Exercice 1.
Soit $K \subseteq L = K(\alpha)$ une extension simple de corps. Démontrez qu'elle est galoisienne si et seulement si α est séparable sur K et $m_{\alpha,K}$ scinde sur L. On dit qu'un polynôme scinde si toute racine de $m_{\alpha,K}$ est contenue dans L.

Solution. Si $K \subseteq L$ est Galoisienne, alors par le Théorème 4.6.17 on sait que L est le corps de décomposition sur K d'un polynôme séparable $f(t) \in K[t]$. Par le corollaire 4.6.18, $K \subseteq L$ est alors séparable (donc α l'est aussi) et par le point (3) de la Poposition 4.6.4, $m_{\alpha,K}$ se scinde.

L'autre direction vient immédiatement du Théorème 4.6.17.

Exercice 2.
Soit $K \subseteq L = K(\alpha)$ une extension simple de degré 2 des corps de caractéristique non 2.

1. Soit $m_{\alpha,K} = x^2 + bx + c$, où $b, c \in K$. Démontrez que la formule quadratique est valide ici. Cela veut dire les deux racines de $m_{\alpha,K}$ sont $\frac{-b+\sqrt{b^2-4c}}{2}$ et $\frac{-b-\sqrt{b^2-4c}}{2}$, où $\beta = \sqrt{b^2-4c} \in L$ est un quelconque élément tel que $\beta^2 = b^2 - 4c$. Cela inclut l'affirmation que tel β n'existe pas dans K. Concluez que L est une extension par une racine (deuxième) d'un élément adéquat de K.

2. Démontrez que $K \subseteq L$ est $\mathbb{Z}/2\mathbb{Z}$-galoisienne .

3. Soit $\mathbb{Q} = K \subseteq L$ une extension de corps $\mathbb{Z}/4\mathbb{Z}$-galoisienne. Démontrez que il existe des entiers rationnels a, $b \neq 0$ et d tel que $L = \mathbb{Q}\Big(\sqrt{a+b\sqrt{d}}\Big)$ et $\sqrt{d} \notin \mathbb{Q}$, $\sqrt{a+b\sqrt{d}} \notin \mathbb{Q}(\sqrt{d})$.

4. Considérons a, $b \neq 0$, $d \in \mathbb{Q}$ tel que $\sqrt{d} \notin \mathbb{Q}$ et $\alpha = \sqrt{a+b\sqrt{d}} \notin \mathbb{Q}\big(\sqrt{d}\big)$. Démontrez que l'extension $K = \mathbb{Q} \subseteq L = \mathbb{Q}(\alpha)$ est $\mathbb{Z}/4\mathbb{Z}$-galoisienne si et seulement si $\sqrt{a-b\sqrt{d}} \in L$ et $\lambda = a^2 - b^2 d$ n'est pas un carré dans $\mathbb{Q}$.

5. Montrez que $\mathbb{Q} \subseteq \mathbb{Q}\big(\sqrt{2+2\sqrt{2}}\big)$ est $\mathbb{Z}/4\mathbb{Z}$-galoisienne.

Solution.

1. Comme 2 est inversible, on peut écrire

$$x^2 + bx + c = 0 \iff x^2 + 2\frac{b}{2}x + \frac{b^2}{4} = \frac{b^2}{4} - c$$

c'est à dire

$$(2x+b)^2 = b^2 - 4c.$$

Ainsi, $\beta = 2\alpha + b$ est une racine carrée de $\frac{b^2}{4} - c$. Notons que $L = K(\alpha) = K(\beta)$. Comme $K \neq L$, on a que $\beta \neq\in K$. Cet élément est une racine carrée d'un élément de K. On voit par calcul direct que $\frac{-b+\beta}{2}$ et $\frac{-b-\beta}{2}$ sont les racines du polynôme minimal.

2. On construit un automorphisme de Galois de L sur K par

$$L = K(\beta) \xleftarrow{\mathrm{ev}_\beta} K[t]/(t^2 - \beta^2) \xrightarrow{\mathrm{ev}_{-\beta}} K(\beta) = L.$$

Comme il envoie $\beta \mapsto -\beta$, il n'est pas l'identité. Comme $|\operatorname{Gal}(L \mid K)| \leq 2$ on a égalité et donc que cette extension est Galoisienne.

3. Soit H l'unique sous-groupe d'ordre 2 dans le groupe de galois $G = \mathrm{Gal}(L \mid K)$. Soit $M = L^H$. Ce corps est de degré 2 sur $\mathbb{Q}$ par la correspondance de Galois. Soit donc $d \in \mathbb{Q}$ avec $M = \mathbb{Q}(\sqrt{d})$. Comme $M \subset L$ est de degré 2 par multiplicativité des degré, il existe un élément $a + b\sqrt{d} \in M$ tel que $L = M(\sqrt{a + b\sqrt{d}})$.

