a} \mathfrak{b}) = \eta_{\mathfrak{p}}(\mathfrak{a}) + \eta_{\mathfrak{p}}(\mathfrak{b}), \quad \eta_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = \min \{\eta_{\mathfrak{p}}(\mathfrak{a}), \eta_{\mathfrak{p}}(\mathfrak{b})\}.
$$

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