TD n°7.

Exercice 1. Soit K un corps et Ω une extension de k. Soit L_1 et L_2 deux sous-corps de Ω contenant K de dimensions finies sur K. On note L_1L_2 le sous-corps de Ω engendré par L_1 et L_2.

a) Montrer que $[L_1L_2 : K] \leq [L_1 : K][L_2 : K]$, et qu'en cas d'égalité, $K = L_1 \cap L_2$.

b) On suppose dorénavant L_1/K galoisienne. Montrer que L_1L_2/L_2 est galoisienne et construire un isomorphisme $\mathrm{Gal}(L_1L_2/L_2) \to \mathrm{Gal}(L_1/L_1 \cap L_2)$.

c) Montrer que $[L_1L_2 : K] = [L_1 : K][L_2 : K]/[L_1 \cap L_2 : K]$.

d) On suppose dorénavant que L_2/K est également galoisienne. Montrer que L_1L_2 et $L_1 \cap L_2$ sont des extensions galoisiennes de K.

e) Construire un morphisme injectif $\phi : \mathrm{Gal}(L_1L_2/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$

f) Montrer que l'image de ϕ est $\{(g_1, g_2) \in \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K), \pi_1(g_1) = \pi_2(g_2)\}$, où $\pi_i : \mathrm{Gal}(L_i/K) \to \mathrm{Gal}(L_1 \cap L_2/K)$ est la surjection canonique.

g) Soit $\mathbb{Q}^{\mathrm{ab}}$ l'ensemble des nombres algébriques x contenus dans une extension galoisienne L de $\mathbb{Q}$ telle $\mathrm{Gal}(L/\mathbb{Q})$ soit commutatif. Montrer que $\mathbb{Q}^{\mathrm{ab}}$ est un corps. Est-ce une extension finie de $\mathbb{Q}$?

Solution. a) Soit $(e_i)_{i\in[1,n]}$ une base de L_2 sur K. Alors $L := L_1e_1 + \cdots + L_1e_n$ est une sous-k-algèbre de Ω contenant L_1 et L_2, de dimension finie, donc c'est un corps, donc $L = L_1L_2$. Donc $[L_1L_2 : L_1] \leq n = [L_2 : K]$, ce qui prouve le résultat voulu par multiplicativité.

En cas dégalité, on a $[L_1L_2 : K] = [L_1 : K][L_2 : K]$. Or en appliquant le résultat précédent en remplaçant K par $L_1 \cap L_2$ on a $[L_1L_2 : L_1 \cap L_2] \leq [L_1 : L_1 \cap L_2][L_2 : L_1 \cap L_2]$ donc en multipliant par $[L_1 \cap L_2 : K]$, on obtient $[L_1L_2 : K] \leq [L_1 : K][|_2 : K]/[L_1 \cap L_2 : K]$, d'où, en combinant avec l'hypothèse, $[L_1 \cap L_2 : K] \leq 1$.

b) Si L_1 est le corps de décomposition de P sur K avec P séparable, alors L_1L_2 est aussi le corps de décomposition de P sur L_2 et P est toujours séparable, donc L_1L_2/L_2 est bien galoisienne.

On considère le morphisme $\phi : \mathrm{Gal}(L_1L_2/L_2) \to \mathrm{Gal}(L_1/L_1 \cap L_2)$ qui à σ associe sa restriction à L_1. ϕ est injective car si $\phi(\sigma) = \mathrm{Id}$, la restriction de σ à L_1 et à L_2 sont l'identité, donc σ est l'identité sur L_1L_2. Pour la surjectivité, soit H l'image de ϕ et $x \in L_1^H$. Pour tout $\sigma \in \mathrm{Gal}(L_1L_2/L_2)$, $\sigma(x) = x$ donc $x \in (L_1L_2)^{\mathrm{Gal}(L_1L_2/L_2)} = L_2$. Comme $x \in L_1$, $x \in L_1 \cap L_2$, donc $L_1^H = L_1 \cap L_2$, ca qui prouve la surjectivité.

c) L'isomorphisme précédent nous dit $[L_1L_2 : L_2] = [L_1 : L_1 \cap L_2]$, et en multipliant par $[L_2 : K]$ des deux côtés, on obtient l'égalité voulue.

d) Si L_i est le corps de décomposition de P_i sur K, avec P_i séparable, L_1L_2 est le corps de décomposition de P_1P_2 sur K qui est aussi séparable, donc L_1L_2/K est galoisienne. Si $\sigma \in \mathrm{Gal}(L_1L_2/K)$, alors $\sigma(L_i) \subset L_i$ car L_i est galoisienne, donc $\sigma(L_1 \cap L_2) \subset L_1 \cap L_2$, ce qui montre que $L_1 \cap L_2/K$ est galoisienne.

e) On pose $\phi(\sigma) = \sigma_{|L_1}, \sigma_{|L_2}$. Le morphisme est injectif car si σ est l'identité sur L_1 et L_2, il est l'identité sur L_1L_2.

f) On a clairement $\Im\phi \subset E := \{(g_1, g_2) \in \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K), \pi_1(g_1) = \pi_2(g_2)\}$. Pour prouver l'égalité, il suffit de calculer le cardinal de E et de comparer avec la formule de la question c. Si on considère le morphisme surjectif $\mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) \to \mathrm{Gal}(L_1 \cap L_2/K) \times \mathrm{Gal}(L_1 \cap L_2/K)$ alors E est l'image réciproque de la diagonal Δ, qui est un sous-groupe d'indice $[L_1 \cap L_2 : K]$ dans $\mathrm{Gal}(L_1 \cap L_2/K) \times \mathrm{Gal}(L_1 \cap L_2/K)$. Donc E est aussi un sous-groupe d'indice $[L_1 \cap L_2 : K]$ de $\mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$, ce qui nous donne le cardinal voulu.

g) Si $x_1 \in L_1$ et $x_2 \in L_2$ avec L_1, L_2 abéliennes sur $\mathbb{Q}$, alors $x_1 + x_2, x_1x_2 \in L_1L_2$ qui est aussi une extension abélienne de $\mathbb{Q}$ d'après e. Donc $\mathbb{Q}^{\mathrm{ab}}$ est une extension de $\mathbb{Q}$. Ce n'est pas une extension finie car elle contient toutes les racine de 1.

Exercice 2. Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré n. Soit E un corps de décomposition de P sur $\mathbb{Q}$, G le groupe de Galois de $E/\mathbb{Q}$. Ecrivons $P = \prod_{i=1}^n (X - \alpha_i)$. Soit $A := \mathbb{Z}[\alpha_1, \cdots, \alpha_n] \subset E$ la sous-$\mathbb{Z}$-algèbre de E engendrée par $(\alpha_i)_i$. Soient p un nombre premier et $\overline{P}$ la réduction de P modulo p. Soit N le cardinal de G.

a) Montrer que A est un $\mathbb{Z}$-module libre de rang N.

b) Montrer que si $g \in G$, $g(A) = A$ et en déduire une action de G sur A.

c) Soit $\mathfrak{m}$ un idéal maximal de A contenant pA (justifier l'existence d'un tel $\mathfrak{m}$). Montrer que $L := A/\mathfrak{m}$ est une extension finie de $\mathbb{F}_p$. On note $\pi/A \to L$ la projection canonique.

d) Montrer que L est un corps de décomposition de $\overline{P}$ sur $\mathbb{F}_p$.

e) On suppose dorénavant que $\text{pgcd}(\overline{P}, \overline{P}') = 1$. Montrer que $\text{pgcd}(P, P') = 1$. On note $\Omega := \{\alpha_i\}$ et $\overline{\Omega} := \{\pi(\alpha_i)\}$.
On a deux injections naturelles $i : G \to \mathfrak{S}_\Omega$ et $j : \text{Gal}(L/\mathbb{F}_p) \to \mathfrak{S}_{\overline{\Omega}}$ et $\pi_\Omega : \Omega \to \overline{\Omega}$ induit un isomorphisme $\pi^* : \mathfrak{S}_{\overline{\Omega}} \to \mathfrak{S}_\Omega$ qui envoie σ sur $\pi_\Omega^{-1} \circ \sigma \circ \pi_\Omega$. L'objectif de l'exercice est de montrer que $\pi^* j(\text{Gal}(L/\mathbb{F}_p)) \subset i(G)$.

f) Montrer que si $(\phi_i)_i$ est une famille de morphismes d'anneaux de A vers L deux à deux distincts, alors $(\phi_i)_i$ est une famille libre du L-espace vectoriel $\text{Hom}_{\mathbb{Z}\text{-Mod}}(A, L)$. En déduire qu'il y a au plus N morphismes d'anneaux de A vers L. *Indice* : si $y \in A$ et $\sum_i a_i \phi_i = 0$, alors $\sum_i a_i(\phi_i(y) - \phi_1(y))\phi_i = 0$.

g) Montrer que tout morphisme d'anneaux $A \to L$ est de la forme $\pi \circ \sigma$ pour un unique $\sigma \in G$.

h) Montrer que si $s \in \text{Gal}(L/\mathbb{F}_p)$, alors $s \circ \pi$ est un morphisme d'anneaux $A \to L$.

i) En déduire un morphisme injectif $\text{Gal}(L/\mathbb{F}_p) \to \text{Gal}(E/\mathbb{Q})$.

j) Conclure.

