EPFL - Printemps 2023	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Série 12	22 mai 2023

Les exercices indiqués par une étoile $\star$ sont optionnels.

Exercice 1 (Corps imparfaits). (a) Soit K un corps de caractéristique $p > 0$ et soit $\alpha \in K \backslash K^p$. Montrer que $x^p - \alpha \in K[x]$ est irréductible.

Soit $L = (\mathbb{F}_p(x))[y]/(y^2 - x(x-1)(x+1))$.

(b) Montrer que L est un corps.

(c) Si $p \neq 2$, montrer que L n'est pas parfait.

(d) Si $p = 2$, montrer que L n'est pas parfait.

Exercice 2 (Extension quadratique pour car$(k) = 2$.).
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 3.
Décrivez le groupe $\mathrm{Gal}(K/\mathbb{Q})$ dans les cas suivants: $K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{7}), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\omega^2)$ où $\omega = e^{2i\pi/3}$.

Exercice 4.
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 5.
Dans les cas suivants, calculez $G = \mathrm{Gal}(\mathbb{Q}(\alpha, \beta)/\mathbb{Q})$, et calculez le pôlynome minimal de $\alpha, \alpha+\beta, \alpha \cdot \beta$ et α^{-1}. Pour calculer les polynômes minimaux, on s'inspirera de l'exemple 4.6.12.

1. $\alpha = \sqrt{3}, \beta = \sqrt{7}$
2. $\alpha = e^{(i\pi/3)}, \beta = -1$
3. $\alpha = e^{(i\pi/3)}, \beta = i$
4. $\alpha = e^{(i\pi/6)}, \beta = i$.

Exercice 6.
Let $f = x^3 + ax + 1 \in \mathbb{Q}[x]$ such that $a > 0$, $a \in \mathbb{Z}$.

1. Show that f is irreducible over $\mathbb{Q}$.
2. Show that f does not have 3 real roots in its splitting field (the splitting field (corps de décomposition) is isomorphic to the subfield of $\mathbb{C}$ generated by the complex roots of f, and hence it makes sense to talk about its element being real).

3. Let $K = \mathbb{Q}[x]/(f)$. Show that K is a degree 3 extension of $\mathbb{Q}$, which is not Galois.
4. Let L be the decomposition field of f over $\mathbb{Q}$. Show that $\mathrm{Gal}(L/Q) \cong S_3$

Exercice 7.
Soit K un corps de caractéristique $p > 0$, et $\alpha \neq 0 \in K$ tel que le pôlynome $f(x) = x^p - x + \alpha \in K[x]$ n'a pas de racines dans K. Soit L le corps de decomposition de f, et $G = \mathrm{Gal}(L/K)$.

1. Montrez que $G \cong \mathbb{Z}/p\mathbb{Z}$. *Indication: Si β est une racine de f, alors $\beta + \gamma$ l'est aussi, pour tout $\gamma \in \mathbb{F}_p$.*
2. Montrez que le pôlynome f est irréductible sur K.
3. Considérons $K = \mathbb{F}_p(t)$. Montrez que le pôlynome $f(x) = x^p - x + t \in K[x]$ n'a pas de racines dans K.
4. Soit K et f comme dans le point précédent. Donnez le corps de décomposition de f sur K.

Exercice 8 (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 décomposition de $t^4 - 2t^2 - 1 \in \mathbb{Q}[t]$.

Indication. Ce corps de décomposition 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 9 ($\star$)**.**
Montrer que tous les groupes finis sont des groupes de Galois. *Indication: on pourra trouver un corps K_n où S_n agit fidèlement.*
Remarque. En utilisant des techniques de géométrie algébrique et de topologie algébrique on peut montrer que tout groupe fini est réalisé comme un groupe de Galois d'une extension de $\mathbb{C}(t)$.

1. Avec de la géométrie algébrique, on voit que les extensions finies de $\mathbb{C}(t)$ correspondent à des morphismes de *courbes algébriques* $X \to \mathbb{P}^1_{\mathbb{C}}$ tel que si ont enlève un nombre fini de points à $\mathbb{P}^1_{\mathbb{C}}$, le morphisme devient un revêtement au sens topologique.
2. $\mathbb{P}^1_{\mathbb{C}}$ privé d'un nombre fini de points est le plan complexe $\mathbb{C}$ privé d'un nombre fini de points. Par la topologie algébrique, on sait que $\pi_1(\mathbb{C} \setminus \{p_1, \ldots, p_n\}) \cong F_n$ le groupe libre sur n-générateurs. Dès lors par la théorie des revêtements, comme tout groupe fini G admet une surjection $F_n \to G$ pour un certain n, il existe un revêtement fini de $\mathbb{C} \setminus \{p_1, \ldots, p_n\}$ avec groupe de Galois égal à G.
3. En retournant à la géométrie algébrique, on obtient alors un morphisme de *courbes algébriques* $X \to \mathbb{P}^1_{\mathbb{C}}$ avec groupe de Galois G et donc une extension de $\mathbb{C}(t)$ avec groupe de Galois G.

Si ce genre de choses vous intrigue, le rédacteur vous encourage à suivre des cours de géométrie algébrique et de topologie algébrique, et/ou à faire des projets dans ces domaines.

Exercice 10 ($\star$)**.**
Soit $n \geq 1$. Calculez le groupe de Galois $\mathrm{Gal}(L_n/\mathbb{C}(t))$ où est L_n est le corps de décomposition de

$$X^{2n} - 2\left(\frac{t+1}{t-1}\right)X^n + 1.$$