EPFL - Printemps 2025	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Série 14	

Les exercices marqués d'une étoile ($\star$) sont optionnels.

Exercice 1 (Correspondance de Galois)**.**
Soit $f = x^5 - 2 \in \mathbb{Q}[x]$, et soit E le corps de décomposition de f sur $\mathbb{Q}$.

1. Montrez que $[E : \mathbb{Q}] = 20$.
2. Montrez qu'il existe un morphisme de groupes $f \colon \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$ tel que
$$\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \rtimes_f \mathbb{Z}/4\mathbb{Z},$$
et identifiez explicitement f.
3. *Un peu de théorie des groupes.*
   (a) Comme $\mathbb{Z}/5\mathbb{Z} \times 0$ est normal dans $\mathbb{Z}/5\mathbb{Z} \rtimes_f \mathbb{Z}/4\mathbb{Z}$, déduisez comme c'est un 5-Sylow qu'il y a un unique sous-groupe d'ordre 5 dans $\mathrm{Gal}(E/\mathbb{Q})$, qu'on note H_5.
   (b) Soit H un sous-groupe d'ordre 10. Montrez que $H_5 \subset H$. En prenant le quotient par H_5 et en utilisant le théorème de correspondance, déduisez que $\mathrm{Gal}(E/\mathbb{Q})$ a un unique sous-groupe d'ordre 10, qu'on note H_{10}, que celui-ci est normal et isomorphe à D_{10}.
   (c) On rappelle que si $H, K \subset G$ sont des sous-groupes normaux d'un groupe avec $H \cap K = \{e\}$, alors HK est un sous-groupe de G isomorphe au produit direct $H \times K$. En utilisant cela, montrez qu'il n'existe pas de sous-groupes normaux d'ordre 4 et 2 dans $\mathrm{Gal}(E/\mathbb{Q})$.
4. Listez toutes les sous-extensions Galoisiennes sur $\mathbb{Q}$ de E et donnez des éléments primitifs pour ces extensions.

Exercice 2.
Soit K un corps de caractéristique différente de 2, soit f un polynôme irréductible séparable sur K, et soient $\alpha_1, \ldots, \alpha_n$ les racines de f dans un corps de décomposition. Le *discriminant* de f est par définition
$$\Delta := \prod_{i<j} (\alpha_i - \alpha_j)^2.$$
Montrez que $\Delta \in K$, et que les conditions suivantes sont équivalentes :

- Δ est un carré dans K;
- le morphisme naturel $\mathrm{Gal}(E/K) \to S_n$ défini par l'action sur les racines de f se factorise dans le groupe alterné A_n.

Indice: $\delta = \prod_{i<j}(\alpha_i - \alpha_j)$ est une racine carrée de Δ.

Exercice 3.
Soit $f = x^3 + ax + b \in \mathbb{Q}[x]$ un polynôme irréductible de discriminant Δ (c.f. l'exercice précédent).

1. Montrez qu'on a deux cas:
   - Si Δ n'est pas un carré dans $\mathbb{Q}$, alors $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$;
   - Si Δ est un carré dans $\mathbb{Q}$, alors $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$.

2. Montrez que $\Delta = -(4a^3 + 27b^2)$.

   Indice: Soient $\alpha_1, \alpha_2, \alpha_3$ les racines de f dans un corps de décomposition. Montrez que $\Delta = -f'(\alpha_1)f'(\alpha_2)f'(\alpha_3)$, et écrivez $x^3 + ax + b = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ pour trouver des relations entre les α_i qui permettent de faire le calcul. Pour vous entraîner, vous pouvez essayer de faire le calcul pour un polynôme de degré 2 sans utiliser les formules pour les solutions (vous devriez trouver le determinant habituel!).

3. Trouvez deux extensions Galoisiennes K_1, K_2 de $\mathbb{Q}$ réelles (i.e. $K_1, K_2 \subseteq \mathbb{R}$) telles que $\mathrm{Gal}(K_1/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$ et $\mathrm{Gal}(K_2/\mathbb{Q}) \cong S_3$.

Exercice 4.
Soit $L = K(a)$ une extension simple, et soit A la matrice de l'application K-linéaire $(\cdot a)\colon L \to L$ par rapport à une base quelconque de L. Soit aussi $E \supseteq L$ un corps de décomposition de $m_{a,K}$.

