# Des extensions de $\mathbb{Q}$ de degré 4, *sans* sous-corps de degré 2[1]

Pour $p$ premier, posons $P = X^4 + pX - p$. Le critère d'Eisenstein montre que $P$ est irréductible dans $\mathbb{Q}[X]$. Il est facile de vérifier que $P$ a deux racines réelles, dont une dans $]0, 1[$.

**Affirmation:** *Soit $\alpha$ une racine complexe de $P$. Alors le corps $L = \mathbb{Q}(\alpha)$, extension de $\mathbb{Q}$ de degré 4, n'a pas d'autre sous–corps que $L$ et $\mathbb{Q}$.*

*dém:* Supposons le contraire, i.e. il existe un sous–corps $K$ de $L$ distinct de $L$ et $\mathbb{Q}$. Alors forcément $[K : \mathbb{Q}] = 2 = [L : K]$, donc le polynôme minimal $\mathrm{Irr}(\alpha, K)$ a degré 2. On en déduit que dans $K[X]$ $P$ peut s'écrire

$$P = (X^2 + aX + b)(X^2 + cX + d)\,.$$

Par identification des coefficients, on en déduit que $c = -a$, $b + d = -ac = a^2$, $a(d - b) = p$, d'où $a \neq 0$ et $d - b = p/a$, enfin $bd = -p$. De là on tire $2d = a^2 + p/a$, $2b = a^2 - p/a$, donc en faisant le produit $-4p = a^4 - p^2/a^2$. Ainsi $a^2$ est racine du polynôme rationnel

$$Q = X^3 + 4pX - p^2\,.$$

Or $a \in K$, donc le degré de $a^2$ sur $\mathbb{Q}$ divise $[K : \mathbb{Q}] = 2$. Ainsi $Q$ admet dans $\mathbb{Q}[X]$ un diviseur (soit $\mathrm{Irr}(a^2, \mathbb{Q})$) de degré 1 ou 2. Il admet donc un facteur de degré 1, i.e. *$Q$ a une racine dans $\mathbb{Q}$.*
Reste à voir que cela n'est pas. Comme $Q$ est unitaire à coefficients entiers, toute racine rationnelle de $Q$ serait un entier divisant $p^2$; clairement positif, de plus. Or $Q'$ est positif sur $\mathbb{R}$, et on a $Q(0) < 0$, $Q(p) = p^2(p + 3) > 0$, donc il ne reste qu'à montrer $Q(1) \neq 0$: et en effet $Q(1)$ est congru à 1 modulo $p$.

**N.B.** Un raisonnement analogue fonctionne pour le polynôme $P = X^4 + X + 1$, irréductible dans $\mathbb{Q}[X]$ car il l'est dans $\mathbb{F}_2[X]$. Le polynôme $Q$ correspondant est $X^3 - 4X - 1$.

**Compléments:**

**1.** L'argument ci–dessus fournit aussi une information sur le *corps de décomposition* de $P$:
*Notons $E$ le sous-corps de $\mathbb{C}$ engendré par les racines $\alpha_1, \ldots, \alpha_4$ de $P$. Alors $[E : \mathbb{Q}]$ est multiple de 12 (c'est donc 12 ou 24).*
En effet la factorisation de $P$ considérée dans la preuve ci–dessus est en tout cas toujours possible dans $E[X]$, avec par exemple $-a = \alpha_1 + \alpha_2$. On obtient alors que $a^2$ est de degré 3 sur $\mathbb{Q}$, puisqu'il annule $Q$ qui est irréductible. Ainsi le degré de $E$ sur $\mathbb{Q}$, qui est multiple de $4 = \deg_{\mathbb{Q}}(\alpha_1)$, est aussi multiple de 3 (et c'est un fait général qu'il divise 4!).

**2.** Les racines (réelles) de $P$ sont *non constructibles*, bien que de degré 4 sur $\mathbb{Q}$; la condition nécessaire "de Wantzel" sur le degré d'un nombre constructible n'est donc pas suffisante.
Pour le voir, on remarque que le même argument développé ci–dessus prouve en fait: *si $\alpha$ est une racine de $P$ dans un corps $K'$ et si $K' \supset K$ est une extension de degré 2 telle que $\alpha \notin K$, alors 3 divise $[K : \mathbb{Q}]$* (en effet on écrit que $\mathrm{Irr}(\alpha, K) = X^2 + aX + b$ divise $P$, et on obtient via l'irréductibilité de $Q$ que $\deg_{\mathbb{Q}}(a^2) = 3$). Ceci montre bien que $\alpha$ ne peut apparaître dans une tour d'extensions quadratiques de $\mathbb{Q}$.

[1] en réponse à une question de Simon Schmidt

**3.** On a en fait le résultat plus général:
*pour tout $n \geq 4$, il existe $K \supset \mathbb{Q}$ extension de degré $n$ sans sous–corps non trivial.*
La preuve utilise les trois points suivants:
- l'existence pour tout $n$ d'une extension galoisienne $L$ de $\mathbb{Q}$ de groupe de Galois $\mathfrak{S}_n$.
- le fait que tout sous–groupe d'indice $n$ de $\mathfrak{S}_n$ est maximal (voir *A. Chambert-Loir, Algèbre corporelle,* exercice du chapitre 4)
- la "correspondance de Galois", bijection qui renverse les inclusions entre les sous–corps de $L$ de degré donné $m$ sur $\mathbb{Q}$ d'une part, et les sous-groupes d'indice $m$ de $\mathfrak{S}_n$ d'autre part (voir partie III du cours).