L3 Algèbre 2 Année 2016/2017

Contrôle 9 mars

— JUSTIFIER TOUTES VOS REPONSES !
— Il n'est pas necessaire de tout faire pour avoir la note maximale.
— You can write in english.

Exercice 1

1. (a) Donner un exemple d'un anneau factoriel qui n'est pas principal.
   (b) Soit K un corps commutatif et on considère l'anneau $A = K[X,Y]/(Y^2 - X^3 - X)$
      i. Montrer que $Y^2 - X^3 - X \in K[X][Y]$ est irrèductible et en déduire que A est intègre.
      ii. Montrer que $\bar{Y} \in A$ est irrèductible. [Indication : tout élément de A a la forme $\bar{R} + \bar{Q}\bar{Y}$ où $R, Q \in K[X]$]
      iii. L'anneau A est factoriel ?
2. Donner un exemple d'un anneau A avec un idéal premier $I \subset A$ qui n'est pas maximal.
3. (a) Soient A, B des anneaux commutatifs et $\phi : A \to B$ un morphisme d'anneaux commutatifs (tel que $\phi(1_A) = 1_B$). Montrer que si $I \subset B$ est un idéal premier alors $\phi^{-1}(I) \subset A$ est un idéal premier.
   (b) Determiner les idéaux maximaux de $\mathbb{R}[X]/(X^2)$.
   [Indication : On pourra considerer le morphisme de réduction $\mathbb{R}[X] \to \mathbb{R}[X]/(X^2)$.]

Exercice 2

Soit A un anneau commutatif unitaire, intègre, A^* le groupe des inversibles de A et $A[X]$ l'anneau de polyômes à coefficients dans A.
Si p est un nombre premier $\mathbb{F}_p$ denote l'aneau quotient $\mathbb{Z}/\mathbb{Z}p$.

1. (a) Montrer que $\forall P, Q \in A[X] \setminus \{0\}$

$$\deg(PQ) = \deg(P) + \deg(Q).$$

   (b) En en déduire que le nombre de racines de P est au plus $\deg(P)$.
2. Soit G un sous groupe fini des inversibles de A.

(a) Soit x un élément $x \in G$ qui maximise l'ordre dans G, c'est-à-dire tel que

$$o(x) \geq o(y), \forall y \in G.$$

Montrer que $o(y)$ divise $o(x)$, $\forall y \in G$.

(b) i. Montrer que G est un groupe cyclique.

ii. En déduire que $H := \{x^2, x \in \mathbb{F}_p^*\}$ est le noyau du morphisme de groupes $\phi : \mathbb{F}_p^* \to \{\bar{1}, \overline{-1}\}$, $y \mapsto y^{(p-1)/2}$.

iii. Montrer que si $a, b \in \mathbb{F}_p^*$ et $a, b \notin H$ alors leur produit $ab \in H$

iv. Monter que $\overline{-1} \in H$ si et seulement si $p = 2$ ou p congru à 1 modulo 4.

(c) Verifier que $\overline{2} \in \mathbb{Z}/13\mathbb{Z}$ est un générateur du groupe des inversibles. Donner une liste de tous les générateurs.

3. Soit $p \neq 2$ un nombre premier et considère $A = \mathbb{F}_p = \mathbb{Z}/\mathbb{Z}p$.

(a) Montrer que $\mathbb{F}_p[X]$ est principal.

(b) Montrer que si $a \in \mathbb{F}_p \setminus \{0\}$ tel que $X^2 + a$ admet une racine dans $\mathbb{F}_p$ alors :

i. $\mathbb{F}_p[X]/(X^2 + a)$ n'est pas intègre

ii. $\mathbb{F}_p[X]/(X^2 + a) \simeq \mathbb{F}_p \times \mathbb{F}_p$.

(c) Pour $p = 5$:

i. Trouver l'inverse de $\overline{3X + 2} \in \mathbb{F}_5[X]/(X^2 + 1)$.

ii. Donner une liste de tous les inversibles de $\mathbb{F}_5[X]/(X^2 + 1)$.

iii. Trouver les $a \in \mathbb{F}_5$ tels que $\mathbb{F}_5[X]/(X^2 + a)$ soit un corps.

(d) i. Montrer que si $\mathbb{F}_p[X]/(X^2 + a)$ est un corps alors il contient exactement p^2 éléments.

ii. Montrer que si $a, b \in \mathbb{F}_p$ tels que $\mathbb{F}_p[X]/(X^2 + a)$ et $\mathbb{F}_p[X]/(X^2 + b)$ sont des corps alors leurs groupes d'inversibles sont isomorphes

iii. Trouver un isomorphisme d'anneaux entre $\mathbb{F}_p[X]/(X^2 + a)$ et $\mathbb{F}_p[X]/(X^2 + b)$. [On pourra considèrer le morphisme

$$\mathbb{F}_p[X] \to \mathbb{F}_p[X],\ P(X) \mapsto P(\alpha X)$$

où $\alpha^2 = ab^{-1}$.]

(e) Pour $p = 13$. Montrer que

$$\mathbb{F}_{13}[X]/(X^3 + 11),\ \mathbb{F}_{13}[X]/(X^3 - 6X^2 + 11X - 6)$$

ne sont pas isomorphe.

4. (a) Montrer que $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$.

(b) Trouver une condition necessaire et sufficient sur p pour que $X^4 + 1$ admet une racine dans $\mathbb{F}_p$.

(c) Montrer que $X^4 + 1$ est réductible dans $\mathbb{F}_p[X]$ pour tout nombre premier p congru à 1 modulo 4.

(d) Montrer que, pour tout nombre premier p, au moins un de $\overline{2}, \overline{-2}, \overline{-1} \in \mathbb{F}_p$ est un carré modulo p. En déduire que $X^4 + 1$ est réductible dans $\mathbb{F}_p[X]$ pour tout nombre premier p.