   Montrons que $b \neq 0$. Si $b = 0$, alors $\sqrt{a} \notin \mathbb{Q}(\sqrt{d})$. Mais alors $L = \mathbb{Q}(\sqrt{a}, \sqrt{d})$ qui a groupe de Galois isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. En effet, un élément σ du groupe de Galois doit envoyer $\sqrt{a}$ sur $\pm\sqrt{a}$ et $\sqrt{d}$ sur $\pm\sqrt{d}$, ce qui force $\sigma^2 = id$. Ainsi, le groupe de Galois serait un groupe d'ordre 2 ou tous les éléments sont d'ordre au plus 2, i.e. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

   Dès lors, notons que $\sqrt{d} \in \mathbb{Q}(\sqrt{a + b\sqrt{d}})$, ce qui permet de conclure que $L = \mathbb{Q}(\sqrt{a + b\sqrt{d}})$.

4. Soit $\alpha = \sqrt{a + b\sqrt{d}}$ et $\beta = \sqrt{a - b\sqrt{d}}$. Notons que $\mathbb{Q}(\sqrt{d})$ est une extension intermédiaire Galoisienne de degré 2 sur $\mathbb{Q}$. Supposons l'extension Galoisienne. Soit $\phi \in \mathrm{Gal}(L \mid K)$ une extension de l'automorphisme de $\mathbb{Q}(\sqrt{d})$ qui envoie $\sqrt{d} \mapsto -\sqrt{d}$ à L par le théorème 4.3.4. On voit alors que $\phi(\alpha) \in L$ est une racine carrée de $a - b\sqrt{d}$. En particulier cet élément appartient à L. A l'inverse, si $\sqrt{a - b\sqrt{d}} \in L$, alors L contient toutes les racines du polynôme minimal de $\sqrt{a + b\sqrt{d}}$, donc $L/\mathbb{Q}$ est Galoisienne par le théorème 4.6.17.

   Ainsi, il suffit de montrer que $a^2 - b^2 d$ n'est pas un carré si et seulement si $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. Notons que $(\alpha\beta)^2 = a^2 - b^2 d$.

   Supposons tout d'abord que $a^2 - b^2 d$ est un carré, et soit $\psi \in \mathrm{Gal}(L/\mathbb{Q})$. Alors $\psi(\alpha) \in \{\pm\alpha, \pm\beta\}$. Si $\psi(\alpha) = \alpha$ ou $-\alpha$, alors $\psi^2(\alpha) = \alpha$ et donc ψ est d'ordre 2. Comme $(\alpha\beta)^2 = a^2 - b^2 d$, on a que $\alpha\beta \in \mathbb{Q}$ et donc vu que

$$\frac{1}{\alpha} = \frac{\beta}{\alpha\beta},$$

   on a

$$\psi(\alpha) = \psi(\alpha\beta/\beta) = \alpha\beta\psi(1/\beta) = \alpha\beta\psi(\beta)^{-1}.$$

   Ainsi, si $\psi(\alpha) = \beta$ ou $-\beta$, on en déduit aussi que $\psi^2(\alpha) = \alpha$, et donc $\psi^2 = id$.

   Ainsi, on a dans tous les cas que $\psi^2 = id$, et donc le groupe de Galois $\mathrm{Gal}(L/\mathbb{Q})$ est 2-torsion. Il ne peut donc pas être isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

   Supposons maintenant que $a^2 - b^2 d$ n'est pas un carré. Alors $\mathbb{Q}(\alpha\beta)$ est une sous-extension de degré 2 sur $\mathbb{Q}$. On alors deux extensions ϕ_1, ϕ_2 de l'automorphisme de Galois non-trivial $\phi\colon \mathbb{Q}(\alpha\beta) \to \mathbb{Q}(\alpha\beta)$ qui envoie $\alpha\beta \mapsto -\alpha\beta$. Ces deux extensions sont déterminées par leur valeur sur α. Par exemple, $\phi_1(\alpha) = \beta$ et alors forcément $\phi_1(\beta) = -\alpha$. Ainsi, il est clair que ϕ_1 est d'ordre 4.

5. C'est immédiat par le point précédent.

Exercice 3.
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 racine de l'unité dans les extensions de K. Supposons à a partir de maintenant que K contient toute ces racines.

2. 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 de $\mathbb{Z}/n\mathbb{Z}$ en tant qu'application K-linéaire sur L. Démontrez le polynôme minimal de ϕ en tant qu'une 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. Pour l'inverse, démontrons que si $n = p$ est premier et 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 $s = p$.

