Correction : Groupes de Galois

Exercice 1. *Du tac au tac*

Rappel : soit K un corps de caratéristique $\neq 2$ et $P \in K[X]$ séparable, unitaire, de degré n. Soient $x_1, \dots, x_n$ ses racines dans un corps de décomposition F et $\Delta = \prod_{i<j}(x_i - x_j) \in F$. Le discriminant de P est $\mathrm{Disc}(P) = \Delta^2$. Alors $\mathrm{Disc}(P)$ est un carré dans K si et seulement si $\Delta \in K$, si et seulement si Δ est fixé par $\mathrm{Gal}_K(P)$. Or, si $\sigma \in \mathrm{Gal}_K(P)$, on vérifie que $\sigma(\Delta) = \varepsilon(\sigma)\Delta$. Il vient que $\mathrm{Disc}(P)$ est un carré dans K si et seulement si $\mathrm{Gal}_K(P) \subset \mathfrak{A}_n$.

De plus, on a $\mathrm{Disc}(X^2 + aX + b) = a^2 - 4b$, et $\mathrm{Disc}(X^3 + pX + q) = -4p^3 - 27q^2$.

— Comme $P = X^3 - X - 1$ est irréductible, $\mathrm{Gal}_{\mathbb{Q}}(P)$ agit transitivement sur les racines. De plus, $\mathrm{Disc}(P) = 4 - 27 = -23$ n'est pas un carré dans $\mathbb{Q}$, et $\mathrm{Gal}_{\mathbb{Q}}(P) \not\subset \mathfrak{A}_3$. Il vient que $\mathrm{Gal}_{\mathbb{Q}}(P) = \mathfrak{S}_3$.

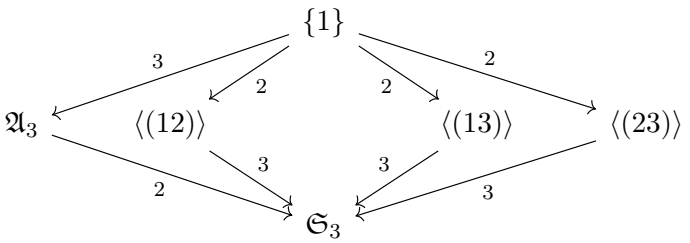
— $P = X^3 + X^2 - 2X + 1$ est irréductible, donc $\mathrm{Gal}_{\mathbb{Q}}(P)$ agit transitivement sur les racines de P.
Le discriminant est invariant par translation d'après sa définition, donc le discriminant de P est également celui de $P(X - \frac{1}{3}) = X^3 - \frac{7}{3}X + \frac{47}{27}$. Le discriminant de P est donc $\mathrm{Disc}(P) = -4 \cdot \left(-\frac{7}{3}\right)^3 - 27 \cdot \left(-\frac{47}{27}\right)^2 = -31 < 0$. Donc $\mathrm{Gal}_{\mathbb{Q}}(P) \not\subset \mathfrak{A}_3$. C'est donc $\mathfrak{S}_3$.

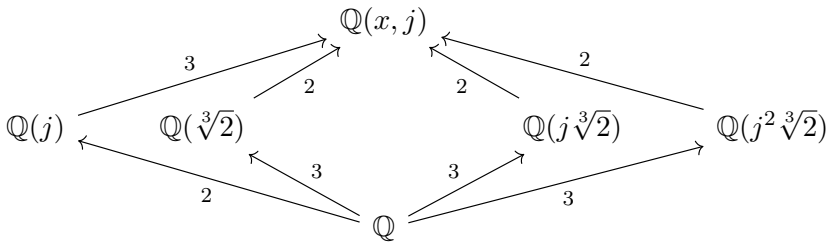
— Le discriminant de $P = X^3 - 3X + 1$ est $-4 \cdot (-3)^3 - 27 \cdot (1)^2 = 81 = 9^2$, donc $\mathrm{Gal}_{\mathbb{Q}}(P) \subset \mathfrak{A}_3$. Puisque P est irréductible, $\mathrm{Gal}_{\mathbb{Q}}(P)$ agit transitivement sur les racines de P, et c'est donc $\mathfrak{A}_3$.

