École Polytechnique
Algèbre et théorie de Galois MAT 451

Contrôle classant du 3 juin 2021 - 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

$$P(X) = X^8 - 1 \in \mathbf{F}_2[X].$$

1) Factoriser P en produit de polynômes irréductibles dans $\mathbf{F}_2[X]$.
2) Quel est le corps de décomposition de $P(X)$ sur $\mathbf{F}_2$?

On considère à présent le polynôme

$$Q(X) = X^8 - 1 \in \mathbf{F}_3[X].$$

3) Montrer que $G = \mathrm{Gal}(Q, \mathbf{F}_3)$ est isomorphe à un sous-groupe de $(\mathbf{Z}/2\mathbf{Z})^2$.
4) Factoriser Q en produit de polynômes irréductibles dans $\mathbf{F}_3[X]$.
5) Quel est le corps de décomposition de Q sur $\mathbf{F}_3$?

Exercice 2

On considère

$$\alpha = (1 + \sqrt{3})^{\frac{1}{3}}.$$

1) Déterminer $[\mathbf{Q}[\alpha] : \mathbf{Q}]$.

Soit $K \subset \mathbf{C}$ le corps engendré par les conjugués de α sur $\mathbf{Q}$.

2) Exprimer K en fonction α, $j = \exp(2i\pi/3)$ et $\beta = (1 - \sqrt{3})^{\frac{1}{3}}$.
3) Montrer que $[K : \mathbf{Q}]$ est 12, 24 ou 36.

4) Montrer que $G = \mathrm{Gal}(K/\mathbf{Q})$ est isomorphe à un sous-groupe du groupe symétrique S_6. Est-ce que G est commutatif ?

5) Montrer que G admet un quotient G' d'ordre 4 isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$.

6) Montrer qu'il existe $\sigma \in G$ dont l'image dans S_6 est une double transposition. Quelle est l'image de σ dans G' ?

7) Montrer que $K' = \mathbf{Q}[j, \sqrt{3}, 2^{\frac{1}{3}}]$ est une sous-extension galoisienne de K dont on calculera le degré $[K' : \mathbf{Q}]$.

8) Montrer qu'il existe une suite exacte

$$0 \to (\mathbf{Z}/3\mathbf{Z}) \to \mathrm{Gal}(K'/\mathbf{Q}) \to (\mathbf{Z}/2\mathbf{Z})^2 \to 0$$

9) Montrer que les éléments de $\mathrm{Gal}(K'/\mathbf{Q})$ sont d'ordre 1, 2, 3 ou 6.

10) Déterminer les sous-corps de K' de degré 2 et de degré 4 sur $\mathbf{Q}$.

11) Montrer que $\mathrm{Gal}(K/K')$ est commutatif. Est-ce que G est un groupe résoluble ?

12) Montrer que $\sqrt{3} \notin \mathbf{Q}[2^{\frac{1}{3}}]$. En déduire $[K : \mathbf{Q}]$ est 12 ou 36.

13) Si on suppose que l'équation $0 = x^3 - 3x^2 + 9x - 3$ n'a pas de solution dans $\mathbf{Q}[2^{\frac{1}{3}}]$, quelle est la valeur de $[K : \mathbf{Q}]$?

Exercice 3

On souhaite montrer qu'un groupe commutatif fini peut être réalisé comme groupe de Galois d'une extension galoisienne de $\mathbf{Q}$.
On rappelle que pour G et G' deux groupes, on a une structure de groupe sur le produit $G \times G'$, la loi étant définie par

$$(g_1, g_1')(g_2, g_2') = (g_1 g_2, g_1' g_2') \text{ pour } g_1, g_2 \in G \text{ et } g_1', g_2' \in G'.$$

Pour k un entier positif, on considère l'entier

$$F_k = 1 + 2^{(2^k)}.$$

1) Montrer que pour $j \neq k$, F_k et F_j sont premiers entre eux.

Soit p_k un nombre premier qui divise F_k.

2) Montrer que 2 est inversible dans $(\mathbf{Z}/p_k\mathbf{Z})$ et calculer son ordre dans le groupe des inversibles $(\mathbf{Z}/p_k\mathbf{Z})^*$.

3) Pour $1 \leq t \leq k+1$ entier, déterminer l'image de p_k dans $\mathbf{Z}/2^t\mathbf{Z}$.

4) Montrer que pour tout entier t, il existe une infinité de nombres premiers congrus à 1 modulo 2^t.

On cherche à présent à généraliser ce résultat avec $p > 2$ premier à la place de 2.
Supposons qu'il existe un nombre fini de nombre premiers $\{q_1, \cdots, q_r\}$ congrus à 1 modulo p^t. Ici $t \geq 1$ est un entier fixé.
Soit $a = 2q_1 \cdots q_r$ et $c = a^{(p^{t-1})}$.

5) Montrer que c est congru à 2 modulo p.
6) Montrer que $c - 1$ et $M = 1 + c + \cdots + c^{p-1}$ sont premiers entre eux.

Soit q un nombre premier divisant M.

7) Montrer que a est inversible dans $(\mathbf{Z}/q\mathbf{Z})$ et calculer son ordre dans $(\mathbf{Z}/q\mathbf{Z})^*$.
8) Montrer que q vaut 1 modulo p^t et conclure.
On considère maintenant un groupe H cyclique d'ordre une puissance m d'un nombre premier.
9) Montrer qu'il existe une sous-extension d'une extension cyclotomique qui est une extension galoisienne de $\mathbf{Q}$ de groupe de Galois H.

Soit $n = p_1 \cdots p_i$ un produit de nombre premiers distincts.

10) Montrer que

$$\mathrm{Gal}(\mathbf{Q}[\exp(2i\pi/n)]/\mathbf{Q}) \simeq (\mathbf{Z}/(p_1\mathbf{Z}))^* \times \cdots \times (\mathbf{Z}/(p_i\mathbf{Z}))^*.$$

11) Soit $H = H_1 \times \cdots \times H_N$ un produit de groupes cycliques H_i dont les ordres sont des puissances m_i de nombres premiers. Montrer que H est le groupe de Galois d'une extension galoisienne de $\mathbf{Q}$.
12) Donner un exemple pour $H = (\mathbf{Z}/4\mathbf{Z}) \times (\mathbf{Z}/4\mathbf{Z})$.

On admet qu'un groupe commutatif fini est isomorphe à un produit de groupes cycliques.

13) Conclure.