EPFL - Printemps 2022	Prof. Z. Patakfalvi
Anneaux et Corps	**Exercices**
Série 13	30 Mai 2022

Exercices

Exercice 1. (a) Montrer que $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$ est primitif dans $\mathbb{Q}$ et calculer son polynôme minimal.

(b) Montrer que $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ est une base de $\mathbb{Q}(\sqrt{2},\sqrt{3})$ comme $\mathbb{Q}$-espace vectoriel.

(c) Montrer que $a\sqrt{3}+b\sqrt{6} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$ est primitif dans $\mathbb{Q}$ si et seulement les nombres rationnels a, b sont non nuls.

(d) Si $a, b, c \in \mathbb{Q}$ sont tous non nuls, montrer que $a\sqrt{2}+b\sqrt{3}+c\sqrt{6} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$ est primitif dans $\mathbb{Q}$.

Exercice 2.
Considérons l'extension $\mathbb{F}_2 \subset \mathbb{F}_{2^n}$. D'après l'exemple 3.6.4 (f), $|\operatorname{Gal}(\mathbb{F}_{2^n}/\mathbb{F}_2)| = n$, et $\operatorname{Gal}(\mathbb{F}_{2^n}/\mathbb{F}_2) = \langle F \rangle$, où F est l'automorphisme Frobenius,

$$F : \mathbb{F}_{2^n} \ni \alpha \mapsto \alpha^2 \in \mathbb{F}_{2^n}.$$

1. Soit $n = 2$, et considérons l'extension $\mathbb{F}_2 \subset \mathbb{F}_4 = \mathbb{F}_2(\alpha)$, où α est une racine de x^2+x+1. Donnez la matrice de l'automorphisme Frobenius dans la base $\{1, \alpha\}$ en tant que $\mathbb{F}_2$-espace vectoriel. Quels sont les valeurs et leurs espaces propres? Peut on diagonaliser la matrice?

2. Soit $n = 3$, et considérons l'extension $\mathbb{F}_2 \subset \mathbb{F}_8 = \mathbb{F}_2(\beta)$, où β est une racine de x^3+x+1. Donnez la matrice de l'automorphisme Frobenius dans la base $\{1, \beta, \beta^2\}$ en tant que $\mathbb{F}_2$-espace vectoriel. Quels sont les valeurs et leurs espaces propres? Peut on diagonaliser la matrice sur $\mathbb{F}_2$? Sur $\mathbb{F}_4$?

Exercice 3.
Soit $f(x) = x^6 + x^3 + 1 \in \mathbb{Q}[x]$.

1. Montrez que f est irréductible sur $\mathbb{Q}$. *Indication: vous pouvez utiliser le critère d'Eisenstein pour montrer que $ev_{y+1}(f)$ est irréductible et conclure.*

2. Soit α une racine de f. Montrez que α est une 9-ième racine primitive d'unité.

3. Soit L le corps de décomposition de f sur $\mathbb{Q}$. Montrez que l'extension $\mathbb{Q} \subseteq L$ est galoisienne avec $\operatorname{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/9\mathbb{Z})^\times$.

4. Construisez une extension galoisienne de $\mathbb{Q}$ de degree 3.

Exercice 4 (Automorphismes de $\mathbb{C}(x)$)**.**
Soit $\mathbb{C}(x)$ le corps de fractions de $\mathbb{C}[x]$. On définit deux $\mathbb{C}$-automorphismes F et G en posant

$$F(x) = \frac{x+i}{x-i} \quad \text{et} \quad G(x) = \frac{ix-i}{x+1}$$

et on considère le groupe $\mathcal{A}$ engendré par F et G.

1. Calculer toutes les puissances de F, G, $F \circ G$ et $G \circ F$.

2. Montrer que les éléments d'ordre deux FG et GF engendrent un sous-groupe normal de $\mathcal{A}$ isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3. Montrer que F et G engendrent un groupe d'automorphismes de $\mathbb{C}(x)$ d'ordre 12.

4. Montrer que ce groupe est isomorphe à A_4.

Exercice 5 (Correspondance de Galois)**.**
Dans chacun des cas suivantes déterminer le groupe de Galois de l'extension donnée, déterminer tous ses sous-groupes et tous les sous-corps de points fixes correspondants.

1. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{7})$.
2. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
3. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.
4. $\mathbb{Q} \subset E$ où E est le corps de rupture de $t^4 - 2t^2 - 1 \in \mathbb{Q}[t]$.

Indication. Ce corps de rupture est de degré 8 et on montrera qu'il s'agit de $\mathbb{Q}(\sqrt{1+\sqrt{2}}, i)$. On explicitera alors un automorphisme d'ordre 2 et un autre d'ordre 4 qui ne commutent pas entre eux, si bien que le groupe de Galois est le groupe dihédral d'ordre 8.

Exercice 6.
Soit $K \subseteq L \subseteq E$ une extension algébrique tel que $K \subseteq L$ et $L \subseteq E$ sont Galois. Montrer que $K \subseteq E$ n'est pas forcément Galois.
Indication. Envisager les extensions $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}})$

Exercice 7. 1. Soit $K \subseteq L \subseteq E$ tel que $K \subseteq L$ et $L \subseteq E$ sont Galois et finis. Montrer qu'il existe $K \subseteq E \subseteq F$ tel que $K \subseteq F$ est Galois.

2. Soit $K \subseteq L \subseteq E$ tel que $K \subseteq L$ et $L \subseteq E$ sont séparable. Monterer que $K \subseteq E$ est séparable.
Indication. Montrer que $L = K(\alpha)$ et $E = L(\beta)$. Pour tout $\sigma \in \mathrm{Gal}(L/K)$, considérons l'homomorphisme induit $\sigma^x : L[x] \to L[x]$. Soit $\{m_{\beta,L} = m_1, m_2, \ldots, m_r\}$ l'orbite $\mathrm{Gal}(L/K)$ de $m_{\beta,L}$. Définissons $g = \prod_{i=1}^{r} m_i$ et soit F le corps de décomposition de g sur L. Montrer que g est séparable sur K.

Exercice 8.
Si K est un corps dénombrable, montrez que $\overline{K}$ est également dénombrable.

Exercice 9.
Montrer que tous les groupes finis sont des groupes de Galois.

Supplementary exercise

Exercice 10. 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 $L_{insep,K}$.