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

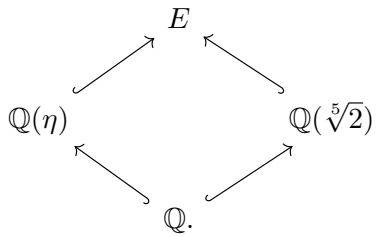
Les exercices marqués d'une étoile ($\star$) sont optionnels.

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.

Solution. Soit $\eta = e^{2i\pi/5}$.

1. On peut poser $E = \mathbb{Q}(\sqrt[5]{2}, \eta)$, et on a ainsi un diagramme d'extensions



   Vu que $[\mathbb{Q}(\eta) : \mathbb{Q}] = 4$ (c.f. exercice 4 de la série 13), on a que 4 divise $[E, \mathbb{Q}]$. Similairement, vu que $[\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 5$ (le polynôme $x^5 - 2$ est irréductible par Gauss et Eisenstein), on a que 5 divise $[E : \mathbb{Q}]$.

   D'un autre côté, $[E : \mathbb{Q}] = [E : \mathbb{Q}(\eta)][\mathbb{Q}(\eta) : \mathbb{Q}] = [E : \mathbb{Q}(\eta)]4$. Vu que $[E : \mathbb{Q}(\eta)] = [\mathbb{Q}(\eta)(\sqrt[5]{2}) : \mathbb{Q}(\eta)] \leq 5$ ($m_{\sqrt[5]{2}, \mathbb{Q}(\eta)}$ divise $x^5 - 2$), on a que $[E : \mathbb{Q}] \leq 20$. On a donc égalité.

2. Comme $E/\mathbb{Q}$ est Galoisienne, on sait que $E/\mathbb{Q}(\eta)$ est aussi Galoisienne (et elle est de degré 5 par le point précédent).

   Ainsi, $x^5 - 2$ est bien le polynôme irréductible de $\sqrt[5]{2}$ sur $\mathbb{Q}(\eta)$ (il a le bon degré), et donc vu que $\sqrt[5]{2}$ et $\eta\sqrt[5]{2}$ sont des racines, on sait alors qu'il existe $\sigma \in \mathrm{Gal}(E/\mathbb{Q}(\eta)) \subseteq \mathrm{Gal}(E/\mathbb{Q})$ envoyant $\sqrt[5]{2}$ sur $\eta\sqrt[5]{2}$. Vu que σ est automatiquement d'ordre 5, on en déduit que
$$\mathrm{Gal}(E/\mathbb{Q}(\eta)) = \langle\sigma\rangle \cong \mathbb{Z}/5\mathbb{Z}.$$

Le même argument qu'avant montre que $x^4+x^3+x^2+x+1 = \frac{x^5-1}{x-1}$ est le polynôme minimal de η sur $\mathbb{Q}(\sqrt[5]{2})$. Vu que η et η^2 sont des racines de ce polynômes, il existe $\tau \in \mathrm{Gal}(E/\mathbb{Q}(\sqrt[5]{2}))$ envoyant η sur η^2. Vu que η est une racine primitive 5eme de l'unité, on en déduit que τ est d'ordre 4. Comme

$$[E : \mathbb{Q}(\sqrt[5]{2})] = 4,$$

on en déduit que

$$\mathrm{Gal}(E/\mathbb{Q}(\sqrt[5]{2})) = \langle \tau \rangle \cong \mathbb{Z}/4\mathbb{Z}.$$

Soit $H := \langle \sigma \rangle$ et $K = \langle \tau \rangle$. Vu que $H \cap K = \{id\}$ (son ordre divise 4 et 5), et que H est normal dans $\mathrm{Gal}(E/\mathbb{Q})$ (l'extension associée, i.e. $\mathbb{Q}(\eta)$, est le corps de décomposition de $x^4+x^3+x^2+x+1$), on en déduit que $HK = \mathrm{Gal}(E/\mathbb{Q})$ et que

$$\mathrm{Gal}(E/\mathbb{Q}) \cong H \rtimes_\phi K,$$

où le morphisme associé $K \to \mathrm{Aut}(H)$ est donné par la conjugaison.

