EPFL - Printemps 2024	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Série 13	

Exercice 1.
Soit $K \subseteq L = K(\alpha)$ une extension simple de corps. Démontrez qu'elle est galoisienne si et seulement si α est séparable sur K et $m_{\alpha,K}$ scinde sur L. On dit qu'un polynôme scinde si toute racine de $m_{\alpha,K}$ est contenue dans L.

Exercice 2.
Soit $K \subseteq L = K(\alpha)$ une extension simple de degré 2 des corps de caractéristique non 2.

1. Soit $m_{\alpha,K} = x^2 + bx + c$, où $b, c \in K$. Démontrez que la formule quadratique est valide ici. Cela veut dire les deux racines de $m_{\alpha,K}$ sont $\frac{-b+\sqrt{b^2-4c}}{2}$ et $\frac{-b-\sqrt{b^2-4c}}{2}$, où $\beta = \sqrt{b^2-4c} \in L$ est un quelconque élément tel que $\beta^2 = b^2 - 4c$. Cela inclut l'affirmation que tel β n'existe pas dans K. Concluez que L est une extension par une racine (deuxième) d'un élément adéquat de K.

2. Démontrez que $K \subseteq L$ est $\mathbb{Z}/2\mathbb{Z}$-galoisienne .

3. Soit $\mathbb{Q} = K \subseteq L$ une extension de corps $\mathbb{Z}/4\mathbb{Z}$-galoisienne. Démontrez que il existe des entiers rationnels a, $b \neq 0$ et d tel que $L = \mathbb{Q}\left(\sqrt{a + b\sqrt{d}}\right)$ et $\sqrt{d} \notin \mathbb{Q}$, $\sqrt{a + b\sqrt{d}} \notin \mathbb{Q}(\sqrt{d})$.

4. Considérons a, $b \neq 0$, $d \in \mathbb{Q}$ tel que $\sqrt{d} \notin \mathbb{Q}$ et $\alpha = \sqrt{a + b\sqrt{d}} \notin \mathbb{Q}(\sqrt{d})$. Démontrez que l'extension $K = \mathbb{Q} \subseteq L = \mathbb{Q}(\alpha)$ est $\mathbb{Z}/4\mathbb{Z}$-galoisienne si et seulement si $\sqrt{a - b\sqrt{d}} \in L$ et $\lambda = a^2 - b^2 d$ n'est pas un carré dans $\mathbb{Q}$.

5. Montrez que $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2 + \sqrt{2}}\right)$ est $\mathbb{Z}/4\mathbb{Z}$-galoisienne.

Exercice 3.
Fixons un entier $n > 0$. Soit K un corps de caractéristique soit 0 soit positive et première avec n.

1. Démontrez que $x^n - 1 \in K[x]$ n'admet pas de racine multiples dans son corps de décomposition sur K.

   Autrement dit il y a n racines distinctes qui sont des n-ième racine de l'unité dans les extensions de K. Supposons à a partir de maintenant que K contient toute ces racines.

2. Considérons une $\mathbb{Z}/n\mathbb{Z}$-galoisienne extension $K \subseteq L$. Démontrez, que $L = K\left(\sqrt[n]{a}\right)$ pour un $a \in K$ adéquat, où $\sqrt[n]{a}$ dénote un élément dont le n-ième puissance égale à a.

   Indice: considérons un générateur ϕ de $\mathbb{Z}/n\mathbb{Z}$ en tant qu'application K-linéaire sur L. Démontrez le polynôme minimal de ϕ en tant qu'une application K linéaire est $x^n - 1$. Utilisez la décomposition en espaces propres pour trouver un vecteur propre $\alpha \in L$ avec valeur propre une n-ième racine primitive de l'unité. Démontrez après que n est l'entier minimal tel que $\alpha^n \in K$.

3. Pour l'inverse, démontrons que si $n = p$ est premier et si $\sqrt[p]{a}$ est une racine fixée de $a \in K \setminus K^p$ (dans un corps de décomposition adéquat), alors $L = K(\sqrt[p]{a})$ est $\mathbb{Z}/p\mathbb{Z}$ galoisienne.

