EPFL - Printemps 2025	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Solutions 10	

Exercice 1. 1. Montrez que $1, \sqrt[3]{2}, \sqrt[3]{4}$ est une $\mathbb{Q}$ base de $\mathbb{Q}(\sqrt[3]{2})$.

2. Écrivez la matrice de la multiplication par

$$1 + \sqrt[3]{2} + \sqrt[3]{4},$$

vue comme application linéaire $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$. Calculez le polynôme caractéristique de cette matrice et déduisez en le polynôme minimal de l'élément ci-dessus.

Solution. Le premier point suit par exemple de l'isomorphisme $\mathbb{Q}[t]/(t^3-2) \cong \mathbb{Q}(\sqrt[3]{2})$ par $t \mapsto \sqrt[3]{2}$. Dans la description par quotient, on voit que l'image de $1, t, t^2$ forme une $\mathbb{Q}$-base.

Pour le deuxième point, la matrice est

$$\begin{pmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}.$$

Le polynôme caractéristique de cette matrice est

$$X^3 - 3X^2 - 3X - 1.$$

Par Cayley-Hamilton l'endomorphisme de multiplication par $1 + \sqrt[3]{2} + \sqrt[3]{4}$ est annulé par ce polynôme. En évaluant en 1 cet endormophisme, on conclut que $1 + \sqrt[3]{2} + \sqrt[3]{4}$ est un zéro de ce polynôme. Comme $1 + \sqrt[3]{2} + \sqrt[3]{4} \notin \mathbb{Q}$ on a forcément que $\mathbb{Q}(1 + \sqrt[3]{2} + \sqrt[3]{4}) = \mathbb{Q}(\sqrt[3]{2})$ car comme $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ il n'y a pas de sous-extensions propres car le degré d'une sous-extension propre diviserait 3. Ainsi le degré du polynôme minimal de $1 + \sqrt[3]{2} + \sqrt[3]{4}$ est 3, ce qui conclut.

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

Solution.

Pour toutes les extensions sauf $\mathbb{Q}(\sqrt[3]{2})$, on est dans un cas de forme $\mathbb{Q}(\alpha)$ avec le polynôme minimal de α de degré 2. Notons α' l'autre racine et $m(t) \in \mathbb{Q}[t]$ le polynôme minimal. En utilisant l'exercice 4 de la Série 7, on voit que $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$. Dès lors

$$\mathbb{Q}(\alpha) \xleftarrow{\mathrm{ev}_\alpha} \mathbb{Q}[t]/(m(t)) \xrightarrow{\mathrm{ev}_{\alpha'}} \mathbb{Q}(\alpha')$$

est un automorpshime non trivial, comme il envoie $\alpha \mapsto \alpha'$. Par le dernier point de la Proposition 4.6.4 on déduit que $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ est cyclique d'ordre 2.

En plongeant $\mathbb{Q}(\sqrt[3]{2})$ dans le corps de décomposition de $x^3 - 2$ on voit qu'un automorphisme doit envoyer $\sqrt[3]{2}$ sur une autre racine de $x^3 - 2$. Mais comme la seule racine de $x^3 - 2$ contenue dans $\mathbb{Q}(\sqrt[3]{2})$ est $\sqrt[3]{2}$ on conclut que $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ est réduit à l'identité.

Exercice 3.
Soit $\xi = e^{\frac{2\pi i}{3}}$. Considérons

$$\mathbb{Q}(\xi, \sqrt[3]{2}) \subseteq \mathbb{C},$$

un corps de décomposition de $x^3 - 2$. (Voir série 8, exercice 4).

On attire l'attention sur le point (3) de la Proposition 4.6.4. Que le groupe $\mathrm{Gal}(L/K)$ *agit transitivement sur les racines d'un polynôme minimal est un théorème* d'existence. *En effet étant donné des racines* α_1, α_2 *d'un polynôme minimal, la transitivité signifie qu'il existe* $\phi \in \mathrm{Gal}(L/K)$ *tel que* $\phi(\alpha_1) = \alpha_2$.

1. Montrez qu'il existe $\phi \in \mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q})$ tel que $\phi(\xi) = \xi$ et $\phi(\sqrt[3]{2}) = \xi\sqrt[3]{2}$. Quel est l'ordre de ϕ ?

