École Polytechnique
Algèbre et théorie de Galois MAT 451

Contrôle classant du 4 avril 2018 - 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.

Dans tout le sujet on suppose le critère d'Eisenstein connu.

Exercice 1

Pour n un entier naturel, on note

$$\phi_n(X) \in \mathbf{Z}[X]$$

le n-ème polynôme cyclotomique.

1) Calculer $\phi_n(X)$ quand $n = p$ est un nombre premier.

2) Soit $n = p^r$ la puissance d'un nombre premier. Montrer que les coefficients de $\phi_n(X)$ sont positifs.

Pour n un entier, on note $\phi(n)$ l'indicatrice d'Euler, c'est-à-dire le nombre d'entiers m premiers avec n et tels que $1 \leq m \leq n$. On rappelle que c'est aussi le degré de $\phi_n(X)$.

3) Calculer $\phi_6(X)$. Commentaire ?

4) Proposer une preuve directe (sans utiliser de réduction modulo p) de l'irréductibilité de $\phi_6(X)$ dans $\mathbf{Q}[X]$.

5) Est-ce que le polygône régulier à 6 côtés est constructible ?

6) Déterminer l'ensemble des éléments du groupe de Galois du corps de décomposition de $\phi_6(X)$.

On considère à présent le polynôme cyclotomique $\phi_{12}(X)$.

7) Calculer son degré $\phi(12)$.

Soit G le groupe de Galois du corps de décomposition K de $\phi_{12}(X)$.

8) Donner deux sous-corps de K de degré 2 sur $\mathbf{Q}$.

9) En déduire l'existence d'un morphisme de groupe

$$\Phi : G \to (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z}).$$

10) Montrer que Φ est un isomorphisme.

11) Rappeler pourquoi il existe un morphisme de groupe injectif vers le groupe symétrique

$$\Psi : G \to S_{\phi(12)}.$$

12) Décrire l'image $\Psi(G)$ dans le groupe symétrique $S_{\phi(12)}$.

Exercice 2

On considère le polynôme à coefficients rationnels

$$P(X) = X^4 - 12X^2 + 25 \in \mathbf{Q}[X].$$

1) Est-ce que $P(X)$ est irréductible dans $\mathbf{Q}[X]$?

Soit K le corps de décomposition de P dans $\mathbf{C}$.

2) Rappeler pourquoi $K/\mathbf{Q}$ est une extension galoisienne.

3) Trouver deux éléments $\alpha, \beta \in \mathbf{C}$ tels que $K = \mathbf{Q}[\alpha, \beta]$ et $\alpha\beta \in \mathbf{Q}$.

4) Montrer que $[K : \mathbf{Q}] = 4$.

Soit $G = \mathrm{Gal}(K/\mathbf{Q})$.

5) Montrer que pour $\sigma \in G$ et $x = \sigma(\alpha)$, on a $\sigma(x) = \alpha$.

6) Est-ce que G est un groupe cyclique ? (c'est-à-dire isomorphe à un groupe $\mathbf{Z}/n\mathbf{Z}$ avec $n > 0$).

7) Rappeler pourquoi il existe un morphisme de groupe injectif vers le groupe symétrique

$$\Psi : G \to S_4.$$

8) Est-ce que l'image de Ψ contient des transpositions ?

9) Déterminer l'image de Ψ.

10) En déduire le nombre de sous-corps de K.

11) Déterminer ces sous-corps.

Exercice 3.

Soit K un corps et $q(X_1, \cdots, X_n)$ un polynôme en n variables à coefficients dans K et de la forme

$$q(X_1, \cdots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{i,j} X_i X_j$$

avec les $a_{i,j} \in K$ non tous nuls.

On suppose qu'il existe une extension L/K de degré fini impair dans laquelle q admet un zéro non-trivial, c'est-à-dire qu'il existe un n-uplet

$$(x_1, \cdots, x_n) \in L^n \setminus \{(0, \cdots, 0)\}$$

tel que

$$q(x_1, \cdots, x_n) = 0.$$

On va montrer que q admet alors un zéro non trivial dans K (théorème de Springer).

1) Donner un contre-exemple dans le cas d'une extension de degré pair. Dans la suite L/K satisfaisant les conditions ci-dessus est supposée de degré impair.

2) Rappeler pourquoi si K est parfait, l'extension L/K est monogène (c'est-à-dire qu'il existe $\alpha \in L$ tel que $L = K[\alpha]$).

3) Montrer que si $n = 2$, alors l'extension $K[x_1, x_2]/K$ est monogène.

4) Montrer que si $n = 3$, alors q admet un zéro non-trivial dans une sous-extension monogène de L.

5) Montrer que pour démontrer le théorème de Springer, il suffit traiter le cas où L/K est monogène.

On suppose dans la suite que L/K est monogène. Soit $\alpha \in L$ tel que $L = K[\alpha]$. On notera $d = [L : K]$ et P le polynôme minimal de α dans $K[X]$.

6) Montrer qu'il existe des polynômes $P_1, \cdots, P_n \in K[X]$ de degré strictement inférieur à d, premiers entre eux dans leur ensemble[1], tels que P divise dans $K[X]$ le polynôme

$$Q(X) = q(P_1(X), \cdots, P_n(X)).$$

Notons

$$\delta = \mathrm{Max}_{1 \leq i \leq n} \deg(P_i).$$

7) Montrer que si $\deg(Q(X)) < 2\delta$, alors q admet un zéro non-trivial dans K.

8) Montrer que si $\deg(Q(X)) = 2\delta$, alors q admet un zéro non trivial dans une extension L'/K de degré impair telle que $[L' : K] < d$.

9) Conclure.

10) Que dire si q est remplacée par une expression de la forme

$$\sum_{1 \leq i \leq j \leq k \leq n} a_{i,j,k} X_i X_j X_k \ ?$$

Exercice 4

Soit G un groupe fini. Est-ce qu'il existe une extension galoisienne finie de corps parfaits dont le groupe de Galois est isomorphe à G ?

[1] C'est-à-dire que seuls les polynômes constants divisent simultanément les n polynômes.