Vu que $\tau\sigma\tau^{-1} = \sigma^2$ (cela se calcule explicitement en étudiant leur action sur les racines de x^5-2), on en déduit qu'à travers les isomorphismes $H \cong \mathbb{Z}/5\mathbb{Z}$ et $K \cong \mathbb{Z}/4\mathbb{Z}$ donnés auparavant, le morphisme $f\colon \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$ envoie 1 (i.e. τ) sur le morphisme $\mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ donné par $(\cdot 2)$, vu qu'il envoie le générateur σ sur σ^2. On a donc

$$\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \rtimes_f \mathbb{Z}/4\mathbb{Z}$$

avec f explicité juste avant.

3. (a) Comme tous les 5-Sylow sont conjugés, et que l'un d'entre eux est normal, on conclut.
   (b) Un groupe d'ordre 10 possède un élément d'ordre 5 car 5 est premier (en utilisant le "théorème de Cayley"). Comme H_5 est le seul-sous groupe d'ordre 5, il suit que $H_5 \subset H$. Comme $\mathrm{Gal}(E/\mathbb{Q})/H_5 \cong \mathbb{Z}/4\mathbb{Z}$ et que ce dernier a un unique sous-groupe normal d'ordre 2, on déduit que H_{10} est l'unique sous-groupe normal d'ordre 10 de $\mathrm{Gal}(E/\mathbb{Q})$. Notons que comme H_{10} est d'indice 2, tout carré de $\mathrm{Gal}(E/\mathbb{Q})$ est dans H_{10}. Dès lors, $\langle \sigma, \tau^2 \rangle \subset H_{10}$. Mais on sait aussi que

   $$\sigma^5 = (\tau^2)^2 = e \quad \sigma\tau^2\sigma^{-1} = \tau^{-2}.$$

   On reconnaît alors la présentation de D_{10}, ce qui conclut.
   (c) S'il y avait un sous-groupe normal d'ordre 4, disons K_4, alors $\mathrm{Gal}(E/\mathbb{Q}) \cong H \times K$, et serait donc abélien, une contradiction. Similairement, s'il y avait un sous-groupe normal d'ordre 2, disons K_2, alors $H_{10} \cong H \times K_2$, et serait donc abélien, une contradiction.

4. Par le point précédent, comme les sous-groupes de $\mathrm{Gal}(E/\mathbb{Q})$ sont d'ordre 2,4,5, ou 10, on conclut que $\mathrm{Gal}(E/\mathbb{Q})$ a exactement quatres sous-groupes normaux

   $$\{e\}, \quad H_5, \quad H_{10}, \quad \mathrm{Gal}(E/\mathbb{Q}).$$

   On calcule donc des éléments primitifs pour les extensions correspondantes des trois premiers sous-groupes, le quatrième correspondant à $\mathbb{Q}$.

   (a) Le sous-groupe fixé par $H_5 = \langle \sigma \rangle$ est d'ordre 4. Par construction on a $\sigma(\eta) = \eta$ et cet élément est d'ordre 4 comme expliqué plus haut. On conclut donc que

   $$E^{H_5} = \mathbb{Q}(\eta).$$

   (b) Le sous-corps fixé par $H_{10} = \langle \sigma, \tau^2 \rangle$ est de degré 2. De plus on sait que c'est une sous-extension de $E^{H_5} = \mathbb{Q}(\eta)$ – en effet $H_5 \subset H_{10}$. Notons que comme $1, \eta, \eta^2, \eta^3, \eta^4$ est une base de $\mathbb{Q}(\eta)$, on voit que $\eta + \eta^4 = \eta + \eta^{-1}$ n'est pas dans $\mathbb{Q}$. Dès lors on conclut que

   $$E^{H_{10}} = \mathbb{Q}(\eta + \eta^{-1}).$$

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.

Solution. Soit E un corps de décomposition de f sur K. Comme f est irréductible et séparable, on sait par le cours que K/E est Galoisienne. Soit $\sigma \in \mathrm{Gal}(L/K)$, et montrons que $\sigma(\Delta) = \Delta$. Un calcul rapide montre que

$$\prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(\alpha_i - \alpha_j),$$

et vu que σ permute les racines, on voit donc que $\sigma(\Delta) = \Delta$. On a donc montré que $\Delta \in L^{\mathrm{Gal}(L/K)} = K$.

