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

Séance 1, 8 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 $\mu\!\!\mu_n$, respectivement $\mu\!\!\mu'_n$, l'ensemble des racines n-èmes, respectivement n-èmes et primitives, de l'unité dans $\mathbb{C}$.
- Le n-ème polynôme cyclotomique $\prod_{\zeta\in\mu\!\!\mu'_n}(X - \zeta)$ sera désigné par Φ_n.

Cyclotomie

Exercice 1. On étudie des propriétés basiques des corps cyclotomiques.

1/ Soient m, n des entiers strictement positifs. Montrer que si $\mathrm{pgcd}(m, n) = 1$, alors $\mathbb{Q}(\mu\!\!\mu_m, \mu\!\!\mu_n) = \mathbb{Q}(\mu\!\!\mu_{mn})$. Indication : On pourra considérer le morphisme $f : \mu\!\!\mu_m \times \mu\!\!\mu_n \to \mu\!\!\mu_{mn}$ définit par $(z, w) \mapsto zw$.

2/ Soit p un nombre premier *impair*. En utilisant que $\Phi_p(1) = p$, montrer que $p^* := (-1)^{(p-1)/2}p$ est un carré en $\mathbb{Q}(\mu\!\!\mu_p)$. En déduire que pour chaque premier impair p, le corps $\mathbb{Q}(\mu\!\!\mu_{4p})$ contient $\sqrt{p}$ et $\mathrm{i}\sqrt{p}$.

3/ Déterminer un corps cyclotomique $\mathbb{Q}(\mu\!\!\mu_n)$ contenant $\sqrt{2}$ et $\mathrm{i}\sqrt{2}$.

4/ En déduire que chaque corps quadratique de nombres est contenu dans un corps cyclotomique.

Exercice 2 (Les polynômes cyclotomiques)**.** Soit $n > 1$. Dans la suite on étudie

$$\Phi_n(X) = \prod_{\zeta\in\mu\!\!\mu'_n} (X - \zeta) \in \overline{\mathbb{Q}}[X],$$

le n-ème polynôme cyclotomique.

(1) Montrer que[1] $\mathbb{\mu}_n = \bigsqcup_{d|n} \mathbb{\mu}'_d$, et utiliser cette équation pour déduire $X^n - 1 = \prod_{d|n} \Phi_d$.

(2) En déduire que $\Phi_n \in \mathbb{Z}[X]$. (Indication : La division Euclidienne "fonctionne" sur $\mathbb{Z}[X]$ tant qu'on divise par des polynômes unitaires.)

(3) Soit p premier. Rappeler la formule $\Phi_p = X^{p-1} + \cdots + 1$.

(4) Pouvez-vous calculer explicitement Φ_{p^m}, où p est premier ? Quel est le lien entre ce dernier et Φ_p ?

(5) Calculer explicitement Φ_6 et Φ_{12}.

Exercice 3 (Une preuve "euclidienne")**.** Soit $n \geqslant 1$ un entier. On souhaite utiliser Φ_n pour donner une preuve "euclidienne" de l'existence d'une infinité de premiers $\equiv 1 \mod n$. (Euclidienne, car en faisant la preuve avec $n = 1$ on arrive à la preuve célèbre d'Euclide sur l'existence d'un nombre infini de premiers.)

1/ Montrer que le coefficient *constant* de Φ_n est toujours ± 1. Utiliser ce fait pour prouver que $\mathrm{pgcd}(\alpha, \Phi_n(\alpha)) = 1$ pour tout entier non-nul α.

2/ Soit α un entier et p un facteur premier de $\Phi_n(\alpha)$. On suppose de plus que p ne divise pas n. Montrer que l'ordre de l'image $\tilde{\alpha}$ de α dans $\mathbb{F}_p^\times$ est n. Indication : Utiliser que $X^n - 1 \in \mathbb{F}_p[X]$ n'a que de racines simples et $X^n - 1 = \Phi_n \cdot F$, avec $F = \prod_{\substack{d|n \\ d<n}} \Phi_d$.

3/ Montrer qu'il existe un nombre infini de premiers $\equiv 1 \mod n$. Indication : Si $p_1, \ldots, p_r$ sont premiers $\equiv 1 \mod n$, on considère $\Phi_n(gnp_1 \cdots p_n)$ pour $g \to +\infty$.

Exercice 4 (Polynômes cyclotomiques : irréductibilité)**.** On fixe $\zeta \in \mathbb{\mu}'_n$, p un premier *qui ne divise pas* n et on écrit $\xi = \zeta^p$. On montrera que Φ_n est irréductible en montrant d'abord que $\Pi_\xi = \Pi_\zeta$.

1/ Les polynômes Π_ζ et Π_ξ de $\mathbb{Q}[X]$ appartiennent en fait à $\mathbb{Z}[X]$: Justifier.

2/ Il existe $F \in \mathbb{Z}[X]$ tel que $\Pi_\zeta(X)F(X) = \Pi_\xi(X^p)$: Justifier.

3/ Utiliser la question précédente pour montrer que les images dans $\mathbb{F}_p[X]$ de Π_ζ et Π_ξ ont un diviseur commun.

4/ Montrer que $\Pi_\zeta = \Pi_\xi$. Indication : Si $\Pi_\zeta \neq \Pi_\xi$, alors $X^n - 1 \in \mathbb{F}_p[X]$ est divisible par un carré.

5/ Monter que $\Phi_n = \Pi_\zeta$ et en déduire que Φ_n est irréductible.

1. On rappelle que $\bigsqcup$ note la réunion disjointe.