

Feuille 5 :

Exercice 1 (Extensions cyclotomiques) On note $r \geq 1$, p premier, ζ une racine primitive p^r -ième de l'unité, $K = \mathbb{Q}[\zeta]$ et \mathcal{O}_K son anneau d'entiers.

1. Montrer que K est une extension normale et que l'on a un morphisme injectif du groupe de Galois G_K vers le groupe $(\mathbb{Z}/p^r\mathbb{Z})^\times$ des inversibles de \mathbb{Z}/p^r . Montrer également que $\mathbb{Z}[\zeta] \subset \mathcal{O}_K$ et que $[\mathbb{Q}[\zeta] : \mathbb{Q}] \leq \varphi(p^r) = p^{r-1}(p-1)$.
2. On appelle *polynôme cyclotomique* Φ_{p^r} le polynôme $\prod_{\zeta \in \mu_{p^r}^{\text{primitive}}} (X - \zeta)$. Montrer que

$$\Phi_{p^r} = \prod_{[i] \in (\mathbb{Z}/p^r\mathbb{Z})^\times} (X - \zeta^i) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1}.$$

3. Soit ξ une autre racine primitive p^r -ième de l'unité. Montrer que $\frac{1-\zeta}{1-\xi}$ est une unité de \mathcal{O}_K (*i.e.* est inversible dans \mathcal{O}_K).
4. Soit $\pi = 1 - \zeta$. En calculant $\Phi_{p^r}(1)$, montrer l'égalité d'idéaux dans \mathcal{O}_K , $(\pi) = (\pi)^{\varphi(p^r)}$. En déduire que le corps $\mathbb{Q}[\zeta]$ est de degré $\varphi(p^r)$ sur \mathbb{Q} et que l'élément π est premier dans \mathcal{O}_K . Quels sont les premiers ramifiés dans K/\mathbb{Q} ? Donner le degré résiduel f et l'indice de ramification e .
5. Calculer la valeur absolue du discriminant $|\text{disc}(\mathbb{Z}[\zeta] : \mathbb{Z})| = \text{Nm}_{K/\mathbb{Q}}(\Phi'_{p^r}(\zeta))$ (on pourra commencer par $r = 1$ avant de traiter le cas général). En déduire que $\text{disc}(\mathcal{O}_K/\mathbb{Z})$ est une puissance de p et que $p^M \mathcal{O}_K \subset \mathbb{Z}[\zeta]$ pour tout entier M suffisamment divisible.
6. Montrer que $\mathbb{Z}[\zeta] + \pi^m \mathcal{O}_K = \mathcal{O}_K$ pour $m \geq 1$. En déduire que l'anneau des entiers de $\mathbb{Q}[\zeta]$ est $\mathbb{Z}[\zeta]$ et que le discriminant de \mathcal{O}_K sur \mathbb{Z} est de valeur absolue $p^{p^{r-1}(p^r-r-1)}$.
7. Soit $p \neq 2$. On définit le symbole quadratique pour $n \in \mathbb{Z}$, par 0 si $(n, p) \neq 1$; et si $(n, p) = 1$ on pose

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{si } n \text{ est un carré mod } p \\ -1 & \text{sinon} \end{cases}$$

Soit ζ une racine primitive p -ième de l'unité et $S = \sum_{v=0}^{p-1} \binom{v}{p} \zeta^v$. Montrer que $S^2 = \left(\frac{-1}{p}\right)p$. En déduire que toute extension quadratique de \mathbb{Q} est contenue dans une extension cyclotomique.

Exercice 2 (Norme numérique) Soient K un corps de nombres et \mathcal{O}_K son anneau d'entiers. Soit \mathfrak{a} un idéal non nul de \mathcal{O}_K . L'indice de \mathfrak{a} dans \mathcal{O}_K est fini et on note la *norme numérique* N :

$$N(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a}).$$

Pour tout idéal \mathfrak{p} premier de \mathcal{O}_K au dessus d'un premier p , on pose $N_{K/\mathbb{Q}}(\mathfrak{p}) := p^{f(\mathfrak{p}/p)}$. On prolonge ceci multiplicativement aux idéaux fractionnaires de \mathcal{O}_K .