Solution. a) A est engendré par les monômes $\alpha_1^{k_1} \cdots \alpha_n^{k_n}$ avec $k_i \leq n-1$, donc A est un $\mathbb{Z}$-module de type fini. Il est sans torsion puisque $A \subset E$ et E est sans torsion en tant que $\mathbb{Q}$-espace vectoriel. Donc A est un $\mathbb{Z}$-module libre et soit $e_1, \cdots, e_k$ une $\mathbb{Z}$-base de A. Alors $e_1, \cdots, e_k$ est aussi une $\mathbb{Q}$-base de E, donc $k = N$.

b) Soit $\Omega = \{\alpha_1, \cdots, \alpha_n\}$. On a $g(\Omega) \subset \Omega$, donc $g(R(\alpha_1, \cdots, \alpha_n) = R(g(\alpha_1), \cdots, g(\alpha_n)) \in A$ si $R \in \mathbb{Z}[X_1, \cdots, X_n]$, donc $g(A) \subset A$. En apliquant ce résultat à g^{-1}, on obtient l'inclusion inverse.

c) Comme $A \simeq \mathbb{Z}^N$ en tant que groupe, $pA \neq A$ donc pA est contenu dans un idéal maximal de A. Comme $p \in \mathfrak{m}$, p est nul dans $A/\mathfrak{m}$, qui est donc bien de caractéristique p. On a une surjection $A/pA \simeq (\mathbb{Z}/p\mathbb{Z})^N \to A/\mathfrak{m}$ donc $A/\mathfrak{m}$ est bien fini.

d) On a $\bar{P} = \prod_i (X - \pi(\alpha_i))$ et $L = \mathbb{F}_p[\alpha_1, \cdots, \alpha_n]$, donc L est un corps de décomposition de $\bar{P}$.

e) L'hypothèse équivaut à $\sharp\overline{\Omega} = n$. Or $\pi_\Omega : \Omega \to \overline{\Omega}$ est surjective, donc $\sharp\overline{\Omega} \geq n$ ce qui montre que les racines de P sont simples.

f) Supposons par l'absurde que les ϕ_i sont liés et soit $\sum_i \lambda_i \phi_i = 0$ une formule de liaison tel que $\{i, \lambda_i \neq 0\}$ soit minimal. Quitte à réordonner les ϕ_i, on peut supposer $\lambda_1 \neq 0$. Alors pour tout $x, y \in A$, $\sum_i \lambda_i \phi_i(x)\phi_i(y) = 0$ et $\sum_i \lambda_i \phi_i(x)\phi_1(y) = 0$. Donc $\sum_i \lambda_i(\phi_i(y) - \phi_1(y))\phi_i = 0$ d'où une formule de liaison avec strictement moins de termes. L'hypothèse de minimalité, donne donc $\phi_i(y) - \phi_1(y) = 0$ pour tout i tel que $\lambda_i \neq 0$. Comme y était quelconque, on en déduit, $\phi_i = \phi_1$. Les ϕ_i étant supposés distincts, on obtient $\phi_1 = 0$, ce qui est impossible.

g) Comme A est un $\mathbb{Z}$-module libre de rang N, $\text{Hom}_{\mathbb{Z}\text{-Mod}}(A, L)$ est un L-espace vectoriel de dimension N, d'où l'inégalité voulue.

h) Si $\sigma \in G$, $\pi\sigma$ est un morphisme d'anneaux en tant que composé de morphismes d'anneaux. Comme *sigma* est entièrement déterminé par sa restriction à Ω et que π_Ω est bijective, on obtient l'unicité de σ. Comme $\sharp G = N$, on obtient donc N morphismes d'anneaux $A \to L$ distincts de la forme $\pi\sigma$. L'inégalité de la question précédente nous dit qu'on les a tous.

i) C'est un morphisme d'anneaux en tant que composée de morphismes d'anneaux.

j) Le morphisme associe à $s \in \text{Gal}(L/\mathbb{F}_p)$ l'unique $\sigma \in G$ tel que $\pi \circ \sigma = s \circ \pi$. En se restreignant à Ω et $\overline{\Omega}$, on a donc $i(\sigma) = \pi_\Omega^{-1} j(s) \pi_\Omega$, comme voulu dans la question e.

Exercice 3. Soit $P = X^4 - 2 \in \mathbb{Q}[X]$ et L le corps de décomposition de P. Décrire le groupe de Galois G de P et toutes les extensions intermédiaires K telles que $\mathbb{Q} \subset K \subset L$.

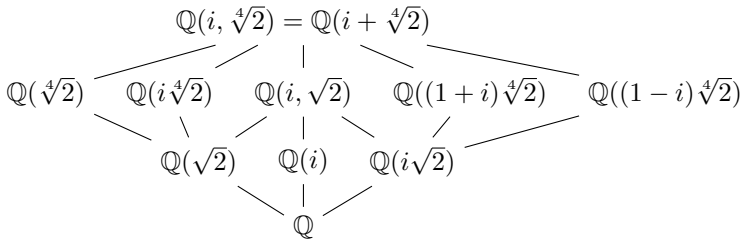
Solution. Le polynôme P est irréductible d'après le critère d'Eisenstein. L'ensemble des racines de P dans $\mathbb{C}$ est $\Omega := \{\zeta \sqrt[4]{2}, \zeta \in \mu_4\}$. Donc $\mathbb{Q}(\sqrt[4]{2})$ est un corps de rupture et $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ et le corps de décomposition est $L := \mathbb{Q}(\Omega) = \mathbb{Q}(\sqrt[4]{2}, i)$. Comme $i \notin \mathbb{Q}(\sqrt[4]{2})$ mais est racine de $X^2 + 1$ qui est de degré 2, $[L : \mathbb{Q}(\sqrt[4]{2})] = 2$ et donc, par multiplicativité, $[L : \mathbb{Q}] = 8$.
1ère méthode : On a une suite d'extensions galoisiennes sur $\mathbb{Q}$, $\mathbb{Q} \subset \mathbb{Q}(i) \subset L$, avec $\text{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$. Si $\sigma \in N := \text{Gal}(L/\mathbb{Q}(i)) \lhd G$, il existe $f(\sigma) \in \mu_4$ tel que $\sigma(\sqrt[4]{2}) = f(\sigma)\sqrt[4]{2}$. Comme $L = \mathbb{Q}(i)(\sqrt[4]{2})$, f est injective et donc surjective, puisque $\text{Gal}(L/\mathbb{Q}(i))$ et μ_4 on le même cardinal, 4. De plus f est un morphisme de groupe :

$$\sigma\sigma'(\sqrt[4]{2}) = \sigma(f(\sigma')\sqrt[4]{2}) = f(\sigma')\sigma(\sqrt[4]{2}) = f(\sigma)f(\sigma')\sqrt[4]{2}.$$

On en déduit donc que $\mathrm{Gal}(L/\mathbb{Q}(i))$ est isomorphe à $\mu_4 \simeq \mathbb{Z}/4\mathbb{Z}$ (en choisissant par exemple i comme générateur de μ_4).
On obtient donc une suite exacte :

$$1 \to \mathbb{Z}/4\mathbb{Z} \to G \to \mathbb{Z}/2\mathbb{Z} \to 1.$$

De plus L'élément non trivial de $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ est la restriction de la conjugaison complexe à $\mathbb{Q}(i)$, que l'on peut prolonger à L en la restriction c de la conjugaison complexe. Comme $c \in G$ est d'ordre 2, c définit une section du morphisme $G \to \mathbb{Z}/2\mathbb{Z}$, ce qui montre que G est un produit semi-direct $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. Il suffit maintenant de décrire l'action de c sur $N \simeq \mathbb{Z}/4\mathbb{Z}$ par conjugaison. Or $cf(i)c^{-1}(\sqrt[4]{2}) = cf(i)(\sqrt[4]{2}) = c(i\sqrt[4]{2}) = -i\sqrt[4]{2}$, donc $cf(i)c^{-1} = f(-i)$. Ce produit semi-direct est le groupe diédral D_4.
2ème méthode : on peut aussi décrire G comme sous-groupe de $\mathfrak{S}_4$ en identifiant $\{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\}$ à $\{1,2,3,4\}$. Le groupe N est alors le groupe engendré par le 4-cycle (1 2 3 4) et la conjugaison complexe c est la transposition (24). En regardant Ω comme un carré dans $\mathbb{C}$, on remarque que (1234) et (24) définissent des isométries du carré, et donc G est le groupe D_4 des isométries du carré.
Les extensions intermédiaires de $L/\mathbb{Q}$ correspondent aux sous-groupes H de D_4. Les sous-groupes non triviaux du groupe diédral sont les suivant : d'ordre 2, il y a le groupe engendré par la rotation (1 3)(2 4) d'angle π (alors $L^H = \mathbb{Q}(i, \sqrt{2})$), les deux groupes engendrés par les symétries (1 3) (alors $L^H = \mathbb{Q}(i\sqrt[4]{2})$), (2 4) (alors $L^H = \mathbb{Q}(\sqrt[4]{2})$), (1 2)(3 4) (alors $L^H = \mathbb{Q}((1+i)\sqrt[4]{2})$) et (14)(23) (alors $L^H = \mathbb{Q}((1-i)\sqrt[4]{2})$) ; d'ordre 4 il y a N ($L^N = \mathbb{Q}(i)$) , et les deux sous groupes $\{id, (1\ 3)(2\ 4), (1\ 3), (2\ 4)\}$ (alors $L^H = \mathbb{Q}(\sqrt{2})$) et $\{id, (1\ 3)(2\ 4), (1\ 2)(3\ 4), (14)(23)\}$ (alors $L^H = \mathbb{Q}(i\sqrt{2})$).