Montrons maintenant l'équivalent de l'exercice. Notez que vu que $\delta^2 = \Delta$ et que les seules racines carrées de Δ sont $\pm\delta$, on a que Δ est un carré dans K si et seulement si $\delta \in K$. Comme L/K est Galoisienne, on en Δ est un carré dans K si et seulement si pour tout $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(\delta) = \delta$.

Considérons ϕ: $\mathrm{Gal}(L/K) \to S_n$ le morphisme correspondant à l'action sur les racines de f. On montre à la main que

$$\sigma(\delta) = \sigma\left(\prod_{i<j}(\alpha_i - \alpha_j)\right) = (-1)^{\mathrm{sgn}(\phi(\sigma))} \prod_{i<j}(\alpha_i - \alpha_j) = (-1)^{\mathrm{sgn}(\phi(\sigma))}\delta,$$

donc vu qu'on est en caractéristique différent de 2 et que $\delta \neq 0$ (f est séparable), on en déduit que $\sigma(\delta) = \delta$ si et seulement si $\mathrm{sgn}(\phi(\sigma)) = 1$, i.e. $\phi(\sigma) \in A_n$.

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 $\mathrm{Gal}(K_2/\mathbb{Q}) \cong S_3$.

Solution.

1. Si Δ n'est pas un carré, alors on sait par l'exercice précédent que l'image de l'inclusion $\mathrm{Gal}(E/\mathbb{Q}) \to S_3$ n'est pas dans A_3. Comme

$$|\mathrm{Gal}(E/\mathbb{Q})| = [E:\mathbb{Q}] \geq 3,$$

et que A_3 est l'unique sous-group d'ordre 3 de S_3, on en déduit que l'injection $\mathrm{Gal}(E/\mathbb{Q}) \to S_3$ est automatiquement surjective.

De même, si Δ est un carré, alors l'image de l'injection $\mathrm{Gal}(E/\mathbb{Q}) \to S_3$ est incluse dans $A_3 \cong \mathbb{Z}/3\mathbb{Z}$. Vu que $|\mathrm{Gal}(E/\mathbb{Q})| \geq 3$, cette injection est automatiquement surjective.

2. En utilisant que $f(x) = x^3 + ax + b = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, on a que

$$\begin{cases} -\alpha_1\alpha_2\alpha_3 = b \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = a \\ \alpha_1 + \alpha_2 + \alpha_3 = 0. \end{cases}$$

Calculons maintenant Δ. On a $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, et donc $f'(x) = (x-\alpha_1)(x-\alpha_2) + (x-\alpha_1)(x-\alpha_3) + (x-\alpha_2)(x-\alpha_3)$. Ainsi,

$$f'(\alpha_1)f'(\alpha_2)f'(\alpha_3) = (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)(\alpha_3-\alpha_2)(\alpha_3-\alpha_1) = -\Delta,$$

donc on a bien l'égalité énoncée dans l'indice.

Comme $f'(x) = 3x^2 + 1$, on a que

$$\begin{aligned} -\Delta &= (3\alpha_1^2 + a)(3\alpha_2^2 + a)(3\alpha_3^2 + a) \\ &= 27(\alpha_1\alpha_2\alpha_3)^2 + 3a^2(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + 9a(\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2) + a^3. \end{aligned}$$

Par la première équation, $(\alpha_1\alpha_2\alpha_3)^2 = b^2$. Par les 2e et 3e équations, on a que

$$0 = (\alpha_1 + \alpha_2 + \alpha_3)^2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + 2a,$$

et donc

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = -2a.$$

Enfin, on a que

$$\begin{aligned} a^2 &= (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)^2 \\ &= \alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2 + \alpha_1\alpha_2\alpha_3(\alpha_1 + \alpha_2 + \alpha_3) \\ &= \alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2. \end{aligned}$$

Ainsi, on en déduit que

$$\begin{aligned} -\Delta &= (3\alpha_1^2 + a)(3\alpha_2^2 + a)(3\alpha_3^2 + a) \\ &= 27(\alpha_1\alpha_2\alpha_3)^2 + 3a^2(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + 9a(\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2) + a^3 \\ &= 27b^2 - 6a^3 + 9a^3 + a^3 = 27b^2 + 4a^3. \end{aligned}$$

3. Pour trouver K_1 (resp. K_2), il faut trouver un polynôme $f = x^3 + ax + b$ irréductible sur $\mathbb{Q}$, ayant trois racines réelles, tel que Δ est un carré (resp. n'est pas un carré). En effet, le premier point conclura en prenant un corps de décomposition de f dans $\mathbb{R}$.

