École Polytechnique
Algèbre et théorie de Galois MAT 451

Contrôle classant du 11 septembre 2020 - 3 heures

Avertissement

Les calculatrices et documents autres que le polycopié de cours sont interdits. La rédaction doit être concise et précise. Les exercices sont indépendants. Il n'est pas nécessaire de terminer le sujet pour avoir une excellente note.

Exercice 1

On considère le polynôme

$$P(X) = X^5 - 4X^2 + 1.$$

1) Trouver un nombre premier p tel que la réduction de $P(X)$ dans $\mathbf{F}_p[X]$ n'a pas de racine dans $\mathbf{F}_{p^2}$.

2) Montrer que P est irréductible dans $\mathbf{Q}[X]$.

Soit S le groupe de Galois de P sur $\mathbf{Q}$.

3) Montrer que S s'identifie naturellement à un sous-groupe du groupe symétrique $\mathfrak{S}_5$.

4) Déterminer le nombre de racines réelles de P et en déduire que S contient une transposition.

5) Montrer que S contient un 5-cycle.

6) Montrer que S est isomorphe à $\mathfrak{S}_5$ [On pourra déterminer les sous-groupes de $\mathfrak{S}_5$ contenant un 5-cycle et une transposition].

Exercice 2

Soit p un nombre premier impair et $\xi = \exp(2i\pi/p) \in \mathbf{C}^*$.

1) Démontrer que $\mathbf{Q}[\xi]/\mathbf{Q}$ est une extension galoisienne.

2) Calculer $[\mathbf{Q}[\xi] : \mathbf{Q}]$ et donner le polynôme minimal de ξ sur $\mathbf{Q}$.

3) Montrer que le groupe de Galois $\mathrm{Gal}(\mathbf{Q}[\xi]/\mathbf{Q})$ est commutatif. Est-ce un groupe cyclique ?

4) Parmi les réponses à la question 3, lesquelles sont encore valables lorsque p n'est pas supposé premier ?

Pour $x \in \mathbf{F}_p^*$, on pose $\left(\frac{x}{p}\right)$ égal à 1 si x est un carré dans $\mathbf{F}_p^*$ et égal à -1 sinon.

5) Montrer que l'application

$$x \mapsto \left(\frac{x}{p}\right)$$

définit un morphisme de groupe de $\mathbf{F}_p^*$ vers le groupe $\{1, -1\}$ muni de la loi produit.

Soit

$$\tau = \sum_{a \in \mathbf{F}_p^*} \left(\frac{a}{p}\right) \exp\left(\frac{2i\pi a}{p}\right).$$

6) Expliquer pourquoi τ est bien défini.
7) Montrer que $\tau \neq 0$.
8) Pour $g \in \mathrm{Gal}(\mathbf{Q}[\xi]/\mathbf{Q})$, déterminer $g(\tau)$.
9) En déduire que $\tau^2 \in \mathbf{Q}^*$.
10) En déduire également que $\tau \notin \mathbf{Q}^*$.

Exercice 3

L'objectif de l'exercice est d'établir une méthode attribuée à Kronecker, mais probablement déjà connue de Galois, permettant de ramener le calcul du groupe de Galois d'un polynôme à un problème de factorisation de polynômes.
Soit

$$f(X) = X^d + a_1 X^{d-1} + \cdots + a_d \in K[X]$$

un polynôme unitaire, de degré d, séparable et à coefficients dans un corps K, et $\xi_1, \ldots, \xi_d$ ses racines dans un corps de décomposition noté L. On a donc une factorisation dans $L[X]$

$$f(X) = \prod_{i=1}^{d} (X - \xi_i).$$

On définit la *résolvante de Kronecker* de f comme

$$R(X, Y_1, \cdots, Y_d) = \prod_{\sigma \in \mathfrak{S}_d} \left(X - \sum_{i=1}^{d} Y_i \xi_{\sigma(i)}\right) \in L[X, Y_1, \ldots, Y_d]$$

avec des indeterminées $X, Y_1, \ldots, Y_d$.

1) Montrer que le polynôme R est invariant par l'action du groupe $\mathfrak{S}_d$ agissant par permutation des variables $Y_1, \ldots, Y_d$.

2) Montrer que le polynôme R est, en fait, à coefficients dans K, c'est-à-dire que

$$R \in K[X, Y_1, \ldots, Y_d].$$

Soit h un facteur irréductible quelconque de R dans $K[X, Y_1, \ldots, Y_d]$, choisi unitaire comme polynôme en X.
Soit $G = \mathrm{Gal}(L/K)$ le groupe de Galois de f sur K. Il agit sur $L[X, Y_1, \ldots, Y_d]$ coefficients par coefficients, en laissant $X, Y_1, \cdots, Y_d$ invariantes.

3) Montrer que si $(X - \sum_{1 \leq i \leq d} Y_i \xi_i)$ est un facteur de h dans $L[X, Y_1, \ldots, Y_d]$, alors

$$h = \prod_{g \in G} \big(X - \sum_{1 \leq i \leq d} Y_i g(\xi_i)\big).$$

Soit S_h le sous-groupe de $\mathfrak{S}_d$ formé des permutations $\sigma \in \mathfrak{S}_d$ (permutant les Y_i) qui laissent h invariant.

4) Déterminer le cardinal de S_h en fonction de h [On pourra considérer h comme un polynôme en X].

On dit que deux sous-groupes H_1, H_2 de $\mathfrak{S}_d$ sont conjugués dans $\mathfrak{S}_d$ si il existe σ dans $\mathfrak{S}_d$ tel que $\sigma H_1 \sigma^{-1} = H_2$.

5) Est-ce que S_h est conjugué, dans $\mathfrak{S}_d$, à G ? (ici G est vu comme un groupe de permutations de $\{\xi_i\}_{1 \leq i \leq d}$).

Question bonus facultative : Montrer que les problèmes suivants sont résolubles algorithmiquement :

- Décomposer un élément de $K[X]$ en facteurs irréductibles.
- Décomposer un élément de $K[T_1, \ldots, T_n]$ en facteurs irréductibles, en supposant algorithmiques les opérations dans K et le fait de décomposer un élément de $K[X]$ en facteurs irréductibles.

On pourra introduire la "factorisation de Kronecker" envoyant un polynôme $f \in K[T_1, \ldots, T_n]$ sur $S_e(f) := f(X, X^e, X^{e^2}, \ldots, X^{e^{n-1}}) \in K[X]$ où l'on choisit e entier strictement supérieur au degré de f dans n'importe laquelle des variables T_i.