EPFL - Printemps 2025	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Solutions 13	

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

Exercice 1 (Correspondance de Galois)**.**
Calculez les groupes de Galois $\mathrm{Gal}(E/\mathbb{Q})$ puis exprimez tous les sous-corps intermédiaires avec leur sous-groupe correspondant ainsi que des éléments primitifs* et polynôme minimaux pour ceux-ci des extensions Galoisiennes E de $\mathbb{Q}$ donnés par

1. le corps de décomposition de x^3-2 dans $\mathbb{C}$,
2. le corps de décomposition de x^4-2 dans $\mathbb{C}$.

Utilisez ce que vous savez déjà grâce aux exercices *Série 10 exercice 3* et *Série 11 exercice 2.*

Solution.

1. On a déjà calculé que $E=\mathbb{Q}(\xi,\sqrt[3]{2})$ et que $\mathrm{Gal}(E/\mathbb{Q})\cong S_3$. Notons r un élément d'ordre 3 et s un élément d'ordre 2 de sorte que $\langle r,s\rangle=\mathrm{Gal}(E/\mathbb{Q})$, avec

   (a) $r(\xi)=\xi$, $r(\sqrt[3]{2})=\xi\sqrt[3]{2}$.
   (b) $s(\sqrt[3]{2})=\sqrt[3]{2}$, $s(\xi)=\xi^2$.

   Les sous-groupes de $\mathrm{Gal}(E/\mathbb{Q})$ sont les suivants (regroupés par classe de conjugaison, avec leur ordre en titre de colonne)

   1 2 3 6

   $$\{e\} \longrightarrow <s>,<sr>,<sr^2> \longrightarrow \mathrm{Gal}(E/\mathbb{Q}), \quad <r> \nearrow \searrow \mathrm{Gal}(E/\mathbb{Q})$$

   Comme ξ est de degré 2, on voit que $\mathbb{Q}(\xi)$ est le sous-corps fixé par $<r>$. Comme $\sqrt[3]{2}$ est de degré 3, on voit que $\mathbb{Q}(\sqrt[3]{2})$ est le sous-corps fixé par $<s>$.

   Notons également que $sr=rsr^{-1}$ et que $sr^2=r^2sr^{-2}$. Ainsi comme les conjugués correspondent à l'image par l'élément de l'extension on obtient que les sous-corps fixés par $<sr>$ et $<sr^2>$ sont respectivement $\mathbb{Q}(\xi\sqrt[3]{2})$ et $\mathbb{Q}(\xi^2\sqrt[3]{2})$. On résume cela en imitant en miroir le tableau des sous-groupes ci-dessus, le nombre de la colonne correspondant maintenant au degré.

   6 3 2 1

   $$\mathbb{Q}(\xi,\sqrt[3]{2}) \longrightarrow \mathbb{Q}(\sqrt[3]{2}),\mathbb{Q}(\xi\sqrt[3]{2}),\mathbb{Q}(\xi^2\sqrt[3]{2}) \longrightarrow \mathbb{Q}, \quad \mathbb{Q}(\xi) \nearrow \searrow \mathbb{Q}$$

   En ce qui est des éléments primitifs, ils sont tous déjà donnés sauf $\xi+\sqrt[3]{2}$ pour l'extension E. Les polynômes minimaux de ξ et $\sqrt[3]{2}$ et leurs conjugués sont x^2+x+1 et x^3+2 respectivement. Quant à $\xi+\sqrt[3]{2}$ – on pourrait multiplier les $x-\alpha$ où α sont tous les conjugés de l'élément.

*C'est à dire des générateurs sur $\mathbb{Q}$ de ces extensions intermédiaires.

C'est un peu fastidieux, alors on écrit la matrice de multiplication par cet élément dans la base de E suivante

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

c'est à dire (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

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

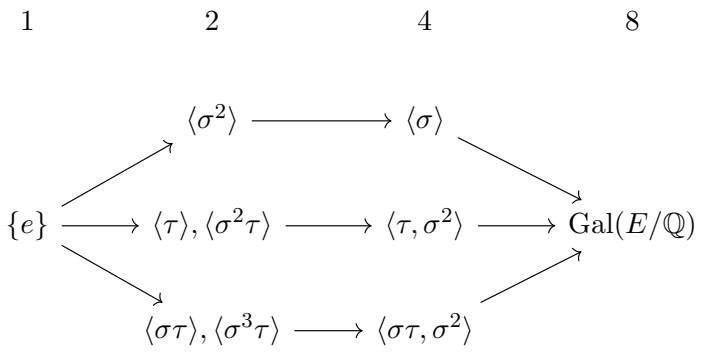
annule $\xi + \sqrt[3]{2}$ – comme il est de degré 6, c'est le polynôme minimal.