Pour trouver un tel polynôme ayant trois racines réelles, on utilise une technique ancestrale : WolphramAlpha.

En jouant un peu, on se rend compte que $f = x^3 - 3x - 1$ a bien trois racines réelles. Montrons qu'il est irréductible. Par Gauss, il suffit de montrer que c'est vrai sur $\mathbb{Z}$, et par un lemme de cours il suffit de le montrer sur $\mathbb{F}_2$. Comme ce polynôme est d'ordre 3 et n'a pas de racine sur $\mathbb{F}_2$, il est donc bien irréductible. On a par le point précédent que $\Delta = -(4 \cdot (-3)^3 + 27) = 3 \cdot 27 = 3^4$, qui est bien un carré. On a donc trouvé une extension réelle $\mathbb{Z}/3\mathbb{Z}$–Galoisienne.

En jouant encore plus, on se rend compte que $f = x^3 - 4x - 1$ a aussi trois racines réelles. Par le même argument que juste avant, cela est une conséquence du fait qu'il n'ait pas de racine sur $\mathbb{F}_3$. Comme $\Delta = -(4 \cdot (-4)^3 + 27) = 4^4 - 27 = 229$ est premier, il ne peut pas être un carré, et donc on a trouvé une extension réelle S_3–Galoisienne.

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

Solution.

1. Le polynôme caractéristique de A est un polynôme qui annule a par Cayley-Hamilton. Mais il est de degré $[K(a)\colon K]$. Comme le coefficient dominant du polynôme caractéristique avec la coefficient choisie est 1, on conclut.
2. Notons A_E pour la matrice multiplication par a vue comme application K-linéaire sur E. Notons qu'on peut identifier le polynôme minimal de A_E en tant qu'application linéaire (le polynôme avec coefficient dominant 1 de plus petit degré qui annule ϕ_E) au polynôme minimal de $m_{a,K}$. Comme on suppose $m_{a,K}$ séparable et E étant son corps de décomposition, on en déduit que le polynôme minimal en tant qu'application linéaire de ϕ_E est scindé à racines simples, ce qui conclut comme en exercice 2 de la série 13.
3. Notons p la caractéristique finie du corps et q la puissance de p minimale telle que $a^q \in K$. Rappelons que dans ce cas la seule racine du polynôme minimal de a^q est a et que ce polynôme minimal est $x^q - a$. On en déduit qu'au signe près le polynôme caractéristique de de A est $x^q - a$. Mais notons que la seule valeur propre sur $K(a)$ de A est a – ce qui conclut.
4. Suit de l'identification du polynôme caractéristique $\det(x\,\mathrm{id} - A) = \phi(x) = m_{a,K}(X)$.
5. On rappelle que dans ce cas, les racines de $m_{a,K}$ sont les conjugués $(g(a))_{g \in \mathrm{Gal}(L|K)}$. Mais alors comme,
$$m_{a,K}(0) = (-1)^{\deg(m_{a,K})} \prod_{g \in \mathrm{Gal}(L|K)} g(a)$$
on conclut par le point précédent et $\deg(m_{a,K}) = [L\colon K]$.

6. Notons $\xi = e^{2\pi i/3}$. La matrice de multiplication par $\xi + \sqrt[2]{2}$ élément dans la base de L suivante

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

est (on utilise $\xi^2 = -1 - \xi$)

$$\begin{pmatrix} 0 & -1 & 0 & 0 & 2 & 0 \\ 1 & -1 & 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 1 & -1 \end{pmatrix}$$

puis on calcule le polynôme caractéristique de cette matrice pour conclure que le polynôme suivant

$$x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9$$

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.