1. Soit \mathcal{O}_K l'anneau des entiers d'un corps de nombres K . Soit \mathfrak{a} un idéal dans \mathcal{O}_K , montrer que $N_{K/\mathbb{Q}}(\mathfrak{a}) = N(\mathfrak{a})$; en déduire $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.

2. En déduire (cf. Samuel p.62) que pour tout entier $x \in \mathcal{O}_K$, on a $N_{K/\mathbb{Q}}(x) = \pm N_{K/\mathbb{Q}}(x\mathcal{O}_K)\mathbb{Z}$.
3. Soient $\mathfrak{b} \subset \mathfrak{a}$ des idéaux fractionnaires de K . Montrer que $(\mathfrak{a} : \mathfrak{b}) = N(\mathfrak{a}^{-1}\mathfrak{b})$.
4. Montrer que $\alpha \in K$ est une unité si et seulement si $\alpha \in \mathcal{O}_K$ et $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.
5. Soit $\alpha \in K$. Si $N_{K/\mathbb{Q}}(\alpha) = \pm 1$, α est-il forcément une unité dans K ?

Exercice 3 (Clôture algébrique de \mathbb{Q}_p) Notons $\overline{\mathbb{Q}_p}$ une clôture algébrique de \mathbb{Q}_p . Supposons par l'absurde que $\overline{\mathbb{Q}_p}$ est complet et posons $\alpha = \sum_{n=1}^{\infty} \zeta_{n'} p^n$ avec $n' = \begin{cases} n & \text{si } (n, p) = 1 \\ 1 & \text{sinon} \end{cases}$ où ζ_m est une racine primitive m -ième de l'unité. Posons $K = \mathbb{Q}_p(\alpha)$.

1. Montrer que $\forall m \in \mathbb{N}, \zeta_{m'} \in \mathcal{O}_K$.
2. En déduire que $\overline{\mathbb{Q}_p}$ n'est pas complet.

Exercice 4 (Lemme de Krasner) Soit K un corps complet pour une valuation non-archimédienne. Soit α, β deux éléments d'une clôture algébrique \overline{K} de K avec α séparable sur $K(\beta)$. On dit que α appartient à β si pour tout conjugué $\sigma\alpha \neq \alpha$ de α ,

$$|\beta - \alpha| < |\sigma\alpha - \alpha|$$

(où $|\cdot|$ désigne l'unique extension de la valeur absolue de K).

1. Montrer que si α appartient à β alors $K(\alpha) \subset K(\beta)$.
2. Si $f = \sum_{i=0}^n a_i X^i \in K[X]$, on pose $|f| := \max_{0 \leq i \leq n} |a_i|$. Soient f et g deux éléments de $K[X]$ unitaires, de même degré n . On suppose que f est irréductible sur K et séparable. Montrer que si $|f - g|$ est suffisamment petite, alors g est aussi irréductible. De plus dans ce cas, si α est une racine de f dans \overline{K} montrer qu'il existe une racine β de g dans \overline{K} telle que $K(\alpha) = K(\beta)$.

Exercice 5 (Extensions totalement ramifiées) Soit K un corps de caractéristique nulle, valué ultramétrique de valuation discrète, complet, d'anneau de valuation A , d'idéal maximal \mathfrak{p} , d'uniformisante π et de corps résiduel fini (ceci est notamment vérifiée par \mathbb{Q}_p). Montrer qu'il n'y a, à isomorphisme près, qu'un nombre fini d'extensions de K totalement ramifiées de degré fixé.

Exercice 6 (Applications de Krasner)

1. Soient $\overline{\mathbb{Q}_p}$ une clôture algébrique de \mathbb{Q}_p et \mathbb{C}_p la complétion de $\overline{\mathbb{Q}_p}$. Montrer que \mathbb{C}_p est algébriquement clos.
2. Soit K une extension finie de \mathbb{Q}_p . Montrer qu'il existe une extension finie L de \mathbb{Q} contenue dans K telle que $[L : \mathbb{Q}] = [K : \mathbb{Q}_p]$ et $L\mathbb{Q}_p = K$.