2. On a déjà calculé que $E = \mathbb{Q}(i, \sqrt[4]{2})$ et que $\mathrm{Gal}(E/\mathbb{Q}) \cong D_8$. Notons σ un élément d'ordre 4 et τ un élément d'ordre 2

   (a) $\sigma(i) = i$, $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$.
   (b) $\tau(i) = -i$, $\tau(\sqrt[4]{2}) = -\sqrt[4]{2}$.

   Notons que $\tau(-\sqrt[4]{2}) = \sqrt[4]{2}$ et $i\sqrt[4]{2}$ et $-i\sqrt[4]{2}$ sont fixés par τ. Notons aussi que $\sigma(\sqrt{2}) = -\sqrt{2}$.

   Les sous-groupes de $\mathrm{Gal}(E/\mathbb{Q})$ sont les suivants (regroupés par classe de conjugaison, avec leur ordre en titre de colonne)



   Notons que $\sqrt{2}$ est fixée par σ^2 et τ et que $i\sqrt{2}$ est fixée par σ^2 et $\sigma\tau$, et que i est fixée par σ, on a en comparant les degrés sur $\mathbb{Q}$ que

$$E^{<\sigma>} = \mathbb{Q}(i) \quad E^{\langle\tau,\sigma^2\rangle} = \mathbb{Q}(\sqrt{2}) \quad E^{\langle\sigma\tau,\sigma^2\rangle} = \mathbb{Q}(i\sqrt{2}).$$

   Comme $\mathbb{Q}(i, \sqrt{2})$ est une sous-Galois extension de de degré 4 on conclut qu'elle corresponds au seul sous-groupe normal d'ordre 2, c'est à dire

$$E^{<\sigma^2>} = \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i + \sqrt{2}).$$

   Comme $i\sqrt[4]{2}$ est fixée par τ et qu'il a degré 4, et que $\sigma^2\tau = \sigma\tau\sigma^{-1}$, on obtient que

$$E^{<\tau>} = \mathbb{Q}(i\sqrt[4]{2}) \qquad E^{<\sigma^2\tau>} = E^{\sigma<\tau>\sigma^{-1}} = \sigma(E^{<\tau>}) = \mathbb{Q}(-\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}).$$

Notons que $\sqrt[4]{2}(1-i) = \sqrt[4]{2} - i\sqrt[4]{2}$ is est fixée par $\sigma\tau$ et de degré 4 car on peut calculer son orbite par le groupe de Galois explicitement et qu'elle est de taille 4, on obtient en comparant les degrés

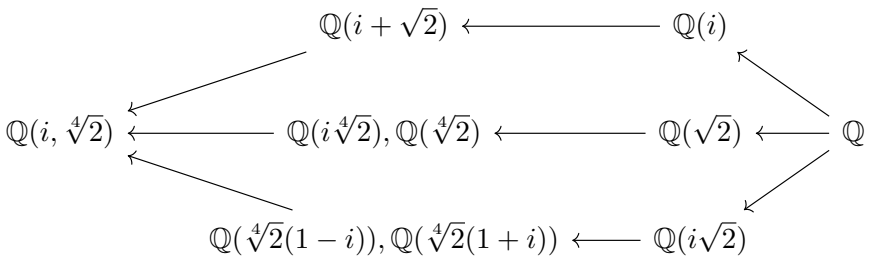
$$E^{<\sigma\tau>} = \mathbb{Q}(\sqrt[4]{2}(1-i)).$$

Maintenant en utilisant le même argument que ci-dessus on obtient finalement

$$E^{<\sigma^3\tau>} = \mathbb{Q}(\sqrt[4]{2}(1+i)).$$

On résume la correspondance obtenue en imitant en miroir le diagramme des sous-groupes ci-dessus.

8 4 2 1



En ce qui est des polynômes minimaux des éléments primitifs apparaissant ci-dessus,

(a) Les polynômes minimaux de $i, \sqrt{2}, i\sqrt{2}$ sont respectivement x^2+1, x^2-2 et x^2+2.

