Correction : Groupes de Galois

Exercice 1.

Soit $P = X^5 - 6X + 3 \in \mathbb{Q}[X]$.

1. Par Eseinstein en réduisant modulo 3.
2. Puisque $P(-2) = -17$, $P(0) = 3$, $P(1) = -2$, $P(2) = 23$, par le théorème des valeurs intermédiaires, P a au moins trois racines réelles distinctes. Avec une étude rapide de sa dérivée, on remarque que P n'as pas de racine dans $\mathbb{R} \setminus [-2, 2]$, puis qu'il n'a pas d'autre racine dans $\mathbb{R}$. Il vient que P a trois racines réelles distinctes et deux racines complexes conjuguées.
3. Puisque P est irréductible, alors $[K : \mathbb{Q}] = |G|$. De plus, K contient un corps de rupture de P, qui est une sous-extension de degré 5 (car P est irréductible, donc tout corps de rupture est isomorphe à $\mathbb{Q}[X]/(P)$). Il vient que $|G|$ est multiple de 5, et G possède donc un élément d'ordre 5, c'est-à-dire un 5-cycle, $\sigma \in G$.

   La conjugaison complexe est un élément de G fixant 3 racines est permuttant les deux racines complexes conjuguées : elle réalise donc une transposition τ.

   On conclut avec le fait que $\mathfrak{S}_5$ est engendré par $\{\sigma, \tau\}$.
4. D'après la correspondance de Galois, les sous-extensions galoisiennes de L sont en bijection avec les sous-groupes distingués de $G = \mathfrak{S}_5$. Or, les seuls sous-groupe distingués de $\mathfrak{S}_5$ sont $\{\mathrm{id}\}$, $\mathfrak{A}_5$ et $\mathfrak{S}_5$.

   On en déduit que les sous-extensions galoisiennes de L sont
   (a) $K^{\{\mathrm{id}\}} = K$,
   (b) $K^{\mathfrak{A}_5}$. Remarquons que si z_0 est l'une des racines complexes de P, alors $\mathbb{Q}(z_0)$ est une sous-extension galoisienne de K, de degré 2. Donc $K^{\{\mathrm{id}\}} = \mathbb{Q}(z_0)$.
   (c) $K^{\mathfrak{S}_5} = \mathbb{Q}$.

Exercice 2.

1. Par hypothèse, l'extension Ω/K est de degré finie. C'est donc une extension algébrique. Puisque Ω est de caractéristique nulle, K aussi, et l'extension Ω/K est donc séparable. Enfin, elle est normale, car Ω est algébriquement clos.
2. Par le théorème de Cauchy, G possède un élément d'ordre p, qui engendre donc un sous-groupe de cardinal p, disons $H \simeq \mathbb{Z}/p\mathbb{Z}$. Alors d'après la correspondance de Galois, $L = \Omega^H$ est une sous-extension de $\Omega/K(i)$, avec Ω/L galoisienne, de groupe de Galois $H \simeq \mathbb{Z}/p\mathbb{Z}$. Ainsi Ω/L est-elle une extension galosienne de degré p.
3. On a Ω/L galoisienne, de groupe de galois cyclique d'ordre p. D'après le cours (Proposition 3.7 du poly), on peut trouver $\alpha \in \Omega$ tel que $a := \alpha^p \in L$ et $\Omega = L(\alpha)$. En particulier, $X^p - a$ est le polynôme minimal de α, et Ω est un corps de rupture de $X^p - a$.
4. On note $N(x) = \prod_{\sigma \in \mathrm{Gal}(\Omega/L)} \sigma(x)$. Soit $\alpha \in \Omega$ une racine de $X^p - a$. Remarquons que $\prod_{\sigma \in \mathrm{Gal}(\Omega/L)} (X - \sigma(\alpha))$ est un polynôme invariant sous l'action de $\mathrm{Gal}(\Omega/L)$, donc est à coefficient dans L. Il est de degré p et annule α : il est égal à son polynôme minimal $X^p - a$. En identifiant les coefficients constants, on a

$$-a = \prod_{\sigma \in \mathrm{Gal}(\Omega/L)} (-\sigma(\alpha)) = (-1)^p N(\alpha),$$

   et $N(\alpha) = (-1)^{p+1} a$

5. Supposons par l'absurde que $p \neq 2$. D'après la question précédente, $N(\alpha) = a$. Comme Ω est algébriquement clos, soit $\lambda \in \Omega$ avec $\alpha = \lambda^p$. Alors $a = N(\alpha) = N(\lambda)^p$, et $N(\lambda)$ est fixé par G, donc $N(\lambda) \in L$. Mais alors, $N(\lambda)$ est une racine de $X^p - a$ dans L, absurde.