   Indice: Soit ξ un p-ième racine primitve d'unité, et soit $\alpha = \sqrt[p]{a}$. Dans Lemme 4.9.1 des notes de cours on a démontré que toute les racines de $m_{\alpha,K}$ sont de forme de $\xi^j\alpha$, et que $K \subseteq L$ est galoisienne avec $\mathrm{Gal}(K/L)$ abélien. Notons aussi que puisque $a \notin K^p$, l'extension $K \subseteq L$ est non-triviale. Prenons donc un élément non-neutre $\phi \in \mathrm{Gal}(K/L)$. Démontrez que le plus petit entier $s > 0$ tel que $\phi^s(\alpha) = \alpha$ est $s = p$.

4. Soit p un entier premier et soit $n > 0$ un entier positif arbitraire. Démontrez que $\mathbb{Q} \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{p^n}}\right)$ est $(\mathbb{Z}/p^n\mathbb{Z})^{\times}$-galoisienne en appliquant le point précédent inductivement pour l'extension $\mathbb{Q}\left(e^{\frac{2\pi i}{p^j}}\right) \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{p^{j+1}}}\right)$ pour $1 \leq j \leq n-1$.

   Indice: Pour $n = 1$, en utilisant comme vu en cours que $x^{p-1} + x^{p-2} + \cdots + 1$ est irréductible montrez que $\mathbb{Q}(e^{\frac{2\pi i}{p}})$ est une extension de degré $p-1$. Ensuite, utilisez le point précédent pour conclure que l'extension $\mathbb{Q} \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{p^n}}\right)$ est de degré $|\,(\mathbb{Z}/p^n\mathbb{Z})^{\times}\,|$. Ensuite, montrez que si ϕ est dans le groupe Galois et $\xi = e^{\frac{2\pi i}{p}}$, alors $\phi(\xi) = \xi^k$ pour un $k \in \mathbb{Z}$ avec $(k,p) = 1$, ce qui donnera lieu en réduisant k modulo p^n à une injection du groupe Galois dans $(\mathbb{Z}/p^n\mathbb{Z})^{\times}$, ce qui permettra de conclure.

Exercice 4. 1. Démontrez que $\mathbb{Q}\left(e^{\frac{2\pi i}{9}} + e^{-\frac{2\pi i}{9}}\right)$ est $\mathbb{Z}/3\mathbb{Z}$-galoisisenne.

   Indice: considérez l'extension $\mathbb{Q}\left(e^{\frac{2\pi i}{9}}\right)$.

2. Plus généralement, démontrez que pour chaque entier premier p, il existe une extension $\mathbb{Q} \subseteq L$ tel que $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}$.

   Indice: Pour $p \geq 3$ considérez l'extension $\mathbb{Q} \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{p^2}}\right)$, et appliquez le théorème fondamental de la théorie de Galois.

Exercice 5.
Soit K un corps parfait, et soit $K \subseteq M = K(\alpha)$ et $K \subseteq N = K(\beta)$ des extensions galoisiennes de K.

1. Démontrez que $K \subseteq L = K(\alpha, \beta)$ est aussi galoisienne.

   Supposons à partir de maintenant que $M \cap N = K$ en tant que sous-corps de L.

2. Démontrez que $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K)$ qui est la restriction sur chaque composante est un isomorphisme.

3. Démontrez que pour chaque entiers premiers distincts p et q, il existe une extension $\mathbb{Q} \subseteq L$ galoisienne tel que $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/pq\mathbb{Z}$.

Exercice 6.
Soit $K \subseteq L$ une extension Q_8-galoisienne (où Q_8 est le groupe des quaternions), et soit $f \in K[x]$ un polynôme irréductible tel que L est un corps de décomposition de f. Démontrez que $\deg f = 8$.

Exercice 7.
Soit $K \subset L \subset M$ des extensions algébriques (non-nécessairement de degré fini) tel que $K \subset L$ et $L \subset M$ sont séparables. Montrez que $K \subset M$ est aussi séparable.