Solution. Let $\alpha \in E$. Then, we have $L \subseteq L(\alpha) \subseteq E$, where the extension $L \subseteq L(\alpha)$ is finite and separable. Now, let $m_{\alpha,L}(x) = \sum_{i=1}^{r} a_i x^i \in L[x]$. Then we have the tower of extensions $K \subseteq K(a_1, \ldots, a_r) \subseteq K(a_1, \ldots, a_r, \alpha) \subseteq L(\alpha)$ where $K \subseteq K(a_1, \ldots, a_r)$ and $K(a_1, \ldots, a_r) \subseteq K(a_1, \ldots, a_r, \alpha)$ are finite and separable. Moreover, we note that $m_{\alpha,L}(x) \in K(a_1, \ldots, a_r)[x]$.

Set F to be the splitting field of $\prod_{i=1}^{r} m_{a_i,K}(x)$ over K. Then $[F : K]$ is finite and F is generated, over K, by the roots of $m_{a_i,K}$ for all $1 \leq i \leq r$. As a_i is separable over K for all $1 \leq i \leq r$, then so are all the other roots of $m_{a_i,K}$ and we deduce that the extension $K \subseteq F$ is separable. Hence, it is Galois. Moreover, we note that $K(a_1, \ldots, a_r) \subseteq F$.

Set G be the splitting field of $m_{\alpha,L}(x)$ over F. Then $[G : F]$ is finite and G is generated, over F, by the roots of the polynomial $m_{\alpha,L}(x)$, see Lemma 4.3.3. As $\alpha \in K(a_1, \ldots, a_r, \alpha)$ is separable over $K(a_1, \ldots, a_r)$, we have that α is separable over F, since $m_{\alpha,F} | m_{\alpha,K(a_1,\ldots,a_r)}$. Therefore, the extension $F \subseteq G$ is Galois and finite. Moreover, we have that $K(a_1, \ldots, a_r, \alpha) \subseteq G$. We have built the following extension diagram:

$$\begin{array}{ccccccc} K & \hookrightarrow & K(a_1, \ldots, a_r) & \hookrightarrow & K(a_1, \ldots, a_r, \alpha) & & \\ & & \downarrow & & \downarrow & & \\ K & \hookrightarrow & F & \hookrightarrow & G & \hookrightarrow & H \end{array}$$

where $K \subseteq H$ is a Galois extension, see item 1. Therefore, H is separable over K, hence, in particular, we have that $K(a_1, \ldots, a_r, \alpha)$ is separable over K. We have shown that all $\alpha \in E$ are separable over K and we conclude that E is separable over K.

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.

Solution.

(a)(i) Let $\alpha \in L \backslash K$. As $\alpha^2 \in K$, it follows that α is a root of the polynomial $x^2 + \alpha^2 \in K[x]$ and thus $[K(\alpha) : K] \leq 2$. On the other hand, we have that $[K(\alpha) : K] \geq 2$, as $\alpha \notin K$, and we conclude that $[K(\alpha) : K] = 2$ and $K(\alpha) = L$.

(ii) The polynomial $x^2 + \alpha^2 \in K[x]$, where $\alpha \in L \backslash K$, admits α as a double root, hence it is irreducible in $K[x]$. Now, as this is a unitary irreducible polynomial of degree 2 and as $\alpha \notin K$, it follows that $m_{\alpha,K}(x) = x^2 + \alpha^2$ and so we conclude that $\alpha \in L \backslash K$ is inseparable.

(b)(i) Let $\alpha \in L \backslash K$ be such that $\alpha^2 \notin K$. First, we have that $[K(\alpha) : K] \geq 2$ and, as $K(\alpha) \subseteq L$, it follows that $[K(\alpha) : K] \leq [L : K] = 2$, and so $[K(\alpha) : K] = 2$, hence $K(\alpha) = L$.

Secondly, as $\alpha^2 \in K(\alpha)$ and $\alpha^2 \notin K$, there exist $a, b \in K$, $a \neq 0$, such that $\alpha^2 = a\alpha + b$. Then:

$$\left(\frac{\alpha}{a}\right)^2 = \left(\frac{\alpha}{a}\right) + \frac{b}{a^2}.$$

Set $\beta = \frac{\alpha}{a} \in K(\alpha)$ and $c = \frac{b}{a^2} \in K$. We have that $K(\alpha) = K(\frac{\alpha}{a}) = K(\beta)$ and so $L = K(\beta)$. Moreover, β is a root of the unitary polynomial $x^2 + x + c \in K[x]$ and, as $[K(\beta) : K] = 2$, we conclude that $m_{\beta,K}(x) = x^2 + x + c$.