(b) Le polynôme minimal de $i+\sqrt{2}$ est

$$x^4 - 2x^2 + 9$$

voir la solution de l'exercice 2 de la série 11.

(c) Le polynôme minimal de $i\sqrt[4]{2}$ et $\sqrt[4]{2}$ est

$$x^4 - 2.$$

(d) Le polynôme minimal de $\sqrt[4]{2}(1-i)$ et $\sqrt[4]{2}(1+i)$ est

$$x^4 + 8.$$

Pour conclure on calcule le polynôme minimal de l'élément primitif de $i+\sqrt[4]{2}$. Pour cela on calcule le produit des $x-\alpha$ où les α sont les conjugués de $i+\sqrt[4]{2}$. On regroupe deux par deux ceux ci $i+i^k\sqrt[4]{2}$ et $-i+i^k\sqrt[4]{2}$ pour $k=0,1,2,3$. On commence par multiplier les polynômes en regroupant par paire comme ci-dessus pour obtenir les quatres polynômes de degré 2

$$x^2 + 2\sqrt[4]{2}x + \sqrt{2}, \quad x^2 - 2\sqrt[4]{2}x + \sqrt{2}, \quad x^2 + 2i\sqrt[4]{2}x - \sqrt{2}, \quad x^2 - 2i\sqrt[4]{2}x - \sqrt{2}.$$

Puis un multipliant les deux premiers puis les deux suivants, on obtient respectivement

$$x^4 - 2\sqrt{2}x^2 + 2, \quad x^4 + 2\sqrt{2}x^2 + 2.$$

Et finalement en multipliant ces deux derniers polynômes,

$$x^8 - 4x^4 + 4.$$

Exercice 2.
Fixons un entier $n > 0$. Soit K un corps de caractéristique soit 0 soit positive et première avec n.

1. Démontrez que $x^n - 1 \in K[x]$ n'admet pas de racine multiples dans son corps de décomposition sur K.

   Autrement dit il y a n racines distinctes qui sont des n-ième racines de l'unité dans les extensions de K.

   Supposons à a partir de maintenant que K contient toutes les racines n-ièmes de l'unité.

2. ($\star$) Considérons une $\mathbb{Z}/n\mathbb{Z}$-galoisienne extension $K \subseteq L$. Démontrez, que $L = K\left(\sqrt[n]{a}\right)$ pour un $a \in K$ adéquat, où $\sqrt[n]{a}$ dénote un élément dont le n-ième puissance égale à a.

   Indice: considérons un générateur ϕ du groupe de Galois en tant qu'application K-linéaire sur L. Démontrez que le polynôme minimal de ϕ en tant qu'application K linéaire est $x^n - 1$. Utilisez la décomposition en espaces propres pour trouver un vecteur propre $\alpha \in L$ avec valeur propre une n-ième racine primitive de l'unité. Démontrez après que n est l'entier minimal tel que $\alpha^n \in K$.

3. Supposons maintenant $n = p$ premier. Démontrez que si $\sqrt[p]{a}$ est une racine fixée de $a \in K \setminus K^p$ (dans un corps de décomposition adéquat), alors $L = K(\sqrt[p]{a})$ est $\mathbb{Z}/p\mathbb{Z}$ galoisienne.

   Indice: Soit ξ un p-ième racine primitve d'unité, et soit $\alpha = \sqrt[p]{a}$. Dans Lemme 4.9.1 des notes de cours on a démontré que toute les racines de $m_{\alpha,K}$ sont de forme de $\xi^j\alpha$, et que $K \subseteq L$ est galoisienne avec $\mathrm{Gal}(K/L)$ abélien. Notons aussi que puisque $a \notin K^p$, l'extension $K \subseteq L$ est non-triviale. Prenons donc un élément non-neutre $\phi \in \mathrm{Gal}(K/L)$. Démontrez que le plus petit entier $s > 0$ tel que $\phi^s(\alpha) = \alpha$ est $s = p$.

   Comme corollaire, déduisez que si $a \in K \setminus K^p$ alors le polynôme $x^p - a$ est irréductible dans $K[x]$. Donnez un contre-exemple à cet énoncé si p n'est pas premier.

4. Soit p un entier premier et soit $n > 0$ un entier positif arbitraire. Démontrez que $\mathbb{Q} \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{p^n}}\right)$ est $(\mathbb{Z}/p^n\mathbb{Z})^\times$-Galoisienne.

