Université de Tours
Master de Mathématiques

Partiel

Algèbre approfondie — Semestre 2

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

Questions de Cours/Td

1) Soit $\varphi : R \to S$ un morphisme d'anneaux unitaires tels que $\varphi(1_R) = 1_S$.
   (a) Montrer que $\ker \varphi$ est un idéal de R.
   (b) Montrer que $\operatorname{Im} \varphi$ est un sous-anneau unitaire de S.
   (c) Montrer si R est un corps alors φ est injectif.
   (d) Montrer que si S est intègre alors $\ker \varphi$ est un idéal premier.
2) Soit $\mathbb{F}$ un corps et soit $P \in \mathbb{F}[X]$ un polynôme de degré 2 ou 3.
   (a) Montrer que P est irréductible si et seulement si P n'admet pas de racine.
   (b) Le critère ci-dessus reste-t-il vrai pour un polynôme de degré 4 ?
   (c) Déterminer tous les polynômes irréductibles de degré inférieur ou égal à 4 dans $\mathbb{F}_2[X]$.

Exercice 1. Soit $P = X^3 + X + 1 \in \mathbb{F}_3[X]$ où $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ est un corps.
1) Déterminer les racines de P dans $\mathbb{F}_3$. En déduire la factorisation de P dans $\mathbb{F}_3$.
2) Soit Q le facteur premier de P de degré ≥ 2 et soit $\mathbb{E} = \mathbb{F}_3[X]/\langle Q \rangle$. Justifiez que $\mathbb{E}$ est un corps.
3) On pose $\alpha = \overline{X} \in \mathbb{E}$. Factoriser Q puis P dans $\mathbb{E}[X]$.
4) Calculer $[\mathbb{E} : \mathbb{F}_3]$.

Exercice 2.
1) Soit p un nombre premier et soit

$$\begin{array}{rccc} \tilde{\pi}_p : & \mathbb{Z}[X] & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})[X] \\ & \sum a_i X^i & \longmapsto & \sum \pi(a_i) X^i \end{array}$$

   où π est la projection canonique de $\mathbb{Z}$ dans $\mathbb{Z}/p\mathbb{Z}$.
   (a) Soit $P = \sum_{i=1}^{n} a_i X^i$ un polynôme de degré n tel que $p \nmid a_n$ et $\tilde{\pi}_p(P)$ est irréductible. Montrer que si P est primitif alors P est irréductible dans $\mathbb{Z}[X]$.
   (b) Pourquoi l'hypothèse $p \nmid a_n$ est-elle indispensable ? On donnera un exemple précis.
   (c) Montrer qu'il existe une infinité de polynômes unitaires de degré 2, 3 et 4 irréductibles dans $\mathbb{Z}[X]$.
2) On souhaite montrer que $P = X^5 + X^2 + X + 2 \in \mathbb{Z}[X]$ est irréductible sur $\mathbb{Z}$.
   (a) Montrer que le critère de la question 1 ne s'applique pas avec $p = 2$.
   (b) En considérant $\tilde{\pi}_2$ montrer que si P se factorise dans $\mathbb{Z}$ c'est nécessairement sous la forme QR où $\deg(Q) = 1$ et $\deg(R) = 4$.
   (c) Conclure.

Exercice 3.
1) Soit $P \in \mathbb{F}[X]$ un polynôme de degré $n \in \mathbb{N}^*$. Montrer que P est irréductible si et seulement si P n'a pas de racine dans les extensions $\mathbb{E}$ de $\mathbb{F}$ qui vérifie $[\mathbb{E} : \mathbb{F}] \leq n/2$.
2) On souhaite dans cette question montrer que $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2[X]$ en utilisant 1).
   (a) Construire un corps $\mathbb{F}_4$ à 4 éléments.
   (b) Montrer que $\mathbb{F}_4$ n'est pas isomorphe à $\mathbb{Z}/4\mathbb{Z}$.
   (c) On admet que toute extension $\mathbb{E}$ de $\mathbb{F}_2$ de degré deux est isomorphe à $\mathbb{F}_4$. Montrer que $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2[X]$.
3) On souhaite étudier le polynôme $X^4 + 1$ sur $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ et $\mathbb{F}_p$ avec p premier.

(a) Décomposer X^4+1 en produits d'irréductibles de $\mathbb{C}[X]$.

(b) Décomposer X^4+1 en produits d'irréductibles de $\mathbb{R}[X]$.

(c) Décomposer X^4+1 en produits d'irréductibles de $\mathbb{Q}[X]$.

(d) Décomposer X^4+1 en produits d'irréductibles de $\mathbb{Z}[X]$.

(e) Décomposer X^4+1 en produits d'irréductibles de $\mathbb{F}_2[X]$.

(f) Soit $p \geq 3$. On admet qu'il existe une unique extension $\mathbb{F}_{p^2}$ de $\mathbb{F}_p$ de degré 2 à isomorphisme près et que $\mathbb{F}_{p^2}^*$ est cyclique. On souhaite montrer que X^4+1 est réductible sur $\mathbb{F}_p$ en utilisant 1).

(i) Montrer que $X^4+1 \mid X^8-1$ dans $\mathbb{F}_p[X]$.

(ii) Montrer que p^2-1 est un mutiple de 8 et que $\mathbb{F}_{p^2}^*$ possède un élément d'ordre 8.

(iii) En déduire que X^4+1 admet une racine dans $\mathbb{F}_{p^2}$.

(iv) Conclure.

Exercice 4. Soit $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}, j)$ où $j = e^{\frac{2i\pi}{3}}$ une extension de $\mathbb{Q}$ incluse dans $\mathbb{C}$.

1) Déterminer $[\mathbb{Q}(j) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$.

2) Déterminer $[\mathbb{K} : \mathbb{Q}]$ puis une base de $\mathbb{K}$ sur $\mathbb{Q}$ à l'aide du théorème de la base télescopique.

3) Soit $x \in \mathbb{K}$ tel que $x^2 \in \mathbb{Q}$. En raisonnant par l'absurde et en considérant $\mathbb{Q}(x, j)$, montrer que l'on a nécessairement $x \in \mathbb{Q}(j)$.

4) Déterminer tous les éléments x de $\mathbb{K}$ tel que $x^2 \in \mathbb{Q}$.

5) Montrer que $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$ sont 3 extensions de $\mathbb{Q}$ de degré 3.

6) Soit $\mathbb{L}$ une extension de $\mathbb{Q}$ incluse dans $\mathbb{K}$ de degré 3. Dans cette question on souhaite montrer que $\mathbb{L}$ est égale à une des 3 extensions de la question précédente. On raisonne par l'absurde et on suppose que ce n'est pas le cas.

(a) Montrer que $\mathbb{L}$ ne contient aucune des racines complexes de X^3-2.

(b) En déduire que $[\mathbb{K} : \mathbb{Q}] \geq 9$ et conclure.