Université Claude Bernard Lyon 1 Semestre de printemps 2025
L3 Anneaux et Corps

2me session
Mercredi 25 juin 2025 — 11h – 12h30
Documents et calculettes interdits
Le barème est donné à titre indicatif

Exercice 1 : (8 pts) Soit ω une racine primitive cube de l'unité, et $\beta = i + \sqrt[3]{2}$. On cherche à déterminer le degré $[\mathbb{Q}(\beta) : \mathbb{Q}]$ et le polynôme minimal de β.

1. Déterminer le degré de l'extension $[\mathbb{Q}(i, \omega) : \mathbb{Q}]$.
2. Montrer que $\mathbb{Q} < \mathbb{Q}(\beta) \leq \mathbb{Q}(i, \sqrt[3]{2})$ et calculer $[\mathbb{Q}(i, \sqrt[3]{2}) : \mathbb{Q}]$.
3. Montrer que si $\mathbb{Q}(\beta) < \mathbb{Q}(i, \sqrt[3]{2})$ alors $i \notin \mathbb{Q}(\beta)$, $\sqrt[3]{2} \notin \mathbb{Q}(\beta)$, et $\mathbb{Q}(\beta, i) = \mathbb{Q}(\beta, \sqrt[3]{2}) = \mathbb{Q}(i, \sqrt[3]{2})$.
   En déduire que $[Q(\beta) : \mathbb{Q}] = 3$ et $\mathbb{Q}(\beta)$ contient une racine de $X^3 - 2$.
   En déduire que $\omega \in \mathbb{Q}(\beta, i)$, et conclure que c'est impossible.
4. Calculer le polynôme minimal de β.

Exercice 2 : (8 pts)

1. Soit $\mathbb{F}_q$ un corps fini.
   (a) Si $\text{car}(\mathbb{F}_q) = 2$, montrer que $x \mapsto x^2$ est surjectif.
   (b) En caractéristique impaire, montrer que l'ensemble C des carrés est de cardinal $\frac{q+1}{2}$. En déduire que pour tout $a \in \mathbb{F}_q$ on a $a - C \cap C \neq \emptyset$.
   (c) En déduire que tout élément de $\mathbb{F}_q$ est la somme de deux carrés.
2. (a) Montrer que le polynôme $X^4 + 1$ est irréductible sur $\mathbb{Q}$.
   (b) Montrer que $X^4 + 1$ est réductible sur $\mathbb{F}_2$.
   (c) Montrer que pour p premier impair, $p^2 - 1 \equiv 0 \mod 8$. En déduire que $\mathbb{F}_{p^2}$ contient une racine primitive 8^{me} de l'unité.
   (d) En déduire que $X^4 + 1$ est réductible sur $\mathbb{F}_p$ pour tout p premier impair.

Exercice 3 : (8 pts) Soit A un anneau commutatif unitaire. Une partie S de A est dite *multiplicative* si elle est close par multiplication, et $0 \notin S$ mais $1 \in S$. Sur le produit $A \times S$ on pose une relation binaire $\sim$ par $(a, s) \sim (a', s')$ si et seulement s'il y a $s'' \in S$ avec $as's'' = a'ss''$.

1. Montrer que $\sim$ est une relation d'équivalence.
   Par la suite on va noter la classe d'équivalence de (a, s) modulo $\sim$ par $[a, s]$.
2. Soit $A_S = (A \times S)/\sim$ l'ensemble des classes d'équivalence. On pose deux opérations :

$$[a, s] \oplus [a', s'] = [as' + a's, ss'] \qquad \text{et} \qquad [a, s] \otimes [a', s'] = [aa', ss'].$$

   (a) Montrer que ces opérations sont bien définies et commutatives.
   (b) Montrer que $(A_S, \oplus)$ est un groupe abélien avec élément neutre $[0, 1]$.
   (c) Montrer que $\otimes$ est associative, avec élément neutre $[1, 1]$.
   (d) Montrer la loi distributive. En déduire que A_S est un anneau unitaire commutatif.
3. Montrer que l'application $f : a \mapsto [a, 1]$ est un morphisme d'anneau de A dans A_S. Déterminer son noyau.