

On appelle $E = \mathbb{Q}(\sqrt{2 \pm \sqrt{5}})$ le corps de décomposition sur $\mathbb{Q}$ de $t^4 - 4t^2 - 1 = 0$. On se propose d'étudier son groupe de Galois $G = \text{Gal}(E/\mathbb{Q})$ et les corps intermédiaire entre $\mathbb{Q}$ et E .

Détermination du groupe de Galois

Les quatre racines de $t^4 - 4t^2 - 1 = 0$ sont les $\pm\sqrt{2 \pm \sqrt{5}}$ avec les quatre combinaisons possibles des deux signes $\pm$. On peut donc voir G comme un sous-groupe de $\mathfrak{S}_4$ opérant sur ces quatre éléments. Mais il y a mieux : puisque $\sqrt{2 + \sqrt{5}}$ et $-\sqrt{2 + \sqrt{5}}$ sont opposés, tout élément de G doit les envoyer sur deux éléments opposés, c'est-à-dire soit eux-mêmes (dans un certain ordre) soit $\sqrt{2 - \sqrt{5}}$ et $-\sqrt{2 - \sqrt{5}}$ (dans un certain ordre). Ceci implique qu'en plaçant les quatre éléments aux quatre sommets d'un carré de sorte que deux éléments opposés soient sur des sommets opposés, i.e.

$$\begin{array}{ccc} \sqrt{2 - \sqrt{5}} & \text{---} & \sqrt{2 + \sqrt{5}} \\ | & & | \\ -\sqrt{2 + \sqrt{5}} & \text{---} & -\sqrt{2 - \sqrt{5}} \end{array} \quad (*)$$

alors G agit en préservant la structure de ce carré, c'est-à-dire qu'il peut se voir comme un sous-groupe du groupe diédral du carré. Ceci n'a rien de particulier à l'équation bicarrée considérée et vaudrait pour n'importe laquelle ; en revanche, on va voir que dans ce cas particulier G est le groupe diédral tout entier (c'est la situation la plus générale, par opposition à ce qui se passe pour $\mathbb{Q}(\sqrt{2 \pm \sqrt{2}})$ par exemple).

Tout d'abord, le polynôme $t^4 - 4t^2 - 1$ est bien irréductible¹. En effet, elle n'a pas de racine dans $\mathbb{Q}$ (c'est tout à fait évident), ce qui exclut une décomposition en degrés 1 + 3, et une décomposition en degrés 2 + 2 est également impossible car on ne peut pas trouver deux parmi les quatre racines dont la somme et le produit soient tous deux rationnelles (ce qui serait impliqué par un facteur de degré 2 sur $\mathbb{Q}$). Une autre façon de rédiger consiste à remarquer que $2 + \sqrt{5}$ n'est pas un carré dans $\mathbb{Q}(\sqrt{5})$ (si on avait $(x + y\sqrt{5})^2 = 2 + \sqrt{5}$ avec $x, y \in \mathbb{Q}$, on en déduirait $(x^2 - 5y^2)^2 = -1$, ce qui est impossible), donc $[\mathbb{Q}(\sqrt{2 + \sqrt{5}}) : \mathbb{Q}] = 4$, ce qui garantit l'irréductibilité. De façon plus efficace, constater que $\sqrt{2 - \sqrt{5}} \notin \mathbb{R}$ (on aura de toute façon à le remarquer plus tard) donc $\sqrt{2 - \sqrt{5}} \notin \mathbb{Q}(\sqrt{5})$ suffit à assurer $[\mathbb{Q}(\sqrt{2 - \sqrt{5}}) : \mathbb{Q}] = 4$, ce qui entraîne de nouveau l'irréductibilité. Enfin, si on préfère réduire modulo 3, on trouve $t^4 - t^2 - 1$, qui n'a pas de racine dans $\mathbb{F}_9$ donc est irréductible sur $\mathbb{F}_3$ ce qui entraîne que $t^4 - 4t^2 - 1$ est irréductible sur $\mathbb{Q}$.