Exercice 4. Soit L/K une extension de corps de degré 2. Montrer que c'est une extension normale.

Solution. Soit $x \in L - K$. Alors $L = K[x]$. Soit $P = X^2 + aX + b$ le polynôme minimal de x sur K, l'autre racine y de P est $-a - x \in L$. Donc $L = K[x, y]$ est un corps de décomposition de P donc est normale sur K.

Exercice 5. Soient $P = X^4 + aX^2 + b \in \mathbb{Q}[X]$ un polynôme irréductible, L le corps de décomposition de P et $G = \mathrm{Gal}(L/\mathbb{Q})$. On note $\pm\alpha, \pm\beta$ les racines de P.

a) Montrer que G est isomorphe à un sous-groupe du groupe diédral D_4 d'ordre 8.

b) Montrer que $G \simeq \mathbb{Z}/4\mathbb{Z}$ si et seulement si $(\alpha/\beta - \beta/\alpha) \in \mathbb{Q}$.

c) Montrer que $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$ si et seulement si $\alpha\beta \in \mathbb{Q}$ ou $\alpha^2 - \beta^2 \in \mathbb{Q}$.

d) Montrer que sinon G est isomorphe à D_4.

e) Déterminer le groupe de Galois de $X^4 - 4X^2 - 1$.

Solution. a) Si $\sigma \in G$, on doit avoir $\sigma(-\alpha) = -\sigma(\alpha)$ et $\sigma(-\beta) = -\sigma(\beta)$. Si on dispose les racines aux sommets d'un carré de façon à ce que α et $-\alpha$ soient deux sommets opposés, alors les permutations des racines vérifiant les deux propriétés ci-dessus sont exactement les isométries du carré. Donc $G \subset D_4$.

b) On rappelle que D_4 à trois sous-groupes d'ordre 4 dont un seul, celui engendré par la rotation $r = (\alpha\ \beta\ -\alpha\ -\beta)$, est monogène (cf. exercice 3) .
On a $r(\alpha/\beta - \beta/\alpha) = \alpha/\beta - \beta/\alpha$, donc $\alpha/\beta - \beta/\alpha \in L^{\langle r\rangle}$. Donc si $G = \langle r\rangle$, alors $\alpha/\beta - \beta/\alpha \in L^G = \mathbb{Q}$.
Réciproquement, si $s \notin \langle r\rangle$, alors $s(\alpha/\beta - \beta/\alpha) = -(\alpha/\beta - \beta/\alpha)$. Donc si $\alpha/\beta - \beta/\alpha \in \mathbb{Q}$, on en déduit que $G \subset \langle r\rangle$, et donc $G = \langle r\rangle$ puisque $4|\sharp G$ puisque P est irréductible.

c) On a deux sous-groupes de G isomorphes à $(\mathbb{Z}/2\mathbb{Z})^2$, à savoir $H_1 := \{id, (1\ 3)(2\ 4), (1\ 3), (2\ 4)\}$ et $H_2 := \{id, (1\ 3)(2\ 4), (1\ 2)(3\ 4), (14)(23)\}$
On a $\sigma(\alpha\beta) = \alpha\beta$ si $\sigma \in H_2$ et $= -\alpha\beta$ si $\sigma \notin H_2$. Donc si $G = H_2$, $\alpha\beta \in L^G = \mathbb{Q}$ et réciproquement si $\alpha\beta \in \mathbb{Q}$, $G \subset H_2$ et donc $G = H_2$ par le même argument de cardinalité qu'à la question précédente.
On a $\sigma(\alpha^2 - \beta^2) = \alpha^2 - \beta^2$ si $\sigma \in H_1$ et $= -(\alpha^2 - \beta^2)$ si $\sigma \notin H_1$. Donc si $G = H_1$, $\alpha^2 - \beta^2 \in L^G = \mathbb{Q}$ et réciproquement si $\alpha^2 - \beta^2 \in \mathbb{Q}$, $G \subset H_1$ et donc $G = H_1$ par le même argument de cardinalité qu'à la question précédente (en fait, le cas $G = H_1$ est impossible car H_1 n'agit pas transitivement sur les racines, et ceci contredit l'irréductibilité de P).

d) Comme $4|\sharp G$ par irréductibilité de P, si $\sharp G \neq 4$, alors $G = D_4$.

e) On a $\alpha = \sqrt{2+\sqrt{5}}$ et $\beta = \sqrt{2-\sqrt{5}}$. On en déduit $\alpha^2 - \beta^2 = 2\sqrt{5} \notin \mathbb{Q}$, $\alpha\beta = \sqrt{-1} \notin \mathbb{Q}$ et $(\alpha^2-\beta^2)/\alpha\beta = \sqrt{-5} \notin \mathbb{Q}$. Donc $G = D_4$.

Exercice 6. Soit $P = (X^2+3)(X^3-3X+1) \in \mathbb{Q}[X]$ et G le groupe de Galois de P.

a) Montrer que G est isomorphe à un sous-groupe de $\mathbb{Z}/2\mathbb{Z} \times \mathfrak{S}_3$

b) Calculer le cardinal de G.

c) Le groupe est-il commutatif ? cyclique ?

Solution. a) Soit $P_1 = X^2+3$ et $P_2 = X^3-3X+1$. Les polynômes P_1 et P_2 sont irréductibles car ils n'ont pas de racines dans $\mathbb{Q}$ (comme ils sont unitaires à coefficients entiers, toute racine rationnelle serait entière divisant le coefficient constant). On a un morphisme injectif $G \to \mathrm{Gal}(P_1) \times \mathrm{Gal}(P_2)$ avec $\mathrm{Gal}(P_1) = \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{Gal}(P_2)$ est un sous-groupe transitif de $\mathfrak{S}_3$, donc $\mathfrak{S}_3$ ou $\mathfrak{A}_3$.

b) Pour déterminer si $\mathrm{Gal}(P_2)$ est $\mathfrak{A}_3$ ou $\mathfrak{S}_3$, il suffit de calculer le discriminant.

$$\mathrm{disc(P_2)} = -(4\cdot(-3)^3 + 27\cdot 1^2) = 27\cdot(4-1) = 81 = 9^2.$$

Comme le discriminant est un carré, $\mathrm{Gal}(P_2) = \mathfrak{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$.
Donc G est un sous-groupe de $\mathbb{Z}/2/Z \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$ de cardinal divisible par 2 et 3 (par irréductibilité de P_1 et P_2), c'est donc $\mathbb{Z}/6\mathbb{Z}$, qui est commutatif et cyclique.

Exercice 7. Si p est un nombre premier et n est un entier premier à p, on note $\left(\frac{n}{p}\right) = 1$ si n est un carré dans $\mathbb{F}_p^\times$ et $\left(\frac{n}{p}\right) = -1$ sinon. Si n est un multiple de p, on note $\left(\frac{n}{p}\right) = 0$
Soient q, p deux nombres premiers impairs distincts. Soient ζ une racine primitive q^{e}de 1 dans une clotûre algébrique $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$ et

$$\tau = \sum_{x\in\mathbb{F}_q} \left(\frac{x}{q}\right)\zeta^x \in \overline{\mathbb{F}_p}$$

a) Montrer que $\sum_{x\in\mathbb{F}_q}\left(\frac{x}{q}\right) = 0$.

b) Soit $x \in \mathbb{F}_p$. Montrer que

$$\sum_{(y,z)\in\mathbb{F}_p^2/y+z=x}\left(\frac{yz}{q}\right) = \left(\frac{-1}{q}\right)\sum_{y\in\mathbb{F}_p^\times}\left(\frac{1-xy^{-1}}{q}\right) = \begin{cases} (-1)^{\frac{q-1}{2}}(q-1) & \text{if} \quad x=0 \\ (-1)^{\frac{q-1}{2}}(-1) & \text{if} \quad x\neq 0 \end{cases}$$

c) En déduire que $\tau^2 = (-1)^{\frac{q-1}{2}}q$.

d) Montrer que $\tau^p = \left(\frac{p}{q}\right)\tau$

e) En déduire deux expressions pour τ^{p-1} et montrer que $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$.

Exercice 8. Soit p un nombre premier impair et $\zeta \in \mathbb{C}$ une racine primitive p^{e}de 1. Soit

$$\tau = \sum_{x\in\mathbb{F}_p}\left(\frac{x}{p}\right)\zeta^x.$$

a) Montrer que $\tau^2 = (-1)^{\frac{p-1}{2}}p$.

b) En déduire que toute extension de degré 2 de $\mathbb{Q}$ est contenue dans une extension cyclotomique $\mathbb{Q}(\zeta_0)$ où ζ_0 est une racine de 1.

Exercice 9. Soit f le polynôme $X^4+8X+12 \in \mathbb{Q}[X]$.
(i) Montrer que f est irréductible sur $\mathbb{Q}$.
(ii) Montrer que $\mathrm{Gal}(f)$ est isomorphe à $\mathfrak{A}_4$.
(iii) Soit L le corps de décomposition de f dans $\mathbb{C}$. Montrer qu'il n'existe pas d'extension quadratique de $\mathbb{Q}$ contenue dans L.

