Université Claude Bernard Lyon 1 — Anneaux et Corps - L3
Semestre de printemps 2023-2024

Examen 1 – Durée 120 min – le mardi 7 mai 2024

Les documents, les téléphones et les calculatrices ne sont pas autorisés.
La notation tiendra compte du soin apporté à la rédaction des réponses.
INDIQUER SON NUMÉRO DE GROUPE DE TD SUR LES COPIES (A,B ou Z)
L'énoncé comporte trois exercices indépendants.

IMPORTANT : merci de rendre deux copies une pour les exos 1 et une autre pour les exos 2 et 3.

Copie 1

Exercice 1. Les idéaux premiers de $\mathbb{Z}[X]$ Soit $\mathfrak{p}$ un idéal premier de $\mathbb{Z}[X]$.

1. L'anneau $\mathbb{Z}[X]$ est-il principal ? Justifier votre réponse.
2. Montrer qu'on a un morphisme injectif $\mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z}) \to \mathbb{Z}[X]/\mathfrak{p}$. En déduire que $\mathfrak{p} \cap \mathbb{Z} = \{0\}$ ou $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ avec p un nombre premier.

   Le but de la suite est de montrer que $\mathfrak{p}$ est engendré par un ou deux éléments.

3. On suppose ici que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. On note $\varphi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ la surjection canonique.
   (a) Montrer que $\varphi(\mathfrak{p})$ est un idéal premier de $\mathbb{F}_p[X]$ puis qu'il existe $P(X) \in \mathbb{Z}[X]$ unitaire tel que $\varphi(\mathfrak{p}) = \varphi(P(X))\mathbb{F}_p[X]$ où $\varphi(P(X)) \in \mathbb{F}_p[X]$ est irréductible.
   (b) Montrer que $\mathfrak{p} \supseteq (p, P(X))$.
   (c) Montrer que $\mathfrak{p} \subseteq (p, P(X))$.
4. On suppose ici que $\mathfrak{p} \cap \mathbb{Z} = \{0\}$ et $\mathfrak{p} \neq \{0\}$.
   (a) On note $\mathfrak{p}\mathbb{Q}[X]$ l'idéal de $\mathbb{Q}[X]$ engendré par les éléments de $\mathfrak{p}$. Montrer que $\mathfrak{p}\mathbb{Q}[X] = P(X)\mathbb{Q}[X]$ avec $P(X) \in \mathbb{Z}[X]$, $\mathrm{c}(P) = 1$.
   (b) Montrer que $\mathfrak{p} \subseteq P(X)\mathbb{Z}[X]$.
   (c) Soit $a \in \mathbb{Z}$. Montrer que si $aP \in \mathfrak{p}$ alors $P \in \mathfrak{p}$.
   (d) Montrer que $P(X)\mathbb{Z}[X] \subseteq \mathfrak{p}$.

Copie 2

Rappel : *On rappelle (pour la suite du sujet) que le groupe multiplicatif d'un corps fini est cyclique.*

Exercice 2. Inversibles de $\mathbb{Z}/p^2\mathbb{Z}$
Soit p un entier premier impair.

1. Quel est le cardinal du groupe $(\mathbb{Z}/p^2\mathbb{Z})^\times$ des inversibles de l'anneau $\mathbb{Z}/p^2\mathbb{Z}$?
2. Montrer que $1 + p$ est d'ordre p dans $(\mathbb{Z}/p^2\mathbb{Z})^\times$.
3. Soit $\varphi : \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}, \bar{k}\ [p^2] \longmapsto \bar{k}\ [p]$. Montrer que φ est un morphisme d'anneaux.
4. Montrer que le noyau de φ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
5. En déduire qu'il existe un élément x_0 de $(\mathbb{Z}/p^2\mathbb{Z})^\times$ d'ordre $p - 1$.
6. En déduire que $(\mathbb{Z}/p^2\mathbb{Z})^\times$ est cyclique.

Tounez SVP

Exercice 3. Un Polynôme irréductible... ou pas. Soit $P(X) = X^4 + 1$.

1. Montrer que $P(X+1)$ est irréductible dans $\mathbb{Q}[X]$.
2. En déduire que P est irréductible dans $\mathbb{Q}[X]$.
3. Montrer que P n'est pas irréductible sur $\mathbb{F}_2$.
4. On suppose à partir de maintenant p est un nombre premier impair.
   (a) Montrer que si P a une racine dans $\mathbb{F}_p$ alors 8 divise $p-1$.
   (b) Montrer que réciproquement, si 8 divise $p-1$ alors P est scindé à racines simples sur $\mathbb{F}_p$.
5. Montrer que 8 divise $p^2 - 1$.
6. En déduire que P est scindé à racines simples dans $\mathbb{F}_{p^2}$.
7. En déduire que P n'est pas irréductible sur $\mathbb{F}_p$.