   Indice: Pour $n = 1$, en utilisant comme vu en cours que $x^{p-1} + x^{p-2} + \cdots + 1$ est irréductible montrez que $\mathbb{Q}(e^{\frac{2\pi i}{p}})$ est une extension de degré $p - 1$. Ensuite, utilisez le point précédent par induction pour conclure que l'extension $\mathbb{Q} \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{p^n}}\right)$ est de degré $|\,(\mathbb{Z}/p^n\mathbb{Z})^\times\,|$. Ensuite, montrez que si ϕ est dans le groupe Galois et $\xi = e^{\frac{2\pi i}{p}}$, alors $\phi(\xi) = \xi^k$ pour un $k \in \mathbb{Z}$ avec $(k, p) = 1$, ce qui donnera lieu en réduisant k modulo p^n à une injection du groupe Galois dans $(\mathbb{Z}/p^n\mathbb{Z})^\times$, ce qui permettra de conclure.

Solution.

1. Si il y avait une racine multiple de $f(x) = x^n - 1$, alors on saurait par le cours que $f(x)$ et $f'(x)$ ne serait pas premiers entre eux. Or, $f'(x) = nx^{n-1}$, qui est premier avec $f(x)$.

2. Soit ϕ un générateur de $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$.

   Notons tout d'abord que comme $\phi^n = id$ par hypothèse, le polynôme minimal de ϕ en tant application K-linéaire divise $x^n - 1$.

   Donnons deux preuves que ϕ admet une racine primitive n-ième de l'unité comme valeur propre.

   Preuve 1. Le polynôme minimal de ϕ est ainsi scindé est à racine simples, donc l'application ϕ est diagonalisable.[†]

[†]On rappelle le *lemme des noyaux* (voir fin de corrigé pour un rappel d'une preuve) qui dit que si $\phi\colon V \to V$ est un endomorphisme d'un K-espace vectoriel, $f(x) = \prod_i g_i(x)$ est une décomposition en irréductibles dans $K[t]$ et que $f(\phi) = 0$ alors $V = \bigoplus_i \ker(g_i(\phi))$. Si f est scindé à racines simples $f = \prod_i (x - \lambda_i)$, alors ϕ restreint au sous-espace correspondant est la multiplication par λ_i, ce qui démontre que ϕ est diagonalisable.

Il suffit de montrer que $x^n - 1$ est le polynôme minimal de l'application linéaire ϕ pour montrer qu"il existe une racine primitive n-ième de l'unité comme valeur propre. Pour cela, il suffit alors de montrer que tout espace propre est de dimension 1. En effet, on aura dès-lors nécessairement n valeurs propres distinctes, et donc que le degré du polynôme minimal est égal à n.

Montrons que tout espace propre est de dimension 1. Soit ξ une valeur propre, qui est nécessairement une racine de l'unité en tant que racine de $x^n - 1$. Notons d son ordre multiplicatif. Soit x un vecteur propre associé à la valeur propre ξ. On note alors que x^i est un vecteur propre associé à la valeur propre ξ^i car $\phi(x^i) = \phi(x)^i = \xi^i x^i$. Cela nous permet de déduire que

$$1, x, x^2, \ldots, x^{d-1}$$

est une base de vecteurs propres à valeurs propres distinctes du sous-espace stable par ϕ qu'est l'extension intermédiaire $K(x)$. En effet x^d étant associé à la valeur propre 1, x^d est fixé par ϕ et donc on a $x^d \in K$ et donc que $[K(x)\colon K] \leq d$. Dès-lors le fait que les valeurs propres des éléments ci-dessus soient distinctes implique leur indépendance linéaire et donc que la liste forme une base de $K(x)$ sur K. Soit x' un autre vecteur propre associé à la valeur propre ξ. Par la correspondance de Galois, il existe une *unique* sous-extension de degré d sur K, car il existe un unique sous-groupe d'ordre n/d dans $\mathbb{Z}/n\mathbb{Z}$. Cela implique donc que $K(x) = K(x')$. Mais alors il suit que x' est colinéaire à x en comparant les valeurs propres, montrant par suite notre assertion que tous les espaces propres sont 1-dimensionnels. □

Preuve 2. Supposons tout d'abord que $n = p^j$ pour un certain $j > 0$ et p premier. Soit $f(t)$ le polynôme minimal de l'application linéraire ϕ (et donc comme noté ci-dessus, $f(t)$ divise $t^{p^j} - 1$). Si par contradiction ϕ n'admettait pas de valeur propre étant une racine primitive p^j'ème de l'unité, alors ϕ devrait automatiquement diviser $t^{p^{j-1}} - 1$, vu que

$$t^{p^j} - 1 = (t^{p^{j-1}} - 1) \prod_{\alpha} (t - \alpha),$$

ou le produit se fait sur les racine primitives p^j'ème de l'unité α.