2. Montrez qu'il existe $\psi \in \mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q})$ avec $\psi(\xi\sqrt[3]{2}) = \xi^2\sqrt[3]{2}$ et $\psi(\sqrt[3]{2}) = \sqrt[3]{2}$. Quel est l'ordre de ψ ?

3. En utilisant l'action de $\mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})$ sur les racines de $x^3 - 2$ et la Proposition 4.6.4 du cours, déduisez que $\mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2}) \cong S_3$.

4. Raisonnez similairement pour calculer les groupes de Galois des extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

Solution.

1. On considère l'extension
$$\mathbb{Q}(\xi) \subset \mathbb{Q}(\xi, \sqrt[3]{2}).$$
Comme $\mathbb{Q}(\xi, \sqrt[3]{2})$ est le corps de décomposition de $x^3 - 2 \in \mathbb{Q}(\xi)[x]$, on peut appliquer le point (3) de la Proposition 4.6.4 pour avoir l'existence d'un $\phi \in \mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q}(xi))$ tel que $\phi(\sqrt[3]{2}) = \xi\sqrt[3]{2}$.

   Explicitement, on peut construire cet automorphisme de la manière suivante.

   On étend l'identité sur $\mathbb{Q}(\xi)$ en utilisant les évaluations
$$\mathbb{Q}(\xi, \sqrt[3]{2}) \xleftarrow{\mathrm{ev}_{\sqrt[3]{2}}} \mathbb{Q}(\xi)[t]/(t^3 - 2)) \xrightarrow{\mathrm{ev}_{\xi\sqrt[3]{2}}} \mathbb{Q}(\xi, \sqrt[3]{2})$$
   le polynôme $t^3 - 2$ étant irréductible dans $\mathbb{Q}(\xi)$ car il n'a pas de racines. En effet toute racine de ce polynôme est de degré 3 sur $\mathbb{Q}$ et ne peut donc être contenue dans $\mathbb{Q}(\xi)$ qui est une extension de degré 2.

2. Comme $\mathbb{Q}(\xi, \sqrt[3]{2})$ est le corps de décomposition de $x^2 + x + 1 \in \mathbb{Q}(\sqrt[3]{2})[x]$, on peut appliquer le point (3) de la Proposition 4.6.4 pour avoir l'existence d'un $\psi \in \mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2}))$ tel que $\psi(\xi) = \xi^2$ et $\psi(\xi\sqrt[3]{2}) = \xi^2\sqrt[3]{2}$.

   Solution commune aux points 1. et 2. On sait comme $\mathbb{Q}(\xi, \sqrt[3]{2})$ est un corps de décomposition d'un polynôme séparable, qu'elle est Galoisienne et donc que
$$|\mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q})| = 6.$$
   Aussi, on sait que si $\phi \in \mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})$ alors forcément
$$\phi(\xi) = \xi, \xi^2 \quad \phi(\sqrt[3]{2}) = \sqrt[3]{2}, \xi\sqrt[3]{2}, \xi^2\sqrt[3]{2}.$$
   Comme on dénombre 6 possibilités d'automorphismes, elles sont forcément toutes réalisées. Cela démontre les points 1. et 2. simultanément.

3. Par le point (2) de la Proposition mentionnée on a un morphisme injectif $\mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q}) \to S_3$. Mais par le quatrième point, on sait que $\mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})$ a $[\mathbb{Q}(\xi, \sqrt[3]{2}) \colon \mathbb{Q}] = 6$ éléments ce qui conclut.

4. Commençons par remarquer que les éléments de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$ doivent envoyer $\sqrt{i} \mapsto \pm\sqrt{i}$ pour $i = 2, 3, 5$. En effet par le point 1 de la Proposition 4.6.4 les racines de (t^2-2) et (t^2-3) et $(t^2 - 5)$ sont respectivement permutées. Ainsi, on voit qu'on au plus 4 (respectivement 8) automorphismes entièrement déterminés par $\sqrt{2} \mapsto \pm\sqrt{2}$ et $\sqrt{3} \mapsto \pm\sqrt{3}$ et $(\sqrt{5} \mapsto \pm\sqrt{5})$.

