§11. Les idéaux premiers et le caractère d'un corps quadratique.

Soit $\mathfrak{p}$ un idéal premier du corps $K = \mathbb{Q}(\sqrt{m})$ de plus petit entier rationnel positif contenu dans $\mathfrak{p}$ est un nombre premier $p$, et comme $\mathfrak{p}/(p)$, $N_{\mathfrak{p}}/N(p) = p^2$. Donc $N_{\mathfrak{p}} = p$ ou $p^2$. On peut alors distinguer 3 cas.

1er cas. $N_{\mathfrak{p}} = p^2$, alors $\mathfrak{p} = (p)$ est un idéal premier, engendré par un nombre premier.

2e cas. $N_{\mathfrak{p}} = p$ et $(p) = \mathfrak{p} \mathfrak{p}'$, $\mathfrak{p} \neq \mathfrak{p}'$. L'idéal $(p)$ engendré par $p$ est le produit de deux idéaux premiers distincts.

3e cas. $N_{\mathfrak{p}} = p$ et $(p) = p^2$, $\mathfrak{p} = \mathfrak{p}'$. L'idéal $(p)$ engendré par $p$ est le carré d'un idéal premier.

Posons encore $\omega = \begin{cases} \sqrt{m} & m \equiv 2 \text{ ou } 3 \pmod{4} \\ \frac{1 + \sqrt{m}}{2} & m \equiv 1 \pmod{4} \end{cases}$

on voit que $[1, \omega]$ est une base du module des entiers de $K$.

Dans les 2-ième et 3-ième cas, $(0, 1, \ldots, p-1)$ est un système complet de restes $\pmod{\mathfrak{p}}$, de sorte—
que \( \omega \equiv \text{un entier rationnel } r \pmod{p} \). Alors

\[
\beta / \omega - 2, \quad \beta' / \omega' - 2 \quad \text{et} \quad \beta / (\omega - 2)(\omega' - 2), \quad \text{où } p / (\omega - 2)(\omega' - 2).
\]

Si \( m \equiv 0 \pmod{4} \), alors \( \omega = \sqrt{m} \) et \( (\omega - 2)(\omega' - 2) = \omega^2 - m \equiv 0 \pmod{p} \).

D'où \( (z2)^2 \equiv 4m \pmod{p} \).

Si \( m \equiv 1 \pmod{4} \), alors \( \omega = \frac{1 + \sqrt{m}}{2} \) et

\[
(\omega - 2)(\omega' - 2) = \frac{(1 - z2 + \sqrt{m})(1 - z2 - \sqrt{m})}{4} = \frac{(1 - z2)^2 - m}{4} \equiv 0 \pmod{p}
\]

D'où \( (1 - z2)^2 \equiv m \pmod{p} \).

Le nombre \( D = (\omega - \omega')^2 = |1/\omega|^2 = \begin{cases} \frac{m}{4} & \text{si } m \equiv 1 \pmod{4} \\ 4m & \text{si } m \equiv 2 \pmod{4} \end{cases} \)

est appelé le discriminant du corps \( \mathbb{Q} / \sqrt{m} \). Nous voyons que, dans le 2-ième et dans le 3-ième cas, c'est-à-dire lorsque \( p \) est le produit de deux idéaux, on a \( D \equiv \text{un carré } \pmod{p} \).

Montrons que réciproquement, si \( D \equiv x^2 \pmod{p} \), \( p \) est le produit de deux idéaux .

Si \( D = tw, m \equiv 2 \pmod{4} \), x doit être pair, \( x = 2r \), d'où \( 2z \equiv m \pmod{p} \), \( \beta / z^2 - m = (\omega - 2)(\omega' - 2) \), et comme \( p \) divise un produit sans doute aucun des facteurs, \( p \) est pas premier.

\( p = \beta \beta' \) avec \( \beta = (p, z - \omega) \), \( \beta' = (p, z - \omega') \).
Si \( D = m \), \( m \equiv 1 \pmod{4} \), \( x \) doit être impair, \( x = 2n - 1 \),
d'où \( (2n - 1)^2 \equiv m \pmod{4p} \) et \( p / (2n - 1 - m) \) de sorte que, comme à-dessus, \( (p) = \mathfrak{p} \mathfrak{p}' \) avec \( \mathfrak{p} = (p,2n-m), \mathfrak{p'} = (p,2n-m) \).