(ii) Note that a polynomial of the form $x^2 + x + c$ is always separable as the derivative is $1 \neq 0$. So, β is automatically separable. Now $\beta + 1 \in K(\beta)$ is a root of $m_{\beta,K}(x)$, as $(\beta+1)^2 + (\beta+1) + c = \beta^2 + \beta + c = 0$, and we conclude that $\tau : K(\beta) \to K(\beta)$ given by $\tau(\beta) = \beta + 1$ is an automorphism of $K(\beta)$. Then, by Proposition 4.6.3.4 we have that $|\mathrm{Gal}(K(\beta)/K)| = 2$.

(iii) Note that $K(\beta)^{\langle\tau\rangle} = K$ by theorem 4.6.13. If $\gamma \in L \setminus K$ then $\tau(\gamma) \neq \gamma$ and by proposition 4.6.3.(3), we get that the minimal polynomial of γ is $(t - \gamma)(t - \tau(\gamma))$. Therefore $K \subset L$ is separable.

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

Solution. Let K be a countable field and consider the polynomial ring $K[x]$. For all $i \geq 0$ define the subsets $K^i[x] \subseteq K[x]$ with $K^i[x] = \{f \in K[x] | \deg(f) = i\}$. We remark that $K[x] = \bigcup_{i \geq 0} K^i[x]$ and that $K^i[x] \cong K^i$, hence $|K^i[x]| = i \cdot |K| = |K|$, for all $i \geq 0$. It follows that $|K[x]| = \aleph_0 \cdot |K| = \aleph_0$ and so $K[x]$ is also countable.

We define the map $\phi : \overline{K} \to K[x]$ by $\phi(\alpha) = m_{\alpha,K}$. Now the subset $\phi(\overline{K})$ of $K[x]$ contains all polynomials of the form $x - \alpha$, where $\alpha \in K$, hence $\phi(\overline{K})$ is also countable. Lastly, for any $m_{\alpha,K} \in \phi(\overline{K})$ we have that the preimage $\phi^{-1}(m_{\alpha,K})$ is non-empty and finite, as $\alpha \in \phi^{-1}(m_{\alpha,K})$ and $m_{\alpha,K}$ admits a finite number of roots. We conclude that $\overline{K}$ has the same cardinality as $\phi(\overline{K})$, hence it is countable.

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 4.2.22, 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.)

Solution.

1. We know that for every j teh field K_{j+1} contains a subfield isomorphic to K_j because by construction $m_j \mid m_{j+1}$. We can then considered the induced inclusion homomorphism $\iota_j : K_j \to K_{j+1}$ for every $j \geq 1$.

2. Recall that if $K_0 \overset{\iota_0}{\hookrightarrow} K_1 \overset{\iota_1}{\hookrightarrow} K_2 \overset{\iota_2}{\hookrightarrow} \dots$ is an infinite sequence of fields with injectiv homomorphisms between each K_j and K_{j+1}. Then the direct colimit is given by

$$\varinjlim_i K_i = \bigsqcup_{i\in\mathbb{N}} K_i \Big/ \begin{array}{l} \text{- } x \equiv \iota_{s-1} \circ \dots \circ \iota_r(x) \text{ et } \iota_{s-1} \circ \dots \circ \iota_r(x) \equiv x \text{ pour chaque entier } \\ \quad s > r, \text{ et } x \in K_r \\ \text{- } x \equiv x \text{ pour chaque } x \in K_r \end{array}$$

   is a field with sum given by $[x] + [y]$ and product given by $[x] \cdot [y]$ for $x \in K_r$ and $y \in K_s$ are defined as follows: if $s > r$, then $[x] = [\iota_{s-1} \circ \dots \circ \iota_r(x)]$ which means that we can suppose $s = r$, and thus we define

   (a) $[x] + [y] = [x + y]$
   (b) $[x] \cdot [y] = [x \cdot y]$

   It is clear that the unit and zero element are given by the inclusion of each the zero and unit element in each field. And since each K_i is a field the sum and multiplication defined as above endow the direct colimit with a ring structure. It is also not difficult to see that each element $[x] \in \bigsqcup_{i\in\mathbb{N}} K_i$ has an inverse, since $x \in K_n$ for some $n \in \mathbb{N}$

   Moreover the inclusion $K_0 \hookrightarrow \bigsqcup_{i\in\mathbb{N}} K_i$ gives us an embedding $K_0 \hookrightarrow \varinjlim_i K_i$.