   Mais par le quatrième point de la Proposition 4.6.4, on sait que la taille des groupes de Galois sont égaux au degré de ces extensions. En effet les extensions considérées sont respectivement les corps de décomposition des polynômes séparables
$$(t^2 - 2)(t^2 - 3) \quad \text{et} \quad (t^2 - 2)(t^2 - 3)(t^2 - 5).$$

Dès lors on sait que $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ a 4 éléments et que $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$ a 8 éléments. En effet on peut calculer le degré de ces extensions en utilisant les extensions successives de degré 2

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2},\sqrt{3}) \subset \mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}).$$

Ainsi, on conclut que les 4 (respectivement 8) automorphismes sont donc entièrement déterminés par $\sqrt{2} \mapsto \pm\sqrt{2}$ et $\sqrt{3} \mapsto \pm\sqrt{3}$ et ($\sqrt{5} \mapsto \pm\sqrt{5}$). Notons τ_i pour l'automorphisme qui envoie $\sqrt{i} \mapsto -\sqrt{i}$ et fixe $\sqrt{j}$ si $j \neq i$ pour $i,j = 2,3,5$. Ces automorphismes génèrent les groupes de Galois considérés et commutent deux à deux. Ainsi on voit que ces groupes de Galois sont abéliens. Notons C_2 pour un groupe d'ordre 2; on conclut maintenant que les morphismes

$$C_2 \oplus C_2 \to \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \quad \text{et} \quad C_2 \oplus C_2 \oplus C_2 \to \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$$

définis en utilisant la propriété universelle de la somme directe de groupe abéliens en envoyant les générateurs des copies de C_2 sur les τ_i sont des isomorphismes.

Exercice 4.
Soit K un corps et L un corps de décomposition généré par des éléments séparables. En utilisant la Proposition 4.6.4 du cours montrez que si $\alpha \in L$ alors si l'orbite de α par l'action $\mathrm{Gal}(L/K)$ est de taille $[L:K]$ on a $L = K(\alpha)$.

Calculez des éléments primitifs pour chacune des extensions apparaissant dans l'exercice 3 en utilisant ce principe.

Solution.

Montrons l'affirmation. Premièrement, si on suppose que l'orbite de α est de taille $[L\colon K]$ alors tous les éléments de l'orbite sont de racines de $m_\alpha(t)$ par le premier point de la Proposition 4.6.4. Ainsi le degré de $m_\alpha(t)$ est au moins $[L\colon K]$. Mais comme il est également au plus $[L\colon K]$, on conclut qu'il est de degré $[L\colon K]$. On conclut alors $K(\alpha) = L$ par égalité des degrés.

Maintenant on en déduit que

$$\xi + \sqrt[3]{2} \quad \text{et} \quad \sqrt{2}+\sqrt{3} \quad \text{et} \quad \sqrt{2}+\sqrt{3}+\sqrt{6}$$

sont des éléments primitifs des extensions de l'exercice 3.

Exercice 5 (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.

Solution.

(a) As $\alpha \notin K^p$ it follows that for all $\beta \in K$ we have $\beta^p \neq \alpha$ and thus $x^p - \alpha \in K[x]$ does not admit roots in K. Let F be a decomposition field of $x^p - \alpha$ over K and let $\beta \in F$ be a root of this polynomial. We have that:

$$x^p - \alpha = x^p - \beta^p = (x-\beta)^p \text{ in } F[x].$$

Let $m_{\beta,K}(x) \in K[x]$ denote the minimal polynomial of β over K. As β is a root of $x^p - \alpha$, it follows that $m_{\beta,K}(x) | x^p - \alpha = (x-\beta)^p$. Therefore there exists some i, $1 \leq i \leq p$, such that $m_{\beta,K}(x) = (x-\beta)^i$. Now, as $m_{\beta,K}(x) \in K[x]$ we have that:

$$(x-\beta)^i = \sum_{j=0}^{i} (-1)^j \binom{i}{j} x^{i-j}\beta^j = x^i - i\beta x^{i-1} + \cdots + (-1)^i\beta^i \in K[x].$$

It follows that $-i\beta = 0$ and so $i = p$. Therefore $m_{\beta,K}(x) = (x-\beta)^p = x^p - \alpha$ and we conclude that $x^p - \alpha \in K[x]$ is irreducible.