Comme le polynôme minimal annule ϕ, on aurait que $\phi^{p^{j-1}} = id$, ce qui contredit l'hypothèse sur l'ordre de ϕ. Ainsi, on est bon dans ce cas.

Soit maintenant n général, et écrivons $n = p_1^{j_1} \ldots p_s^{j_s}$. Pour tout $1 \leq r \leq s$, on sait par le théorème fondamental de la théorie de Galois qu'il existe une (unique) sous-extension Galoisienne F_r de L de groupe de Galois $\mathbb{Z}/p_j^{r_j}\mathbb{Z}$ (la sous-extension est Galoisienne, car on est dans un groupe abélien, donc tous les sous-groupes sont normaux). Comme F_r/K est Galoisienne, on sait par le cours que ϕ fixe F_r. De plus, la restriction de ϕ à F_r correspond à une surjection $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p_r^{j_r}\mathbb{Z}$, donc l'image de ϕ doit être une générateur de $\mathrm{Gal}(F_r/K)$. En particulier, $\phi|_{F_r}$ est d'ordre $p_j^{j_r}$. Ainsi, on sait par le cas précédent que $\phi|_{F_r}$ admet un vecteur propre $a_r \in F_r$ de valeur propre λ_r une racine primitive $p_r^{j_r}$ de l'unité.

Il est direct de vérifier que $a_1 \ldots a_s$ est alors aussi un vecteur propre, de valeur propre une racine primitive n-ième de l'unité. □

Soit alors x un vecteur propre associé à une racine *primitive* n-ième de l'unité. On voit alors en suivant le même raisonnement que dans la première preuve que $L = K(x)$ avec une base de vecteurs propre pour ϕ

$$1, x, x^2, \ldots, x^{n-1}$$

et que $a = x^n$ satisfait à l'énoncé.

3. Notons que L est Galoisienne car le polynôme minimal du générateur de l'extension est scindé et séparable. Il suffit de montrer que l'ordre de l'extension est p car la seule classe d'isomorphisme de groupe d'ordre p est celle de $\mathbb{Z}/p\mathbb{Z}$. Soit ϕ non trivial dans le groupe de

Galois. Notons que $\phi(\alpha) = \xi\alpha$ pour ξ une racine primitive p-ième de l'unité car ϕ permute les racines du polynôme minimal. Mais alors $\phi^s(\alpha) = \xi^s\alpha$ et donc le premier minimal tel que $\phi^s(\alpha) = \alpha$ est p, ce qui démontre l'assertion.

Démontrons le corollaire. Nous voyons par ci-dessus que $K(\sqrt[p]{a})$ est de degré p sur K. Comme $x^p - a$ annule le générateur de cette extension, il en suit que c'est le polynôme minimal de ce dernier, concluant. Un contre exemple pour n pas premier: Dans $K = \mathbb{Q}(i, \sqrt{2})$, il n'y a pas de racine quatrième de 2 (voir. premier exercice) et

$$x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2}).$$

qui n'est donc pas irréductible.

4. Comme $x^{p-1} + \cdots + x + 1$ est irréductible par un exemple du cours, on voit que

$$\mathbb{Q} \subset \mathbb{Q}(e^{\frac{2\pi i}{p}})$$

est de degré $p-1$. Maintenant, par le point précédent, on voit que $\mathbb{Q}\left(e^{\frac{2\pi i}{p^j}}\right) \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{p^{j+1}}}\right)$ pour $1 \leq j \leq n-1$ sont de degré p. Dès lors, on voit que