L'irréductibilité assure que G opère transitivement sur $\{\pm\sqrt{2 \pm \sqrt{5}}\}$. Notamment, il existe un élément $\tilde{\sigma} \in G$ qui envoie $\sqrt{2 + \sqrt{5}}$ sur $\sqrt{2 - \sqrt{5}}$. On peut aussi justifier ce fait en remarquant que l'automorphisme non trivial $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$ (envoyant $\sqrt{5}$ sur $-\sqrt{5}$) doit se prolonger à E puisque E est galoisien, et ce prolongement doit envoyer $\sqrt{2 + \sqrt{5}}$ sur $\pm\sqrt{2 - \sqrt{5}}$, et quitte à composer avec un élément de $\text{Gal}(E/\mathbb{Q}(\sqrt{5}))$ qui échange $\sqrt{2 - \sqrt{5}}$ et $-\sqrt{2 - \sqrt{5}}$ (il y en a certainement un !) on peut supposer que $\tilde{\sigma}(\sqrt{2 + \sqrt{5}}) = \sqrt{2 - \sqrt{5}}$.

(Tout ceci vaudrait encore pour $\mathbb{Q}(\sqrt{2 \pm \sqrt{2}})$. Ce qui va différer entre ces deux cas c'est qu'on puisse ou non choisir *indépendamment* les deux signes $\pm$ dans la recherche d'un automorphisme envoyant $\sqrt{2 + \sqrt{\Delta}}$ sur $\pm\sqrt{2 - \sqrt{\Delta}}$ et $\sqrt{2 - \sqrt{\Delta}}$ sur $\pm\sqrt{2 + \sqrt{\Delta}}$.)

⁽¹⁾ L'exemple de la situation à exclure est celle de $t^4 - 6t^2 + 25 = 0$, qui a pour racines $\pm\sqrt{3 \pm 4\sqrt{-1}}$ et dont on pourrait manquer de constater qu'elles se réécrivent $\pm 2 \pm \sqrt{-1}$ c'est-à-dire que le polynôme se factorise comme produit de $t^2 + 4t + 5$ et de $t^2 - 4t + 5$: on a $\mathbb{Q}(\sqrt{3 \pm 4\sqrt{-1}}) = \mathbb{Q}(\sqrt{-1})$.

Or il existe un automorphisme $\tau \in G = \text{Gal}(E/\mathbb{Q})$ qui échange $\sqrt{2 - \sqrt{5}}$ et $-\sqrt{2 - \sqrt{5}}$ tout en laissant $\sqrt{2 + \sqrt{5}}$ fixe (et, bien sûr, $\sqrt{5}$, de sorte qu'en fait $\tau \in \text{Gal}(E/\mathbb{Q}(\sqrt{5}))$) : en effet, τ est réalisé par la conjugaison complexe. C'est cette constatation qui va assurer que G a bien huit éléments (et est le groupe diédral du carré).

On sait que $\tilde{\sigma}(\sqrt{2 - \sqrt{5}}) = \pm\sqrt{2 + \sqrt{5}}$, mais on ne savait pas encore *a priori* quel(s) choix de signe étai(en)t possible(s). Or quitte à remplacer $\tilde{\sigma}$ par $\tilde{\sigma}\tau$ le cas échéant, on peut assurer que $\tilde{\sigma}(\sqrt{2 - \sqrt{5}}) = -\sqrt{2 + \sqrt{5}}$. C'est-à-dire, sur le carré $(\star)$ ci-dessus, que $\tilde{\sigma}$ réalise une rotation d'un quart de tour. On a $\tilde{\sigma}^4 = \text{id}$ et $\tilde{\sigma}\tau = \tau\tilde{\sigma}^3$.

Finalement, on a bien prouvé que $G = \{1, \tilde{\sigma}, \tilde{\sigma}^2, \tilde{\sigma}^3, \tau, \tau\tilde{\sigma}, \tau\tilde{\sigma}^2, \tau\tilde{\sigma}^3\}$ est le groupe diédral du carré.