Solution. (i) Montrons que ce polynôme ne se factorise pas en produit de facteurs de degrés 2

$$X^4+8X+12=(X^2+aX+b)(X^2+cX+d).$$

On aurait alors $a+c=0$, $ac+b+d=0$, $ad+bc=8$ et $bd=12$. Soit $c=-a$ et $a^2=(b+d)$. Mais $(b,d)=\pm(1,12),\pm(2,6),\pm(3,4)$ soit finalement $a^2=\pm13,\pm8,\pm7$ ce qui n'est pas possible.
(ii) Le discriminant de f est $2^{12}.3^4$. Souvenons nous que ce discriminant vaut (à un carré près) $(-1)^{n(n-1)/2}\mathrm{Res}(P,P')=\mathrm{Res}(P,P')$. On a

$$\mathrm{Res}(P,P')=\begin{vmatrix}1&0&0&p&q&0&0\\0&1&0&0&p&q&0\\0&0&1&0&0&p&q\\4&0&0&p&0&0&0\\0&4&0&0&p&0&0\\0&0&4&0&0&p&0\\0&0&0&4&0&0&p\end{vmatrix}=\begin{vmatrix}1&0&0&p&q&0&0\\0&1&0&0&p&q&0\\0&0&1&0&0&p&q\\0&0&0&-3p&-4q&0&0\\0&0&0&0&-3p&-4q&0\\0&0&0&0&0&-3p&-4q\\0&0&0&4&0&0&p\end{vmatrix}=\begin{vmatrix}-3p&-4q&0&0\\0&-3p&-4q&0\\0&0&-3p&-4q\\4&0&0&p\end{vmatrix}$$

On a donc $\Delta=p\cdot(-3p)^3-4\cdot(-4q)^3=-27p^4+256q^3$. Dans le cas particulier où $p=8$, $q=12$, on obtient $\Delta=2^8\cdot3^3\cdot2^6-3^3\cdot2^{12}=2^{12}3^4$ qui est un carré dans $\mathbb{Q}$, donc $\mathrm{Gal}(f)$ est contenu dans $\mathfrak{A}_4$ (exercice précédent). (La formule générale du calcul du discriminant de X^n+pX+q est dans le polycopié de votre cours, p. 218). Je ne résiste pas au cas général :

$$\Delta=\begin{vmatrix}1&0&\cdots&\cdots&p&q&0&\cdots&0\\0&1&\cdots&&\cdots&p&q&0&0\\\vdots&&\ddots&\ddots&&&&\ddots&\vdots\\&&&1&0&\cdots&&p&q\\n&0&\cdots&\cdots&p&0&\cdots&&0\\0&n&\cdots&&\cdots&p&0&\cdots&0\\\vdots&&\ddots&\ddots&&\ddots&&&\vdots\\\vdots&&&\ddots&\ddots&&\ddots&&\vdots\\0&\cdots&&\cdots&n&\cdots&&\cdots&p\end{vmatrix}=\begin{vmatrix}1&0&\cdots&&\cdots&p&q&0&\cdots&0\\0&1&\cdots&&&\cdots&p&q&0&0\\\vdots&&\ddots&\ddots&&&&&\ddots&\vdots\\&&&1&\cdots&&&\cdots&p&q\\0&0&\cdots&\cdots&(1-n)p&-nq&\cdots&&\cdots&0\\0&0&\cdots&&\cdots&(1-n)p&-nq&\cdots&&0\\\vdots&&\ddots&\ddots&&&\ddots&&&\vdots\\\vdots&&&0&\ddots&&&\ddots&(1-n)p&-nq\\0&\cdots&&\cdots&n&\cdots&&\cdots&&p\end{vmatrix}$$

donc

$$\Delta=\begin{vmatrix}(1-n)p&-nq&0&\cdots&\cdots&0\\0&(1-n)p&-nq&\cdots&&0\\\vdots&&&\ddots&\ddots&\vdots\\n&&0&\cdots&\cdots&0&p\end{vmatrix}=p[(1-n)p]^{n-1}+(-1)^{n+1}n[(-nq)]^{n-1}=(1-n)^{n-1}p^n+n^nq^{n-1}$$

Si nous montrons que 3 divise l'ordre du groupe de Galois nous avons terminé. En effet, nous savons par ailleurs, f étant irréductible de degré 4, que l'ordre de $\mathrm{Gal}(f)$ est divisible par 4. Par suite, 12 divise l'ordre de $\mathrm{Gal}(f)$, d'où $\mathrm{Gal}(f)=\mathfrak{A}_4$.
Il reste à montrer l'assertion que 3 divise l'ordre du groupe de Galois.
1re méthode : il suffit de trouver un nombre premier p tel que la réduction de P modulo p ait un facteur irréductible de degré 3 et d'appliquer l'exercice 2. Comme 2 et 3 divisent le discriminant de P, essayons $p=5$. Alors $\overline{P}=X^4+3X+2$ admet -1 comme racine, $\overline{P}=(X+1)(X^3-X^2+X+2)$ et X^3-X^2+X+2 est irréductible car n'a pas de racines. Donc le corps de décomposition de $\overline{P}$ est $\mathbb{F}_{125}$ et son groupe de Galois est $\mathbb{Z}/3\mathbb{Z}$. L'exercice 2 nous dit donc que $\mathbb{Z}/3\mathbb{Z}$ s'injecte dans le groupe de Galois de P, ce qui permet de conclure.

2e méthode : Nous allons montrer un résultat intermédiaire qui permet de montrer comment l'ordre du groupe de Galois G d'un polynôme de degré 4 peut être divisible par 3. (c'est aussi dans votre cours, p. 221)
Soit donc P un polynôme irréductible unitaire de degré 4 de $\mathbb{Z}[X]$ et soit x_1, x_2, x_3 et x_4 ses racines dans un corps de décomposition L de P (elles sont distinctes car en caractéristique nulle tous les polynômes sont séparables). On écrit $P(x)=X^4+a_3X^3+a_2X^2+a_1X+a_0$ et on note σ_i le polynôme symétrique élémentaire de degré i en les racines x_i. Ainsi, on a

$$\sigma_1=x_1+x_2+x_3+x_4=-a_3,\qquad \sigma_2=x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4=a_2,$$

$$\sigma_3=x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4=-a_1\qquad\text{et}\qquad\sigma_4=x_1x_2x_3x_4=a_0.$$

Posons maintenant $\alpha = x_1x_2+x_3x_4$, $\beta = x_1x_3+x_2x_4$ et $\gamma = x_1x_4+x_2x_3$ qui sont des éléments de L. Remarquons que les éléments $A_1 = \alpha+\beta+\gamma$, $A_2 = \alpha\beta+\alpha\gamma+\beta\gamma$ et $A_3 = \alpha\beta\gamma$ sont des polynômes symétriques en les racines x_i ils s'expriment donc en fonction des σ_i c'est-à-dire qu'il sont dans $\mathbb{Z}$. Ainsi le polynôme

$$Q(X) = X^3 - A_1X^2 + A_2X - A_3 = (X-\alpha)(X-\beta)(X-\gamma)$$

est dans $\mathbb{Z}[X]$ et ses racines (α, β et γ) sont dans L. Soit alors $K = \mathbb{Q}(\alpha,\beta,\gamma)$ c'est le corps décomposition du polynôme $Q(X)$. Il contient $\mathbb{Q}(\alpha)$ et en particulier si Q est irréductible, ce dernier corps est de degré 3. On a alors

$$[\mathbb{Q}(\alpha):\mathbb{Q}][L:\mathbb{Q}(\alpha)] = |[L:\mathbb{Q}] = |G|$$

donc 3 divise l'ordre de G.
Pour vérifier que le polynôme Q est irréductible, il faut bien sûr pouvoir le calculer. C'est un peu fastidieux mais il suffit d'exprimer les A_i en fonction des σ_i. Calculons celà. On a

$$A_1 = \alpha+\beta+\gamma = \sigma_2 = a_2.$$

On calcule ensuite

$$A_2 \quad = \quad \alpha\beta+\alpha\gamma+\beta\gamma = x_1^2x_2x_3 + \cdots + x_2x_3x_4^2 = \sigma_3\sigma_1 - 4\sigma_4$$

Enfin, on a

$$\begin{array}{rcl} A_3 & = & \alpha\beta\gamma = (x_1^3x_2x_3x_4 + \cdots + x_1x_2x_3x_4^3) + 4(x_1^2x_2^2x_3^2 + \cdots + x_2^2x_3^2x_4^2) \\ & = & (x_1^2 + \cdots + x_4^2)\sigma_4 + 4(\sigma_3^2 - 2(x_1^2x_2^2x_3x_4 + \cdots + x_1x_2x_3^2x_4^2)) \\ & = & (\sigma_1^2 - 2\sigma_2)\sigma_4 + 4(\sigma_3^2 - 2\sigma_4\sigma_2). \end{array}$$