Exercice 2.

Soient $x = \sqrt[3]{2}$, $j = e^{2\pi i/3}$ et $K = \mathbb{Q}[x, j]$.

1. Remarquons que $K = D_{\mathbb{Q}}(X^3 - 2)$, donc c'est une extension galoisienne.
   Remarquons que le polynôme minimal de j sur $\mathbb{Q}(\sqrt[3]{2})$ est $X^2 + X + 1$, donc j est de degré 2 sur $\mathbb{Q}(\sqrt[3]{2})$. Il vient $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 6$.
   Pour conclure, on a plusieurs méthodes :
   (a) On vérifie que l'on peut construire un automorphisme qui fixe j et qui permute cyliquement $(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2})$, ainsi qu'un automorphisme qui fixe $\sqrt[3]{2}$ et qui réalise la transposition (j, j^2). Et c'est gagné.
   (b) On invoque le fait que le cardinal de $\mathrm{Gal}_{\mathbb{Q}}(P)$ est le degré de $[D_{\mathbb{Q}}(P) : \mathbb{Q}]$. C'est donc un sous-groupe de $\mathfrak{S}_3$ d'ordre 6 : c'est $\mathfrak{S}_3$.
2.





Exercice 3. *Équation bicarrées*

1. On a $K = \mathbb{Q}(\alpha, \beta)$ donc $[K : \mathbb{Q}] = [\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$. Comme P est irreductible, on a $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. De plus $P = (X^2 - \alpha^2)(X^2 - \beta^2)$ donc β est annulé par le polynôme $X^2 - \beta^2 = X^2 + a + \alpha^2$ à coefficients dans $\mathbb{Q}(\alpha)$, et donc β est de degré 1 ou 2 sur $\mathbb{Q}(\alpha)$, d'où le résultat.
2. D'après le cours, G est isomorphe à un sous-groupe de $\mathfrak{S}_4$. Un élément $\sigma \in G$ est uniquement déterminé par $\sigma(\alpha)$ et $\sigma(\beta)$:
   — si $\sigma(\alpha) \in \{\alpha, -\alpha\}$, alors $\sigma(\beta) \in \{\beta, -\beta\}$. C'est donc une permutation parmi id, $(\alpha, -\alpha)$, $(\beta, -\beta)$, et $(\alpha, -\alpha)(\beta, -\beta)$.
   — si $\sigma(\alpha) = \beta$, alors $\sigma(-\alpha) = -\beta$, et :
      · si $\sigma(\beta) = \alpha$, alors σ est la permutation $(\alpha, \beta)(-\alpha, -\beta)$.
      · si $\sigma(\beta) = -\alpha$, alors σ est la permutation $(\alpha, \beta, -\alpha, -\beta)$.

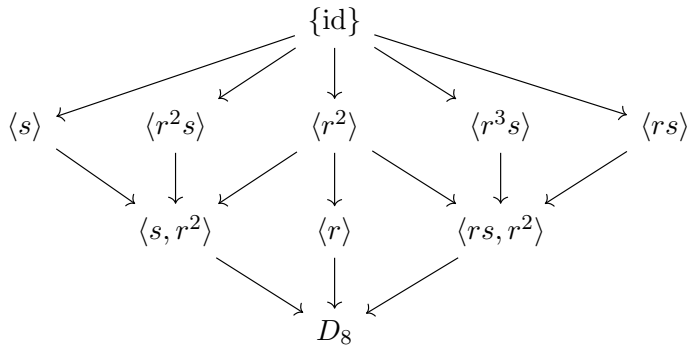
   Toutes ces permutations engendrent D_4, donc G est un sous-groupe de D_4.
3. Si G est d'ordre 8, c'est D_4. Sinon, il est d'ordre 4. Les seuls groupes d'ordre 4 de D_8 étant isomorphes à $\mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, le résultat s'en suit.
4. on sait que $\alpha^2 + \beta^2 = -a \in \mathbb{Q}$. Si $\alpha^2 - \beta^2 \in \mathbb{Q}$, alors $\alpha^2, \beta^2 \in \mathbb{Q}$. C'est impossible, car P est irréductible.
5. Supposons que $\tau \in G$ est d'ordre 4. Montrons que τ ou τ^{-1} est la permutation recherchée. Tout d'abord, on ne peut avoir $\tau(\alpha) = -\alpha$, car sinon, $\tau(\beta) = \pm\beta$, et τ est d'ordre 2. Il vient que $\tau(\alpha) = \pm\beta$. Deux cas s'offrent à nous :
   — Si $\tau(\alpha) = \beta$, alors nécessairement, $\tau(\beta) = -\alpha$, sinon τ est d'ordre 2. Il vient que $\sigma = \tau$ est donc la permutation cherchée.
   — Si $\tau(\alpha) = -\beta$, alors le même raisonnement montre que $\sigma = \tau^{-1}$ est la permutation cherchée.