Il n'est à distinguer les 2-ième et 3-ième cas. Si \( (p) = \mathfrak{p} \mathfrak{p}' \)
\( \mathfrak{p} = \mathfrak{p}' \), alors \( m \equiv 2 \pmod{4p} \) et \( m' \equiv 2 \pmod{4p} \), d'où
\( m - m' \equiv 0 \pmod{4p} \) et \( \mathfrak{p}^2 / (m - m')^2 \) ou \( p / D \).
Mentionnons que n'importe quel si \( p / D \), on a \( (p) = \mathfrak{p}^2 \).
D'abord, si \( p \nmid m \), on a \( (p) = (p, \sqrt{m})^2 \). Ensuite,
si \( p \mid m \) et \( p / D \), on a \( p = 2 \) et \( m \equiv 3 \pmod{4}, D = 4m \); alors \( (2) = (2, \sqrt{m} - 1)^2 \) comme on l'affirme ailleurs :
\( (2, \sqrt{m} - 1)^2 = (4, 2\sqrt{m} - 2, m + 1 - 2\sqrt{m}) = (2)(2, \sqrt{m} - 1 \ \frac{m + 1 - \sqrt{m}}{2}) = (2)(2, \frac{m - 1}{2}) = (2) \).

Nous voyons que \( (p) \) est le carré d'un idéal si \( p / D \) et dans ce cas seulement.

Si \( p \) est impair et \( p / D \), \( D \) est rendu quadratique \( (\pmod{4p}) \) en même temps que \( (\pmod{p}) \), car
\( x^2 \equiv D \pmod{p} \), \( x \) ou \( x+p \) est de même parité que \( D \) et \( D \equiv x^2 \) ou \( (x + p)^2 \pmod{4p} \). En utilisant le symbolé de Legendre, nous voyons que...
l'idéal \((\mathfrak{p})\) se décompose ou ne se décompose pas selon que
\[
\left(\frac{D}{\mathfrak{p}}\right) = 1 \quad \text{ou} \quad \left(\frac{D}{\mathfrak{p}}\right) = -1.
\]
Si \(p = 2\) et \(D\) est impair, comme \(D \equiv 1 \pmod{4}\), on a \(D \equiv 1\) ou \(5 \pmod{8}\). Si \(D \equiv 1 \pmod{8}\),
\(D\) est résidu quadratique \(\pmod{8}\) et (2) ne se décompose tandis que ce n'est pas le cas si \(D \equiv 5 \pmod{8}\).
Remarquons que si \(D \equiv 1 \pmod{8}\) on a \((\frac{D}{8}) = 1\),
et \((\frac{D}{8}) = -1\) si \(D \equiv 5 \pmod{8}\).

Pour énoncer sous forme concise les résultats obtenus,
it est commode d'introduire une fonction \(\chi(x)\) appelée le caractère du corps \(\mathbb{Q}\) de discriminant \(D\).

**Définition.** On appelle caractère du corps \(\mathbb{Q}\) de discriminant \(D\), et l'on dénote par \(\chi(x) = \chi_D(x)\), la fonction définie pour \(x\) entier positif par les conditions suivantes:

a) elle est multiplicative : \(\chi(ab) = \chi(a)\chi(b)\)

b) pour \(x\) premier, on a
\[
\chi(x) = \begin{cases} 
0 & \text{si } x \nmid D \\
\left(\frac{D}{x}\right) & \text{si } x \text{ est premier impair et } x \nmid D, \\
(-1)^{\frac{D-1}{8}} & \text{si } x = 2 \text{ et } D \text{ est impair.}
\end{cases}
\]
Nous pouvons alors énoncer le théorème suivant qui résume les résultats obtenus.

**Théorème.** Dans le corps quadratique de caractère $\chi(x)$, l'idéal $(p)$ engendré par un nombre premier $p$ est la carré d'un idéal, le produit de deux idéaux premiers distincts ou est lui-même un idéal premier, selon que $\chi(p) = 0$, $1$ ou $-1$.

En utilisant la loi de réciprocité quadratique, nous allons donner une autre expression de $\chi(x)$ et nous verrons que sa valeur ne dépend que du reste de $x \mod D$.

