EPFL - Printemps 2023	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Série 9	1 mai 2023

Les exercices indiqués par une étoile $\star$ sont optionnels.
Si vous le souhaitez, vous pouvez rendre votre solution de l'exercice bonus sur la page Moodle du cours avant le dimanche 14 mai, 18h.

Exercice 1.
Soit K un corps et L une extension quadratique, i.e. $[L : K] = 2$.

1. Montrez que toute extension de K de degré 1 est égale à K.
2. Montrez qu'il existe un élément $\alpha \in L$ tel que $L = K(\alpha)$.
3. Soit K de caractéristique différente de 2. Montrez qu'il existe un élément $\delta \in L$ avec $\delta^2 = d \in K$ tel que $L = K(\delta) = K(\sqrt{d})$.
4. Soit M une extension de K et $\delta \in M \setminus K$ un élément avec $\delta^2 \in K$. Montrez que $K(\delta)$ est une extension quadratique de K.

Exercice 2.
Soient $a, b \in \mathbb{Z}$.

1. Quand est-ce que les corps $\mathbb{Q}(\sqrt{a})$ et $\mathbb{Q}(\sqrt{b})$ sont isomorphes en tant que $\mathbb{Q}$-espaces vectoriels?
2. Quand est-ce que les corps $\mathbb{Q}(\sqrt{a})$ et $\mathbb{Q}(\sqrt{b})$ sont isomorphes en tant que corps?

Exercice 3.

1. Soit L une extension de K avec $[L : K]$ impair. Montrer que $K(\alpha) = K(\alpha^2)$ pour tout $\alpha \in L \setminus K$.
2. Soient $p, q \in \mathbb{Z}$ deux nombres premiers distincts. Montrez que $\sqrt{p} \notin \mathbb{Q}(\sqrt{q})$ et $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$. Calculez $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}]$.
3. Soit L une extension de K et soient $\alpha, \beta \in L$ des éléments tels que $[K(\alpha) : K] = m$ et $[K(\beta) : K] = n$ sont premiers entre eux. Montrer que $[K(\alpha, \beta) : K] = mn$.

Exercice 4.
Soit $K = \mathbb{Q}(\sqrt{3} + \sqrt{7})$. Montrez que $[K : \mathbb{Q}] = 4$.

Exercice 5.
Dans tous les cas suivants, calculez le degré de l'extension.

1. $[\mathbb{R}(e^{2i\pi/p}) : \mathbb{R}]$ pour p un nombre premier;
2. $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ pour α une racine de $t^{42} + t^{41} + \cdots + t^2 + t + 1$;
3. $[\mathbb{Q}(i, \sqrt[5]{13}) : \mathbb{Q}]$;
4. $[\mathbb{F}_3(\alpha) : \mathbb{F}_3]$ où α est une racine de $t^4 - t^3 - t^2 - t - [1]_3 \in \mathbb{F}_3[t]$ (disons que α vit dans le corps de décomposition de ce polynôme sur $\mathbb{F}_3$ pour fixer les idées) La réponse peut changer en fonction de la racine considérée.
5. $[\mathbb{Q}(\sqrt{14 + 6\sqrt{5}}, \sqrt{3}) : \mathbb{Q}]$ (on pourra calculer $(3 + \sqrt{5})^2$ pour commencer);

6. $[\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}((\sqrt[6]{7})^2)\,]$;

7. $[\mathbb{F}_2(\alpha) : \mathbb{F}_2(\alpha^2)\,]$ où α est une racine de $t^3 + t + [1]_2 \in \mathbb{F}_2[t]$.

Exercice 6.
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 bonus 5. 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 dans $\mathbb{Z}[t]$. (*c.f.* exemple 3.9.4.(2))

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 $(n, p) = 1$ (Voir Proposition 4.4.10).

4. 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 $p > m$.

Exercice 7 ($\star$).
Calculer $\pi_0(\mathbb{Q}[\mathbb{Z}/n\mathbb{Z}])$.