Remarque : la méthode générale pour exprimer un polynôme symétrique comme polynôme en ses racines est très bien expliqué dans Jacobson et dans votre cours. Le discriminant de Q est le même que celui de P.
Ainsi dans le cas d'un polynôme de la forme X^4+pX+q ce qui est le cas de notre polynôme $(X^4+8X+12)$, on a $\sigma_1 = 0$, $\sigma_2 = 0$, $\sigma_3 = -p$ et $\sigma_4 = q$. On trouve alors

$$A_1 = 0 \quad A_2 = -4q \quad A_3 = 4p^2$$

ce qui nous donne le polynôme

$$X^3 - 4qX - 4p^2.$$

Dans notre cas on a le polynôme $X^3-48X-256$. Il faut montrer qu'il est irréductible. On va le réduire modulo 5 et montrer qu'il est alors irréductible ce qui entraînera qu'il est irréductible sur $\mathbb{Z}$. La réduction modulo 5 de ce polynôme est $R(X) = X^3+2X-1$. Il suffit de montrer qu'il n'a pas de racine modulo 5, or on a $R(0) = -1$, $R(1) = 2$, $R(2) = 1$, $R(-1) = 1$ et $R(-2) = 2$ donc le polynôme est irréductible.
(iii) Supposons qu'il existe une extension quadratique K de $\mathbb{Q}$ contenue dans L. L'extension L/K est galoisienne de degré 6, de sorte que le groupe de Galois de L sur K est un sous-groupe d'ordre 6 de $\mathrm{Gal}(L/\mathbb{Q})$. Puisque $\mathrm{Gal}(L/\mathbb{Q})$ est isomorphe à $\mathfrak{A}_4$, il suffit de prouver que $\mathfrak{A}_4$ n'a pas de sous-groupe d'ordre 6. Supposons qu'il existe un tel sous-groupe H de $\mathfrak{A}_4$. Alors ce groupe contient nécessairement des éléments d'ordre 3 sinon il ne contiendrait que 4 éléments (produits de transpositions à support disjoint). Il contient un 3-cycl donc tous les 3 cycles (qui sont conjugués donc il contient $\mathfrak{A}_4$.

Exercice 10. Soit f le polynôme $X^4+X+1 \in \mathbb{Q}[X]$.
(i) Montrer que f est irréductible sur $\mathbb{Q}$.
(ii) Montrer que $\mathrm{Gal}(f)$ est isomorphe à $\mathfrak{S}_4$.
(iii) Soit α une racine de f dans $\mathbb{C}$. Montrer qu'il n'existe pas d'extension quadratique de $\mathbb{Q}$ contenue dans $\mathbb{Q}(\alpha)$.

Solution. (i) Ce polynôme est irréductible modulo 2 car ses racines sont d'ordre 15 (en effet si $\alpha^4 = 1+\alpha$, alors $\alpha^8 = 1+\alpha^2$ et $\alpha^{16} = 1+\alpha^4 = \alpha$. Donc $\alpha^{15} = 1$ sans que $\alpha^3 = 1$ (sinon on aurait $\alpha^4 = \alpha$) ni $\alpha^5 = 1$ (sinon $\alpha^2 = \alpha+1$ et α serait d'ordre 3)).
(ii) Nous utilisons la même technique qu'à l'exercice précédent pour montrer que 12 divise l'ordre du groupe de Galois. 1$^{\text{re}}$méthode : réduisons modulo 3, $\bar{P} = (X-1)(X^3+X^2+X-1)$, avec X^3+X^2+X-1 irréductible, donc d'après l'exercice 2, l'ordre du groupe de Galois de P est divisible par 3.
2$^{\text{e}}$méthode : il faut maintenant montrer que le polynôme X^3-4X-4 est irréductible. Il suffit encore une fois de considérer ses racines qui doivent être entières et diviser 4. C'est ±1, ±2 ou ±4.
On déduit de ce qui précède que 12 divise l'ordre de $\mathrm{Gal}(f)$. Le discriminant de f est 229 qui n'est pas un carré dans $\mathbb{Q}$ (c'est un nombre premier), donc $\mathrm{Gal}(f)$ n'est pas contenu dans $\mathfrak{A}_4$. Puisque $\mathfrak{A}_4$ est le seul sous-groupe d'ordre 12 de $\mathfrak{S}_4$, on a donc $\mathrm{Gal}(f) = \mathfrak{S}_4$.

(ш) Supposons qu'il existe une telle extension quadratique K. Notons L le corps de décomposition de f dans $\mathbb{C}$ et H le groupe de Galois de L sur K. L'ordre de H est 12. Par suite, on a $H = \mathfrak{A}_4$. Puisque H contient le goupe de Galois de L sur $\mathbb{Q}(\alpha)$, qui est d'ordre 6, on en déduit que $\mathfrak{A}_4$ contient un sous-groupe d'ordre 6. D'où une contradiction (cf. l'exercice précédent et le résultat.

Exercice 11. Soient p un nombre premier et f un polynôme irréductible de $\mathbb{Q}[X]$ de degré p. Soit K le corps de décomposition de f dans $\mathbb{C}$. On suppose que f possède exactement deux zéros non réels. Montrer que le groupe de Galois de K sur $\mathbb{Q}$ est isomorphe à $\mathfrak{S}_p$.
Application. Montrer que le groupe de Galois du polynôme $f = X^5 - 4X^3 - 2 \in \mathbb{Q}[X]$ est isomorphe à $\mathfrak{S}_5$.

Solution. Posons $G = \mathrm{Gal}(K/\mathbb{Q})$. On peut supposer que p est ≥ 3, car l'énoncé est vrai si $p = 2$. Soit α une racine de f. Puisque $\mathbb{Q}(\alpha)$ est contenu dans K, et que le degré de $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}$ est p, l'ordre de G est divisible par p. Il en résulte que G a un élément d'ordre p (un groupe dont l'ordre est divisible par un nombre premier p possède un élément d'ordre p). Par ailleurs la conjugaison complexe induit un automorphisme de K, i.e. "un élément de G ; en effet, f étant à" coefficients dans $\mathbb{Q}$, si z est racine de f, son conjugué $\bar{z}$ l'est aussi. Puisque f a exactement deux racines non réelles, la conjugaison complexe laisse fixe les $p-2$ racines réelles de f et échange les deux racines imaginaires. On en déduit que l'image de G dans $\mathfrak{S}_p$ contient une transposition. Puisqu'elle contient un cycle d'ordre p, il en résulte que l'image de G dans $\mathfrak{S}_p$ est $\mathfrak{S}_p$ tout entier $(*)$. D'où le résultat.
$(*)$ Il s'agit de vérifier l'assertion suivante : Soient p un nombre premier et H un sous-groupe de $\mathfrak{S}_p$ contenant une transposition et un cycle d'ordre p. Alors, on a $H = \mathfrak{S}_p$.
Démonstration : Il suffit de vérifier qu'un sous-groupe conjugué de H est $\mathfrak{S}_p$. Soit (a, b) une transpostion de H. Il existe $u \in \mathfrak{S}_p$ tel que $u(a) = 1$ et $u(b) = 2$. On a l'égalité $u(a,b)u^{-1} = \big(u(a), u(b)\big) = (1, 2)$. Quitte à remplacer H par uHu^{-1}, on peut ainsi supposer que $(1, 2)$ est dans H. Soit $c = (1, x_2, \cdots, x_p)$ un cycle d'ordre p de H. En modifiant c par une puissance convenable, on peut supposer que $x_2 = 2$. Par ailleurs, il existe $v \in \mathfrak{S}_p$ tel que l'on ait

$$v(1) = 1, \quad v(2) = 2 \quad \text{et} \quad v(x_i) = i \ \text{ pour } \ i \geq 3.$$

On a les égalités

$$v(1,2)v^{-1} = (1,2) \quad \text{et} \quad vcv^{-1} = \big(v(1), v(2), \cdots, v(x_p)\big) = (1, 2, \cdots, p).$$

Par suite, quitte à remplacer de nouveau H par vHv^{-1} on peut supposer que

$$t = (1,2) \in H \quad \text{et} \quad c = (1, 2, \cdots, p) \in H.$$

Pour tout entier i tel que $1 \leq i \leq p-2$, on a

$$c^i(1,2)c^{-i} = (i+1, i+2) \in H.$$

Pour tout un tel entier i, on a l'égalité

$$(i+1, i+2)(1, i+1)(i+1, i+2) = (1, i+2).$$

On en déduit que pour tout i compris entre 2 et p la transposition $(1, i)$ appartient à H. Pour tout $i \neq j$, l'égalité

$$(1,i)(1,j)(1,i) = (i,j),$$

implique alors que les transpositions sont dans H. Puisque $\mathfrak{S}_p$ est engendré par les transpositions, on a donc $H = \mathfrak{S}_p$. D'où le résultat.
Application. On vérifie que f a trois racines réelles et deux racines imaginaires : on a $f' = X^2(5X^2 - 12)$, et en notant ξ_1, ξ_2 les deux racines non nulles de f' telles que $\xi_1 < \xi_2$, on constate que $f(\xi_1) > 0$ et $f(\xi_2) < 0$. D'où l'assertion.

