Feuille 9 – Correspondance galoisienne : illustrations

Exercice 1. Déterminer le groupe de Galois des polynômes et extensions de corps suivants, puis expliciter la correspondance de Galois dans chaque cas, en donnant des générateurs de chaque extension intermédiaire :

1. Le polynôme $X^5 - 2$ sur $\mathbb{Q}$.
2. L'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.
3. L'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$.
4. L'extension $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}$, où $\alpha = (2+\sqrt{2})(3+\sqrt{6})$ (on commencera par étudier $\mathbb{Q}(\alpha)/\mathbb{Q}$).
5. Le polynôme $X^8 - 2$ sur $\mathbb{Q}$.

Correction.

1. **Cardinal du groupe de Galois.** Le corps de décomposition de $X^5 - 2$ est $K = \mathbb{Q}(\sqrt[5]{2}, \zeta)$ où ζ est une racine primitive 5-ième de l'unité. Il est de degré 20 sur $\mathbb{Q}$: en effet, on a :

$$[K : \mathbb{Q}] = [\mathbb{Q}(\zeta)(\sqrt[5]{2}) : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}] = 4[\mathbb{Q}(\zeta)(\sqrt[5]{2}) : \mathbb{Q}(\zeta)],$$

et le polynôme $X^5 - 2$ étant irréductible sur $\mathbb{Q}$ (et même sur $\mathbb{Z}$, on le montre par exemple grâce au critère d'Eisenstein), il l'est également sur $\mathbb{Q}(\zeta)$ (voir TD8, exercice 4 : on a $d = 1$ ici). Autrement dit, $\mathbb{Q}(\zeta)(\sqrt[5]{2})/\mathbb{Q}(\zeta)$ est le corps de rupture de $X^5 - 2$ sur $\mathbb{Q}(\zeta)$, donc $[\mathbb{Q}(\zeta)(\sqrt[5]{2}) : \mathbb{Q}(\zeta)] = 5$, et on obtient le degré annoncé. Le groupe de Galois de $K/\mathbb{Q}$ est donc de cardinal 20. Notons-le G.

Structure du groupe de Galois. Précisons ses éléments : on a la suite d'extensions monogènes

$$\mathbb{Q} \subseteq \mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\zeta)(\sqrt[5]{2}) = K.$$

Il existe 4 $\mathbb{Q}$-morphismes $\sigma_j : \mathbb{Q}(\zeta) \to \bar{\mathbb{Q}}$ caractérisés par l'image de ζ, qui doit être une racine de son polynôme minimal Φ_5, c'est-à-dire une autre racine primitive de l'unité (donc de la forme ζ^j pour $j \in (\mathbb{Z}/5\mathbb{Z})^*$). Chacun de ces morphismes σ_j se prolonge de 5 manières différentes en un $\mathbb{Q}$-morphisme $\sigma_{j,k} : K \to \bar{\mathbb{Q}}$ caractérisé par l'image de $\sqrt[5]{2}$, qui doit être une racine de son polynôme minimal sur $\mathbb{Q}(\zeta)$ (on a vu qu'il s'agissait de $X^5 - 2$), donc $\zeta^k \sqrt[5]{2}$ pour $k \in \mathbb{Z}/5\mathbb{Z}$. Comme $K/\mathbb{Q}$ est une extension normale, on a $\sigma_{j,k}(K) = K$, donc $\sigma_{j,k} \in G$ pour tout $(j,k) \in (\mathbb{Z}/5\mathbb{Z})^* \times \mathbb{Z}/5\mathbb{Z}$. On a exhibé 20 éléments de G, donc on les a tous :

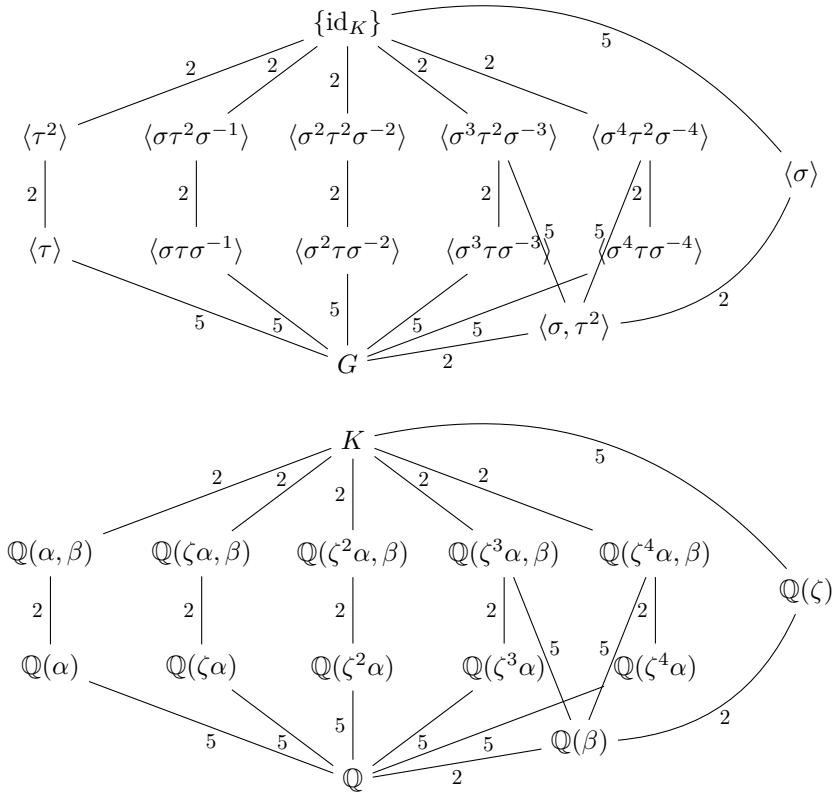
$$G = \left\{ \sigma_{j,k} : \left| \begin{array}{ccc} K & \to & K \\ \zeta & \mapsto & \zeta^j \\ \sqrt[5]{2} & \mapsto & \zeta^k \sqrt[5]{2} \end{array} \right. , (j,k) \in (\mathbb{Z}/5\mathbb{Z})^* \times \mathbb{Z}/5\mathbb{Z} \right\},$$