   Ainsi, on a $p = 2$. Mais alors, $ia \in L$, car $i \in K(i) \subset L$ et $a \in L$. Soit λ une racine carrée de α dans Ω. Alors $\lambda^2 = \alpha$, d'où $N(\lambda)^2 = N(\alpha) = -a = (i\alpha)^2$. Il vient que $N(\lambda) \in \{i\alpha, -i\alpha\}$. Puisque $N(\lambda) \in L$, on a $i\alpha \in L$. Comme $i \in K(i) \subset L$, on a $\alpha \in L$, absurde.

   En conclusion, aucun nombre premier ne divise $|G|$, donc $[\Omega, K(i)] = 1$, et $\Omega = K(i)$.

Exercice 3.

Puisque K et x sont stabilisés par $\mathrm{Stab}(x)$, on a $K[x] \subset L^{\mathrm{Stab}(x)}$. Réciproquement, soit

Exercice 4.

On note $P = X^4 - 6 \in \mathbb{Q}[X]$. Dans $\overline{\mathbb{Q}}[X]$, on a $P = (X - \sqrt[4]{6})(X - i\sqrt[4]{6})(X + \sqrt[4]{6})(X + i\sqrt[4]{6})$.

1. Montrons $\mathbb{Q}(\sqrt[4]{6}, i) = \mathbb{Q}(\pm\sqrt[4]{2}, \pm i\sqrt[4]{6})$. C'est simplement dû au fait que $i, \sqrt[4]{6} \in \mathbb{Q}(\pm\sqrt[4]{2}, \pm i\sqrt[4]{6})$, et $i\sqrt[4]{6} \in \mathbb{Q}[\sqrt[4]{6}, i]$. Ainsi, $L = \mathbb{Q}(\sqrt[4]{6}, i)$ est un corps de décomposition de P.

   Puisque $L = \mathbb{Q}[\sqrt[4]{6}][i]$, on a $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{6})][\mathbb{Q}(\sqrt[4]{6}) : \mathbb{Q}]$.

   Remarquons que $\mathbb{Q}(\sqrt[4]{6})$ est un corps de rupture de P, qui est irréductible (par Eisenstein par exemple) : il vient que $[\mathbb{Q}(\sqrt[4]{6}) : \mathbb{Q}] = \deg(P) = 4$.

   Finalement, comme $i \notin \mathbb{Q}(\sqrt[4]{6})$, alors $X^2 + 1$ est le polynôme minimal de i sur $\mathbb{Q}(\sqrt[4]{6})$, et $[L : \mathbb{Q}(\sqrt[4]{6})] = 2$. Le résultat s'en suit.

2. Soit $s \colon L \to L$ la conjugaison complexe. C'est clairement un automorphisme de L fixant $\mathbb{Q}$ et vérifiant $s(i) = -i$, $s(\sqrt[4]{6}) = \sqrt[4]{6}$.

   Puisque G agit transitivement sur $\{\pm\sqrt[4]{6}, \pm i\sqrt[4]{6}\}$, soit $\rho \in G$ avec $\rho(\sqrt[4]{6}) = i\sqrt[4]{6}$. Alors $\rho(-\sqrt[4]{6}) = -i\sqrt[4]{6}$. Il vient que $\rho(i\sqrt[4]{6}) \in \{\pm\sqrt[4]{6}\}$.

   (a) Si $\rho(i\sqrt[4]{6}) = \sqrt[4]{6}$, alors $\rho(i) = \rho(\frac{i\sqrt[4]{6}}{\sqrt[4]{6}}) = \frac{\rho(i\sqrt[4]{6})}{\rho(\sqrt[4]{6})} = \frac{\sqrt[4]{6}}{i\sqrt[4]{6}} = -i$, et $r = s \circ \rho$ convient,

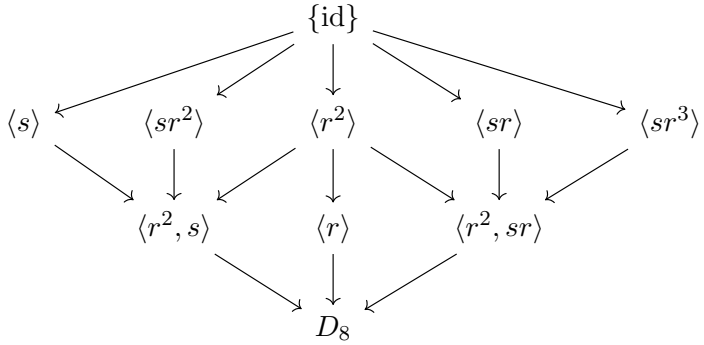
   (b) Si $\rho(\sqrt[4]{6}) = -\sqrt[4]{6}$, alors $\rho(i) = i$ et $r = \rho$ convient.

3. G est isomorphe à un sous-groupe de $\mathfrak{S}_4$ d'ordre 8, donc un 2-Sylow. Les sous-groupes de $\mathfrak{S}_4$ d'ordre 8 sont conjugués entre eux, donc tous isomorphes, en particulier au groupe diédral.