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 en appliquant le point précédent inductivement pour l'extension $\mathbb{Q}\left(e^{\frac{2\pi i}{p^j}}\right) \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{p^{j+1}}}\right)$ pour $1 \leq j \leq n-1$.

   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 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 $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$.

   Donnons deux preuves que ϕ admet une racine primitive n'ème de l'unité. Alors $\phi^n = id$ par hypothèse, et donc le polynôme minimal de ϕ en tant application K-linéaire divise $x^n - 1$.

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

   Pour montrer que c'est le polynôme minimal, 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 on a $x^d \in K = K \cdot 1$ 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

*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 (λ_i), alors ϕ restreint au sous-espace correspondant est la multiplication par λ_i, ce qui démontre que ϕ est diagonalisable.

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.

Maintenant que l'on sait que $x^n - 1$ est le polynôme minimal, soit x un vecteur propre associé à une racine *primitive* n-ième de l'unité. On voit alors en suivant le même raisonnement que ci-dessus 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.

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_j 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_j. 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'ème de l'unité.

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.

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.

Exercice 4. 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: 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 5.
Soit K un corps, et soit $K \subseteq M = K(\alpha)$ et $K \subseteq N = K(\beta)$ des extensions galoisienne 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 $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K)$.

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. Par le théorème 4.6.17, les polynômes $m_{\alpha,K}$ et $m_{\beta,K}$ sont séparables et se scinde sur $K(\alpha)$ et $K(\beta)$ respectivement. Ainsi, le polynôme $m_{\alpha,K}m_{\beta,K}$ est aussi séparable et se scinde sur $K(\alpha, \beta)$, donc par le même theorème, $K(\alpha, \beta)$ est Galoisien sur K.

2. Comme M/K est Galoisienne, on sait par la proposition 4.6.19 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 4, 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 6.
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. En combinant le théorème 4.6.17 (qui dit que $K(\alpha)$ est un corps de décomposition) et le corollaire 4.6.7, on 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.

Exercice 7.
Soit $K \subset L \subset M$ des extensions algébriques (non-nécessairement de degré fini) tel que $K \subset L$ et $L \subset M$ sont séparables. Montrez que $K \subset M$ est aussi séparable.

Solution.

On commence par étudier le cas particulier avec $K \subset L$ Galoisienne finie. On se ramènera à ce cas ensuite.

Soit $\alpha \in L$ et $m_{\alpha,L}$ le polynôme minimal de α sur L, séparable par hypothèse. Soit $\{h_1 = m_{\alpha,L}, \ldots, h_r\}$ l'orbite de $m_{\alpha,L}$ par $\mathrm{Gal}(L/K)$. Notons que tous ces polynômes sont séparables car image par un automorphisme d'un polynôme séparable : comme l'image par un automorphisme de la dérivée est la dérivée de l'image, on voit cela par le critère de la dérivée. Notons que par invariance par action du groupe de Galois $\mathrm{Gal}(L/K)$

$$f = \prod_{i=1}^{r} h_i$$

est à coefficients dans K et annule α. Par construction, ce polynôme est un produit d'irréductibles séparables distincts de $L[t]$. Si ces polynômes avaient une racine commune, ils seraient égaux, étant égaux au polynôme minimal sur L de cette racine commune. On déduit alors que f est à racines distinctes, ce qui montre que α est séparable sur K.[†]

On traite maintenant le cas général. Soit à nouveau $\alpha \in M$. Soit $a_0, \ldots, a_n \in L$ les coefficients de $m_{\alpha,L}$. Soit $M \subset M'$ un corps de décomposition des polynômes $m_{a_i,K}$ sur M. Soit alors L' le corps de décomposition inclut dans M' des polynômes $m_{a_i,K}$ sur K qui est donc une extension Galoisienne finie sur K en tant que corps de décomposition de polynômes séparables. Maintenant $K \subset L' \subset L'(\alpha)$ rentre dans le cas de figure ci-dessus. En effet $L' \subset L'(\alpha)$ est séparable car $m_{\alpha,L}$ est un polynôme séparable à coefficients dans L' qui annule α. Ainsi, on déduit par le cas précédent que $m_{\alpha,K}$ est séparable, ce qui conclut.

[†]En fait $f = m_{\alpha,K}$. Il n'est pas logiquement nécessaire de savoir cela pour la preuve mais voici pourquoi : comme $m_{\alpha,L} \mid m_{\alpha,K}$ on voit que tout h_i doit diviser $m_{\alpha,K}$ et donc que f divise $m_{\alpha,K}$.

Preuve du lemme des noyaux. Dans l'exercice 3.2 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 $\ker(fg(\phi))$.