1. Montrez que le polynôme caractéristique $\phi(x) = \det(x\,\mathrm{id} - A)$ de A est égal au polynôme minimal $m_{a,K}$.

2. Montrez que si a est séparable, alors A est diagonalisable dans E.

3. ($\star$) Montrez que si a est purement inséparable, alors A a un seul bloc de Jordan dans E.

4. Montrez que $\det(A) = (-1)^{[L:K]} m_{a,K}(0)$.

5. Montrez que si L/K est Galois, alors $\det(A) = \prod_{g \in G} g(a)$ où $G = \mathrm{Gal}(L/K)$.

6. Calculez ce polynôme minimal pour L le corps de décomposition de $x^3 - 2$ sur $\mathbb{Q}$, et $a = \sqrt[3]{2} + e^{2\pi i/3}$.

Exercice 5 ($\star$)**.**
Montrez que si $K \subseteq L$ et $L \subseteq E$ sont deux extensions séparables (pas nécessairement finies), alors $K \subseteq E$ est aussi séparable.

Exercice 6 (Extension quadratique pour $\mathrm{car}(k) = 2$) ($\star$)**.**
Soit K un corps de caractéristique 2 et soit $K \subseteq L$ une extension de degré 2.

(a) Supposons que pour tous $\alpha \in L \backslash K$ nous avons que $\alpha^2 \in K$. Montrer que:

   (i) $L = K(\alpha)$, où $\alpha \in L \backslash K$.

   (ii) tout $\alpha \in L \backslash K$ est inséparable.

(b) Supposons qu'il existe $\alpha \in L \backslash K$ tel que $\alpha^2 \notin K$. Montrer que:

   (i) $L = K(\beta)$, où $\beta \in L \backslash K$ est tel que $m_{\beta,K}(x) = x^2 + x + c \in K[x]$.

   (ii) $\tau : K(\beta) \to K(\beta)$ donné par $\tau|_K = \mathrm{Id}_K$ et $\tau(\beta) = \beta + 1$ est un automorphisme de $K(\beta)$. Conclure que $\mathrm{Gal}(K(\beta)/K) \cong \mathbb{Z}/2\mathbb{Z}$.

   (iii) tout $\alpha \in L \backslash K$ est séparable, c'est à dire que $K \subset L$ est une extension séparable.

Exercice 7 ($\star$)**.**
Si K est un corps dénombrable, montrez que $\overline{K}$ est également dénombrable.

Exercice 8 ($\star$)**.**
Fixons un entier premier p. Soit $n_j = p^{m_j}$ où $m_j = \prod_{i=1}^{j} i$ pour chaque entier $j \geq 1$, et soit $K_j = \mathbb{F}_{n_j}$.

1. Démontrez que les K_j peuvent être mis dans un système direct. Autrement dit, il existe des homomorphismes injectifs $\iota_j : K_j \to K_{j+1}$ pour chaque entier $j \geq 1$.

2. Fixons ι_j comme dans le point précédent. Montrez que la colimite directe K, comme définie dans le Lemme 4.8.7, est un corps, et de plus il existe un plongement $\mathbb{F}_p \to K$

3. Démontrez que K est algébrique sur $\mathbb{F}_p$

4. Démontrez que chaque polynôme $f \in \mathbb{F}_p$ scinde sur K. (Autrement dit K est la clôture algébrique de $\mathbb{F}_p$, et on le dénote d'habitude par $\overline{\mathbb{F}}_p$. Dans une manière similaire, le corps de nombres algébriques $\mathbb{C}_{alg,\mathbb{Q}}$, en utilisant la notation du Cor 4.2.21, est la clôture algébrique de $\mathbb{Q}$. Aussi, $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$. On étudiera plus des clotûre algébriques à la fin du semestre.)

Exercice 9 ($\star$). 1. Si $K \subseteq L$ est une extension purement inséparable, alors $\mathrm{Gal}(L/K) = \{\mathrm{Id}_L\}$.

2. Soit $K \subseteq L$ une extension finie tel que

$$[L_{insep,K} : K]|\,\mathrm{Gal}(L/K)| = [L : K].$$

Montrer que L est séparable sur $L_{insep,K}$.