Leonid Monin
Léo Navarro Chafloque

EPFL, semestre de printemps 2026
Rings and fields

Exercice – Semaine 10

Exercice 1.
Soit $n > 0$ un entier positif. Montrez que $\cos(2\pi/n)$ et $\sin(2\pi/n)$ sont des nombres algébriques sur $\mathbb{Q}$.

Exercice 2. 1. Montrez que $1, \sqrt[3]{2}, \sqrt[3]{4}$ est une $\mathbb{Q}$ base de $\mathbb{Q}(\sqrt[3]{2})$.

2. Écrivez la matrice de la multiplication par

$$1 + \sqrt[3]{2} + \sqrt[3]{4},$$

vue comme application linéaire $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$. Calculez le polynôme caractéristique de cette matrice et déduisez en le polynôme minimal de l'élément ci-dessus.

Exercice 3.
Soit $\xi = e^{\frac{2\pi i}{n}}$ pour un entier $n > 2$. Démontrez que les corps de décomposition de $x^n - 2$ et de $x^{2n} - 3x^n + 2$ sur $\mathbb{Q}$ sont isomorphes entre eux, et aussi isomorphes à

$$\mathbb{Q}(\xi, \sqrt[n]{2}) \subseteq \mathbb{C}.$$

Exercice 4.
Soit $f = x^7 - y^5 \in \mathbb{C}[x, y]$. Le but de cet exercice est de démontrer que f est irréductible dans $\mathbb{C}[x, y]$. Soit $K = \mathbb{C}(y)$ et L le corps de décomposition de f sur K. Soit α une racine de f dans L, et $\beta = \frac{\alpha^3}{y^2}$.

1. Montrez que $[K(\beta) : K] = 7$. *Indication: Trouvez un polynôme sur K dont β est une racine.*
2. Montrez que $K(\beta) = K(\alpha)$.
3. Déduisez que f est irréductible dans $\mathbb{C}[x, y]$.

Exercice 5. 1. Considérons la situation suivante:

- $\phi : K \to K'$ est un isomorphisme des corps,
- $K \subseteq L$ et $K' \subseteq L'$ sont deux extensions de corps
- $L = K(\alpha)$ et $L' = K'(\alpha')$ avec α et α' algébriques sur K et K' respectivement
- si $\xi : K[x] \to K'[x]$ est l'isomorphisme induit par ϕ, alors $\xi(m_{\alpha,K}) = m_{\alpha',K'}$

Démontrez qu'il existe une extension unique de ϕ à un isomorphisme $\eta : L \to L'$ tel que $\eta(\alpha) = \alpha'$

2. Démontrez que $K(x)[\sqrt{x+1}] \cong K(x)[\sqrt{x+2}]$
3. Démontrez que $K(x, y)[\sqrt{xy}] \cong K(x, y)[\sqrt{x(x+y)}]$

Exercice 6.
Soit $n \geq 1$ un entier. On dit qu'une racine n-ième de l'unité $\xi \in \mathbb{C}$ est primitive si n est le plus petit entier tel que $\xi^n = 1$. On pose,

$$\Phi_n(t) = \prod_{\substack{\xi \text{ racine} \\ \text{primitive} \\ n\text{-ième} \\ \text{de l'unité}}} (t - \xi) \in \mathbb{C}[t].$$

1. Montrer que $t^n - 1 = \prod_{d|n} \Phi_d(t)$ et que $\Phi_n(t) \in \mathbb{Z}[t]$.

2. Soit p un nombre premier et $n \geq 1$. En utilisant le critère d'Eisenstein et le changement de variable $t \mapsto t + 1$, montrer que $\Phi_{p^n}(t)$ est irréductible. (*c.f.* changement de variable et Eisentsein vu en cours)

3. Soit $n \geq 1$ un entier et p un premier qui est premier avec n. On note ξ_n une racine primitive n-ième de l'unité. Soit $m(t) \in \mathbb{Q}[t]$ le polynôme minimal de ξ_n. Montrer que $m(t) \in \mathbb{Z}[t]$. Montrer que si ξ est une racine de $m(t)$, alors ξ^p est une racine de $m(t)$. En déduire que $m(t) = \Phi_n(t)$.

   Indication: on pourra montrer par l'absurde que si ξ^p n'est pas une racine de $m(t)$ alors $t^n - 1$ a une racine double modulo p, ce qui est absurde comme $(n, p) = 1$ (Utiliser la dérivée).

4. Soit p un premier et $n \geq 1$ un entier tel que $(n, p) = 1$. Montrer que si $\overline{\Phi_n(t)} \in \mathbb{F}_p[t]$ a une racine dans $\mathbb{F}_p[t]$ alors c'est une racine primitive de l'unité dans $\mathbb{F}_p$, c'est à dire un élément dont l'ordre multiplicatif est n.

   Indication: On considère k le corps de décomposition de $t^n - 1$ sur $\mathbb{F}_p$. On utilise la dérivée pour argumenter qu'il y a n-racines distinctes de ce polynôme dans k. On montre ensuite par récurrence sur les diviseurs $d \mid n$ que les racines de $\overline{\Phi_d(t)}$ dans k sont exactement les racines primitives d-ièmes de l'unité dans k.

5. Montrer qu'il existe une infinité de premiers p tel que $\Phi_n(t)$ a une racine dans $\mathbb{F}_p[t]$. En déduire qu'il existe une infinité de premiers p tel que $p \equiv 1 \mod n$.

   Indication: pour tout m suffisamment grand si un nombre premier p divise $\Phi_n(m!)$ alors $p > m$.