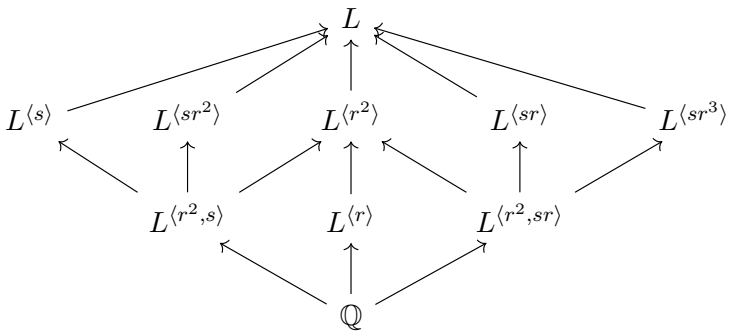
   Le résultat suit.

4. Remarquons que s, sr^2 sont conjugués d'ordre 2, sr et sr^3 sont conjugués d'ordre 2, et r^2 est d'ordre 2. On a donc 5 sous-groupes d'ordre 2, $\langle s \rangle$, $\langle sr^2 \rangle$, $\langle sr \rangle$ $\langle sr^3 \rangle$, et $\langle r^2 \rangle$. De plus, r est d'ordre 4 et engendre un sous-groupe d'ordre 4. Finalement, $\langle s, r^2$ et $\langle sr, r^2 \rangle$ sont deux sous-groupes d'ordre 4, isomorphes au groupe de Klein. On vérifie qu'il n'y a pas d'autres sous-groupes.

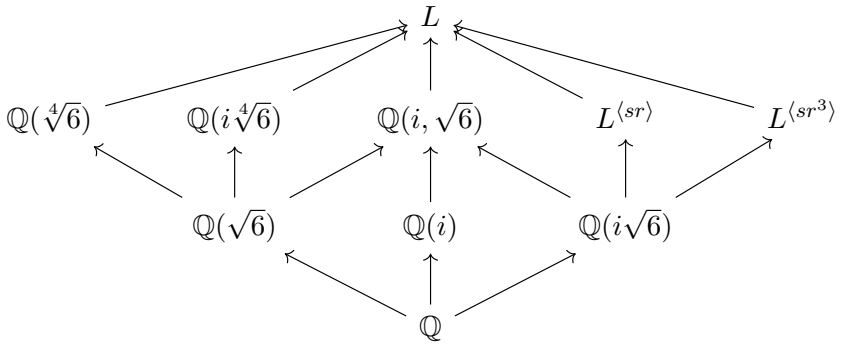
   On en déduit le treillis des sous-groupes de D_8 suivant



Tous saufs $\langle r\rangle$, $\langle sr^2\rangle$, $\langle sr\rangle$ et $\langle sr^3\rangle$ sont distingués.
D'après la correspondance de Galois, on a le treillis suivant des sous-extensions de L.



où les seules sous-extensions non galoisiennes sont $L^{\langle r\rangle}$, $L^{\langle sr^2\rangle}$, $L^{\langle sr\rangle}$ et $L^{\langle sr^3\rangle}$.
Dans L, les éléments i, $\sqrt{6} = (\sqrt[4]{6})^2$ et $i\sqrt{6} = i\cdot\sqrt{6}$ sont d'ordre 2. Donc $\mathbb{Q}(i), \mathbb{Q}(\sqrt{6})$ et $\mathbb{Q}(i\sqrt{6})$ sont des sous-extensions de L de degré 2. Puisque r fixe i, alors $L^{\langle r\rangle} = \mathbb{Q}(i)$. Remarquons que l'on a $r(\sqrt{6}) = \left(r(\sqrt[4]{6})\right)^2 = (i\sqrt[4]{6})^2 = -\sqrt{6}$, donc r^2 fixe $\sqrt{6}$. Comme s aussi, alors $L^{\langle r^2,s\rangle} = \mathbb{Q}(\sqrt{6})$. Il vient que $\mathbb{Q}(i\sqrt{6}) = L^{\langle r^2,sr\rangle}$. On a donc toutes les sous-extensions de degré 2.
Recherchons celles de degré 4. Tout d'abord, s stabilise $\sqrt[4]{6}$, qui est de degré 4. Donc $L^{\langle s\rangle} = \mathbb{Q}(\sqrt[4]{6})$. De la même manière, remarquons que $sr^2(i\sqrt[4]{6}) = i\sqrt[4]{6}$, et donc $L^{\langle sr^2} = \mathbb{Q}(i\sqrt[4]{6})$.
D'après les expressions trouvées pour $L^{\langle r^2,s\rangle}$ et $L^{\langle r\rangle}$, on a $L^{\langle r^2\rangle} = \mathbb{Q}(i,\sqrt{6})$.



Les seules sous-extensions galoisiennes de L sont donc dans le diagramme suivant