Examen

13/12/2017. Durée : 3h

Aucun document, aucun appareil électronique autorisé. Le sujet contient 3 exercices indépendants.
On rédigera **lisiblement**, *en justifiant les réponses avec soin.*

Exercice 1.

On considère le polynôme $P(X) = X^6 - 25 \in \mathbb{Q}[X]$. On note K un corps de décomposition de P sur $\mathbb{Q}$.

1. Factoriser P en produit d'irréductibles de $\mathbb{Q}[X]$.
2. Donner un polynôme de degré 3 dont K est corps de décomposition sur $\mathbb{Q}$.

Dans la suite on voit K comme un sous-corps du corps des nombres complexes $\mathbb{C}$.

3. Montrer que $K = \mathbb{Q}(\sqrt[3]{5}, \omega)$ où $\sqrt[3]{5}$ est l'image de 5 par la fonction définie sur $\mathbb{R}_{>0}$ par $x \mapsto x^{1/3}$ et $\omega \neq 1$ est un nombre complexe satisfaisant $\omega^3 = 1$.
4. Justifier que $K/\mathbb{Q}$ est une extension galoisienne et que le groupe $G = \mathrm{Gal}(K/\mathbb{Q})$ s'identifie à un sous-groupe de $\mathcal{S}_3$ (le groupe symétrique sur 3 lettres).
5. Que vaut $[K : \mathbb{Q}]$? Justifier. Déduire que $G \simeq \mathcal{S}_3$.
   [On pourra introduire le corps intermédiaire $M = \mathbb{Q}(\sqrt[3]{5})$.]
6. Montrer qu'il existe des éléments τ et σ de G vérifiant respectivement
$$\tau(\omega) = \omega^2\,, \qquad \tau(\sqrt[3]{5}) = \sqrt[3]{5}\,,$$
$$\sigma(\omega) = \omega\,, \qquad \sigma(\sqrt[3]{5}) = \omega\sqrt[3]{5}\,.$$
7. Montrer qu'il n'existe pas d'élément $\theta \in G$ tel que $\theta(\sqrt[3]{5}) = \omega$.
8. On se donne des éléments σ et τ de G vérifiant les conditions de la question 6.
   (a) Quel est le sous-corps fixe de K par le sous-groupe $H = \langle \sigma\tau \rangle$ engendré la composée des éléments σ et τ de G ?
   [On pourra calculer d'abord l'ordre de la composée $\sigma\tau$.]
   (b) L'extension $K^H/\mathbb{Q}$, où $H = \langle \sigma\tau \rangle$, est-elle galoisienne ?

Exercice 2.

Soit k un corps fini à q éléments. On étudie dans cet exercice certaines propriétés des extensions finies de k. On rappelle que si L est un corps fini quelconque, le groupe multiplicatif $L^\times$ de L est cyclique.

1. Soit k' une extension finie de k.
   (a) Justifier que $|k'| = q^r$ pour un certain entier $r \geq 1$.
   (b) Donner un polynôme à racines simples $f(X) \in k[X]$ dont k' est un corps de décomposition sur k.
   (c) On note σ l'automorphisme de k' défini par $\sigma(x) = x^q$ pour tout $x \in k'$. Montrer que σ est d'ordre r dans le groupe des automorphismes de k'.
   (d) Déduire que k'/k est galoisienne de groupe de Galois cyclique.

2. On note p la caractéristique de k et on considère le polynôme $f(X) = X^q - X - 1 \in k[X]$. On note k_f un corps de décomposition de f sur k et, comme dans la question précédente, on note σ l'automorphisme de k_f défini par $\sigma(x) = x^q$ pour tout $x \in k_f$.
   (a) Soit α une racine de f dans k_f. Calculer $\sigma(\alpha)$. En déduire σ^p.
   (b) Déduire quel est le degré des facteurs irréductibles de f sur k.
   (c) Montrer que le corps de rupture associé à l'un quelconque des facteurs irréductibles de f sur k est isomorphe à k_f.

Exercice 3.

1. Soit G un groupe agissant sur des ensembles finis X et Y (dans les deux cas on note $g \cdot x$ l'action de $g \in G$ sur x, élément de X ou Y). On suppose que G agit *transitivement* sur Y, et qu'il existe $f\colon X \to Y$ tel que
$$\forall g \in G \,, \forall x \in X \,, f(g \cdot x) = g \cdot f(x) \,. \qquad (\star)$$
   (a) Montrer que pour tout $y, y' \in Y$, les images réciproques $f^{-1}(y)$ et $f^{-1}(y')$ sont en bijection.
   (b) Déduire que $|Y|$ divise $|X|$.
2. Soit G un groupe fini et p un nombre premier. On se donne un sous-groupe *distingué* N de G. On souhaite appliquer la première question pour montrer que $n_p(N) \mid n_p(G)$ (où, pour tout groupe fini H, on désigne par $n_p(H)$ le nombre de p-Sylow de H).
   (a) Justifier que l'application $P \mapsto P \cap N$ envoie un p-Sylow P de G sur un p-Sylow de N.

   On note $f\colon \{p\text{-Sylow de } G\} \to \{p\text{-Sylow de } N\}$ l'application ainsi définie.
   (b) Montrer que l'application f vérifie bien $(\star)$, où l'on considère l'action par conjugaison de G sur ses p-Sylow ainsi que sur les p-Sylow de N.
   (c) Conclure, et illustrer la nécessité de l'hypothèse $N \triangleleft G$ en considérant le nombre de 3-Sylow des groupes alternés $\mathcal{A}_4$ et $\mathcal{A}_5$.

FIN

Correction disponible sur `www.math.u-bordeaux.fr/~fjouve001` à partir de 9h environ le 14/12.