Exercice 12. Soit $P \in K[X]$ un polynôme unitaire à racine simples dans toute extension de K et L son corps de décomposition. Soit $\Omega = \{\alpha_1, \cdots, \alpha_n\}$ l'ensemble des racines de P dans L. On note $d = disc(P) = \prod_{i<j}(\alpha_i - \alpha_j)^2 \in K$ et $\sqrt{d} = \prod_{i<j}(\alpha_i - \alpha_j)$. On identifie $G = \mathrm{Gal}(L/K)$ avec un sous-groupe de $\mathfrak{S}_n$. On note $H = G \cap \mathfrak{A}_n$.

a) Soit $g \in G$. Montrer que $g(\sqrt{d}) = \epsilon(g)\sqrt{d}$, où $\epsilon : G \to \{\pm 1\}$ est le morphisme signature.

b) Montrer que $G \subset \mathfrak{A}_n$ si et seulement si d est un carré dans K.

c) Montrer que $K[\sqrt{d}] = L^H$.

d) Soit $P = X^3 + pX + q \in \mathbb{Q}[X]$ sans racines dans $\mathbb{Z}$. Montrer que, si $-(4p^3 + 27q^2)$ est un carré dans $\mathbb{Q}$, le groupe de Galois de P est $\mathbb{Z}/3\mathbb{Z}$ et, sinon, $\mathfrak{S}_3$.

Solution. C'est le théorème 20.27 du cours. Pour la dernière question, le calcul du discriminant de X^3+pX+q est donné dans la proposition 20.26 (cf. aussi la proposition 20.30).

Exercice 13. Soit $P \in K[X]$ un polynôme irréductible et α, β deux racines distinctes dans un corps de décomposition de P.
On suppose K de caractéristique nulle, montrer que $\alpha - \beta \notin Q$.

Solution. Il existe un automorphisme σ du corps de décomposition de P qui envoie α sur β par irréductibilité de P. Supposons par l'absurde que $k := \alpha - \beta \in K$. On montre alors par récurrence sur $n \in \mathbb{N}$ que $\sigma^n(\alpha) = \alpha - nk$. Comme K est de caractéristique nulle et $k \neq 0$, on en déduit $\sigma^n(\alpha) \neq \alpha$ pour tout $n \geq 1$, ce qui est impossible puisque σ doit être d'ordre fini.

Exercice 14. Pour chacun des polynômes suivants, calculer l'action du groupe de Galois sur les racines, faire la liste des sous-corps d'un corps de décomposition et pour chacun d'eux donner un élément primitif du corps et dire s'il est normal.

a) $P = X^4 - 7$, b) $\Phi_{20} = X^8 - X^6 + X^4 - X^2 + 1$, c) $X^6 + 3$,

d) $(X^2-2)(X^2-3)$, e) $X^3 - 1$, f) $(X^2 - 2X - 1)(X^2 - 2X - 7)(X^2 - 2X + 2)$,

g) $\Phi_9 = X^6 + X^3 + 1$, h) $X^3 + X + 1$.

Exercice 15. Calculer les groupes de Galois de sur $\mathbb{Q}$ de :

a) $X^4 + 2X^2 + X + 3$;

b) $X^4 + 3X^3 - 3X - 2$;

c) $X^6 + 22X^5 - 9X^4 + 12X^3 - 37X^2 - 29X - 15$.

Indice : on réduira modulo 2, 3 et 5.

Exercice 16. Montrer que pour tout $n \geq 1$, il existe un polynôme unitaire $P \in \mathbb{Z}[X]$ dont le groupe de Galois sur $\mathbb{Q}$ soit $\mathfrak{S}_n$.

Exercice 17. Soient $a, b \in \mathbb{Z}$. Soit $\sqrt{b}$ une racine carrée de b dans $\mathbb{C}$ et α une racine carrée de $a + \sqrt{b}$ dans $\mathbb{C}$.

a) Montrer que si $a^2 - b$ est un carré dans $\mathbb{Z}$, l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne de degré au plus 4.

b) Supposons $(a, b) = (7, 16)$. Montrer que l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne.

c) Si $(a, b) = (4, 3)$ montrer que l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ n'est pas galoisienne.
On pose $F = X^4 - 2aX^2 + a^2 - b \in \mathbb{Z}[X]$.

d) Calculer le discriminant de F.
On suppose que F est irréductible sur $\mathbb{Q}$.

e) Montrer que si $a^2 - b$ est un carré dans $\mathbb{Z}$, l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne de groupe de Galois isomorphe à $C_2 \times C_2$.

f) Montrer que si $a^2 - b$ appartient à $b\mathbb{Z}^2$, l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne de groupe de Galois isomorphe à C_4.

Solution.

a) α est racine du polynôme $P_{a,b} = (X^2 - a)^2 - b = X^4 - 2aX^2 + (a^2 - b)$. Les autres racines sont $-\alpha$ et $\pm\beta$, avec $\beta = \sqrt{a - \sqrt{b}}$. Si $a^2 - b = c^2$, avec $c \in \mathbb{Z}$, alors ces deux dernières racines peuvent s'écrire $\pm c/\alpha$ et sont dans $\mathbb{Q}(\alpha)$. Comme on ne sait pas si $P_{a,b}$ est irréductible, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ n'est pas connu.

b) Ici $\sqrt{b} = \pm 4$, donc α est une racine carrée de 11 ou de 3 et $\mathbb{Q}(\alpha)/\mathbb{Q}$ est quadratique donc galoisienne.

c) Si $\mathbb{Q}(\alpha)/\mathbb{Q}$ était galoisienne, elle contiendrait $\alpha^2 - 4 = \sqrt{3}$ et $\alpha\beta = \sqrt{13}$ et on aurait $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3}, \sqrt{13})$. On peut alors résoudre l'équation $\alpha^2 = 4 + \sqrt{3}$ dans le corps $\mathbb{Q}(\sqrt{3}, \sqrt{13})$ et voir qu'elle n'a pas de solution.

d) On a $F' = 4X(X^2 - a)$, donc le discriminant de F est

$$4^4(a^2 - b)N(\alpha^2 - a) = 2^8(a^2 - b)F(\sqrt{a})F(-\sqrt{a}) = 2^8 b^2(a^2 - b).$$

e) Ici le degré est 4, et on a vu que les racines de F sont $\pm\alpha$ et $\pm c/\alpha$ si $\sigma \in \mathrm{Gal}(F)$, pour toute racine γ de f et tout σ, on a $\sigma^2(\gamma) = \gamma$. Donc $\mathrm{Gal}(f)$ ne contient pas d'élément d'ordre 4 ; c'est donc $C_2 \times C_2$.

f) Ici $\alpha^2\beta^2 = a^2 - b = bt^2$, donc $\beta = t\sqrt{b}/\alpha \in \mathbb{Q}(\alpha)$ qui est donc galoisien. Soit $\sigma \in \mathrm{Gal}(F)$ tel que $\sigma(\alpha) = \beta$. Comme $\sigma(\alpha) \neq \pm\alpha$, on a $\sigma(\alpha^2) \neq \alpha^2$ et $\sigma(\sqrt{b}) = -\sqrt{b}$. On a donc $\sigma(\beta) = t\sigma(\sqrt{b})/\sigma(\alpha) = -\alpha$. On en déduit que σ est un 4-cycle et $\mathrm{Gal}(F) = C_4$.

Exercice 18. Soit $P_1(T) = T^3 - 7T + 7 \in \mathbb{Q}[X]$

a)Montrer que le polynôme P_1 a trois racines réelles x_1, x_2 et x_3 vérifiant $x_1 > x_2 > 0 > x_3$. Calculer le degré de l'extension $M = \mathbb{Q}(x_1)$ de $\mathbb{Q}$.

b) Montrer que l'extension $M/\mathbb{Q}$ est galoisienne, et décrire son groupe de Galois.

c) On note $\pm y_1$, $\pm y_2$ et $\pm y_3$ les racines de $P_2(T) = T^6 - 7T^2 + 7$, numérotées de façon que $x_i = y_i^2$, et L le corps $\mathbb{Q}(y_1, y_2, y_3)$.

a) Montrer que y_3 n'appartient pas à $\mathbb{Q}(y_1, y_2)$.

b) Montrer que y_2 n'appartient pas à $\mathbb{Q}(y_1)$.

c) Calculer le degré de M sur L.

d) L'extension $L/\mathbb{Q}$ est-elle galoisienne ? Abélienne ?

d) On note G le groupe $\mathrm{Aut}(L)$. Montrer que, pour $i \in \{1, 2, 3\}$, il existe deux éléments τ_i et τ_i' de G tels que, pour $j \neq i$, on ait

$$\tau_i(y_i) = -y_i, \quad \tau_i'(y_i) = y_i, \quad \tau_i(y_j) = y_j, \quad \tau_i'(y_j) = -y_j.$$

Montrer qu'il existe un élément τ de G tel que

$$\forall i \in \{1, 2, 3\}, \quad \tau(y_i) = -y_i.$$

Donner la liste des sous-corps N de L contenant M et tels que $[L : N] = 2$.

e) Montrer qu'il existe un élément σ de G tel que

$$\sigma(y_1) = y_2, \quad \sigma(y_2) = y_3, \quad \sigma(y_3) = y_1,$$

et calculer

$$\tau_1\sigma\tau_3, \quad \tau_1\sigma^2\tau_1, \quad \tau_3'\sigma\tau_2'.$$

f) Montrer que $\sqrt{-7}$ appartient à L et déterminer le groupe $\mathrm{Aut}(L/\mathbb{Q}(\sqrt{-7}))$.

g) On pose $\theta = y_1 + y_2 + y_3$. Calculer le degré de θ sur $\mathbb{Q}$ (on pourra étudier les images de θ sous l'action de G). Quelle est la structure du groupe $\mathrm{Aut}(L/\mathbb{Q}(\theta))$? Est-il distingué dans G ?

h) Indiquer combien de sous-corps de $\mathbb{Q}(\theta)$ contiennent $\sqrt{-7}$.