   Réciproquement, supposons que $\sigma \in G$ avec $\sigma(\alpha) = \beta$ et $\sigma(\beta) = -\alpha$. Alors σ n'est ni d'ordre 1, ni d'ordre 2, et son ordre divisant 4, σ est d'ordre 4.
6. Supposons $G \simeq \mathbb{Z}/4\mathbb{Z}$, qui possède un élément d'ordre 4. Soit σ donné par la question précédente. Alors on vérifie que $\frac{\alpha}{\beta} - \frac{\beta}{\alpha}$ est fixé par σ, qui ne fixe aucun des éléments de $\{\pm\alpha, \pm\beta\}$, et donc ne fixe que les rationnels. Donc $\frac{\alpha}{\beta} - \frac{\beta}{\alpha} \in \mathbb{Q}$. Puisque $(\alpha\beta)\frac{\alpha}{\beta} - \frac{\beta}{\alpha} = \alpha^2 - \beta^2 \notin \mathbb{Q}$ d'après la question 4, on a $\alpha\beta \notin \mathbb{Q}$.
7. Puisque $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, tous les éléments sont d'ordre divisant 2. P étant irréductible, G agit transitivement : soit $\sigma \in G$ avec $\sigma(\alpha) = \beta$. Alors $\sigma(-\alpha) = -\beta$, et σ est la double transposition $(\alpha, \beta)(-\alpha, -\beta)$. De la même manière, on peut trouver $\tau \in G$ réalisant la double transposition $(\alpha, -\beta)(-\alpha, \beta)$. On vérifie que $\sigma\tau$ fixe $\alpha\beta$, et donc est dans $\mathbb{Q}$. On conclut de la même manière qu'à la question 6.
8. Même raisonnement mais avec le groupe diédral : soit τ dans G élément avec $\tau(\beta) = \alpha$ qui n'est pas le 4 cycle $(\alpha, \beta, -\alpha, -\beta)$. On montre que τ ne fixe ni $\alpha\beta$ ni $\frac{\alpha}{\beta} - \frac{\beta}{\alpha}$.

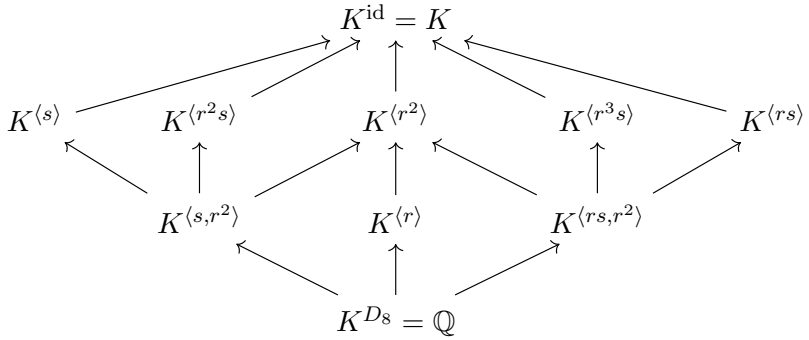
Dans les questions 9 et 10, on considère le polynôme $P = X^4 - 2X^2 + 2$.