qui est manifestement engendré par $\tau = \sigma_{2,0}$ et $\sigma = \sigma_{1,1}$ (notons que 2 engendre $(\mathbb{Z}/5\mathbb{Z})^*$), donc $G = \langle \sigma, \tau \rangle$ (il est difficile d'avoir une plus jolie description).

Sous-groupes du groupe de Galois. Il est de cardinal $20 = 2^2 \cdot 5$, donc les ordres de ses sous-groupes sont dans {1,2,4,5,10,20} par le théorème de Lagrange. Étudions toutes ces éventualités :
– Ordres 1 et 20 : il s'agit des sous-groupes triviaux $\{\mathrm{id}_K\}$ et G.
– Ordre 5 : il s'agit des 5-sous-groupes de Sylow de G. On peut les compter grâce aux théorèmes de Sylow : on a $n_5 \equiv 1 \bmod 5$ et $n_5 | 4$ (où n_5 est le nombre de 5-Sylow), donc $n_5 = 1$. Il n'y a qu'un seul 5-sous-groupe de Sylow (qui est donc distingué), et il s'agit de $\langle \sigma \rangle$. On pouvait aussi montrer l'unicité en se souvenant que G est un sous-groupe de $\mathfrak{S}_5$, qui n'a qu'un seul sous-groupe d'ordre 5 (engendré par le 5-cycle (12345)).

– Ordre 4 : il s'agit des 2-sous-groupes de Sylow de G (remarquons que $\langle\tau\rangle$ en est un). On peut les compter grâce aux théorèmes de Sylow : on a $n_2 \equiv 1 \bmod 2$ et $n_2|5$, donc $n_2 \in \{1,5\}$. Mais si $n_2 = 1$, alors tous les sous-groupes de Sylow de G sont distingués, et comme ils sont d'intersection triviale on en déduit que G est isomorphe à leur produit ; mais la description donnée montre qu'ils sont abéliens, donc G serait abélien : absurde. Donc $n_2 = 5$. Les 2-sous-groupes de Sylow sont tous conjugués, ils sont donc de la forme $\langle\sigma^n\tau\sigma^{-n}\rangle$, pour $n \in \mathbb{Z}/5\mathbb{Z}$.
– Ordre 2 : ces groupes sont engendrés par des éléments d'ordre 2. Il n'y en a que cinq, puisque les éléments d'ordre 1, 4 et 5 épuisent déjà le cardinal de G : on a 1 élément d'ordre 1 (l'élément neutre), 10 éléments d'ordre 4 (chaque 2-sous-groupe de Sylow est cyclique, donc admet deux éléments d'ordre 4) et 4 éléments d'ordre 5 (ceux de $\langle\sigma\rangle$), donc il y a au plus $20-1-10-4=5$ éléments d'ordre 2. Il s'agit précisément des éléments d'ordre 2 contenus dans les 2-Sylow, qui engendrent les sous-groupes conjugués $\langle\sigma^n\tau^2\sigma^{-n}\rangle$, pour $n \in \mathbb{Z}/5\mathbb{Z}$.
– Ordre 10 : l'étude précédente montre qu'il n'y a pas d'élément d'ordre 10, donc un sous-groupe d'ordre 10 est nécessairement engendré par un élément d'ordre 5 et un élément d'ordre 2. Peu importent les éléments qu'on choisit, on obtient dans tous les cas l'unique sous-groupe $\langle\sigma,\tau^2\rangle$ (qui est distingué).

Correspondance de Galois. On obtient la correspondance de Galois suivante entre sous-groupes et de sous-corps (on note $\alpha = \sqrt[5]{2}$ et $\beta = \zeta + \zeta^{-1} = \frac{\sqrt{5}-1}{2}$ pour alléger les notations) :

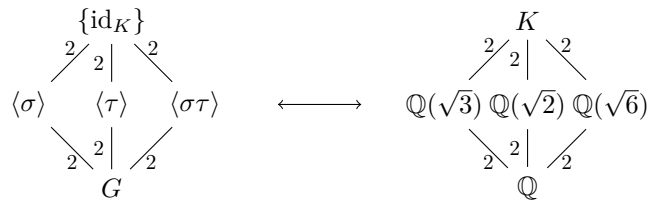


Montrons, par exemple, comment on obtient $K^{\langle\tau\rangle}$, $K^{\langle\tau^2\rangle}$, $K^{\langle\sigma\rangle}$ et $K^{\langle\sigma,\tau^2\rangle}$. Les deux premiers corps sont faciles à déterminer : d'une part, par définition τ fixe $\mathbb{Q}(\alpha)$ qui est de degré 5 sur $\mathbb{Q}$, comme $K^{\langle\tau\rangle}$ (ainsi que le prédit le théorème de correspondance de Galois), donc $K^{\langle\tau\rangle} = \mathbb{Q}(\alpha)$ par égalité des degrés et inclusion ; d'autre part, $\tau^2(\zeta) = \zeta^{-1} = \bar{\zeta}$ n'est rien d'autre que la conjugaison complexe, donc τ^2 fixe $\beta = \zeta + \zeta^{-1}$. On a $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha,\beta) \subseteq K^{\langle\tau^2\rangle}$, et β n'appartient pas à $\mathbb{Q}(\alpha)$