Solution.

a) La fonction $t \mapsto P_1(t)$ atteint son minimum sur $\mathbb{R}^+$ au point $\sqrt{7/3}$, où elle vaut

$$\frac{7}{3\sqrt{3}}(3\sqrt{3} - 2\sqrt{7}) < 0.$$

Comme $P_1(0)$ et $P_1(1)$ sont positifs et $P_1(-4) = -29$ est négatif, P_1 a trois racines réelles distinctes, dont une seule est négative. Si une des racines de P_1 était rationnelle, ce serait un entier divisant 7, ce qui ne laisse que 4 possibilités, dont aucune n'est racine de P_1. On en déduit que P_1 est irréductible sur $\mathbb{Q}$, et le degré de M sur $\mathbb{Q}$ est 3. On aurait aussi pu invoquer le critère d'Eisenstein pour le nombre premier 7.

b) Le discriminant $\Delta = -(4(-7)^3 + 27.7^2) = 49$ est un carré sur $\mathbb{Q}$. L'extension M/Q est galoisienne. Le groupe de Galois agit sur les trois racines de P_1 comme le groupe alterné : les deux automorphismes non triviaux de M permutent circulairement x_1, x_2 et x_3.

c) a) Le corps $\mathbb{Q}(y_1, y_2)$ est inclus dans $\mathbb{R}$ et ne peut donc contenir y_3 qui est imaginaire pur.

b) L'automorphisme de M qui envoie x_1 sur x_2 se prolonge en un automorphisme ψ de L qui envoie y_1 sur $\pm y_2$ et y_2 sur $\pm y_3$. Si $y_2 \in \mathbb{Q}(y_1)$, il existe une fraction rationnelle R coefficients dans $\mathbb{Q}$ telle que $R(y_1) = y_2$. En appliquant ψ, on trouve $R(\pm y_2) = \pm y_3$, donc $y_3 \in \mathbb{Q}(y_1, y_2)$, en contradiction avec la question précédente.

c) Le même raisonnement qu'au b) montre que $y_1 \notin M$ et $\mathbb{Q}(y_1)$ est quadratique sur M, donc de degré 6 sur $\mathbb{Q}$ (on peut aussi voir par le critère d'Eisenstein que P_2 est irréductible sur $\mathbb{Q}$). Les questions 2 b) et 2 a) montrent que $\mathbb{Q}(y_1, y_2)$ est une extension quadratique de $\mathbb{Q}(y_1)$ et L est une extension quadratique de $\mathbb{Q}(y_1, y_2)$. En conclusion, L/M est de degré 8 et $L/\mathbb{Q}$ de degré 24.

d) L est le corps de décomposition de P_2, c'est donc une extension galoisienne de $\mathbb{Q}$. Si elle était abélienne, tous ses sous-corps seraient galoisiens. Ce n'est pas le cas, puisque $\mathbb{Q}(y_1)$ ne contient pas le conjugué y_3 de y_1.

d) Le groupe $\mathrm{Gal}(L/M)$ est d'ordre 8. Pour tout élément τ de ce groupe, on a $\tau(x_i) = x_i$, donc $\tau(y_i) = \epsilon_i y_i$, avec $\epsilon_i = \pm 1$ pour $i \in \{1,2,3\}$. L'application qui τ associe le triplet $(\epsilon_1(\tau), \epsilon_2(\tau), \epsilon_3(\tau))$ induit donc un isomorphisme de $\mathrm{Gal}(L/M)$ sur $\{\pm 1\}^3$. Par exemple, le τ_1 de l'énoncé est l'image réciproque de $(-1,1,1)$ et le τ de l'énoncé est l'image réciproque de $(-1,-1,-1)$. Les 7 éléments non triviaux de $\mathrm{Gal}(L/M)$ sont les τ_i, les τ_i' et τ. Leurs corps fixes sont les 7 sous-corps de L contenant M et de degr 4 sur M. Le corps fixe de τ_1 est $\mathbb{Q}(y_2, y_3)$, celui de τ_1' est $\mathbb{Q}(y_1, y_2y_3)$. Enfin, le corps fixe de τ est $M(y_1y_2, y_2y_3)$.

e) L'élément ψ de G construit la question 3 b) envoie y_1 sur $\epsilon_2 y_2$, y_2 sur $\epsilon_3 y_3$ et y_3 sur $\epsilon_1 y_1$. En le composant gauche par l'élément de $\mathrm{Gal}(L/M)$ qui envoie y_i sur $\epsilon_i y_i$, on trouve l'élément σ de G cherché. Un élément de G est uniquement caractérisé par son action sur les y_i. On en déduit

$$\tau_1\sigma\tau_3 = \tau_3\sigma\tau_2 = \tau_2\sigma\tau_1 = \tau_3'\sigma\tau_2' = \tau_2'\sigma\tau_1' = \tau_1'\sigma\tau_3' = \sigma.$$

Quant $\tau_1\sigma^2\tau_1 = \tau_2'\sigma^2$, il n'a rien de remarquable... (Il y a une faute de frappe dans l'énoncé).

f) On a $x_1x_2x_3 = -7$, et $y_1y_2y_3 = \pm\sqrt{-7} \in L$. L'image de $\sqrt{-7}$ par σ est donc $\sqrt{-7}$. Le groupe de Galois de $L/\mathbb{Q}(\sqrt{-7})$ a 12 éléments, soit

$$H = \{Id, \sigma, \sigma^2, \tau_i', \tau_i'\sigma, \tau_i'\sigma^2\}.$$

Il est isomorphe au groupe alterné $\mathfrak{A}_4$.

g) Les 8 images $\pm y_1 \pm y_2 \pm y_3$ sont distinctes, puisque une égalité entre elles donnerait une relation linéaire entre y_1, y_2 et y_3 sur $\mathbb{Q}$. On en déduit que θ est de degré 8 sur $\mathbb{Q}$, et le groupe de Galois $\mathrm{Gal}(L/\mathbb{Q}(\theta)$ a 3 éléments : c'est $\{Id, \sigma, \sigma^2\}$, qui est cyclique d'ordre 3. On a vu plus haut que $\tau_1\sigma^2\tau_1^{-1} = \tau_1\sigma^2\tau_1 = \tau_2'\sigma^2$ n'est pas dans ce sous-groupe, qui n'est donc pas distingué.

h) Un sous-corps de $\mathbb{Q}(\theta)$ qui contient $\sqrt{-7}$ correspond un sous-groupe de H qui contient $\{Id, \sigma, \sigma^2\}$. Un tel sous-groupe, s'il n'est pas réduit $\{Id, \sigma, \sigma^2\}$, contient l'un des τ_i', par exemple τ_1', donc il contient aussi $\tau_2' = \sigma\tau_1'\sigma^2$ et $\tau_3' = \tau_1'\tau_2'$. Finalement, le groupe contient H tout entier, et il n'y a aucun corps intermédiaire entre $K(\theta)$ et $\mathbb{Q}(\sqrt{-7})$.

Exercice 19. Soit K un corps de caractéristique $p > 0$ et L une extension finie de K. On note K_s l'ensemble des éléments de L séparables sur K et K_r l'ensemble des $x \in L$ tels qu'il existe $k \in \mathbb{N}$ tel que $x^{p^k} \in K$.

a) Montrer que K_s et K_r sont des corps et $K_s \cap K_r = K$.

b) Soit $x \in L$. Montrer que $x \in K_s$ si et seulement si $K(x^p) = K(x)$.

c) Montrer que pour tout $x \in L$, il existe $k \in \mathbb{N}$ tel que $x^{p^k} \in K_s$.

d) Soit $x \in K_s$ et $P \in K[X]$ le polynôme minimal de x. Montrer que P est irréductible dans $K_r[X]$.

e) Montrer que $[L : K_r] \geq [K_s : K]$.

f) On suppose l'extension L/K normale et soit $G = \mathrm{Aut(L/K)}$.

i) Montrer que K_s/K est une extension galoisienne.

ii) Montrer que L/K_r est galoisienne de groupe de Galois G.

iii) Construire un isomorphisme $G \to \mathrm{Gal}(K_s/K)$.

Solution. a) Si $x, y \in K_s$ alors $K(x,y)$ est une extension séparable de K d'après le cours, donc xy^{-1} et $x - y$ sont dans K_s. Donc K_s est bien un corps. Si $x, y \in K_{pi}$, on peu prendre le même k quitte à prendre le max dans la définition de K_{pi}. Alors $(x-y)^{p^k} = x^{p^k} - y^{p^k} \in K$ puisque le frobenius est un morphisme d'anneau, et la même preuve fonctionne pour xy^{-1}. Donc K_{pi} est un corps.

