Développement : Galois inverse

Algèbre & Géométrie

Référence : [TAU] Tauvel P., *Corps commutatifs et théorie de Galois - Cours et exercices*, Calvage et Mounet, 2008, p187.

Pour les leçons :
- 104 : Groupes finis. Exemples et applications.
- 108 : Exemples de parties génératrices d'un groupe. Applications.
- 105 : Groupe des permutations d'un ensemble fini. Applications.
- 125 : Extensions de corps. Exemples et applications.
- 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
- 144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

Lemme 1.

Soit $p \geqslant 5$ un nombre premier. Alors, il existe $P \in \mathbb{Q}[X]$ irréductible dans $\mathbb{Q}[X]$ tel que P a exactement $p-2$ racines réelles.

Preuve : Soit $m \in \mathbb{N}^*$ pair. On pose :

$$Q(X) = (X^2+m)\prod_{i=1}^{p-2}(X-2i),$$
$$P(X) = Q(X) - 2.$$

Étape 1 : Montrons que P est irréductible dans $\mathbb{Q}[X]$.
En considérant $\bar{P}$, la réduction modulo P dans $\mathbb{F}_2[X]$, on a $\bar{P} = \bar{Q} = X^p$ (car m est pair).
De plus, le coefficient constant de P est -2, et P est unitaire.
Donc P vérifie les hypothèses du critère d'Eseinstein pour l'entier premier 2. Par conséquent :

$$\boxed{P \text{ est irréductible dans } \mathbb{Q}[X].}$$

Étape 2 : Soit $k \in \mathbb{N}^*$ impair. Montrons que $|Q(k)| > 2$.
Comme $m \geqslant 2$ et $k \geqslant 1$, $k^2 + m > 2$. De plus, pour $i \in [\![1; p-2]\!]$, k et $2i$ ne sont pas de même parité, donc $k - 2i \neq 0$ (et ce sont des entiers). Donc $\left|\prod_{i=1}^{p-2}(k-2i)\right| \geqslant 1$. Ainsi :

$$\boxed{|Q(k)| > 2.}$$

Étape 3 : Soit $r \in [\![0; p-2]\!]$. Étudions le signe de $Q(2r+1)$. Déjà, d'après l'étape 2, on a $Q(2r+1) \neq 0$.
De plus, le signe de $Q(2r+1)$ est celui de $(-1)^s$, où $s = |\{i \in [\![1; p-2]\!] \mid 2r+1 < 2i\}|$.
Or, pour $i \in [\![1; p-1]\!]$:

$$\begin{aligned} 2r+1 < 2i &\iff 2r+1 \leqslant 2i-1 \\ &\iff r+1 \leqslant i. \end{aligned}$$

Donc $s = p-2-(r+1)+1 = p-2-r$. On en déduit que s et $r+1$ ont la même parité.
Ainsi :

$$\boxed{Q(2r+1)\begin{cases} <0 & \text{si } r \text{ est pair} \\ >0 & \text{si } r \text{ est impair} \end{cases}.}$$

Étape 4 : Montrons que P possède au moins $p-2$ racines réelles (distinctes).
Soit $r \in [\![0; p-3]\!]$. D'après l'étape 2 et l'étape 3, $P(2r+1)\begin{cases} <0 & \text{si } r \text{ est pair} \\ >0 & \text{si } r \text{ est impair} \end{cases}$.
Comme $P : x \longmapsto P(x)$ est une fonction polynomiale donc continue, d'après le théorème des valeurs intermédiaires, P a une racine dans $]2r+1, 2r+3[$, pour tout $r \in [\![0; p-3]\!]$.

$$\boxed{\text{Ainsi, } P \text{ a au moins } p-2 \text{ racines réelles distinctes.}}$$