$$\mathbb{Q} \subset \mathbb{Q}(e^{\frac{2\pi i}{p^n}})$$

est de degré $p^n - p^{n-1} = p^{n-1}(p-1) = |\,(\mathbb{Z}/p^n\mathbb{Z})^\times\,|$. Notons G le groupe de Galois et prenons $\phi \in G$. Notons $j(\phi) \in \mathbb{Z}$ un entier tel que $\phi(e^{\frac{2\pi i}{p^n}}) = e^{\frac{2\pi i j(\phi)}{p^n}}$. Notons que $(j(\phi), p) = 1$ car cette dernière racine est nécessairement primitive, en tant qu'image par un automorphisme d'une racine primitive. Ainsi, on voit que $G \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ qui envoie $\phi \mapsto \phi(j) \mod n$ est un morphisme de groupe bien défini. Comme un automorphisme est entièrement déterminé par sa valeur en $e^{\frac{2\pi i}{p^n}}$, on conclut que ce morphisme est injectif, et donc un isomorphisme par cardinalité.

Preuve du lemme des noyaux. Dans le point 2 de l'exercice ci-dessus on fait appel à un petit lemme d'algèbre linéaire qui suit du résultat suivant. *Soit $\phi\colon V \to V$ un endomorphisme d'un K-espace vectoriel et $f, g \in K[t]$ deux polynômes tels que $(f, g) = 1$. Alors*

$$\ker(fg(\phi)) = \ker(f(\phi)) \oplus \ker(g(\phi)).$$

Preuve. On rappelle que $f(\phi)$ désigne l'image par f du morphisme $\mathrm{ev}_\phi\colon K[t] \to End(V)$. Soit $a, b \in K[t]$ avec $1 = af + bg$, donc $\mathrm{id} = af(\phi) + bg(\phi)$. Si $fg(\phi)(v) = 0$, alors $f(\phi)bg(\phi)(v) = fbg(\phi)(v) = 0$ et $g(\phi)af(\phi)(v) = gaf(\phi)(v) = 0$. Il suit que $bg(\phi)$ et $af(\phi)$ sont les deux projecteurs désirés sur $\ker(fg(\phi))$.

Exercice 3. 1. Démontrez que $\mathbb{Q}\left(e^{\frac{2\pi i}{9}} + e^{-\frac{2\pi i}{9}}\right)$ est $\mathbb{Z}/3\mathbb{Z}$-galoisisenne.

Indice: considérez l'extension $\mathbb{Q}\left(e^{\frac{2\pi i}{9}}\right)$.

2. Plus généralement, démontrez que pour chaque entier premier p, il existe une extension $\mathbb{Q} \subseteq L$ tel que $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}$.

Indice: Pour $p \geq 3$ considérez l'extension $\mathbb{Q} \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{p^2}}\right)$, et appliquez le théorème fondamental de la théorie de Galois.

Solution.

1. Soit $\alpha := e^{2i\pi/p}$ (et donc $\alpha^{-1} = e^{-2i\pi/9}$).

   Par le point 4 de l'exercice précédent, on sait que l'extension $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ est $(\mathbb{Z}/9\mathbb{Z})^\times$-Galoisienne. De plus, $(\mathbb{Z}/9\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$ (ce groups multiplicatif est généré par 2), et donc il existe un unique élément d'ordre 2.

   De plus, la conjugaison complexe σ agit sur $\mathbb{Q}(\alpha)$, vu que $\sigma(\alpha) = \overline{\alpha} = \alpha^{-1}$. Ainsi, $\sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ et correspond donc a cet unique élément d'ordre 2 (et son élément correspondant dans $\mathbb{Z}/6\mathbb{Z}$ est nécessairement 3). Comme le sous-groupe $H\langle\sigma\rangle \subseteq \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ est normal, on sait par le théorème fondamental que l'extension $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)^H$ est Galoisienne, de groupe de Galois

   $$\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})/H \cong (\mathbb{Z}/6\mathbb{Z})/\langle 3\rangle \cong \mathbb{Z}/3\mathbb{Z}.$$

   Il suffit donc de montrer que $\mathbb{Q}(\alpha)^H = \mathbb{Q}(\alpha + \alpha^{-1})$. L'inclusion $\mathbb{Q}(\alpha + \alpha^{-1}) \subseteq \mathbb{Q}(\alpha)^H$ est immédiate, car $\alpha + \alpha^{-1}$ est fixé par σ. Comme $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)^H$ est de degré 3, il suffit de montrer que $\mathbb{Q} \subseteq \mathbb{Q}(\alpha + \alpha^{-1})$ est aussi de degré 3. Or, on a que

   $$3 = [\mathbb{Q}(\alpha)^H : \mathbb{Q}] = [\mathbb{Q}(\alpha)^H : \mathbb{Q}(\alpha + \alpha^{-1})][\mathbb{Q}(\alpha + \alpha^{-1}) : \mathbb{Q}]$$

   donc si par contradiction $\mathbb{Q}(\alpha + \alpha^{-1}) \neq \mathbb{Q}(\alpha)^H$, alors automatiquement $\mathbb{Q} = \mathbb{Q}(\alpha + \alpha^{-1})$, en d'autres termes que $\alpha + \alpha^{-1} = \mathbb{Q}$.

