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

Séance 6, 26 mars 2021

Premiers inertes, ramifies et totalement décomposés

- Pour chaque $n > 1$, resp. 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.

Correction. On sait que $d = m$ si $m \equiv 1\ (4)$ et $d = 4m$ si $d \equiv 2, 3\ (4)$. Donc, soit $L = \mathbb{Q}(\sqrt{n})$, avec n sans facteur carré, de discriminant d. Si $n \equiv 1\ (4)$ on a $n = m$ ou $n = 4m$. Puisque $4 \nmid n$, on doit forcément avoir $n = m$. Si $n \equiv 2, 3\ (4)$, alors on a $4n = m$ ou $4n = 4m$. Puisque $4 \nmid m$, on doit forcément avoir $4n = 4m$. Dans tous les cas, $K = L$. □

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

Correction. C'est Stickelberger, mais dans ce cas on peut le démontrer directement : si $m \equiv 2, 3 \mod 4$ alors $d = 4m \equiv 0 \mod 4$. Si $m \equiv 1 \mod 4$ alors $d = m \equiv 1 \mod 4$. □

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

Correction. On sait que $K = \mathbb{Q}(\sqrt{m})$ avec m un entier sans facteur carré. Si $m \equiv 2, 3\ (4) \Rightarrow \delta = 2m + \sqrt{m}$. Comme $\{1, \sqrt{m}\}$ est base entière et $\sqrt{m} = \delta - 2m$, on déduit que $\{1, \delta\}$ est base entière.

Si $m \equiv 1\ (4)$, on sait que $1, \dfrac{1 + \sqrt{m}}{2}$ est base entière. On pose $m = 1 + 4k$. Il suit que $\delta = \dfrac{1 + \sqrt{m}}{2} + 2k$ est entier algébrique. Ensuite, $\dfrac{1 + \sqrt{m}}{2} = \delta - 2k$ et $1, \delta$ est base entière. □

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

Correction. Le poly minimal de δ est $\left(X - \frac{d+\sqrt{d}}{2}\right)\left(X - \frac{d-\sqrt{d}}{2}\right) = X^2 - dX + \frac{d^2-d}{4}$. On prendra ainsi

$$\boxed{f = X^2 - dX + \frac{d^2-d}{4}.}$$

□

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 $\mathbb{R}[X]$.)

Correction. On complète le carré : $F = (X + b/2)^2 - \Delta/4$.

Si $\Delta = 0$, clairement F est le carré d'un polynôme linéaire. Si $F = (X + a)^2$, alors $\Delta = 0$ par un calcul direct.

Si Δ est le carré d'un élément $\sqrt{\Delta}$, alors $F = (X + b/2 - \sqrt{\Delta}/2)(X + b/2 + \sqrt{\Delta}/2)$. Si $F = (X - \alpha)(X - \beta)$, alors un calcul facile montre que $\Delta = (\beta - \alpha)^2$.

Si Δ n'est pas un carré, alors F n'a pas de racines et est ainsi irréductible. Si Δ est un carré, alors on sait que F est produit de polynômes linéaires et ne peut pas ainsi être irréductible. □

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

Correction. On sait que p ramifie si et seulement si f a multiplicité > 1. Or, sur $\mathbb{F}_p$, on sait que ceci arrive si et seulement si le discriminant de f, à savoir d, est nul. □

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

Correction. Le discriminant de f est d. Alors p va se décomposer totalement $\Leftrightarrow$ f possède deux racines distinctes $\Leftrightarrow$ $p \nmid d$ et $\left(\frac{d}{p}\right) = 1$. □

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

Correction. Même chose que avant. □

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

Correction. On sait que 2 ramifie $\Leftrightarrow f = X^2$ ou $f = (X+1)(X+1) = X^2+1$ en $\mathbb{F}_2[X]$. Ceci signifie que 2 ramifie si et seulement si l'une des deux pairs de congruences a lieu :

$$\begin{array}{ll} d \equiv 0 \mod 2 \\ d^2 \equiv d \mod 8 \end{array} \quad \text{ou} \quad \begin{array}{ll} d \equiv 0 \mod 2 \\ d^2 \equiv d+4 \mod 8. \end{array}$$

Si $d \equiv 1 \mod 4$ alors 2 ne se ramifie pas. Si $d = 4e$ avec e impair, alors $d = 4+8k$ et $d^2 \equiv d+4 \mod 8$. Si $d = 8e$, alors $d^2 \equiv d \mod 8$. □

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

Correction. On sait que 2 se décompose $\Leftrightarrow f$ possède deux racines distinctes dans $\mathbb{F}_2$ $\Leftrightarrow f = X(X+1) = X^2+X \Leftrightarrow d \equiv 1\ (2)$ et $d^2 \equiv d\ (8)$. En écrivant $d = 1+2e$ alors $d^2 - d = 2e+4e^2$ est divisible par $8 \Leftrightarrow e+2e^2 \equiv 0\ (4) \Leftrightarrow e \equiv 0\ (4)$, comme on voit en regardant cas par cas. □

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

Correction. L'unique poly irréductible de $\mathbb{F}_2[X]$ de degré 2 est X^2+X+1. Donc, 2 est inerte $\Leftrightarrow d \equiv 1\ (2)$ et $d^2 - d \equiv 4\ (8)$. Si $d = 1+2e$ alors $d^2 - d = 2e+4e^2 \equiv 4\ (8)$ $\Leftrightarrow e+2e^2 \equiv 2\ (4) \Leftrightarrow e \equiv 2\ (4)$ comme on voit regardant cas par cas. Or, $e \equiv 2\ (4) \Leftrightarrow$ $d \equiv 5\ (8)$. □

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.

