École polytechnique

Contrôle classant du 14 avril 2010 MATH 451 Théorie de Galois

Durée 3 heures

Avertissement

Les calculatrices et documents autres que le polycopié de cours sont interdits. Il est interdit d'utiliser les téléphones portables durant l'épreuve. La rédaction doit être concise et précise. On énoncera clairement les théorèmes utilisés. Il est fortement recommandé de lire le sujet en entier. Il n'est nullement nécessaire de terminer le sujet pour avoir une excellente note. On privilégiera les copies ayant abordé significativement certains exercices plutôt que les questions résolues isolément.

Exercice 1.[Un lemme sur le groupe symétrique]

Soit p un nombre premier impair. On identifie le groupe symétrique S_p aux bijections de $\mathbf{Z}/p\mathbf{Z}$ et on note $\bar{m}$ la classe de l'entier m dans $\mathbf{Z}/p\mathbf{Z}$. Soient i, j deux entiers avec $1 \leq i < j \leq p$ et G le sous-groupe de S_p engendré par le cycle $(\bar{1}, \bar{2}, \cdots, \bar{p})$ et la transposition $(\bar{i}, \bar{j})$.

1) Montrer que pour tout $k \in \mathbf{Z}$, on a $(\bar{i} + \bar{k}, \bar{j} + \bar{k}) \in G$ puis que

$$(\bar{i} + k\overline{(j-i)}, \bar{i} + (k+1)\overline{(j-i)}) \in G.$$

2) Montrer par récurrence sur $k \in [1, \cdots, p-1]$

$$(\bar{i}, \bar{i} + k\overline{(j-i)}) \in G.$$

3) Montrer que l'équation $\bar{i} + \bar{k}\overline{(j-i)} = \bar{i} + 1$ a une solution $\bar{k} \in (\mathbf{Z}/p\mathbf{Z})^*$.

4) Montrer que $(\bar{i}, \bar{i} + 1) \in G$ puis

$$\forall \bar{t} \in \mathbf{Z}/p\mathbf{Z},\ (\bar{t}, \bar{t} + 1) \in G.$$

5) Montrer $G = S_p$.

6) Soit c un p-cycle et τ une transposition de S_p. Montrer que S_p est engendré par c et τ.

7) [Plus difficile] Montrer que le résultat précédent tombe en défaut si on ne suppose pas p premier.

Exercice 2.[Un lemme sur les corps finis]

Soient k un corps et $P \in k[X]$ de degré $n > 0$.

1) Montrer que si P est réductible, il a une racine dans une extension de k de degré $\leq n/2$.

Soient p un nombre premier et $P \in \mathbf{F}_p[X]$ de degré $n > 0$.

2) Montrer que P est irréductible si et seulement si il n'a pas de racine dans les corps $\mathbf{F}_{p^d}, d \leq n/2$.

3) Conclure de la question précédente que P est irréductible si et seulement si

$$\forall d,\ 1 \leq d \leq n/2,\ \mathrm{PGCD}(P, X^{p^d} - X) = 1.$$

Exercice 3.[Un groupe de Galois] Soit $P = X^5 - X + 3 \in \mathbf{Q}[X]$ et G son groupe de Galois sur $\mathbf{Q}$.

1) Montrer que P est séparable. En déduire que G se plonge dans S_5.

2) Factoriser P dans $\mathbf{F}_3[X]$

3) Montrer que P est irréductible dans $\mathbf{F}_5[X]$. [On pourra utiliser l'exercice 2].

4) Montrer que G est isomorphe à S_5 [On pourra utiliser l'exercice 1].

5) Montrer que P est irréductible sur $\mathbf{Q}$.

6) Existe-t-il un entier $n > 0$ tel qu'au moins une racine de P soit contenue dans $\mathbf{Q}[\exp(\frac{2i\pi}{n})]$?

Exercice 4.[Un autre groupe de Galois] On munit $\mathbf{C}$ de sa structure de plan euclidien orienté dans le sens trigonométrique. Soit C l'ensemble des 4 sommets d'un carré et ω son centre. On note Γ le sous-groupe des bijections g de C telles

$$\forall x, y \in C,\ |g(x) - g(y)| = |x - y|.$$

Soit ρ la rotation de centre ω et d'angle $\frac{\pi}{2}$ et σ une symétrie par rapport à une diagonale de C (ou plutôt leurs restrictions à C).

1) Montrer que si $g \in \Gamma$ fixe deux sommets consécutifs de C, alors $g = \mathrm{Id}$.

2) Montrer l'égalité

$$\Gamma = \{\rho^\alpha, \rho^\beta\sigma,\ \alpha, \beta \in [1, \cdots, 4]\}$$

et qu'on a la formule $\sigma\rho\sigma = \rho^{-1}$.

3) Montrer que Γ est un groupe d'ordre 8 non abélien et qu'on a une suite exacte de groupes

$$1 \to \mathbf{Z}/4\mathbf{Z} \to \Gamma \to \mathbf{Z}/2\mathbf{Z} \to 1.$$

4) Donner tous les sous-groupes de Γ. Lesquels sont distingués ? En particulier, combien Γ a-t-il de sous-groupes d'ordre 2 ? 4 ?

Soit G le groupe de Galois sur $\mathbf{Q}$ de $X^4 - 2$, c'est à dire de $K/\mathbf{Q}$ où K est le sous-corps de $\mathbf{C}$ engendré par l'ensemble C des racines complexes de $X^4 - 2$. On pose $x = 2^{1/4}$.

5) Montrer que $L = \mathbf{Q}[x]$ est non galoisien sur $\mathbf{Q}$. En déduire que G est un groupe non commutatif.

6) Montrer $K = \mathbf{Q}[x, i]$ et $[K : \mathbf{Q}] = 8$. En déduire le cardinal de G.

7) Montrer que l'action de G sur C induit un isomorphisme de G sur Γ.

8) Montrer qu'il existe un unique élément $r \in G$ tel que $r(x) = ix$ et $r(i) = i$. Quel est l'ordre de r ?

9) Montrer qu'il existe un unique élément $s \in G$ tel que $s(i) = -i$ et $s(x) = x$. Quel est l'ordre de s ?

10) Montrer la formule $srs = r^{-1}$. Montrer en outre que s et r engendrent G.

11) Trouver tous les sous-corps de K. Lesquels sont galoisiens sur $\mathbf{Q}$? En particulier, combien y a-t-il de sous-corps de degré 2 ? 4 ?

12) Donner un élément primitif de K sur $\mathbf{Q}$.

Exercice 5.[Très difficile] Soit K/k une extension algébrique de corps parfaits. On suppose que tout polynôme non constant à coefficients dans k admet au moins une racine dans K. Montrer que K est une clôture algébrique de k.