Détermination des corps intermédiaires

Le groupe G a, outre $\{1\}$ et G tout entier, huit autres sous-groupes : cinq sous-groupes à deux éléments correspondant aux idempotents $\tilde{\sigma}^2, \tau, \tau\tilde{\sigma}^2, \tau\tilde{\sigma}$ et $\tau\tilde{\sigma}^3$, et trois sous-groupes d'indice deux, dont l'un est cyclique d'ordre 4 ($\{1, \tilde{\sigma}, \tilde{\sigma}^2, \tilde{\sigma}^3\}$) et les deux autres sont isomorphes à $(\mathbb{Z}/2\mathbb{Z})^2$ (ils sont engendrés par deux idempotents qui commutent, et qui peuvent être $\tilde{\sigma}^2$ et τ ou bien $\tilde{\sigma}^2$ et $\tau\tilde{\sigma}$). Parmi ces dix sous-groupes, six sont distingués ($\{1\}$ et G , bien sûr, ainsi que les trois sous-groupes d'indice 2, et enfin $\{1, \tilde{\sigma}^2\}$) et les quatre autres sont conjugués deux à deux (sous l'action de $\tilde{\sigma}$). On cherche donc à décrire dix corps intermédiaires entre $\mathbb{Q}$ et $E = \mathbb{Q}(\sqrt{2 \pm \sqrt{5}})$, dont six sont galoisiens sur $\mathbb{Q}$ et les quatre autres sont deux à deux conjugués.

Avant de commencer, notons que $[E : \mathbb{Q}] = 8$. Si on veut en trouver une base, on peut l'écrire comme composée d'extensions quadratiques : d'abord $\mathbb{Q}(\sqrt{5})$ a une $\mathbb{Q}$ -base formée de 1 et $\sqrt{5}$, ensuite $\mathbb{Q}(\sqrt{2 + \sqrt{5}})$ a une $\mathbb{Q}(\sqrt{5})$ -base formée de 1 et $\sqrt{2 + \sqrt{5}}$ donc la $\mathbb{Q}$ -base 1, $\sqrt{5}$, $\sqrt{2 + \sqrt{5}}$, $\sqrt{10 + 5\sqrt{5}}$, et enfin $\mathbb{Q}(\sqrt{2 \pm \sqrt{5}})$ admet donc la $\mathbb{Q}$ -base 1, $\sqrt{5}$, $\sqrt{2 + \sqrt{5}}$, $\sqrt{10 + 5\sqrt{5}}$, $\sqrt{2 - \sqrt{5}}$, $\sqrt{10 - 5\sqrt{5}}$, $\sqrt{-1}$, $\sqrt{-5}$.

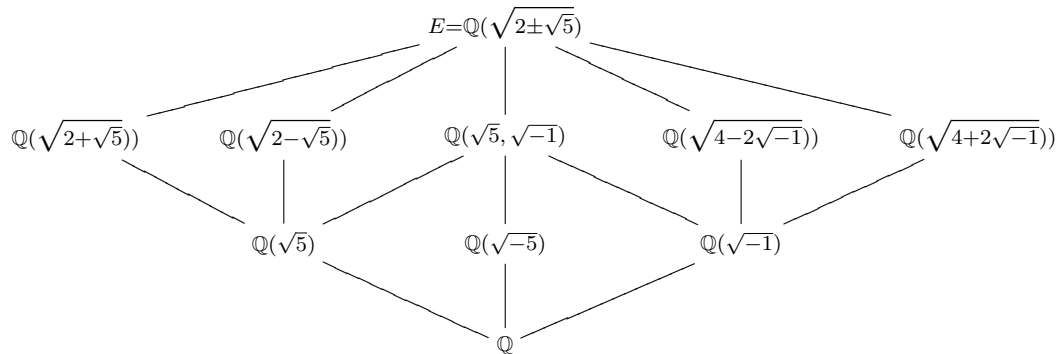
De façon générale, pour déterminer le corps fixe associé à un sous-groupe H du groupe de Galois, on utilise des techniques d'algèbre linéaire : une fois connue une base de E sur $\mathbb{Q}$, on peut en déterminer le sous-espace fixe par n'importe quel ensemble H d'endomorphismes. Ici, cependant, en raison de sa construction « en étages » par extensions quadratiques, la base trouvée a la propriété agréable que pour tout élément $\rho \in G$ et tout élément e de la base, on a $\rho(e) = \pm e'$ pour un autre élément e' de la base, et les sous-espaces fixes et opposés par l'action de Galois sont assez évidents à déterminer. On voit alors que :

