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

Séance 5, 23 mars 2021

Notations et conventions.

— Pour chaque $n > 1$, μ_n, respectivement μ'_n, note l'ensemble des racines de l'unité dans $\mathbb{C}$, respectivement les racines primitives.

— Si K est un corps de nombres, $\mathfrak{O}_K$ désigne son anneau d'entiers.

— 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 $\mathbb{F}_\mathfrak{p}$.

Calcul d'anneaux d'entiers

Exercice 1 (Une extension non-monogène)**.** Soient $0 < m < n$ des nombres naturels sans facteur carré et premiers entre eux, x le réel $\sqrt[3]{m^2 n}$ et K le corps $\mathbb{Q}(x)$.

1/ Montrer que $y = \sqrt[3]{mn^2} \in \mathfrak{O}_K$ et que $\mathscr{B} = \{1, x, y\}$ est une base de K. Ensuite calculer $\Delta_K(\mathscr{B})$.

2/ Pour chaque $\alpha = a + bx + cy \in K$, calculer $\mathrm{N}_K(\alpha)$ et $\mathrm{Tr}_K(\alpha)$.

On suppose maintenant que mn n'est pas divisible par 3.

3/ Soit G le groupe quotient $\mathfrak{O}_K/\mathbb{Z} + \mathbb{Z}x + \mathbb{Z}y$. Montrer que son ordre est une puissance de 3.

4/ En supposant $m = 5$ et $n = 7$, montrer que $\mathscr{B}$ est une base entière. (Il est possible de traiter des cas plus généraux que ceci.)

5/ Soit $\theta = bx + cy$ avec $b, c \in \mathbb{Z}$. Calculer le quotient $\lambda := \dfrac{\Delta_K(1, \theta, \theta^2)}{\Delta_K(1, x, y)}$. En étudiant λ modulo 7, montrer que $\{1, \theta, \theta^2\}$ ne peut pas être une base entière de $\mathfrak{O}_K$.

6/ Soit $\theta = a + bx + cy$ avec $a, b, c \in \mathbb{Z}$. Montrer que si $\{1, \theta, \theta^2\}$ est base entière de $\mathfrak{O}_K$ et $\sigma = \theta - a$, alors $\{1, \sigma, \sigma^2\}$ est aussi base entière de $\mathfrak{O}_K$. Déduire que l'anneau des entiers de $\mathbb{Q}(\sqrt[3]{175})$ n'est pas de la forme $\mathbb{Z}[\theta]$.

Premiers décomposés, inertes et ramifiés

Exercice 2 (Vocabulaire)**.** Soit p un nombre premier et soient $K \subset L$ des corps de nombres. Montrer les implications suivantes :

1/ Si p se ramifie dans K alors il se ramifie dans L.

2/ Si p se décompose totalement en L, alors il se décompose totalement en K.

3/ Si p est inerte en L alors il est inerte en K aussi.