Université de Tours
Master de Mathématiques

Examen

Algèbre approfondie — Semestre 2

L'épreuve dure 4h. Les exercices sont indépendants. La notation tiendra compte de la clarté de la rédaction. Toute affirmation doit être justifiée.

Questions de Cours/Td

1) Déterminer le corps de décomposition E de $P = X^4 - 1 \in \mathbb{Q}[X]$ et calculer $[\mathbb{E} : \mathbb{Q}]$.
2) Soit $\mathbb{E} : \mathbb{F}$ une extension de corps.
   (a) Définir le groupe de Galois de $G := \mathsf{Gal}(\mathbb{E} : \mathbb{F})$ et montrer que c'est bien un groupe.
   (b) Soit H un sous-groupe de G. Montrer que
   $$\mathsf{Fix}(H) = \{x \in \mathbb{E} \mid \theta(x) = x, \forall \theta \in H\}$$
   est un sous-corps de $\mathbb{E}$ contenant $\mathbb{F}$.
   (c) Soit $\theta \in G$ et soit $P \in \mathbb{F}[X]$. Montrer que si $\alpha \in \mathbb{E}$ vérifie $P(\alpha) = 0$ alors $P(\theta(\alpha)) = 0$.
3) Soit p un nombre premier. Calculer $\Phi_p \in \mathbb{Q}[X]$ et montrer que Φ_p est irréductible sur $\mathbb{Q}$.
   [On pourra utiliser la formule $X^n - 1 = \prod_{d|n} \Phi_d$.]
4) Soit p un nombre premier et $\xi_p = e^{\frac{2i\pi}{p}}$. Montrer que $\mathsf{Gal}(\mathbb{Q}(\xi_p) : \mathbb{Q})$ est isomorphe à $\mathbb{F}_p^\times$.

Exercice 1. Soit $\mathbb{E}$ le corps de décomposition du polynôme $P = X^4 - 7X \in \mathbb{Q}[X]$.
1) Déterminer $\mathbb{E}$ et calculer le degré $[\mathbb{E} : \mathbb{Q}]$.
2) Déterminer l'ordre et la structure de $G = \mathsf{Gal}(\mathbb{E} : \mathbb{Q})$.
3) Écrire la correspondance de Galois pour $\mathbb{E} : \mathbb{Q}$.

Exercice 2. Soit $n \in \mathbb{N}^*$.
1) Montrer que si $\cos(2\pi/n) \in \mathbb{Q}$ alors $\cos(2\pi k/n) \in \mathbb{Q}$ pour tout $k \in \mathbb{N}$.
2) Montrer que si $\cos(2\pi/n) \in \mathbb{Q}$ alors $[\mathbb{Q}(t^k) : \mathbb{Q}] \leq 2$ pour tout $k \in \mathbb{N}$ où $t = e^{2\pi i/n}$.
   [Considérer le polynôme $X^2 - 2\cos(2\pi k/n)X + 1$.]
3) Soit p un nombre premier positif. Montrer que si $\cos(2\pi/n) \in \mathbb{Q}$ et si $p \mid n$ alors $p = 2, 3$.
   [Remarquer que si $t = e^{2\pi i/n}$ et $n = p\ell$ alors $t^\ell = e^{2\pi i/p}$.]
4) (a) Montrer en utilisant les polynômes cyclotomiques, que
   $$[\mathbb{Q}(e^{2\pi i/8}) : \mathbb{Q}] = 4, \quad [\mathbb{Q}(e^{2\pi i/9}) : \mathbb{Q}] = 6 \quad \text{et} \quad [\mathbb{Q}(e^{2\pi i/12}) : \mathbb{Q}] = 4.$$
   (b) Trouver tous les entiers $n > 0$ tels que $\cos(2\pi/n) \in \mathbb{Q}$.

Exercice 3. Soit $P = X^9 - X + 1 \in \mathbb{F}_3[X]$.
1) Soit $\mathbb{K}$ un corps fini à p^n éléments. Montrer que tout élément x de $\mathbb{K}$ est racine de $X^{p^n} - X$.
2) Montrer que P n'a pas de racines dans $\mathbb{F}_3$ ni dans $\mathbb{F}_9$.
3) Montrer que le polynôme $Q = X^3 - X - 1$ est irréductible sur $\mathbb{F}_3$. En déduire que $\mathbb{L} := \mathbb{F}_3[X]/\langle Q \rangle$ est un corps fini dont on déterminera le cardinal. On note $\alpha \in \mathbb{L}$ la classe de X dans $\mathbb{L}$.
4) Déterminer les racines de Q dans $\mathbb{L}$ (on pourra étudier la différence de deux racines de Q).
5) Montrer que toute racine de Q dans $\mathbb{L}$ est une racine de P.
6) Montrer que toute racine de P dans $\mathbb{L}$ est une racine de Q.
   [On pourra utiliser le fait que le morphisme de Frobenius permute les racines de P.]
7) En déduire une factorisation de P en irréductible sur $\mathbb{F}_3[X]$.
   [On pourra utiliser le résultat suivant : Soit $P \in k[X]$ un polynôme de degré $n \in \mathbb{N}^*$. Alors P est irréductible si et seulement si P n'a pas de racine dans toutes les extensions $\mathbb{E}$ de k telles que $[\mathbb{E} : \mathbb{F}] \leq n/2$.]
8) Déterminer l'ordre de α dans le groupe $\mathbb{L}^\times$. En déduire l'ordre de $-\alpha$.

Exercice 4. Le théorème fondamental de l'algèbre affirme que tout polynôme complexe de degré supérieur ou égal à 1 admet une racine. L'objectif de cet exercice est de prouver ce théorème à l'aide de la théorie de Galois. Nous aurons besoin des deux résultats suivants que vous pouvez utiliser :

(R1) Tout groupe d'ordre $2^m \cdot n$ où n est impair possède un sous groupe d'ordre 2^m.

(R2) Un groupe d'ordre 2^m possède un sous groupe d'ordre 2^k pour tout $k \in \{0, \dots, m\}$.

1) (a) Montrer qu'il n'existe pas d'extension de $\mathbb{R}$ de degré impair.

   (b) Montrer qu'il n'existe pas d'extension de $\mathbb{C}$ de degré 2.
   [Aide : Vous pouvez utiliser le fait que tout nombre complexe admet une racine carrée.]

2) Montrer qu'il suffit de prouver que tout polynôme de $\mathbb{R}[X]$ admet une racine complexe.
[Aide : Si $P \in \mathbb{C}[X]$ on pourra considérer le polynôme $P\overline{P}$.]

3) Soit $P \in \mathbb{R}[X]$ et soit $\mathbb{E}$ le corps de décomposition de P. On considère l'extension $\mathbb{E}(i) : \mathbb{R}$ et on pose

$$[\mathbb{E}(i) : \mathbb{R}] = 2^m \cdot n \quad \text{où} \quad n \text{ est impair.}$$

   (a) Montrer que $\mathbb{E}(i)$ est le corps de décomposition d'un polynôme de $\mathbb{R}[X]$. En déduire que le groupe de Galois $G := \mathsf{Gal}(\mathbb{E}(\mathsf{i}) : \mathbb{R})$ est d'ordre $2^m \cdot n$.

   (b) A l'aide de (R1) et de la correspondance de Galois, montrer que $n = 1$.

   (c) A l'aide de (R2) et de la correspondance de Galois, montrer que $m = 1$.

   (d) Montrer que $[\mathbb{E}(i) : \mathbb{C}] = 1$ et conclure.