- Le corps fixe de G tout entier est $\mathbb{Q}$.
- Le corps fixe de $\{1, \tilde{\sigma}^2, \tau, \tau\tilde{\sigma}^2\}$ (réflexions par les diagonales dans le carré $(\star)$) est $\mathbb{Q}(\sqrt{5})$.
On a ainsi $\text{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ et $\text{Gal}(E/\mathbb{Q}(\sqrt{5})) \cong (\mathbb{Z}/2\mathbb{Z})^2$.
- Le corps fixe de $\{1, \tilde{\sigma}^2, \tau\tilde{\sigma}, \tau\tilde{\sigma}^3\}$ (réflexions par les axes dans le carré $(\star)$) est $\mathbb{Q}(\sqrt{-1})$.
On a ainsi $\text{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ et $\text{Gal}(E/\mathbb{Q}(\sqrt{-1})) \cong (\mathbb{Z}/2\mathbb{Z})^2$.
- Le corps fixe de $\{1, \tilde{\sigma}, \tilde{\sigma}^2, \tilde{\sigma}^3\}$ (rotations dans le carré $(\star)$) est $\mathbb{Q}(\sqrt{-5})$. On a ainsi $\text{Gal}(\mathbb{Q}(\sqrt{-5})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ et $\text{Gal}(E/\mathbb{Q}(\sqrt{-5})) \cong \mathbb{Z}/4\mathbb{Z}$.
- Le corps fixe de $\{1, \tilde{\sigma}^2\}$ est $\mathbb{Q}(\sqrt{5}, \sqrt{-1})$: on a ainsi $\text{Gal}(\mathbb{Q}(\sqrt{5}, \sqrt{-1})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ et $\text{Gal}(E/\mathbb{Q}(\sqrt{5}, \sqrt{-1})) \cong \mathbb{Z}/2\mathbb{Z}$.
- Le corps fixe de $\{1, \tau\}$ est $\mathbb{Q}(\sqrt{2 + \sqrt{5}})$: on a ainsi $\text{Gal}(E/\mathbb{Q}(\sqrt{2 + \sqrt{5}}))$, en revanche $\mathbb{Q}(\sqrt{2 + \sqrt{5}})$ n'est pas galoisien sur $\mathbb{Q}$. De même, le corps fixe associé à $\{1, \tau\tilde{\sigma}^2\}$ est $\mathbb{Q}(\sqrt{2 - \sqrt{5}})$. Ces deux sous-corps de E sont conjugués par l'action de Galois.
- Le corps fixe associé à $\{1, \tau\tilde{\sigma}\}$ est moins évident à représenter sur la base qu'on a trouvée : on sait qu'il contient au moins $\mathbb{Q}(\sqrt{-1})$, et on peut lui trouver comme générateur

$\sqrt{2 + \sqrt{5}} - \sqrt{2 - \sqrt{5}} = \sqrt{4 - 2\sqrt{-1}}$. De même, le corps fixe associé à $\{1, \tau\tilde{\sigma}^3\}$ est $\mathbb{Q}(\sqrt{4 + 2\sqrt{-1}})$. Ces deux corps sont conjugués par l'action de Galois.

–Le corps fixe de $\{1\}$ est évidemment $E = \mathbb{Q}(\sqrt{2 \pm \sqrt{5}})$ tout entier.

On a finalement le diagramme suivant des corps intermédiaires :



(Ce diagramme permet d'exprimer E de différentes autres manières : on a par exemple $E = \mathbb{Q}(\sqrt{4 \pm 2\sqrt{-1}})$ ou $E = \mathbb{Q}(\sqrt{-1}, \sqrt{2 + \sqrt{5}})$.)