(il n'est pas invariant par τ), donc $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)]>1$ et $K^{\langle\tau^2\rangle}=\mathbb{Q}(\alpha,\beta)$ en comparant les degrés. On procède semblablement pour les deux corps suivants : par définition σ fixe $\mathbb{Q}(\zeta)$, donc $\mathbb{Q}(\zeta)\subseteq K^{\langle\sigma\rangle}$ et les deux corps sont de degré 4 sur $\mathbb{Q}$, d'où l'égalité. Alors, les éléments de $K^{\langle\sigma,\tau^2\rangle}$ sont les réels inclus dans $\mathbb{Q}(\zeta)$, c'est-à-dire $K^{\langle\sigma,\tau^2\rangle}=\mathbb{Q}(\beta)$.
On en déduit $K^{\langle\sigma^k\tau\sigma^{-k}\rangle}$ et $K^{\langle\sigma^k\tau^2\sigma^{-k}\rangle}$ presque immédiatement : comme τ est le 4-cycle $(\zeta\alpha,\zeta^2\alpha,\zeta^4\alpha,\zeta^3\alpha)$, son conjugué $\sigma^k\tau\sigma^{-k}$ égale $(\sigma^k(\zeta\alpha),\sigma^k(\zeta^2\alpha),\sigma^k(\zeta^4\alpha),\sigma^k(\zeta^3\alpha))$, donc son seul point fixe parmi les racines est $\sigma^k(\alpha)=\zeta^k\alpha$, et on conclut comme ci-dessus avec les degrés. On procède de même avec $\tau^2=(\zeta\alpha,\zeta^4\alpha)(\zeta^2\alpha,\zeta^3\alpha)$. Nous avons traité tous les corps intermédiaires.

Remarquons qu'il existe une méthode systématique, étant donnée une extension galoisienne L/K de groupe de Galois G, pour déterminer L^H où $H\subseteq G$ (une fois qu'on a déterminé G explicitement) : en effet, si on connaît *a priori* l'action de G sur les éléments $x_1,\dots,x_n$ qui engendrent L sur K, alors on connaît aussi l'action de G sur une K-base de L de la forme $(x_1^{k_1}\cdots x_n^{k_n})_{k_1,\dots,k_n}$. De fait, pour $x\in L^H$, le système d'équations $\{\sigma(x)=x,\sigma\in H\}$ est un système linéaire qu'on peut résoudre systématiquement (par le pivot de Gauss par exemple). Nous n'avons pas procédé ainsi dans cet exemple, parce qu'il était plus rapide de reconnaître des éléments primitifs fixés par les automorphismes en jeu.
Enfin : nous avons, pour $\langle\tau\rangle$ et $\langle\tau^2\rangle$, commencé par chercher les points fixes du plus grand groupe (obtenant ainsi d'abord le plus petit corps), et nous avons procédé dans l'autre sens pour $\langle\sigma\rangle$ et $\langle\sigma,\tau^2\rangle$, afin de permettre de comparer les deux approches.

2. **Cardinal du groupe de Galois.** Le groupe de Galois G de $K/\mathbb{Q}=\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ est de cardinal
$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}),\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=4;$$
on vérifie en effet immédiatement que $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$, puisque cela impliquerait une égalité du type $3=(a+b\sqrt{2})^2=(a^2+2b^2)+2ab\sqrt{2}$ avec a,b rationnels, et par liberté de la $\mathbb{Q}$-famille $(1,\sqrt{2})$ on aurait $3=a^2+2b^2$ et $ab=0$, qui mène rapidement à une contradiction.
Structure du groupe de Galois. On a la suite d'extensions monogènes $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{2})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})=K$. Il existe 2 $\mathbb{Q}$-morphismes $\sigma_\varepsilon:\mathbb{Q}(\sqrt{2})\to\bar{\mathbb{Q}}$ caractérisés par l'image de $\sqrt{2}$, qui doit être une racine de son polynôme minimal X^2-2, c'est-à-dire $\varepsilon\sqrt{2}$ avec $\varepsilon\in\{\pm1\}$. Chacun de ces morphismes σ_ε se prolonge de 2 manières différentes en un $\mathbb{Q}$-morphisme $\sigma_{\varepsilon,\varepsilon'}:K\to\bar{\mathbb{Q}}$ caractérisé par l'image de $\sqrt{3}$, qui doit être une racine de son polynôme minimal sur $\mathbb{Q}(\sqrt{2})$ (qui est X^2-3), donc $\varepsilon'\sqrt{3}$ avec $\varepsilon'\in\{\pm1\}$. Comme $K/\mathbb{Q}$ est une extension normale, on a $\sigma_{\varepsilon,\varepsilon'}(K)=K$, donc $\sigma_{\varepsilon,\varepsilon'}\in G$ pour tout $(\varepsilon,\varepsilon')\in\{\pm1\}^2$. On a exhibé 4 éléments de G, donc on les a tous :
$$G=\left\{\sigma_{\varepsilon,\varepsilon'}:\left|\begin{array}{ccc}K&\to&K\\ \sqrt{2}&\mapsto&\varepsilon\sqrt{2}\\ \sqrt{3}&\mapsto&\varepsilon'\sqrt{3}\end{array}\right.,(\varepsilon,\varepsilon')\in\{\pm1\}^2\right\},$$
qui est engendré par $\sigma=\sigma_{-1,1}$ et $\tau=\sigma_{1,-1}$, lesquels sont d'ordre 2, donc $G=\langle\sigma,\tau\rangle\simeq(\mathbb{Z}/2\mathbb{Z})^2$.
Sous-groupes du groupe de Galois. Il existe trois groupes non triviaux, ce sont ceux engendrés par les éléments d'ordre 2, à savoir $\langle\sigma\rangle$, $\langle\tau\rangle$ et $\langle\sigma\tau\rangle$.
Correspondance de Galois. On obtient la correspondance de Galois suivante :

