ENS Lyon — Algèbre 1
L3 — 2007-2008

TD 3 : Polynômes, corps finis

Exercice 1 Soit A un anneau intègre. Pour tous polynômes non nuls $P, Q \in A[X]$, montrer la formule $\deg(PQ) = \deg P + \deg Q$.

Exercice 2 Soit A un anneau intègre.

1. Montrer que les inversibles de $A[X]$ coïncident avec les inversibles de A.
2. Montrer que cette propriété peut être en défaut lorsque A n'est pas intègre, par exemple pour $A = \mathbb{Z}/4\mathbb{Z}$.

Exercice 3 Soit A un anneau intègre. Montrer que tout irréductible de A est irréductible dans $A[X]$.

Exercice 4 Soit $P = \sum a_i X^i \in A[X]$ et soit $a \in A$.

1. Montrer que P s'écrit de manière unique sous la forme $P = \sum c_i (X - a)^i$.
2. Montrer que les c_i sont des polynômes à coefficients entiers en les a_i et en a.

Exercice 5 Pour quels entiers $n \geq 1$, le polynôme $X^2 + X + 1$ divise-t-il $X^4 + 3X^3 + X^2 + 6X + 10$ dans $\mathbb{Z}/n\mathbb{Z}[X]$?

Exercice 6 Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire.

1. Montrer que toute racine rationnelle de P est nécessairement entière.
2. À quelle classe d'anneaux peut-on généraliser ce résultat ?
3. Montrer que le polynôme $X^3 - X + 1$ n'admet pas de racine rationnelle.

Exercice 7 Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ et p un nombre premier. On suppose les conditions suivantes vérifiées

1. $p \nmid a_n$;
2. Pour tout $k \in \{0, 1, \ldots, n-1\}$, on a $p \mid a_k$;
3. $p^2 \nmid a_0$.

Montrer que P est irréductible dans $\mathbb{Q}[X]$ (on pourra raisonner par l'absurde et montrer que $P = QR$ avec $Q, R \in \mathbb{Z}[X]$ puis considérer le terme constant de P). Ce résultat est connu sous le nom de *critère d'Eisenstein*.

Exercice 8 Décomposer le polynôme $P = X^4 + 1$ en irréductibles dans $\mathbb{C}[X]$, puis dans $\mathbb{R}[X]$. En déduire que P est irréductible dans $\mathbb{Q}[X]$.

Exercice 9 Décomposer les polynômes suivants en irréductibles de $\mathbb{Z}[X]$

$$3X + 6; \quad 4X^2 + 10X + 4; \quad 2X^3 - 2X^2 - X + 1.$$

Exercice 10 Déterminer les noyaux des morphismes suivants

$$\begin{array}{ccc} \mathbb{R}[X] \to \mathbb{R} & \mathbb{R}[X] \to \mathbb{C} & \mathbb{Z}[X] \to \mathbb{R} \\ P \mapsto P(0) & P \mapsto P(i) & P \mapsto P(\sqrt{2}). \end{array}$$

Exercice 11 Montrer que $Y^2 - X^3$ est irréductible dans $\mathbb{C}[X, Y]$ (on pourra se placer dans $\mathbb{C}[X][Y]$, et utiliser le degré d'un polynôme par rapport à Y).

Exercice 12 Soit K un corps de caractéristique $p > 0$.

1. Montrer que l'application de K dans K définie par $x \mapsto x^p$ est un morphisme d'anneaux injectif.
2. Pour tout polynôme $P \in K[X]$, montrer l'identité $P(X)^p = P(X^p)$.

Exercice 13 Expliciter un isomorphisme entre les groupes $\mathbb{F}_5^*$ et $\mathbb{Z}/4\mathbb{Z}$. Combien le groupe $\mathbb{F}_5^*$ possède-t-il de générateurs ?

Exercice 14 Faire la liste des éléments de $\mathbb{F}_7^*$ et déterminer l'ordre de chacun d'entre eux.

Exercice 15 Décomposer le polynôme $X^3 + 1$ en irréductibles dans $\mathbb{F}_2[X]$. Même question dans $\mathbb{F}_3[X]$, puis dans $\mathbb{F}_5[X]$.

Exercice 16 Le but de cet exercice est de montrer que dans un corps fini, tout élément est somme de deux carrés. Soit $\mathbb{F}_q$ un corps fini à q éléments.

1. Si $q = 2^n$, montrer que tout élément de $\mathbb{F}_{2^n}$ est un carré (utiliser l'exercice 12).
2. On suppose q impair. Calculer le cardinal de $S = \{x^2, x \in \mathbb{F}_q\}$ (on pourra considérer le morphisme $x \mapsto x^2$ dans $\mathbb{F}_q^*$).
3. Pour tout $a \in \mathbb{F}_q$, montrer que $S \cap (a - S) \neq \emptyset$.
4. Conclure.

Exercice 17 Soit p un nombre premier impair. On veut montrer le *critère d'Euler* : $x \in \mathbb{F}_p^*$ est un carré si et seulement si $x^{(p-1)/2} = 1$.

1. Montrer l'implication directe.
2. En comptant les carrés de $\mathbb{F}_p^*$ et les racines de $X^{(p-1)/2} - 1$, montrer l'implication réciproque.
3. Résoudre l'équation $x^5 = 1$ dans $\mathbb{F}_{11}$.

Exercice 18 Soit p un nombre premier et n un diviseur de $p - 1$. Montrer que l'équation $x^n = 1$ admet exactement n solutions dans $\mathbb{F}_p$.

Exercice 19

1. Montrer qu'il existe un unique polynôme irréductible de degré 2 dans $\mathbb{F}_2[X]$.
2. Soit p premier impair. Montrer qu'il existe un polynôme de degré 2 irréductible dans $\mathbb{F}_p[X]$ sans racine dans $\mathbb{F}_p$ (on pourra utiliser l'exercice 17).

Exercice 20 Soit p un nombre premier. On travaille dans une clôture algébrique $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$. On rappelle que le corps $\mathbb{F}_{p^n}$ à p^n éléments est défini par

$$\mathbb{F}_{p^n} = \{x \in \overline{\mathbb{F}_p}, x^{p^n} = x\}.$$

Soit $P \in \mathbb{F}_p[X]$ un polynôme irréductible unitaire de degré 2. Le polynôme P est scindé dans $\overline{\mathbb{F}_p}[X]$, soit $P = (X - \alpha)(X - \beta)$ avec $\alpha, \beta \in \overline{\mathbb{F}_p}$.

1. Montrer que $\beta = \alpha^p$ et $\alpha = \beta^p$ (on pourra utiliser l'exercice 12).
2. En déduire que $\alpha, \beta \in \mathbb{F}_{p^2}$.
3. Montrer que P divise $X^{p^2} - X$ dans $\mathbb{F}_p[X]$.