Correction. On sait que $\mathfrak{O}_K = \mathbb{Z}[\alpha]$ où $\alpha = \sqrt[3]{2}$ car $2 \not\equiv \pm 1\ (9)$. Donc, on doit décomposer X^3-2 en irréductibles unitaires de $\mathbb{F}_5[X]$. On note que que $3^3 \equiv 2\ (5)$, donc $X^3-2 = (X-3)(X^2+3X-1)$. Ensuite, X^2+3X-1 a discriminant $13 \equiv 2\ (5)$ et 2 n'est pas un carré modulo 5. Il suit que $5\mathfrak{O}_K = \mathfrak{pq}$ avec $\mathfrak{p} = (5, \alpha-3)$ et $\mathfrak{q} = (5, \alpha^2+3\alpha-1)$; on note que $\deg(\mathfrak{p}) = [\mathbb{F}_\mathfrak{p} : \mathbb{F}_5] = 1$ et $\deg(\mathfrak{q}) = 2$.

De même, on doit décomposer X^3-2 en irréductibles en $\mathbb{F}_7$. On note que 2 n'est pas un cube en $\mathbb{F}_7$ et donc ce polynôme est irréductible et (7) est premier.

Finalement, 2 est un cube modulo 11 car $7^3 \equiv 2\ (11)$. Il suit que $(X-7)(X^2+7X+5) = X^3-2$. Pour déterminer si X^2+7X+5 est irréductible, on regarde son discriminant qui est 7. Or, 7 n'est pas un carré modulo 11 par réciprocité quadratique. Donc ce polynôme est irréductible et $(11) = \mathfrak{pq}$, avec $\mathfrak{p} = (11, \alpha-7)$ de degré 1 et $\mathfrak{q} = (11, \alpha^2+7\alpha+5)$ de degré 2. □

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.

Correction. On sait que $p \mid a_0$ et donc $\mathfrak{p}^e \mid a_0$. On pose $a_0 = pa'_0$. Si $\mathfrak{p} \mid a'_0$, alors $a'_0 \in \mathfrak{p} \cap \mathbb{Z}$ et $p \mid a'_0$, ce qui est impossible. □

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.

Correction. On sait que $e \leqslant n$ d'après le cours. Comme $\alpha^n \equiv 0 \mod p\mathfrak{O}_K$, on déduit que $\mathfrak{p} \mid \alpha^n$ d'où $\mathfrak{p} \mid \alpha$ et en particulier, $\mathfrak{p}^n \mid \alpha^n$. Comme $p \mid a_i$ pour $i = 1, \ldots, n-1$, on déduit que $\mathfrak{p}^e\mathfrak{p} \mid a_i\alpha^i$. Donc :

$$\underbrace{\alpha^n}_{\in\mathfrak{p}^n} + \underbrace{a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha}_{\in\mathfrak{p}^{e+1}}. \qquad (*)$$

Si $e < n$ alors $e + 1 \leqslant n$ et $\mathfrak{p}^{e+1} \mid a_0$, une contradiction. □

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 $(\mathbb{Z}/n)^*$.

Correction. Si f est le degré de $\mathbb{F}_p(\zeta)$, alors $\zeta^{p^f-1} = 1$. Donc, ζ est aussi une racine $(p^f - 1)$-ème de l'unité. Il suit que $n \mid p^f - 1$, c'est-à-dire, $p^f \equiv 1 \mod n$. Ensuite, si $p^g \equiv 1 \mod n$, alors $\zeta^{p^g} = \zeta$ et $p^f = [\mathbb{F}_p(\zeta) : \mathbb{F}_p] \leqslant p^g$. D'où f est exactement l'ordre de p dans $(\mathbb{Z}/n)^*$. □

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

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

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

Correction. Soit m l'ordre de ζ, de sorte que $\zeta \in \mu\!\!\mu'_m$. On note la réduction modulo $\mathfrak{p}$ par un tilde. On suppose que pour un certain $0 < d < m$ on ait $\widetilde{\zeta}^d = \widetilde{1}$. On sait que $X^n - 1 = \prod_{\omega\in\mu\!\!\mu_n}(X - \omega)$ en $\mathfrak{O}_K[X]$. Comme $\zeta^d \neq \zeta^m = 1$, on sait que $(X - \zeta^d)(X - 1) \mid X^n - 1$ en $\mathfrak{O}_K[X]$. Donc, $(X - \widetilde{1})^2 \mid X^n - \widetilde{1}$ en $\mathbb{F}_\mathfrak{p}[X]$, ce qui est impossible car $X^n - \widetilde{1}$ ne possède pas de racines multiples en $\mathbb{F}_\mathfrak{p}$. □

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

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