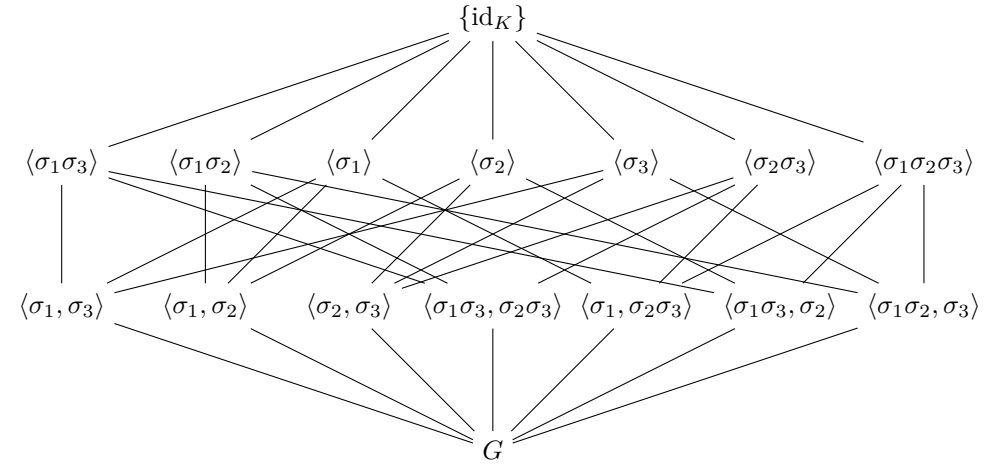


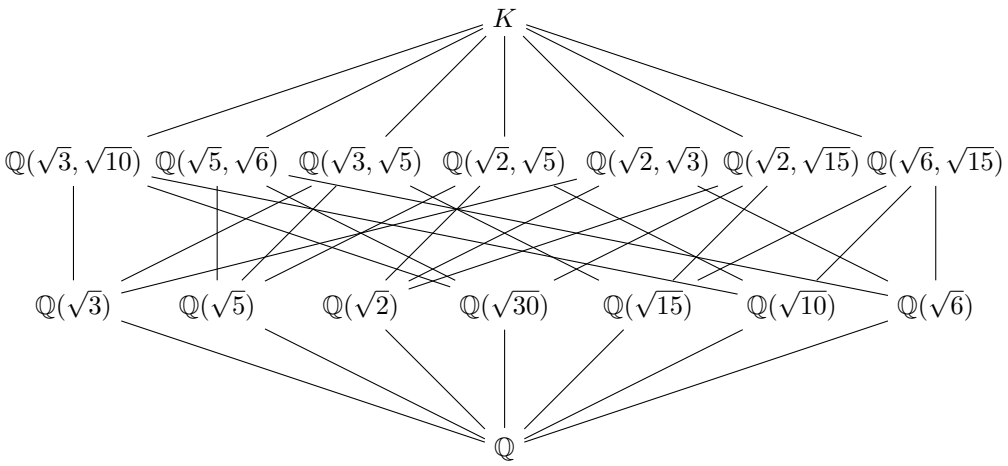
La détermination des corps de points fixes est immédiate, sauf peut-être pour $\langle\sigma\tau\rangle$: illustrons le procédé systématique sur cet exemple simple. Si $x \in K^{\langle\sigma\tau\rangle}$ s'écrit $x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}$ (les coefficients sont dans $\mathbb{Q}$), alors :

$$\sigma\tau(x) = x \iff a - b\sqrt{2} - c\sqrt{3} + d\sqrt{2}\sqrt{3} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \iff b = c = 0$$

par liberté de la famille $(1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3})$. D'où $K^{\langle\sigma\tau\rangle} = \mathbb{Q}(\sqrt{6})$.