Étape 5 : Montrons que, pour m assez grand, P possède deux racines non réelles.
Soient $\alpha_1, \dots, \alpha_p$ (resp. $\beta_1, \dots, \beta_p$) les racines de P (resp. de Q) dans $\mathbb{C}$. Les relations coefficients-racines fournissent :

$$\sum_{i=1}^{p} \alpha_j = \sum_{i=1}^{p} \beta_j = 2\sum_{j=1}^{p-2} j,$$

et :

$$\sum_{1 \leqslant i < j \leqslant p} \alpha_i \alpha_j = \sum_{1 \leqslant i < j \leqslant p} \beta_i \beta_j = m + 4 \sum_{1 \leqslant i < j \leqslant p-2} ij.$$

Donc :

$$\begin{aligned} \sum_{i=1}^{p} \alpha_j^2 &= \left(\sum_{i=1}^{p} \alpha_j \right)^2 - 2 \sum_{1 \leqslant i < j \leqslant p} \alpha_i \alpha_j \\ &= 4 \left(\sum_{j=1}^{p-2} j \right)^2 - 2m - 8 \sum_{1 \leqslant i < j \leqslant p-2} ij \\ &= 4 \sum_{j=1}^{p-2} j^2 - 2m. \end{aligned}$$

Pour m assez grand, on a en outre $\sum_{i=1}^{p} \alpha_i^2 \leqslant 0$, ce qui n'est pas possible si les α_i sont tous réels. Ainsi, il existe $i \in [\![1; p]\!]$ tel que $\alpha_i \in \mathbb{C} \backslash \mathbb{R}$.

$$\boxed{\text{En outre, } P \text{ a deux racines non réelles.}}$$

Comme $P \in \mathbb{Q}[X] \subset \mathbb{R}[X]$, $\overline{\alpha_i} \in \mathbb{C}$ est aussi une racine complexe de P non réelle, différente de α_i.
Cela prouve le lemme. □

Théorème 2.

Soit $p \geqslant 5$ un nombre premier. Alors, il existe $P \in \mathbb{Q}[X]$ dont le corps de décomposition admet $\mathfrak{S}_p$ comme groupe de Galois.

Preuve : Soit $P \in \mathbb{Q}[X]$ le polynôme donné par le lemme précédent.
Tout automorphisme de Galois permute les p racines de P, donc $\mathrm{Gal}(\mathcal{D}/\mathbb{Q})$ est isomorphe à un sous-groupe G de $\mathfrak{S}_p$.
Soit α une racine complexe de P. En notant $\mathcal{D}$ le corps de décomposition de P sur $\mathbb{Q}$, on a :

$$|\mathrm{Gal}(\mathcal{D}/\mathbb{Q})| = [\mathcal{D} : \mathbb{Q}] = [\mathcal{D} : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Comme P est irréductible dans $\mathbb{Q}[X]$ et annule α, P est le polynôme minimal de α sur $\mathbb{Q}[X]$.
Donc $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(P) = p$, ce qui prouve que $p || \mathrm{Gal}(\mathcal{D}/\mathbb{Q})|$.

Remarque 3.

Un autre argument est possible, en passant par les actions de groupes (donc à utiliser si le développement est dans une leçon sur les groupes par exemple) :
$\mathrm{Gal}(\mathcal{D}/\mathbb{Q})$ agit transitivement sur les racines de P. Donc p (qui est le cardinal de l'unique orbite pour cette action) divise $|\mathrm{Gal}(\mathcal{D}/\mathbb{Q})|$.

D'après le théorème de Cauchy, il existe $\sigma \in G$ d'ordre p.
Ensuite, la restriction de la conjugaison complexe à $\mathcal{D}$ est un automorphisme qui permute les deux racines complexes de P et fixe les autres. G contient donc une transposition (c'est l'image de la conjugaison complexe par l'isomorphisme entre $\mathrm{Gal}(\mathcal{D}/\mathbb{Q})$ et G).
Ainsi, $\mathrm{Gal}(\mathcal{D}/\mathbb{Q}) \subset \mathfrak{S}_p$ contient une transposition et un p-cycle, qui engendrent $\mathfrak{S}_p$. Donc :

$$\boxed{\mathrm{Gal}(\mathcal{D}/\mathbb{Q}) \simeq \mathfrak{S}_p.}$$

□