(b) To show that L is a field, we will show that the polynomial $y^2 - x(x-1)(x+1) \in (\mathbb{F}_p(x))[y]$ is irreducible. As $y^2 - x(x-1)(x+1)$ is a unitary polynomial, it is primitive and so, by Gauss III, it is irreducible in $(\mathbb{F}_p(x))[y]$ if and only if it is irreducible in $(\mathbb{F}_p[x])[y]$. Now, $x \in \mathbb{F}_p[x]$ is irreducible and we use Eisenstein with "$p = x$" (here p denotes the irreducible in Eisenstein criterion) to deduce that $y^2 - x(x-1)(x+1)$ is irreducible in $(\mathbb{F}_p[x])[y]$.

(c) By Proposition 4.5.7, as $\mathrm{char}(L) = p$, we have that L is perfect if and only if $L^p = L$. We will show that $x \notin L^p$.

Assume by contradiction that $x \in L^p$. Then, there exists $f \in L$ such that $x = f^p$. It follows that $f \in L$ is a root of the polynomial $t^p - x \in \mathbb{F}_p(x)[t]$. As $x \in \mathbb{F}_p(x)$ is not a p^{th} power, we see this using from example the degree of polynomials, it follows that the polynomial $t^p - x$ is irreducible in $(\mathbb{F}_p(x))[t]$, see item (a). This shows that $m_{f,\mathbb{F}_p(x)}(t) \sim t^p - x \in (\mathbb{F}_p(x))[t]$.

Consider the chain of extensions:

$$\mathbb{F}_p(x) \subseteq (\mathbb{F}_p(x))(f) \subseteq L$$

and we have $[(\mathbb{F}_p(x))(f) : \mathbb{F}_p(x)] | [L : \mathbb{F}_p(x)]$. But $[L : \mathbb{F}_p(x)] = 2$ and $[(\mathbb{F}_p(x))(f) : \mathbb{F}_p(x)] = p$, where $p \neq 2$. We have arrived at a contradiction.

(d) We have that $L = (\mathbb{F}_2(x))[y]/(y^2 + x(x+1)^2)$. Note that the polynomial $y^2 + x(x+1)^2 \in (\mathbb{F}_2(x))[y]$ admits $\sqrt{x}(x+1)$ as a double root and so it is irreducible in $(\mathbb{F}_2(x))[y]$. Now, by Proposition 4.2.25, it follows that $L = (\mathbb{F}_2(x))(\sqrt{x}(x+1)) = (\mathbb{F}_2(x))(\sqrt{x}) = \mathbb{F}_2(\sqrt{x})$. For the last equality, note that $\mathbb{F}_2(\sqrt{x}) \subseteq (\mathbb{F}_2(x))(\sqrt{x})$ and, as $\mathbb{F}_2(x) \subseteq \mathbb{F}_2(\sqrt{x})$, we have $(\mathbb{F}_2(x))(\sqrt{x}) \subseteq (\mathbb{F}_2(\sqrt{x}))(\sqrt{x}) = \mathbb{F}_2(\sqrt{x})$.

As $\mathrm{char}(L) = 2$, it follows that L is perfect if and only if $L^2 = L$, see Proposition 4.5.7. But

$$\begin{aligned} L^2 &= \{f(\sqrt{x})^2 |\ f(\sqrt{x}) \in L\} = \left\{ \left(\frac{f_1(\sqrt{x})}{f_2(\sqrt{x})} \right)^2 |\ f_1(\sqrt{x}), f_2(\sqrt{x}) \in \mathbb{F}_2[\sqrt{x}],\ f_2(\sqrt{x}) \neq 0 \right\} \\ &= \left\{ \frac{f_1(x)}{f_2(x)} |\ f_1(x), f_2(x) \in \mathbb{F}_2[x],\ f_2(x) \neq 0 \right\} = \mathbb{F}_2(x) \end{aligned}$$

and clearly $\sqrt{x} \notin L^2$.

Exercice 6.
Soit $p > 0$ un nombre premier, posons $L = \mathbb{F}_p(x, y)$ et $K = \mathbb{F}_p(x^p, y^p) \subseteq L$.

1. Calculer le degré de l'extension $K \subseteq L$.
2. Calculer $\mathrm{Gal}(L/K)$.
3. Montrer que cette extension ne peut pas être générée par un seul élément.
4. Montrer que pour tout $\gamma \neq \gamma' \in K$, on a que $K(x+\gamma y) \neq K(x+\gamma' y)$. En déduire qu'il existe une infinité de sous-extensions $K \subseteq F \subseteq L$ différentes.

Solution.