3. **Cardinal du groupe de Galois.** Le même traitement que ci-dessus montre que le groupe de Galois G de $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ sur $\mathbb{Q}$ est de cardinal 8.
Structure du groupe de Galois. Le même traitement que ci-dessus montre que le groupe de Galois G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$, engendré par les automorphismes $\sigma_1 = \sigma_{-1,1,1}$, $\sigma_2 = \sigma_{1,-1,1}$ et $\sigma_3 = \sigma_{1,1,-1}$, où $\sigma_{\varepsilon,\varepsilon',\varepsilon''}$ est défini par $\begin{cases} K & \to & K \\ \sqrt{2} & \mapsto & \varepsilon\sqrt{2} \\ \sqrt{3} & \mapsto & \varepsilon'\sqrt{3} \\ \sqrt{5} & \mapsto & \varepsilon''\sqrt{5} \end{cases}$.
Sous-groupes du groupe de Galois. Il existe 7 groupes d'ordre 2, ce sont ceux engendrés par les éléments d'ordre 2, à savoir les $\langle\sigma_i\rangle$ pour $i \in \{1,2,3\}$, $\langle\sigma_i\sigma_j\rangle$ pour i, j distincts dans $\{1,2,3\}$, et $\langle\sigma_1\sigma_2\sigma_3\rangle$. Il existe 7 groupes d'ordre 4, engendrés par deux éléments d'ordre 2.
Correspondance de Galois. On obtient la correspondance de Galois suivante :





4. L'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ n'est rien d'autre que l'extension $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ déjà étudiée, galoisienne et de groupe de Galois $(\mathbb{Z}/2\mathbb{Z})^2$. Soient σ_i, σ_j et σ_k ses éléments d'ordre 2 ; ils fixent respectivement $\sqrt{2}$, $\sqrt{3}$ et $\sqrt{6}$ en envoyant les deux autres racines carrées sur leurs opposés. Ceci permet de remarquer que $\frac{\sigma(\alpha)}{\alpha}$ est toujours le carré d'un élément de $\mathbb{Q}(\alpha)$, par exemple :

$$\frac{\sigma_i(\alpha)}{\alpha} = \frac{3-\sqrt{6}}{3+\sqrt{6}} = \left(\frac{\sqrt{3}}{3+\sqrt{6}}\right)^2.$$

En particulier, $\sqrt{\alpha} \notin \mathbb{Q}(\alpha)$, sinon on aurait $\sigma_i(\sqrt{\alpha}) = \sqrt{\alpha}$, mais aussi $\sigma_i(\sqrt{\alpha}) = \left(\pm\frac{\sqrt{3}}{3+\sqrt{6}}\right)\sqrt{\alpha} \neq \sqrt{\alpha}$ (et cela vaut de même pour σ_j et σ_k). L'extension $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}(\alpha)$ est donc galoisienne de degré 2, et son groupe de Galois est isomorphe à $\mathbb{Z}/2\mathbb{Z}$, engendré par un élément τ, qu'on voit désormais comme un élément de $G = \mathrm{Gal}(\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q})$ *.

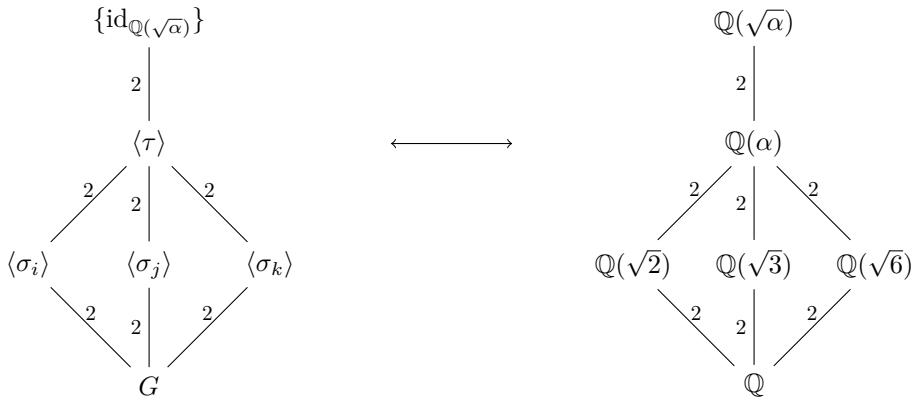
Maintenant, les $\mathbb{Q}$-morphismes $\sigma : \mathbb{Q}(\alpha) \to \bar{\mathbb{Q}}$ se prolongent en des morphismes encore notés $\sigma : \mathbb{Q}(\sqrt{\alpha}) \to \bar{\mathbb{Q}}$ en envoyant $\sqrt{\alpha}$ sur une racine de $X^2 - \sigma(\alpha)$. On peut donc prolonger σ_i et σ_j à $\mathbb{Q}(\sqrt{\alpha})$ en posant

$$\sigma_i(\sqrt{\alpha}) = \frac{\sqrt{3}}{3+\sqrt{6}}\sqrt{\alpha} \text{ et } \sigma_j(\sqrt{\alpha}) = \frac{\sqrt{6}}{(2+\sqrt{2})(3+\sqrt{6})}\sqrt{\alpha},$$

puis $\sigma_k = \sigma_i\sigma_j$. Un calcul direct montre alors que $\sigma_i^2(\sqrt{\alpha}) = \sigma_j^2(\sqrt{\alpha}) = \sigma_k^2(\sqrt{\alpha}) = -\sqrt{\alpha}$, donc $\sigma_i^2 = \sigma_j^2 = \sigma_k^2 = \tau$, mais aussi $\sigma_i\sigma_j\sigma_k = \tau$ et $\tau^2 = \mathrm{id}_{\mathbb{Q}(\sqrt{\alpha})}$: on reconnaît la table de multiplication des quaternions. On a donc $G \simeq \mathbb{H} = \{\pm 1, \pm i, \pm j, \pm k\}$, où τ est envoyé sur -1, et i et j envoyés sur les automorphismes (nommés de manière très suggestive) σ_i et σ_j.