9. On montre l'irréductibilité par Eisenstein. En calculant explicitement $\alpha = \sqrt[4]{2}e^{i\frac{\pi}{8}}$ et $\beta = \overline{\alpha}$, on a $\alpha\beta \notin \mathbb{Q}$ et $\frac{\alpha}{\beta} - \frac{\beta}{\alpha} \notin \mathbb{Q}$. Le résultat suit de la question 8.

10. Le treillis des sous-groupes de D_4 est donné par



où r est la permutation cyclique $(\alpha, \beta, -\alpha, -\beta)$, et s est la transposition $(\alpha, -\alpha)$. Toutes les flèches sont des injections d'indice 2. On a donc par la correspondance de Galois le treillis des sous-extensions

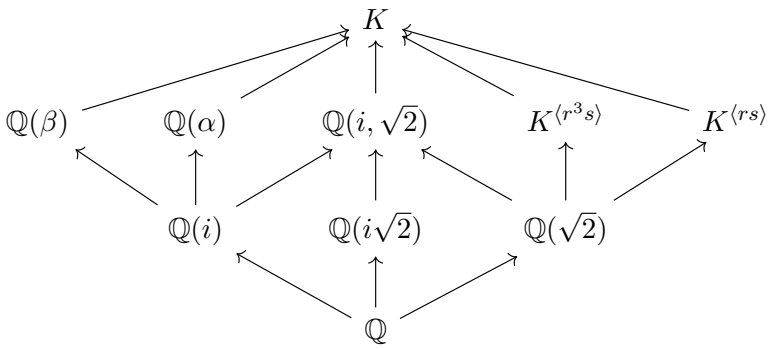


En premier lieu, remarquons que s fixe β, qui est de degré 4 que $\mathbb{Q}$. Ainsi, $K^{\langle s\rangle} = \mathbb{Q}(\beta)$. De même, r^2s fixe α, qui est de degré 4, et donc $K^{\langle r^2s\rangle} = \mathbb{Q}(\alpha)$. De plus, $\alpha^2 = i + 1$, donc $i \in \mathbb{Q}(\alpha)$. Il vient que $\mathbb{Q}(i)$ est une sous-extension de degré 2 de $\mathbb{Q}(\alpha)$: c'est forcément $K^{\langle s,r^2\rangle}$.

Tout d'abord, remarquons que $\alpha+\beta = 2\sqrt[4]{2}\cos\frac{\pi}{8} = \sqrt[4]{2}\sqrt{2+2\sqrt{2}}$, $\alpha-\beta = 2i\sqrt[4]{2}\sin\frac{\pi}{8} = i\sqrt{2\sqrt{2}-2}$, $\frac{\alpha}{\beta} + \frac{\beta}{\alpha} = 2\cos\frac{\pi}{4} = \sqrt{2}$ et $\frac{\alpha}{\beta} - \frac{\beta}{\alpha} = i\sqrt{2}$. Les corps engendrés par ces éléments sont donc des sous-corps de K. Remarquons de plus que $\alpha^2 = 1 + i$. Donc $i \in K$, et comme $i\sqrt{2}$ et $i\sqrt{2\sqrt{2}-2}$ aussi, on a $\sqrt{2} \in K$ et $\sqrt{2\sqrt{2}-2} \in K$. On a donc trouvé plusieurs sous-corps Déterminons le sous corps fixés par chacun de ces sous-groupes de D_8.

On vient donc de trouver plusieurs sous-extensions monogènes : $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i\sqrt{2})$ (qui sont de degré 2), et $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$, $\mathbb{Q}(\sqrt{2\sqrt{2}-2})$ et $\mathbb{Q}(\sqrt{2+2\sqrt{2}})$, qui sont de degré 4. On vérifie aisément qu'elles sont distinctes. D'après la correspondance de Galois, il ne manque qu'une seule extension de degré 4 : c'est $\mathbb{Q}(i, \sqrt{2})$.

Remarquons que r fixe $i\sqrt{2}$, et que $\langle r\rangle$ est d'indice 2 : ainsi, $K^{\langle r\rangle} = \mathbb{Q}(i\sqrt{2})$.



On en déduit le treillis des sous-extensions de K

11. Trouver des polynômes irréductibles de degré 4 sur $\mathbb{Q}$ correspondant à chacun des cas de la question 3.