Contrôle Continu 2

Algèbre – M1 Mathématiques et Informatique Cryptographique

14 novembre 2023

Durée : 1h30. Les documents et les calculatrices ne sont pas autorisés.

Exercice 1. (a) Soit A un anneau et $\mathfrak{p}$ un idéal vérifiant la propriété suivante : pour tous idéaux I_1, I_2 de A tels que $\mathfrak{p}$ contienne $I_1 I_2$, alors $\mathfrak{p}$ contient I_1 ou $\mathfrak{p}$ contient I_2. Montrer que $\mathfrak{p}$ est un idéal premier. Étudier la réciproque.

(b) Soit $f : A \to B$ un morphisme d'anneaux, et $\mathfrak{r}$ un idéal premier de B. Montrer que $f^{-1}(\mathfrak{r})$ est un idéal premier de A. Si $\mathfrak{r}$ est maximal, $f^{-1}(\mathfrak{r})$ est-il nécessairement maximal ?

Exercice 2. Soit $\mathfrak{p}$ un idéal premier non nul de $\mathbb{Z}[X]$.

(a) Montrer que, pour tout $R \in \mathfrak{p}$ non nul, $\mathfrak{p}$ contient l'un des diviseurs irréductibles de R.

(b) Supposons que $\mathfrak{p}$ ne contienne qu'un seul polynôme irréductible P (à inversible près). Montrer que $\mathfrak{p} = (P)$.

(c) Montrer que si $P \in \mathbb{Z}[X]$ est un polynôme irréductible, l'idéal $\mathfrak{p} = (P)$ est premier. Quels sont les irréductibles contenus dans $\mathfrak{p}$?

Dans toute la suite, on suppose que $\mathfrak{p}$ contient au moins deux polynômes irréductibles non associés.

(d) Soient $P, Q \in \mathbb{Z}[X]$ deux polynômes irréductibles non associés. Quel est le pgcd de P, Q dans $\mathbb{Q}[X]$? En déduire qu'il existe un entier $m \geq 1$ et des polynômes $A, B \in \mathbb{Z}[X]$ tels que $A(X)P(X) + B(X)Q(X) = m$.

(e) En déduire que $\mathfrak{p}$ contient un nombre premier p.

(f) Soit $\varphi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ le morphisme de réduction modulo p. Montrer que $\mathfrak{q} := \varphi(\mathfrak{p})$ est un idéal et que $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$. En déduire que $\mathfrak{q}$ est un idéal premier non nul.

(g) Montrer que $\mathfrak{p}$ est engendré par un couple (p, P), où $P \in \mathbb{Z}[X]$ est unitaire et $\varphi(P)$ est irréductible, et que c'est un idéal maximal de $\mathbb{Z}[X]$.

Exercice 3. (a) Pour $q = 2, 3, 7$, décomposer le polynôme $X^3 - X - 1$ en produit de facteurs irréductibles dans $\mathbb{F}_q[X]$.

(b) Démontrer que le polynôme $X^3 - 6X^2 + 9X - 27$ est irréductible dans $\mathbb{Z}[X]$.

(c) Démontrer que le polynôme $2X^3 - 36X^2 - 27X + 21$ est irréductible dans $\mathbb{Z}[X]$.

(d) Lorsque k est un corps, montrer que $Y^2 - X^3 - 1$ est irréductible dans $k[X, Y]$.