Un discriminant $D$ est dit **primitif**, s'il n'est divisible que par un nombre premier. Les discriminants primitifs sont les nombres

- $D = p^2$, où $p$ est premier et $p \equiv 1 \mod 4$, pour $\mathbb{Q}(\sqrt{p})$;
- $D = -4$, $8$ et $-8$ pour les corps $\mathbb{Q}(\sqrt{17})$, $\mathbb{Q}(\sqrt{19})$, $\mathbb{Q}(\sqrt{23})$.  

Tout discriminant d'un corps quadratique est un produit de discriminants primitifs.
Soient en effet \( p_1, p_2, \ldots, p_k \) les facteurs premiers impairs du discriminant \( D \) qui sont \( \equiv 1 \pmod{4} \) et \( q_1, q_2, \ldots, q_s \) ceux qui sont \( \equiv 3 \pmod{4} \). Si \( D \) est impair, \( D = \pm p_1 \cdots p_k q_1 \cdots q_s = \pm (-1)^d \pmod{4} \), comme \( D \equiv 1 \pmod{4} \), la signe \( \pm \) est celui de \( (-1)^d \) et \( D = p_1 \cdots p_k (-q_1) \cdots (-q_s) \). C'est bien un produit de discriminants primilifs. Si \( D = 4m \) et \( m \equiv 3 \pmod{4} \),

\[
m = \pm p_1 \cdots p_k q_1 \cdots q_s \equiv \pm (-1)^d \equiv -1 \pmod{4} \text{ et }
\]

\[
m = - p_1 \cdots p_k (-q_1) \cdots (-q_s) , \quad D = (-4) \prod p_k (-q_1) \cdots (-q_s).
\]

Enfin, si \( D = 4m \) et \( m \equiv 2 \pmod{4} \), on a

\[
D = \pm 8 \ p_1 \cdots p_k (-q_1) \cdots (-q_s).
\]

Pour un discriminant primilif \( D = p_1, q_1, q_2, \ldots \), le caractère \( \chi_D(x) \) du corps correspondant est égal, en vertu de la loi de réciprocité, pour \( x \) premier à \( D \), à

\[
\chi_D(x) = \left( \frac{x}{p_1} \right) , \quad \chi_D(x) = \left( \frac{x}{q_1} \right) , \quad \chi_D(x) = \left( \frac{x}{q_2} \right) , \quad \chi_D(x) = \left( \frac{x}{q_3} \right) , \quad \chi_D(x) = \left( \frac{x}{q_4} \right) .
\]

et

\[
\chi_D(x) = \left( \frac{x}{q_5} \right) \chi_D(x) = \left( \frac{x}{q_6} \right) .
\]

Il résulte de la loi qu'il ne dépend que du reste de \( x \) (mod \( D \)).
Soit maintenant $D = D_1 D_2 \ldots D_k$ un discriminant quelconque, produit des discriminants premiers $D_i$. Il résulte de la définition du caractère et des propriétés du symbole de Legendre que l'on a

$$
\chi_D(x) = \chi_{D_1}(x) \chi_{D_2}(x) \ldots \chi_{D_k}(x).
$$

Comme $\chi_{D_i}(x)$ ne dépend que du caractère vert de $x$ $(\text{mod } D_i)$, $\chi_D(x)$ ne dépend que du vert de $x$ $(\text{mod } D)$. Le caractère $\chi(x)$ du corps de discriminant $D$ jouit de la propriété que $\chi(x_2) = \chi(x_1)$ si $x_1 \equiv x_2 \pmod{D}$.

Toute fonction multiplicative jouissant de cette propriété et non identiquement nulle est appelée un caractère $(\text{mod } D)$. Le fonction considérée ici n'est qu'un exemple :

En tenant compte de ce qui précède, on vérifie que, pour $(x, D) = 1$, on a

\[
\chi_D(x) = \begin{cases} 
1 & \text{si } D = 4m \text{ ou } m \equiv 1 \pmod{4}, \\
(-1)^{\frac{x}{m}} (\frac{x}{m}) & \text{si } D = 4m \text{ et } m \equiv 3 \pmod{4}, \\
\varepsilon(D) \cdot \chi(D) & \text{si } D = 4m \equiv 8m'. 
\end{cases}
\]