1. Soit $F = \mathbb{F}_p(x, y^p)$. Calculons les degrés des extensions $K \subseteq F$ et $F \subseteq L$. Nous calculerons uniquement le degré de $K \subseteq F$, car l'autre calcul est identique.

   Montrons que le polynôme $f(t) = t^p - x^p \in K[t] = \mathbb{F}_p(x^p, y^p)[t]$ est irréductible. Si on pouvait écrire $f(t) = g(t)h(t)$ avec $g, h \in K[t]$, alors on a aussi l'égalité

$$t^p - x^p = f(t) = g(t)h(t)$$

dans $\mathbb{F}_p(x,y)$!

Or, on peut écrire $t^p - x^p = (t-x)^p$ dans $\mathbb{F}_p(x,y)[t]$ (on ne pouvait pas le faire dans $K[t]$, vu que $x \notin K$). Cela implique qu'à unité près, on a $g(t) = (t-x)^a$ et $h(t) = (t-x)^b$ avec $a+b=p$. Le coefficient constant de $(t-x)^a$ est x^a, et vu que $g(t) \in K[t]$, cela force $x^a \in K$. Le seul cas ou c'est possible est que $a=0$ ou $a=p$, i.e. $g(t) = f(t)$ ou est constant (à unité près). On a donc montré que $f(t)$ était irréductible de degré p, et donc

$$[F:K] = p.$$

Le même calcul montre que $[L:F] = p$, et donc

$$[L:K] = [L:F][F:K] = p^2.$$

2. Soit $\sigma \in \mathrm{Gal}(L/K)$, et soit $\alpha \in L$. Notons que $\alpha^p \in K$. En effet, c'est le cas pour x et y, et vu que ces deux éléments génèrent L/K et que la puissance p est un morphisme d'anneaux (on est en caractéristique p), c'est aussi le cas de tout $\alpha \in L$.

   On a donc
   $$\alpha^p = \sigma(\alpha^p) = \sigma(\alpha)^p,$$
   ou la première égalité vient que $\alpha^p \in K$ et $\sigma|_K = id_K$.

   On a donc
   $$(\sigma(\alpha) - \alpha)^p = \sigma(\alpha)^p - \alpha^p = 0,$$
   donc on a forcément que $\sigma(\alpha) = \alpha$. On a donc montré que $\sigma = id$, et donc
   $$\mathrm{Gal}(L/K) = \{id\}.$$

3. Supposons que L/K soit générée par un élément, disons β. Vu que $\beta^p \in K$ (cf plus haut), on déduit que β satisfait l'équation algébrique $t^p - \beta^p \in K[t]$. Soit m le polynôme minimal de β sur K. Alors automatiquement m divise $t^p - \beta^p$, et on a donc
   $$p^2 = [L:K] = [K(\beta):K] = \deg(m) \leq \deg(t^p - \beta^p) = p,$$
   ce qui est une contradiction.

4. Pour tout $\gamma \in K$, considérons l'extension intermédiaire
   $$F_\gamma := K(x + \gamma y) \subseteq L.$$
   Montrons que pour $\gamma \neq \gamma'$, on a $F_\gamma \neq F_{\gamma'}$. Cela conclura la preuve, car K est infini.

   Soient $\gamma \neq \gamma' \in K$, et supposons par l'absurde que $F_\gamma = F_{\gamma'}$. Notons F ce corps. Alors par construction, on a que
   $$\begin{cases} x + \gamma y \in F \\ x + \gamma' y \in F. \end{cases}$$
   On peut alors sousraire et obtenir que
   $$(\gamma - \gamma')y \in F.$$
   Comme $\gamma \neq \gamma'$ et que K est un corps, on peut diviser et déduire que
   $$y \in F.$$
   Or si $x + \gamma y \in F$ et $y \in F$, on a donc que $x \in F$. Vu que $x, y \in F$, on déduit alors que $F = L$. Or, F est généré par un élément, ce qui contredit le point précédent.

Remarque. Le théorème principal de la théorie de Galois montre en particulier que si $K \subseteq L$ est une extension Galoisienne, alors il y a un nombre fini de sous-extensions $K \subseteq F \subseteq L$. L'exercice ci-dessus montre que cette conséquence est fausse dans le cas inséparable. Le troisième point montre aussi que le théorème de l'élément primitif est faux dans le cas inséparable.