Université Paris Diderot
M1 Arithmétique
2009-2010

Feuille d'exercices VII

Dans cette feuille, p désigne un nombre premier, f est un entier strictement positif et $q = p^f$. Soit en outre $\mathbb{F}$ un corps à q éléments. Soit $A = \mathbb{F}[T]$ l'anneau des polynômes à une variable T et à coefficients dans $\mathbb{F}$. Pour tout polynôme $f \in A$, soit

$$|f| := q^{\deg(f)}.$$

Le symbole P, avec ou sans indice, désigne un élément irréductible dans l'anneau principal A.

Exercice 1 On dit qu'un anneau commutatif et unifère est local s'il n'admet qu'un idéal maximal.

1) Montrer que, si R est un anneau lo-

cal et si $\mathfrak{m}$ est l'idéal maximal de R, alors les éléments dans $R \setminus \mathfrak{m}$ sont inversibles dans R.

2) Soient B un anneau principal et b un élément irréductible dans B. Montrer que, pour tout entier n, l'anneau quotient $B/b^n B$ est local. Déterminer son idéal maximal.

Exercice 2 Pour tout $f \in A$, soit $\varphi(f)$ le cardinal de $(A/fA)^\times$.

1) Montrer que la fonction φ est multiplicative, autrement dit, si f et g sont deux polynômes premiers entre eux, alors $\varphi(fg) = \varphi(f)\varphi(g)$.

2) Soit P un polynôme irréductible. Déterminer $\varphi(P^e)$, où e est un entier strictement positif.

3) En déduire que

$$\varphi(f) = |f| \prod_{P|f} \Big(1 - \frac{1}{|P|}\Big).$$

4) Soient f et g deux polynômes dans A tels que $\mathrm{pgcd}(f, g) = 1$. Montrer que

$$g^{\varphi(f)} \equiv 1 \pmod{f}.$$

5) Soit P un polynôme irréductible dans A. Montrer la relation

$$X^{|P|-1} - 1 \equiv \prod_{0 \leqslant \deg(f) < \deg(P)} (X - f)$$

dans $(A/PA)[X]$.

6) En déduire que, si d est un entier strictement positif qui divise $|P| - 1$, alors le polynôme $X^d - 1$ a exactement d racines distinctes dans $(A/PA)^*$.

7) Montrer que

$$\prod_{0 \leqslant \deg(f) < \deg(P)} f \equiv -1 \pmod{P}.$$

8) Pour tout entier $m \geqslant 1$, soit $f_m(T) = T^{q^m} - T$. Montrer que

$$f_m = \prod_{\substack{P \text{ unitaire} \\ \deg(P) | m}} P.$$

9) En déduire que $\prod_{i=1}^{m} f_i$ est le ppcm des polynômes de degré m.