   Montrons que ce n'est pas le cas. On a que

   $$(\alpha + \alpha^{-1}) = e^{2i\pi/3} + e^{-2i\pi/3} + 3(\alpha + \alpha^{-1}) = -1 + 3(\alpha + \alpha^{-1})$$

   donc $\alpha + \alpha^{-1}$ est une racine de $f(x) = x^3 - 3x + 1$. Il suffit donc de montrer que $f(x) \in \mathbb{Q}[x]$ est irréductible. Par Gauss et réduction modulo 2, il suffit de montrer que $x^3 + x + 1 \in \mathbb{F}_2[x]$ est irréductible. Or, c'est immédiat car ce polynôme est de degré 3 et n'a pas de racines.

2. Pour $p = 2$, on a déjà vu par exemple que $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ était Galoisienne de degré 2. Supposons maintenant $p \geq 3$, et posons $\alpha = e^{2i\pi/p^2}$. Alors par l'exercice précédent, $\mathbb{Q}(\alpha)/\mathbb{Q}$ est Galoisien de groupe de Galois $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Ce groupe est abélien d'ordre $\varphi(p^2) = p(p-1)$, donc par le théorème structural des groupe abéliens, on sait que l'on a

   $$(\mathbb{Z}/p^2\mathbb{Z})^\times \cong \mathbb{Z}/p\mathbb{Z} \times H$$

   pour H un groupe abélien d'ordre $p - 1$. Ce groupe est automatiquement normal (car tout est abélien ici), et donc par le théorème fondamental de la théorie de Galois, $\mathbb{Q}(\alpha)^H/\mathbb{Q}$ est Galoisienne de groupe de Galois

   $$(\mathbb{Z}/p\mathbb{Z} \times H)/H \cong \mathbb{Z}/p\mathbb{Z}.$$

Exercice 4.
Soit K un corps, et soit $K \subseteq M = K(\alpha)$ et $K \subseteq N = K(\beta)$ des extensions galoisiennes de K.

1. Démontrez que $K \subseteq L = K(\alpha, \beta)$ est aussi galoisienne.

Supposons à partir de maintenant que $M \cap N = K$ en tant que sous-corps de L.

2. Démontrez que $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K)$ qui est la restriction sur chaque composante est un isomorphisme.

3. Démontrez que pour chaque entiers premiers distincts p et q, il existe une extension $\mathbb{Q} \subseteq L$ galoisienne tel que $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/pq\mathbb{Z}$.

Solution.

1. On sait par le cours qu'une extension est Galoisienne si et seulement si c'est un corps de décomposition d'un polynôme séparable. Ainsi les polynômes $m_{\alpha,K}$ et $m_{\beta,K}$ sont séparables et se scindent sur $K(\alpha)$ et $K(\beta)$ respectivement. Ainsi, le polynôme $m_{\alpha,K}m_{\beta,K}$ est aussi séparable et se scinde sur $K(\alpha,\beta)$. Comme $K(\alpha,\beta)$ est généré par les racines de $m_{\alpha,K}m_{\beta,K}$ (il est généré par α et β), c'est bien un corps de décomposition de $m_{\alpha,K}m_{\beta,K}$. Par le même fait rappelé plus haut, $K(\alpha,\beta)$ est Galoisien sur K.

2. Comme M/K est Galoisienne, on sait que pour tout $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(M) = M$. Ainsi, σ se restricte en un élément $\sigma|_M \in \mathrm{Gal}(M/K)$, et on a donc un morphisme de groupes $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$. En faisant la même chose pour N, on en déduit un morphisme de groupes

$$\begin{aligned} \mathrm{Gal}(L/K) &\xrightarrow{\quad\phi\quad} \mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K) \\ \sigma &\longmapsto (\sigma|_M, \sigma|_N) \end{aligned}$$

   Ce morphisme est automatiquement injectif, car si $\sigma \in \mathrm{Gal}(L/K)$ se restreint à l'identité sur M et sur N, alors il fixe α et β. Come $L = K(\alpha,\beta)$, on doit avoir $\sigma = id$.

