TD n°9.

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 $\mathbb{Q} \subset K \subset L$.

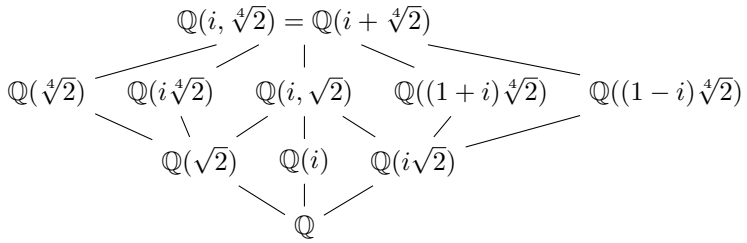
Solution. Le polynôme P est irréductible d'après le critère d'Eisenstein. L'ensemble des racines de P dans $\mathbb{C}$ est $\Omega := \{\zeta \sqrt[4]{2}, \zeta \in \mu_4\}$. Donc $\mathbb{Q}(\sqrt[4]{2})$ est un corps de rupture et $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ et le corps de décomposition 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 p un nombre premier.

a) Montrer qu'un groupe de cardinal p^2 est commutatif.

b) Montrer qu'un groupe de cardinal p^n est résoluble.

Indice : Commencer par montrer que le centre du groupe n'est pas réduit à l'élément neutre.

Solution. Si G est un p-groupe non trivial, considérons l'action de G sur lui-même par conjugaison. Les cardinaux des orbites divisent le cardinal de G, donc sont soit 1 soit divisible par p et la somme des cardinaux des orbites est le cardinal de G qui est divisible par p. Le nombre d'orbites de cardinal 1 est donc divisible par p. Or les orbites de cardinal 1 correspondent exactement aux éléments du centre, donc le cardinal du centre $Z(G)$ de G est divisible par p, donc est > 1.

a) Si $x \notin Z(G)$, le commutant de x contient $Z(G)$ et x donc c'est un sous-groupe de G contenant strictement $Z(G)$. Comme l'indice de $Z(G)$ divise p, on en déduit que le commutant de x est G, ce qui contredit l'hypothèse $x \notin Z(G)$. Donc G est commutatif.

b) $Z(G)$ est un sous-groupe distingué de G, il est commutatif donc résoluble. $G/Z(G)$ est un p-groupe d'ordre $<$ à celui de G, donc par réccurence $G/Z(G)$ est résoluble. G est alors résoluble en tant qu'extension d'un groupe résoluble par un groupe résoluble.

Exercice 5. 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 6. 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 7. 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 8. 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 9. 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 10. 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 $a^2 = \pm 13, \pm 8, \pm 7$ 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 $\Delta = 2^8 \cdot 3^3 \cdot 2^6 - 3^3 \cdot 2^{12} = 2^{12}3^4$ 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 :

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

donc

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

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.

2$^{\text{e}}$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

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

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 11. 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. (ı) 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)).
(ıı) Nous utilisons la même technique qu'à l'exercice précédent pour montrer que 12 divise l'ordre du groupe de Galois. 1re 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.
2e 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 $\mathrm{Gal}(f) = \mathfrak{S}_4$.
(ıı) 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 12. 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.