Sorbonne Université
Théorie des Nombres 2 (MU4MA034)
Mars–Mai 2021.

Séance 6, 26 mars 2021

Premiers inertes, ramifies et totalement décomposés

- Pour chaque $n > 1$, μ_n, resp. μ_n', note l'ensemble des racines de l'unité dans $\mathbb{C}$, resp. les racines primitives.
- Si K est un corps de nombres, Δ_K note *le* discriminant de K. Il s'agit d'un entier.
- Si K est un corps de nombres, un idéal premier de K est un idéal premier de $\mathfrak{O}_K$. Pour un tel premier $\mathfrak{p}$, le corps résiduel $\mathfrak{O}_K/\mathfrak{p}$ sera noté $\mathbb{F}_\mathfrak{p}$.

Exercice 1. Soit $m \in \mathbb{Z} \smallsetminus \{0, 1\}$ un entier sans facteur carré et $K = \mathbb{Q}(\sqrt{m})$. Le discriminant de K sera noté par d dans la suite.

1/ Rappeler le lien entre d et m. En déduire que d détermine K.

2/ L'entier d est soit $\equiv 0$, soit $\equiv 1$ modulo 4. Justifier.

3/ En écrivant $\delta = \dfrac{d + \sqrt{d}}{2}$, montrer que $\{1, \delta\}$ est toujours une base entière de $\mathfrak{O}_K$.

4/ Soit p un nombre premier. Exprimer $\mathfrak{O}_K/(p)$ comme $\mathbb{F}_p[X]/(f(X))$, où f est un polynôme unitaire.

On fixe $p > 2$ un nombre premier.

5/ Soit $F = X^2 + bX + c \in \mathbb{F}_p[X]$ et $\Delta = b^2 - 4c$. Montrer que si $\Delta = 0$ si et seulement si F est le carré d'un polynôme de degré 1. Montrer que $\Delta \neq 0$ est un carré de $\mathbb{F}_p^*$ si et seulement si F est le produit de deux polynômes linéaires distincts. Montrer que Δ n'est pas un carré si et seulement si F est irréductible. (Dit autrement, sur $\mathbb{F}_p[X]$ la théorie "marche" comme sur $\mathbb{R}[X]$.)

6/ Montrer que p se ramifie dans K si et seulement si $p \mid d$.

7/ Montrer que p se décompose en K si et seulement si d est un carré modulo p.

8/ Montrer que p est inerte dans K si et seulement si d n'est pas un carré modulo p.

9/ Montrer que 2 ramifie si et seulement si $d \equiv 0 \mod 4$.

10/ Montrer que 2 se décompose si et seulement si $d \equiv 1 \mod 8$.

11/ Montrer que 2 est inerte si et seulement si $d \equiv 5 \mod 8$.

Exercice 2. Soient $\alpha = \sqrt[3]{2}$ et $K = \mathbb{Q}(\alpha)$. Décomposer 5, 7 et 11 en premiers dans $\mathfrak{O}_K$. En suite, calculer le degré de chaque premier dans les décompositions.

Exercice 3. Soit p un nombre premier, $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme p-Eisenstein, α une racine de f et $K = \mathbb{Q}(\alpha)$.

1/ Soit $\mathfrak{p}$ un premier de $\mathfrak{O}_K$ au dessus de p et soit e la puissance maximale de $\mathfrak{p}$ qui divise p. Montrer que e est aussi la puissance maximale de $\mathfrak{p}$ qui divise a_0.

2/ En regardant la puissance maximale de $\mathfrak{p}$ qui divise $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha = -a_0$, montrer que $e = n$, c'est-à-dire, que p est totalement ramifié.

Exercice 4. On souhaite étudier la décomposition des nombres premiers dans une extension cyclotomique. On fixe ainsi p un nombre premier et $n > 1$ un entier qui n'est pas divisible par p.

1/ Soient $E/\mathbb{F}_p$ une extension finie et $\zeta \in E$ une racine primitive n-ème de l'unité. Montrer que $f = [\mathbb{F}_p(\zeta) : \mathbb{F}_p]$ est l'ordre de p dans $(\mathbb{Z}/n)^*$.

2/ Soit $K = \mathbb{Q}(\mu_n)$ et $\mathfrak{p}$ un idéal premier de K au-dessus p, c'est-à-dire, $p \in \mathfrak{p}$. Montrer que pour chaque $\zeta \in \mu_n$, l'égalité suivante

$$\text{ordre de } \zeta \text{ dans } \mu_n = \text{ ordre de } \zeta + \mathfrak{p} \text{ dans } \mathbb{F}_\mathfrak{p}^*$$

est vérifiée. Indication : On regardera les racines du polynôme $X^n - 1$ en $\mathbb{F}_\mathfrak{p}$.

À partir de maintenant, n est une puissance d'un premier ℓ.

3/ $\star$ Soit $K = \mathbb{Q}(\mu_n)$. Montrer que $p\mathfrak{O}_K$ n'est pas ramifié, c'est-à-dire, il existe des premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ deux-à-deux distincts de K tels que

$$p\mathfrak{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

4/ $\star$ On garde les notations de la question précédente. Prouver que le degré de chaque $\mathfrak{p}_i$ (qui vaut $[\mathbb{F}_{\mathfrak{p}_i} : \mathbb{F}_p]$), est l'ordre de p dans $(\mathbb{Z}/n)^*$. Indication : Faire appel à la question 2. En déduire que si $p \equiv 1 \mod n$, alors p est totalement décomposé en K.

5/ $\star$ On suppose $n = 8$ et $p = 3$. Décomposer l'idéal $p\mathfrak{O}_K$ en premiers.