   De plus, $|\mathrm{Gal}(L/K)| = [L:K]$ et

$$|\mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K)| = |\mathrm{Gal}(M/K) \cdot |\mathrm{Gal}(N/K)| = [M:K][N:K].$$

   Supposons que l'on a prouvé que $[L:M] = [N:K]$. Alors

$$[M:K][N:K] = [M:K][L:M] = [L:K].$$

   Ainsi, ϕ est un morphisme injectif entre groupes finis ayant le même cardinal. C'est donc automatiquement un isomorphisme, ce qui conclut la preuve.

   Montrons maintenant que $[L:M] = [N:K]$ (c'est ici ou on utilisera que $M \cap N = K$!). Comme $L = M(\beta)$, il est équivalent de montrer que $\deg(m_{\beta,M}) = \deg(m_{\beta,K})$. Comme $m_{\beta,M}$ divise $m_{\beta,K}$, ce qu'il faut réellement montrer est que $m_{\beta,M} = m_{\beta,K}$.

   Comme $m_{\beta,K}$ sur scinde sur N, on a que

$$m_{\beta,K}(t) = \prod_i (t - \beta_i) \in N[t],$$

   où le produit se fait sur les racines de $m_{\beta,K}$. Ainsi, en voyant $m_{\beta,M}(t)$ comme un élément de $L[t]$, on a nécessairement que

$$m_{\beta,M}(t) = c\prod_j (t - \beta_j)$$

   où $c \in L$ et les β_j sont certaines racines de $m_{\beta,K}$. Comme $m_{\beta,M}$ est unitaire, $c = 1$ et donc comme tous les β_j sont dans N, on en déduit que $m_{\beta,M}(t) \in N[t]$. Ainsi $m_{\beta,M}(t) \in M[t] \cap N[t] = K[t]$, et comme il s'annule en β, il est divisible par $m_{\alpha,K}(t)$. Cela conclut donc la preuve.

3. Par l'exercice précédent, on sait qu'il existe des extensions $\mathbb{Q} \subseteq M \subseteq \mathbb{C}$ et $\mathbb{Q} \subseteq N \subseteq \mathbb{C}$, de groupes de Galois sur $\mathbb{Q}$ valant $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$ respectivement.

   Montrons que $M \cap N = \mathbb{Q}$. Par les extensions $\mathbb{Q} \subseteq M \cap N \subseteq N$ et le fait que $[N:\mathbb{Q}]$ est un nombre premier, on a que soit $M \cap N = \mathbb{Q}$, soit $M \cap N = N$. En faisant le même raisonnement pour M, on en déduit que soit $M = M \cap N = N$, soit $M \cap N = \mathbb{Q}$. Le premier cas est impossible, car $p \neq q$.

   Par le théorème de l'élément primitif, on peut écrire $M = \mathbb{Q}(\alpha)$ et $N = \mathbb{Q}(\beta)$, donc par les deux points précédents, $L = \mathbb{Q}(\alpha,\beta)$ est Galoisienne sur $\mathbb{Q}$, de groupe de Galois

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}.$$

Exercice 5.
Soit $K \subseteq L$ une extension Q_8-galoisienne (où Q_8 est le groupe des quaternions), et soit $f \in K[x]$ un polynôme irréductible tel que L est un corps de décomposition de f. Démontrez que $\deg f = 8$.

Solution.

Supposons par l'absurde que $d := \deg(f) < 8$, et soit $\alpha \in L$ une racine de f. Alors $[K(\alpha) : K] = d < 8$, donc il suffit de montrer que $K(\alpha) = L$ pour obtenir une contradiction.

Comme tous les sous-groupes de Q_8 sont normaux (nous vous laissons le soin de faire ce calcul), l'extension $K(\alpha)/K$ est Galoisienne par le théorème fondamental de la théorie de Galois. On sait que dans une extension Galoisienne, tout les polynômes minimaux des éléments scindent, les racines de ces polynômes étant formant des orbites sous le groupe de Galois. O<n en déduit que $m_{\alpha,K} = f$ se scinde sur $K(\alpha)$. Comme L est le corps de décomposition de L, on a donc forcément que $L = K(\alpha)$, ce qui donne une contradiction.