Corrigé du devoir à la maison du 28 avril

Exercice 1 Soit $\mathbb{Q} \leq K$ une extension quadratique. Montrons qu'il existe ζ une racine de l'unité telle que $K \leq \mathbb{Q}(\zeta)$.

Soit $x \in K \setminus \mathbb{Q}$. Alors comme $\mathbb{Q} \neq \mathbb{Q}(x) \leq K$ et comme $[K : \mathbb{Q}] = 2$, on a forcément $K = \mathbb{Q}(x)$ et x est de degré 2 sur $\mathbb{Q}$.

Soit P_x le polynôme unitaire minimal de x sur $\mathbb{Q}$. On a $P_x = X^2 + aX + b$ où $a, b \in \mathbb{Q}$. Posons $\Delta = a^2 - 4b \in \mathbb{Q}$. Soit $\delta \in \mathbb{C}$ tel que $\delta^2 = \Delta$. Comme $x = \frac{-a \pm \delta}{2}$, $K = \mathbb{Q}(x) = \mathbb{Q}(\delta)$.

Soient r, s des entiers (non nuls) tels que $\Delta = \frac{r}{s}$. Si $n = rs$, on a : $(s\delta)^2 = rs$ donc $K = \mathbb{Q}(s\delta)$ et $s\delta = \pm\sqrt{n}$.

Décomposons $n = \pm p_1 ... p_l$ en produit de nombre premiers p_j, $1 \leq j \leq l$. D'après les questions *a)* et *c)* de l'exercice 2, on a $\mathbb{Q}(\sqrt{p_i}) \subseteq \mathbb{Q}(\zeta_i)$ pour une certaine racine de l'unité ζ_i d'ordre n_i. On a aussi $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$. Donc :

$$K = \mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\zeta_4, \zeta_1, ..., \zeta_l) \subseteq \mathbb{Q}(\zeta_N)$$

où $N = \text{ppcm}(4, n_1, ..., n_l)$ d'après l'exercice 1a) de la fiche 8. **Q.e.d.**

Exercice 2 Montrons que le groupe de Galois sur $\mathbb{Q}$ du polynôme $P(X) = X^5 + 20X + 16$ est isomorphe à $\mathfrak{A}_5$. Modulo 3, on a :

$$P(X) = X^5 - X + 1 \ .$$

Ce polynôme n'a pas de racine dans $\mathbb{F}_3$ donc n'a pas de facteur irréductible de degré 1. Montrons que P n'a pas non plus de facteur irréductible de degré 2 dans $\mathbb{F}_3[X]$. Sur $\mathbb{F}_3$, les seuls polynômes irréductibles unitaires de degré 2 sont :

$$X^2 + 1,\ X^2 + X - 1,\ X^2 - X - 1$$

et dans $\mathbb{F}_3[X]$, on a :

$$X^5 - X + 1 = (X^2 + 1)(X^3 - X) + 1$$

$$X^5 - X + 1 = (X^2 + X - 1)(X^3 - X^2 + 2X - 1) + 2X$$

$$X^5 - X + 1 = (X^2 - X - 1)(X^3 + X^2 + 2X) + X + 1$$

donc $P(X)$ n'a pas non plus de facteur irréductible de degré 2 sur $\mathbb{F}_3$.

Comme P est de degré 5, cela suffit pour conclure à l'irréductibilité de P modulo 3. En particulier P est irréductible sur $\mathbb{Q}$. Notons x_1, x_2, x_3, x_4, x_5 les racines complexes de P et $K = \mathbb{Q}(x_1, x_2, x_3, x_4, x_5)$. La restriction à l'ensemble $\{x_1, x_2, x_3, x_4, x_5\}$ induit un morphisme injectif de groupes :

$$\varphi : \text{Aut}(K) \to \mathfrak{S}_5 \ .$$

D'après le théorème de Dirichlet (sur la réduction modulo p), l'image de φ contient un $5-$cycle car P est irréductible $\mod 3$.

Modulo 7, on a :

$$P(X) = X^5 - X + 2 = (X + 2)(X + 3)(X^3 + 2X^2 + 5X + 5)$$

et $X^3 + 2X^2 + 5X + 5$ est irréductible sur $\mathbb{F}_7$ car sans racine.

Donc d'après le théorème de Dirichlet (en réduisant modulo 7), l'image de φ dans $\mathfrak{S}_5$ contient un 3−cycle.

Or le discriminant de P est

$$\Delta = \prod_{1\leq i<j\leq 5}(x_i - x_j)^2 = \prod_{1\leq i\leq 5} P'(x_i)$$

$$= \prod_{1\leq i\leq 5}(5x_i^4 + 20)$$

Or $x_i^5 + 20x_i + 16 = 0 \Rightarrow x_i^4 + 20 + \frac{16}{x_i} = 0$.

Donc

$$\Delta = \prod_{1\leq i\leq 5}(5x_i^4 + 20) = \prod_{1\leq i\leq 5}(-80 - \frac{80}{x_i})$$

$$= -80^5 \prod_{1\leq i\leq 5}(1 + \frac{1}{x_i}) = -\frac{80^5}{\prod_{1\leq i\leq 5} x_i} \prod_{1\leq i\leq 5}(x_i + 1)$$

$$= -\frac{80^5}{16}\prod(-1 - x_i)$$

$$= -80^4.5.P(-1)$$

car $P(X) = (X-x_1)(X-x_2)(X-x_3)(X-x_4)(X-x_5)$. Donc $\Delta = -80^4.5.(-5) = 80^4.5^2 = 3200^2$.

Donc $\delta := \prod_{1\leq i<j\leq 5}(x_i - x_j) = \pm 3200 \in \mathbb{Q}$.

Mais alors pour tout $\sigma \in \mathrm{Aut}(K)$, $\sigma(\delta) = \delta$ car $\delta \in \mathbb{Q}$. Mais on a $\sigma(\delta) = \prod_{1\leq i<j\leq 5}(x_{\sigma(i)} - x_{\sigma(j)}) = \epsilon(\sigma)\delta \Rightarrow \epsilon(\sigma) = 1$ et $\sigma \in \mathfrak{A}_5$.

Donc $G = \varphi(\mathrm{Aut}(K)) \leq \mathfrak{A}_5$. Comme G contient un 3−cycle et un 5−cycle, $\mathfrak{A}_5/G$ est de cardinal $n = 4, 2$ ou 1.

Or $\mathfrak{A}_5$ est simple. Donc le morphisme de groupes $A_5 \to \mathfrak{S}_n$ induit par la multiplication à gauche : $^\forall hG \in \mathfrak{A}_5/G$, $\sigma.hG := \sigma hG$ est injectif ou trivial (constant d'image 1). Comme $|\mathfrak{A}_5| = 60 > n!$ si $n = 1$, ou 4, on a forcément un morphisme trivial. Donc :

$$^\forall \sigma, h, \in \mathfrak{A}_5,\ \sigma hG = hG \Rightarrow \sigma G = G \Rightarrow \sigma \in G$$

$\Rightarrow \mathfrak{A}_5 \leq G$ et $G \simeq \mathfrak{A}_5$.