Sous-groupes du groupe de Galois. Les sous-groupes non triviaux de $\mathbb{H}$ sont bien connus (ils ont la particularité, notamment, d'être tous cycliques et distingués), il s'agit de $\langle -1\rangle$ (d'ordre 2), $\langle i\rangle$, $\langle j\rangle$ et $\langle k\rangle$ (d'ordres 4).

Correspondance de Galois. On obtient :



Les définitions de σ_i et σ_j donnent immédiatement les extensions quadratiques de $\mathbb{Q}$. Enfin, le corps des points fixes de τ est bien entendu $\mathbb{Q}(\alpha)$, puisque par définition τ engendre le groupe de Galois de $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}(\alpha)$.

∗. Notons que $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}$ est bien galoisienne : il suffit de vérifier que tous ses conjugués sont bien dans $\mathbb{Q}(\sqrt{\alpha})$, et c'est le cas ; on vérifie aisément que ses conjugués sont $-\sqrt{\alpha}$ et les $\pm\sqrt{\sigma_i(\alpha)}$, $\pm\sqrt{\sigma_j(\alpha)}$ et $\pm\sqrt{\sigma_k(\alpha)}$ (on change tous les signes possibles dans les racines carrées), et le calcul précédent montre bien que toutes ces quantités restent dans $\mathbb{Q}(\sqrt{\alpha})$.

5. **Cardinal du groupe de Galois.** Le corps de décomposition de X^8-2 sur $\mathbb{Q}$ est $K=\mathbb{Q}(\sqrt[8]{2},\zeta)$, où $\zeta=\exp\left(\frac{2i\pi}{8}\right)$ est une racine primitive 8-ième de l'unité. Remarquons que $\zeta=\frac{\sqrt{2}}{2}(1+i)$ (on peut le démontrer par de pures manipulations algébriques), donc en vérité $K=\mathbb{Q}(\sqrt[8]{2},i)$. Il est de degré :
$$[K:\mathbb{Q}]=[\mathbb{Q}(i,\sqrt[8]{2}):\mathbb{Q}(\sqrt[8]{2})][\mathbb{Q}(\sqrt[8]{2}):\mathbb{Q}]=2\cdot 8=16,$$
car X^2+1 est clairement sans racine sur $\mathbb{Q}(\sqrt[8]{2})$, donc est le polynôme minimal de i sur ce corps.

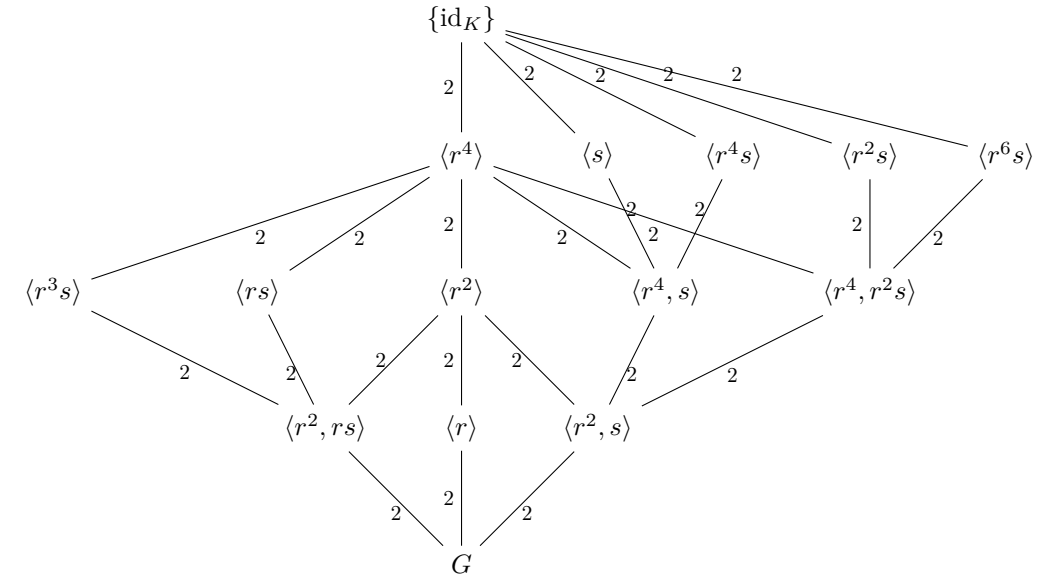
Remarque importante : on pourrait préférer travailler avec ζ plutôt que i, en utilisant son polynôme minimal $X^2-\sqrt{2}X+1$ sur $\mathbb{Q}(\sqrt[8]{2})$ † pour déterminer l'image par un automorphisme de G de ζ, mais attention cependant : un examen attentif de la démonstration du théorème de prolongement des morphismes montre qu'un prolongement d'un morphisme $\sigma:\mathbb{Q}(\sqrt[8]{2})\to\bar{\mathbb{Q}}$ à $K=\mathbb{Q}(\sqrt[8]{2},\zeta)\to\bar{\mathbb{Q}}$ *n'envoie pas* ζ sur une racine de son polynôme minimal sur $\mathbb{Q}(\sqrt[8]{2})$, qui est $X^2-\sqrt{2}X+1$, mais sur une racine de $\sigma(X^2-\sqrt{2}X+1)$, qui peut être $X^2+\sqrt{2}X+1$ si par exemple $\sigma(\sqrt[8]{2})=\zeta\sqrt[8]{2}$! En particulier, *il n'existe pas* de $\sigma:K\to K$ défini par $\sigma(\sqrt[8]{2})=\zeta\sqrt[8]{2}$ et $\sigma(\zeta)=\zeta$ (il est facile de montrer qu'on aurait alors $\sigma(\zeta)=-\sigma(\zeta)$). Au moins, comme le polynôme de minimal de i sur $\mathbb{Q}(\sqrt[8]{2})$ est X^2+1, et qu'il est invariant par tout $\mathbb{Q}$-morphisme, le prolongement de morphismes n'apporte pas de complications avec i au lieu de ζ (mais ce n'est pas obligatoire : le lecteur en exercice pourra tenter de poursuivre ce travail en persistant avec ζ).