Si $x \in K_s \cap K_{pi}$, alors x est racine de $P = X^{p^k} - x^{p^k} \in K[X]$. Donc le polynôme minimal de x divise P et, par séparabilité, est à racine simple dans une clôture algébrique. Or $P = (X-x)^{p^k}$ donc le polynôme minimal de x est $X - x$, et donc $x \in K$. La réciproque est évidente.

b) x est racine de $(X-x)^p = X^p - x^p \in K(x^p)[X]$. Si x est séparable sur K, il l'est aussi sur $K(x^p)$ et donc $Irr_{K(x^p)}x$ est séparable divisant $(X-x)^p$, c'est donc $X - x$, et donc $x \in K(x^p)$. Réciproquement, si x n'est pas séparable, le polynôme minimal de x sur K est de la forme $P = \sum_i a_i X^{pi}$ et donc x^p est racine de $\sum_i a_i X^i$ qui est de degré strictement inférieur à celui de P. Donc $[K(x^p) : K] < [K(x) : K]$, et donc $K(x^p) \neq K(x)$.

c) La suite décroissante d'extensions $K(x) \supset K(x^p) \supset K(x^{p^2}) \supset K(x^{p^3}) \supset \cdots$ doit être stationnaire (c'est une suite décroissante de sous-K-espaces vectoriels d'un espace vectoriel de dimension finie), et donc il existe k tel que $K(x^{p^k}) = K(x^{p^{k+1}})$, et donc $x^{p^k} \in K_s$ d'après la question précédente.

d) Si $Q = \sum b_i X^i$ est le polynôme minimal de x dans $K_{pi}[X]$, il existe k tel que pour tout i, $b_i^{p^k} \in K$. Soit $Q_0 = \sum b_i^{p^k} x^i \in K[X]$. Alors $Q_0(x^{p^k}) = Q(x)^{p^k} = 0$. Donc $[K(x^{p^k}) : K] \leq \deg(\mathrm{Q}_0) = \deg(\mathrm{Q})$. Or comme x est séparable sur K, d'après b), $[K(x^{p^k}) : K] = [K(x) : K] = \deg(\mathrm{P})$. On obtient donc $\deg(\mathrm{Q}) \geq \deg(\mathrm{P})$, ce qui prouve que P est irréductible dans $K_{pi}[X]$.

e) Comme K_s/K est séparable, elle admet un élément primitif $x \in K_s$. D'après la question précédente $[K_{pi}(x) : K_{pi}] = [K(x) : K] = [K_s : K]$. Comme $K_{pi}(x) \subset L$ on en déduit l'inégalité voulu (en fait, on a même la divisibilité).

f) i) K_s/K est une extension séparable par définition. Si $g \in G$ et $x \in K_s$ alors $g(x)$ a le même polynôme minimal sur K que x, donc est aussi dans K_s. Donc K_s est stable par G, donc c'est une extension normale.

ii) Si $g \in G$ et $x^{p^k} \in K$, alors $g(x)^{pk} = g(x^{p^k}) = x^{p^k}$, donc $g(x) = x$ par injectivité du frobenius. Donc $K_{pi} \subset L^G$. Réciproquement, soit $x \in L^G$. Il existe k tel que $x^{p^k} \in K_s$. Si $g \in \mathrm{Gal}(K_s/K)$, alors g se prolonge en un élément $\tilde{g}$ de G. On a alors $g(x^{p^k}) = \tilde{g}(x)^{p^k} = x^{p^k}$. Donc $x^{p^k} \in K_s^{\mathrm{Gal}(K_s/K)} = K$, et donc $x \in K_{[}pi$.

iii) La restriction à K_s définit un morphisme surjectif $\pi : G \to \mathrm{Gal}(K_s/K)$. Soit $g \in G$ tel que $\pi(g) = id$ et soit $x \in L$. Il existe k tel que $x^{p^k} \in K_s$. Donc $g(x^{p^k}) = x^{p^k}$. Or $g(x^{p^k}) = g(x)^{p^k}$, donc par injectivité du frobénius, $g(x) = x$. Donc g est l'identité, ce qui montre l'injectivité de π.
On en déduit en particulier $[L : K_{pi}] = [K_s : K]$.

Exercice 20. Soient K un corps et $P, Q \in K[X]$ deux polynômes non constants. On note n le degré de P et m le degré de Q. Soit L un corps de décomposition de $P \circ Q = P(Q(X))$. On suppose de plus que L/K est une extension séparable.

i) Montrer que L/K est une extension galoisienne.

ii) On note K_0 le sous-corps de L engendré par K et les racines de P contenues dans L. Montrer que K_0/K est une extension galoisienne.

iii) Montrer que $P \circ Q = \prod_{i=1}^n R_i$ où $R_1, \cdots, R_n \in K_0[X]$ sont des polynômes de degré m.

iv) En déduire que $[L : K]$ divise $n!(m!)^n$.

Solution. i) L/K est une extension de décomposition, c'est donc une extension normale. Comme elle est de plus supposée séparable, elle est galoisienne.

ii) Soit $\sigma \in \mathrm{Gal}(L/K)$, et x une racine de P dans L, alors $\sigma(x)$ est aussi une racine de P donc $\sigma(x) \in K_0$. On en déduit donc que K_0 est stable par $\mathrm{Gal}(L/K)$, donc K_0/K est une extension galoisienne.

iii) Si $P = P_1 P_2$ avec $P_1, P_2 \in K[X]$ et $deg(P_1 \geq 1)$. Le polynôme $P_1 \circ Q$ divise $P \circ Q$ donc a une racine α dans L. Alors $Q(\alpha)$ est une racine de P_1 dans L. On a donc montré que tout facteur non constant de P admettait une racine dans L. Comme L/K est galoisienne, P est donc scindé sur L et donc aussi sur K_0. Donc $P = \prod_{i=1}^n (X - \beta_i)$ dans $K_0[X]$.
Alors $P \circ Q = \prod_{i=1}^n (Q(X) - \beta_i)$ dans $K_0[X]$. Il suffit de poser $R_i = Q(X) - \beta_i$.

iv) On a $[L : K] = [L : K_0][K_0 : K]$. Comme K_0 est engendré par des racines de P qui est de degré n, $[K_0 : K]$ divise $n!$. Comme L est le corps de décomposition de $\prod_{i=1}^n R_i$ sur K_0, où chaque R_i est de degré m, $[L : K_0]$ divise $(m!)^n$.
D'où le résultat.

Exercice 21. Soit $K \subset L$ une extension galoisienne de corps tel que $G := \mathrm{Gal}(L/K)$ soit cyclique de cardinal n. On suppose de plus que K contient une racine ζ exactement $n$ième de 1. On veut montrer qu'il existe $a \in K$ tel que $L \simeq K[X]/(X^n - a)$.
Soit σ un générateur de G et $N : L \to K$ l'application qui à x associe $\prod_g g(x)$.

i) Soit $x \in L$ tel que $N(x) = 1$. Montrer que $\phi_x = id + x\sigma + \cdots + [x\sigma(x) \cdots \sigma^{n-2}(x)]\sigma^{n-1} : L \to L$ n'est pas nulle.

ii) Soit $y \in \mathrm{Im}\ \phi_x - \{0\}$. Montrer que $x = y/\sigma(y)$.

iii) Soit $b \in L$ tel que $b/\sigma(b) = \zeta$. Montrer que $L = K[b]$ et que $b^n \in K$.

iv) Conclure.

Solution. i) En considérant G comme une partie finie du L-espace vectoriel $\mathrm{End}_K(L)$ des endomorphismes K-linéaires de L, le théorème de Dedekind nous dit que G forme une famille libre de $\mathrm{End}_K(L)$ (la preuve est analogue à celle de l'exo 2f)). Donc la combinaison linéaire ne peut être nulle.

ii) Si $y = \phi_x(a)$,

$$x\sigma(y) = x\sigma\big(\sum_{i=0}^{n-1}\prod_{k=0}^{i-1}\sigma^k(x)\sigma^i(a)\big)$$

$$= \sum_{i=0}^{n-1} x\prod_{k=1}^{i}\sigma^k(x)\sigma^{i+1}(a)$$

$$= \sum_{i=0}^{n-1}\prod_{k=0}^{i}\sigma^k(x)\sigma^{i+1}(a).$$

Les termes de la somme finale sont ceux de y, décalés de 1. Il suffit donc de vérifier

$$\prod_{k=0}^{n-1}\sigma^k(x)\sigma^n(a) = a.$$

Or $\sigma^n = id$ et $\prod_{k=0}^{n-1}\sigma^k(x) = N(x) = 1$. D'où le résultat.

iii) Supposons $b \neq 0$ et $\sigma(b) = \zeta^{-1}b$. Comme $\zeta \in K$ est fixé par σ, on obtient par récurrence $\sigma^k(b) = \zeta^{-k}b$. Donc $\mathrm{Gal}(L/K[b]) =_G (b) = \{Id\}$ puisque ζ est une racine primitive $n$ième de 1, donc par le théorème d'Artin, $K[b] = L$. De plus $\sigma(b^n) = \sigma(b)^n = \zeta^{-n}b^n = b^n$, donc $b^n \in L^G = K$.

iv) Comme$\zeta \in K$, on a $N(\zeta) = \zeta^n = 1$, donc d'après i, il existe $y \in L$ tel que $b := \phi_x(y)$ soit non nul. Alors d'après ii), b satisfait la condition de iii). Posant $a = b^n$, $X^n - a$ est un polynôme annulateur de b, or $\deg(X^n - a) = n = [K[b] : K]$, donc $X^n - a$ est le polynôme minimal de b et $L = K[b]$ est le corps de rupture de $X^n - a$.