3. Note that $\mathbb{F}_p \subset K$. Moreover each extension $K_j \subset K_{j+1}$ is a finite extension therefore it is an algebraic extension. Thus we have that each K_j is algebraic over $\mathbb{F}_p$. We then have that K is algebraic over $\mathbb{F}_p$ because each of its element lives in one of the K_j.

4. Let g be a polynomial in $K[t]$. Since g has a finite sum of coefficients, then there exists $n \in \mathbb{N}$ such that $g \in K_n[t]$. Let α be a root of g, then $K_n \subset K_n(\alpha)$ is a finite extension of degree r, for some $r \in \mathbb{N}$. Therefore $K_n(\alpha)$ is a field with p^{rn} elements. Hence $K_n(\alpha)$ is also a finite field containing F_p. Then we have that $K_n(\alpha) = K_{rn}$. So the root α is also an element of K since $\alpha \in K_{rn} \subset K$. Thus K is the algebraic closure of $\mathbb{F}_p$.

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

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

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

Solution.

1. As $K \subseteq L$ is a purely inseparable extension, it follows that $\alpha \in L \backslash K$ is purely inseparable over K, thus there exists $n \geq 1$ such that $\alpha^{p^n} \in K$. We fix such an $\alpha \in L \backslash K$ and we let $\sigma \in \mathrm{Gal}(L/K)$. It suffices to show that $\sigma(\alpha) = \alpha$.

   The element $\alpha \in L/K$ is the unique p^nth root of α^{p^n}, see Exercise 2.(a) of Series 11. Therefore, it suffices to show that $(\sigma(\alpha))^{p^n} = \alpha^{p^n}$. We have:

   $$(\sigma(\alpha))^{p^n} = \sigma(\alpha^{p^n}) = \alpha^{p^n}.$$

   We conclude that $\mathrm{Gal}(L/K) = \{\mathrm{Id}_L\}$.

2. First, we will show that $L_{insep,K} \subseteq L^{\mathrm{Gal}(L/K)}$. For this, let $\alpha \in L_{insep,K}$ and let $\sigma \in \mathrm{Gal}(L/K)$. As $\alpha \in L_{insep,K}$, there exists $n \in \mathbb{Z}_{\geq 0}$ such that $\alpha^{p^n} \in K$. Then:

   $$\sigma(\alpha)^{p^n} = \sigma(\alpha^{p^n}) = \alpha^{p^n} \in K$$

   and it follows that $\sigma(\alpha) \in L_{insep,K}$. Hence the restriction $\sigma|_{L_{insep,K}}$ is a K-automorphism of $L_{insep,K}$ and thus $\sigma|_{L_{insep,K}} = \mathrm{Id}_{L_{insep,K}}$, see item 1. Therefore $\sigma(\alpha) = \sigma|_{L_{insep,K}}(\alpha) = \alpha$ for all $\alpha \in L_{insep,K}$ and thus $L_{insep,K} \subseteq L^{\mathrm{Gal}(L/K)}$.

   We now consider the extension tower:

   $$K \subseteq L_{insep,K} \subseteq L^{\mathrm{Gal}(L/K)} \subseteq L.$$

   We have that $[L : K] = [L : L_{insep,K}][L_{insep,K} : K]$, hence $[L : L_{insep,K}] = |\mathrm{Gal}(L/K)|$.On the other hand, we have $[L : L^{\mathrm{Gal}(L/K)}] = |\mathrm{Gal}(L/K)|$, see Theorem 4.6.12, and we deduce that $[L^{\mathrm{Gal}(L/K)} : L_{insep,K}] = 1$, hence $L^{\mathrm{Gal}(L/K)} = L_{insep,K}$. Lastly, the extension $L^{\mathrm{Gal}(L/K)} \subseteq L$ is separable, see Proposition 4.6.10, and we conclude that $L_{insep,K} \subseteq L$ is separable.