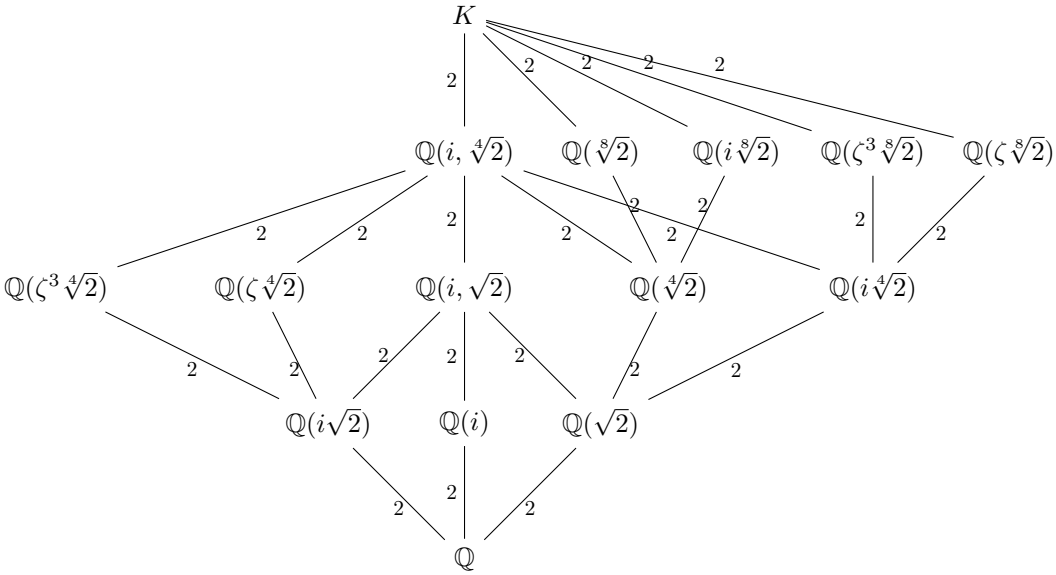
Structure du groupe de Galois. On a la suite d'extensions monogènes
$$\mathbb{Q}\subseteq\mathbb{Q}(\sqrt[8]{2})\subseteq\mathbb{Q}(\sqrt[8]{2},i)=K.$$
Il existe 8 $\mathbb{Q}$-morphismes $\sigma_j:\mathbb{Q}(\sqrt[8]{2})\to\bar{\mathbb{Q}}$ caractérisés par l'image de $\sqrt[8]{2}$, qui doit être une racine de son polynôme minimal X^8-2, c'est-à-dire $\zeta^j\sqrt[8]{2}$ avec $j\in\mathbb{Z}/8\mathbb{Z}$. Chacun de ces morphismes σ_j se prolonge de 2 manières différentes en un $\mathbb{Q}$-morphisme $\sigma_{j,\varepsilon}:K\to\bar{\mathbb{Q}}$ caractérisé par l'image de i, qui doit être une racine de son polynôme minimal sur $\mathbb{Q}(\sqrt[8]{2})$ (c'est-à-dire X^2+1), donc εi avec $\varepsilon\in\{\pm 1\}$. Comme $K/\mathbb{Q}$ est une extension normale, on a $\sigma_{j,\varepsilon}(K)=K$, donc $\sigma_{j,\varepsilon}\in G$ pour tout $(j,\varepsilon)\in\mathbb{Z}/8\mathbb{Z}\times\{\pm 1\}$. On a exhibé 16 éléments de G, donc on les a tous :
$$G=\left\{\sigma_{j,\varepsilon}:\left|\begin{array}{ccc}K&\to&K\\ \sqrt[8]{2}&\mapsto&\zeta^j\sqrt[8]{2}\\ i&\mapsto&\varepsilon i\end{array}\right.,(j,\varepsilon)\in\mathbb{Z}/8\mathbb{Z}\times\{\pm 1\}\right\},$$
qui est engendré par $r=\sigma_{1,1}$ et $s=\sigma_{0,-1}$: on a $G=\langle r,s\rangle$ (on peut même préciser la structure : on vérifie que $srs=r^3$, et ceci permet d'écrire un produit semi-direct $G\simeq\mathbb{Z}/8\mathbb{Z}\rtimes\mathbb{Z}/2\mathbb{Z}$ où le produit est tordu par l'application $\mathbb{Z}/2\mathbb{Z}\to\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z})\simeq\{\pm 1,\pm 3\}$ qui envoie 1 sur 3).

