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

Séance 2, 12 mars 2021

Notations et conventions.

— Pour $r \in \mathbb{Q}$ positif, le symbole $\sqrt{r}$ est le réel usuel.
— Le nombre algébrique α a "degré" n quand $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.
— Pour chaque nombre algébrique α, on désigne par $\Pi_\alpha \in \mathbb{Q}[X]$ son polynôme minimal.
— Si K un corps de nombres de degré n, l'ensemble de plongements de K dans $\mathbb{C}$ est noté $\Sigma(K)$. Si $\alpha \in K$ est donné, les conjugués de α sont les complexes ayant la forme $\sigma(\alpha)$ pour $\sigma \in \Sigma(K)$. La K-norme $\mathrm{N}_K(\alpha)$ est $\prod_{\sigma\in\Sigma(K)} \sigma(\alpha)$ et la K-trace $\mathrm{Tr}_K(\alpha)$ est $\sum_{\sigma\in\Sigma(K)} \sigma(\alpha)$. (Une notation plus précise et plus encombrante serait $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ et $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$.)
— Pour $n \geqslant 1$, on désigne par μ_n, respectivement μ'_n, l'ensemble des racines n-èmes, respectivement n-èmes et primitives, de l'unité dans $\mathbb{C}$.
— Le n-ème polynôme cyclotomique $\prod_{\zeta\in\mu'_n}(X - \zeta)$ sera désigné par Φ_n.

Exercice 1 (Le caractère quadratique de 2 via $\mathbb{Q}(\mu_8)$)**.** Soient $p > 2$ premier et ζ une racine primitive 8-ème de l'unité. On désigne par $\mathfrak{O}$ l'anneau des entiers du corps[2] $\mathbb{Q}(\mu_8)$.

1/ Montrer que $g := \zeta + \zeta^{-1}$ est une racine carré de 2.

2/ Rappeler la congruence $\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \mod p$ et montrer ensuite que $g^p \equiv \left(\frac{2}{p}\right) g \mod p\mathfrak{O}$.

3/ Justifier la congruence $g^p \equiv \zeta^p + \zeta^{-p} \mod p\mathfrak{O}$. En déduire que

$$g^p \equiv \begin{cases} g \mod p\mathfrak{O}, & \text{si } p \equiv \pm 1\ (8) \\ -g \mod p\mathfrak{O}, & \text{si } p \equiv \pm 3\ (8) \end{cases}$$

4/ Prouver que 2 est un carré modulo p si et seulement si $p \equiv \pm 1$ (8)

Les conjugués, la signature, la norme et la trace

Exercice 2. Soit $F \in \mathbb{Z}[X_1, \ldots, X_6]$ un polynôme symétrique. Soit $\zeta = e^{2i\pi/7}$. Alors le nombre complexe $F(\zeta, \zeta^2, \ldots, \zeta^6)$ est un *entier*. Expliquer.

2. Il est possible d'utiliser l'idée de cet étude pour démontrer la réciprocité quadratique.

Exercice 3 (Une mesure de "l'algébricité")**.** Pour chaque nombre algébrique α, on définit

$$\begin{aligned}\|\alpha\| &= \sup\{|\beta| \,:\, \beta \text{ est racine de } \Pi_\alpha\}\\ &= \sup\{|\beta| \,:\, \beta \text{ est conjugué à } \alpha\}.\end{aligned}$$

1/ Soit K un corps de nombres et $R > 0$. Montrer que

$$B_R = \{\alpha \in \mathfrak{O}_K \,:\, \|\alpha\| \leqslant R\}$$

est un ensemble fini. Indication : On considère la fonction $\Pi : B_R \to \mathbb{Z}[X]$ définie par $\alpha \mapsto \Pi_\alpha$ et on montre que l'image par Π de chaque $B_{R,n} = \{\alpha \in B_R \,:\, \alpha \text{ a degré } n\}$ est finie.

2/ En déduire que le groupe des racines de l'unité dans K est fini.

3/ Utiliser la question précédente pour montrer un théorème de L. Kronecker de 1857 : Si α est un entier algébrique dont tous les conjugués ont valeur absolue $\leqslant 1$, alors α est une racine de l'unité.

Exercice 4. On étudie la signature d'un corps de nombres.

1/ Soit $n > 1$. Déterminer les plongements dans $\mathbb{C}$ du corps $\mathbb{Q}(\mu_n)$. Même question avec $\mathbb{Q}(\cos(2\pi/n))$.

2/ Donner des exemples de corps de nombres de signature $(3, 0)$.

3/ Si K est un corps de nombres de degré 4, quelle peut-être sa signature ? Donnez des exemples dans chaque cas.

Exercice 5 (Quelques remarques sur la norme et la trace)**.** Soit K un corps de nombres de degré n et $\Sigma(K) = \{\sigma_j : K \to \mathbb{C}\}_{j=1}^{n}$ les plongements de K. On fixe $\alpha \in K$.

1/ Quel est le lien entre $\mathrm{N}_K(\alpha)$, resp. $\mathrm{Tr}_K(\alpha)$, et $\mathrm{N}_{\mathbb{Q}(\alpha)}(\alpha)$, resp. $\mathrm{Tr}_{\mathbb{Q}(\alpha)}(\alpha)$?

2/ Soit $\beta \in K$ conjugué à α. Montrer que $\mathrm{N}_K(\alpha) = \mathrm{N}_K(\beta)$ et $\mathrm{Tr}_K(\beta) = \mathrm{Tr}_K(\alpha)$.

3/ Soit $K = \mathbb{Q}(\mathrm{i}, \sqrt{2}, \sqrt{3})$. Calculer $\mathrm{N}_K(\sqrt{2})$.

Exercice 6. Soit K un corps de nombres et $\alpha \in \mathfrak{O}_K$ un entier algébrique.

1/ Montrer que $\alpha \in \mathfrak{O}_K^\times$ si et seulement si $\mathrm{N}_K(\alpha) = \pm 1$. Indication : La norme est, à signe près, le coefficient constant de $\chi_{\alpha,K}$. En déduire que si α appartient à $\mathfrak{O}_L^\times$ pour une extension finie L/K, alors $\alpha \in \mathfrak{O}_K^\times$.

2/ Montrer que si $\mathrm{N}_K(\alpha)$ est un nombre premier, alors α est irréductible.

Exercice 7. Soit K le corps de nombres $\mathbb{Q}(\zeta)$ où $\zeta = e^{2\pi \mathrm{i}/5}$.

1/ Calculer $\mathrm{N}_K(1 - \zeta)$.

2/ Calculer $\mathrm{N}_K(a - b\zeta)$ pour chaque couple d'entiers a, b. Utiliser votre résultat pour déterminer si $\zeta + 2$, $\zeta - 2$ et $\zeta + 3$ sont irréductibles ou non dans $\mathfrak{O}_K$.