Calculs de groupes de Galois :

Soit $P := X^5 + 10X^3 - 10X^2 + 35X - 18$.

Modulo 3, voici la décomposition en facteurs irréductibles de P :

$$P = X \cdot (X+2) \cdot (X^3 + X^2 + 2X + 1) \bmod 3 \ .$$

Donc P est séparable sur $\mathbb{Q}$ (car il l'est sur $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$) et le groupe de Galois de P (vu comme sous-groupe de S_5) contient un 3−cycle).

On calcule le discriminant de P (sans logiciel de calcul formel c'est un peu long et fastidieux), la méthode la plus « pratique » ici est d'utiliser la formule :

$$\Delta_P = \begin{vmatrix} 5 & s_1 & s_2 & s_3 & s_4 \\ s_1 & s_2 & s_3 & s_4 & s_5 \\ s_2 & s_3 & s_4 & s_5 & s_6 \\ s_3 & s_4 & s_5 & s_6 & s_7 \\ s_4 & s_5 & s_6 & s_7 & s_8 \end{vmatrix}$$

où $s_i = x_1^i + ... + x_5^i$ avec $x_1, ..., x_5$ les racines de P dans $\mathbb{C}$. On a ici $s_1 = 0$ et par exemple comme $P(x_i) = 0$, $s_5 = -10s_3 + 10s_2 - 35s_1 - 18s_0$, ... d'où :

$$\Delta_P = \begin{vmatrix} 5 & 0 & -20 & 30 & 60 \\ 0 & -20 & 30 & 60 & -410 \\ -20 & 30 & 60 & -410 & 400 \\ 30 & 60 & -410 & 400 & 3290 \\ 60 & -410 & 400 & 3290 & -9660 \end{vmatrix}$$

et après de longs calculs :

$$\Delta_P = 2^6 5^8 11^2 \ .$$

Donc le groupe de Galois G de P sur $\mathbb{Q}$ est contenu dans A_5.

Modulo 7, P n'a pas de racine donc soit P est irréductible modulo 7 soit $P = P_1 P_2 \bmod 7$ avec P_1, P_2 irréductibles sur $\mathbb{F}_7$ de degrés 2 et 3. Ce dernier cas est impossible car alors G contiendrait une permutation de la forme $t \circ s$ avec un 3−cycle s et une transposition t ce qui n'est pas un élément de A_5. Donc P est irréductible $\bmod 7$ donc irréductible sur $\mathbb{Q}$.

Finalement G est un sous-groupe transitif de S_5, contenu dans A_5. Mais alors G est d'ordre 15, 30 ou 60 (car divisible par $3, 5$ et $|A_5| = 60$). Or les groupes d'ordre 15 sont cycliques et il n'y a pas délément d'ordre 15 dans S_5. Donc G est d'ordre 30 ou 60. Comme A_5 est simple, il n'y a pas de sous-groupe d'indice 2 dans A_5. D'où $G = A_5$.

Soit $Q := X^5 + 10X^3 - 15$.

On a :

$$Q = (X + 1) \cdot (X^4 + X^3 + X^2 + X + 1) \bmod 2 \ .$$

Or $X^4+X^3+X^2+X+1$ est irréductible sur $\mathbb{F}_2$ (car $X^4+X^3+X^2+X+1$ n'a pas de racine dans $\mathbb{F}_2$ et n'est pas divisible par le seul polynôme irréductible sur $\mathbb{F}_2$ de degré 2 qui est X^2+X+1). Donc le groupe de Galois de Q contient un $4-$cycle. De plus par le critère d'Eisenstein, Q est irréductible sur $\mathbb{Q}$.

On a aussi la décomposition en facteurs irréductibles sur $\mathbb{F}_{19}$:

$$Q = (X^2 + X + 3) \cdot (X^3 + 18X^2 + 8X + 14) \bmod 19$$

(c'est quand même plus rapide avec un ordinateur).

Donc le groupe de Galois de Q vu comme sous-groupe de S_5 contient un élément ts où t est une transposition et s un $3-$cycle à supports disjoints. En élevant au cube, on trouve que $t = (ts)^3 \in G$.

Or on a le :

Lemme 1 *Soit G un sous-groupe transitif de S_n contenant un $(n-1)-$cycle et une transposition. Alors $G = S_n$.*

Démonstration : On peut supposer que le $n-1-$cycle est $\sigma = (2...n)$ et (comme G est transitif) que la transposition est de la forme $t = (1i)$ avec $2 \leq i \leq n$.

En conjuguant t par σ^k, on trouve :

$$\sigma^k t \sigma^{-k} = (1\sigma^k(i)) \in G$$

pour tout k et donc

$$\langle (12), ..., (1n) \rangle = S_n = G \ .$$

<u>*q.e.d.*</u>

On a donc $X^5 + 10X^3 - 15$ de groupe de Galois S_5 sur $\mathbb{Q}$.

*

Fiche 12, exo. 4 : Pour tout d et pour tout nombre premier p, il existe un élément primitif $\alpha \in \mathbb{F}_{p^d}$ tel que :

$$\mathbb{F}_{p^d} = \mathbb{F}_p(\alpha) \ .$$

Alors le polynôme minimal de α sur $\mathbb{F}_p$ est irréductible de degré d. En « relevant » dans $\mathbb{Z}$, on en déduit l'existence d'un polynôme irréductible sur $\mathbb{Q}$ de degré d unitaire à coefficients entiers pour tout d.

En particulier, si $n \geq 4$ est fixé, il existe f_1 un polynôme entier unitaire de degré n irréductible modulo 2, f_2 un polynôme unitaire entier de degré n qui a un facteur irréductible de degré $n-1$ modulo 3, f_3 un polynôme unitaire entier de degré n qui modulo 5 a un facteur de degré 2 et 1 ou 2 facteurs de degrés impairs (distincts) tous irréductibles.

Le polynôme

$$f := -15f_1 + 10f_2 + 6f_3$$

vérifie :

$$f = f_1 \bmod 2$$

$$f = f_2 \bmod 3$$

$$f = f_3 \bmod 5$$

donc f est irréductible sur $\mathbb{Q}$ (car f est irréductible sur $\mathbb{F}_2$) et son groupe de Galois contient un $n-1-$cycle et une transposition. Donc f a pour groupe de Galois S_n sur $\mathbb{Q}$.