Sous-groupes du groupe de Galois. Les sous-groupes de G sont, d'après le théorème de Lagrange, d'ordre 1, 2, 4, 8 ou 16, et grâce à la formule $srs=r^3$ on peut calculer simplement les puissances de r^ks pour tout $k\in\mathbb{Z}/8\mathbb{Z}$ (par exemple : $(r^3s)^2=r^3(sr^3s)=r^{12}=r^4$, donc $(r^3s)^4=1$). On voit aussi que r^2 est dans le centre de G (il l'engendre même).
- Ordres 1 et 16 : il s'agit des sous-groupes triviaux.
- Ordre 2 : ils sont engendrés par les éléments d'ordre 2, c'est-à-dire r^4, s, r^2s, r^4s et r^6s.
- Ordre 4 : ils sont soit cycliques, donc engendrés par un élément d'ordre 4 (donc : $\langle r^2\rangle$, $\langle rs\rangle$ et $\langle r^3s\rangle$), soit engendrés par deux éléments d'ordre 2 qui commutent (donc : $\langle r^4,s\rangle$ et $\langle r^4,r^2s\rangle$).
- Ordre 8 : on a $\langle r\rangle$, $\langle r^2,rs\rangle$ et $\langle r^2,s\rangle$.

Correspondance de Galois. On obtient :

†. On l'obtient à l'aide de l'expression de ζ ci-dessus, car $i=\zeta^2$, ou en constatant que $X^4+1=(X^2+1)^2-2X^2=(X^2+1-\sqrt{2}X)(X^2+1+\sqrt{2}X)$; les relations coefficients-racines et le fait que $\bar{\zeta}$ doit être racine du même polynôme réel permettent d'éliminer $X^2+\sqrt{2}X+1$.





Comme r fixe i par définition, on a $K^{\langle r\rangle} = \mathbb{Q}(i)$ (égalité des degrés). De plus, $r(\zeta) = -\zeta$, donc r^2 fixe ζ, et encore une fois on en déduit $K^{\langle r^2\rangle} = \mathbb{Q}(\zeta)$ (qu'il est plus commode d'écrire $\mathbb{Q}(i, \sqrt{2})$ selon les cas de figure) grâce aux degrés. On voit facilement que $r^4(\sqrt[8]{2}) = -\sqrt[8]{2}$, donc r^4 fixe $\sqrt[4]{2}$ en plus de i, et $K^{\langle r^4\rangle} = \mathbb{Q}(i, \sqrt[4]{2})$. On remarque que s est la conjugaison complexe, donc ses points fixes sont des nombres réels de K, c'est-à-dire $\mathbb{Q}(\sqrt[8]{2})$. Ainsi, les points fixes de r^2 et s sont dans $\mathbb{Q}(\sqrt{2}, i) \cap \mathbb{R} = \mathbb{Q}(\sqrt{2})$, et de même on en déduit que $K^{\langle r^4, s\rangle} = \mathbb{Q}(\sqrt[4]{2}, i) \cap \mathbb{R} = \mathbb{Q}(\sqrt[4]{2})$. Déterminer $K^{\langle rs\rangle}$ est moins instinctif : écrivons $x \in K^{\langle rs\rangle} \subseteq K^{\langle r^4\rangle} = \mathbb{Q}(i, \sqrt[4]{2})$ sous la forme $x = a + bi + c\sqrt[4]{2} + di\sqrt[4]{2} + e\sqrt{2} + fi\sqrt{2} + g\sqrt[4]{2}^3 + hi\sqrt[4]{2}^3$. Il est invariant par rs si, et seulement si :

$$a - bi + ci\sqrt[4]{2} + d\sqrt[4]{2} - e\sqrt{2} + fi\sqrt{2} - gi\sqrt[4]{2}^3 - h\sqrt[4]{2}^3 = a + bi + c\sqrt[4]{2} + di\sqrt[4]{2} + e\sqrt{2} + fi\sqrt{2} + g\sqrt[4]{2}^3 + hi\sqrt[4]{2}^3,$$

et donc, par indépendance linéaire, $b = e = g = h = 0$, ainsi que $c = d$, ce qui nous donne $x = a + c\sqrt[4]{2}(1+i) + fi\sqrt{2} \in \mathbb{Q}\left(\sqrt[4]{2}(1+i)\right) = \mathbb{Q}(\sqrt[4]{2}\zeta)$ (on remarque qu'on a extrait une racine carrée de $i\sqrt{2}$). Le lecteur en exercice procèdera de même pour déterminer toutes les extensions intermédiaires (ou en étudiant la décomposition de $X^8 - 2$ sur les différentes extensions déjà connues : les corps de rupture de ses éléments irréductibles doivent se trouver parmi les surcorps qu'on veut déterminer).

Remarque générale. Pour les extensions intermédiaires qui ne sont pas normales, en déterminer une seule suffit à déterminer toutes ses conjuguées. On montre en effet très facilement que si L/K est galoisienne de groupe de Galois G, et H est un sous-groupe de G, alors pour tout $g \in G$, $g(L^H) = L^{gHg^{-1}}$. En effet, pour tout $x \in g(L^H)$, on a $h(g^{-1}(x)) = g^{-1}(x)$ pour tout $h \in H$ si, et seulement si $ghg^{-1}(x) = x$ pour tout $h \in H$, si et seulement si $x \in L^{gHg^{-1}}$. Ceci généralise le raisonnement fait à la main pour déterminer les extensions intermédiaires de $\mathbb{Q}(\sqrt[5]{2}, \zeta)/\mathbb{Q}$: le corps des points fixes de $\langle\tau\rangle$ étant $\mathbb{Q}(\alpha)$, celui de $\langle\sigma^k\tau\sigma^{-k}\rangle$ est $\sigma^k(\mathbb{Q}(\alpha)) = \mathbb{Q}(\zeta^k\alpha)$. Procéder de même pour le dernier exemple traité.